

Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Konnektor

Version: [5.1011.0 CC](#)
Revision: [242687269785](#)
Stand: [30-0617.08.2020](#)
Status: [zur Abstimmung](#) freigegeben
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemSpec_Kon

Dokumentinformationen

Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
5.1.0	05.10.17		Initialversion Online-Produktivbetrieb (Stufe 2.1)	gematik
5.2.0	18.12.17		Einarbeitung Erratas 1.6.4-1 bis 1.6.4-3, P15.1	gematik
5.3.0	14.05.18		Einarbeitung P15.2, P15.4 und P15.5	gematik
5.4.0	26.10.18		Einarbeitung P15.8 und P15.9	gematik
5.5.0	18.12.19		Einarbeitung P17.1	gematik
5.6.0	15.05.19		Einarbeitung P18.1	gematik
5.7.0	28.06.19		Einarbeitung P19.1	gematik
5.8.0	02.10.19		Einarbeitung P20.1/2	gematik
5.9.0	02.03.20		Einarbeitung P21.1	gematik
5.9.1	26.06.20		Einarbeitung P21.3	gematik
5.10.0	30.06.20		Einarbeitung P22.1	gematik
5.11.0 CC	17.08.20		Einarbeitung Scope-Themen zu R4.0.1 zur Abstimmung freigegeben	gematik

Inhaltsverzeichnis

30	1 Einordnung des Dokumentes	23
31	1.1 Zielsetzung	23
32	1.2 Zielgruppe	23
33	1.3 Geltungsbereich	23
34	1.4 Abgrenzung des Dokuments	24
35	1.5 Methodik	24
36	1.5.1 Anforderungen	24
37	1.5.2 Offene Punkte	24
38	1.5.3 Erläuterungen zur Spezifikation des Außenverhaltens	24
39	1.5.4 Erläuterungen zur Dokumentenstruktur und „Dokumentenmechanismen“	25
40	1.5.4.1 Modulare Spezifikation über Funktionsmerkmale	25
41	1.5.4.2 Technische Use Cases – TUCs	26
42	1.5.4.3 Event Mechanismus	28
43	1.5.4.4 Konfigurationsparameter und Zustandswerte	28
44	2 Systemüberblick	29
45	2.1 Logische Struktur	31
46	2.2 Sicherer Datenspeicher	33
47	2.3 Überblick Konnektoridentität	33
48	2.4 Mandantenfähigkeit	34
49	2.5 Versionierung	34
50	2.6 Fachanwendungen	34
51	2.7 Netzseitige Einsatzszenarien	35
52	2.7.1 Parameter ANLW_ANBINDUNGS_MODUS	35
53	2.7.2 Parameter ANLW_INTERNET_MODUS	35
54	2.8 Lokale und entfernte Kartenterminals	36
55	2.9 Standalone-Szenario	36
56	3 Übergreifende Festlegungen	37
57	3.1 Konnektoridentität und gSMC-K	40
58	3.1.1 Organisatorische Anforderungen und Sperrprozesse	41
59	3.2 Bootup-Phase	43
60	3.3 Betriebszustand	44
61	3.3.1 Betriebsaspekte	57
62	3.4 Fachliche Anbindung der Clientsysteme	58
63	3.4.1 Betriebsaspekte	61
64	3.5 Clientsystemschnittstelle	63
65	3.5.1 SOAP-Schnittstelle	63
66	3.5.2 Statusrückmeldung und Fehlerbehandlung	64
67	3.5.3 Transport großer Dokumente	66

68	3.6 Verwendung manuell importierter CA-Zertifikate	67
69	3.7 Testunterstützung	67
70	4 Funktionsmerkmale	70
71	4.1 Anwendungskonnektor	70
72	4.1.1 Zugriffsberechtigungsdiens	70
73	4.1.1.1 Funktionsmerkmalweite Aspekte	70
74	4.1.1.2 Durch Ereignisse ausgelöste Reaktionen	81
75	4.1.1.3 Interne TUCs, nicht durch Fachmodule nutzbar	81
76	4.1.1.4 Interne TUCs, auch durch Fachmodule nutzbar	81
77	4.1.1.4.1 TUC_KON_000 „Prüfe Zugriffsberechtigung“	81
78	4.1.1.5 Operationen an der Außenschnittstelle	93
79	4.1.1.6 Betriebsaspekte	93
80	4.1.2 Dokumentvalidierungsdienst	93
81	4.1.2.1 Funktionsmerkmalweite Aspekte	94
82	4.1.2.2 Durch Ereignisse ausgelöste Reaktionen	94
83	4.1.2.3 Interne TUCs, nicht durch Fachmodule nutzbar	94
84	4.1.2.4 Interne TUCs, auch durch Fachmodule nutzbar	94
85	4.1.2.4.1 TUC_KON_080 „Dokument validieren“	94
86	4.1.2.5 Operationen an der Außenschnittstelle	97
87	4.1.2.6 Betriebsaspekte	97
88	4.1.3 Dienstverzeichnisdienst	97
89	4.1.3.1 Funktionsmerkmalweite Aspekte	97
90	4.1.3.2 Durch Ereignisse ausgelöste Reaktionen	101
91	4.1.3.3 Interne TUCs, nicht durch Fachmodule nutzbar	101
92	4.1.3.4 Interne TUCs, auch durch Fachmodule nutzbar	101
93	4.1.3.4.1 TUC_KON_041 „Einbringen der Endpunktinformationen während der	
94	Bootup-Phase“	101
95	4.1.3.5 Operationen an der Außenschnittstelle	102
96	4.1.3.6 Betriebsaspekte	103
97	4.1.4 Kartenterminaldienst	104
98	4.1.4.1 Funktionsmerkmalweite Aspekte	108
99	4.1.4.2 Durch Ereignisse ausgelöste Reaktionen	111
100	4.1.4.3 Interne TUCs, nicht durch Fachmodule nutzbar	112
101	4.1.4.3.1 TUC_KON_050 „Beginne Kartenterminalsitzung“	112
102	4.1.4.3.2 TUC_KON_054 „Kartenterminal hinzufügen“	118
103	4.1.4.3.3 TUC_KON_053 „Paire Kartenterminal“	120
104	4.1.4.3.4 TUC_KON_055 „Befülle CT-Object“	125
105	4.1.4.4 Interne TUCs, auch durch Fachmodule nutzbar	126
106	4.1.4.4.1 TUC_KON_051 „Mit Anwender über Kartenterminal interagieren“	126
107	4.1.4.4.2 TUC_KON_056 „Karte anfordern“	128
108	4.1.4.4.3 TUC_KON_057 „Karte auswerfen“	131
109	4.1.4.4.4 TUC_KON_058 „Displaygröße ermitteln“	133
110	4.1.4.5 Operationen an der Außenschnittstelle	135
111	4.1.4.5.1 RequestCard	135
112	4.1.4.5.2 EjectCard	138
113	4.1.4.6 Betriebsaspekte	140

114	4.1.4.6.1 Allgemeine Betriebsaspekte	140
115	4.1.4.6.2 Kartenterminals-pflegen	142
116	4.1.4.6.3 Import der Kartenterminal-Informationen	146
117	4.1.5 Kartendienst	147
118	4.1.5.1 Funktionsmerkmalweite Aspekte	149
119	4.1.5.2 Durch Ereignisse ausgelöste Reaktionen	154
120	4.1.5.3 Interne TUCs, nicht durch Fachmodule nutzbar	155
121	4.1.5.3.1 TUC_KON_001 „Karte öffnen“	155
122	4.1.5.4 Interne TUCs, auch durch Fachmodule nutzbar	157
123	4.1.5.4.1 TUC_KON_026 „Liefere CardSession“	157
124	4.1.5.4.2 TUC_KON_012 „PIN verifizieren“	159
125	4.1.5.4.3 TUC_KON_019 „PIN ändern“	164
126	4.1.5.4.4 TUC_KON_021 „PIN entsperren“	168
127	4.1.5.4.5 TUC_KON_022 „Liefere PIN Status“	172
128	4.1.5.4.6 TUC_KON_027 „PIN Schutz ein /ausschalten“	174
129	4.1.5.4.7 TUC_KON_023 „Karte reservieren“	178
130	4.1.5.4.8 TUC_KON_005 „Card to Card authentisieren“	179
131	4.1.5.4.9 TUC_KON_202 „LeseDatei“	184
132	4.1.5.4.10 TUC_KON_203 „SchreibeDatei“	185
133	4.1.5.4.11 TUC_KON_204 „LöscheDateiInhalt“	188
134	4.1.5.4.12 TUC_KON_209 „LeseRecord“	190
135	4.1.5.4.13 TUC_KON_210 „SchreibeRecord“	192
136	4.1.5.4.14 TUC_KON_211 „LöscheRecordInhalt“	194
137	4.1.5.4.15 TUC_KON_214 „FügeHinzuRecord“	196
138	4.1.5.4.16 TUC_KON_215 „SucheRecord“	198
139	4.1.5.4.17 TUC_KON_018 „eGK-Sperrung prüfen“	200
140	4.1.5.4.18 TUC_KON_006 „Datenzugriffsaudit eGK schreiben“	201
141	4.1.5.4.19 TUC_KON_218 „Signiere“	203
142	4.1.5.4.20 TUC_KON_219 „Entschlüssele“	205
143	4.1.5.4.21 TUC_KON_200 „SendeAPDU“	207
144	4.1.5.4.22 TUC_KON_024 „Karte zurücksetzen“	208
145	4.1.5.4.23 TUC_KON_216 „LeseZertifikat“	210
146	4.1.5.4.24 TUC_KON_036 „LiefereFachlicheRolle“	211
147	4.1.5.5 Operationen an der Außenschnittstelle	213
148	4.1.5.5.1 VerifyPin	214
149	4.1.5.5.2 ChangePin	217
150	4.1.5.5.3 GetPinStatus	220
151	4.1.5.5.4 UnblockPin	223

152	4.1.5.5.5 EnablePin	226
153	4.1.5.5.6 DisablePin	229
154	4.1.5.6 Betriebsaspekte	232
155	4.1.5.6.1 TUC_KON_025 "Initialisierung Kartendienst"	232
156	4.1.5.6.2 Kartenübersicht und PIN-Management	233
157	4.1.6 Systeminformationsdienst	234
158	4.1.6.1 Funktionsmerkmalweite Aspekte	235
159	4.1.6.2 Durch Ereignisse ausgelöste Reaktionen	237
160	4.1.6.3 Interne TUCs, nicht durch Fachmodule nutzbar	237
161	4.1.6.4 Interne TUCs, auch durch Fachmodule nutzbar	237
162	4.1.6.4.1 TUC_KON_256 „Systemereignis absetzen“	237
163	4.1.6.4.2 TUC_KON_252 „Liefere KT_Liste“	242
164	4.1.6.4.3 TUC_KON_253 „Liefere Karten_Liste“	243
165	4.1.6.4.4 TUC_KON_254 „Liefere Ressourcendetails“	245
166	4.1.6.5 Operationen an der Außenschnittstelle	247
167	4.1.6.5.1 GetCardTerminals	248
168	4.1.6.5.2 GetCards	251
169	4.1.6.5.3 GetResourceInformation	256
170	4.1.6.5.4 Subscribe	260
171	4.1.6.5.5 Unsubscribe	263
172	4.1.6.5.6 RenewSubscriptions	264
173	4.1.6.5.7 GetSubscription	267
174	4.1.6.5.8 GetLeCards	269
175	4.1.6.6 Betriebsaspekte	269
176	4.1.7 Verschlüsselungsdienst	270
177	4.1.7.1 Funktionsmerkmalweite Aspekte	270
178	4.1.7.2 Durch Ereignisse ausgelöste Reaktionen	272
179	4.1.7.3 Interne TUCs, nicht durch Fachmodule nutzbar	272
180	4.1.7.4 Interne TUCs, auch durch Fachmodule nutzbar	272
181	4.1.7.4.1 TUC_KON_070 „Daten hybrid verschlüsseln“	272
182	4.1.7.4.2 TUC_KON_071 „Daten hybrid entschlüsseln“	280
183	4.1.7.4.3 TUC_KON_072 „Daten symmetrisch verschlüsseln“	285
184	4.1.7.4.4 TUC_KON_073 „Daten symmetrisch entschlüsseln“	286
185	4.1.7.4.5 TUC_KON_075 „Symmetrisch verschlüsseln“	287
186	4.1.7.4.6 TUC_KON_076 „Symmetrisch entschlüsseln“	289
187	4.1.7.5 Operationen an der Außenschnittstelle	290
188	4.1.7.5.1 EncryptDocument	290
189	4.1.7.5.2 DecryptDocument	303
190	4.1.7.6 Betriebsaspekte	306
191	4.1.8 Signaturdienst	306
192	4.1.8.1 Funktionsmerkmalweite Aspekte	306
193	4.1.8.1.1 Dokumentensignatur	306

194	4.1.8.1.2 Signaturrichtlinien	314
195	4.1.8.1.3 Signaturzeitpunkt	314
196	4.1.8.1.4 Jobnummer	314
197	4.1.8.1.5 Komfortsignatur	316
198	4.1.8.2 Durch Ereignisse ausgelöste Reaktionen	318
199	4.1.8.3 Interne TUCs, nicht durch Fachmodule nutzbar	318
200	4.1.8.3.1 TUC_KON_155 „Dokumente zur Signatur vorbereiten“	319
201	4.1.8.3.2 TUC_KON_165 „Signaturvoraussetzungen für nonQES prüfen“	323
202	4.1.8.3.3 TUC_KON_166 „nonQES Signaturen erstellen“	324
203	4.1.8.3.4 TUC_KON_152 „Signaturvoraussetzungen für QES prüfen“	326
204	4.1.8.3.5 TUC_KON_154 „QES Signaturen erstellen“	327
205	4.1.8.3.6 TUC_KON_168 „Einzelsignatur QES erstellen“	331
206	4.1.8.3.7 TUC_KON_158 „Komfortsignaturen erstellen“	332
207	4.1.8.4 Interne TUCs, auch durch Fachmodule nutzbar	335
208	4.1.8.4.1 TUC_KON_160 „Dokumente nonQES signieren“	335
209	4.1.8.4.2 TUC_KON_161 „nonQES Dokumentsignatur prüfen“	341
210	4.1.8.4.3 TUC_KON_162 „Kryptographische Prüfung der XML-	
211	Dokumentensignatur“	348
212	4.1.8.4.4 TUC_KON_150 „Dokumente QES signieren“	349
213	4.1.8.4.5 Anforderungen an die Stapelsignatur	355
214	4.1.8.4.6 TUC_KON_151 „QES Dokumentensignatur prüfen“	357
215	4.1.8.4.7 TUC_KON_170 „Dokumente mit Komfort signieren“	363
216	4.1.8.4.8 TUC_KON_171 „Komfortsignatur einschalten“	366
217	4.1.8.4.9 TUC_KON_172 „Komfortsignatur ausschalten“	368
218	4.1.8.4.10 TUC_KON_173 „Liefere Signaturmodus“	370
219	4.1.8.5 Operationen an der Außenschnittstelle	372
220	4.1.8.5.1 SignDocument (nonQES und QES)	372
221	4.1.8.5.2 VerifyDocument (nonQES und QES)	386
222	4.1.8.5.3 StopSignature	392
223	4.1.8.5.4 GetJobNumber	393
224	4.1.8.5.5 ActivateComfortSignature	394
225	4.1.8.5.6 DeactivateComfortSignature	396
226	4.1.8.5.7 GetSignatureMode	397
227	4.1.8.6 Betriebsaspekte	399
228	4.1.9 Zertifikatsdienst	401
229	4.1.9.1 Funktionsmerkmalweite Aspekte	401
230	4.1.9.2 Durch Ereignisse ausgelöste Reaktionen	407
231	4.1.9.3 Interne TUCs, nicht durch Fachmodule nutzbar	407
232	4.1.9.3.1 TUC_KON_032 „TSL aktualisieren“	407
233	4.1.9.3.2 TUC_KON_031 „BNetzA-VL aktualisieren“	410

234	4.1.9.3.3 TUC_KON_040 „CRL aktualisieren“	411
235	4.1.9.3.4 TUC_KON_033 „Zertifikatsablauf prüfen“	413
236	4.1.9.4 Interne TUCs, auch durch Fachmodule nutzbar	416
237	4.1.9.4.1 TUC_KON_037 „Zertifikat prüfen“	416
238	4.1.9.4.2 TUC_KON_042 „CV-Zertifikat prüfen“	421
239	4.1.9.4.3 TUC_KON_034 „Zertifikatsinformationen extrahieren“	423
240	4.1.9.5 Operationen an der Außenschnittstelle	426
241	4.1.9.5.1 CheckCertificateExpiration	427
242	4.1.9.5.2 ReadCardCertificate	430
243	4.1.9.5.3 VerifyCertificate	434
244	4.1.9.6 Betriebsaspekte	436
245	4.1.9.6.1 TUC_KON_035 „Zertifikatsdienst initialisieren“	436
246	4.1.10 Protokollierungsdienst	441
247	4.1.10.1 Funktionsmerkmalweite Aspekte	442
248	4.1.10.2 Durch Ereignisse ausgelöste Reaktionen	444
249	4.1.10.3 Interne TUCs, nicht durch Fachmodule nutzbar	444
250	4.1.10.4 Interne TUCs, auch durch Fachmodule nutzbar	444
251	4.1.10.4.1 TUC_KON_271 „Schreibe Protokolleintrag“	444
252	4.1.10.5 Operationen an der Außenschnittstelle	448
253	4.1.10.6 Betriebsaspekte	448
254	4.1.10.6.1 TUC_KON_272 „Initialisierung Protokollierungsdienst“	450
255	4.1.11 TLS Dienst	452
256	4.1.11.1 Funktionsmerkmalweite Aspekte	452
257	4.1.11.2 Durch Ereignisse ausgelöste Reaktionen	452
258	4.1.11.3 Interne TUCs, nicht durch Fachmodule nutzbar	452
259	4.1.11.4 Interne TUCs, auch durch Fachmodule nutzbar	452
260	4.1.11.4.1 TUC_KON_110 „Kartenbasierte TLS-Verbindung aufbauen“	452
261	4.1.11.4.2 TUC_KON_111 „Kartenbasierte TLS-Verbindung abbauen“	454
262	4.1.11.5 Operationen an der Außenschnittstelle	455
263	4.1.11.6 Betriebsaspekte	455
264	4.1.12 LDAP-Proxy	455
265	4.1.12.1 Funktionsmerkmalweite Aspekte	455
266	4.1.12.2 Durch Ereignisse ausgelöste Reaktionen	455
267	4.1.12.3 Interne TUCs, nicht durch Fachmodule nutzbar	455
268	4.1.12.4 Interne TUCs, auch durch Fachmodule nutzbar	456
269	4.1.12.4.1 TUC_KON_290 „LDAP-Verbindung aufbauen“	456
270	4.1.12.4.2 TUC_KON_291 „Verzeichnis abfragen“	457
271	4.1.12.4.3 TUC_KON_292 „LDAP-Verbindung trennen“	457
272	4.1.12.4.4 TUC_KON_293 „Verzeichnisabfrage abbrechen“	458
273	4.1.12.5 Operationen an der Außenschnittstelle	459
274	4.1.12.5.1 Unterstützte LDAPv3-Operationen	459
275	4.1.12.6 Betriebsaspekte	460
276	4.1.13 Authentifizierungsdienst	460
277	4.1.13.1 Funktionsmerkmalweite Aspekte	460
278	4.1.13.1.1 Externe Authentisierung	460

279	4.1.13.2 Durch Ereignisse ausgelöste Reaktionen	461
280	4.1.13.3 Interne TUCs	461
281	4.1.13.4 Operationen an der Außenschnittstelle	461
282	4.1.13.4.1 ExternalAuthenticate	461
283	4.1.13.5 Betriebsaspekte	465
284	4.2 Netzkonnektor	466
285	4.2.1 Anbindung LAN/WAN	466
286	4.2.1.1 Funktionsmerkmalweite Aspekte	466
287	4.2.1.1.1 Netzwerksegmentierung	467
288	4.2.1.1.2 Routing und Firewall	469
289	4.2.1.2 Durch Ereignisse ausgelöste Reaktionen	478
290	4.2.1.3 Interne TUCs, nicht durch Fachmodule nutzbar	478
291	4.2.1.3.1 TUC_KON_305 „LAN Adapter initialisieren“	478
292	4.2.1.3.2 TUC_KON_306 „WAN Adapter initialisieren“	480
293	4.2.1.3.3 TUC_KON_304 „Netzwerk Routen einrichten“	481
294	4.2.1.4 Interne TUCs, auch durch Fachmodule nutzbar	484
295	4.2.1.5 Operationen an der Außenschnittstelle	484
296	4.2.1.6 Betriebsaspekte	484
297	4.2.2 DHCP Server	491
298	4.2.2.1 Funktionsmerkmalweite Aspekte	491
299	4.2.2.2 Durch Ereignisse ausgelöste Reaktionen	491
300	4.2.2.3 Interne TUCs, nicht durch Fachmodule nutzbar	491
301	4.2.2.4 Interne TUCs, auch durch Fachmodule nutzbar	492
302	4.2.2.5 Operationen an der Außenschnittstelle	492
303	4.2.2.5.1 Liefere Netzwerkinformationen über DHCP	492
304	4.2.2.6 Betriebsaspekte	493
305	4.2.2.6.1 TUC_KON_343 „Initialisierung DHCP Server“	496
306	4.2.3 DHCP Client	497
307	4.2.3.1 Funktionsmerkmalweite Aspekte	497
308	4.2.3.2 Durch Ereignisse ausgelöste Reaktionen	498
309	4.2.3.3 Interne TUCs, nicht durch Fachmodule nutzbar	498
310	4.2.3.3.1 TUC_KON_341 „DHCP Informationen beziehen“	498
311	4.2.3.4 Interne TUCs, auch durch Fachmodule nutzbar	499
312	4.2.3.5 Operationen an der Außenschnittstelle	499
313	4.2.3.6 Betriebsaspekte	499
314	4.2.4 VPN Client	500
315	4.2.4.1 Funktionsmerkmalweite Aspekte	500
316	4.2.4.2 Durch Ereignisse ausgelöste Reaktionen	501
317	4.2.4.3 Interne TUCs, nicht durch Fachmodule nutzbar	502
318	4.2.4.3.1 TUC_KON_321 „Verbindung zu dem VPN-Konzentrator der TI	
319	aufbauen“	502
320	4.2.4.3.2 TUC_KON_322 „Verbindung zu dem VPN-Konzentrator des SIS	
321	aufbauen“	504
322	4.2.4.4 Interne TUCs, auch durch Fachmodule nutzbar	507
323	4.2.4.5 Operationen an der Außenschnittstelle	507
324	4.2.4.6 Betriebsaspekte	507
325	4.2.5 Zeitdienst	508
326	4.2.5.1 Funktionsmerkmalweite Aspekte	509

327	4.2.5.2 Durch Ereignisse ausgelöste Reaktionen.....	510
328	4.2.5.3 Interne TUCs, nicht durch Fachmodule nutzbar.....	510
329	4.2.5.4 Interne TUCs, auch durch Fachmodule nutzbar.....	510
330	4.2.5.4.1 TUC_KON_351 „Liefere Systemzeit“.....	510
331	4.2.5.5 Operationen an der Außenschnittstelle.....	511
332	4.2.5.5.1 Sync_Time.....	511
333	4.2.5.6 Betriebsaspekte.....	511
334	4.2.5.6.1 TUC_KON_352 Initialisierung Zeitdienst.....	512
335	4.2.6 Namensdienst und Dienstlokalisierung.....	514
336	4.2.6.1 Funktionsmerkmalweite Aspekte.....	514
337	4.2.6.2 Durch Ereignisse ausgelöste Reaktionen.....	515
338	4.2.6.3 Interne TUCs, nicht durch Fachmodule nutzbar.....	515
339	4.2.6.4 Interne TUCs, auch durch Fachmodule nutzbar.....	516
340	4.2.6.4.1 TUC_KON_361 „DNS-Namen auflösen“.....	516
341	4.2.6.4.2 TUC_KON_362 „Liste der Dienste abrufen“.....	518
342	4.2.6.4.3 TUC_KON_363 „Dienstdetails abrufen“.....	519
343	4.2.6.5 Operationen an der Außenschnittstelle.....	520
344	4.2.6.5.1 GetIPAddress.....	521
345	4.2.6.6 Betriebsaspekte.....	521
346	4.2.7 Optionale Verwendung von IPv6.....	523
347	4.3 Konnektormanagement.....	523
348	4.3.1 Zugang und Benutzerverwaltung des Konnektormanagements.....	526
349	4.3.2 Konnektornamen und Versionsinformationen.....	528
350	4.3.3 Konfigurationsdaten: Persistieren sowie Export-Import.....	529
351	4.3.4 Administration von Fachmodulen.....	531
352	4.3.5 Neustart und Werksreset.....	532
353	4.3.6 Leistungsumfänge und Standalone-Szenarios.....	533
354	4.3.7 Online-Anbindung verwalten.....	534
355	4.3.8 Remote Management (Optional).....	537
356	4.3.9 Software- und Konfigurationsaktualisierung (KSR-Client).....	542
357	4.3.9.1 Funktionsmerkmalweite Aspekte.....	542
358	4.3.9.2 Durch Ereignisse ausgelöste Reaktionen.....	543
359	4.3.9.3 Interne TUCs, nicht durch Fachmodule nutzbar.....	543
360	4.3.9.3.1 TUC_KON_280 „Konnektoraktualisierung durchführen“.....	543
361	4.3.9.3.2 TUC_KON_281 „Kartenterminalaktualisierung anstoßen“.....	548
362	4.3.9.3.3 TUC_KON_282 „UpdateInformationen beziehen“.....	550
363	4.3.9.3.4 TUC_KON_283 „Infrastruktur-Konfiguration aktualisieren“.....	552
364	4.3.9.4 Interne TUCs, auch durch Fachmodule nutzbar.....	556
365	4.3.9.4.1 TUC_KON_285 „UpdateInformationen für Fachmodul beziehen“.....	556
366	4.3.9.4.2 TUC_KON_286 „Paket für Fachmodul laden“.....	558
367	4.3.9.5 Operationen an der Außenschnittstelle.....	560
368	4.3.9.6 Betriebsaspekte.....	560
369	4.3.9.6.1 TUC_KON_284 KSR-Client initialisieren.....	560
370	4.3.10 Konnektorstatus.....	568
371	4.4 Hardware-Merkmale des Konnektors.....	568

372	5 Anhang A – Verzeichnisse	571
373	5.1 Abkürzungen	571
374	5.2 Glossar	573
375	5.3 Abbildungsverzeichnis	573
376	5.4 Tabellenverzeichnis	575
377	5.5 Referenzierte Dokumente	600
378	5.5.1 Dokumente der gematik	600
379	5.5.2 Weitere Dokumente	601
380	6 Anhang B – Profilierung der Signatur und	
381	Verschlüsselungsformate (normativ)	609
382	6.1 Profilierung der Verschlüsselungsformate	609
383	6.2 Profilierung der Signaturformate	609
384	6.3 Profilierung VerificationReport	611
385	6.4 Profilierung der Dokumentenformate und Nachrichten	616
386	7 Anhang D – Übersicht über die verwendeten Versionen	618
387	8 Anhang F – Übersicht Events	627
388	9 Anhang H – Mapping von „Architektur der TI-Plattform“ auf	
389	Konnektorspezifikation	645
390	10 Anhang I – Umsetzungshinweise (informativ)	654
391	10.1 Systemüberblick	654
392	10.1.1 Hinweise zur Sicherheitsevaluierung nach Common Criteria	654
393	10.1.1.1 Separationsmechanismen des Konnektors	654
394	10.1.1.2 Granularität der TSF	655
395	10.2 Übergreifende Festlegungen	656
396	10.2.1 Interne Mechanismen	656
397	10.2.1.1 Zufallszahlen und Schlüssel	656
398	10.3 Funktionsmerkmale	656
399	10.3.1 Anwendungskonnektor	656
400	10.3.1.1 Administration des Informationsmodells	656
401	10.3.1.2 Vorgehensvariante für das Handling von CardSessions	657
402	10.3.1.3 Darstellung von Terminal-Anzeigen auf einem Kartenterminal	658
403	11 Anhang K – Szenarien im dezentralen Umfeld	661
404	11.1 Szenario 1: Einfache Installation ohne spezielle Anforderungen und ohne	
405	bestehende Infrastruktur	661
406	11.1.1 Beschreibung des Szenarios	661
407	11.1.2 Voraussetzungen	662
408	11.1.3 Auswirkungen	662
409	11.2 Szenario 2: Installation mit mehreren Behandlungsräumen	663
410	11.2.1 Beschreibung des Szenarios	663
411	11.2.2 Voraussetzungen	663

412	11.2.3 Auswirkungen	664
413	11.3 Szenario 3: Integration in bestehende Infrastruktur ohne	
414	Netzsegmentierung	664
415	11.3.1 Beschreibung des Szenarios	664
416	11.3.2 Voraussetzungen	665
417	11.3.3 Auswirkungen	665
418	11.4 Szenario 4: Integration in bestehende Infrastruktur mit	
419	Netzsegmentierung	666
420	11.4.1 Beschreibung des Szenarios	666
421	11.4.2 Voraussetzungen	666
422	11.4.3 Auswirkungen	667
423	11.5 Szenario 5: Zentral gesteckter HBA	667
424	11.5.1 Beschreibung des Szenarios	667
425	11.5.2 Voraussetzungen	668
426	11.5.3 Auswirkung	668
427	11.6 Szenario 6: Installation mit zentralem PS	669
428	11.6.1 Beschreibung des Szenarios	669
429	11.6.2 Voraussetzungen	670
430	11.6.3 Auswirkungen	670
431	11.7 Szenario 7: Mehrere Mandanten	671
432	11.7.1 Beschreibung des Szenarios	671
433	11.7.2 Voraussetzungen	671
434	11.7.3 Auswirkungen	672
435	11.8 Szenario 9: Standalone Konnektor – Physische Trennung	673
436	11.8.1 Beschreibung des Szenarios	673
437	11.8.2 Voraussetzungen	674
438	11.8.3 Auswirkung	674
439	12 Anhang L – Datentypen von Eingangs- und Ausgangsdaten..	675
440	1 Einordnung des Dokumentes	23
441	1.1 Zielsetzung	23
442	1.2 Zielgruppe	23
443	1.3 Geltungsbereich	23
444	1.4 Abgrenzung des Dokuments	24
445	1.5 Methodik	24
446	1.5.1 Anforderungen	24
447	1.5.2 Offene Punkte	24
448	1.5.3 Erläuterungen zur Spezifikation des Außenverhaltens	24
449	1.5.4 Erläuterungen zur Dokumentenstruktur und „Dokumentenmechanismen“	25
450	1.5.4.1 Modulare Spezifikation über Funktionsmerkmale	25
451	1.5.4.2 Technische Use Cases - TUCs	26
452	1.5.4.3 Event-Mechanismus	28
453	1.5.4.4 Konfigurationsparameter und Zustandswerte	28
454	2 Systemüberblick	29
455	2.1 Logische Struktur	31

456	2.2 Sicherer Datenspeicher	33
457	2.3 Überblick Konnektoridentität.....	33
458	2.4 Mandantenfähigkeit.....	34
459	2.5 Versionierung	34
460	2.6 Fachanwendungen.....	34
461	2.7 Netzseitige Einsatzszenarien	35
462	2.7.1 Parameter ANLW ANBINDUNGS MODUS	35
463	2.7.2 Parameter ANLW INTERNET MODUS	35
464	2.8 Lokale und entfernte Kartenterminals	36
465	2.9 Standalone-Szenario	36
466	3 Übergreifende Festlegungen	37
467	3.1 Konnektoridentität und gSMC-K	40
468	3.1.1 Organisatorische Anforderungen und Sperrprozesse	41
469	3.2 Bootup-Phase	43
470	3.3 Betriebszustand.....	44
471	3.3.1 Betriebsaspekte	57
472	3.4 Fachliche Anbindung der Clientsysteme	58
473	3.4.1 Betriebsaspekte	61
474	3.5 Clientsystemschnittstelle	63
475	3.5.1 SOAP-Schnittstelle	63
476	3.5.2 Statusrückmeldung und Fehlerbehandlung	64
477	3.5.3 Transport großer Dokumente.....	66
478	3.6 Verwendung manuell importierter CA-Zertifikate	67
479	3.7 Testunterstützung	67
480	4 Funktionsmerkmale	70
481	4.1 Anwendungskonnektor.....	70
482	4.1.1 Zugriffsberechtigungsdienst	70
483	4.1.1.1 Funktionsmerkmalweite Aspekte	70
484	4.1.1.2 Durch Ereignisse ausgelöste Reaktionen.....	81
485	4.1.1.3 Interne TUCs, nicht durch Fachmodule nutzbar	81
486	4.1.1.4 Interne TUCs, auch durch Fachmodule nutzbar	81
487	4.1.1.4.1 TUC KON 000 „Prüfe Zugriffsberechtigung“	81
488	4.1.1.5 Operationen an der Außenschnittstelle	93
489	4.1.1.6 Betriebsaspekte	93
490	4.1.2 Dokumentvalidierungsdienst.....	93
491	4.1.2.1 Funktionsmerkmalweite Aspekte	94
492	4.1.2.2 Durch Ereignisse ausgelöste Reaktionen.....	94
493	4.1.2.3 Interne TUCs, nicht durch Fachmodule nutzbar	94
494	4.1.2.4 Interne TUCs, auch durch Fachmodule nutzbar	94
495	4.1.2.4.1 TUC KON 080 „Dokument validieren“	94
496	4.1.2.5 Operationen an der Außenschnittstelle	97
497	4.1.2.6 Betriebsaspekte	97
498	4.1.3 Dienstverzeichnisdienst.....	97

499	4.1.3.1 Funktionsmerkmalweite Aspekte	97
500	4.1.3.2 Durch Ereignisse ausgelöste Reaktionen	101
501	4.1.3.3 Interne TUCs, nicht durch Fachmodule nutzbar	101
502	4.1.3.4 Interne TUCs, auch durch Fachmodule nutzbar	101
503	4.1.3.4.1 TUC KON 041 „Einbringen der Endpunkthinformationen während der	
504	Bootup-Phase“	101
505	4.1.3.5 Operationen an der Außenschnittstelle	102
506	4.1.3.6 Betriebsaspekte	103
507	4.1.4 Kartenterminaldienst	104
508	4.1.4.1 Funktionsmerkmalweite Aspekte	108
509	4.1.4.2 Durch Ereignisse ausgelöste Reaktionen	111
510	4.1.4.3 Interne TUCs, nicht durch Fachmodule nutzbar	112
511	4.1.4.3.1 TUC KON 050 „Beginne Kartenterminalsitzung“	112
512	4.1.4.3.2 TUC KON 054 „Kartenterminal hinzufügen“	118
513	4.1.4.3.3 TUC KON 053 „Paire Kartenterminal“	120
514	4.1.4.3.4 TUC KON 055 „Befülle CT-Object“	125
515	4.1.4.4 Interne TUCs, auch durch Fachmodule nutzbar	126
516	4.1.4.4.1 TUC KON 051 „Mit Anwender über Kartenterminal interagieren“ ...	126
517	4.1.4.4.2 TUC KON 056 „Karte anfordern“	128
518	4.1.4.4.3 TUC KON 057 „Karte auswerfen“	131
519	4.1.4.4.4 TUC KON 058 „Displaygröße ermitteln“	133
520	4.1.4.5 Operationen an der Außenschnittstelle	135
521	4.1.4.5.1 RequestCard	135
522	4.1.4.5.2 EjectCard	138
523	4.1.4.6 Betriebsaspekte	140
524	4.1.4.6.1 Allgemeine Betriebsaspekte	140
525	4.1.4.6.2 Kartenterminals pflegen	142
526	4.1.4.6.3 Import der Kartenterminal-Informationen	146
527	4.1.5 Kartendienst	147
528	4.1.5.1 Funktionsmerkmalweite Aspekte	149
529	4.1.5.2 Durch Ereignisse ausgelöste Reaktionen	154
530	4.1.5.3 Interne TUCs, nicht durch Fachmodule nutzbar	155
531	4.1.5.3.1 TUC KON 001 „Karte öffnen“	155
532	4.1.5.4 Interne TUCs, auch durch Fachmodule nutzbar	157
533	4.1.5.4.1 TUC KON 026 „Liefere CardSession“	157
534	4.1.5.4.2 TUC KON 012 „PIN verifizieren“	159
535	4.1.5.4.3 TUC KON 019 „PIN ändern“	164
536	4.1.5.4.4 TUC KON 021 „PIN entsperren“	168
537	4.1.5.4.5 TUC KON 022 „Liefere PIN-Status“	172
538	4.1.5.4.6 TUC KON 027 „PIN-Schutz ein-/ausschalten“	174
539	4.1.5.4.7 TUC KON 023 „Karte reservieren“	178
540	4.1.5.4.8 TUC KON 005 „Card-to-Card authentisieren“	179
541	4.1.5.4.9 TUC KON 202 „LeseDatei“	184

542	4.1.5.4.10 TUC KON 203 „SchreibeDatei“	185
543	4.1.5.4.11 TUC KON 204 „LöscheDateiInhalt“	188
544	4.1.5.4.12 TUC KON 209 „LeseRecord“	190
545	4.1.5.4.13 TUC KON 210 „SchreibeRecord“	192
546	4.1.5.4.14 TUC KON 211 „LöscheRecordInhalt“	194
547	4.1.5.4.15 TUC KON 214 „FügeHinzuRecord“	196
548	4.1.5.4.16 TUC KON 215 „SucheRecord“	198
549	4.1.5.4.17 TUC KON 018 „eGK-Sperrung prüfen“	200
550	4.1.5.4.18 TUC KON 006 „Datenzugriffsaudit eGK schreiben“	201
551	4.1.5.4.19 TUC KON 218 „Signiere“	203
552	4.1.5.4.20 TUC KON 219 „Entschlüssele“	205
553	4.1.5.4.21 TUC KON 200 „SendeAPDU“	207
554	4.1.5.4.22 TUC KON 024 „Karte zurücksetzen“	208
555	4.1.5.4.23 TUC KON 216 „LeseZertifikat“	210
556	4.1.5.4.24 TUC KON 036 „LiefereFachlicheRolle“	211
557	4.1.5.5 Operationen an der Außenschnittstelle	213
558	4.1.5.5.1 VerifyPin	214
559	4.1.5.5.2 ChangePin	217
560	4.1.5.5.3 GetPinStatus	220
561	4.1.5.5.4 UnblockPin	223
562	4.1.5.5.5 EnablePin	226
563	4.1.5.5.6 DisablePin	229
564	4.1.5.6 Betriebsaspekte	232
565	4.1.5.6.1 TUC KON 025 "Initialisierung Kartendienst"	232
566	4.1.5.6.2 Kartenübersicht und PIN-Management	233
567	4.1.6 Systeminformationsdienst	234
568	4.1.6.1 Funktionsmerkmalweite Aspekte	235
569	4.1.6.2 Durch Ereignisse ausgelöste Reaktionen	237
570	4.1.6.3 Interne TUCs, nicht durch Fachmodule nutzbar	237
571	4.1.6.4 Interne TUCs, auch durch Fachmodule nutzbar	237
572	4.1.6.4.1 TUC KON 256 „Systemereignis absetzen“	237
573	4.1.6.4.2 TUC KON 252 „Liefere KT Liste“	242
574	4.1.6.4.3 TUC KON 253 „Liefere Karten Liste“	243
575	4.1.6.4.4 TUC KON 254 „Liefere Ressourcendetails“	245
576	4.1.6.5 Operationen an der Außenschnittstelle	247
577	4.1.6.5.1 GetCardTerminals	248
578	4.1.6.5.2 GetCards	251
579	4.1.6.5.3 GetResourceInformation	256
580	4.1.6.5.4 Subscribe	260

581	4.1.6.5.5 Unsubscribe	263
582	4.1.6.5.6 RenewSubscriptions	264
583	4.1.6.5.7 GetSubscription	267
584	4.1.6.5.8 GetLeCards	269
585	4.1.6.6 Betriebsaspekte	269
586	4.1.7 Verschlüsselungsdienst	270
587	4.1.7.1 Funktionsmerkmalweite Aspekte	270
588	4.1.7.2 Durch Ereignisse ausgelöste Reaktionen	272
589	4.1.7.3 Interne TUCs, nicht durch Fachmodule nutzbar	272
590	4.1.7.4 Interne TUCs, auch durch Fachmodule nutzbar	272
591	4.1.7.4.1 TUC KON 070 „Daten hybrid verschlüsseln“	272
592	4.1.7.4.2 TUC KON 071 „Daten hybrid entschlüsseln“	280
593	4.1.7.4.3 TUC KON 072 „Daten symmetrisch verschlüsseln“	285
594	4.1.7.4.4 TUC KON 073 „Daten symmetrisch entschlüsseln“	286
595	4.1.7.4.5 TUC KON 075 „Symmetrisch verschlüsseln“	287
596	4.1.7.4.6 TUC KON 076 „Symmetrisch entschlüsseln“	289
597	4.1.7.5 Operationen an der Außenschnittstelle	290
598	4.1.7.5.1 EncryptDocument	290
599	4.1.7.5.2 DecryptDocument	303
600	4.1.7.6 Betriebsaspekte	306
601	4.1.8 Signaturdienst	306
602	4.1.8.1 Funktionsmerkmalweite Aspekte	306
603	4.1.8.1.1 Dokumentensignatur	306
604	4.1.8.1.2 Signaturrichtlinien	314
605	4.1.8.1.3 Signaturzeitpunkt	314
606	4.1.8.1.4 Jobnummer	314
607	4.1.8.1.5 Komfortsignatur	316
608	4.1.8.2 Durch Ereignisse ausgelöste Reaktionen	318
609	4.1.8.3 Interne TUCs, nicht durch Fachmodule nutzbar	318
610	4.1.8.3.1 TUC KON 155 „Dokumente zur Signatur vorbereiten“	319
611	4.1.8.3.2 TUC KON 165 „Signaturvoraussetzungen für nonQES prüfen“	323
612	4.1.8.3.3 TUC KON 166 „nonQES Signaturen erstellen“	324
613	4.1.8.3.4 TUC KON 152 "Signaturvoraussetzungen für QES prüfen"	326
614	4.1.8.3.5 TUC KON 154 "QES Signaturen erstellen"	327
615	4.1.8.3.6 TUC KON 168 „Einzelsignatur QES erstellen“	331
616	4.1.8.3.7 TUC KON 158 "Komfortsignaturen erstellen"	332
617	4.1.8.4 Interne TUCs, auch durch Fachmodule nutzbar	335
618	4.1.8.4.1 TUC KON 160 „Dokumente nonQES signieren“	335
619	4.1.8.4.2 TUC KON 161 „nonQES Dokumentsignatur prüfen “	341
620	4.1.8.4.3 TUC KON 162 „Kryptographische Prüfung der XML-	
621	Dokumentensignatur“	348

622	4.1.8.4.4 TUC KON 150 „Dokumente QES signieren“	349
623	4.1.8.4.5 Anforderungen an die Stapelsignatur	355
624	4.1.8.4.6 TUC KON 151 „QES Dokumentensignatur prüfen“	357
625	4.1.8.4.7 TUC KON 170 „Dokumente mit Komfort signieren“	363
626	4.1.8.4.8 TUC KON 171 „Komfortsignatur einschalten“	366
627	4.1.8.4.9 TUC KON 172 „Komfortsignatur ausschalten“	368
628	4.1.8.4.10 TUC KON 173 „Liefere Signaturmodus“	370
629	4.1.8.5 Operationen an der Außenschnittstelle	372
630	4.1.8.5.1 SignDocument (nonQES und QES)	372
631	4.1.8.5.2 VerifyDocument (nonQES und QES)	386
632	4.1.8.5.3 StopSignature	392
633	4.1.8.5.4 GetJobNumber	393
634	4.1.8.5.5 ActivateComfortSignature	394
635	4.1.8.5.6 DeactivateComfortSignature	396
636	4.1.8.5.7 GetSignatureMode	397
637	4.1.8.6 Betriebsaspekte	399
638	4.1.9 Zertifikatsdienst	401
639	4.1.9.1 Funktionsmerkmalweite Aspekte	401
640	4.1.9.2 Durch Ereignisse ausgelöste Reaktionen	407
641	4.1.9.3 Interne TUCs, nicht durch Fachmodule nutzbar	407
642	4.1.9.3.1 TUC KON 032 „TSL aktualisieren“	407
643	4.1.9.3.2 TUC KON 031 „BNetzA-VL aktualisieren“	410
644	4.1.9.3.3 TUC KON 040 „CRL aktualisieren“	411
645	4.1.9.3.4 TUC KON 033 „Zertifikatsablauf prüfen“	413
646	4.1.9.4 Interne TUCs, auch durch Fachmodule nutzbar	416
647	4.1.9.4.1 TUC KON 037 „Zertifikat prüfen“	416
648	4.1.9.4.2 TUC KON 042 „CV-Zertifikat prüfen“	421
649	4.1.9.4.3 TUC KON 034 „Zertifikatsinformationen extrahieren“	423
650	4.1.9.5 Operationen an der Außenschnittstelle	426
651	4.1.9.5.1 CheckCertificateExpiration	427
652	4.1.9.5.2 ReadCardCertificate	430
653	4.1.9.5.3 VerifyCertificate	434
654	4.1.9.6 Betriebsaspekte	436
655	4.1.9.6.1 TUC KON 035 „Zertifikatsdienst initialisieren“	436
656	4.1.10 Protokollierungsdienst	441
657	4.1.10.1 Funktionsmerkmalweite Aspekte	442
658	4.1.10.2 Durch Ereignisse ausgelöste Reaktionen	444
659	4.1.10.3 Interne TUCs, nicht durch Fachmodule nutzbar	444
660	4.1.10.4 Interne TUCs, auch durch Fachmodule nutzbar	444
661	4.1.10.4.1 TUC KON 271 „Schreibe Protokolleintrag“	444
662	4.1.10.5 Operationen an der Außenschnittstelle	448

663	4.1.10.6 Betriebsaspekte	448
664	4.1.10.6.1 TUC KON 272 „Initialisierung Protokollierungsdienst	450
665	4.1.11 TLS-Dienst	452
666	4.1.11.1 Funktionsmerkmalweite Aspekte	452
667	4.1.11.2 Durch Ereignisse ausgelöste Reaktionen	452
668	4.1.11.3 Interne TUCs, nicht durch Fachmodule nutzbar	452
669	4.1.11.4 Interne TUCs, auch durch Fachmodule nutzbar.....	452
670	4.1.11.4.1 TUC KON 110 „Kartenbasierte TLS-Verbindung aufbauen“	452
671	4.1.11.4.2 TUC KON 111 „Kartenbasierte TLS-Verbindung abbauen“	454
672	4.1.11.5 Operationen an der Außenschnittstelle	455
673	4.1.11.6 Betriebsaspekte	455
674	4.1.12 LDAP-Proxy	455
675	4.1.12.1 Funktionsmerkmalweite Aspekte	455
676	4.1.12.2 Durch Ereignisse ausgelöste Reaktionen	455
677	4.1.12.3 Interne TUCs, nicht durch Fachmodule nutzbar	455
678	4.1.12.4 Interne TUCs, auch durch Fachmodule nutzbar.....	456
679	4.1.12.4.1 TUC KON 290 „LDAP-Verbindung aufbauen“	456
680	4.1.12.4.2 TUC KON 291 „Verzeichnis abfragen“	457
681	4.1.12.4.3 TUC KON 292 „LDAP-Verbindung trennen“	457
682	4.1.12.4.4 TUC KON 293 „Verzeichnisabfrage abbuchen“	458
683	4.1.12.5 Operationen an der Außenschnittstelle	459
684	4.1.12.5.1 Unterstützte LDAPv3 Operationen	459
685	4.1.12.6 Betriebsaspekte	460
686	4.1.13 Authentifizierungsdienst.....	460
687	4.1.13.1 Funktionsmerkmalweite Aspekte	460
688	4.1.13.1.1 Externe Authentisierung	460
689	4.1.13.2 Durch Ereignisse ausgelöste Reaktionen	461
690	4.1.13.3 Interne TUCs	461
691	4.1.13.4 Operationen an der Außenschnittstelle	461
692	4.1.13.4.1 ExternalAuthenticate	461
693	4.1.13.5 Betriebsaspekte	465
694	4.2 Netzkonnektor.....	466
695	4.2.1 Anbindung LAN/WAN	466
696	4.2.1.1 Funktionsmerkmalweite Aspekte	466
697	4.2.1.1.1 Netzwerksegmentierung.....	467
698	4.2.1.1.2 Routing und Firewall	469
699	4.2.1.2 Durch Ereignisse ausgelöste Reaktionen.....	478
700	4.2.1.3 Interne TUCs, nicht durch Fachmodule nutzbar	478
701	4.2.1.3.1 TUC KON 305 „LAN-Adapter initialisieren“	478
702	4.2.1.3.2 TUC KON 306 „WAN-Adapter initialisieren“	480
703	4.2.1.3.3 TUC KON 304 „Netzwerk-Routen einrichten“	481
704	4.2.1.4 Interne TUCs, auch durch Fachmodule nutzbar	484
705	4.2.1.5 Operationen an der Außenschnittstelle	484
706	4.2.1.6 Betriebsaspekte	484
707	4.2.2 DHCP-Server	491
708	4.2.2.1 Funktionsmerkmalweite Aspekte	491

709	4.2.2.2 Durch Ereignisse ausgelöste Reaktionen	491
710	4.2.2.3 Interne TUCs, nicht durch Fachmodule nutzbar	491
711	4.2.2.4 Interne TUCs, auch durch Fachmodule nutzbar	492
712	4.2.2.5 Operationen an der Außenschnittstelle	492
713	4.2.2.5.1 Liefere Netzwerkinformationen über DHCP	492
714	4.2.2.6 Betriebsaspekte	493
715	4.2.2.6.1 TUC KON 343 „Initialisierung DHCP-Server“	496
716	4.2.3 DHCP-Client	497
717	4.2.3.1 Funktionsmerkmalweite Aspekte	497
718	4.2.3.2 Durch Ereignisse ausgelöste Reaktionen	498
719	4.2.3.3 Interne TUCs, nicht durch Fachmodule nutzbar	498
720	4.2.3.3.1 TUC KON 341 „DHCP-Informationen beziehen“	498
721	4.2.3.4 Interne TUCs, auch durch Fachmodule nutzbar	499
722	4.2.3.5 Operationen an der Außenschnittstelle	499
723	4.2.3.6 Betriebsaspekte	499
724	4.2.4 VPN-Client.....	500
725	4.2.4.1 Funktionsmerkmalweite Aspekte	500
726	4.2.4.2 Durch Ereignisse ausgelöste Reaktionen	501
727	4.2.4.3 Interne TUCs, nicht durch Fachmodule nutzbar	502
728	4.2.4.3.1 TUC KON 321 „Verbindung zu dem VPN-Konzentrator der TI	
729	aufbauen“	502
730	4.2.4.3.2 TUC KON 322 „Verbindung zu dem VPN-Konzentrator des SIS	
731	aufbauen“	504
732	4.2.4.4 Interne TUCs, auch durch Fachmodule nutzbar	507
733	4.2.4.5 Operationen an der Außenschnittstelle	507
734	4.2.4.6 Betriebsaspekte	507
735	4.2.5 Zeitdienst.....	508
736	4.2.5.1 Funktionsmerkmalweite Aspekte	509
737	4.2.5.2 Durch Ereignisse ausgelöste Reaktionen	510
738	4.2.5.3 Interne TUCs, nicht durch Fachmodule nutzbar	510
739	4.2.5.4 Interne TUCs, auch durch Fachmodule nutzbar	510
740	4.2.5.4.1 TUC KON 351 „Liefere Systemzeit“	510
741	4.2.5.5 Operationen an der Außenschnittstelle	511
742	4.2.5.5.1 Sync Time	511
743	4.2.5.6 Betriebsaspekte	511
744	4.2.5.6.1 TUC KON 352 Initialisierung Zeitdienst	512
745	4.2.6 Namensdienst und Dienstlokalisierung	514
746	4.2.6.1 Funktionsmerkmalweite Aspekte	514
747	4.2.6.2 Durch Ereignisse ausgelöste Reaktionen	515
748	4.2.6.3 Interne TUCs, nicht durch Fachmodule nutzbar	515
749	4.2.6.4 Interne TUCs, auch durch Fachmodule nutzbar	516
750	4.2.6.4.1 TUC KON 361 „DNS-Namen auflösen“	516
751	4.2.6.4.2 TUC KON 362 „Liste der Dienste abrufen“	518
752	4.2.6.4.3 TUC KON 363 „Dienstdetails abrufen“	519
753	4.2.6.5 Operationen an der Außenschnittstelle	520
754	4.2.6.5.1 GetIPAddress	521
755	4.2.6.6 Betriebsaspekte	521
756	4.2.7 Optionale Verwendung von IPv6	523

757	4.3 Konnektormanagement	523
758	4.3.1 Zugang und Benutzerverwaltung des Konnektormanagements	526
759	4.3.2 Konnektorname und Versionsinformationen	528
760	4.3.3 Konfigurationsdaten: Persistieren sowie Export-Import	529
761	4.3.4 Administration von Fachmodulen	531
762	4.3.5 Neustart und Werksreset	532
763	4.3.6 Leistungsumfänge und Standalone-Szenarios	533
764	4.3.7 Online-Anbindung verwalten	534
765	4.3.8 Remote Management (Optional)	537
766	4.3.9 Software- und Konfigurationsaktualisierung (KSR-Client)	542
767	4.3.9.1 Funktionsmerkmalweite Aspekte	542
768	4.3.9.2 Durch Ereignisse ausgelöste Reaktionen	543
769	4.3.9.3 Interne TUCs, nicht durch Fachmodule nutzbar	543
770	4.3.9.3.1 TUC KON 280 „Konnektoraktualisierung durchführen“	543
771	4.3.9.3.2 TUC KON 281 „Kartenterminalaktualisierung anstoßen“	548
772	4.3.9.3.3 TUC KON 282 „UpdateInformationen beziehen“	550
773	4.3.9.3.4 TUC KON 283 „Infrastruktur Konfiguration aktualisieren“	552
774	4.3.9.4 Interne TUCs, auch durch Fachmodule nutzbar	556
775	4.3.9.4.1 TUC KON 285 „UpdateInformationen für Fachmodul beziehen“	556
776	4.3.9.4.2 TUC KON 286 „Paket für Fachmodul laden“	558
777	4.3.9.5 Operationen an der Außenschnittstelle	560
778	4.3.9.6 Betriebsaspekte	560
779	4.3.9.6.1 TUC KON 284 KSR-Client initialisieren	560
780	4.3.10 Konnektorstatus	568
781	4.4 Hardware-Merkmale des Konnektors	568
782	5 Anhang A – Verzeichnisse	571
783	5.1 Abkürzungen	571
784	5.2 Glossar	573
785	5.3 Abbildungsverzeichnis	573
786	5.4 Tabellenverzeichnis	575
787	5.5 Referenzierte Dokumente	600
788	5.5.1 Dokumente der gematik	600
789	5.5.2 Weitere Dokumente	601
790	6 Anhang B – Profilierung der Signatur- und	
791	Verschlüsselungsformate (normativ)	609
792	6.1 Profilierung der Verschlüsselungsformate	609
793	6.2 Profilierung der Signaturformate	609
794	6.3 Profilierung VerificationReport	611
795	6.4 Profilierung der Dokumentenformate und Nachrichten	616
796	7 Anhang D – Übersicht über die verwendeten Versionen	618
797	8 Anhang F – Übersicht Events	627

798	9 Anhang H – Mapping von „Architektur der TI-Plattform“ auf	
799	Konnektorspezifikation	645
800	10 Anhang I – Umsetzungshinweise (informativ)	654
801	10.1 Systemüberblick	654
802	10.1.1 – Hinweise zur Sicherheitsevaluierung nach Common Criteria	654
803	10.1.1.1 Separationsmechanismen des Konnektors	654
804	10.1.1.2 Granularität der TSF	655
805	10.2 Übergreifende Festlegungen	656
806	10.2.1 Interne Mechanismen	656
807	10.2.1.1 Zufallszahlen und Schlüssel	656
808	10.3 Funktionsmerkmale	656
809	10.3.1 Anwendungskonnektor	656
810	10.3.1.1 Administration des Informationsmodells	656
811	10.3.1.2 Vorgehensvariante für das Handling von CardSessions	657
812	10.3.1.3 Darstellung von Terminal-Anzeigen auf einem Kartenterminal	658
813	11 Anhang K – Szenarien im dezentralen Umfeld	661
814	11.1 Szenario 1: Einfache Installation ohne spezielle Anforderungen und ohne	
815	bestehende Infrastruktur	661
816	11.1.1 Beschreibung des Szenarios	661
817	11.1.2 Voraussetzungen	662
818	11.1.3 Auswirkungen	662
819	11.2 Szenario 2: Installation mit mehreren Behandlungsräumen	663
820	11.2.1 Beschreibung des Szenarios	663
821	11.2.2 Voraussetzungen	663
822	11.2.3 Auswirkungen	664
823	11.3 Szenario 3: Integration in bestehende Infrastruktur ohne	
824	Netzsegmentierung	664
825	11.3.1 Beschreibung des Szenarios	664
826	11.3.2 Voraussetzungen	665
827	11.3.3 Auswirkungen	665
828	11.4 Szenario 4: Integration in bestehende Infrastruktur mit	
829	Netzsegmentierung	666
830	11.4.1 Beschreibung des Szenarios	666
831	11.4.2 Voraussetzungen	666
832	11.4.3 Auswirkungen	667
833	11.5 Szenario 5: Zentral gesteckter HBA	667
834	11.5.1 Beschreibung des Szenarios	667
835	11.5.2 Voraussetzungen	668
836	11.5.3 Auswirkung	668
837	11.6 Szenario 6: Installation mit zentralem PS	669
838	11.6.1 Beschreibung des Szenarios	669
839	11.6.2 Voraussetzungen	670
840	11.6.3 Auswirkungen	670
841	11.7 Szenario 7: Mehrere Mandanten	671
842	11.7.1 Beschreibung des Szenarios	671
843	11.7.2 Voraussetzungen	671
844	11.7.3 Auswirkungen	672

845	<u>11.8 Szenario 9: Standalone Konnektor - Physische Trennung</u>	673
846	<u>11.8.1 Beschreibung des Szenarios.....</u>	673
847	<u>11.8.2 Voraussetzungen.....</u>	674
848	<u>11.8.3 Auswirkung</u>	674
849	<u>12 Anhang L – Datentypen von Eingangs- und Ausgangsdaten..</u>	675
850		

ENTWURF

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb des Produkttyps Konnektor.

Dieses Dokument beschreibt die dezentrale Komponente zur sicheren Anbindung von Clientsystemen der Institutionen und Organisationen des Gesundheitswesens an die Telematikinfrastruktur – den Konnektor. Der Konnektor ist einerseits verantwortlich für den Zugriff auf die in der Einsatzumgebung befindlichen Kartenterminals sowie Karten und andererseits für die Kommunikation mit den zentralen Diensten der TI-Plattform und fachanwendungsspezifischen Diensten. Aus den Kommunikationsbeziehungen mit Clientsystem, Kartenterminals, Karten und zentralen Diensten der TI-Plattform und fachanwendungsspezifischen Diensten resultieren vom Konnektor anzubietende Schnittstellen, die gemeinsam in diesem Dokument sowie den fachanwendungsspezifischen Fachmodulspezifikationen normativ geregelt werden. Vom Konnektor genutzte Schnittstellen liegen zumeist in anderen Verantwortungsbereichen (zentrale TI-Plattform aber auch Schnittstellen der Kartenterminals und Karten). Diese werden in den übergreifenden Spezifikationen der TI sowie den Produkttypspezifikationen definiert.

Dieses Dokument regelt somit nur einen Teil des Konnektors (wenngleich auch den Wesentlichen). Für die Implementierung eines Konnektors ist entsprechend die Kenntnis aller weiteren Spezifikationen erforderlich. Die Gesamtheit aller für den Konnektor relevanten Dokumente wird im Produkttypsteckbrief des Konnektors erhoben.

1.2 Zielgruppe

Das Dokument richtet sich an Konnektorhersteller sowie Hersteller und Anbieter von Produkttypen (dies beinhaltet auch die Anbieter zur G2-Ausschreibung), die hierzu eine Schnittstelle besitzen.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des Deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren werden durch die gematik GmbH in gesonderten Dokumenten (z. B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Wichtiger Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen

890 Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik
891 GmbH übernimmt insofern keinerlei Gewährleistungen.

892 1.4 Abgrenzung des Dokuments

893 Spezifiziert werden in dem Dokument die von dem Produkttyp bereitgestellten
894 (angebotenen) Schnittstellen. Benutzte Schnittstellen werden hingegen in der
895 Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt.
896 Auf die entsprechenden Dokumente wird referenziert.

897 Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept-
898 und Spezifikationsdokumenten, diese sind in dem Produkttypsteckbrief des Produkttyps
899 Konnektor verzeichnet.

900 1.5 Methodik

901 1.5.1 Anforderungen

902 Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID
903 sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen
904 deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN
905 gekennzeichnet.

906 Sie werden im Dokument wie folgt dargestellt:

907 **<AFO-ID> - <Titel der Afo>**

908 Text / Beschreibung

909 [**<=>**]

910

911 Dabei umfasst die Anforderung sämtliche innerhalb der Afo-ID und der Textmarke
912 angeführten Inhalte.

913 1.5.2 Offene Punkte

914 Zum Zeitpunkt der Spezifikationserstellung konnten nicht alle Details abschließend
915 geklärt werden, insbesondere, da Abstimmungsbedarf mit der umsetzenden Industrie
916 besteht. Details, die keine produkttypübergreifenden Auswirkungen haben und die im
917 Rahmen des Verhandlungsverfahrens mit der Industrie besprochen werden müssen,
918 werden als „Offene Punkte“ ausgewiesen und wie folgt im Dokument kenntlich gemacht:

919 Die XYZ müssen noch definiert werden.

Die XYZ müssen noch definiert werden.

920

921

922 1.5.3 Erläuterungen zur Spezifikation des Außenverhaltens

923 Der Konnektor stellt einen vergleichsweise komplexen Produkttyp dar, dessen
924 Beschreibung eine Herausforderung darstellt und somit in vielen verschiedenen Varianten

925 möglich wäre. An dieser Stelle folgen daher wesentliche Informationen, die das korrekte
926 Verstehen der Spezifikation fördern:

927 Die Spezifikation des Konnektors ist eine Black-Box-Spezifikation, das heißt alle
928 Festlegungen dienen ausschließlich der Beschreibung des von der Komponente
929 verlangten Verhaltens an der Außenschnittstelle.

930 Normative Festlegungen, die eine Festlegung des inneren Verhalten vermuten lassen
931 (beispielsweise die Definitionen der Technischen Use Cases - TUCs) sind nur in so weit
932 normativ, wie ihre Festlegungen auf die Außenschnittstelle wirken. Sie legen explizit nicht
933 die intern zu verwendende Implementierung fest. Die Notwendigkeit für diese Art der
934 „scheinbaren internen Beschreibung“ ergibt sich aus der Komplexität der
935 Gesamtkomponente, sowie dem Bedarf, wiederholt ähnlich Verhaltensweisen in
936 Außenschnittstellen darstellen zu müssen. In diesem Fall werden die sich wiederholenden
937 Verhaltensanteile in internen TUCs zur editoriellen Wiederverwendung gekapselt. Die
938 konkrete konnektorinterne Modularisierung bleibt dem Hersteller freigestellt.
939 Insbesondere bleibt es dem Hersteller freigestellt, intern bereits Mechanismen für
940 kommende Releases zu realisieren, sofern diese an der Außenschnittstelle keine
941 Auswirkung zeigen.

942 Die einzige Abweichung von dieser Vorgehensweise ergibt sich für Sicherheitsaspekte.
943 Hier können interne Vorgänge normativ gefordert sein, die sich an der Außenschnittstelle
944 nicht manifestieren (Beispiel „Verpflichtung auf sicheres Löschen eines temporären
945 Schlüssels nach Gebrauch“). In diesem Fall erfolgt die Überprüfung der Einhaltung dieser
946 Anforderungen im Rahmen der CC-Evaluierung.

947 **1.5.4 Erläuterungen zur Dokumentenstruktur und** 948 **„Dokumentenmechanismen“**

949 **1.5.4.1 Modulare Spezifikation über Funktionsmerkmale**

950 Die Beschreibung des Konnektors erfolgt soweit wie möglich modular, d. h. alle Aspekte,
951 die für einen logischen Bereich relevant sind, werden in einem Kapitel beschrieben. Diese
952 logischen Bereiche werden als Funktionsmerkmal bezeichnet.

953 Funktionsmerkmale kennzeichnet ein eigener Verantwortungsbereich. In diesen
954 Verantwortungsbereich greifen keine anderen Funktionsmerkmale ein. So kann ein
955 logischer Bereich vollständig durchdrungen werden, ohne dass in anderen Kapiteln
956 Anforderungen zu erwarten wären, die das Verhalten des Funktionsmerkmals
957 beeinflussen. Da zwischen Funktionsmerkmalen Wechselwirkungen bestehen (Die
958 Erkennung einer gesteckten Karte im Kartenterminaldienst löst eine Reaktion im
959 Kartendienst aus), wurden zur „dokumententechnischen Interaktion“ zwischen
960 Funktionsmerkmalen ein interner Event-Mechanismus sowie Konfigurationsparameter
961 und Zustandswerte eingeführt (siehe Folgekapitel).

962 Funktionsmerkmale bestehen (bis auf wenige Ausnahmen) immer aus folgenden
963 Unterkapiteln:

- 964 1. Funktionsmerkmalweite Aspekte
- 965 2. Durch Ereignisse ausgelöste Reaktionen
- 966 3. Interne TUCs, **nicht** durch Fachmodule nutzbar
- 967 4. Interne TUCs, **auch** durch Fachmodule nutzbar
- 968 5. Operationen an der Außenschnittstelle
- 969 6. Betriebsaspekte

970 Die Unterkapitel 1-5 dienen der funktionalen Beschreibung des Funktionsmerkmals.
 971 Punkte, die zum Funktionieren des Funktionsmerkmals relevant sind:
 972 Initialisierungsaspekte, durch den Administrator festzulegenden Konfigurationsparameter
 973 etc., werden im Unterkapitel Betriebsaspekte erfasst.
 974 In jedem Funktionsmerkmal sind immer alle Unterkapitel enthalten, auch wenn es im
 975 konkreten Einzelfall dort keine Inhalte gibt. Diese feste Struktur innerhalb der
 976 Funktionsmerkmale erleichtert die Orientierung und erhöht somit die Lesbarkeit.

977 **1.5.4.2 Technische Use Cases - TUCs**

978 Innerhalb der Funktionsmerkmale in Kapitel 4 erfolgt eine Unterscheidung der TUCs in
 979 solche, die nur durch die Basisdienste des Konnektors aufgerufen werden dürfen (rein
 980 interne TUCs) und solche die neben den Basisdiensten auch durch Fachmodule genutzt
 981 werden dürfen. Diese Unterteilung ergibt sich ausschließlich aus dem Bedarf der
 982 editoriiellen Steuerung der verschiedenen Spezifikationen (Konnektor- und
 983 Fachmodulspezifikationen). Es besteht im Rahmen der Implementierung des Konnektors
 984 keine Anforderung diese Trennung intern durchzusetzen.

985 Die Beschreibung der TUCs erfolgt nach folgendem Muster:

- 986 • TUC-Tabelle
- 987 • Aktivitäts- oder Sequenzdiagramm (optional)
- 988 • Fehlercodetabelle

989 Dabei wird innerhalb der TUC-Tabelle in der Zeile „Standardablauf“ ausschließlich der
 990 Gut-Durchlauf beschrieben. Fehler, die innerhalb dieses Ablaufs auftreten können,
 991 werden in der Zeile „Fehlerfälle“ erhoben. Dabei wird auf die jeweilige Schrittnummer
 992 innerhalb des Ablaufs referenziert. In dieser Tabellenzeile werden nur Fehlercodes
 993 erhoben, die im jeweiligen Fehlerfall geworfen werden müssen. Die genauen
 994 Festlegungen zu den Fehlern, neben Fehlercode auch: ErrorType, Severity und
 995 Fehlertext, werden in der Fehlercodetabelle festgelegt.

996 Die Spezifikation, in der ein TUC definiert wird, ist an den mittleren drei Buchstaben der
 997 TUC-Referenz zu erkennen:

- 998 • TUC_KON_xxx entsprechend in dieser Konnektorspezifikation
- 999 • TUC_PKI_xxx in der PKI-Spezifikation [gemSpec_PKI]
- 1000 • TUC_VPN_ZD-xxxx in der Spezifikation des VPN-Zugangsdienstes
 1001 [gemSpec_VPN_ZugD]
- 1002 • TUC_VZD_xxx in der Spezifikation des Verzeichnisdienstes [gemSpec_VZD]

1003 **Festlegungen zur Schreibweise von Eingangs- und Ausgangsdaten von TUCs**

1004 a) Eingangs- und Ausgangsparameter werden in TUC-Tabellen wie folgt beschrieben:

1005 Name des Eingangs- bzw. Ausgangsparameters

1006 gefolgt von (falls definiert): [Datentyp]

1007 gefolgt von (falls zutreffend):

- 1008 - *optional*; *default*: <Defaultwert> bzw.
- 1009 - *optional*; <erklärender Text>

1010 Hierbei bedeuten:

1011

1012 - *optional*; kennzeichnet optionale Ein- und Ausgangsparameter

1013 *default*: <Defaultwert> definiert den Defaultwert für den Fall, dass der

1014 Eingangsparameter leer ist bzw. nicht übergeben wurde

1015 /<erklärender Text> beschreibt Bedingungen, unter denen der

1016 Eingangsparameter optional ist

1017 gefolgt von (falls vorhanden): (<erklärender Text>)

1018 b) Namen mit kleinem Anfangsbuchstaben bezeichnen Ein- und Ausgangsparameter;

1019 Namen mit großem Anfangsbuchstaben bezeichnen Datentypen.

1020 Beispiel:

Eingangsdaten	<ul style="list-style-type: none"> • mandantId • allWorkplaces [Boolean] – <i>optional</i>; <i>default</i>: <i>false</i> (Dieser Schalter gibt an, ob eine mandantenweite Zugriffsberechtigung zum Tragen kommt...) • userId – <i>optional/verpflichtend</i>, wenn <i>cardType = HBAX</i>
Ausgangsdaten	<ul style="list-style-type: none"> • pinStatus [PinStatus] • leftTries – <i>optional/verpflichtend</i>, wenn pinStatus = VERIFYABLE (Anzahl der verbleibenden Versuche für die Verifikation der PIN)

1021

1022

1023 Die im Dokument verwendeten Datentypen sind definiert in [Anhang L – Datentypen von

1024 Eingangs- und Ausgangsdaten].

1025 Festlegungen zur Schreibweise des Aufrufs von TUCs

1026 Ein TUC-Aufruf erfolgt nach folgendem Muster:

1027 <TUC-Bezeichner> {

1028 <TUC-Eingangsparameter Name> = <TUC Eingangsparameter Wert>;

1029 ... }

1030 Beispiel:

1031 TUC_KON_256 {

1032 topic = „CT/DISCONNECTED“;

1033 eventType = Op;

1034 severity = Info;

1035 parameters = („CtID=\$CT.CTID, Hostname=\$CT.HOSTNAME“) }

1036 Vereinfachung:

1037 Ist <TUC-Eingangsparameter Name> des aufzurufenden TUCs gleich der Variablen, die
1038 als < TUC Eingangsparameter Wert> gesetzt wird, so kann dieser Bezeichner ohne
1039 Zuweisung geschrieben werden.

1040 Beispiel: (cardSession und pinRef sind Eingangsdaten des aufrufenden TUCs):

1041 TUC_KON_022 „Liefere PIN-Status“ {cardSession=cardSession; pinRef=pinRef}

1042 vereinfachte Schreibweise:

1043 TUC_KON_022 „Liefere PIN-Status“ {cardSession; pinRef}

1044 **1.5.4.3 Event-Mechanismus**

1045 Der in Kapitel 4.1.6 spezifizierte Event-Mechanismus zur Unterrichtung von
1046 Clientsystemen wird innerhalb dieser Spezifikation auch zur internen Verzahnung der
1047 einzelnen Funktionsmerkmale eingesetzt. So wird ein Ereignis, das in der
1048 Managementschnittstelle durch Änderung eines Konfigurationsparameters ausgelöst wird,
1049 innerhalb des DHCP-Kapitels als Trigger für eine Lease-Erneuerung verwendet. Dies
1050 bedeutet nicht, dass im Rahmen der Implementierung intern ein Event-Mechanismus
1051 zwischen den Modulen verwendet werden muss. Auch hier dient die Form der Darstellung
1052 (Events) lediglich der editoriiellen Kopplung verschiedener Verhaltensbeschreibungen.

1053 Um den Ursprung eines Events erkennen zu können, verwenden alle Events ein Haupt-
1054 Topic passend zum Funktionsmerkmal: „DHCP/LAN_CLIENT/RENEW“ wird im
1055 Funktionsmerkmal DHCP ausgelöst, „CARD/INSERTED“ wird im Funktionsmerkmal
1056 Kartendienst ausgelöst usw.

1057 **1.5.4.4 Konfigurationsparameter und Zustandswerte**

1058 Werte die der Administrator des Konnektors einsehen oder verändern können muss,
1059 werden zusätzlich zu den Festlegungen in Kapitel 4.3 Konnektormanagement auch pro
1060 Funktionsmerkmal in den jeweiligen Unterkapiteln „Betriebsaspekte“ erhoben. Diese
1061 **Konfigurationsparameter** werden über eine ReferenzID definiert. Definierte
1062 Konfigurationsparameter können in allen Kapiteln der Spezifikation referenziert werden.
1063 Den Ort, an welchem ein solcher Konfigurationsparameter definiert/erhoben und somit
1064 dessen Bedeutung beschrieben wird, lässt sich über den Präfix der ReferenzID erkennen:
1065 CERT_CRL_DOWNLOAD_ADDRESS (also „Cert“) wird im Zertifikatsdienst definiert,
1066 MGM_LU_ONLINE (also „MGM“) wird im Konnektormanagement definiert usw.

1067 Die ReferenzIDs der Konfigurationsparameter besitzen in ihrer Schreibweise nur
1068 innerhalb des Dokuments Gültigkeit. In der Umsetzung können für die
1069 Konfigurationswerte herstellerspezifische Beschreibungen und Labels verwendet werden.

1070 Vergleichbar zu diesen Konfigurationsparametern, sind **Zustandswerte**. Auch diese
1071 werden über ReferenzIDs definiert, nur können sie nicht durch den Administrator
1072 verändert oder eingesehen werden. Sie finden nur konnektorintern Verwendung und sind
1073 für die Beschreibung der Verhaltensweise notwendig, Beispiele sind CTM_CT_LIST für
1074 die Liste der durch den Konnektor verwalteten Kartenterminals oder CM_CARD_LIST für
1075 die Liste der aktuell erreichbaren Karten. Zustandswerte verwenden die gleichen Präfixe
1076 wie Konfigurationsparameter.

1077

2 Systemüberblick

- 1078 Der Konnektor ist ein Produkttyp der TI gemäß [gemKPT_Arch_TIP#5.3.9].
- 1079 Er bietet seine Basisdienste sowohl intern den in ihm laufenden Fachmodulen an, als
1080 auch externen Clientsystemen über die Konnektorauschnittstellen.
- 1081 Im lokalen Netz der Einsatzumgebung kommuniziert das Clientsystem mit dem
1082 Konnektor über dessen LAN-seitiges Ethernet-Interface. Alleinig der Konnektor
1083 kommuniziert mit den in lokalen Netzen angeschlossenen Kartenterminals und Karten.
1084 Auch die Kommunikation mit den zentralen Diensten der TI-Plattform und
1085 fachanwendungsspezifischen Diensten erfolgt ausschließlich über den Konnektor über
1086 dessen WAN-seitiges Ethernet-Interface.
- 1087 Um die lokale Anzeige für die Signaturerstellung und Signaturprüfung zu realisieren, wird
1088 ein Signaturproxy verwendet, der die Schnittstellen I_Sign_Operations und
1089 I_SAK_Operations sowie ServiceDirectory kapselt. Der Signaturproxy ist aus Gründen der
1090 Übersichtlichkeit nicht in der Abbildung PIC_KON_116 dargestellt, seine Spezifikation
1091 findet sich in [gemSpec_Kon_SigProxy].
- 1092 Abbildung PIC_KON_116 stellt die Schnittstellen im Umfeld des Konnektors dar.

1093

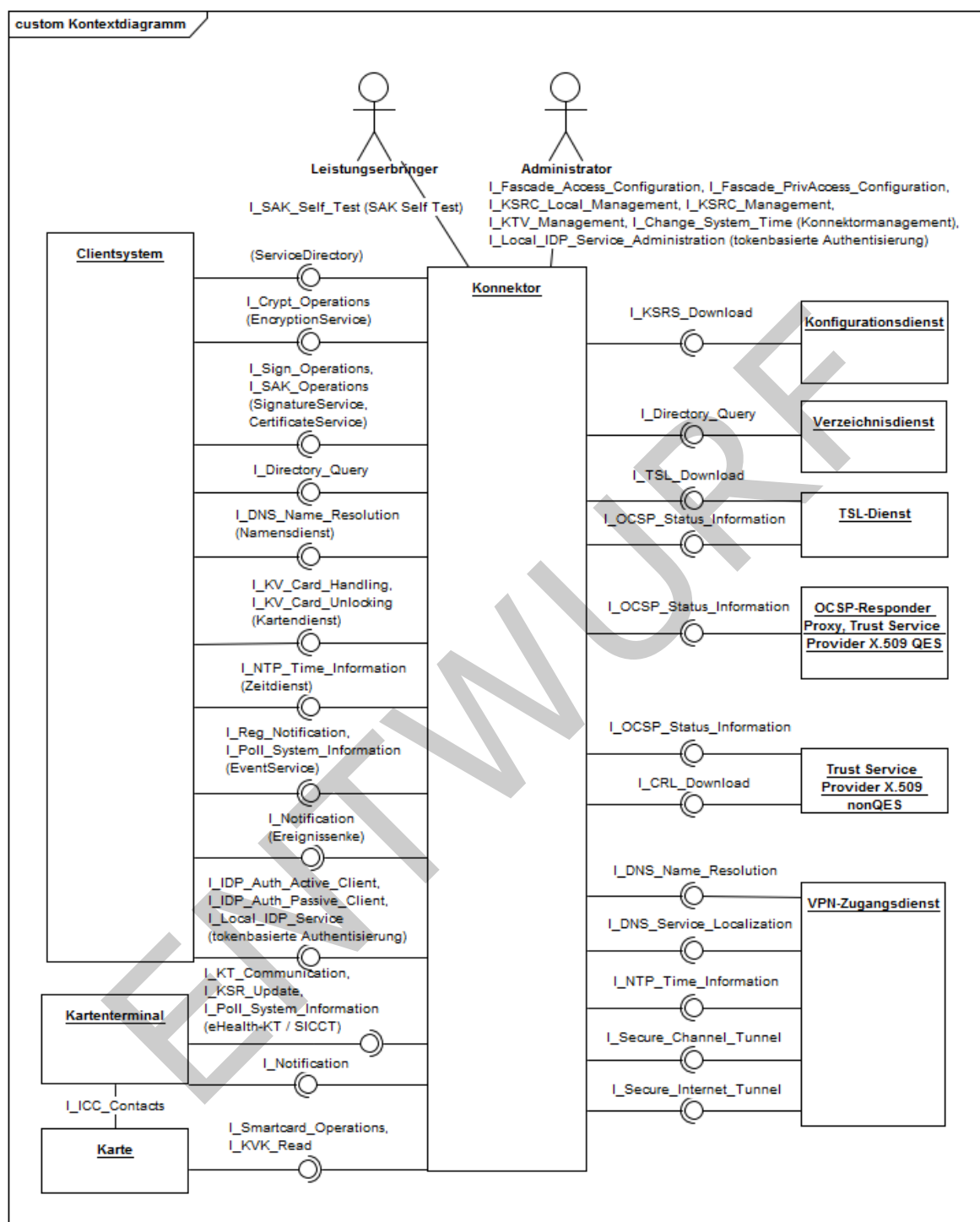


Abbildung 1: PIC_KON_116 Schnittstellen des Konnektors von und zu anderen Produkttypen

Die logischen Außenschnittstellen aus [gemKPT_Arch_TIP] werden im Konnektor technisch vorrangig als SOAP-Schnittstellen ausgeprägt. Von dieser Regel wird insbesondere bei Netzwerkschnittstellen abgewichen, wenn bereits etablierte Schnittstellenstandards für Basisdienste existieren (IPsec, TLS, NTP, DNS etc.). Eine

- 1102 Übersicht der Zuordnung „logische Schnittstellen → technische Schnittstellen“ findet sich
1103 in Anhang H.
- 1104 Zum Nachweis der Sicherheit müssen Konnektoren im Rahmen der Zulassung nach
1105 Common Criteria gegen die Schutzprofile [PP_NK] und [PP_KON] evaluiert und zertifiziert
1106 werden.
- 1107 Die zu verwendenden kryptographischen Verfahren und zugehörige Parameter (z. B.
1108 Schlüssellängen) für alle kryptographischen Operationen innerhalb der
1109 Telematikinfrastruktur, werden durch das Dokument „Verwendung kryptographischer
1110 Algorithmen in der Telematikinfrastruktur“ [gemSpec_Krypt] normativ geregelt.

1111 2.1 Logische Struktur

- 1112 Der Produkttyp Konnektor besitzt eine Vielzahl verschiedenster Operationen und
1113 Verhaltensweisen an seiner Außenschnittstelle. Um sein komplexes Gesamtverhalten
1114 sinnvoll beschreiben zu können, wird der Konnektor innerhalb dieser Spezifikation logisch
1115 unterteilt und strukturiert. Es wird primär zwischen Anwendungs- und Netzkonnektor
1116 unterschieden, begleitet von Mechanismen, die blockübergreifend beschrieben werden.
- 1117 Der logische Aufbau des Konnektors ist in Abbildung PIC_KON_117 dargestellt.
- 1118 • Der Anwendungskonnektor bietet anwendungsnahe Basisdienste (inklusive
1119 Signaturdienst) und Fachmodule zur Nutzung durch ein Clientsystem an.
 - 1120 • Der Anwendungskonnektor bietet zusätzlich zu den in Kap. 4.1 beschriebenen
1121 Basisdiensten den optionalen Dienst „tokenbasierte Authentisierung“, der in
1122 [gemSpec_Kon_TBAuth] beschrieben ist.
 - 1123 • Der Netzkonnektor bietet transportnahe Basisdienste und verbindet das lokale
1124 Netz der Nutzer mit der zentralen TI-Plattform.
 - 1125 • Die gSMC-K ist zwar ein eigenständiger Produkttyp innerhalb der TI, wird im
1126 Konnektor jedoch als Verbaukomponente betrachtet. Sie enthält die
1127 kryptographischen Identitäten des Konnektors, sowie Steuerdaten
1128 (Umgebungsinformationen TU/RU/PU, zugehörige Adressbereiche,
1129 herstellerspezifische Konfigurationsdaten), die aus Sicherheitsgründen
1130 unveränderlich in den Konnektor eingebracht werden müssen.
 - 1131 • Das Konnektormanagement dient der administrativen Verwaltung und Steuerung
1132 des gesamten Konnektors.
 - 1133 • Der Sichere Datenspeicher dient der integeren, vertraulichen und authentischen
1134 Persistierung von veränderlichen Daten (siehe auch Kapitel 2.2).
 - 1135 • Der Signaturproxy ist eine Komponente, die zwischengeschaltet auf der
1136 Kommunikationsstrecke zwischen Client-System und Konnektor dafür sorgt, dass
1137 die zu signierenden oder zu prüfenden Dokumente dem Nutzer angezeigt werden.
1138 Die Beschreibung des Signaturproxy befindet sich in [gemSpec_Kon_SigProxy]

1139

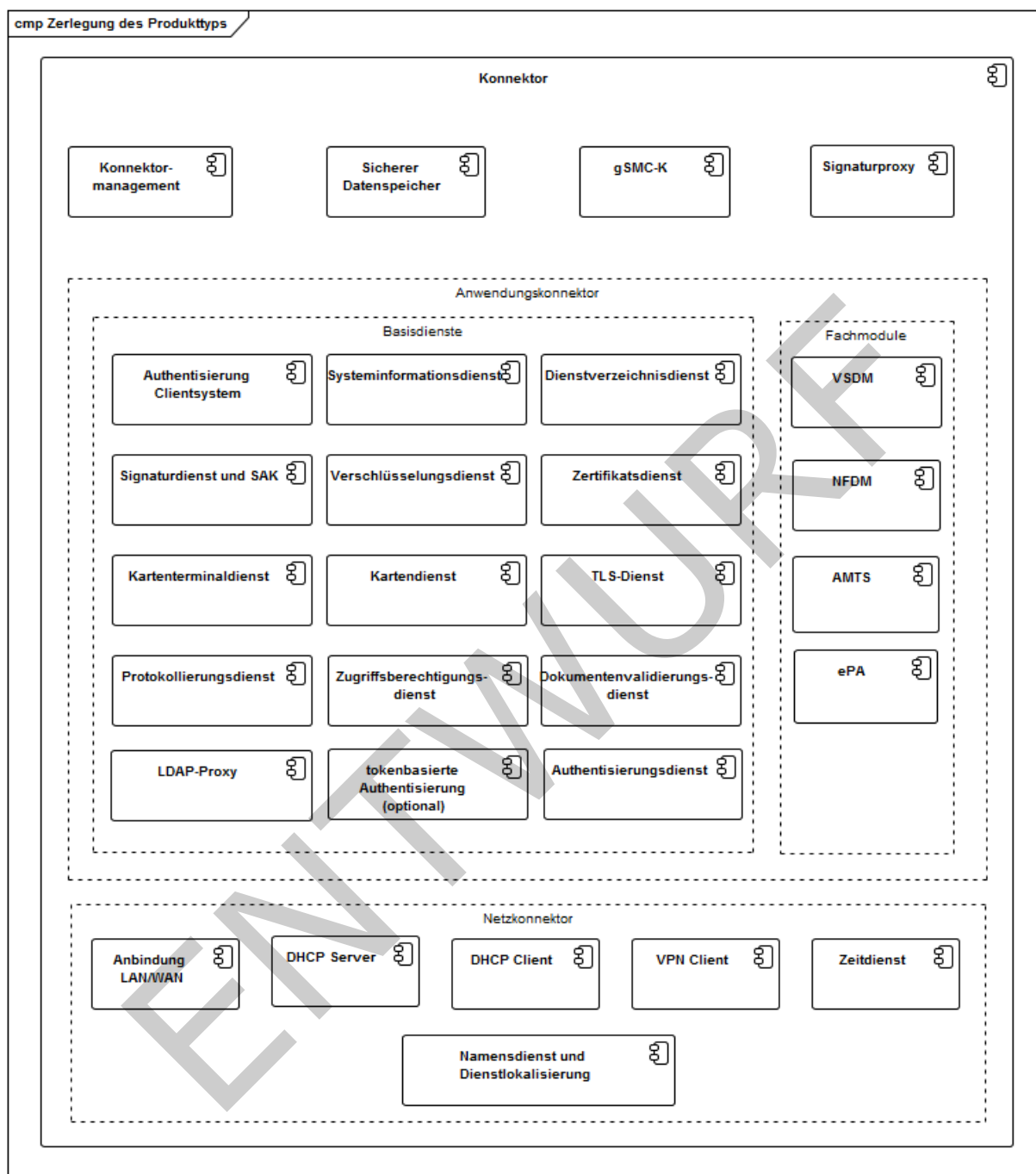


Abbildung 2: PIC_KON_117 Logische Zerlegung des Konnektors in Anwendungs- und Netzkonnektor

Diese logische Unterteilung schreibt in keiner Art und Weise die spätere Implementierung durch den Hersteller vor. Der Hersteller kann seine interne Modularisierung des Konnektors frei wählen. Normativ wirksam ist ausschließlich das durch die Detailfestlegungen in Summe beschriebene Verhalten an den Außenschnittstellen des Konnektors als Ganzes.

1149 2.2 Sicherer Datenspeicher

1150 Wie im vorherigen Kapitel dargestellt, wird für den Konnektor ein Datenspeicher
1151 angenommen, in welchem der Konnektor alle sicherheitskritischen, veränderlichen Daten
1152 dauerhaft speichert, die für seinen Betrieb relevant sind. Dieser Datenspeicher sichert die
1153 Integrität, Authentizität und Vertraulichkeit der in ihm hinterlegten Daten bzw. der aus
1154 ihm entnommenen Daten. Alleinig der Konnektor hat auf diesen Datenspeicher Zugriff.
1155 Für folgende, im weiteren Verlauf der Spezifikation anfallende Daten wird angenommen,
1156 dass diese im Sicheren Datenspeicher persistiert werden:

- 1157 • Der Trust Store des Zertifikatsdienstes
- 1158 • Die Konfigurationsdaten des Konnektormanagements
- 1159 • Die Konfigurationsdaten aller Funktionsmerkmale

1160 Ferner stellt der Konnektor den in ihm laufenden Fachmodulen ebenfalls eine Nutzung
1161 dieses Datenspeichers für ihre sensiblen Daten zur Verfügung.

1162 Da es sich bei dem Sicheren Datenspeicher um ein internes Modul handelt, welches an
1163 der Außenschnittstelle nicht testbar ist, werden an dieses Modul im Rahmen dieser
1164 Spezifikation keine Anforderungen erhoben. Da dieses logische Modul aber essenzielle
1165 Sicherheitsfunktionen bietet, ohne die ein Konnektor nicht sicher betrieben werden kann,
1166 werden die Funktionen, die ein Hersteller für sein Konnektormodell real umsetzt, um die
1167 notwendigen sicheren Speicherfunktionen zu realisieren, im Rahmen der CC-Evaluierung
1168 geprüft werden. Näheres hierzu regeln die Schutzprofile des Konnektors.

1169 2.3 Überblick Konnektoridentität

1170 Die Geräteidentität des Konnektors (Konnektoridentität) teilt sich in drei Identitäten auf:

- 1171 • ID.NK.VPN für den Netzkonnektor
1172 Die Identität des Netzkonnektors dient der Authentisierung gegenüber den
1173 zentralen Netzwerkdiensten und wird für die Anmeldung an den VPN-Konzentrator
1174 genutzt.
- 1175 • ID.AK.AUT für den Anwendungskonnektor
1176 Die Identität des Anwendungskonnektors dient der Authentisierung gegenüber
1177 den Clientsystemen im Rahmen von TLS-Verbindungen.
- 1178 • ID.SAK.AUT für die im Anwendungskonnektor enthaltene
1179 Signaturanwendungskomponente
1180 Die Identität des Signaturdienstes dient zur Authentisierung gegenüber den
1181 Kartenterminals. Darüber hinaus muss sich der Signaturdienst des Konnektors
1182 gegenüber dem Heilberufsausweis mittels eines kartenverifizierbaren Zertifikats
1183 (C.SAK.AUTD_CVC) mit entsprechendem Profil ausweisen, um Stapelsignaturen
1184 durchführen zu können.

1185 In der Regel ergibt sich aus dem Kontext, welche Identität gemeint ist, sodass in diesen
1186 Fällen nur kurz von der Konnektoridentität geschrieben wird.

1187 Die Geräteidentitäten werden durch asymmetrische Schlüssel und X.509-Zertifikate
1188 umgesetzt. In Abhängigkeit vom gewählten kryptographischen Verfahren werden RSA-
1189 Schlüssel bzw. ECC-Schlüssel verwendet.

1190 2.4 Mandantenfähigkeit

1191 Den Anforderungen aus [gemKPT_Arch_TIP#TIP1-A_2200] folgend, wird die
1192 Mandantenfähigkeit innerhalb des Konnektors nicht durch eine einzelne Funktion,
1193 sondern durch Berücksichtigung in einer Reihe von Funktionsmerkmalen umgesetzt.

1194 Die Mandantenfähigkeit wirkt dabei auf:

- 1195 • Zugriffsberechtigungsdienst: Kapitel 4.1.1
1196 (und über diesen auf alle Karten- und Kartenterminaloperationen)
- 1197 • Systeminformationsdienst: Kapitel 4.1.6

1198 2.5 Versionierung

1199 Gemäß [gemSpec_OM] müssen Konnektor und Kartenterminals über eine Versionierung
1200 verfügen. Die relevanten Versionsinformationen sind durch das O&M-Schema
1201 ProductInformation.xsd definiert. Ferner definiert [gemSpec_OM], dass Konnektor und
1202 Kartenterminal das Konzept der Firmware-Gruppe verwenden müssen. Daher verfügen
1203 die beiden Produkttypen auch über eine aktuelle Firmware-Gruppenversion.

1204 Versionsinformationen werden innerhalb des Konnektor an folgenden Stellen ver- und
1205 bearbeitet:

- 1206 • Dienstverzeichnisdienst (Kapitel 4.1.3): Ausgabe der Konnektorversion über SOAP
- 1207 • Kartenterminaldienst (Kapitel 4.1.4): Anzeige der Versionsinformationen der
1208 verwalteten Kartenterminals
- 1209 • Konnektormanagement (Kapitel 4.3):
 - 1210 • Anzeige der Versionsinformationen des Konnektors (Kapitel 4.3.2)
 - 1211 • Software-Aktualisierung (KSR-Client) für Konnektor und Kartenterminals
1212 (Kapitel 4.3.9)

1213 2.6 Fachanwendungen

1214 Der Konnektor ist als Plattformkomponente der TI für die Erbringung von Basisdiensten
1215 verantwortlich. Fachliche Funktionalitäten werden über die Fachmodule bereitgestellt.

1216 Das Fachmodul wird dabei als integraler Bestandteil des Konnektors verstanden
1217 (Konnektor als Monolith), d. h., die Spezifikationen zu Konnektor (als
1218 Plattformkomponente) und dem Fachmodul sind zwar getrennt, werden aber von einem
1219 Hersteller in einer Gesamtkomponente umgesetzt. Die inneren Schnittstellen zwischen
1220 Fachmodul und Konnektor sind von außen nicht erkennbar.

1221 In dieser Ausbaustufe unterstützt der Konnektor die Fachanwendungen VSDM,
1222 AMTS, NFDM und ePA über jeweils ein Fachmodul.

1223 Neben Fachanwendungen, die über ihr Fachmodul mit einem gesicherten Fachdienst
1224 kommunizieren, unterstützt der Konnektor einen Zugriff von Clientsystemen auf offene
1225 Fachdienste.

2.7 Netzseitige Einsatzszenarien

Der Konnektor unterstützt unterschiedliche netzseitige Einsatzszenarien, die in Anhang K beispielhaft dargestellt sind.

Der Konnektor bietet hierzu Konfigurations-Parameter, die je nach netzseitigem Einsatzszenario konfiguriert werden müssen.

2.7.1 Parameter ANLW_ANBINDUNGS_MODUS

Konfiguration 1: Konnektor als Gateway (ANLW_ANBINDUNGS_MODUS = InReihe):

Diese Konfiguration ist geeignet für Szenarien, in denen der Konnektor zwischen das lokale Netz und das Internet Access Gateway (IAG) (z. B. Router mit DSL-/Kabelmodem) geschaltet wird. (vgl. Anhang K, Szenario 1)

Konfiguration 2: Konnektor eingebettet in existierende Infrastruktur (ANLW_ANBINDUNGS_MODUS = Parallel): Diese Konfiguration ist geeignet für Szenarien, in denen der Konnektor als weiteres Gerät in die bestehende Netzwerkinfrastruktur integriert wird. (vgl. Anhang K, Szenario 3)

Aus Sicherheitsgründen soll die Kommunikation der Clientsysteme mit dem Konnektor hierbei verschlüsselt erfolgen (ANCL_TLS_MANDATORY=Enabled). Falls diese Kommunikation unverschlüsselt erfolgt (ANCL_TLS_MANDATORY=Disabled), übernimmt der Nutzer die Verantwortung für die Sicherstellung der vertraulichen Übertragung.

Für den Einsatz und die Nutzung von DHCP gibt es im Zusammenhang mit diesem Konfigurationsparameter folgende Möglichkeiten:

- Die Netzwerkinfrastruktur der Einsatzumgebung verwendet den DHCP-Server des Konnektors (siehe Kap. 4.2.2).
- Ein bestehender DHCP-Server im Netz der Einsatzumgebung wird weiter verwendet und derart konfiguriert, dass als Default Gateway und DNS-Server entweder bestehende Infrastruktur oder der Konnektor verwendet wird.
- Es kommt kein DHCP-Server zum Einsatz. Bei allen Clients im Netz der Einsatzumgebung werden das Default Gateway und der DNS-Server statisch auf den Konnektor gesetzt.

Die DHCP-Konfiguration ist in Konfiguration 1 in aller Regel die folgende: Die WAN-Seite des Konnektors verwendet den DHCP-Server des bestehenden IAG. An der LAN-Seite stellt der Konnektor einen DHCP-Server für alle Clients zur Verfügung.

2.7.2 Parameter ANLW_INTERNET_MODUS

Grundsätzlich routet der Konnektor im Modus ANLW_INTERNET_MODUS=SIS alle für das Internet bestimmten Pakete von Clients, die ihn als Default Gateway verwenden, in den VPN-Tunnel zum SIS, während er im Modus ANLW_INTERNET_MODUS=Keiner diese Pakete verwirft.

Im Unterschied zu (ANLW_ANBINDUNGS_MODUS = InReihe) ist die Nutzung des SIS bei (ANLW_ANBINDUNGS_MODUS = Parallel) optional. Alternativ können auch die Clients, die den Konnektor als Default Gateway verwenden, per Redirect direkt ins Internet verwiesen werden (ANLW_INTERNET_MODUS=IAG).

1267 2.8 Lokale und entfernte Kartenterminals

1268 Gemäß [gemKPT_Arch_TIP] ermöglicht die Telematikinfrastruktur dem Anwender die
1269 PIN-Eingabe zur Freischaltung eines HBAs oder einer SMC-B wahlweise lokal oder über
1270 das Remote-PIN-Eingabeverfahren durchzuführen. Deshalb unterscheidet auch der
1271 Konnektor zwischen einem lokalen Kartenterminal – räumlich („in Sichtweite“) dem
1272 Arbeitsplatz zugeordnet – und einem entfernten Kartenterminal.

1273 Ein lokales Kartenterminal befindet sich lokal an einem Arbeitsplatz und kann von diesem
1274 aus genutzt werden. Hingegen ist das entfernte Kartenterminal einem entfernten oder
1275 auch – für zentral steckende Karten – keinem Arbeitsplatz fest zugewiesen. Ein lokales
1276 Kartenterminal kann als sogenanntes Remote-PIN-KT verwendet werden, um die PIN für
1277 eine in einem entfernten Kartenterminal steckende Karte einzugeben.

1278 2.9 Standalone-Szenario

1279 Gemäß § 291 SGB V Absatz 2b müssen „Diese Dienste [zur Online-Aktualisierung der
1280 Versichertendaten auf der eGK] [...] auch ohne Netzanbindung an die
1281 Praxisverwaltungssysteme der Leistungserbringer online genutzt werden können.“

1282 Dies bedeutet, dass der Konnektor ohne ein steuerndes Clientsystem ereignisgetrieben
1283 Fachanwendungen ausführen können muss. Aus Fachsicht „steht der Konnektor alleine“,
1284 ohne Clientsysteme. Die konkreten Aktionen, die Fachanwendungen in diesen Fällen
1285 ausführen, sowie deren Auslöser werden in den jeweiligen Fachmodulspezifikationen
1286 beschrieben.

1287 Ein solcher alleinstehender Konnektor mit Zugang zur TI muss zur Durchführung der
1288 Fachanwendungen durch einen weiteren Konnektor unterstützt werden, der in direkter
1289 Verbindung zum Clientsystem steht, selbst aber keine Online-Anbindung besitzt.

1290

3 Übergreifende Festlegungen

1291 Für die folgenden Inhalte bitte die Hinweise in Kapitel 1.5.3 „Erläuterungen zur
1292 Spezifikation des Außenverhaltens,“ sowie Kapitel 1.5.4 Erläuterungen zur
1293 Dokumentenstruktur und „Dokumentenmechanismen“ beachten.

1294 In diesem Kapitel werden die Aspekte des Konnektors behandelt, die
1295 Funktionsmerkmalübergreifend geregelt werden müssen.

1296 Die Managementschnittstelle/Administrationsoberfläche des Konnektors wird dabei nicht
1297 als übergreifender Aspekt, sondern als eigenes Funktionsmerkmal gewertet. Die
1298 Festlegungen hierzu finden sich entsprechend in Kapitel 4.3.

1299 A_18605 - Option Basisdienst TBAuth

1300 Der Konnektor SOLL den Basisdienst TBAuth [gemSpec_Kon_TBAuth] unterstützen. [≤]

1301 Wird die SOLL-Anforderung A_18605 nicht umgesetzt, so ist die Umsetzung mit einem
1302 Firmwareupdate im Jahr 2021 nachzuholen.

1303 Dokumentformate

1304 Mit dem Aufruf einer Operation, die Dokumente verarbeitet, muss durch den Aufrufer
1305 festgelegt werden können, um welches Dokumentenformat es sich handelt, damit die
1306 unterschiedlichen Formate zur Verarbeitung und etwaigen Anzeige unterschieden werden
1307 können. Die nicht-XML-Formate werden dabei nach MIME-Typ-Klassen unterschieden:

- 1308 • „PDF/A“ für MIME-Typ „application/pdf-a“ gemäß [ISO 19005],
- 1309 • „Text“ für MIME-Typ „text/plain“,
- 1310 • „TIFF“ für MIME-Typ „image/tiff“ gemäß [TIFF6]
- 1311 • „Binär“ für alle übrigen MIME-Typen.

1312 Folgende Bezeichner werden verwendet:

1313 Alle_DocFormate: XML, PDF/A, Text, TIFF, Binär

1314 nonQES_DocFormate: XML, PDF/A, Text, TIFF, Binär

1315 QES_DocFormate: XML, PDF/A, Text, TIFF

1316 Für nonQES_DocFormate wird, trotz Gleichheit zu Alle_DocFormate, ein eigener
1317 Referenzbezeichner verwendet, da sich diese Liste noch ändern könnte. TIFF wird durch
1318 [gemKPT_Arch_TIP] nicht für die nonQES verlangt. Die Unterstützung dieses Formats für
1319 nonQES bedeutet jedoch keinen Mehraufwand, da die Routinen durch QES bereits
1320 implementiert sind und nachgenutzt werden können.

1321 TIP1-A_4500 - Dokumentgrößen von 25 MB

1322 Der Konnektor MUSS für alle Außenschnittstellen, in denen ein Dokument verarbeitet
1323 wird, Dokumente mit einer Größe ≤ 25 MB unterstützen. Der Konnektor KANN
1324 Dokumente mit einer Größe > 25 MB unterstützen. [≤]

1325 A_19052 - Vorgaben für Dokumentformate und Nachrichten

1326 Der Konnektor MUSS für die Verarbeitung von Dokumenten und Nachrichten die
1327 Vorgaben aus TAB_KON_775 erfüllen. [≤]

1328 TIP1-A_4502 - Zeichensatzcodierungen UTF-8 und ISO-8859-15

1329 Der Konnektor MUSS bei der Verarbeitung von Dokumenten der Formate XML und Text
1330 die Zeichensatzkodierungen UTF-8 und ISO-8859-15 unterstützen. Das verarbeitete

1331 Dokument MUSS der Konnektor mit demselben Zeichensatz kodieren, in dem das
1332 Eingangsdokument kodiert war. [≤]

1333 TIP1-A_5541-01 - Referenzen in Dokumenten nicht dynamisch auflösen
1334 Der Konnektor DARF in Dokumenten eventuell vorhandene Referenzen auf externe
1335 Ressourcen NICHT auflösen, es sei denn es sind Verweise auf im Konnektor sicher
1336 eingebrachte vorliegende Schemata oder dies wird im Einzelfall normativ gefordert. [≤]

1337 Kartentypen

1338 Der Konnektor unterstützt eine Reihe von Kartentypen. Die folgende Tabelle enthält die
1339 Liste der Referenzbezeichner für die verschiedenen Kartentypen, wie sie im weiteren
1340 Verlauf verwendet werden. Die Unterstützung von Karten der Generation 2 (G2.x: G2.0,
1341 G2.1 und höher) beschränkt sich bei diesen auf die Datenstrukturen und Schlüssel, die
1342 aus Gründen der Abwärtskompatibilität zu den Karten der Generation 1+ vorhanden sind.
1343 Eine Ausnahme hiervon bilden die Geräte-CVCs, die bereits für dieses Release basierend
1344 auf ECC verwendet werden.

1346 **Tabelle 1: TAB_KON_500 Wertetabelle Kartentypen**

ReferenzID Kartentyp	Karten- generatio n	Beschreibung
EGK	G1+	Die elektronische Gesundheitskarte gemäß [gemSpec_eGK_P1] und [gemSpec_eGK_P2]
EGK	G2	Die elektronische Gesundheitskarte gemäß [gemSpec_COS] und [gemSpec_eGK_ObjSys] bzw. [gemSpec_eGK_ObjSys_G2.1]
HBA-qSig	-	HBA-Vorläuferkarte gemäß [HPC-P1] und [HPC-P2]
HBA	G2	Der elektronische Heilberufsausweis (HBA) gemäß [gemSpec_COS] und [gemSpec_HBA_ObjSys]
SMC-B	G2	Die Institutionskarte Typ B (Secure Module Card) gemäß [gemSpec_COS] und [gemSpec_SMC-B_ObjSys]
HSM-B		HSM-Variante einer SM-B. Das HSM-B wird in dieser Fassung als ein oder mehrere virtuelle Kartenterminals verstanden, in denen virtuelle Karten stecken.
SMC-KT	G2	Die Karte Typ KT (Secure Module Card) gemäß [gemSpec_COS] und [gemSpec_gSMC-KT_ObjSys]
KVK	-	Die Krankenversichertenkarte gemäß der Spezifikation [KVK]
ZOD_2.0	-	HBA-Vorläuferkarte gemäß [HPC-P1] und [HPC-P2]
UNKNOWN		Eine nicht erkannte Karte oder nicht lesbare Karte
		Zusammenfassende ReferenzIDs

HBA-VK		Adressiert die HBA-Vorläuferkarten HBA-qSig und ZOD_2.0. Wird dieser Referenzbezeichner verwendet, gelten die zugehörigen Aussagen und Festlegungen für beide Kartentypen.
HBAx		Adressiert sowohl den HBA, als auch die HBA-Vorläuferkarten (HBA-VK) Wird dieser Referenzbezeichner verwendet, gelten die zugehörigen Aussagen und Festlegungen für alle drei Kartentypen.
SM-B		Adressiert sowohl eine echte SMC-B als auch eine in einem HSM-B enthaltene virtuelle SMC-B. Wird dieser Referenzbezeichner verwendet, gelten die zugehörigen Aussagen und Festlegungen für beide Typen.

1347

1348 Übergreifende Festlegungen zum Aufbau von sicheren Verbindungen

1349 TIP1-A_7254 - Reaktion auf OCSP-Abfrage beim TLS-Verbindungsaufbau

1350 Der Konnektor MUSS beim Aufbau von TLS-gesicherten Verbindungen zu einem zentralen
1351 Dienst der TI-Plattform oder zu einem fachanwendungsspezifischen Dienst, bei denen
1352 eine OCSP-Abfrage des Serverzertifikats nach TUC_PKI_006 erfolgt, neben Fehlerfällen
1353 bei folgenden Warnungen gemäß [gemSpec_PKI#Tab_PKI_274]

- 1354 • CERT_REVOKED
- 1355 • CERT_UNKNOWN
- 1356 • OCSP_CHECK_REVOCATION_FAILED

1357 mit Abbruch des Verbindungsaufbaus reagieren. [≤=]

1358 In [gemSpec_Krypt#6] wird das Kommunikationsprotokoll zwischen einem Client und
1359 einer Vertrauenswürdigen Ausführungsumgebung (VAU) spezifiziert. Dabei wird ein
1360 sicherer Kanal auf HTTP-Anwendungsschicht zwischen dem Client und der VAU (Server)
1361 aufgebaut. Der Client ist hier ein Fachmodul des Konnektors; der Server ist ein
1362 Fachdienst.

1363 A_17225 - Aufbau einer sicheren Verbindung zur Vertrauenswürdige
1364 Ausführungsumgebung (VAU)

1365 Der Konnektor MUSS für Fachmodule den Aufbau einer sicheren Verbindung zur
1366 Vertrauenswürdigen Ausführungsumgebung (VAU) gemäß Kommunikationsprotokoll
1367 [gemSpec_Krypt#6] unterstützen und das vom Server übergebene Zertifikat wie folgt
1368 prüfen:

```

1369 TUC_KON_037 „Zertifikat prüfen“ {
1370     certificate = C.FD.AUT;
1371     qualifiedCheck = not_required;
1372     offlineAllowNoCheck = false;
1373     policyList = oid_fd_aut;
1374     intendedKeyUsage= intendedKeyUsage(C.FD.AUT);
1375     intendedExtendedKeyUsage = id-kp-serverAuth;
1376     validationMode = OCSP}

```

1377 Der Konnektor MUSS die vom Fachmodul übergebene Rolle gegen die aus dem Zertifikat
1378 ermittelte Rolle prüfen. [≤=]

1379 A_17777 - sicherheitstechnische Festlegungen zum Abruf von kryptographischen
1380 Schlüsseln von einem Schlüsselgenerierungsdienst

1381 Der Konnektor MUSS für Fachmodule für die Nutzung der
 1382 Schlüsselableitungsfunktionalität die sicherheitstechnischen Festlegungen gemäß
 1383 [gemSpec_Krypt#3.15.5 Schlüsselableitungsfunktionalität ePA] und [gemSpec_SGD]
 1384 bereitstellen. [≤]

1385 Der Gesamtablauf der Schlüsselableitungsfunktionalität gemäß [gemSpec_SGD#2.3] für
 1386 den Konnektor als Client ist aufgeteilt zwischen Basiskonnektor und Fachmodul. Die
 1387 kryptographischen Vorgaben (u.a. Durchführung des ECDH, Schlüsselerzeugung, Ver-
 1388 und Entschlüsselung, Signaturerzeugung und -prüfung) werden dabei durch den
 1389 Basiskonnektor realisiert.

1390 3.1 Konnektoridentität und gSMC-K

1391 TIP1-A_4503 - Verpflichtung zur Nutzung von gSMC-K
 1392 Der Konnektor MUSS das geheime Schlüsselmaterial zur Geräteidentität (ID.NK.VPN,
 1393 ID.AK.AUT, ID.SAK.AUT) und der Rolle SAK (C.SAK.AUTD_CVC) über Smartcards des
 1394 Typs gSMC-K gemäß [gemSpec_gSMC-K_ObjSys] nutzen. Der Konnektor MUSS mit einer
 1395 gSMC-K bestückt sein. Er KANN mit mehr als einer gSMC-K bestückt sein.
 1396 [≤]

1397 Die Notwendigkeit, den Konnektor mit mehr als einer gSMC-K zu bestücken, kann sich
 1398 aus den Lastanforderungen aus [gemSpec_Perf#4.1.2] ergeben.

1399 TIP1-A_4504 - Keine Administratorinteraktion bei Einsatz mehrerer gSMC-Ks
 1400 Verwendet der Konnektor mehrere gSMC-Ks, DARF eine Administratorinteraktion für
 1401 diese Belange NICHT erforderlich sein.
 1402 [≤]

1403 TIP1-A_5543 - Keine manuelle PIN-Eingabe für gSMC-K
 1404 Der Konnektor DARF Anwender und Administratoren außer bei der Inbetriebnahme
 1405 (erstmalig oder nach Werksreset) NICHT auffordern, eine PIN für eine gSMC-K
 1406 einzugeben.
 1407 [≤]

1408 TIP1-A_4505 - Schutz vor physischer Manipulation gSMC-K (Sichere Verbundenheit der
 1409 gSMC-K)
 1410 Die gSMC-K des Konnektors MÜSSEN durch den Einsatz physikalischer Sperren oder
 1411 manipulationssicherer Siegel so mit dem Konnektor verbunden sein, dass physischer
 1412 Missbrauch oder physische Manipulation erkennbar ist.
 1413 [≤]

1414 gSMC-Ks gemäß [gemSpec_gSMC-K_ObjSys] verfügen über die Möglichkeit zur
 1415 nachträglichen Generierung von Schlüsselpaaren und dem Nachladen der zugehörigen
 1416 Zertifikate. Dieser Mechanismus wird erst in kommenden Releases durch den Konnektor
 1417 unterstützt. Initial sind alle Identitäten bereits einmal auf der gSMC-K vorhanden.

1418 TIP1-A_4506 - Initiale Identitäten der gSMC-K
 1419 In Abhängigkeit vom kryptographischen Verfahren MUSS der Konnektor folgende Objekte
 1420 der gSMC-K als Quelle seiner Identitäten verwenden:

1421 **Tabelle 2: TAB_KON_856: Identitäten des Konnektors auf der gSMC-K**

Identifizier	Verzeichnis	Objekt der gSMC-K in Abhängigkeit vom kryptographischen Verfahren	
		RSA	ECC

ID.NK.VPN	MF/DF.NK	EF.C.NK.VPN.R2048	EF.C.NK.VPN2.XXXX
ID.AK.AUT	MF/DF.AK	EF.C.AK.AUT.R2048	EF.C.AK.AUT2.XXXX
ID.SAK.AUT	MF/DF.SAK	EF.C.SAK.AUT.R2048	EF.C.SAK.AUT2.XXXX
C.SAK.AUTD_CVC	MF/DF.SAK	-	EF.C.SAK.AUTD_CVC.E256

1422
1423 [\leq]

1424

1425 3.1.1 Organisatorische Anforderungen und Sperrprozesse

1426 TIP1-A_5392 - gSMC-K-Verantwortung durch den Hersteller des Konnektors
1427 Der Hersteller des Konnektors MUSS die Rolle des Kartenherausgebers für in seinen
1428 Konnektoren verbauten gSMC-Ks einnehmen.
1429 Der Hersteller des Konnektors KANN die von ihm verantwortete Personalisierung der
1430 gSMC-K durch einen von ihm zu beauftragenden Dienstleister in seinem Namen
1431 vornehmen lassen.
1432 [\leq]

1433 TIP1-A_5696 - Prüfung der personalisierten gSMC-K
1434 Der Hersteller des Konnektors MUSS sich von der korrekten Personalisierung der
1435 herausgegebenen gSMC-K überzeugen.
1436 [\leq]

1437 A_18928 - Ausstattung mit dual-personalisierten gSMC-K-X.509-Zertifikaten
1438 Der Hersteller des Konnektors MUSS die Konnektoren mit einer gSMC-K mit
1439 personalisierten RSA- und ECC-Zertifikaten gemäß TAB_KON_856 ausstatten. [\leq]

1440

1441 A_18930 - Unterstützung von gSMC-K Personalisierungsvarianten
1442 Der Konnektor MUSS unterschiedliche gSMC-K-Personalisierungsvarianten sowohl mit als auch ohne
1443 ECC-Zertifikate für ID.NK.VPN, ID.AK.AUT und ID.SAK.AUT unterstützen. [\leq]

1444 Die Anforderung ist für die Anwendungsfälle Registrierung, IPsec-Authentisierung und
1445 Autorisierung beim VPN-Zugangsdienst, TLS-Authentisierung zum eHealth-
1446 Kartenterminal, TLS-Authentisierung zum Primärsystem nachzuweisen. Wenn RSA-2048
1447 in der TI abgekündigt wird, entfällt dadurch die Anforderung.
1448

1449 TIP1-A_5393 - Dokumentation der Konnektorzertifikatszuordnungen
1450 Der Hersteller des Konnektors MUSS die Zuordnung von Konnektor und jeweils
1451 eingebrachtem C.NK.VPN-Zertifikat mit dem Ziel dokumentieren, anhand eines
1452 Sperrauftrages für einen Konnektor, das zu sperrende C.NK.VPN-Zertifikat identifizieren
1453 zu können.
1454 [\leq]

1455 Das bedeutet, dass der Konnektorhersteller je Konnektor die für die Identifikation des
1456 C.NK.VPN-Zertifikates relevanten Daten wie z. B. Seriennummer des Konnektors und Art
1457 der verbauten Komponenten, Seriennummer der gSMC-K, etc. für seinen Sperrprozesse
1458 dokumentieren muss.

1459 TIP1-A_5394 - Bereitstellen eines Konnektorsperrprozesses

- 1460 Der Hersteller des Konnektors MUSS für die von ihm verantworteten Konnektoren einen
1461 Sperrprozess etablieren, unterhalten und der gematik zugänglich machen.
1462 Der Hersteller des Konnektors KANN die operative Durchführung des Sperrprozesses an
1463 Dritte delegieren.
1464 **[<=]**
- 1465 Sperrberechtigt ist die gematik im Rahmen des Change-Verfahrens (siehe
1466 [gemRL_Betr_TI#5.4]).
- 1467 TIP1-A_5395 - Sperrberechtigung der gematik gegenüber Konnektorhersteller
1468 Der Hersteller des Konnektors MUSS im Rahmen der Change-Durchführung erteilte
1469 Sperraufträge der gematik fristgemäß (gemäß Change-Auftrag) bei dem TSP X.509
1470 nonQES (Zertifikatsaussteller) umsetzen.
1471 **[<=]**
- 1472 Dazu bedient er die standardmäßige Schnittstelle zum TSP (siehe
1473 [gemSpec_X.509_TSP#TIP1-A_3643]).
- 1474 TIP1-A_5396 - Prüfung des Sperrauftrages für Konnektoren
1475 Der Hersteller des Konnektors MUSS vor der Umsetzung des Sperrauftrages für einen
1476 Konnektor die Sperrberechtigung des Beauftragenden prüfen und verhindern, dass
1477 Konnektoren missbräuchlich gesperrt werden.
1478 **[<=]**
- 1479 TIP1-A_5397 - Umsetzung von Sperraufträgen für Konnektoren
1480 Der Hersteller des Konnektors MUSS nach erfolgreicher Prüfung der Sperrberechtigung
1481 des Beauftragenden die Sperrung der entsprechenden C.NK.VPN-Zertifikate unverzüglich
1482 bei dem TSP X.509 nonQES (Zertifikatsaussteller) beauftragen.
1483 **[<=]**
- 1484 TIP1-A_5398 - Beschränkung der Sperrberechtigung des Konnektorherstellers
1485 Der Hersteller des Konnektors DARF NICHT die Sperrung von C.NK.VPN-Zertifikaten bei
1486 dem TSP X.509 nonQES (Zertifikatsaussteller) beauftragen, wenn er nicht durch einen für
1487 den Konnektor Sperrberechtigten dazu beauftragt wurde.
1488 **[<=]**
- 1489 TIP1-A_5399 - Protokollierung der Sperrung von Konnektoren
1490 Der Hersteller des Konnektors MUSS die Durchführung der Sperrung eines Konnektors
1491 protokollieren und der gematik auf Anfrage übermitteln.
1492 Dabei MÜSSEN folgende Informationen protokolliert werden:
- 1493 • Zeitpunkt der Beantragung und Umsetzung der Sperrung
 - 1494 • Grund der Sperrung
 - 1495 • Konnektoridentifikation
- 1496 **[<=]**
- 1497 Der Hersteller des Konnektors übernimmt im Rahmen der organisatorischen Sperrung die
1498 Aufgabe der Anwenderkommunikation gegenüber den betroffenen Anwendern. Die
1499 Eckpunkte zur Kommunikation sind Bestandteil des Beschlusses zur Außerbetriebnahme
1500 einer Konnektor-Baureihe und im Rahmen des Change-Verfahrens zwischen den
1501 Beteiligten abgestimmt.
- 1502 TIP1-A_5400 - Fortführen des Konnektor-Sperrprozesses
1503 Der Hersteller des Konnektors MUSS die Fortführung des Sperrprozesses über die
1504 Einstellung seiner Geschäftstätigkeit hinaus gewährleisten.
1505 **[<=]**

1506 Dies kann bspw. durch Übertragung der Aufgabe an einen Dritten realisiert werden.
 1507 Dabei sind die Zuordnungen Konnektor zu Zertifikat gemäß Anforderung „Dokumentation
 1508 der Konnektorzertifikatszuordnungen“ zur Verfügung zu stellen.

1509 Bei der Schlüsselerzeugung für die gSMC-K muss insbesondere auch mit technischen
 1510 Maßnahmen die Vertraulichkeit der relevanten Schlüssel sichergestellt werden:

1511 TIP1-A_7225 - Schlüsselerzeugung bei einer Schlüsselspeicherpersonalisierung
 1512 Der Hersteller des Konnektors, der Schlüssel für die gSMC-K erzeugt, MUSS diese
 1513 Schlüssel mittels eines technischen Sicherheitsmoduls (HSM, Chipkarte, TPM etc.)
 1514 erzeugen, welches

- 1515 1. über einen Zugriffsschutz verfügt, sodass nur Berechtigte Schlüssel darauf nutzen
 1516 können,
- 1517 2. in einem zutrittsgeschützten Bereich aufbewahrt wird und
- 1518 3. mindestens nach FIPS 140-2 Level 3 oder [COS-G2] (CC-zertifizierte Chipkarte
 1519 der TI) zertifiziert ist.

1520 Wird für die Schlüsselerzeugung eine Schlüsselableitung verwendet, so MUSS die
 1521 Schlüsselableitung die fachlichen Anforderungen aus GS-A_5386 erfüllen.
 1522 Es ist zulässig, dass asymmetrische Schlüssel bei der Personalisierung auf der gSMC-K
 1523 selbst erzeugt werden und symmetrische Schlüssel mittels einer Schlüsselableitung
 1524 erzeugt werden, bei dem sich der Ableitungsschlüssel (Masterkey) innerhalb eines nach
 1525 3. zulässigen Hardwaresicherheitsmoduls befindet.

1526 Es ist zulässig, sicherheitstechnisch geeignete Maßnahmen zur Sicherstellung der
 1527 Verfügbarkeit der Ableitungsschlüssel (Masterkey) umzusetzen (bspw. Shamir Secret-
 1528 Sharing-Verfahren).

1529 Der Hersteller des Konnektors MUSS die Schlüsselerzeugung und die Schlüsselverwaltung
 1530 in einem Konzept darstellen, das die technischen und organisatorischen Maßnahmen
 1531 beschreibt, die den Schutzbedarf der verarbeiteten Informationsobjekte befriedigen. Der
 1532 Hersteller des Konnektors MUSS dieses Konzept der gematik zur Verfügung stellen.[<=]

1533 TIP1-A_5703 - Geschützte Übertragung von Daten zum Kartenpersonalisierer
 1534 Der Hersteller des Konnektors, der Daten für die gSMC-K erzeugt (bspw. Schlüssel),
 1535 MUSS diese Daten bei der Übertragung zum Kartenpersonalisierer hinsichtlich
 1536 Vertraulichkeit, Authentizität und Integrität mit einem Verfahren nach [gemSpec_Krypt]
 1537 schützen.
 1538 [<=]

1539 3.2 Bootup-Phase

1540 TIP1-A_4507 - Isolation während der Bootup-Phase
 1541 Da während der Bootup-Phase des Konnektors noch nicht alle Sicherheitsmechanismen
 1542 ihre Leistung erbringen können, DÜRFEN die Dienste des Konnektors während dem
 1543 Bootup über physikalische Schnittstellen von außen NICHT erreichbar sein.
 1544 [<=]

1545 TIP1-A_4508 - Konnektorzustand nach Bootup
 1546 Der Konnektor MUSS nach Beendigung der Bootup-Phase die Initialisierung der
 1547 Funktionsmerkmale durchlaufen haben. Die Startreihenfolge der Funktionsmerkmale
 1548 kann unter Berücksichtigung von TIP1-A_4507 herstellerspezifisch gestaltet werden.
 1549 Im Rahmen der Bootup-Phase MÜSSEN folgende TUCs ausgeführt werden:
 1550 TUC_KON_025, TUC_KON_035, TUC_KON_272, TUC_KON_341, TUC_KON_343,
 1551 TUC_KON_352 (die Reihenfolge der TUC-Ausführung ist herstellerspezifisch).
 1552 Treten während der Bootup-Phase Fehler auf, so MUSS die Bootup-Phase, sofern

1553 möglich, abgeschlossen werden.
 1554 Sobald die Bootup-Phase abgeschlossen ist, MUSS TUC_KON_256 „Systemereignis
 1555 absetzen“ mit folgenden Parameter aufgerufen werden:

```
1556 TUC_KON_256 {
1557     topic = "BOOTUP/BOOTUP_COMPLETE";
1558     eventType = Op;
1559     severity = Info;
1560 }
1561 [ $\leq$ ]
```

1562 Die hier gelisteten TUCs bilden nicht die abschließende Menge der während der Bootup-
 1563 Phase zu erfüllenden Anforderungen. In den einzelnen Funktionsmerkmalen werden
 1564 weitere Einzelanforderungen erhoben, die als Ausführungszeitpunkt die Bootup-Phase
 1565 benennen (siehe Unterkapitel „Betriebsaspekte“ der einzelnen Funktionsmerkmal-
 1566 Kapiteln, sowie Kapitel 4.3 Konnektormanagement).

1567 3.3 Betriebszustand

1568 TIP1-A_4509 - Betriebszustand erfassen

1569 Der Konnektor MUSS seinen Betriebszustand gemäß Tabelle TAB_KON_503
 1570 Betriebszustand_Fehlerzustandsliste über Fehlerzustände \$EC erfassen.
 1571 Tritt die in Spalte „Beschreibung“ charakterisierte Fehlersituation eines Fehlerzustandes
 1572 \$EC ein, wird sein Wert \$EC.value = true. Sobald die Fehlersituation beendet ist, springt
 1573 der Wert auf \$EC.value = false. Die Fehlerzustände müssen dabei innerhalb der „max.
 1574 Feststellungszeit“ (Tabellenspalte) erfasst werden. Eine maximale Feststellungszeit von
 1575 einen Tag (1 day) verlangt, dass einmal am Tag der Zustand geprüft werden muss,
 1576 unabhängig davon, welche TUCs aufgerufen werden. Eine maximale Feststellungszeit von
 1577 1 sec, 10 sec, 1 min und 300 sec verlangt, dass nach der Feststellung einer Fehlfunktion
 1578 innerhalb eines TUCs die Zustandsänderung innerhalb der angegebenen Zeit stattfinden
 1579 muss.
 1580 Nach Abschluss des Boot-Vorgangs müssen sämtliche Fehlerzustände mit einer „max.
 1581 Feststellungszeit“ von „1 day“ erfasst worden sein.
 1582 [\leq]

1583 TIP1-A_4597 - Unterstützung von Missbrauchserkennungen

1584 Der Konnektor MUSS zur Unterstützung von Missbrauchserkennungen für alle
 1585 Operationen, die in EVT_MONITOR_OPERATIONS gelistet sind und deren Alarmwert > 0
 1586 ist, kontinuierlich folgende Aktivitäten durchlaufen:

- 1587 1. Minütlich gleitende 10-Minuten-Summe je in EVT_MONITOR_OPERATIONS
 1588 gelistete Operation berechnen. Dazu gehen
 - 1589 • erfolgreiche Abschlüsse der Operation mit dem OK_Val der Operation ein
 - 1590 • eine fehlerhaft beendete Operation mit dem NOK_Val der Operation ein
- 1591 2. Überschreitet der gleitende 10-Minuten-Summenwert einer in
 1592 EVT_MONITOR_OPERATIONS gelisteten Operation den zugehörigen Alarmwert, so
 1593 setze EC_CRYPTOPERATION_ALARM auf True.

1594 [\leq]

1595 Erklärung „Minütlich gleitende 10-Minuten-Summe“: Für die jeweilige Operation wird die
 1596 Summe aller OK_Val und NOK_Val der letzten 10 Minuten gebildet. Diese Summe wird
 1597 jede Minute neu berechnet.

1598 TIP1-A_4512-02 - Ereignis bei Änderung des Betriebszustandes

1599 Der Konnektor MUSS per Ereignisdienst TUC_KON_256 über Änderungen des
 1600 Betriebszustandes (Tabelle TAB_KON_503 Betriebszustand_Fehlerzustandsliste)
 1601 informieren.
 1602 Der Konnektor muss dazu für jeden Fehlerzustand \$EC mit Error Condition
 1603 \$EC.errorcondition mit verändertem Wert \$EC.value den technischen Anwendungsfall
 1604 TUC_KON_256 „Systemereignis absetzen“ mit folgenden Parametern aufrufen:
 1605 TUC_KON_256 {
 1606 topic = "OPERATIONAL_STATE/\$EC.errorcondition";
 1607 eventType = \$EC.type;
 1608 severity = \$EC.severity;
 1609 parameters = („Value=\$EC.value, \$EC.parameterlist“)
 1610 }

1611 **Tabelle 3: TAB_KON_503 Betriebszustand_Fehlerzustandsliste**

ErrorCondition (siehe Hinweis 1)	Beschreibung	Type	Sev e rity	max. Fest stell ungs - zeit	Parameterlist (siehe Hinweis 2)
EC_CardTerminal_ Software_Out_Of_ Date (\$ctId)	Software auf Kartenterminal(\$ctId) ist nicht aktuell	Op	Info	1 day	CtID=\$ctId; Bedeutung= \$EC.description
EC_CardTerminal_ gSMC-KT_Certificate_ Expires_Soon (\$ctId)	Das Zertifikat der gSMC-KT im Kartenterminal(\$ctId) läuft in weniger als 5 Wochen ab	Op	Info	7 day s	CtID=\$ctId; Bedeutung= \$EC.description
EC_Connector_ Software_Out_ Of_Date	I_KSRS_Download::list_ Updates liefert mindestens eine UpdateInformation mit einer UpdateInformation/Firmware/ FWVersion > aktuelle Version der Konnektorsoftware, deren UpdateInformation/Firmware/ FWPriority = „Kritisch“	Op	Info	1 day	Bedeutung= \$EC.description
EC_FW_Update_Availa ble	I_KSRS_Download::list_ Updates liefert mindestens eine UpdateInformation mit einer UpdateInformation/Firmware/ FWVersion > aktuelle Version der Konnektor- oder Kartenterminalsoftware	Op	Info	1 day	Bedeutung= \$EC.description

EC_FW_Not_Valid_Status_Blocked	Konnektor Firmware muss aktualisiert werden. Zugang zur TI momentan nicht erlaubt.	Sec	Fatal	1 day	Bedeutung=\$EC.description
EC_Time_Sync_Not_Successful	der letzte Synchronisationsversuch der Systemzeit war nicht erfolgreich.	Op	Info	1 sec	LastSyncAttempt=\$lastSyncAttemptTimestamp; LastSyncSuccess=\$lastSyncSuccessTimestamp; Bedeutung=\$EC.description
EC_TSL_Update_Not_Successful	das letzte Update der TSL war nicht erfolgreich.	Op	Info	1 sec	Bedeutung=\$EC.description; LastUpdateTSL=\$lastUpdateTSLTimestamp
EC_TSL_Expiring	Systemzeit t mit $t > \text{NextUpdate-Element der TSL} - 7 \text{ Tage}$ und $t \leq \text{NextUpdate-Element der TSL}$	Sec	Info	1 day	NextUpdateTSL=\$NextUpdate-Element der TSL; Bedeutung=\$EC.description
EC_BNetzA_VL_Update_Not_Successful	Das letzte Update der BNetzA-VL war nicht erfolgreich	Op	Info	1 sec	LastUpdateBNetzAVL=\$lastUpdateBNetzAVLTimestamp; Bedeutung=\$EC.description
EC_BNetzA_VL_not_valid	Systemzeit t mit $t > \text{NextUpdate-Element der BNetzA-VL}$	Sec	Warning	1 day	NextUpdateBNetzAVL=\$NextUpdate-Element der BNetzA-VL; Bedeutung=\$EC.description
EC_TSL_Trust_Anchor_Expiring	Gültigkeit des Vertrauensankers ist noch nicht abgelaufen, läuft aber innerhalb von 30 Tagen ab.	Sec	Info	1 day	ExpiringDateTrustAnchor=Ablaufdatum der Vertrauensanker gültigkeit; Bedeutung=\$EC.description

EC_LOG_OVERFLOW	<p>Wenn im Rahmen der Regeln für die rollierende Speicherung von Logging-Einträgen Einträge gelöscht werden, die nicht älter als <code>SECURITY_LOG_DAYS</code>, <code>LOG_DAYS</code> bzw. <code>FM_<fmName>_LOG_DAYS</code> sind, tritt der Fehlerzustand ein. Der Fehlerzustand kann nur durch einen Administrator wieder zurückgesetzt werden. Unter Protokoll wird die Liste der auslösenden Protokolle angegeben.</p>	Op	Warning	1 sec	Protokoll=\$Protokoll; Bedeutung=\$EC.description
EC_CRL_Expiring	<p>Systemzeit <code>t</code> > NextUpdate der CRL – 3 Tage</p>	Sec	Warning	1 day	ExpiringDateCRL=NextUpdate der CRL; Bedeutung=\$EC.description
EC_Time_Sync_Pending_Warning	<p><code>MGM_LU_ONLINE=Enabled</code> und keine erfolgreiche Synchronisation der Systemzeit seit <code>d</code> Tagen und <code>d</code> > <code>NTP_WARN_PERIOD</code> und <code>d</code> <= <code>NTP_GRACE_PERIOD</code>. Nach einer Korrektur oder Bestätigung der Systemzeit durch einen Administrator muss der Konnektor wie nach einer erfolgreichen Zeitsynchronisation verfahren, d.h., der Tagezähler wird auf 0 zurückgesetzt.</p>	Sec	Warning	1 day	LastSyncSuccess=\$lastSyncSuccessTimestamp; Bedeutung=\$EC.description
EC_TSL_Out_Of_Date_Within_Grace_Period	<p>Systemzeit <code>t</code> mit <code>t</code> > NextUpdate-Element der TSL und <code>t</code> <= NextUpdate-Element der TSL + <code>CERT_TSL_DEFAULT_GRACE_PERIOD_DAYS</code> und eine neue TSL ist nicht verfügbar</p>	Sec	Warning	1 day	NextUpdateTSL=\$NextUpdate-Element der TSL; GracePeriodTSL= <code>CERT_TSL_DEFAULT_GRACE_PERIOD_DAYS</code> ; Bedeutung=\$EC.description

EC_CardTerminal_Not_Available (\$ctId)	Kartenterminal(\$ctId) ist nicht verfügbar. Dieser Betriebszustand bezieht sich auf die als „aktiv“ gekennzeichneten KTs.	Op	Error	1 sec	CtID=\$ctId; Bedeutung=\$EC.description
EC_No_VPN_TI_Connection	Kein sicherer Kanal (VPN) in die Telematikinfrastruktur aufgebaut. Der Wert 300 sec ist abgeleitet aus der maximalen Verbindungsaufbauzeit bei einem Standortausfall des VPN-Zugangsdienstes.	Op	Error	300 sec	Bedeutung=\$EC.description
EC_No_VPN_SIS_Connection	Kein sicherer Kanal (VPN) zu den Sicheren Internet Services aufgebaut. Der Wert 300 sec ist abgeleitet aus der maximalen Verbindungsaufbauzeit bei einem Standortausfall des VPN-Zugangsdienstes.	Op	Error	300 sec	Bedeutung=\$EC.description
EC_No_Online_Connection	Konnektor kann Dienste im Transportnetz nicht erreichen.	Op	Error	10 sec	Bedeutung=\$EC.description
EC_IP_Addresses_Not_Available	Die IP-Adressen des Netzkonnektors sind nicht oder falsch gesetzt.	Sec	Error	1 sec	Bedeutung=\$EC.description
EC_CRL_Out_Of_Date	Systemzeit t > Next Update der CRL	Sec	Fatal	1 day	NextUpdateCRL=\$NextUpdate der CRL; Bedeutung=\$EC.description
EC_Firewall_Not_Reliable	Firewall-Regeln konnten nicht fehlerfrei generiert werden oder beim Laden der Firewall-Regeln ist ein Fehler aufgetreten.	Sec	Fatal	1 sec	Bedeutung=\$EC.description

EC_Random_Generator_Not_Reliable	Der Zufallszahlengenerator kann die Anforderungen an die zu erzeugende Entropie nicht erfüllen.	Sec	Fatal	1 sec	Bedeutung= \$EC.description
EC_Secure_KeyStore_Not_Available	Sicherer Zertifikats- und Schlüsselspeicher des Konnektors (gSMC-K oder Truststore) nicht verfügbar	Sec	Fatal	1 sec	Bedeutung= \$EC.description
EC_Security_Log_Not_Writable	Das Sicherheitslog kann nicht geschrieben werden.	Op	Fatal	1 sec	Bedeutung= \$EC.description
EC_Software_Integrity_Check_Failed	Eine oder mehrere konnektorinterne Integritätsprüfungen der aktiven Konnektorbestandteile sind fehlgeschlagen.	Sec	Fatal	1 day	Bedeutung= \$EC.description
EC_Time_Difference_Intolerable	Abweichung zwischen der lokalen Zeit und der per NTP empfangenen Zeit bei der Zeitsynchronisation größer als NTP_MAX_TIMEDIFFERENCE. Nach einer Korrektur oder Bestätigung der Systemzeit durch einen Administrator muss der Konnektor den Fehlerzustand zurücksetzen.	Sec	Fatal	1 sec	NtpTimedifference= Zeitabweichung; NtpMaxAllowed Timedifference =NTP_MAX_TIMEDIFFERENCE; Bedeutung= \$EC.description

EC_Time_Sync_Pending_Critical	MGM_LU_ONLINE= Enabled und keine erfolgreiche Synchronisation der Systemzeit seit d Tagen und $d > \text{NTP_GRACE_PERIOD}$ Nach einer Korrektur oder Bestätigung der Systemzeit durch einen Administrator muss der Konnektor wie nach einer erfolgreichen Zeitsynchronisation verfahren, d.h., der Tagezähler wird auf 0 zurückgesetzt.	Sec	Fatal	1 day	LastSyncSuccess = \$lastSync SuccessTimestamp; NtpGracePeriod= NTP_GRACE_PERIOD; Bedeutung= \$EC.description
EC_TSL_Trust_Anchor_Out_Of_Date	Gültigkeit des Vertrauensankers ist abgelaufen	Sec	Fatal	1 day	ExpiringDateTrust Anchor= Ablaufdatum der Vertrauensanker gültigkeit; Bedeutung= \$EC.description
EC_TSL_Out_Of_Date_Beyond_Grace_Period	Systemzeit t mit $t > \text{NextUpdate-Element der TSL} + \text{CERT_TSL_DEFAULT_GRACE_PERIOD_DAYS}$ und eine neue TSL ist nicht verfügbar	Sec	Fatal	1 day	NextUpdateTSL = \$NextUpdate-Element der TSL; GracePeriodTSL = CERT_TSL_DEFAULT_GRACE_PERIOD_DAYS; Bedeutung= \$EC.description
EC_CRYPTOPERATION_ALARM	Gemäß TIP1-A_4597 wurde ein potentieller Missbrauch einer Kryptooperation erkannt. Nur der Administrator kann die Alarmmeldung zurücksetzen.	Sec	Warning	1 min	Operation= \$Operationsname; Count=\$Summenwert; Arbeitsplatz= \$<Liste operationsaufrufen workplaceIDs>; Meldung= 'Auffällige Häufung von Operationsaufrufen in den letzten 10 Minuten'

EC_OTHER_ ERROR_ STATE(\$no)	Herstellerspezifische Fehlerzustände, die per \$no (von 1 aufsteigend nummeriert) identifiziert werden. \$Type, \$Severity und \$ParameterList legt der Hersteller nach Bedarf fest.	\$Type	\$Severity	<= 1 day	Bedeutung= \$EC.description
------------------------------------	--	--------	------------	-------------	--------------------------------

1612 **Erläuterungen zu TAB_KON_503:**

1613 Hinweis 1:
1614 Jeder Fehlerzustand wird durch einen eindeutigen ErrorCondition identifiziert. Dieser kann
1615 einen Parameter enthalten. Sind etwa die Kartenterminals mit ctId=47 und das mit ctId=93
1616 nicht erreichbar, so lauten die ErrorCondition „EC_CardTerminal_Not_Available(47)“ und
1617 „EC_CardTerminal_Not_Available(93)“.

1618 Hinweis 2:
1619 EC.description referenziert den Text, der in der Spalte „Beschreibung“ des Zustandes
1620 spezifiziert wurde.

1621 **[<=]**

1622 Unter „kartenbasiert“ sind nicht nur Lösungen mit Smartcards sondern auch solche mit
1623 HSMs (Hardware Security Modules) zu verstehen.

1624 A_17085 - Bedingung für den Fehlerzustand EC_No_VPN_TI_Connection
1625 Wenn MGM_LU_ONLINE=Enabled nicht erfüllt ist, DARF der Konnektor den
1626 Zustand EC_No_VPN_TI_Connection NICHT annehmen. [**<=**]

1627 A_17086 - Bedingung für den Fehlerzustand EC_No_VPN_SIS_Connection
1628 Wenn MGM_LU_ONLINE=Enabled oder ANLW_INTERNET_MODUS=SIS nicht erfüllt ist,
1629 DARF der Konnektor den Zustand EC_No_VPN_SIS_Connection NICHT annehmen. [**<=**]

1630 A_17087 - Bedingung für den Fehlerzustand EC_No_Online_Connection
1631 Wenn MGM_LU_ONLINE=Enabled nicht erfüllt ist, DARF der Konnektor den
1632 Zustand EC_No_Online_Connection NICHT annehmen. [**<=**]

1633

1634 **Tabelle 4: TAB_KON_504 Ausführungserlaubnis für Dienste in kritischen**
1635 **Fehlerzuständen**

	EC_ Soft ware _ Inte grity _ Chec k_ Faile d	EC_ Rand om_ Gene rator _ Not_ Relia ble	EC_ Sec urity _ Log _ Not_ Writ able	EC_ Tim e_ Syn c_ Pen ding _ Criti cal	EC_ _ Ti me _ Dif fe ren ce _ Int ole r abl e	E C _ C RL _ O ut _ Of _ D at e	EC_ TSL _ Out _ Of_ Dat e_ Bey ond _ Gra ce_ Peri od	EC_ TSL _ Tru st_ Anc hor _ Out _ Of_ Dat e	EC_ Secu re_ KeyS tore _ Not_ Avail able	EC_ FW _ Not_ Vali d_ Sta tus _ Blo cke d
--	--	--	--	---	---	--	--	---	--	--

Technische Use Cases (TUCs) der Basisdienste relevant für Fachanwendung und die Kommunikation mit Weiteren Anwendungen und SIS										
Zugriffsberechtigungsdienst										
TUC_KON_000 Prüfe Zugriffsberechtigung	-	x	x	x	x	x	x	x	x	x
Dienstverzeichnisdienst										
TUC_KON_041 Einbringen der Endpunktnformationen während der Bootup-Phase	-	-	-	x	x	x	x	x	x	x
Kartenterminaldienst										
TUC_KON_051 Mit Anwender über Kartenterminal interagieren	-	-	-	-	-	x	x	x	-	x
Kartendienst										
TUC_KON_005 Card-to-Card authentisieren	-	-	-	-	-	x	x	x	-	x
TUC_KON_006 Datenzugriffsaudit eGK schreiben	-	-	-	-	-	x	x	x	-	x
TUC_KON_018 eGK-Sperrung prüfen	-	-	-	-	-	x	x	x	-	x
TUC_KON_024 Karte zurücksetzen	-	-	-	-	-	x	x	x	-	x
TUC_KON_026 Liefere CardSession	-	-	-	-	-	x	-	x	-	-
TUC_KON_200 SendeAPDU	-	-	-	-	-	x	x	x	-	x
TUC_KON_202 LeseDatei	-	-	-	-	-	x	x	x	-	x

TUC_KON_203 SchreibeDatei	-	-	-	-	-	x	x	x	-	x
TUC_KON_209 LeseRecord	-	-	-	-	-	x	x	x	-	x
Systeminformationsdienst										
TUC_KON_256 Systemereignis absetzen	-	x	x	x	x	x	x	x	x	x
Verschlüsselungsdienst										
TUC_KON_072 Daten symmetrisch verschlüsseln	-	-	-	x	x	x	x	x	-	x
TUC_KON_073 Daten symmetrisch entschlüsseln	-	-	-	x	x	x	x	x	-	x
Zertifikatsdienst										
TUC_KON_034 Zertifikatsi nformationen extrahieren	-	-	-	x	x	x	x	x	-	x
Protokollierungsdienst										
TUC_KON_271 Schreibe Protokolleintrag	-	x	x	x	x	x	x	x	x	x
TLS-Dienst										
TUC_KON_110 Kartenbasi erte TLS- Verbindung aufbauen	-	-	-	-	-	-	-	-	-	-
Verbindung zum VPN- Konzentrator										
TUC_VPN-ZD_0001 „IPsec Tunnel TI aufbauen“	-	-	-	-	-	-	-	-	-	-

TUC_VPN-ZD_0002 „IPsec Tunnel SIS aufbauen“	-	-	-	-	-	-	-	-	-	-
Operationen der Basisdienste										
Kartendienst										
VerifyPin	-	-	-	-	-	x	x	x	-	x
UnblockPin	-	-	-	-	-	x	x	x	-	x
ChangePin	-	-	-	-	-	x	x	x	-	x
GetPinStatus	-	-	-	-	-	x	x	x	-	x
Systeminformationsdienst										
Schnittstelle der Ereignissenke	-	x	x	x	x	x	x	x	x	x
GetCardTerminals	-	x	x	x	x	x	x	x	x	x
GetCards	-	x	x	x	x	x	x	x	x	x
GetResourceInformation	-	x	x	x	x	x	x	x	x	x
Subscribe	-	x	x	x	x	x	x	x	x	x
RenewSubscription	-	x	x	x	x	x	x	x	x	x
Unsubscribe	-	x	x	x	x	x	x	x	x	x
GetSubscription	-	x	x	x	x	x	x	x	x	x
Verschlüsselungsdienst										
EncryptDocument	-	-	-	-	-	x	x	x	-	x
DecryptDocument	-	-	-	-	-	x	x	x	-	x
Signaturdienst										
SignDocument	-	-	-	-	-	x	x	x	-	x

VerifyDocument	-	-	-	-	-	x	x	x	-	x
GetJobNumber	-	-	-	-	-	x	x	x	-	x
StopSignature	-	-	-	-	-	x	x	x	-	x
ActivateComfortSignature	-	-	-	-	-	x	x	x	-	x
DeactivateComfortSignature	-	-	-	-	-	x	x	x	-	x
GetSignatureMode	-	-	-	-	-	x	x	x	-	x
Authentifizierungsdienst										
ExternalAuthenticate	-	-	-	-	-	x	x	x	-	x
Zertifikatsdienst										
ReadCardCertificate	-	-	-	-	-	x	x	x	x	x
CheckCertificateExpiration	-	-	-	-	-	x	x	x	x	x
VerifyCertificate	-	-	-	-	-	x	-	x	x	x
Zeitdienst										
I_NTP_Time_Information	-	-	-	-	-	x	x	x	x	-
Konnektormanagement										
Softwareaktualisierung	x	x	x	x	x	x	x	x	x	x
Protokolleinsicht	x	x	x	x	x	x	x	x	x	x
Werksreset	x	x	x	x	x	x	x	x	x	x
Sonstiges	-	x	x	x	x	x	x	x	x	x

In den kritischen Fehlerzuständen, in denen keine TLS-Verbindung ins LAN aufgebaut werden (EC_Random_Generator_Not_Reliable, EC_Software_Integrity_Check_Failed, EC_Security_Log_Not_Writable, EC_Time_Sync_Pending_Critical, EC_Time_Difference_Intolerable), kann keine Verbindung zu den Kartenterminals aufgebaut werden. Infolge sind hier keine Kartenoperationen zugelassen.

1641 Wenn keine Verbindung zum VPN-Konzentrator des SIS aufgebaut werden kann, ist
1642 dadurch das Internet nicht über den Konnektor erreichbar. Wenn keine Verbindung zum
1643 VPN-Konzentrator der TI aufgebaut werden kann, sind Bestandsnetze nicht erreichbar.

1644 Bezüglich der Administration des Konnektors im Zustand EC_FIREWALL_NOT_RELIABLE
1645 ist eine Abstimmung mit der Prüfstelle und der Zertifizierungsstelle notwendig.

1646 A_16203 - Nutzbarkeit im Zustand EC_FIREWALL_NOT_RELIABLE

1647 Im Zustand EC_Firewall_Not_Reliable DARF der Konnektor NICHT nutzbar sein.

1648 Möglichkeiten zur Behebung des Zustandes EC_Firewall_Not_Reliable sind mit dem CC -
1649 Evaluierer und Zertifizierer abzustimmen. [\leq]

1650 Die Architektur der TI ist so angelegt, dass die Fehlerzustände mit Severity=Fatal in den
1651 Tabellen TAB_KON_504 und TAB_KON_503 mit vernachlässigbarer Wahrscheinlichkeit
1652 von externen Einflüssen abhängen. Die SLAs für Dienste der zentralen TI-Plattform sind
1653 so gefasst, dass diese schwerwiegend verletzt werden müssten, um dadurch einen
1654 Konnektor in einen solchen kritischen Zustand zu bringen (externer Fehler aus Sicht des
1655 Konnektors). Dass beispielsweise der TSL-Dienst über den Zeitraum der Grace-Period-
1656 TSL (typisch: 7 Tage) nicht erreichbar ist (ErrorCondition EC_TSL_Out_Of_Date
1657 _Beyond_Grace_Period), kann nur bei massiver Verletzung der für zentrale Dienste
1658 festgelegten SLAs eintreten.

1659 Um die konnektorinternen Fehlerquellen zu erfassen, die dazu führen, dass ein
1660 Fehlerzustand mit Severity=Fatal eintritt oder ein anderer Zustand, in dem der
1661 Konnektor nicht verwendbar ist, wird Folgendes gefordert:

1662 TIP1-A_5148 - Performance - Konnektor - Mittlerer Abstand zwischen Ausfällen

1663 Der Konnektorhersteller MUSS den mittleren Zeitabstand zwischen Ausfällen (MTBF) als
1664 Produkteigenschaft ausweisen. Der Konnektor soll einen mittleren Zeitabstand zwischen
1665 Ausfällen (MTBF) von mindestens 50 Jahren haben.

1666 Ein „Ausfall“ gilt dann als eingetreten, wenn

- 1667 • der Konnektor nicht mehr gebootet werden kann, d. h. kein
1668 „BOOTUP/BOOTUP_COMPLETE“ Event ausgelöst wird, und dies nicht auf einen
1669 externen Fehler zurückzuführen ist,
- 1670 • oder sich der Konnektor in einem Fehlerzustand mit Severity=Fatal befindet, der
1671 nicht auf einen externen Fehler zurückzuführen ist,
- 1672 • oder Funktionen des Konnektors ausgefallen sind, ohne dass dies auf externe
1673 Fehler zurückzuführen ist.

1674 [\leq]

1675 Bei einem mittleren Zeitabstand zwischen Ausfällen (MTBF) von 50 Jahren ist die
1676 Wahrscheinlichkeit, dass ein Fehlerzustand mit Severity=Fatal auftritt, kleiner 2 % pro
1677 Jahr.

1678 TIP1-A_4510-03 - Sicherheitskritische Fehlerzustände

1679 Der Konnektor MUSS bei eingetretenem Fehlerzustand aus Tabelle Tab_Kon_503
1680 Betriebszustand_Fehlerzustandsliste mit Severity=Fatal dafür sorgen, dass von den
1681 Operationen der Basisdienste und Technische Use Cases (TUCs) der Basisdienste, die
1682 relevant für Fachanwendungen sind, nur erlaubte Operationen und TUCs gestartet und
1683 ausgeführt werden.

1684 Welche Operationen und TUCs je eingetretenem Fehlerzustand ausgeführt werden
1685 dürfen, legt Tabelle „TAB_KON_504 Ausführungserlaubnis für Dienste in kritischen
1686 Fehlerzuständen“ fest: Jede Erlaubnis ist dort durch ein „x“ definiert.

1687 Abweichend zu Angaben in der Tabelle TAB_KON_504 DÜRFEN folgende Operationen und
1688 TUCs NICHT im Zustand EC_Firewall_Not_Reliable ausgeführt werden:

- 1689 • TUC_KON_000 PrüfeAufrufkontext
- 1690 • TUC_KON_041 Einbringen der Endpunktinformationen während der Bootup-Phase
- 1691 • GetCardTerminals
- 1692 • GetCards
- 1693 • GetResourceInformation
- 1694 • Subscribe
- 1695 • RenewSubscription
- 1696 • Unsubscribe
- 1697 • GetSubscription
- 1698 • ReadCardCertificate
- 1699 • CheckCertificateExpiration
- 1700 • VerifyCertificate

1701 Sind mehrere Fehlerzustände gleichzeitig eingetreten, dürfen nur die Operationen und
 1702 TUCs ausgeführt werden, die für alle eingetretenen Fehlerzustände erlaubt sind. Der
 1703 Konnektor muss Anfragen, die auf Grund eines kritischen Fehlerzustandes nicht
 1704 ausgeführt oder abgebrochen werden, mit einem Fehler (Fehlercode 4002) beantworten.
 1705

1706 **Tabelle 5: TAB_KON_502 Fehlercodes „Betriebszustand“**

Fehlercode	ErrorType	Severity	Fehlertext
4002	Security	Fatal	Der Konnektor befindet sich in einem kritischen Betriebszustand

1707
 1708 [\leq]

1709 3.3.1 Betriebsaspekte

1710 Der Konnektor soll per Signaleinrichtung am Konnektor die Fehlerzustände mit Severity
 1711 „Error“ und „Fatal“ anzeigen (siehe [TIP1-A_4843]).

1712 TIP1-A_4513 - Betriebszustände anzeigen und Fehlerzustände zurücksetzen
 1713 Der Konnektor MUSS es dem Administrator ermöglichen, den aktuellen Betriebszustand
 1714 einzusehen und Fehlerzustände zurückzusetzen, soweit diese Möglichkeit in Tabelle
 1715 „TAB_KON_503 Betriebszustand_Fehlerzustandsliste“ für den jeweiligen Fehlerzustand
 1716 festgelegt ist.

1717 Ferner MUSS es die Managementschnittstelle dem Administrator ermöglichen,
 1718 Konfigurationsänderungen gemäß Tabelle TAB_KON_505 vorzunehmen:

1719 **Tabelle 6: TAB_KON_505 Konfigurationswerte Missbrauchserkennung**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
EVT_MONITOR_OPERATIONS	Liste von: - Operationsname - OK_Val (Nummer) - NOK_Val	Der Administrator MUSS in der Liste der zur Missbrauchserkennung überwachbaren Operationen alle Listeneinträge einsehen können. Er MUSS den jeweiligen Alarmwert

	(Nummer) - Alarmwert (Nummer)	editieren können (0-9999, 0=deaktiviert). OK_VAL und NOK_VAL DÜRFEN durch den Administrator NICHT veränderbar sein.
--	-------------------------------------	---

1720
1721 [\leq]

1722 3.4 Fachliche Anbindung der Clientsysteme

1723 Für die Schnittstellen des Konnektors zu den Clientsystemen kann gesteuert werden:

- 1724 • ob die Kommunikation zwischen Konnektor und Clientsystemen hinsichtlich
- 1725 Vertraulichkeit, Integrität und Authentizität zwingend durch TLS gesichert
- 1726 werden muss
- 1727 • ob sich Clientsysteme zwingend authentisieren müssen
- 1728 • welche Clientsysteme auf den Konnektor zugreifen dürfen (Whitelisting)

1729 Dabei werden die folgenden zwei Nutzungsszenarien nicht unterschieden:

- 1730 • Nutzung von Fachanwendungen (in Form von Fachmodulen)
- 1731 • Nutzung von Basisdiensten des Konnektors

1732 Sowohl die Anbindung zur Administration des Konnektors, als auch die Anbindung zur

1733 Nutzung von Bestandsnetzen oder dem gesicherten Internetzugang sind nicht

1734 Gegenstand dieser Schnittstellenfestlegungen. Für die Anbindung zu Administration wird

1735 diese im Kapitel Konnektormanagement beschrieben, für die Anbindung von

1736 Bestandsnetzen bzw. dem gesicherten Internetzugang ist diese Art der Regelung nicht

1737 erforderlich, da es sich dort um Routing-Funktionen handelt.

1738 Die seitens des Administrators einstellbaren Werte und Listen sind, der allgemeinen

1739 Struktur dieses Dokuments folgend, im Unterkapitel 3.4.1 Betriebsaspekte beschrieben.

1740

1741 TIP1-A_4514 - Verfügbarkeit einer TLS-Schnittstelle

1742 Der Konnektor MUSS TLS in Richtung der Clientsysteme für alle Außenschnittstellen der

1743 Basisdienste:

- 1744 • Dienstverzeichnisdienst
- 1745 • Kartenterminaldienst
- 1746 • Systeminformationsdienst
- 1747 • Verschlüsselungsdienst
- 1748 • Signaturdienst
- 1749 • Zertifikatsdienst
- 1750 • Kartendienst
- 1751 • LDAP-Proxy

1752 unterstützen.

1753 Ferner MUSS der Konnektor für die SOAP-Endpunkte der Fachmodule TLS unterstützen.

1754 Der Konnektor MUSS sich mittels ID.AK.AUT gegenüber dem Client authentisieren.

1755 [\leq]

- 1756 TIP1-A_4515 - Verpflichtung zur Nutzung der TLS-Verbindung
 1757 Der Konnektor MUSS immer TLS-Verbindungsanfragen von Clientsystemen annehmen.
 1758 Der Konnektor MUSS bei gesetzter Variable ANCL_TLS_MANDATORY = Enabled den
 1759 Verbindungsversuch von Clientsystemen ohne TLS ablehnen. Ausgenommen hiervon sind
 1760 Anfragen an den Dienstverzeichnisdienst bei gesetzter Variable ANCL_DVD_OPEN =
 1761 Enabled.
 1762 [\leq]
- 1763 TIP1-A_4516 - Authentifizierung der Clients über Basic-Auth und X.509-Zertifikate
 1764 Der Konnektor MUSS zur Client-Authentifizierung die Verfahren Basic Authentication
 1765 (Username/Password) [RFC2617] über HTTP/TLS [RFC2818] und zertifikatsbasierte
 1766 Client-Authentifizierung (X.509) [gemSpec_PKI#8.3.1.4] über TLS anbieten.
 1767 Dabei MUSS für eine erfolgreiche Prüfung bei Basic Authentication:
- 1768 • das seitens des Clientsystems präsentierte Credential in ANCL_CUP_LIST
 - 1769 enthalten sein
- 1770 Für eine erfolgreiche Prüfung mit zertifikatsbasierter Client-Authentifizierung MUSS:
- 1771 • das seitens des Clientsystems präsentierte Zertifikat in ANCL_CCERT_LIST
 - 1772 enthalten sein
 - 1773 • die Zertifikatsprüfung (nur Prüfung auf „mathematische Korrektheit“ und
 - 1774 „Gültigkeit nicht abgelaufen“) erfolgreich durchlaufen werden
- 1775 Schlägt die Prüfung fehl, MUSS der Verbindungsversuch des Clientsystem abgelehnt
 1776 werden.[\leq]
- 1777 Bei der Authentisierung des Clientsystems geht es um eine Authentisierung in zwei
 1778 Richtungen:
- 1779 1. Authentisierung des Clientsystems in der Rolle eines Clients gegenüber dem
 - 1780 Konnektor für die Übertragung von SOAP-Requests.
 - 1781 2. Authentisierung des Clientsystems in der Rolle eines Servers gegenüber dem
 - 1782 Konnektor zum Empfang von CETP-Ereignismitteilungen des
 - 1783 Systeminformationsdienstes.
- 1784 Für beide Richtungen kann das Clientsystem dasselbe Zertifikat verwenden.
- 1785 TIP1-A_5009 - Authentifizierungsvarianten für Verbindungen zwischen Konnektor und
 1786 Clientsystemen
 1787 Der Konnektor MUSS für Verbindungen zu Clientsystemen als Authentifizierungsmethode
 1788 ausschließlich folgende Varianten erlauben:
- 1789 1. Für Verbindungen mit dem Konnektor in der Rolle des Servers (SOAP-Requests):
 - 1790 • TLS-Server-Authentifizierung des Konnektors und TLS-Client-Authentifizierung
 - 1791 des Clientsystems
 - 1792 • TLS-Server-Authentifizierung des Konnektors und BasicAuthentifizierung des
 - 1793 Clientsystems
 - 1794 • TLS-Server-Authentifizierung des Konnektors ohne TLS-Client-
 - 1795 Authentifizierung des Clientsystems
 - 1796 • Keine Authentifizierung des Konnektors und des Clientsystems
 - 1797 2. Für Verbindungen mit dem Konnektor in der Rolle des Clients (CETP-Protokoll):
 - 1798 • TLS-Server-Authentifizierung des Clientsystems und TLS-Client-
 - 1799 Authentifizierung des Konnektors

1800 • TLS-Server-Authentifizierung des Clientsystems ohne TLS-Client-
1801 Authentifizierung des Konnektors

1802 • Keine Authentifizierung des Konnektors und des Clientsystems

1803 Alle anderen Verbindungsversuche von Clientsystemen MÜSSEN vom Konnektor
1804 abgelehnt werden.
1805 [\leq]

1806 Für die Anbindung der Clientsysteme ergeben sich verschiedene Konfigurationsvarianten
1807 bezüglich der Absicherung der Verbindungen zwischen Konnektor und Clientsystemen.
1808 Tabelle TAB_KON_852 listet die Varianten für die Verbindungen zum Aufruf der
1809 WebService-Schnittstellen (Varianten SOAP1 bis SOAP4), für die Verbindungen zum
1810 Senden von Events (Varianten CETP1 und CETP2) und für Verbindungen zum Abruf des
1811 Dienstverzeichnisses (Varianten DVD1, DVD2 und DVD3).

1812 **Tabelle 7: TAB_KON_852 Konfigurationsvarianten der Verbindungen zwischen Konnektor**
1813 **und Clientsystemen**

Konfigu- rations- variant e	ANCL_ TLS_ MAN- DATORY	ANCL_ CAUT_ MAN- DATORY	ANCL_ CAUT_ MODE	ANCL_ DVD_ OPEN	Bedeutung
CETP1	Enabled	Irrelevant	Irrelevant	Irrelevant	Der Konnektor sendet Events ausschließlich über TLS. Er authentisiert sich, wenn ihn das Clientsystem im Rahmen des TLS-Handshakes dazu auffordert.
CETP2	Disabled	Irrelevant	Irrelevant	Irrelevant	Der Konnektor sendet Events immer über eine TCP-Verbindung ohne TLS.
SOAP1	Enabled	Enabled	CERTIFICATE	Irrelevant	Der Konnektor akzeptiert vom Clientsystem nur Aufrufe über TLS. Der Konnektor verlangt beim TLS-Handshake die Authentisierung des Clientsystems per Zertifikat.
SOAP2	Enabled	Enabled	PASSWORD	Irrelevant	Der Konnektor akzeptiert vom Clientsystem nur Aufrufe über TLS. Der Konnektor prüft auf Anwendungsebene, dass Aufrufer sich per Username/Password [RFC2617] authentisieren.
SOAP3	Enabled	Disabled	Irrelevant	Irrelevant	Der Konnektor akzeptiert vom Clientsystem nur Aufrufe über TLS. Der Konnektor nimmt keine Clientauthentifizierung vor.

SOAP4	Disabled	Irrelevant	Irrelevant	Irrelevant	Der Konnektor akzeptiert vom Clientsystem sowohl Aufrufe ohne TLS als auch über TLS. Im zweiten Fall sollte der Konnektor das Clientsystem nicht authentifizieren, wenn er es aber für den Sonderfall ANCL_CAUT_MANDATORY=Enabled aktuell tut, sehen wir das nicht als Fehler.
DVD1	Irrelevant	Irrelevant	Irrelevant	Enabled	Zugriff auf Dienstverzeichnisdienst kann über HTTP und HTTPS erfolgen.
DVD2	Enabled	*	*	Disabled	Zugriff auf Dienstverzeichnisdienst kann nur über HTTPS erfolgen. *) Bzgl. Clientauthentisierung wirken die Schalter wie in SOAP 1, SOAP 2, SOAP 3
DVD3	Disabled	Irrelevant	Irrelevant	Disabled	Zugriff auf Dienstverzeichnisdienst kann über HTTP und HTTPS erfolgen.

3.4.1 Betriebsaspekte

Damit sich ein Clientsystem mittels X.509 authentisieren kann, muss es über ein entsprechendes Zertifikat verfügen. Diese Zertifikate kann der Administrator entweder mit seinen lokalen Mitteln selbst oder mittels des Konnektors erzeugen. In beiden Fällen müssen diese Zertifikate sowohl im Clientsystemen (hier zusammen mit ihren privaten Schlüsseln), als auch im Konnektor vorhanden sein.

Da es sich um eine lokal begrenzte Authentisierung im Verantwortungsbereich des Betreibers des lokalen Netzes handelt, werden keine weiteren Vorgaben zu den Schlüsselspeichern auf Clientsystemseite erhoben. Auch hinsichtlich der außerhalb des Konnektors erzeugten Zertifikate gelten keine weiteren Vorgaben. Ferner ist eine Online-Prüfung dieser Zertifikate nicht erforderlich.

TIP1-A_4517 - Schlüssel und X.509-Zertifikate für die Authentisierung des Clientsystems erzeugen und exportieren sowie X.509-Zertifikate importieren

Der Konnektor MUSS die Erstellung und den Export von X.509-Zertifikaten für Clientsysteme und der zugehörigen privaten Schlüssel durch den Administrator über das Managementinterface ermöglichen. Hierbei MUSS der Konnektor dem Administrator die Möglichkeit geben, das kryptographische Verfahren RSA-2048 oder ECC-256 auszuwählen. Als Exportformat MUSS PKCS#12 verwendet werden. Die so erstellten Zertifikate werden zu ANCL_CCERT_LIST angefügt.

Der Konnektor MUSS dem Administrator ferner den Import von konnektorfremden X.509-Zertifikaten für Clientsysteme über das Managementinterface ermöglichen. Die so importierten Zertifikate werden zu ANCL_CCERT_LIST angefügt.

[<=]

TIP1-A_4518 - Konfiguration der Anbindung Clientsysteme

1838 Der Administrator MUSS in der Managementoberfläche die in TAB_KON_506 genannten
1839 Parameter im Managementinterface konfigurieren können.
1840 Wird ANCL_TLS_MANDATORY auf ENABLED gewechselt, MÜSSEN alle nicht per TLS
1841 gesicherten http-Verbindungen geschlossen werden, sobald die in den Verbindungen
1842 jeweils aktuell laufenden Außenschnittstelle-Operationen abgeschlossen wurden, mit
1843 Ausnahme von http-Verbindungen zum Dienstverzeichnisdienst.
1844 Der Konnektor MUSS den Administrator geeignet und verständlich auf seine
1845 Verantwortung für die Sicherung der Kommunikation hinweisen.

1846 **Tabelle 8: TAB_KON_506 Konfigurationsparameter der Clientsystem-Authentisierung**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
ANCL_TLS_MANDATORY	Enabled/Disabled	Der Administrator MUSS die verpflichtende Verwendung eines TLS gesicherten Kanals an- oder abschalten können. Wenn ANLW_ANBINDUNGS_MODUS = Parallel MUSS der Administrator vor dem Disablen von ANCL_TLS_MANDATORY einen Warnhinweis bestätigen, der ihn über die mit der Abschaltung verbundenen Risiken informiert und darlegt, dass in diesem Fall der Nutzer die Verantwortung für die Sicherstellung der vertraulichen Übertragung übernimmt. Default-Wert: Enabled
ANCL_CAUT_MANDATORY	Enabled/Disabled	Der Administrator MUSS die verpflichtende Authentifizierung der Clientsysteme an- oder abschalten können. Default-Wert: Enabled
ANCL_CAUT_MODE	CERTIFICATE / PASSWORD	Der Administrator MUSS konfigurieren können, welcher Client Authentifizierungsmodus genutzt werden kann bzw. genutzt werden muss. Default-Wert: CERTIFICATE
ANCL_CCERT_LIST	Liste von X.509-Zertifikaten zugeordnet zu ClientID	Whitelist an importierten oder vom Konnektor erzeugten X.509-Zertifikaten und dazugehörigen Clientsystem IDs. Der Administrator MUSS die Liste der Zertifikate und den zugehörigen Clientsystemen verwalten können, der Inhalt der Zertifikate MUSS menschlich lesbar dargestellt werden. Es muss für den Administrator erkennbar sein, welches kryptographische Verfahren (RSA-2048

		oder ECC -256) dem jeweiligen Zertifikat zugrunde liegt.
ANCL_CUP_LIST	Liste von Benutzer/Passwort Kombinationen, zugeordnet zu ClientID	Whitelist an UserCredentials und dazugehörigen Clientsystem IDs. Der Administrator MUSS eine Liste von Credentials und zugehörigem Clientsystem verwalten können. Bei diesen Benutzer-/Passwortkombinationen handelt es sich nicht um personenbezogene Credentials, sondern um clientbezogene.
ANCL_DVD_OPEN	Enabled/Disabled	Der Administrator MUSS konfigurieren können, ob der Zugriff auf den Dienstverzeichnisdienst auch dann über einen ungesicherten http-Kanal erfolgen kann (ENABLED), wenn ANCL_TLS_MANDATORY = ENABLED ist. Default-Wert: Enabled

1847
1848 [\leq]

1849 3.5 Clientsystemschnittstelle

1850 TIP1-A_5401 - Parallele Nutzbarkeit Clientsystemschnittstelle
1851 Alle Schnittstellen, die der Konnektor den Clientsystemen zur Verfügung stellt, MÜSSEN
1852 parallel durch mehrere Aufrufer nutzbar sein.
1853 [\leq]

1854 3.5.1 SOAP-Schnittstelle

1855 Für die Beschreibung der SOAP-Schnittstelle zum Clientsystem wird in dieser
1856 Spezifikation WSDL Version 1.1 [WSDL1.1] eingesetzt. Die Interoperabilität zwischen
1857 verschiedenen SOAP-Implementierungen wird durch die Vorgaben des WS-I Basic Profile
1858 erreicht.

1859 A_15601 - SOAP für Web-Services der Basisdienste
1860 Der Konnektor MUSS für die an der Clientsystemschnittstelle definierten Web-Services
1861 der Basisdienste [SOAP1.1] verwenden. [\leq]

1862 TIP1-A_4519 - Web-Services konform zu [BasicProfile1.2]
1863 Der Konnektor MUSS die für die Clientsystemschnittstelle definierten Web-Services
1864 konform zu [BasicProfile1.2] anbieten.
1865 Abweichend von R1012 in [BasicProfile1.2] MUSS der Konnektor nur das Character
1866 Encoding UTF-8 unterstützen. Andere Kodierungen MUSS der Konnektor mit einem Fehler
1867 beantworten. [\leq]

1868 TIP1-A_4519-01 - ab PTV4: Web-Services konform zu [BasicProfile1.2]
1869 Der Konnektor MUSS die für die Clientsystemschnittstelle definierten Web-Services der
1870 Basisdienste konform zu [BasicProfile1.2] anbieten.
1871 [\leq]

1872 A_15606 - Character Encoding für Web-Services
 1873 Abweichend von R1012 in [BasicProfile1.2] und [BasicProfile2.0] MUSS der Konnektor
 1874 nur das Character Encoding UTF-8 unterstützen. Andere Kodierungen MUSS der
 1875 Konnektor mit einem Fehler beantworten. [≤]
 1876 Da der Konnektor UTF-16 nicht unterstützt, muss das Clientsystem den Request in UTF-8
 1877 kodieren. Diese Festlegungen gelten nur für die eigentliche SOAP-Nachricht. Sind in der
 1878 SOAP-Nachricht base64-encodierte XML-Elemente vorhanden, so können diese XML-
 1879 Elemente andere Zeichencodierungen aufweisen.

1880 Fachmodule

1881 Fachmodule können für Web-Services, die Clientsystemen bereitgestellt werden,
 1882 entweder [SOAP1.1] mit [BasicProfile1.2] oder [SOAP1.2] mit [BasicProfile2.0]
 1883 verwenden. Die genaue Ausprägung erfolgt in der jeweiligen Interfacebeschreibung des
 1884 Web-Services für das Fachmodul.

1885 A_15607 - SOAP für Web-Services der Fachmodule
 1886 Der Konnektor MUSS für die an der Clientsystemschnittstelle definierten Web-Services
 1887 der Fachmodule [SOAP1.1] und [SOAP1.2] unterstützen. Die SOAP-Version pro Web-
 1888 Service Endpunkt wird durch die WSDL des jeweiligen Web-Service definiert. [≤]

1889 A_15608 - Web-Services der Fachmodule konform zu [BasicProfile1.2]
 1890 Der Konnektor MUSS für die an der Clientsystemschnittstelle definierten Web-Services
 1891 der Fachmodule bei [SOAP1.1] die Profilierung konform zu [BasicProfile1.2]
 1892 anbieten. [≤]

1893 A_15609 - Web-Services der Fachmodule konform zu [BasicProfile2.0]
 1894 Der Konnektor MUSS für die an der Clientsystemschnittstelle definierten Web-Services
 1895 der Fachmodule bei [SOAP1.2] die Profilierung konform zu
 1896 [BasicProfile2.0] anbieten. [≤]
 1897

1898 3.5.2 Statusrückmeldung und Fehlerbehandlung

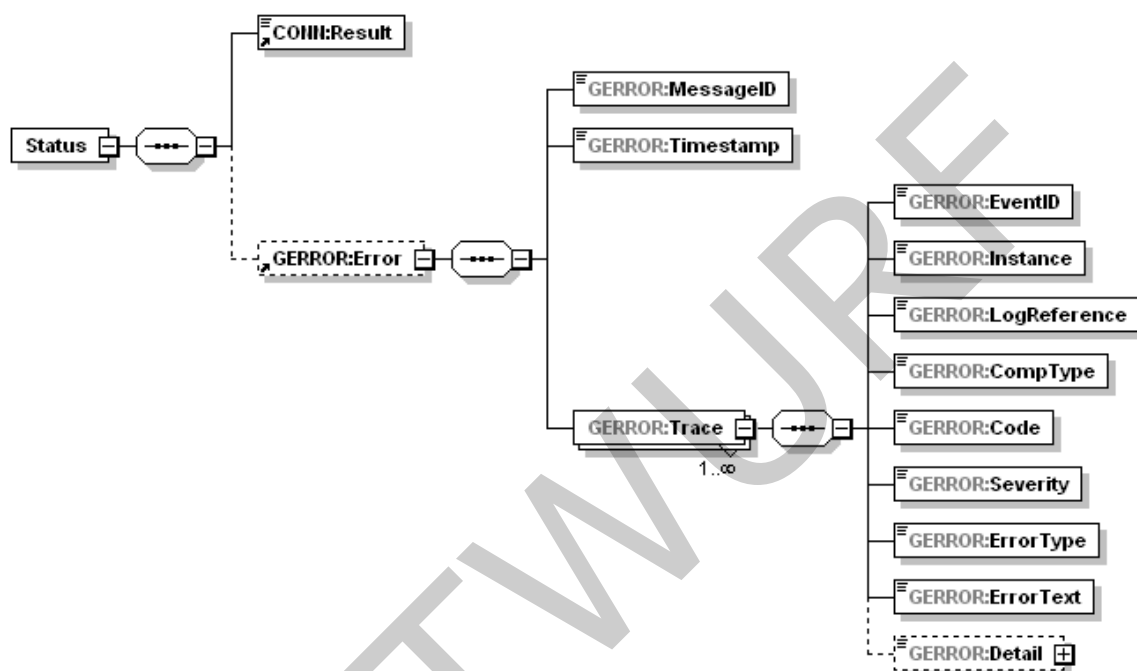
1899 Der Konnektor bietet Operationen an der Außenschnittstelle über SOAP-Webservices an.
 1900 Treten bei der Ausführung einer Operation Fehler auf, so werden diese an das aufrufende
 1901 System gemeldet. Die von den Basisdiensten des Konnektors angebotenen SOAP-
 1902 Webservices melden Fehler, die bei der Ausführung einer Operation auftreten, über eine
 1903 SOAP-Fault-Nachricht (siehe auch [gemSpec_OM#3.2.3]).

1904 TIP1-A_5058 - Fehlerübermittlung durch gematik-SOAP-Fault
 1905 Der Konnektor MUSS Fehlermeldungen, die im Rahmen einer über die Außenschnittstelle
 1906 aufgerufenen Operation auftreten, an das Clientsystem mittels gematik-SOAP-Faults
 1907 melden.
 1908 [≤]

1909 TIP1-A_5058-01 - ab PTV4: Fehlerübermittlung durch gematik-SOAP-Fault
 1910 Der Konnektor MUSS Fehlermeldungen, die im Rahmen einer über die Außenschnittstelle
 1911 aufgerufenen Operation eines Basisdienst-SOAP-Webservices auftreten, an das
 1912 Clientsystem mittels gematik-SOAP-Faults melden.
 1913 [≤]

1914 Treten bei konnektorinternen Operationen (TUCs) Fehler auf, so werden diese an den
 1915 Aufrufer (aufrufender TUC oder aufrufende Operation) zurückgegeben. Der Aufrufer kann
 1916 den aufgetretenen Fehler in seinem Kontext neu interpretieren. Das bedeutet
 1917 insbesondere, dass ein Error eines aufgerufenen TUCs nicht zwingend zum Abbruch des
 1918 aufrufenden TUCs bzw. der aufrufenden Operation führen muss. So ist es dem Aufrufer

- 1919 möglich, einen Error als Warnung zu interpretieren und an den eigenen internen oder
 1920 externen Aufrufer zurückzumelden. Diese dabei erzeugte Fehlerkette wird in Form einer
 1921 Fehler-Trace-Struktur abgebildet, um eine Nachverfolgung von Fehlern zu ermöglichen.
 1922 Operationen an der Außenschnittstelle können die Fehlerkette zu Informationszwecken in
 1923 der SOAP-Antwort an das Clientsystem senden. Dazu enthält jede SOAP-Antwort das
 1924 Element Status, dass gemäß dem XML-Schema [ConnectorCommon.xsd] aufgebaut ist
 1925 (siehe auch Abbildung PIC_KON_107 XML-Struktur des Status-Elements einer SOAP-
 1926 Antwort).
 1927



- 1928
 1929

1930 **Abbildung 3: PIC_KON_107 XML-Struktur des Status-Elements einer SOAP-Antwort**

- 1931 Schlägt eine Operation fehl, so wird eine SOAP-Fault-Meldung an das Clientsystem
 1932 versendet. Im Erfolgsfall wird das Status-Element in die Antwortnachricht an das
 1933 Clientsystem aufgenommen. Ist der Fehler-Trace leer (Element GERROR:Error ist nicht
 1934 vorhanden), so wird CONN:Result auf OK gesetzt. Andernfalls, d. h. wenn in
 1935 GERROR:Trace Fehler der Schwere Info oder Warning (zu Informationszwecken)
 1936 enthalten sind, wird CONN:Result auf Warning gesetzt.

- 1937 TIP1-A_4521 - Protokollierung von Fehlern inkl. Trace-Struktur
 1938 Der Konnektor MUSS Fehler protokollieren, die in fachlichen und technischen Abläufen
 1939 von der gematik spezifiziert oder herstellerspezifisch definiert sind und den Schweregrad
 1940 (Severity) Warning, Error oder Fatal haben. Zur Nachvollziehbarkeit des Fehlers MÜSSEN
 1941 Fehlerursache, fachliche und technische Auslöser des Fehlverhaltens aus den
 1942 Protokolleinträgen erkennbar sein.
 1943 [**<=**]

- 1944 A_14159 - Rückgabe von Fehlermeldungen an der Außenschnittstelle
 1945 Der Konnektor MUSS bei der Rückgabe von Fehlermeldungen an der Außenschnittstelle
 1946 sicherstellen, dass im letzten "GERROR:Trace"-Element der GERROR-Struktur ein von der
 1947 gematik spezifizierter Fehler steht. Die GERROR-Struktur kann weitere gematik- und
 1948 herstellerspezifische Fehler enthalten.
 1949 [**<=**]

- 1950 In der Regel ist es ausreichend, wenn die GERROR-Struktur an der Außenschnittstelle nur
1951 ein Element „GERROR:Trace“ mit einem gematik-Fehler enthält.
- 1952 Wenn für eine Fehlersituation kein Fehlercode spezifiziert ist, kann ein
1953 herstellerspezifischer Fehler zur Detaillierung verwendet werden. In diesem Fall muss ein
1954 passender gematik-Fehler als letztes GERROR:Trace-Element gewählt werden. Bei
1955 Fehlern in technischen Abläufen kann Fehlercode 4001 als letztes GERROR:Trace-Element
1956 verwendet werden. Die Wahl des letzten GERROR:Trace-Elements ist mit der gematik
1957 abzustimmen.
- 1958 Zur Struktur von Fehlermeldungen siehe auch [gemSpec_OM#GS-A_3856].

1959 **3.5.3 Transport großer Dokumente**

- 1960 SOAP Message Transmission Optimization Mechanism (MTOM) ermöglicht den direkten
1961 Transport von binären Daten in Webservices, d.h. ohne dass eine zur Laufzeit aufwändige
1962 Verpackung der binären Daten in ein Base64-XML-Element notwendig wird. Auf die
1963 Definition der Webservices und ihre Funktionalität hat dieser Optimierungsmechanismus
1964 keinen Einfluss. Der Einsatz von MTOM dient der Verbesserung des Performance-
1965 Verhaltens für große Dokumente.
- 1966 Das Clientsystem kann die Optimierung des Transports großer Dokumente per SOAP
1967 Message Transmission Optimization Mechanism (MTOM) anstoßen. In den WSDL-Dateien
1968 werden keine MTOM Serialization Policy Assertion [WS-MTOMPolicy] eingebettet.
- 1969 TIP1-A_5694 - SOAP Message Transmission Optimization Mechanism für Basisdienste
1970 Der Konnektor KANN SOAP Message Transmission Optimization Mechanism (MTOM)
1971 gemäß [MTOM] unterstützen.
1972 Wenn der Konnektor MTOM unterstützt, MUSS er MTOM für Signatur- und
1973 Verschlüsselungsdienst unterstützen, DARF aber NICHT MTOM für andere Dienste
1974 unterstützen.
1975 Wenn der Konnektor MTOM unterstützt, MUSS er, vergleichbar dem Einsatz des Attributs
1976 `wsp:Optional="true"` einer MTOM Serialization Policy Assertion [WS-MTOMPolicy], genau
1977 dann MTOM für die Antwortnachricht verwenden, wenn entweder
- 1978 • die Aufrufnachricht eine `application/xop+xml` Nachricht ist
 - 1979 • oder der `Accept` HTTP header der Aufrufnachricht folgenden Wert hat:
1980 `multipart/related; type=application/xop+xml`
- 1981 **[<=]**
- 1982 TIP1-A_5694-02 - ab PTV4: SOAP Message Transmission Optimization Mechanism für
1983 Basisdienste
1984 Der Konnektor KANN SOAP Message Transmission Optimization Mechanism (MTOM)
1985 gemäß [MTOM-SOAP1.1] für Basisdienste unterstützen. **[<=]**
- 1986 A_15786 - SOAP Message Transmission Optimization Mechanism für Basisdienste -
1987 Einschränkung
1988 Wenn der Konnektor MTOM für Basisdienste unterstützt, MUSS er MTOM für Signatur-
1989 und Verschlüsselungsdienst unterstützen, DARF aber NICHT MTOM für andere Dienste
1990 unterstützen. **[<=]**
- 1991 A_15610 - Verwendung von MTOM für Antwortnachricht
1992 Wenn der Konnektor MTOM unterstützt, MUSS er, vergleichbar dem Einsatz des Attributs
1993 `wsp:Optional="true"` einer MTOM Serialization Policy Assertion [WS-MTOMPolicy], genau
1994 dann MTOM für die Antwortnachricht verwenden, wenn entweder
- 1995 • die Aufrufnachricht eine `application/xop+xml` Nachricht ist

- 1996 • oder der Accept HTTP header der Aufrufnachricht folgenden Wert hat:
1997 multipart/related; type=application/xop+xml.

1998 [**<=**]

1999 A_15611 - SOAP Message Transmission Optimization Mechanism für Fachmodule
2000 Der Konnektor MUSS SOAP Message Transmission Optimization Mechanism (MTOM)
2001 gemäß [MTOM] für Fachmodule unterstützen, wenn es in der Schnittstellenbeschreibung
2002 des Fachmodules explizit gefordert wird. [**<=**]

2003 **3.6 Verwendung manuell importierter CA-Zertifikate**

2004 TI-fremde X.509-Zertifikate werden im Rahmen des Verschlüsselungsdienstes verwendet.
2005 Um den Vertrauensraum für diese Zertifikate abzubilden, erlaubt der Konnektor, X.509-
2006 CA-Zertifikate zu diesen TI-fremden X.509-Zertifikaten in eine interne Liste
2007 (CERT_IMPORTED_CA_LIST) zu importieren.

2008 Der Konnektor kann dann im Rahmen der Hybridverschlüsselung den symmetrischen
2009 Schlüssel empfängerspezifisch mit diesem TI-fremden X.509-Zertifikat verschlüsseln. Die
2010 TI-fremden Zertifikate dürfen nicht zu einem anderen Zweck als diesem eingesetzt
2011 werden.

2012 TIP1-A_5433 - Manuell importierte X.509-CA-Zertifikate nur für hybride Verschlüsselung
2013 Der Konnektor DARF End-Entity-Zertifikate, die lediglich gegen manuell importierte
2014 X.509-CA-Zertifikate geprüft werden, die von CAs außerhalb der TI stammen
2015 (CERT_IMPORTED_CA_LIST), NICHT für andere Zwecke als zur hybriden Verschlüsselung
2016 von Dokumenten verwenden.

2017 [**<=**]

2018 Die Berücksichtigung der CA-Zertifikate aus CERT_IMPORTED_CA_LIST muss auf
2019 folgende Anwendungsfälle beschränkt werden:

- 2020 1. Prüfung eines Zertifikates im Rahmen der hybriden Verschlüsselung
2021 2. Prüfung eines Zertifikates im Rahmen eines Aufrufes der Operation "VerifyCertificate"

2022

2023 TIP1-A_5660 - Hinweise im Handbuch für manuell importierte X.509-CA-Zertifikate
2024 Das Handbuch des Konnektors MUSS sinngemäß folgende Hinweise enthalten:

- 2025 • Der Administrator übernimmt die Verantwortung für die Verlässlichkeit der
2026 importierten CA-Zertifikate.
- 2027 • Der Administrator kann sich bei seiner Entscheidung für einen Import von CA-
2028 Zertifikaten auf die Informationen der gematik stützen.
- 2029 • Die gematik veröffentlicht dazu Informationen über CA-Betreiber, welche die
2030 Erfüllung der Sicherheitsanforderungen der gematik nachgewiesen haben.

2031 [**<=**]

2032 **3.7 Testunterstützung**

2033 Gemäß Testkonzept Online-Rollout (Stufe 1) [gemKPT_Test_ORS1#TIP1-A_2839] muss
2034 ein Hersteller eines Konnektors seine Modelle in drei Ausführungen vorsehen: Eine für die
2035 Testumgebung, eine für die Referenzumgebung und eine für die Produktivumgebung.

2036 Damit trotz dieser Forderung die Firmware je Konnektorversion für alle Umgebungen
 2037 identisch ist, wird die Erkennung der Umgebung an die gSMC-K gebunden. Die
 2038 Konnektor-Firmware muss zwischen den Umgebungen PU und RU/TU unterscheiden. Die
 2039 gSMC-K besitzt hierzu den Datencontainer MF/EF.EnvironmentSettings, der die jeweilige
 2040 Umgebungskennung enthält (PU bzw. TU/RU). Die Umgebungskennung wird read-only
 2041 auf der gSMC-K gespeichert.

2042 TIP1-A_4981 - Steuerung der Betriebsumgebung via gSMC-K
 2043 Der Produkttyp Konnektor MUSS sowohl in der Testumgebung (TU), der
 2044 Referenzumgebung (RU) wie auch der Produktivumgebung (PU) betreibbar sein.
 2045 Die Information, ob eine Konnektorinstanz in der TU/RU oder PU betrieben wird, MUSS
 2046 der Konnektor dem File MF/EF.EnvironmentSettings der gSMC-K entnehmen.
 2047 Abhängig von der ermittelten Betriebsumgebung MÜSSEN die Konfigurationswerte gemäß
 2048 Tabelle TAB_KON_812 verwendet werden.
 2049

2050 **Tabelle 9: TAB_KON_812 Umgebungsabhängige Konfigurationsparameter**

Betriebs umgebung	Konfigurations parameter	Konfigurations wert	Beschreibung
PU	NET_TI_ZENTRAL	siehe [gemSpec_Net#Tab_Adrkonzept_Produktiv]	Siehe TAB_KON_680. Dieser Wert MUSS für den Administrator über die Managementschnittstelle einsehbar, DARF aber NICHT änderbar sein.
	NET_TI_GESICHERTE_FD	siehe [gemSpec_Net#Tab_Adrkonzept_Produktiv]	Siehe TAB_KON_680. Dieser Wert MUSS für den Administrator über die Managementschnittstelle einsehbar, DARF aber NICHT änderbar sein.
	NET_TI_OFFENE_FD	siehe [gemSpec_Net#Tab_Adrkonzept_Produktiv]	Siehe TAB_KON_680. Dieser Wert MUSS für den Administrator über die Managementschnittstelle einsehbar, DARF aber NICHT änderbar sein.
	DNS_TOP_LEVEL_DOMAIN_TI	telematik.	Siehe TAB_KON_731. Dieser Wert MUSS für den Administrator über die Managementschnittstelle einsehbar, DARF aber NICHT änderbar sein.
RU/TU	NET_TI_ZENTRAL	siehe [gemSpec_Net#Tab_Adrkonzept_Test]	Siehe TAB_KON_680. Dieser Wert MUSS für den Administrator über die Managementschnittstelle mit dem Konfigurationswert voreingestellt und änderbar sein.

NET_TI_GESICHERTE_FD	siehe [gemSpec_Net#Tab_Adrkonzept_Test]	Siehe TAB_KON_680. Dieser Wert MUSS für den Administrator über die Managementschnittstelle mit dem Konfigurationswert voreingestellt und änderbar sein.
NET_TI_OFFENE_FD	siehe [gemSpec_Net#Tab_Adrkonzept_Test]	Siehe TAB_KON_680. Dieser Wert MUSS für den Administrator über die Managementschnittstelle mit dem Konfigurationswert voreingestellt und änderbar sein.
DNS_TOP_LEVEL_DOMAIN_TI	telematik-test.	Siehe TAB_KON_731. Dieser Wert MUSS für den Administrator über die Managementschnittstelle einsehbar, aber nicht änderbar sein.

2051
2052
2053

[<=]

2054 TIP1-A_4707 - Betrieb in Test- und Referenzumgebung

2055 Der Produkttyp Konnektor MUSS auch in der Test- und Referenzumgebung betrieben
2056 werden können. Dafür MUSS der Vertrauensanker des Konnektors für diese Umgebung
2057 ausgetauscht werden können. Dies KANN durch Lieferung eines neuen Konnektors oder
2058 durch Austausch der gSMC-K durch den Hersteller ermöglicht werden. Der Hersteller
2059 MUSS sicherstellen, dass Konnektoren ausschließlich mit den zu ihrer Einsatzumgebung
2060 gehörenden Vertrauensankern ausgestattet werden.

2061 **[<=]**

2062 TIP1-A_4982 - Anzeige von TU/RU in der Managementschnittstelle

2063 Die Administrationsoberfläche MUSS, wenn der Konnektor in der Testumgebung (TU)
2064 oder Referenzumgebung (RU) betrieben wird, die Umgebungsbezeichnung zu jeder Zeit
2065 erkennbar in der Managementschnittstelle anzeigen.

2066 Die Anzeige eines Betriebs in der Produktivumgebung DARF NICHT explizit angezeigt
2067 werden.

2068 **[<=]**

2069

4 Funktionsmerkmale

2070 Für die folgenden Inhalte bitte die Hinweise in Kapitel 1.5.3 „Erläuterungen zur
2071 Spezifikation des Außenverhaltens,“ sowie Kapitel 1.5.4 Erläuterungen zur
2072 Dokumentenstruktur und „Dokumentenmechanismen“ beachten.

2073 4.1 Anwendungskonnektor

2074 4.1.1 Zugriffsberechtigungsdienst

2075 Der Zugriffsberechtigungsdienst ist ein interner Dienst. Er ermöglicht es Operationen eine
2076 Prüfung auf Zugriffsberechtigung für die von ihnen benötigten Ressourcen
2077 durchzuführen. Die Prüfung erfolgt direkt nach Aufruf einer Operation des Konnektors
2078 durch das Clientsystem und basiert auf den im Clientaufruf enthaltenen Parametern.

2079 Der Zugriffsberechtigungsdienst definiert über ein Informationsmodell die erlaubten
2080 Zugriffsmöglichkeiten. Um dies zu erreichen, modelliert es Mandanten und ordnet ihnen
2081 Clientsysteme sowie die vom Konnektor verwalteten externen Ressourcen
2082 (Kartenterminal mit Slots, Arbeitsplatz mit Signaturproxy und SMC-Bs) zu. Diese durch
2083 einen Administrator persistent zu modellierenden Entitäten und Beziehungen beinhalten
2084 die erlaubten Zugriffswege vom Clientsystem über Arbeitsplatz zum Kartenterminal und
2085 dessen Slots. Sie werden im Konnektor administrativ konfiguriert. Der Signaturproxy hat
2086 keine eigene Identität im Informationsmodell, da er den Kontext des aufrufenden
2087 Clientsystems verwendet.

2088 Neben diesen persistenten Entitäten und Beziehungen bildet das Modell auch die in den
2089 Slots temporär gesteckten Karten und die zugehörigen Kartensitzungen als transiente
2090 Entitäten und Beziehungen ab.

2091 Abbildung PIC_Kon_100 stellt das Informationsmodell dar. Die persistenten Entitäten
2092 haben einen grünen Hintergrund, die transienten einen weißen.

2093 Tabelle TAB_KON_507 beschreibt die Entitäten und legt ihren Identitätsschlüssel fest.
2094 Tabelle TAB_KON_508 beschreibt die Attribute. Tabelle TAB_KON_509 beschreibt die
2095 Entitätsbeziehungen und referenziert dabei die in Abbildung PIC_Kon_100 durch Zahlen
2096 in eckigen Klammern markierten Beziehungen. Tabelle TAB_KON_510 definiert
2097 Constraints, die zusätzlich zu den in Abbildung PIC_Kon_100 definierten Kardinalitäten
2098 gelten. Die Constraints werden mittels Object Constraint Language (OCL) definiert.

2099 4.1.1.1 Funktionsmerkmalweite Aspekte

2100 TIP1-A_4522 - Zugriffsberechtigungs-Informationsmodell des Konnektors
2101 Der Konnektor MUSS die Entitäten, Attribute und Beziehungen des Informationsmodells
2102 intern vorhalten, dabei für die Einhaltung der definierten Constraints sorgen und die
2103 persistenten Entitäten und Beziehungen dauerhaft speichern. Der Konnektor MUSS dabei
2104 eine Mindestanzahl von 999 Mandanten unterstützen.
2105 Das Informationsmodell ist definiert durch das UML-Diagramm „PIC_Kon_100
2106 Informationsmodell des Konnektors,“ und die Tabelle „TAB_KON_510 Informationsmodell
2107 Constraints“. Der Konnektor darf nur Daten in sein Informationsmodell übernehmen, die
2108 alle Eigenschaften des Informationsmodells, insbesondere die Constraints, erfüllen.
2109 Die Entitäten werden in Tabelle „TAB_KON_507 Informationsmodell Entitäten“
2110 beschrieben, die Attribute in Tabelle „TAB_KON_508 Informationsmodell Attribute“ und

2111 die Beziehungen in Tabelle „TAB_KON_509 Informationsmodell Entitätenbeziehungen“.
2112 [**<=**]

2113 *Hinweis zu den Bezeichnern der Entitäten und ihrer Attribute: Im Folgenden beginnen*
2114 *Entitäten mit einem Großbuchstaben, Attribute mit einem Kleinbuchstaben. Werden die*
2115 *Entitäten und Attribute in XML-Dokumenten verwendet, so beginnen die zugeordneten*
2116 *XML-Elementbezeichner grundsätzlich mit einem Großbuchstaben und verwenden den*
2117 *englischen Begriff, der im Folgenden in Klammern angegeben ist, wenn zur besseren*
2118 *Lesbarkeit im Modell ein deutscher Begriff verwendet wird.*

ENTWURF

2119

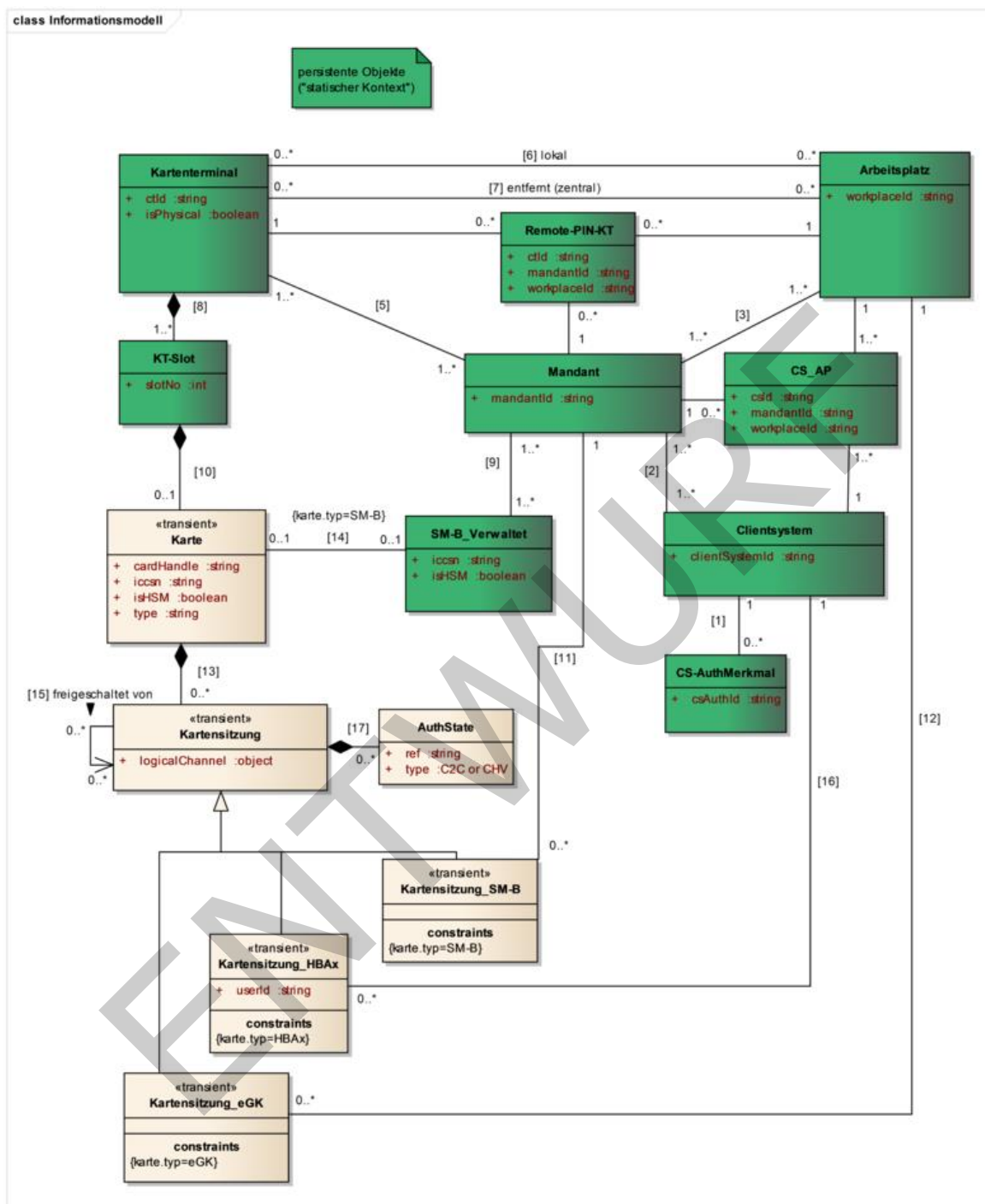


Abbildung 4: PIC_Kon_100 Informationsmodell des Konnektors

Tabelle 10: TAB_KON_507 Informationsmodell Entitäten

Entität	persistent/ transient	Identitätsschlüssel	Beschreibung
---------	--------------------------	---------------------	--------------

Mandant	persistent	mandantId	Zu Mandanten und Mandantenfähigkeit siehe Kapitel Mandantenfähigkeit.
Clientsystem	persistent	clientSystemId	Unter einem Clientsystem wird hier ein einzelnes oder eine Gruppe von Systemen verstanden, welche im LAN der Einsatzumgebung auf die Clientsystem-Schnittstelle des Konnektors zugreifen.
CS-AuthMerkmal (CS-AuthProperty)	persistent	csAuthId	Das Authentifizierungsmerkmal dient der Authentifizierung, wenn sich das Clientsystem gegenüber dem Konnektor authentisiert. Der Identitätsschlüssel csAuthId wird bei der Administration vergeben
Arbeitsplatz (Workplace)	persistent	workplaceId	alle dem Konnektor bekannten Arbeitsplätze
Kartenterminal (CardTerminal)	persistent	ctId	alle dem Konnektor bekannten Kartenterminals.
KT-Slot (CT-Slot)	persistent	ctId, slotNo	Die sich in den Kartenterminals befindenden Chipkartenslots (Functional Unit Type 00)
Karte (Card)	transient	cardHandle oder iccsn	Die in den Kartenterminals steckenden Smartcards des Gesundheitswesens, die persönliche Identitäten oder Rollen repräsentieren (eGK, HBA, SMC-B). Karten, die nur Geräteidentitäten tragen (gSMC-K, gSMC-KT) werden in diesem Modell nicht betrachtet. Karten im Sinne dieses Informationsmodells existieren maximal so lange, wie sie im Kartenterminal stecken. Die aktuell im System steckenden Karten werden

			<p>vom Clientsystem über das cardHandle adressiert. Die iccsn erlaubt eine dauerhafte Adressierung einer Karte.</p> <p>Für den Kartentyp „SM-B“ kann hier auch eine in einem HSM-B enthaltene virtuelle SMC-B abgebildet werden.</p>
Kartensitzung (CardSession)	transient	siehe konkrete Kartensitzungen	<p>Kartensitzungen stellen ein wesentliches Konzept im Sicherheitsmodell des Konnektors dar. Eine Kartensitzung verwaltet einen aktuellen logischen Sicherheitsstatus einer Karte. Die Kartensitzungen sind einer Karte fest zugewiesen.</p> <p>Zu einer Karte kann es mehrere Kartensitzungen geben, die voneinander logisch unabhängige Sicherheitsstatus einer Karte verwalten.</p> <p>Der Konnektor führt alle Zugriffe auf eine Karte im Kontext einer Kartensitzung zu dieser Karte aus.</p> <p>Das Attribut logischerKanal bezeichnet den logischen Kanal zur Karte, der im Rahmen der Kartensitzung verwendet wird (gemäß Standard [7816-4]).</p>
Kartensitzung_eGK (CardSession_eGK)	transient	cardHandle	<p>Kartensitzung für eine eGK. Die KVK ist im Modell nicht explizit dargestellt. Soweit anwendbar, gelten für die KVK die gleichen Aussagen wie für die eGK.</p>
Kartensitzung_SM-B (CardSession_SM-B)	transient	cardHandle, mandantId	<p>Kartensitzung für eine SM-B</p>

Kartensitzung_HBAx (CardSession_HBAx)	transient	cardHandle, clientSystemId, userId	Kartensitzung für einen HBAx. Unter dem Typ „HBAx“ sind auch die Vorläuferkarten wie „HBA-qSig“ und „ZOD_2.0“ inkludiert.
SM-B_Verwaltet (SM-B_managed)	persistent	iccsn	SM-Bs müssen im Gegensatz zu den übrigen Karten im Konnektor vor ihrer Verwendung persistent im Informationsmodell als „SM-B_Verwaltet“ per Administration aufgenommen werden. Dies gilt auch für die in einem HSM-B enthaltenen virtuellen SMC-Bs.
CS_AP	persistent	mandantId, clientSystemId, workplaceId	CS_AP legt die von einem Clientsystem pro Mandanten nutzbaren Arbeitsplätze fest. Ein Clientsystem kann dabei mehrere Arbeitsplätze bedienen. Ebenso können Arbeitsplätze von mehreren Clientsystemen, auch gleichzeitig, genutzt werden, z. B. bei zwei unterschiedlichen, voneinander unabhängigen Praxisprogrammen.
Remote-PIN-KT	persistent	mandantId, workplaceId, ctId	Remote-PIN-KT legt pro Mandant und Arbeitsplatz fest, über welches Kartenterminal eine Remote PIN-Eingabe erfolgen soll, wenn an diesem Arbeitsplatz die PIN-Eingabe für eine Karte erforderlich ist, die nicht in einem dem Arbeitsplatz lokal zugeordneten Kartenterminal steckt.
AuthState	transient	cardHandle, (clientSystemId), (userId), ref	Zu einer Kartensitzung gibt es höhere AuthorizationStates, die durch (type =C2C) Freischaltung oder durch PIN-Eingabe (type=CHV) erreicht werden können.

			Für eGK G2.0 wird der Zustand der MRPINs nicht in AuthState gespeichert.
--	--	--	--

2126

2127

2128

Tabelle 11: TAB_KON_508 Informationsmodell Attribute

Attribut	Beschreibung
cardHandle	Das Identifikationsmerkmal einer Karte für die Dauer eines Steckzyklusses. Es wird mit dem Entfernen der Karte aus dem Kartenterminal ungültig. Es wird automatisch vom Konnektor vergeben.
clientSystemId	Das Identifikationsmerkmal eines Clientsystems. Es wird per Administration dem Mandanten im Clientsystem und im Konnektor zugeordnet.
csAuthId	Das Identifikationsmerkmal eines Authentifizierungsmerkmals.
ctId	Das Identifikationsmerkmal eines Terminals. Es ist eine fixe Eigenschaft des Kartenterminals.
iccsn	Die Seriennummer einer Karte. Sie identifiziert eine Karte dauerhaft.
isHSM	Attribut der Entitäten Karte und SM-B_Verwaltet. Es ist false, wenn eine echte Smardcard abgebildet wird und true, wenn es sich um eine virtuelle SMC-B handelt, die in einem HSM-B enthalten ist.
isPhysical	Attribut des Kartenterminals das den Wert „Ja“ hat, wenn es sich um ein tatsächlich existierendes Kartenterminal handelt. Ist der Wert „Nein“, dann handelt es sich um ein logisches Kartenterminal im Zusammenhang mit einem HSM-B.
logicalChannel	Referenz auf ein Objekt, das einen logischen Kanal repräsentiert.
mandantId	Das Identifikationsmerkmal eines Mandanten. Es wird per Administration dem Mandanten im Clientsystem und im Konnektor zugeordnet.
ref	Das Identifikationsmerkmal eines AuthState zu einer gegebenen Kartensitzung. Im Falle C2C handelt es sich um die

	KeyRef (mit einer bestimmten Rolle) und in Falle CHV um eine referenzierte PIN.
slotNo	Das Identifikationsmerkmal eines Slot für ein bestimmtes Kartenterminal. Diese fortlaufende Nummer ist eine fixe Eigenschaft des Kartenterminals. Sie beginnt bei 1.
type	Als Kartenattribut: Typ einer Karte. Im Folgenden berücksichtigte Werte: „HBAX“, „SM-B“, „EGK“. Als Attribute eines AuthState: Typ des AuthState. „C2C“ steht für gegenseitige Kartenauthentisierung. „CHV“ steht für Card Holder Verification per PIN-Eingabe.
userId	Das Identifikationsmerkmal des Nutzers im Clientsystem (Die userId wird durch das Clientsystem vergeben und verwaltet). Die userId wird im Kontext eine Kartensitzung_HBAX vom Konnektor verwendet, um als Bestandteil des Identitätsschlüssels die Kartensitzung_HBAX zu identifizieren.
workplaceId	Das Identifikationsmerkmal eines Arbeitsplatzes. Es wird per Administration dem Mandanten im Clientsystem und im Konnektor zugeordnet.

2129

2130

Tabelle 12: TAB_KON_509 Informationsmodell Entitätenbeziehungen

Entitätenbeziehung	persistent/ transient	Beschreibung
Authentifikationsmerkmale des Clientsystems [1]	persistent	Diese Relation legt für jedes Clientsystem eine Menge von Authentisierungsmerkmalen fest. Mit einem dieser Authentisierungsmerkmale muss sich ein Client gegenüber dem Konnektor authentisiert haben, um als das entsprechende Clientsystem vom Konnektor akzeptiert zu werden.
Clientsysteme des Mandanten [2]	persistent	Diese Relation weist Clientsystemen Mandanten zu.
Arbeitsplätze des Mandanten [3]	persistent	Diese Relation weist Arbeitsplätze Mandanten zu. Arbeitsplätze können von mehreren Mandanten genutzt werden. Z. B. kann ein von mehreren Mandanten genutzter gemeinsamer Empfang als ein Arbeitsplatz modelliert werden.
Kartenterminals des Mandanten [5]	persistent	Diese Relation weist Kartenterminals Mandanten zu.

Lokale Kartenterminals [6]	persistent	Diese Relation erfasst die Kartenterminals, die sich lokal an einem Arbeitsplatz befinden und von diesem genutzt werden können. Die Modellierung lässt es zu, dass Kartenterminals mehreren Arbeitsplätzen lokal zugewiesen werden. Jeder an der TI teilnehmende Arbeitsplatz wird in der Regel mindestens ein lokales Kartenterminal benötigen.
Entfernte Kartenterminals [7]	persistent	Diese Relation beschreibt, auf welche Kartenterminals Arbeitsplätze (remote) zugreifen dürfen. Dies ist für zentral steckende Karten vorgesehen.
Slot eines Kartenterminals [8]	persistent	Die Zuordnung von Slots zu einem Kartenterminal ergibt sich automatisch aus den Eigenschaften des Kartenterminals.
SM-B_Verwaltet eines Mandanten [9]	persistent	Diese Relation legt fest, welche verwalteten SM-Bs einem Mandanten zugeordnet sind.
Kartenterminal-Slot, in dem eine Karte steckt [10]	transient	Sobald eine Karte in ein Kartenterminal gesteckt wird, ergibt sich implizit eine Relation der Karte zu dem Slot, in dem sie steckt, [6] und indirekt über [4] zum Kartenterminal.
Mandant der Kartensitzung SM-B [11]	transient	Beim Anlegen einer Kartensitzung SM-B wird diese immer dem zugreifenden Mandanten zugeordnet.
Arbeitsplatz der Kartensitzung eGK [12]	transient	Eine Kartensitzung eGK ist immer einem Arbeitsplatz zugeordnet.
Karte einer Kartensitzung [13]	transient	Jeder Kartensitzung ist genau einer Karte zugeordnet.
Gesteckte SM-B [14]	transient	Wird eine SM-B gesteckt und handelt es sich um eine verwaltete SM-B, ergibt sich über die iccsn die Zuordnung.
Freischaltung einer Karte [15]	transient	Diese Relation erfasst die Freischaltung einer Karte durch eine andere Karte.
Bindung der Kartensitzung_HBAx an Clientsystem [16]	transient	Kartensitzungen HBAx sind einem Clientsystem zugeordnet.
AuthState pro Kartensitzung [17]	transient	Eine Kartensitzung kann erhöhte Sicherheitszustände (Authorization State) haben.

2132 **Tabelle 13: TAB_KON_510 Informationsmodell Constraints**

#	Beschreibung	Definition mittels OCL (Die Constraints werden im UML ergänzenden Standard OCL definiert.)
C1	Eine eGK muss eine oder keine Kartensitzung haben.	context Karte inv: self.type = "eGK" implies self.kartensitzung.size() <= 1
C2	Wenn zwei Kartensitzungen einer HBAX dem gleichen Clientsystem zugeordnet sind und ihre userIds gleich sind, dann müssen die beiden Kartensitzungen identisch sein.	context Kartensitzung-HBAX inv: forAll(k1, k2 : Kartensitzung-HBAX k1.karte = k2.karte and k1.clientsystem = k2.clientsystem and k1.userId = k2.userId implies k1 = k2)
C3	Wenn zwei SM-B-Kartensitzungen einer Karte dem gleichen Mandanten zugeordnet sind, dann müssen die beiden Kartensitzungen identisch sein.	context Kartensitzung-SM-B inv: forAll(k1, k2 : Kartensitzung-SM-B k1.karte = k2.karte and k1.mandant = k2.mandant implies k1 = k2)
C4	Die Seriennummer iccsn einer Karte muss eindeutig sein.	context Karte inv: Karte.allInstances -> isUnique(iccsn)
C5	Die Seriennummer iccsn einer Karte muss für die vom Konnektor verwalteten SM-Bs eindeutig sein.	context SM-B_Verwaltet inv: SM-B_Verwaltet.allInstances -> isUnique(iccsn)
C6	Das CardHandle einer Karte muss eindeutig sein.	context Karte inv: Karte.allInstances -> isUnique(cardHandle)
C7	Die Identifikationsnummer des Clientsystems muss eindeutig sein.	context Clientsystem inv: Clientsystem.allInstances -> isUnique(clientSystemId)

C8	Die Identifikationsnummer des Mandanten muss eindeutig sein.	context Mandant inv: Mandant.allInstances -> isUnique (mandantId)
C9	Die Identifikationsnummer des Arbeitsplatzes muss eindeutig sein.	context Arbeitsplatz inv: Arbeitsplatz.allInstances -> isUnique (workplaceId)
C10	Die Identifikationsnummer des Kartenterminals muss eindeutig sein.	context Kartenterminal inv: Kartenterminal.allInstances -> isUnique (ctId)
C11	Die Identifikationsnummer (slotNo) des Kartenterminal-Slots für ein gegebenes Kartenterminal muss eindeutig sein.	context Kartenterminal inv: self.kT-Slot -> isUnique (slotNo)
C12	Es muss gewährleistet sein, dass nur Arbeitsplätze und Clientsysteme einander im Rahmen eines Mandanten zugeordnet werden, die diesem Mandanten selbst zugeordnet sind.	context CS-AP inv: self.arbeitsplatz.mandant.includes (self.mandant) inv: self.clientsystem.mandant.includes (self.mandant)
C13	Es muss gewährleistet sein, dass nur Kartenterminals und Arbeitsplätze einander im Rahmen eines Mandanten zur Remote-PIN-Eingabe zugeordnet werden, die diesem Mandanten selbst zugeordnet sind.	context Remote-PIN-KT inv: self.arbeitsplatz.mandant.includes (self.mandant) inv: self.kartenterminal.mandant.includes (self.mandant)

C14	Zur Remote-PIN-Eingabe muss ein <u>lokales</u> Kartenterminal ausgewählt sein.	context Remote-PIN-KT inv: self.arbeitsplatz .localKartenterminal .includes(self.kartenterminal) inv: not self.arbeitsplatz .entferntKartenterminal .includes(self.kartenterminal)
C15	Zur Remote-PIN-Eingabe darf pro Mandanten und Arbeitsplatz nicht mehr als ein Kartenterminal ausgewählt werden.	context Remote-PIN-KT inv: forAll(r1, r2 : Remote-PIN-KT r1.arbeitsplatz = r2.arbeitsplatz and r1.mandant = r2.mandant implies r1 = r2)
C16	Eine Kartensitzung-HBAX muss immer eine zugehörige userId haben.	context Kartensitzung-HBAX inv: self.userId <> null

2133 *Hinweis zur Remote-PIN-Eingabe: Constraints C14 und C15 legen fest, dass auch im Fall*
 2134 *mehrerer lokaler Kartenterminals an einem Arbeitsplatz nur eines (oder keines) dieser*
 2135 *Kartenterminals pro Mandant für die Remote-PIN-Eingabe im Informationsmodell*
 2136 *konfiguriert wird.*

2137 TIP1-A_4523 - Sicherung der Aktualität des Informationsmodells
 2138 Zugriffsberechtigungsdienst
 2139 Der Konnektor MUSS seine Entscheidungen zur Zugriffsberechtigung basierend auf den
 2140 aktuellen, realen statischen wie transienten Entitäten und Beziehungen des
 2141 Informationsmodells treffen. Veränderungen an der statischen Definition (durch den
 2142 Administrator), sowie Veränderungen an den Entitäten (Änderung der Verfügbarkeit und
 2143 Zustandsänderung von Karten, Kartenterminals und Clientsystemen) MÜSSEN bei
 2144 Zugriffsanfragen unmittelbare Auswirkung auf die Entscheidung des
 2145 Zugriffsberechtigungsdienstes zur Folge haben.
 2146 [\leq]

2147 4.1.1.2 Durch Ereignisse ausgelöste Reaktionen

2148 Keine.

2149 4.1.1.3 Interne TUCs, nicht durch Fachmodule nutzbar

2150 Keine.

2151 4.1.1.4 Interne TUCs, auch durch Fachmodule nutzbar

2152 4.1.1.4.1 TUC_KON_000 „Prüfe Zugriffsberechtigung“

2153 Vor Ausführung jeder Operation an der Außenschnittstelle muss der Konnektor prüfen, ob
 2154 die Operation ausgeführt werden darf (Autorisierung). Diese Prüfung auf
 2155 Zugriffsberechtigung wird in TUC_KON_000 „Prüfe Zugriffsberechtigung“ gekapselt.

TUC_KON_000 „Prüfe Zugriffsberechtigung“ hat als Aufrufparameter den Aufrufkontext der Operation (siehe Abbildung PIC_KON_101), optional das cardHandle einer Karte, optional eine Kartenterminal-ID ctId und optional die Steuerungsparameter „needCardSession“ sowie „allWorkplaces“. Über den Steuerungsparameter „needCardSession“ wird festgelegt, ob zu den CardHandles im Rahmen der Operationsausführung eine Kartensitzung benötigt wird. Über den Steuerungsparameter „allWorkplaces“ wird festgelegt, ob die Auswertung im Rahmen der Operation arbeitsplatzübergreifend für alle vom Mandanten für das angegebene Clientsystem erreichbaren Kartenterminals erfolgen soll.

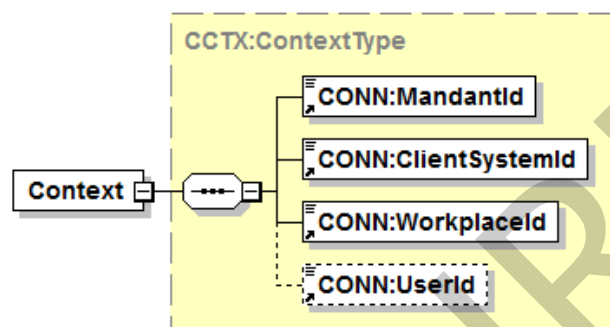


Abbildung 5: PIC_KON_101 Aufrufkontext der Operation

TIP1-A_4524-02 - TUC_KON_000 „Prüfe Zugriffsberechtigung“
Der Konnektor MUSS den technischen Use Case TUC_KON_000 „Prüfe Zugriffsberechtigung“ umsetzen.

Tabelle 14: TAB_KON_511 – TUC_KON_000 „Prüfe Zugriffsberechtigung“

Element	Beschreibung
Name	TUC_KON_000 "Prüfe Zugriffsberechtigung"
Beschreibung	Es wird geprüft, ob eine Autorisierung im Rahmen der angegebenen Eingangsdaten erteilt wird. Die Autorisierung wurde erteilt, wenn der TUC erfolgreich durchlaufen wurde (kein Abbruch durch Fehlermeldung)."
Eingangs-anforderungen	keine
Auslöser und Vorbedingungen	Aufruf einer Operation des Konnektors durch das Clientsystem.

Eingangsdaten	<ul style="list-style-type: none"> • mandantId • clientSystemId • workplaceId • userId - <i>optional</i> • ctId - <i>optional</i> (Kartenterminalidentifikator) • cardHandle - <i>optional</i> • needCardSession [Boolean] – <i>optional; default: true</i> („needCardSession“=true; „doNotNeedCardSession“=false) Dieser Schalter gibt an, ob eine Kartensitzung benötigt wird <ul style="list-style-type: none"> - true, der aufrufende TUC verwendet eine Kartensitzung - false, der aufrufende TUC verwendet keine Kartensitzung Die Berechtigungsprüfung geht im Default-Fall, davon aus, dass eine Kartensitzung benötigt wird, und prüft für diesen Fall die Berechtigung mit. • allWorkplaces [Boolean] – <i>optional; default: false</i> Dieser Schalter gibt an, ob eine mandantenweite Zugriffsberechtigung gemeint ist. Dieser Parameter muss dann (true) gesetzt werden, wenn die Berechtigungsprüfung nicht auf die vom angegebenen Arbeitsplatz erreichbaren Kartenterminals beschränkt ist, sondern sich auf alle vom Clientsystem (clientSystemId) und dem Mandant (mandantId) insgesamt erreichbaren Kartenterminals beziehen soll. Ist dieser Schalter gleich true, wird die Berechtigung unabhängig vom Eingangsparameter workplaceId geprüft.
Komponenten	Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> • keine
Nachbedingungen	<ul style="list-style-type: none"> • Autorisierung erteilt

Standardablauf	<ol style="list-style-type: none"> 1. Prüfe, ob die Pflichtparameter (mandantId, clientSystemId, workplaceId) vollständig gesetzt sind. 2. Falls ANCL_CAUT_MANDATORY = Enabled, dann prüfe, ob die gemäß [TIP1-A_4516] durchgeführte Authentifizierung über ein dem Clientsystem zugeordnetes CS-AuthMerkmal erfolgte. 3. Ermittle Zugriffsregel R zu den Aufrufparametern: <ol style="list-style-type: none"> 3.1. Falls der Parameter cardHandle nicht null ist, muss das Kartenobjekt des Informationsmodells Karte(cardHandle) ermittelt werden. 3.2. Zu den Parametern (ctId, cardHandle, needCardSession, allWorkplaces) muss mittels Tabelle „TAB_KON_513 Zugriffsregeln Regelzuordnung“ die Zugriffsregel R ermittelt werden. 4. Prüfe die Bedingungen der in Schritt 3 ermittelten Regel R: <ol style="list-style-type: none"> 4.1. Zur Regel R muss die relevante Spalte in Tabelle „TAB_KON_514 Zugriffsregeln Definition“ ermittelt werden. 4.2. Jede Zeile, die in der Spalte R ein „x“ hat, muss geprüft werden: <ol style="list-style-type: none"> 4.2.1 Prüfe, ob die in Spalte „Bedingung“ mittels OCL formulierte Bedingung für die Eingangsdaten erfüllt ist.
Varianten/ Alternativen	<ol style="list-style-type: none"> 2. Bei einem Aufruf mit einem cardHandle zu den Kartentypen SMC-KT und UNKNOWN wird Schritt 3 in folgender Variante durchlaufen: Ermittle Zugriffsregel R zu den Aufrufparametern: <ol style="list-style-type: none"> 3.1. ctId wird zum cardHandle bestimmt Zu den Parametern (<ol style="list-style-type: none"> ctId, cardHandle = null, needCardSession = false, allWorkplaces = false) muss mittels Tabelle „TAB_KON_513 Zugriffsregeln Regelzuordnung“ die Zugriffsregel R ermittelt werden.
Fehlerfälle	<p>Fehler im Ablauf (Standardablauf oder Varianten) führen in den folgend ausgewiesenen Schritten zu einem Abbruch der Verarbeitung mit den ausgewiesenen Fehlercodes:</p> <ol style="list-style-type: none"> (→1) Es sind nicht alle Pflichtparameter gesetzt, Fehlercode: 4021 (→2) Clientsystem aus dem Aufrufkontext nicht authentifiziert, Fehlercode: 4204 (→3.1) Karte nicht als gesteckt identifiziert,

	Fehlercode: 4008 (→3.2) Zu den Parametern konnte keine Regel ermittelt werden, Fehlercode: 4019 (→4.2.1) Bedingung nicht erfüllt Fehlercode: wie in Spalte „ErrorCode“ der geprüften Zeile aus Tabelle „TAB_KON_514-01 Zugriffsregeln Definition“
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	PIC_KON_118 Aktivitätsdiagramm zu „TUC_KON_000 Prüfe Zugriffsberechtigung“

2174
2175
2176
2177
2178
2179

[<=]

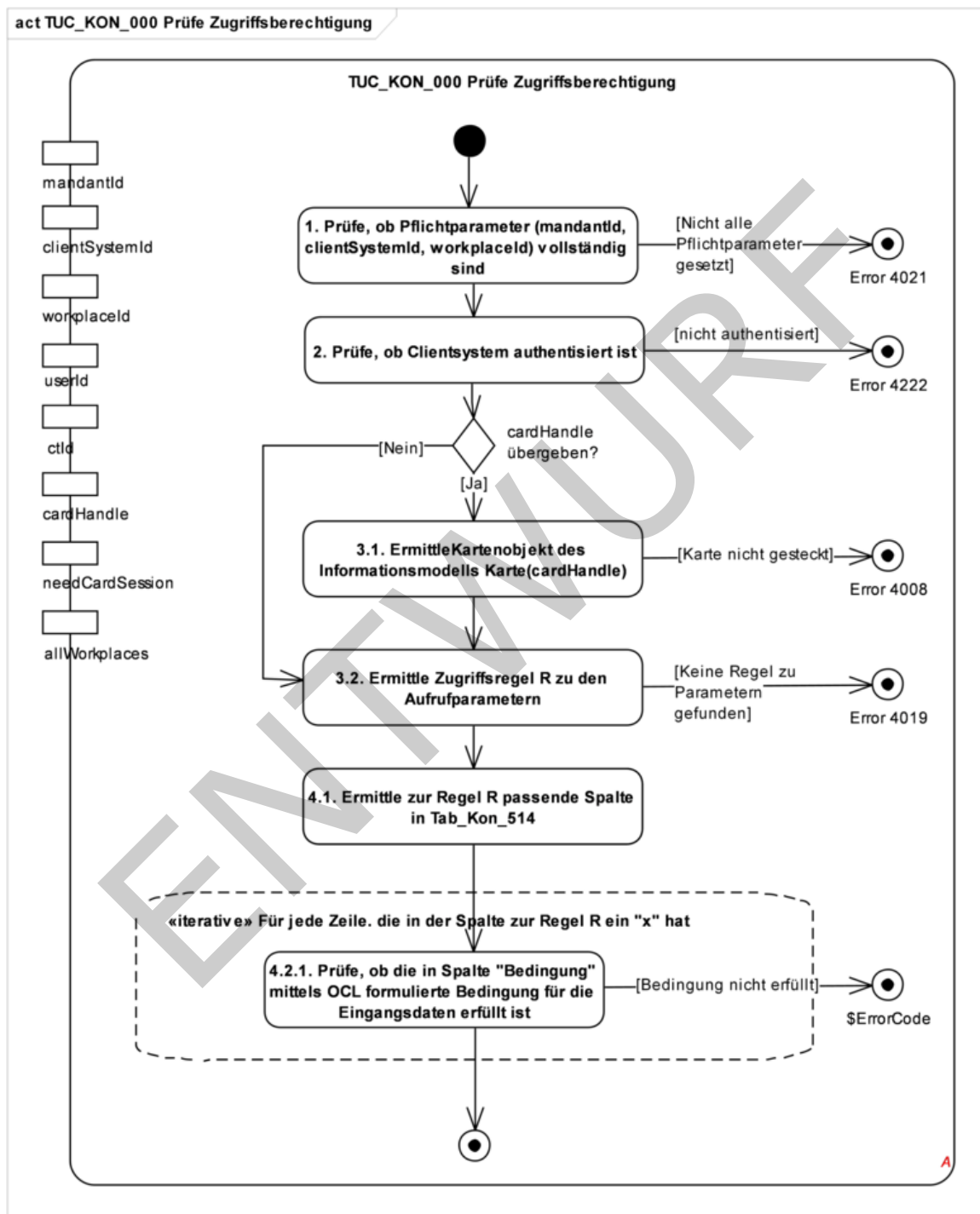
Eine Beschreibung aller Zugriffsregeln gibt Tabelle TAB_KON_512.

Tabelle 15: TAB_KON_512 Zugriffsregeln Beschreibung

Regel	Beschreibung
R1	Innerhalb des Mandanten m darf das Clientsystem cs verwendet werden.
R2	Innerhalb des Mandanten m darf das Clientsystem cs auf das Kartenterminal kt zugreifen.
R3	Innerhalb des Mandanten m darf das Clientsystem cs den Arbeitsplatz ap nutzen.
R4	Innerhalb des Mandanten m darf das Clientsystem cs über den Arbeitsplatz ap auf das Kartenterminal kt zugreifen.
R5	Innerhalb des Mandanten m darf das Clientsystem cs über den Arbeitsplatz ap auf die lokal gesteckte eGK zugreifen. Eine Kartensitzung wird nicht benötigt.
R6	Innerhalb des Mandanten m darf das Clientsystem cs über den Arbeitsplatz ap auf die lokal gesteckte eGK zugreifen. Eine Kartensitzung wird benötigt. Wenn bereits eine Kartensitzung besteht, ist sichergestellt, dass sie vom Arbeitsplatz ap gestartet wurde.
R7	Innerhalb des Mandanten m darf das Clientsystem cs über den Arbeitsplatz ap auf die SM-B zugreifen. Es wird dabei sichergestellt, dass es sich um eine im Mandanten verwaltete SM-B handelt.
R8	Innerhalb des Mandanten m darf das Clientsystem cs auf den HBAX zugreifen. Eine Kartensitzung wird nicht benötigt.
R9	Innerhalb des Mandanten m darf das Clientsystem cs auf den HBAX zugreifen. Eine Kartensitzung wird benötigt. Wenn bereits Kartensitzungen zum HBAX bestehen, wird der Zugriff auf den HBAX verhindert, wenn es eine

Kartensitzung zum selben Clientsystem, aber einer anderen UserId gibt, deren Sicherheitszustand erhöht ist.

2180



2181

2182

2183

Abbildung 6: PIC_KON_118 Aktivitätsdiagramm zu „TUC_KON_000 Prüfe Zugriffsberechtigung“

2184

2185

Welche Zugriffsregel für einen gegebenen Satz an Aufrufparametern anzuwenden ist, wird in Tabelle TAB_KON_513 ermittelt. Die Pflichtfelder mandantId, clientSystemId und

workplaceId und das optionale Feld userId sind zwar für die Auswertung der Regeln wichtig, tragen aber nicht zur Auswahl der Regel bei und sind daher in der Tabelle nicht vorhanden. Zur Auswahl einer Regel ist relevant,

- ob ctId bzw. cardHandle als Aufrufparameter gesetzt sind (not null) oder leer sind (null),
- von welchem Typ eine Karte ist, falls der Aufrufparameter cardHandle gesetzt ist,
- und welchen Wert die Aufrufparameter „needCardSession“ und „allWorkplaces“ annehmen.

Tabelle 16: TAB_KON_513 Zugriffsregeln Regelzuordnung

Parameter	R1	R2	R3	R4	R5	R6	R7	R8	R9
ctId	null	not null	null	not null					
cardHandle	null	null	null	null	not null	not null	not null	not null	not null
Karte(cardHandle).type					eGK oder KVK	eGK oder KVK			
Karte(cardHandle).type							SM-B		
Karte(cardHandle).type								HBAX	HBAX
needCardSession	false	false	false	false	false	true	true oder false	false	true
allWorkplaces	true	true	false	false	false	false	false	false	false

Tabelle TAB_KON_514 definiert einzelne Bedingungen, ordnet sie den Regeln zu und definiert ErrorCodes für den Fall, dass eine Bedingung nicht erfüllt ist.

Die Bedingungen in Tabelle TAB_KON_514 sind wie folgt gruppiert:

- Entitäten: Hier wird geprüft, ob die Entitäten, die mit den Aufrufparametern adressiert werden, im Informationsmodell existieren.
- Mandantenbezug: Hier wird geprüft, ob die adressierten Entitäten im Informationsmodell dem adressierten Mandanten zugeordnet sind.
- Relationen: Hier wird geprüft, ob die benötigten Zugriffsbeziehungen zum Zugriff auf die adressierten Entitäten im Informationsmodell existieren.
- Kartensitzungen: Hier wird geprüft, ob die benötigte Kartensitzung im Rahmen der bereits existierenden Kartenbeziehungen existieren darf.

Die Fehlercodes mit Beschreibung, ErrorType und Severity Tabelle TAB_KON_515.

2210 **Tabelle 17: TAB_KON_514-01 Zugriffsregeln Definition**

	Bedingung (siehe Hinweis 1)	R1	R2	R3	R4	R5	R6	R7	R8	R9	Error Code
Entität (siehe Hinweis 2)	inv : userId <> null									x	4003
	let m : Mandant = Mandant(mandantId) inv : m <> null	x	x	x	x	x	x	x	x	x	4021 an der Außenschnittstelle 4004 im Protokoll (siehe Hinweis 3)
	let cs : Clientsystem = Clientsystem (clientSystemId) inv : cs <> null	x	x	x	x	x	x	x	x	x	4021 an der Außenschnittstelle 4005 im Protokoll (siehe Hinweis 3)
	let ap : Arbeitsplatz = Arbeitsplatz (workplaceId) inv : ap <> null			x	x	x	x	x	x	x	4021 an der Außenschnittstelle 4006 im Protokoll (siehe Hinweis 3)
	let kt : Kartenterminal = Kartenterminal (ctId) inv : kt <> null		x		x						4007
	let k : Karte = Karte (cardHandle) inv : k <> null					x	x	x	x	x	4008
Mandant bezug	let m : Mandant = Mandant(mandantId) let cs : Clientsystem = Clientsystem (clientSystemId) inv : cs.mandant. includes(m)	x	x	x	x	x	x	x	x	x	4010
	let m : Mandant = Mandant(mandantId) let ap : Arbeitsplatz = Arbeitsplatz (workplaceId) inv : ap.mandant. includes(m)			x	x	x	x	x	x	x	4011

	<pre>let m : Mandant = Mandant(mandantId) let kt : Kartenterminal = Kartenterminal(ctId) inv : kt.mandant. includes(m)</pre>		x	x						4012
	<pre>let m : Mandant = Mandant(mandantId) let k : Karte = Karte(cardHandle) inv : k.kT-Slot. kartenterminal.mandant .includes(m)</pre>				x	x	x	x	x	4012
Relation	<pre>let k : Karte = Karte(cardHandle) inv : k.SM-B_Verwaltet <> null</pre>						x			4009
	<pre>let m : Mandant = Mandant(mandantId) let k : Karte = Karte(cardHandle) inv : k.SM-B_Verwaltet .mandant -> includes(m)</pre>						x			4013
	<pre>let m : Mandant = Mandant(mandantId) let cs : Clientsystem = Clientsystem (clientSystemId) let ap : Arbeitsplatz = Arbeitsplatz (workplaceId) inv : CS_AP.allInstances -> exists(c : CS_AP c.mandant = m and c.arbeitsplatz = ap and c.clientsystem = cs)</pre>			x	x	x	x	x	x	4014

<pre> let ap : Arbeitsplatz = Arbeitsplatz (workplaceId) let kt : Kartenterminal = Kartenterminal (ctId) inv : ap.lokalKartenterminal .includes(kt) or ap.entferntKarten terminal .includes(kt) </pre>				x						4015
<pre> let ap : Arbeitsplatz = Arbeitsplatz (workplaceId) let kt : Kartenterminal = Karte(cardHandle).kT- Slot.kartenterminal inv : ap.lokalKartenterminal .includes(kt) or ap.entferntKarten terminal .includes(kt) </pre>						x	x	x		4015
<pre> let m : Mandant = Mandant (mandantId) let kt : Kartenterminal = Kartenterminal(ctId) let cs : Clientsystem = Clientsystem (clientSystemId) inv : CS_AP.allInstances -> exists(c : CS_AP c.arbeitsplatz .lokalKartenterminal .includes(kt) or c.arbeitsplatz .entferntKartenterminal .includes(kt) and c.mandant = m and c.arbeitsplatz.mandant .includes(m) and c.clientsystem = cs) </pre>		x								4020

	<pre>let ap : Arbeitsplatz = Arbeitsplatz (workplaceId) let kt : Kartenterminal = Karte(cardHandle).kT- Slot.kartenterminal inv : ap.lokalKartenterminal .includes(kt)</pre>					x	x					4016
Karten sitzungen	<pre>let ap : Arbeitsplatz = Arbeitsplatz (workplaceId) let k : Karte = Karte(cardHandle) inv : k.kartensitzung -> not exists(ks : Kartensitzung ks.arbeitsplatz <> ap)</pre>						x					4017
	<pre>let k : Karte = Karte (cardHandle) let cs : Clientssystem = Clientssystem (clientSystemId) inv : k.kartensitzung -> not exists (ks : Kartensitzung ks .clientsystem = cs and ks .userId <> userId and ks .authState.size() > 0)</pre>									x		4018

2211 Erläuterungen zu TAB_KON_514-01:

- 2212 Hinweis 1:
 2213 Jede Bedingung ist als Constraint mittels OCL definiert, ist einzeln prüfbar und hat als
 2214 Eingangsparameter mandantId, clientSystemId, workplaceId, ctId, cardHandle und userId.
- 2215 Hinweis 2:
 2216 Zur Bezeichnung einer Objektinstanz, die im Informationsmodell vorhanden ist, wird die
 2217 Notation <<Entitätsbezeichner>>(<<Komma separierte Liste der Identitätsschlüssel>>
 2218 verwendet.
- 2219 Hinweis 3:
 2220 Bei manchen Bedingungen gibt es unterschiedliche Fehlermeldungen für die
 2221 Außenschnittstelle und für die interne Protokollierung. Dann wird folgende Notation in
 2222 Spalte "Error Code" verwendet:

- 2223 "<<Fehlercode>> an der Außenschnittstelle" für den Fehlercode, der über die
2224 Außenschnittstelle zurückgegeben werden muss
2225 "<<Fehlercode>> im Protokoll" für den Fehlercode, der für die interne Protokollierung
2226 verwendet werden muss.

2227

2228 **Tabelle 18: TAB_KON_515 Fehlercodes TUC_KON_000 „Prüfe Zugriffsberechtigung“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4003	Technical	Error	Keine User-ID angegeben, die zur Identifikation der Kartensitzung_HBAX benötigt wird.
4004	Technical	Error	Ungültige Mandanten-ID
4005	Technical	Error	Ungültige Clientsystem-ID
4006	Technical	Error	Ungültige Arbeitsplatz-ID
4007	Technical	Error	Ungültige Kartenterminal-ID
4008	Technical	Error	Karte nicht als gesteckt identifiziert
4009	Security	Error	SM-B ist dem Konnektor nicht als SM-B_Verwaltet bekannt
4010	Security	Error	Clientsystem ist dem Mandanten nicht zugeordnet
4011	Security	Error	Arbeitsplatz ist dem Mandanten nicht zugeordnet
4012	Security	Error	Kartenterminal ist dem Mandanten nicht zugeordnet
4013	Security	Error	SM-B_Verwaltet ist dem Mandanten nicht zugeordnet
4014	Security	Error	Für den Mandanten ist der Arbeitsplatz nicht dem Clientsystem zugeordnet
4015	Security	Error	Kartenterminal ist weder lokal noch entfernt vom Arbeitsplatz aus zugreifbar

4016	Security	Error	Kartenterminal ist nicht lokal vom Arbeitsplatz aus zugreifbar
4017	Security	Error	Die eGK hat bereits eine Kartensitzung, die einem anderen Arbeitsplatz zugeordnet ist.
4018	Security	Error	Der HBAX hat mindestens eine Kartensitzung zu einer anderen UserId, deren Sicherheitszustand erhöht ist. (Sicherheitszustand wird bei PIN-Eingabe erhöht.)
4019	Technical	Error	Zu den Parametern konnte keine Regel ermittelt werden.
4020	Security	Error	Kartenterminal ist weder lokal noch entfernt über irgendeinen dem Clientsystem zugeordneten Arbeitsplatz aus zugreifbar
4021	Technical	Error	Es sind nicht alle Pflichtparameter mandantId, clientSystemId, workplaceId gefüllt.
4204	Security	Error	Clientsystem aus dem Aufrufkontext konnte nicht authentifiziert werden.

2229 Hinweis zu Fehler 4018: Sicherheitszustand wird bei PIN-Eingabe erhöht.

2230 4.1.1.5 Operationen an der Außenschnittstelle

2231 Keine

2232 4.1.1.6 Betriebsaspekte

2233 TIP1-A_4525 - Initialisierung Zugriffsberechtigungsdienst

2234 Der Konnektor MUSS mit Abschluss der Bootup-Phase den Ist-Zustand transienter Entitäten und Beziehungen des Informationsmodells erfasst haben.

2236 [\leq]

2237

2238 TIP1-A_4526 - Bearbeitung Informationsmodell Zugriffsberechtigungsdienst

2239 Für die Administration MUSS der Konnektor eine Administrationsoberfläche zur Pflege des Informationsmodells zur Verfügung stellen. Die Oberfläche muss es ermöglichen, sämtliche persistente Entitäten und Beziehungen des durch Abbildung „PIC_Kon_100 Informationsmodell des Konnektors“ und Tabelle „TAB_KON_510 Informationsmodell Constraints“ definierten Informationsmodells initial anzulegen, zu ändern und zu löschen.

2244 [\leq]

2245 Im Anhang I „Umsetzungshinweise“ werden Empfehlungen zur Umsetzung der Administration des Informationsmodells gegeben.

2247 4.1.2 Dokumentvalidierungsdienst

2248 Der Dokumentvalidierungsdienst ist ein Dienst, der nur intern genutzt wird, d. h., dass dessen definierte Verhaltensweisen nur in anderen TUCs des Konnektors nachgenutzt

2250 werden. Er bietet Schnittstellen zum Validieren von Dokumenten an. Dabei werden
 2251 diejenigen spezifischen Dokumentformate unterstützt, die an den Außenschnittstellen
 2252 anderer Dienste wie Signatur- und Verschlüsselungsdienst auftreten können
 2253 (`Alle_DocFormate` gemäß Kapitel 3).

2254 Die jeweils gültigen XML-Schemas der Fachmodule werden den Herstellern von der
 2255 gematik bereitgestellt.

2256 **4.1.2.1 Funktionsmerkmalweite Aspekte**

2257 A_18780 - PDF/A-3 DARF NICHT unterstützt werden
 2258 Der Konnektor DARF Dokumente im PDF/A-3 Format NICHT unterstützen.
 2259 [`<=`]

2260 **4.1.2.2 Durch Ereignisse ausgelöste Reaktionen**

2261 Keine.

2262 **4.1.2.3 Interne TUCs, nicht durch Fachmodule nutzbar**

2263 Keine

2264 **4.1.2.4 Interne TUCs, auch durch Fachmodule nutzbar**

2265 *4.1.2.4.1 TUC_KON_080 „Dokument validieren“*

2266

2267 TIP1-A_4527-01 - TUC_KON_080 „Dokument validieren“
 2268 Der Konnektor MUSS den technischen Use Case TUC_KON_080 „Dokument validieren“
 2269 umsetzen.

2270

2271 **Tabelle 19: TAB_KON_143 – TUC_KON_080 „Dokument validieren“**

Element	Beschreibung
Name	TUC_KON_080 „Dokument validieren“
Beschreibung	Dieser TUC prüft das Format eines Dokuments und führt dokumententyp-spezifische Validierungen durch. Unterstützt werden <code>Alle_DocFormate</code> (außer „Binär“).
Auslöser	<ul style="list-style-type: none"> • Aufruf durch Fachmodul • Aufruf durch Basisdienst
Vorbedingungen	Keine
Eingangsdaten	<ul style="list-style-type: none"> • <code>documentToBeValidated</code> (Zu validierendes Dokument.) • <code>documentFormat</code> (mögliche Werte siehe Definition <code>Alle_DocFormate</code>; Formatangabe für das Dokument) <p>Optional für XML-Dokumente:</p>

	<ul style="list-style-type: none"> xmlSchemas – optional/nur für XML-Dokumente (XML-Schema und ggf. weitere vom Hauptschema benutzte Schemata) signaturePolicyIdentifier – optional/nur für XML-Formate gemäß einer referenzierten Signaturreichtlinie (URI identifiziert die Signaturreichtlinie)
Komponenten	Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> documentValidationProtocol (Prüfprotokoll) Die Ausprägung dieses Konnektor-internen Parameters erfolgt herstellerspezifisch.
Nachbedingungen	Keine
Standardablauf	<p>Validierung der Dokumente auf Typkonformität Der Konnektor führt je nach Format des Dokuments (documentFormat) eine der folgenden Prüfungen durch:</p> <p>A) XML-Dokumentvalidierung Im Fall eines XML-Dokuments prüft der Konnektor:</p> <ul style="list-style-type: none"> Prüfe die XML-Wohlgeformtheit des Dokumentes (documentToBeValidated) Wenn signaturePolicyIdentifier vorhanden ist, dann ermittle das xmlSchema aus der referenzierten Signaturreichtlinie und prüfe die Validität von documentToBeValidated in Bezug auf das hinterlegte XML-Schema. Der Eingangsparameter xmlSchemas wird ignoriert. Wenn signaturePolicyIdentifier nicht vorhanden ist und xmlSchemas übergeben wurden, dann prüfe die Wohlgeformtheit von xmlSchemas und die Validität von documentToBeValidated in Bezug auf xmlSchemas. Wenn nicht durch Prüfung gegen XML-Schema bereits erfolgt, dann prüfe die Eindeutigkeit der ID-Attributwerte im XML-Dokument. <p>B) PDF/A-Dokumentvalidierung PDF/A-Dokumente werden geprüft, ob sie sich als PDF/A Dokumente in ihren PDF/A-Metadaten ausweisen: Es wird geprüft, ob diese eines der folgenden Elemente enthalten</p> <pre><pdfaid:part xmlns:pdfaid="http://www.aiim.org/pdfa/ns/id/">1</pdfaid:part> <pdfaid:part xmlns:pdfaid="http://www.aiim.org/pdfa/ns/id/">2</pdfaid:part> <pdfaid:part xmlns:pdfaid="http://www.aiim.org/pdfa/ns/id/">3</pdfaid:part></pre>

	<p>C) TIFF-Dokumentvalidierung Der Konnektor prüft, ob das Dokument an Hand seiner ersten 8 Byte als TIFF-Dokument [TIFF6] zu identifizieren ist.</p> <p>D) MIME-Dokumentvalidierung Die Struktur von MIME-Dokumenten wird entsprechend [MIME] validiert.</p> <p>E) Text-Dokumentvalidierung Der Konnektor prüft die Konformität zum im Dokumentenformat vorgegebenen Character-Encoding. Für Binärdokumente findet keine Validierung statt. Hinweis: Byte-order-marks (BOM) sind im Rahmen von UTF-8 kodierten Dokumenten gemäß UTF8 Standard ([RFC3629], Kapitel 6) erlaubt, aber nicht notwendigerweise im Dokument vorhanden.</p>
Varianten/ Alternativen	
Fehlerfälle	<p>Standardablauf: Bei der Dokumentenvalidierung protokolliert der TUC alle aufgetretenen Fehler im Rückgabewert documentValidationProtocol.</p> <p>(→A) Fehlerfälle bei XML-Dokumentvalidierung Wenn keine Schemata übergeben wurden (xmlSchemas oder signaturePolicyIdentifier nicht vorhanden): Fehlercode 4193 Wenn eines der übergebenen Schemata selbst nicht wohlgeformt oder invalide ist, wird Fehlercode 4026 gemeldet. Wenn das XML-Dokument nicht wohlgeformt ist, wird Fehlercode 4022 gemeldet. Das XML-Dokument ist nicht valide in Bezug auf das zur Validierung benutzte Schema (xmlSchemas bzw. signaturePolicyIdentifier): Fehlercode 4023.</p> <p>(→B) Fehlerfälle bei PDF/A-Dokumentvalidierung Bei fehlgeschlagener Validierung: Fehlercode 4024, Dokumentformat = PDF/A</p> <p>(→C) Fehlerfälle bei TIFF-Dokumentvalidierung Bei fehlgeschlagener Validierung: Fehlercode 4024, Dokumentformat = TIFF</p> <p>(→D) Fehlerfälle bei MIME-Dokumentvalidierung Bei fehlgeschlagener Validierung: Fehlercode 4024, Dokumentformat = MIME</p> <p>(→E) Fehlerfälle bei Text-Dokumentvalidierung Bei fehlgeschlagener Validierung: Fehlercode 4024, Dokumentformat = Text</p>
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

Tabelle 20: TAB_KON_144 Fehlercodes TUC_KON_080 „Dokument validieren“

Fehlercode	ErrorType	Severity	Fehlertext
------------	-----------	----------	------------

Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4022	Security	Error	XML-Dokument nicht wohlgeformt
4023	Security	Error	XML-Dokument nicht valide in Bezug auf XML-Schema
4024	Security	Error	Formatvalidierung fehlgeschlagen (<Dokumentformat>) Der Parameter Dokumentformat kann die Werte XML, PDF/A, TIFF, MIME und Text annehmen.
4026	Security	Error	XML-Schema nicht valide
4193	Security	Warning	kein XML-Schema für XML-Dokument vorhanden

2275

2276 [\leq]2277 **4.1.2.5 Operationen an der Außenschnittstelle**

2278 Keine

2279 **4.1.2.6 Betriebsaspekte**

2280 Keine

2281 **4.1.3 Dienstverzeichnisdienst**

2282 Der Dienstverzeichnisdienst liefert dem aufrufenden Clientsystem sowohl Informationen
 2283 über die Version und Produktkenndaten des Konnektors, als auch die SOAP-Endpunkte,
 2284 über die das Clientsystem die einzelnen Dienstoperationen erreichen kann.

2285 **4.1.3.1 Funktionsmerkmalweite Aspekte**

2286 Die Endpunkte der Basisdienste werden in WSDL spezifiziert. Diese Endpunkte und
 2287 weitere konnektormodellspezifische Informationen werden dem Clientsystem in Form
 2288 eines Dienstverzeichnisdienstes gesammelt angeboten.

2289 Der prinzipielle Ablauf sieht dabei folgendermaßen aus:

2290 Das Clientsystem ruft beim Initialisieren des Systems mit HTTP-GET die vordefinierte
 2291 URL: `https://<ANLW_LAN_IP_ADDRESS`
 2292 oder `MGM_KONN_HOSTNAME>/connector.sds` oder `http://<ANLW_LAN_IP_ADDRESS`
 2293 oder `MGM_KONN_HOSTNAME>/connector.sds` des Konnektors auf.

2294 Der Konnektor stellt die Liste der Dienste, der Versionen und die Endpunkte der Dienste
 2295 in einem XML-Dokument zusammen. Jeder über SOAP erreichbare Basisdienst des
 2296 Konnektors wird in dieser Liste geführt. Ferner können Fachmodule ihre eigenen
 2297 Endpunkte über TUC_KON_041 „Einbringen der Endpunktinformationen während der
 2298 Bootup-Phase“ einbringen. Die so erstellte Liste der Dienste wird als Antwort an das
 2299 Clientsystem übergeben.

2300 Das Clientsystem prüft, ob die gewünschten Dienste und Versionen unterstützt werden
 2301 und merkt sich die Endpunkte der Dienste für die späteren Aufrufe. Danach kann das
 2302 Clientsystem diese Dienstendpunkte nach Bedarf aufrufen.

2303 TIP1-A_4528 - Bereitstellen des Dienstverzeichnisdienst

2304 Der Konnektor MUSS den Dienstverzeichnisdienst anbieten. Dieser Dienst veröffentlicht
 2305 auf: `https://$ANLW_LAN_IP_ADDRESS` oder `$MGM_KONN_HOSTNAME>/connector.sds`
 2306 `s`
 2307 oder `http://$ANLW_LAN_IP_ADDRESS` oder `$MGM_KONN_HOSTNAME>/connector.sds`
 2308 `.`
 2309 Die Datei MUSS über https erreichbar sein.
 2310 Wenn (ANCL_DVD_OPEN = Enabled) oder (ANCL_TLS_MANDATORY = Disabled) MUSS
 2311 die Datei auch über http erreichbar sein.
 2312 [**<=**]

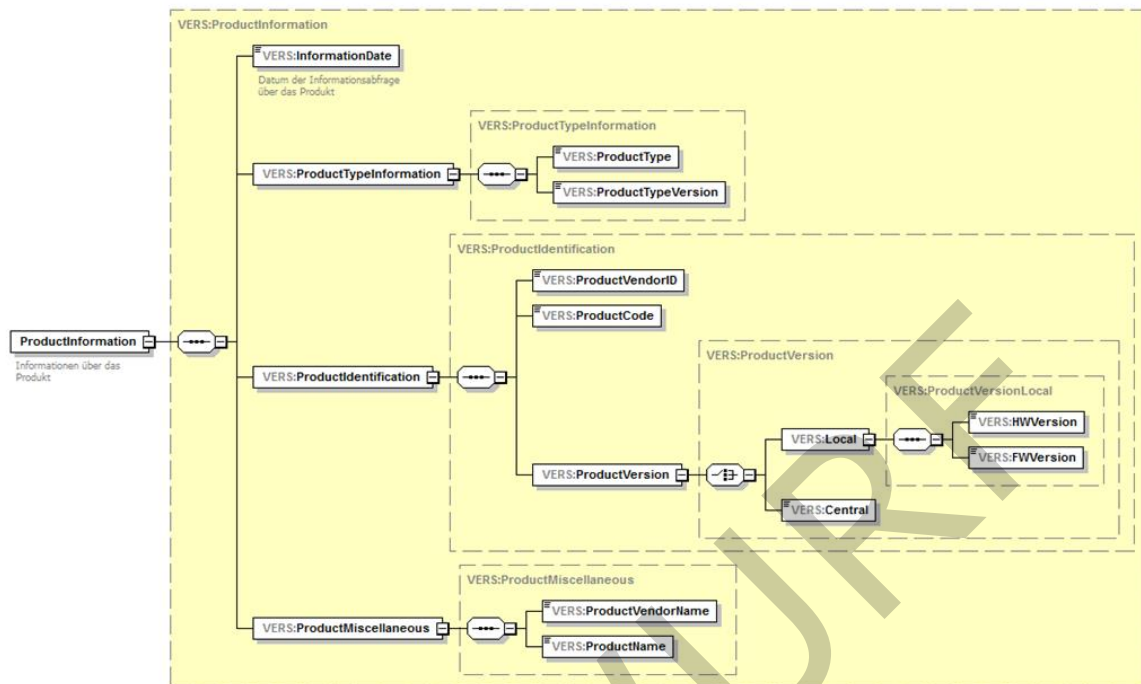
2313 TIP1-A_4529 - Formatierung der Ausgabedatei
 2314 Das XML-Dokument, welches als „connector.sds“ dem Aufrufer zurückgeliefert wird,
 2315 MUSS gemäß dem Schema „conn/ServiceDirectory.xsd“ formatiert sein.
 2316 conn/ServiceDirectory.xsd referenziert die Schemata
 2317 „tel/version/ProductInformation.xsd“ (siehe [gemSpec_OM]) und
 2318 „conn/ServiceInformation.xsd“.
 2319 TAB_KON_516, TAB_KON_517 und TAB_KON_518 beschreiben die Elemente der zu
 2320 verwendenden Schemastruktur.
 2321

2322 **Tabelle 21: TAB_KON_516 Basisanwendung Dienstverzeichnisdienst**

Name	ConnectorServiceDirectory
Version	Siehe Anhang D
Namensraum	Siehe Anhang D
Namensraum-Kürzel	CONN
Operationen	Lesen der vom Konnektor unterstützten Dienste
WSDL	Keine
Schema	ServiceDirectory.xsd

2323
2324

Tabelle 22: TAB_KON_517 Schemabeschreibung Produktinformation (ProductInformation.xsd)

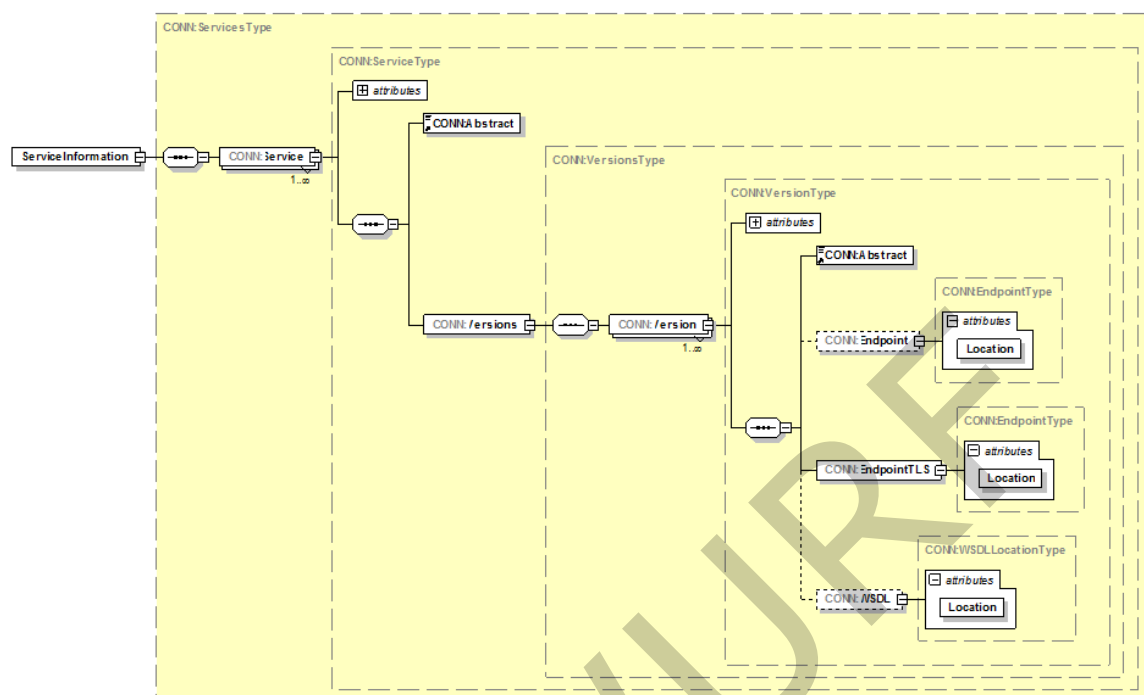


2325
2326

Element	Bedeutung
ProductInformation/InformationDate	Datum der Informationsabfrage über das Produkt
ProductInformation/ProductTypeInfoInformation/ProductType	Produkttyp (Konnektor)
ProductInformation/ProductTypeInfoInformation/ProductTypeVersion	Produkttypversion des Konnektormodells
ProductInformation/ProductIdentification/ProductVendorID	ID des Konnektorherstellers
ProductInformation/ProductIdentification/ProductCode	Produktkürzel
ProductInformation/ProductIdentification/ProductVersion/Local/HWVersion	Hardwareversion des Konnektormodells
ProductInformation/ProductIdentification/ProductVersion/Local/FWVersion	Firmwareversion des Konnektormodells
ProductInformation/ProductMiscellaneous/ProductVendorName	Name des Konnektorherstellers
ProductInformation/ProductMiscellaneous/ProductName	Produktname

2327
2328

**Tabelle 23: TAB_KON_518 Schemabeschreibung Serviceinformation
(Serviceinformation.xsd)**



Element	Bedeutung
ServiceInformation/Service	Element beschreibt einen Dienst oder ein Fachmodul
ServiceInformation/Service/@Name	Name des Dienstes. Dieser Wert korrespondiert mit dem Feld „Name“ aus der jeweiligen Basisanwendung/Dienstbeschreibung (englischer Dienstname in Tabelle TAB_KON_798).
ServiceInformation/Service/Abstract	eine kurze textuelle Beschreibung des Dienstes/Fachmoduls
ServiceInformation/Service/Versions	die Liste der unterstützten Versionen
ServiceInformation/Service/Versions/Version	Beschreibung der Dienstversion/Fachmodulversion
ServiceInformation/Service/Versions/Version/@TargetNamespace	der Namensraum der Dienst-/Fachmodulversion
ServiceInformation/Service/Versions/Version/@Version	Vollständige Versionsnummer (Konnektordienstversion) des Dienstes/Fachmoduls. Dieser Wert entspricht dem Wert „WSDL-Version“ des jeweiligen Dienstes in Tabelle TAB_KON_798.

ServiceInformation/Service/Versions/Version/Abstract	Eine kurze textuelle Beschreibung dieser Version des Dienstes/Fachmoduls
ServiceInformation/Service/Versions/Version/EndpointTLS/@Location	Absoluter URL des über TLS erreichbaren Dienstes.
ServiceInformation/Service/Versions/Version/Endpoint/@Location	Absoluter URL des erreichbaren Dienstes (ohne TLS).
ServiceInformation/Service/Versions/Version/WSDL/@Location	(optional) Absoluter URL der WSDL-Beschreibung

2329
2330
2331

[<=]

2332 TIP1-A_4530 - Aufbau Dienst URLs

2333 Die URLs der Dienste KÖNNEN herstellerspezifisch aufgebaut werden.

2334 [<=]

2335 4.1.3.2 Durch Ereignisse ausgelöste Reaktionen

2336 Keine.

2337 4.1.3.3 Interne TUCs, nicht durch Fachmodule nutzbar

2338 Keine

2339 4.1.3.4 Interne TUCs, auch durch Fachmodule nutzbar

2340 Da der Konnektor als Black-Box mit inkludierten Fachmodulen ohne erkennbare
2341 Innenschnittstellen spezifiziert wird, stellt der folgende TUC lediglich einen Mechanismus
2342 zur editoriellen Kopplung der Fachmodulspezifikationen mit der Konnektorspezifikation
2343 dar:

2344 4.1.3.4.1 TUC_KON_041 „Einbringen der Endpunktinformationen während der Bootup-
2345 Phase“

2346 TIP1-A_4531 - TUC_KON_041 „Einbringen der Endpunktinformationen während der
2347 Bootup-Phase“

2348 Der Dienstverzeichnisdienst des Konnektors MUSS es den Fachmodulen ermöglichen, die
2349 zum jeweiligen Fachmodul gehörenden Endpunkte während der Bootup-Phase des
2350 Konnektors in den Dienstverzeichnisdienst einzubringen.

2351

2352 **Tabelle 24: TAB_KON_519 - TUC_KON_041 „Einbringen der Endpunktinformationen**
2353 **während der Bootup-Phase“**

Element	Beschreibung
Name	TUC_KON_041 „Einbringen der Endpunktinformationen während der Bootup-Phase“
Beschreibung	Fachmodule MÜSSEN ihre Endpunktinformationen während der Bootup-Phase in den Dienstverzeichnisdienst einbringen können.

Auslöser und Vorbedingungen	Keine
Eingangsdaten	<ul style="list-style-type: none"> serviceInformation (Ein XML-Dokument mit dem Wurzelement „ServiceInformation“ gemäß dem Schema „ServiceInformation.xsd“. Eine Beschreibung des Schemas befindet sich in TAB_KON_518.)
Komponenten	Konnektor, Fachmodule
Ausgangsdaten	<ul style="list-style-type: none"> Keine
Standardablauf	Die übergebenen Serviceinformationen des Fachmoduls werden in die Gesamtstruktur „connector.sds“ aufgenommen. Falls beim Speichern der eingebrachten Endpunktinformationen ein Fehler auftritt, wird Fehler 4027 ausgelöst.
Varianten/Alternativen	Keine
Fehlerfälle	4027: Die Endpunktinformationen konnten nicht übernommen werden.
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 25: TAB_KON_520 Fehlercodes TUC_KON_041 „Einbringen der Endpunktinformationen während der Bootup-Phase“

Fehlercode	ErrorType	Severity	Fehlertext
4027	Technical	Error	Die Endpunktinformationen konnten nicht übernommen werden.

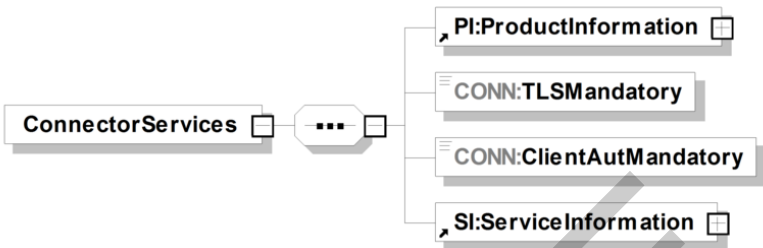
[<=]

4.1.3.5 Operationen an der Außenschnittstelle

TIP1-A_4532 - Schnittstelle der Basisanwendung Dienstverzeichnisdienst
Der Dienstverzeichnisdienst des Konnektors MUSS die in Tabelle TAB_KON_521 Schnittstelle der Basisanwendung Dienstverzeichnisdienst beschriebene Schnittstelle anbieten.

Tabelle 26: TAB_KON_521 Schnittstelle der Basisanwendung Dienstverzeichnisdienst

Dienstname	ConnectorServiceDirectory
Beschreibung	Der Aufruf liefert Angaben über den Hersteller, über das Konnektormodell und die Liste der Dienste, Konnektordienstversionen (KDV) und Endpunkte der Dienste.
Aufruf	GET /connector.sds HTTP/1.1 Host: ANLW_LAN_IP_ADDRESS oder MGM_KONN_HOSTNAME

Rückgabe	Das Antwortdokument ist in der Schemadatei <code>ServiceDirectory.xsd</code> beschrieben.	
	ConnectorServices	
		
	Name	Beschreibung
	ProductInformation	Kurzbeschreibung des Konnektormodells
	ServiceInformation	Beschreibung der Dienste
	ProductInformation: Das Schema wird in TAB_KON_517 beschrieben. Die Felder sind gemäß [gemSpec_OM] zu befüllen und gemäß dem Schema „ProductInformation.xsd“ zu formatieren.	
	TLS-Mandatory: Boolean Wert der festlegt, ob die Verwendung eines TLS-Kanals für Dienstaufrufe verpflichtend ist. Definierende Variable ist: ANCL_TLS_MANDATORY ClientAutMandatory: Boolean Wert der festlegt, ob Client Authentifizierung verpflichtend ist. Definierende Variable ist: ANCL_CAUT_MANDATORY.	
	ServiceInformation: Das Schema wird in TAB_KON_518 beschrieben. Die Felder sind gemäß dem Schema <code>ServiceInformation.xsd</code> zu formatieren. Falls (ANCL_CAUT_MANDATORY = Enabled) oder (ANCL_TLS_MANDATORY = Enabled), MUSS die Rückgabedatei ausschließlich https-Endpunkte enthalten.	
	Fehlercodes	Die Standard HTTP1.1 Fehlercodes [RFC2616]
Vorbedingungen	Keine	
Nachbedingungen	Keine	
Hinweise	Keine	

[<=]

4.1.3.6 Betriebsaspekte

TIP1-A_4533 - Dienstverzeichnisdienst initialisieren.

Mit Abschluss der Bootup-Phase MUSS der Dienstverzeichnisdienst an der Außenschnittstelle die vollständige Liste aller Services bereitstellen, die der

2372 Anwendungskonnektor den Clientsystemen anbietet, inklusive der Services der
 2373 Fachmodule.
 2374 [\leq]

2375 4.1.4 Kartenterminaldienst

2376 Die Aufgabe des Kartenterminaldienstes ist das Management aller vom Konnektor
 2377 adressierbaren Kartenterminals. Dies umfasst alle administrativen Prozesse
 2378 (insbesondere das Pairing, vgl. [gemSpec_KT#2.5.2]). Ferner kapselt der
 2379 Kartenterminaldienst die Zugriffe auf Kartenterminals durch Basisdienste und
 2380 Fachmodule.

2381 Für die TLS-Verbindungen zu den Kartenterminals muss der Konnektor die Vorgaben aus
 2382 [gemSpec_Krypt#3.3.2] und hinsichtlich ECC-Migration die Vorgaben aus
 2383 [gemSpec_Krypt#5] befolgen.

2384 Innerhalb des Kartenterminaldienstes werden folgende Präfixe für Bezeichner verwendet:

- 2385 • Events (Topic Ebene 1): „CT“
- 2386 • Konfigurationsparameter: „CTM_“

2387 Der Kartenterminaldienst verwaltet hinsichtlich der Kartenterminals mindestens die in der
 2388 informativen Tabelle TAB_KON_522 Parameterübersicht des Kartenterminaldienstes
 2389 ausgewiesenen Parameter, weitere herstellerspezifische Parameter sind möglich. Die
 2390 normative Festlegung wann welche Parameter mit welchen Werten belegt werden, erfolgt
 2391 in den folgenden Abschnitten und Unterkapiteln.

2392 Dabei beschrieben CTM_xyz-Bezeichner Parameter, die den Dienst als Ganzes betreffen.
 2393 Zu jedem Kartenterminal selbst werden dessen Parameter in einem CT-Object gekapselt.
 2394 Die folgende Tabelle zeigt die Attribute der jeweiligen CT-Objekte über
 2395 Punktschreibweise.

2396 **Tabelle 27: TAB_KON_522 Parameterübersicht des Kartenterminaldienstes**

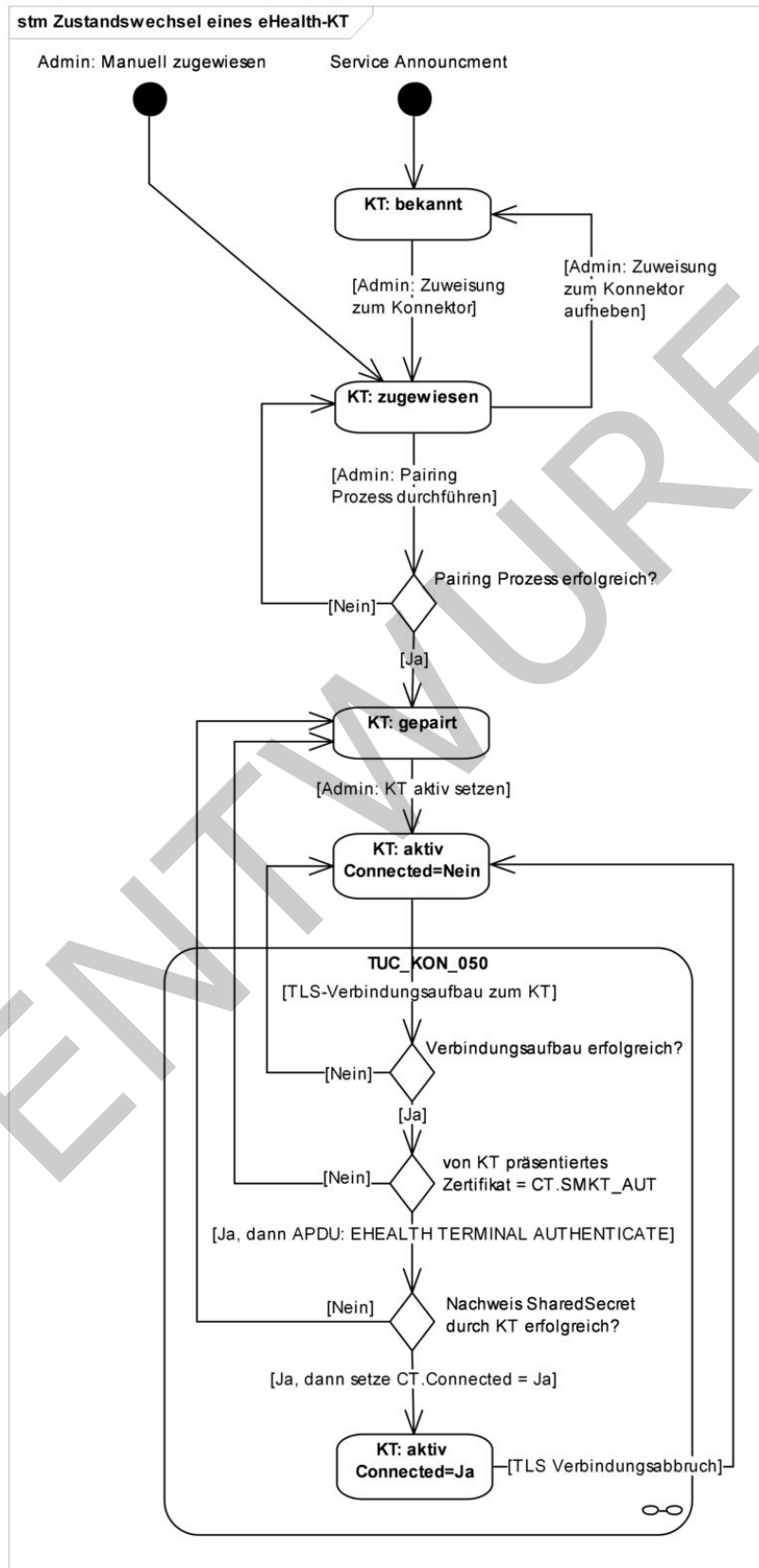
ReferenzID	Belegung	Zustandswerte
CTM_CT_LIST	Liste von CT-Objekten	Eine Liste von Repräsentanzen (CT-Objects) der dem Konnektor bekannten Kartenterminals.
Pro CTM_CT_LIST Eintrag:		
Gerätekenndaten		
CT.CTID	Identifizier	Eindeutige, statische Identifikation des Kartenterminals
CT.IS_PHYSICAL	Ja/Nein	Kennzeichnung, ob es sich um ein physisches oder logisches Kartenterminal handelt, zur Unterscheidung von eHealth-Kartenterminals und HSM-Bs. Da dieser Unterschied gemäß der aktuellen HSM-B-Lösung für den Konnektor transparent ist, wird der Parameter in dieser Spezifikation immer auf „Ja“ gesetzt.

		Der Parameterwert „Nein“ ist für zukünftige Nutzung vorgesehen.
CT.MAC_ADRESS	MAC-Adresse	Die MAC-Adresse des Kartenterminals
CT.HOSTNAME	String	SICCT-Terminalname des Kartenterminals, auch als FriendlyName bezeichnet
CT.IP_ADRESS	IP-Adresse	Die IP-Adresse des Kartenterminals
CT.TCP_PORT	Portnummer	Der TCP-Port des SICCT-Kommandointerpreters des Kartenterminals
CT.SLOT_COUNT	Nummer	Anzahl der Slots des Kartenterminals
CT.SLOTS_USED	Liste	Liste der aktuell mit Karten belegten Slots
CT.PRODUCT_INFORMATION	Inhalt ProductInformation.xsd	Die Herstellerinformationen zum Kartenterminal gemäß [gemSpec_OM]
CT.EHEALTH_INTERFACE_VERSION	Version	Die EHEALTH-Interface-Version des Kartenterminals, die mittels GET STATUS aus dem Element VER des Discretionary Data Objects ermittelt wurde.
CT.VALID_VERSION	Boolean	True, wenn die Version des Kartenterminals (CT.EHEALTH_INTERFACE_VERSION) durch den Konnektor unterstützt wird, d.h. zu den in CTM_SUPPORTED_KT_VERSIONS passt Default-Wert = false
CT.DISPLAY_CAPABILITIES	Datenstruktur	Displayeigenschaften wie in der Struktur Display Capabilities Data Object in [SICCT#5.5.10.17] beschrieben
Pairingdaten		
CT.SMKT_AUT	X.509-Cert	C.SMKT.AUT-Zertifikat des Kartenterminals, gespeichert im Rahmen des Pairings
CT.SHARED_SECRET		ShS.KT.AUT, gespeichert im Rahmen des Pairings
Verbindungsdaten		
CT.CORRELATION	bekannt zugewiesen gepairt	Der Korrelationsstatus zum Konnektor:

	aktiv aktualisierend	<ul style="list-style-type: none"> • bekannt (über Service Announcement/Service Discovery gelernte Kartenterminals), • zugewiesen (durch den Administrator aus dem Bereich der bekannten Kartenterminals oder manuell konfigurierte Kartenterminals), • gepairt (Pairing erfolgreich aber noch nicht zum Verbindungsaufbau freigegeben) • aktiv (durch Administrator zum Verbindungsaufbau freigegeben), • aktualisierend (ein laufender Updatevorgang, ausgelöst durch den Konnektor; Der Zustand tritt ein, wenn der Kartenterminaldienst das Event „KSR/UPDATE/START“ fängt und endet mit dem Event „KSR/UPDATE/END“)
CT.CONNECTED	Ja/Nein	Der Verfügbarkeitsstatus des Kartenterminals (Ja = nach Aufbau der TLS-Verbindung und erfolgter zweiter Authentifizierung)
CT.ACTIVEROLE	User/Admin	Benutzerrolle, die für die aktuelle Session verwendet wird
KT-Admin-Credentials		
CT.ADMIN_USERNAME	String	Username des Administrators am KT
CT.ADMIN_PASSWORD	String	Password des Administrators am KT

2397

2398 Zum besseren Verständnis sind die Zustände, die ein Kartenterminal einnehmen kann, im
2399 nachfolgenden Zustandsdiagramm PIC_KON_071 dargestellt.



2400

2401 **Abbildung 7: PIC_KON_071 Korrelationszustände eines eHealth-KT**2402 **4.1.4.1 Funktionsmerkmalweite Aspekte**

2403 TIP1-A_4534 - Kartenterminals nach eHealth-KT-Spezifikation

2404 Der Kartenterminaldienst MUSS Kartenterminals nach der eHealth-Kartenterminal
2405 Spezifikation [gemSpec_KT] unterstützen.2406 [**<=**]2407 Zur Unterstützung von HSM-Bs benötigt der Konnektor virtuelle Kartenterminals
2408 (CT.IS_PHYSICAL=Nein), in denen virtuelle SMC-Bs „stecken“ können (siehe Kapitel
2409 4.1.4). Diese Kartenterminals werden innerhalb des Zugriffsberechtigungsdienstes sowie
2410 des Systeminformationsdienstes wie normale Kartenterminals berücksichtigt. Weitere
2411 Details zu den logischen Kartenterminals finden sich im Kapitel Betriebsaspekte.

2412 TIP1-A_4535 - Unterstützung logischer Kartenterminals für HSMs

2413 Der Kartenterminaldienst MUSS logische Kartenterminals mit logischen Slots
2414 unterstützen. Zu jedem verwalteten HSM (siehe Kartendienst) MUSS der Konnektor ein
2415 oder mehrere logische Kartenterminal mit folgenden Bedingungen vorhalten:

- 2416
- Jedes logische KT MUSS als CT-Object mit eindeutiger CTID in CTM_CT_LIST
2417 enthalten sein
 - Die CT-Attribute MÜSSEN gemäß TAB_KON_522 Parameterübersicht des
2418 Kartenterminaldienstes gesetzt werden.

2420 [**<=**]

2421 TIP1-A_4536 - TLS-Verbindung zu Kartenterminals halten

2422 Der Kartenterminaldienst MUSS jede mit einem Kartenterminal etablierte Verbindung
2423 durch Nutzung des in [SICCT#6.1.4.5] definierten Keep-Alive Mechanismus halten. Der
2424 Konnektor MUSS für das Heartbeat-Interval gemäß [SICCT#6.1.4.5] den Wert
2425 CTM_KEEP_ALIVE_INTERVAL verwenden und beim Ausbleiben von Terminal-Antworten
2426 eines Kartenterminals nach der Anzahl von CTM_KEEP_ALIVE_TRY_COUNT Versuchen
2427 die Netzwerkverbindung zu diesem Kartenterminal beenden.2428 [**<=**]

2429 TIP1-A_6725 - Lebensdauer von Textanzeigen am Kartenterminal

2430 Der Konnektor MUSS steuern, dass Textanzeigen am Kartenterminal nur so lange
2431 angezeigt werden, wie sie im jeweiligen Anwendungskontext benötigt werden.2432 [**<=**]2433 Ziel der Textanzeigen am Kartenterminal ist die Kommunikation mit dem Benutzer zur
2434 Unterstützung der Anwendungsfälle. Die Anzeige am Kartenterminal muss daher einen
2435 engen zeitlichen Bezug zum jeweiligen Anwendungskontext haben.2436 Nachrichten, deren Anwendungskontext mit einem Event beendet werden, wie etwa die
2437 Aufforderung zum Stecken der Karte im Kontext von TUC_KON_056, deren inhaltliche
2438 Berechtigung mit dem Stecken der Karte erlischt, (ebenso zum Ziehen der Karte im
2439 Rahmen von TUC_KON_057) müssen sofort gelöscht werden, wenn das Event eintritt.2440 Nachrichten, deren Lebensdauer nicht durch ein natürliches Event beendet wird, müssen
2441 eine vordefinierte Lebensdauer erhalten, die per Konfiguration an die Bedürfnisse der
2442 Leistungserbringer anpassbar sein sollte. Das gilt für Ergebnisanzeigen oder Anzeigen
2443 von Fehlern.2444 TIP1-A_4537 - KT-Statusanpassung bei Beendigung oder Timeout einer
2445 Netzwerkverbindung

- 2446 Tritt ein Timeout ein oder wird eine Netzwerkverbindung zu einem Kartenterminal (oder
2447 zu einem HSM, welches einem logischen Kartenterminal zugeordnet ist) beendet oder
2448 zurückgesetzt und ist CT.CONNECTED = Ja, so MUSS der Konnektor:
- 2449 • CT.CONNECTED für das Kartenterminal auf „Nein“ setzen
 - 2450 • Für jeden in CT.SLOTS_USED gelisteten Slot X zur weiteren internen Bearbeitung
2451 TUC_KON_256 {
2452 topic = „CT/SLOT_FREE“;
2453 eventType = Op;
2454 severity = Info;
2455 parameters = („CtID=\$CT.CTID, SlotNo=\$X“);
2456 doLog = false;
2457 doDisp = false }
2458 rufen
 - 2459 • TUC_KON_256 {
2460 topic = „CT/DISCONNECTED“;
2461 eventType = Op;
2462 severity = Info;
2463 parameters = („CtID=\$CT.CTID, Hostname=\$CT.HOSTNAME“) }
2464 auslösen
 - 2465 • CT.SLOTS_USED leeren
- 2466 [**<=**]
- 2467 TIP1-A_4538 - Wiederholter Verbindungsversuch zu den KTs
2468 Sind in CTM_CT_LIST Kartenterminals mit CT.CONNECTED=Nein und CT.VALID_VERSION
2469 = True und CT.CORRELATION = „aktiv“ und ist CTM_SERVICE_DISCOVERY_CYCLE>0,
2470 MUSS der Konnektor im ZeitabstandCTM_SERVICE_DISCOVERY_CYCLE-Minuten entweder
2471 eine Service Discovery-Nachricht an alle KTs als Broadcast oder an jedes einzelne dieser
2472 unverbundenen KTs als Unicast senden.
2473 [**<=**]
- 2474 TIP1-A_4538-02 - ab PTV4: Wiederholter Verbindungsversuch zu den KTs
2475 Sind in CTM_CT_LIST Kartenterminals mit CT.CONNECTED=Nein und CT.VALID_VERSION
2476 = True und CT.CORRELATION = „aktiv“ und ist CTM_SERVICE_DISCOVERY_CYCLE>0,
2477 MUSS der Konnektor im ZeitabstandCTM_SERVICE_DISCOVERY_CYCLE-Minuten an jedes
2478 einzelne dieser unverbundenen KTs eine Service-Discovery-Nachricht als Unicast senden.
2479 [**<=**]
- 2480 TIP1-A_6478 - Erlaubte SICCT-Kommandos bei CT.CONNECTED=Nein
2481 Der Kartenterminaldienst DARF SICCT-bzw. EHEALTH-Kommandos NICHT an ein
2482 Kartenterminal senden, wenn für dieses Kartenterminal CT.CONNECTED=Nein gesetzt ist.
2483 Ausgenommen hiervon sind die in TAB_KON_785 gelisteten EHEALTH- bzw. SICCT-
2484 Kommandos.
2485 [**<=**]
- 2486 **Tabelle 28: TAB_KON_785 Erlaubte SICCT-Kommandos bei CT.CONNECTED=Nein**

SICCT-Kommando
SICCT CT INIT CT SESSION
SICCT CT CLOSE SESSION
SICCT GET STATUS
SICCT SET STATUS

SICCT CT DOWNLOAD INIT
SICCT CT DOWNLOAD DATA
SICCT CT DOWNLOAD FINISH
EHEALTH TERMINAL AUTHENTICATE

2487 TIP1-A_4539 - Robuster Kartenterminaldienst
2488 Das Ziehen einer Karte während einer Kartenaktion DARF NICHT dazu führen, dass das
2489 verwaltete Kartenterminal im Anschluss durch den Konnektor nicht weiter genutzt
2490 werden kann. Die entsprechende Ressource MUSS nach Erkennung der Fehlersituation
2491 freigegeben werden. Ein manuelles Eingreifen DARF NICHT erforderlich sein.
2492 [**<=**]

2493 TIP1-A_5408 - Terminal-Anzeigen beim Anfordern und Auswerfen von Karten
2494 Der Konnektor MUSS beim Anfordern und Auswerfen von Karten die folgenden Display-
2495 Nachrichten für die Anzeige im Kartenterminal verwenden, wenn der Aufrufer keine
2496 konkrete Display-Nachricht übergeben hat. Der Verweis auf den Kartenterminal-Slot
2497 SOLL in der Display-Nachricht entfallen, wenn es keine Slot-Auswahl am Kartenterminal
2498 gibt.
2499

2500 **Tabelle 29: TAB_KON_727 Terminalanzeigen beim Anfordern und Auswerfen von Karten**

Kontext	Kartentyp	Terminal-Anzeige
Karte anfordern	EGK	Bitte • 0x0BeGK • 0x0Bin • 0x0BSLOT X • 0x0Bstecken
	HBA, HBAX, HBA-qSig	Bitte • 0x0BHBA • 0x0Bin • 0x0BSLOT X • 0x0Bstecken
	SMC-B	Bitte • 0x0BSMC-B • 0x0Bin • 0x0BSLOT X • 0x0Bstecken
	sonstiger Kartentyp oder kein explizit angegebener Kartentyp	Bitte • 0x0BKarte • 0x0Bin • 0x0BSLOT X • 0x0Bstecken
Karte auswerfen	EGK	Bitte • 0x0BeGK • 0x0Baus • 0x0BSLOT X • 0x0Bentnehmen
	HBA, HBAX, HBA-qSig	Bitte • 0x0BHBA • 0x0Baus • 0x0BSLOT X • 0x0Bentnehmen
	SMC-B	Bitte • 0x0BSMC-B • 0x0Baus • 0x0BSLOT X • 0x0Bentnehmen
	sonstiger Kartentyp oder kein explizit angegebener Kartentyp	Bitte • 0x0BKarte • 0x0Bentnehmen

2501 [**<=**]

4.1.4.2 Durch Ereignisse ausgelöste Reaktionen

TIP1-A_4540 - Reaktion auf Dienstbeschreibungspakete

Der Konnektor MUSS Service Announcement für das Auffinden von Kartenterminals entsprechend [SICCT] und [gemSpec_KT] unterstützen. Der Konnektor MUSS

Dienstbeschreibungspakete auf UDP Port `CTM_SERVICE_ANNOUNCEMENT_PORT` entgegennehmen.

Erhält er ein solches Dienstbeschreibungspaket, MUSS er

- TUC_KON_054 mit Mode=AutoAdded und IP-Adresse; TCP-Port; MAC-Adresse; Hostname aus dem Dienstbeschreibungspaket, aufrufen
- für das mit der MAC-Adressen in `CTM_CT_LIST` korrelierende CT-Object, wenn `CT.CORRELATION > "bekannt"` und `CT.VALID_VERSION = true` ist, TUC_KON_050 { `ctId = CT.CtId`; `role = „User“` } aufrufen.

[<=]

TIP1-A_4541 - Reaktion auf KT-Slot-Ereignis – Karte eingesteckt

Der Kartenterminaldienst MUSS auf SICCT-Ereignisnachrichten „Slot-Ereignis – Karte eingesteckt“ ([SICCT#6.1.4.4], TAG ,84') wie folgt reagieren:

- das meldende Kartenterminal CT in `CTM_CT_LIST` ermitteln,
- den in der Ereignisnachricht benannten Slot (FU-Nummer) in `CT.SLOTS_USED` aufnehmen,
- zur weiteren internen Bearbeitung rufe TUC_KON_256 {
`topic = „CT/SLOT_IN_USE“;`
`eventType = Op;`
`severity = Info;`
`parameters = („CtID=$CT.CTID,`
`SlotNo=<FU-Nummer aus Ereignisnachricht>„);`
`doLog = false;`
`doDisp = false } auf.`

[<=]

TIP1-A_4542 - Reaktion auf KT-Slot-Ereignis – Karte entfernt

Der Kartenterminaldienst MUSS auf SICCT-Ereignisnachrichten „Slot-Ereignis – Karte entfernt“ ([SICCT#6.1.4.4], TAG ,85') wie folgt reagieren:

- das meldende Kartenterminal CT in `CTM_CT_LIST` ermitteln,
- den in der Ereignisnachricht benannten Slot (FU-Nummer) aus `CT.SLOTS_USED` entfernen,
- zur weiteren internen Bearbeitung rufe TUC_KON_256 {
`topic = „CT/SLOT_FREE“;`
`eventType = Op;`
`severity = Info;`
`parameters = („CtID=$CT.CTID,`
`SlotNo==<FU-Nummer aus Ereignisnachricht>„);`
`doLog = false;`
`doDisp = false } auf.`

[<=]

TIP1-A_4543 - KT-Statusanpassung bei Beginn eines Updatevorgangs

Tritt der Event "KSR/UPDATE/START" mit „Target=KT“ ein, MUSS der Konnektor:

2548 • Setze CT = CTM_CT_LIST(CTID-Parameter des Ereignisses)

2549 • CT.CORRELATION für das Kartenterminal merken und auf „aktualisierend“ setzen

2550 • Für jeden in CT.SLOTS_USED gelisteten Slot X zur weiteren internen Bearbeitung

2551 TUC_KON_256 {

2552 topic = „CT/SLOT_FREE“;

2553 eventType = Op;

2554 severity = Info;

2555 parameters = („CtID=\$CT.CTID, SlotNo=\$CT.SLOTS_USED[X]“);

2556 doLog = false;

2557 doDisp = false

2558 } aufrufen

2559 [**<=**]

2560 TIP1-A_4544 - KT-Statusanpassung bei Ende eines Updatevorgangs

2561 Tritt der Event "KSR/UPDATE/END" mit „Target=KT“ ein, MUSS der Konnektor:

2562 • Setze CT = CTM_CT_LIST(CTID-Parameter des Ereignisses)

2563 • CT.CORRELATION auf den beim „KSR/UPDATE/START“ gemerkten Wert setzen

2564 • Aktualisiere Gerätedaten durch Aufruf TUC_KON_055 „Befülle CT-Object“ {ctId =

2565 CTID}

2566 • Wenn CT.VALID_VERSION = true, Rufe TUC_KON_050 „Beginne

2567 Kartenterminalsitzung“ {ctId = CTID; role = „User“}

2568 • Wenn CT.VALID_VERSION = false und CT.CORRELATION = „aktiv“, setze

2569 CT.CORRELATION=„gepairt“

2570 [**<=**]

2571 4.1.4.3 Interne TUCs, nicht durch Fachmodule nutzbar

2572 4.1.4.3.1 TUC_KON_050 „Beginne Kartenterminalsitzung“

2573 TIP1-A_4545-03 - TUC_KON_050 „Beginne Kartenterminalsitzung“

2574 Der Konnektor MUSS den technischen Use Case „Beginne Kartenterminalsitzung“ gemäß

2575 TUC_KON_050 umsetzen.

2576

2577 **Tabelle 30: TAB_KON_039 – TUC_KON_050 „Beginne Kartenterminalsitzung“**

Element	Beschreibung
Name	TUC_KON_050 „Beginne Kartenterminalsitzung“
Beschreibung	TUC_KON_050 baut eine TLS-Verbindung vom Konnektor zum Kartenterminal auf und beginnt eine SICCT-Sitzung. Anschließend erfolgt die 2. Authentifizierung des Kartenterminals (Prüfung SharedSecret).

Auslöser	<ul style="list-style-type: none"> • Neustart des Konnektors • nach dem Setzen eines Kartenterminals auf „aktiv“ • im Rahmen eines erneuten Verbindungsversuchs
Vorbedingungen	ctId ist in CTM_CT_LIST vorhanden
Eingangsdaten	<ul style="list-style-type: none"> • ctId (zu verbindendes Kartenterminal) • role (Benutzerrolle; gültig sind: „User“ und „Admin“)
Komponenten	Konnektor, Kartenterminal
Ausgangsdaten	keine
Nachbedingungen	<ul style="list-style-type: none"> • TLS-Kanal und SICCT-Session mit gewünschter Benutzerrolle aufgebaut, wenn CT.CORRELATION >= "gepairt" • TLS-Kanal und SICCT-Session mit leerem Username, Password und Session ID aufgebaut, wenn CT.CORRELATION <= „zugewiesen“ • Steck-Ereignisse für alle im KT befindlichen Karten ausgelöst, wenn CT.CORRELATION >= „gepairt“

Standardablauf	<p>Setze CT = CTM_CT_LIST(ctId)</p> <ol style="list-style-type: none"> 1. Wenn CT.IS_PHYSICAL = Nein: prüfen, ob role = „User“ Wenn CT.CONNECTED = Ja: TUC endet erfolgreich Nein: - Verbindung zu HSM in Slot 1 aufbauen - weiter mit Schritt 9 2. Wenn CT.CONNECTED = Ja prüfen, ob CT.ACTIVEROLE = role Ja: TUC endet erfolgreich Nein: - Schließen der Cardterminal Session mit dem Kartenterminalkommando SICCT CLOSE CT SESSION, - weiter ab Schritt 6 (halten der TLS-Verbindung und nur Wechsel der Session) 3. Aufbau einer TLS-Verbindung mit dem Kartenterminal unter Verwendung von ID.SAK.AUT. Dabei Prüfung des KT-Zertifikats mittels TUC_KON_037 { certificate= C.SMKT.AUT; qualifiedCheck=not_required; offlineAllowNoCheck=true; policyList= oid_smkt_aut; intendedKeyUsage= intendedKeyUsage(C.SMKT.AUT); intendedExtendedKeyUsage=id-kp-serverAuth; validationMode=NONE } 4. Wenn CT.CORRELATION <= „zugewiesen“: <ol style="list-style-type: none"> a. Öffne eine Cardterminal Session mit dem Kartenterminalkommando SICCT INIT CT SESSION (siehe [SICCT#5.10]) mit leerem Username, Password und Session ID b. Nur Verbindung in niedriger Korrelation, daher setze CT.CONNECTED = Nein, um fachliche Nutzung des KT zu verhindern c. beende TUC erfolgreich 5. Prüfe, ob das Zertifikat aus der TLS-Verbindung mit den zum Kartenterminal gespeicherten Referenzdaten (CT.SMKT_AUT) übereinstimmt. <ol style="list-style-type: none"> a. Läuft das Zertifikat CT.SMKT_AUT (oder C.SMKT.AUT, sie müssen hier identisch sein), dann geht der Konnektor über in den Betriebszustand EC_CardTerminal_SMC-KT_Certificate_Expires_Soon (ctId). 6. Parallelisierung <ol style="list-style-type: none"> a. Generierung eines zufälligen Werts (Challenge) mit mindestens 16 Byte Länge gemäß [gemSpec_Krypt#2.2] (siehe [gemSpec_KT#DO_KT_0004]), b. Öffnen einer Cardterminal Session mit dem Kartenterminalkommando SICCT INIT CT SESSION (siehe
----------------	---

	<p>[SICCT#5.10]) mit</p> <ul style="list-style-type: none"> - ctId als Adressat - Wenn role = User dann mit leerem Username, Password und Session ID Wenn role = „Admin dann mit leerer Session ID aber mit CT.ADMIN_USERNAME und CT.ADMIN_PASSWORD <p>7. Senden der Challenge mittels Kartenterminalkommando EHEALTH TERMINAL AUTHENTICATE (siehe [gemSpec_KT#3.7.2]) in der Ausprägung VALIDATE mit:</p> <ul style="list-style-type: none"> - Kartenterminal als Empfänger - und mit der in Schritt 6a generierten Challenge im Shared Secret Challenge DO <p>8. Prüfe Antwort des Kartenterminals, ob sie einen korrekten Hashwert über Challenge und angehängtes CT.SHARED_SECRET gemäß [gemSpec_KT#SEQ_KT_0002] Schritt 4-5 enthält</p> <p>9. Setze:</p> <ul style="list-style-type: none"> a. CT.ACTIVEROLE = \$role b. CT.CONNECTED = Ja <p>10. Wenn TLS-Verbindung neu aufgebaut werden musste, rufe TUC_KON_256 { topic = „CT/CONNECTED“; eventType = „Op“; severity = Info; parameters = („CtID=\$CT.CTID, Hostname=\$CT.HOSTNAME“) }</p> <p>11. Ermittle alle im KT gesteckten Karten und befülle entsprechend CT.SLOTS_USED</p> <p>Für jeden in CT.SLOTS_USED gelisteten Slot X zur weiteren internen Bearbeitung TUC_KON_256{ topic = „CT/SLOT_IN_USE“; eventType = Op; severity = Info; parameters = („CtID=\$CT.CTID, SlotNo=\$CT.SLOTS_USED[X]“); doLog = false; doDisp = false } rufen.</p>
--	---

Varianten/ Alternativen	Keine.
Fehlerfälle	<p>Fehler in den folgenden Schritten des Ablaufs führen zu: Aufruf von TUC_KON_256 { topic = "CT/TLS_ESTABLISHMENT_FAILURE"; eventType = \$ErrorType; severity = \$Severity; parameters = („CtID=\$CT.ID, Name=\$CT.HOSTNAME, Error=\$Fehlercode, Bedeutung=\$Fehlertext“) } Abbruch der Verarbeitung mit den ausgewiesenen Fehlercodes</p> <p>(→1): Admin-Rolle für logische KTs nicht möglich (hätte bei korrekter Implementierung nicht stattfinden dürfen), Fehlercode: 4032 (→1): Verbindungsaufbau zu HSM fehlgeschlagen, Fehlercode: 4032 (→3): Fehler im TLS-Verbindungsaufbau bzw. Zertifikatsprüfung, Fehlercode: 4028 und setze CT.CONNECTED auf „Nein“ (→3): TLS-Verbindung konnte nicht innerhalb von CTM_TLS_HS_TIMEOUT Sekunden aufgebaut werden , Fehlercode: 4028 und setze CT.CONNECTED auf „Nein“ (→5): Präsentiertes Zertifikat nicht das aus dem Pairing, Fehlercode: 4029 und setze CT.CORRELATION auf „gepairt“ und setze CT.CONNECTED auf „Nein“ und terminiere TLS-Verbindung (→6b): Hinterlegte KT-Admin-Credentials fehlerhaft, Fehlercode: 4030 und in die User-Session zurückzuwechseln (damit das KT für den normalen Fachbetrieb weiterhin zur Verfügung steht) (→8): Prüfung auf Nachweis SharedSecret fehlgeschlagen, Fehlercode 4029 und setze CT.CORRELATION auf „gepairt“ und setze CT.CONNECTED auf „Nein“ und terminiere TLS-Verbindung</p>
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	Abbildung PIC_KON_110 Aktivitätsdiagramm zu „Beginne Kartenterminalsitzung

```
graph TD
    Start(( )) --> TUC_KON_050[TUC_KON_050 Beginne Kartenterminalsitzung]
    TUC_KON_050 --> CT_IS_PHYSICAL{CT IS_PHYSICAL?}
    CT_IS_PHYSICAL -- Ja --> CT_CONNECTED_1{CT CONNECTED?}
    CT_CONNECTED_1 -- Ja --> TUC_endet[TUC endet erfolgreich]
    CT_CONNECTED_1 -- Nein --> CT_CONNECTED_2{CT CONNECTED?}
    CT_CONNECTED_2 -- Ja --> TUC_endet
    CT_CONNECTED_2 -- Nein --> Fehler_4032_1((Fehler 4032))
    Fehler_4032_1 --> Benutzermote_Is_User{Benutzermote = User?}
    Benutzermote_Is_User -- Ja --> CT_CONNECTED_1
    Benutzermote_Is_User -- Nein --> Fehler_4032_2((Fehler 4032))
    Fehler_4032_2 --> Baue_Verbindung[Baue Verbindung zu HSM in Slot 1 auf]
    Baue_Verbindung --> Fehler_4032_3((Fehler 4032))
    Fehler_4032_3 --> Baue_Verbindung
    Baue_Verbindung --> CT_ACTIVE_ROLE{CT ACTIVE ROLE = Benutzermote?}
    CT_ACTIVE_ROLE -- Ja --> CT_CONNECTED_1
    CT_ACTIVE_ROLE -- Nein --> CT_CONNECTED_3{CT CONNECTED?}
    CT_CONNECTED_3 -- Ja --> TUC_endet
    CT_CONNECTED_3 -- Nein --> ID_SAK_AUT[ID SAK_AUT]
    ID_SAK_AUT --> Baue_TLS_Verbindung[Baue TLS-Verbindung zum KT auf]
    Baue_TLS_Verbindung -- [mit Fehler] --> Fehler_4028((Fehler 4028))
    Fehler_4028 --> Setze_CT_CONNECTED_Nein[Setze CT.CONNECTED auf "Nein"]
    Setze_CT_CONNECTED_Nein --> Fehler_4028
    Baue_TLS_Verbindung -- [Ohne Fehler] --> CT_CORRELATION{CT CORRELATION <= "zugewiesen" ?}
    CT_CORRELATION -- Ja --> Baue_TLS_Verbindung
    CT_CORRELATION -- Nein --> Sende_APDU_4a[Sende APDU - Öffne KT-Sitzung command = INIT CT SESSION (Username, Passwort und Session ID leer)]
    Sende_APDU_4a -- [a] --> Setze_CT_CONNECTED_Nein
    Sende_APDU_4a -- [mit Fehler] --> Fehler_4029_1((Fehler 4029))
    Fehler_4029_1 --> Setze_CT_CONNECTED_Nein
    Sende_APDU_4a -- [Ohne Fehler] --> CT_SMKT_AUT[CT SMKT_AUT]
    CT_SMKT_AUT --> Vergleiche_TLS_Zertifikat[5. Vergleiche TLS-Zertifikat mit KT-Referenzdaten]
    Vergleiche_TLS_Zertifikat -- [Zertifikate stimmen nicht überein] --> Setze_CT_CONNECTED_Nein
    Vergleiche_TLS_Zertifikat -- [Zertifikate stimmen überein] --> Benutzermote_Is_Admin{Benutzermote?}
    Benutzermote_Is_Admin -- Admin --> Sende_APDU_6b_1[Sende APDU - Öffne KT-Sitzung command = INIT CT SESSION (CT.ADMIN_USERNAME, CT.ADMIN_PASSWORD, Session ID leer)]
    Benutzermote_Is_Admin -- User --> Sende_APDU_6b_2[Sende APDU - Öffne KT-Sitzung command = INIT CT SESSION (Username, Passwort und Session ID leer)]
    Sende_APDU_6b_1 --> Fehler_4030_1((Fehler 4030))
    Fehler_4030_1 --> Fehler_4030_2((Fehler 4030))
    Fehler_4030_2 --> Fehler_4030_3((Fehler 4030))
    Fehler_4030_3 --> Fehler_4030_4((Fehler 4030))
    Fehler_4030_4 --> Fehler_4030_5((Fehler 4030))
    Fehler_4030_5 --> Fehler_4030_6((Fehler 4030))
    Fehler_4030_6 --> Fehler_4030_7((Fehler 4030))
    Fehler_4030_7 --> Fehler_4030_8((Fehler 4030))
    Fehler_4030_8 --> Fehler_4030_9((Fehler 4030))
    Fehler_4030_9 --> Fehler_4030_10((Fehler 4030))
    Fehler_4030_10 --> Fehler_4030_11((Fehler 4030))
    Fehler_4030_11 --> Fehler_4030_12((Fehler 4030))
    Fehler_4030_12 --> Fehler_4030_13((Fehler 4030))
    Fehler_4030_13 --> Fehler_4030_14((Fehler 4030))
    Fehler_4030_14 --> Fehler_4030_15((Fehler 4030))
    Fehler_4030_15 --> Fehler_4030_16((Fehler 4030))
    Fehler_4030_16 --> Fehler_4030_17((Fehler 4030))
    Fehler_4030_17 --> Fehler_4030_18((Fehler 4030))
    Fehler_4030_18 --> Fehler_4030_19((Fehler 4030))
    Fehler_4030_19 --> Fehler_4030_20((Fehler 4030))
    Fehler_4030_20 --> Fehler_4030_21((Fehler 4030))
    Fehler_4030_21 --> Fehler_4030_22((Fehler 4030))
    Fehler_4030_22 --> Fehler_4030_23((Fehler 4030))
    Fehler_4030_23 --> Fehler_4030_24((Fehler 4030))
    Fehler_4030_24 --> Fehler_4030_25((Fehler 4030))
    Fehler_4030_25 --> Fehler_4030_26((Fehler 4030))
    Fehler_4030_26 --> Fehler_4030_27((Fehler 4030))
    Fehler_4030_27 --> Fehler_4030_28((Fehler 4030))
    Fehler_4030_28 --> Fehler_4030_29((Fehler 4030))
    Fehler_4030_29 --> Fehler_4030_30((Fehler 4030))
    Fehler_4030_30 --> Fehler_4030_31((Fehler 4030))
    Fehler_4030_31 --> Fehler_4030_32((Fehler 4030))
    Fehler_4030_32 --> Fehler_4030_33((Fehler 4030))
    Fehler_4030_33 --> Fehler_4030_34((Fehler 4030))
    Fehler_4030_34 --> Fehler_4030_35((Fehler 4030))
    Fehler_4030_35 --> Fehler_4030_36((Fehler 4030))
    Fehler_4030_36 --> Fehler_4030_37((Fehler 4030))
    Fehler_4030_37 --> Fehler_4030_38((Fehler 4030))
    Fehler_4030_38 --> Fehler_4030_39((Fehler 4030))
    Fehler_4030_39 --> Fehler_4030_40((Fehler 4030))
    Fehler_4030_40 --> Fehler_4030_41((Fehler 4030))
    Fehler_4030_41 --> Fehler_4030_42((Fehler 4030))
    Fehler_4030_42 --> Fehler_4030_43((Fehler 4030))
    Fehler_4030_43 --> Fehler_4030_44((Fehler 4030))
    Fehler_4030_44 --> Fehler_4030_45((Fehler 4030))
    Fehler_4030_45 --> Fehler_4030_46((Fehler 4030))
    Fehler_4030_46 --> Fehler_4030_47((Fehler 4030))
    Fehler_4030_47 --> Fehler_4030_48((Fehler 4030))
    Fehler_4030_48 --> Fehler_4030_49((Fehler 4030))
    Fehler_4030_49 --> Fehler_4030_50((Fehler 4030))
    Fehler_4030_50 --> Fehler_4030_51((Fehler 4030))
    Fehler_4030_51 --> Fehler_4030_52((Fehler 4030))
    Fehler_4030_52 --> Fehler_4030_53((Fehler 4030))
    Fehler_4030_53 --> Fehler_4030_54((Fehler 4030))
    Fehler_4030_54 --> Fehler_4030_55((Fehler 4030))
    Fehler_4030_55 --> Fehler_4030_56((Fehler 4030))
    Fehler_4030_56 --> Fehler_4030_57((Fehler 4030))
    Fehler_4030_57 --> Fehler_4030_58((Fehler 4030))
    Fehler_4030_58 --> Fehler_4030_59((Fehler 4030))
    Fehler_4030_59 --> Fehler_4030_60((Fehler 4030))
    Fehler_4030_60 --> Fehler_4030_61((Fehler 4030))
    Fehler_4030_61 --> Fehler_4030_62((Fehler 4030))
    Fehler_4030_62 --> Fehler_4030_63((Fehler 4030))
    Fehler_4030_63 --> Fehler_4030_64((Fehler 4030))
    Fehler_4030_64 --> Fehler_4030_65((Fehler 4030))
    Fehler_4030_65 --> Fehler_4030_66((Fehler 4030))
    Fehler_4030_66 --> Fehler_4030_67((Fehler 4030))
    Fehler_4030_67 --> Fehler_4030_68((Fehler 4030))
    Fehler_4030_68 --> Fehler_4030_69((Fehler 4030))
    Fehler_4030_69 --> Fehler_4030_70((Fehler 4030))
    Fehler_4030_70 --> Fehler_4030_71((Fehler 4030))
    Fehler_4030_71 --> Fehler_4030_72((Fehler 4030))
    Fehler_4030_72 --> Fehler_4030_73((Fehler 4030))
    Fehler_4030_73 --> Fehler_4030_74((Fehler 4030))
    Fehler_4030_74 --> Fehler_4030_75((Fehler 4030))
    Fehler_4030_75 --> Fehler_4030_76((Fehler 4030))
    Fehler_4030_76 --> Fehler_4030_77((Fehler 4030))
    Fehler_4030_77 --> Fehler_4030_78((Fehler 4030))
    Fehler_4030_78 --> Fehler_4030_79((Fehler 4030))
    Fehler_4030_79 --> Fehler_4030_80((Fehler 4030))
    Fehler_4030_80 --> Fehler_4030_81((Fehler 4030))
    Fehler_4030_81 --> Fehler_4030_82((Fehler 4030))
    Fehler_4030_82 --> Fehler_4030_83((Fehler 4030))
    Fehler_4030_83 --> Fehler_4030_84((Fehler 4030))
    Fehler_4030_84 --> Fehler_4030_85((Fehler 4030))
    Fehler_4030_85 --> Fehler_4030_86((Fehler 4030))
    Fehler_4030_86 --> Fehler_4030_87((Fehler 4030))
    Fehler_4030_87 --> Fehler_4030_88((Fehler 4030))
    Fehler_4030_88 --> Fehler_4030_89((Fehler 4030))
    Fehler_4030_89 --> Fehler_4030_90((Fehler 4030))
    Fehler_4030_90 --> Fehler_4030_91((Fehler 4030))
    Fehler_4030_91 --> Fehler_4030_92((Fehler 4030))
    Fehler_4030_
```

gemSpec_Kon_V5.docx
Version: 5.11.0 CC

2580
2581

2582 **Tabelle 31: TAB_KON_523 Fehlercodes TUC_KON_050 „Beginne Kartenterminalsitzung“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4028	Technical	Error	Fehler beim Versuch eines Verbindungsaufbaus zu KT
4029	Security	Error	Fehler bei der KT-Authentisierung. KT möglicherweise manipuliert
4030	Security	Error	Admin-Werte für KT fehlerhaft
4032	Technical	Error	Verbindung zu HSM konnte nicht aufgebaut werden

2583
2584
2585
2586 [\leq]
2587

2588 **4.1.4.3.2 TUC_KON_054 „Kartenterminal hinzufügen“**

2589 TIP1-A_4546 - TUC_KON_054 „Kartenterminal hinzufügen“

2590 Der Konnektor MUSS den technischen Use Case TUC_KON_054 „Kartenterminal
2591 hinzufügen“ umsetzen.

2592 **Tabelle 32: TAB_KON_524 – TUC_KON_054 „Kartenterminal hinzufügen“**

Element	Beschreibung
Name	TUC_KON_054 „Kartenterminal hinzufügen“
Beschreibung	Dieser TUC nimmt ein neues Kartenterminal in die zentrale Verwaltung auf (CTM_CT_LIST) oder aktualisiert die Einträge zu einem bereits erfassten Kartenterminal.
Auslöser	<ul style="list-style-type: none"> • ein empfangenes Dienstbeschreibungspaket ohne vorheriges Service Discovery • manuelles Hinzufügen eines KT-Eintrags • ein empfangenes Dienstbeschreibungspaket nach vorherigem Auslösen eines manuellen Service Discovery
Vorbedingungen	<ul style="list-style-type: none"> • entweder ist das KT noch nicht in CTM_CT_LIST enthalten • oder das KT ist unter anderer IP/anderem Hostnamen schon gelistet
Eingangsdaten	<ul style="list-style-type: none"> • Mode (AutoAdded, ManuallyAdded, ManuallyModified) • IP-Adresse (IPv4) • TCP-Port (optional) • MAC-Adresse (optional) • Hostname (optional)

Komponenten	Konnektor, Kartenterminal
Ausgangsdaten	<ul style="list-style-type: none"> keine
Nachbedingungen	<ul style="list-style-type: none"> Das Kartenterminal ist mit allen Gerätekenndaten in CTM_CT_LIST vorhanden
Standardablauf	<ol style="list-style-type: none"> Sofern optionale Parameter nicht übergeben wurden oder Mode<>AutoAdded, ermittle Port, MAC und Hostname via Service Discovery als UDP/IP-Unicast an IP-Adresse und Port CTM_SERVICE_DISCOVERY_PORT Finde CT in CTM_CT_LIST über MAC-Adresse Wenn MAC-Adresse nicht in CTM_CT_LIST: <ol style="list-style-type: none"> Erzeuge neuen CT-Object-Eintrag in CTM_CT_LIST und <ul style="list-style-type: none"> Generiere eindeutige CT.CTID setze CT.MAC_ADRESS auf MAC-Adresse Setze CT.CORRELATION = „bekannt“ Setze CT.CONNECTED = „Nein“ Wenn Mode= ManuallyAdded setze CT.CORRELATION = „zugewiesen“ Wenn CT.CONNECTED = Ja und (IP-Adresse <> CT.IP_ADRESS oder TCP-Port <> CT.TCP_PORT), beende TLS-Verbindung und setze CT.CONNECTED = „Nein“ Befülle: CT.IP_ADRESS, CT.Hostname, CT.TCP_PORT Wenn CT.CORRELATION>=„zugewiesen“ rufe TUC_KON_055 „Befülle CT-Object“
Varianten/ Alternativen	Keine
Fehlerfälle	<p>Fehler im Ablauf (Standardablauf oder Varianten) führen in den folgend ausgewiesenen Schritten zu einem Abbruch der Verarbeitung mit den ausgewiesenen Fehlercodes:</p> <p>(→1) Keine Antwort innerhalb CTM_SERVICE_DISCOVERY_TIMEOUT, Fehlercode: 4033</p> <p>(→1) Ermittelte MAC-Adresse weicht von übergebener MAC-Adresse ab, Fehlercode: 4035</p> <p>(→1) Ermittelter Hostname-Adresse weicht von übergebenem Hostname ab, Fehlercode: 4036</p> <p>(→2) Wenn Mode=ManuallyModified und nicht gefunden, Fehlercode: 4037</p> <p>Zusätzlich im Abbruchfall:</p> <ul style="list-style-type: none"> Aufruf von TUC_KON_256 { topic = "CT/CT_ADDING_ERROR"; eventType = \$ErrorType; severity = \$Severity; parameters = („IP=\$IP-Adresse, Name=\$HOSTNAME, Error=\$Fehlercode, Bedeutung=\$Fehlertext“) }

	- Keine Veränderung an CTM_CT_LIST
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	keine

2593 **Tabelle 33: TAB_KON_525 Fehlercodes TUC_KON_054 „Kartenterminal hinzufügen“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4033	Technical	Error	Kartenterminal antwortet nicht, Zufügen fehlgeschlagen
4035	Technical	Error	Angegebener IP-Adresse gehört zu einer anderen MAC-Adresse als die, die übergeben wurde. Angaben zur MAC prüfen
4036	Technical	Error	Angegebener IP-Adresse gehört zu einem anderen Hostname als der, der übergeben wurde. Angaben zum Hostname prüfen
4037	Technical	Error	Verwaltung der Kartenterminals inkonsistent

2594
2595
2596 **[<=]**

2597 **4.1.4.3.3 TUC_KON_053 „Paire Kartenterminal“**

2598 TIP1-A_4548-02 - TUC_KON_053 „Paire Kartenterminal“
2599 Der Konnektor MUSS den technischen Use Case „Paire Kartenterminal“ gemäß
2600 TUC_KON_053 umsetzen.

2601 **Tabelle 34: TAB_KON_041 – TUC_KON_053 „Paire Kartenterminal“**

Element	Beschreibung
Name	TUC_KON_053 „Paire Kartenterminal“
Beschreibung	TUC_KON_053 führt das Pairing zwischen dem Konnektor und einem eHealth-Kartenterminal durch.
Auslöser	Dialoge zur Administration des Konnektors. Der Administrator hat ein Kartenterminal im Dialog der Managementschnittstelle ausgewählt und das Pairing aufgerufen.
Vorbedingungen	<ul style="list-style-type: none"> KT ist in CTM_CT_LIST vorhanden CT.CORRELATION = „zugewiesen“ CT.IS_PHYSICAL = Ja

Eingangsdaten	<ul style="list-style-type: none"> ctId
Komponenten	Konnektor, Kartenterminal
Ausgangsdaten	<ul style="list-style-type: none"> Keine
Nachbedingunge n	<ul style="list-style-type: none"> CT.CORRELATION = „aktiv“, wenn Pairing erfolgreich CT.CORRELATION = „zugewiesen“, wenn Pairing nicht erfolgreich CT.CONNECTED = „Ja“, wenn Pairing erfolgreich
Standardablauf	<p>Setze CT = CTM_CT_LIST(ctId)</p> <ol style="list-style-type: none"> 1. Prüfe CT.VALID_VERSION = true 2. Aufbau einer TLS-Verbindung mit dem Kartenterminal unter Verwendung von ID.SAK.AUT. Dabei: <ol style="list-style-type: none"> a. Speichern des präsentierten KT-Zertifikats in CT.SMKT_AUT b. Prüfung des KT-Zertifikats mittels TUC_KON_037{ <pre>certificate = C.SMKT.AUT; qualifiedCheck = not_required; offlineAllowNoCheck = true; policyList = oid _smkt_aut; intendedKeyUsage= intendedKeyUsage(C.SMKT.AUT)</pre> ; <pre>intendedExtendedKeyUsage = id-kp-serverAuth; validationMode = NONE }</pre> 3. Der Konnektor entnimmt den Fingerprint dem KT-Zertifikat und stellt dies dem Administrator im Dialog der Managementschnittstelle dar. Der Konnektor fordert den Administrator auf, den Fingerprint zu akzeptieren oder zurückzuweisen. 4. Wenn der Administrator den Fingerprint bestätigt, <ol style="list-style-type: none"> a. generiert der Konnektor einen neuen Schlüssel, das Shared Secret ShS.KT.AUT gemäß [gemSpec_Krypt#2.2] (siehe [gemSpec_KT#3.7]) und speichert es in CT.SHARED_SECRET b. und eröffnet der Konnektor mit dem Kartenterminalkommando SICCT INIT CT SESSION (siehe [SICCT#5.10]) mit <ul style="list-style-type: none"> - ctId als Adressat - und mit leerem Username, Password und Session ID eine Cardterminal Session. 5. Der Konnektor sendet mittels Kartenterminalkommando EHEALTH TERMINAL AUTHENTICATE (siehe [gemSpec_KT#3.7.2]) in der Ausprägung CREATE mit <ul style="list-style-type: none"> - ctId als Empfänger - und mit dem in Schritt 4.a generierten Schlüssel im Shared Secret DO und der Display Message „KT:\$CT.MAC_ADRESS MIT

	<p>KON:\$MGM_KONN_HOSTNAME PAIREN OK?", wobei die MAC-Adresse mit Trenner im folgenden Format dargestellt werden MUSS: „AABBCC:DDEEFF“</p> <p>das Shared Secret an das Kartenterminal.</p> <p>6. Der Konnektor prüft ob in der Antwort des Kartenterminals eine</p> <p>korrekte Signatur des Shared Secrets gemäß [gemSpec_KT#SEQ_KT_0001] Schritt 7, ausgeführt mit dem Schlüssel zum Zertifikat CT.SMKT_AUT vorliegt.</p> <p>7. CT.CORRELATION wird auf „gepairt“ gesetzt</p> <p>8. TLS-Verbindung, die zum Pairen diente, beenden und zuvor das Kartenterminalkommando SICCT CLOSE CT SESSION mit ctId als Adressat senden</p> <p>9. Automatischer Zustandsübergang CT.CORRELATION = „gepairt“ nach „aktiv“ (implizite Aktion des Administrators durch Aufruf von TUC_KON_053).</p> <p>10. „Arbeits“-TLS-Verbindung neu aufbauen durch Aufruf TUC_KON_050 { ctId; role = „User“}</p>
Varianten/ Alternativen	<p>(→4): weist der Administrator den Fingerprint in Schritt 3 ab, wird TUC_KON_053 nach Ausführung folgender Aktivitäten beendet:</p> <p>4.1.a) Löschen von CT.SMKT_AUT</p> <p>4.1.b) Abbau der TLS-Verbindung, Setzen von CT.CONNECTED auf „Nein“</p>
Fehlerfälle	<p>Fehler in den folgenden Schritten des Ablaufs führen zu:</p> <p>a) Aufruf von TUC_KON_256 { topic = "CT/ERROR"; eventType = \$ErrorType; severity = \$Severity; parameters = („CtID=\$ctId, Name=\$CT.HOSTNAME, Error=\$Fehlercode, Bedeutung=\$Fehlertext"); doDisp = false }</p> <p>b) Löschen von CT.SMKT_AUT, CT.SHARED_SECRET</p> <p>c) Direkte Anzeige der Fehlermeldung für den Administrator</p> <p>d) Abbruch der Verarbeitung mit den ausgewiesenen Fehlercodes</p> <p>(→1) Version des KT wird nicht unterstützt, Fehlercode: 4042</p> <p>(→2b) Zertifikat ist zeitlich nicht gültig, Fehlercode: 1021 (CERTIFICATE_NOT_VALID_TIME)</p> <p>(→2) Fehler im TLS Verbindungsaufbau bzw. Zertifikatsprüfung, Fehlercode: 4040</p> <p>(→4b) Fehler in SICCT INIT CT SESSION, Fehlercode: 4041 mit Angabe des SICCT-Fehlers</p> <p>(→5) Fehler in EHEALTH TERMINAL AUTHENTICATE, Fehlercode: 4041 mit Angabe des SICCT-Fehlers</p> <p>(→6) Signaturprüfung fehlgeschlagen, Fehlercode: 4041</p>

Zugehörige Diagramme	Siehe PIC_KON_057
----------------------	-------------------

2602 **Tabelle 35: TAB_KON_113 Fehlercodes TUC_KON_053 „Paire Kartenterminal“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4040	Security	Error	Fehler beim Versuch eines Verbindungsaufbaus zum KT
4041	Technical	Error	Fehler im Pairing, SICCT-Fehler ^(Nur wenn dieser Fehler wegen eines Fehlers auf der SICCT-Schnittstelle auftritt, ist der SICCT-Fehlercode mit anzugeben.) : <SICCT-Fehler>
4042	Technical	Error	Die Version des Kartenterminals wird nicht unterstützt

2603 Hinweis zu Fehler 4041:

2604 Nur wenn dieser Fehler wegen eines Fehlers auf der SICCT-Schnittstelle auftritt, ist der SICCT-

2605 Fehlercode mit anzugeben.

2606

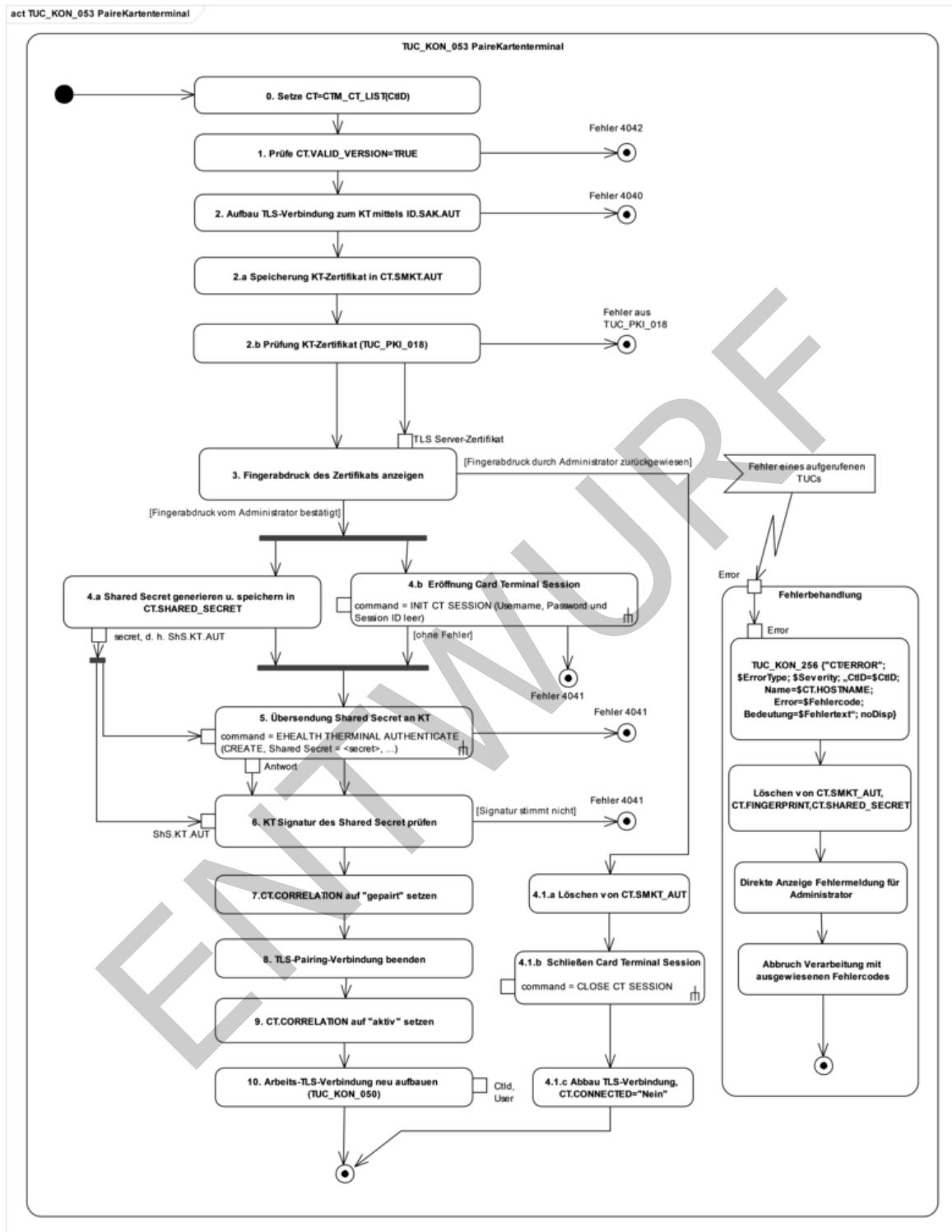


Abbildung 9: PIC_KON_057 Aktivitätsdiagramm zu „PaireKartterminal“

[<=]

- 2611 4.1.4.3.4 TUC_KON_055 „Befülle CT-Object“
- 2612 TIP1-A_4985 - TUC_KON_055 „Befülle CT-Object“
- 2613 Der Konnektor MUSS den technischen Use Case TUC_KON_055 „Befülle CT-Object“
- 2614 umsetzen.
- 2615

2616 **Tabelle 36: TAB_KON_526 – TUC_KON_055 „Befülle CT-Object“**

Element	Beschreibung
Name	TUC_KON_055 „Befülle CT-Object“
Beschreibung	Dieser TUC befüllt ein vorhandenes CT-Object aus CTM_CT_LIST mit den aktuellen Produktinformationen, die vom Kartenterminal bezogen werden und prüft, ob die Version des Kartenterminals unterstützt wird.
Auslöser	<ul style="list-style-type: none"> • TUC_KON_054 • Ereignis „KSR/UPDATE/END“ mit „Target=KT“ • Verändern von CT.CORRELATION auf „zugewiesen“ • Administratoraktion
Vorbedingungen	<ul style="list-style-type: none"> • ctId ist in CTM_CT_LIST vorhanden
Eingangsdaten	<ul style="list-style-type: none"> • ctId
Komponenten	Konnektor, Kartenterminal
Ausgangsdaten	<ul style="list-style-type: none"> • Supported (Boolean, True, wenn die Version des KT unterstützt wird)
Nachbedingungen	<ul style="list-style-type: none"> • Die Gerätekenndaten des Kartenterminals in CTM_CT_LIST sind aktualisiert
Standardablauf	<p>Setze CT = CTM_CT_LIST(ctId)</p> <ol style="list-style-type: none"> 1. Wenn CT.CONNECTED=Nein: Rufe TUC_KON_050 { ctId, role = „User“ } 2. Folgende CT.Werte via SICCT GET STATUS ermitteln und befüllen: <ul style="list-style-type: none"> • CT.SLOTCOUNT • CT.PRODUCTINFORMATION • CT.EHEALTH_INTERFACE_VERSION (Element VER aus Discretionary Data Data Object (DD DO)) • CT.DISPLAY_CAPABILITIES (aus Display Capabilities Data Object in [SICCT#5.5.10.17]) 3. Finde Eintrag in CTM_SUPPORTED_KT_VERSIONS anhand der ersten beiden Stellen (Haupt- und Nebenversionsnummer) aus CT.EHEALTH_INTERFACE_VERSION <p><u>Eintrag gefunden:</u> Die dritte Stelle der KT-Version ist im Vergleich zur dritten Stelle im gefundenen</p>

	<ul style="list-style-type: none"> • <i>displayMessage</i> – <i>optional/nicht erforderlich bei opmode= OutputErase, sonst mandatory</i> (Text zur Darstellung am KT, Länge durch KT begrenzt); • <i>opMode</i> [KtOutputMode] (Kommando-Modus) • <i>inputLength</i> – <i>optional/nur bei opMode=Input</i> (erwartete Eingabelänge, 0 für „beliebig“ lang) • <i>waitTimer</i> – <i>optional/nur bei opMode=OutputWait</i> (Wartezeit bis zur ersten Eingabe in Sekunden)
Komponenten	Konnektor, Kartenterminal
Ausgangsdaten	<ul style="list-style-type: none"> • <i>opResult</i> [OK ABBRUCH] – <i>optional/verpflichtend, wenn opMode=Input oder opMode=OutputConfirm</i> (Nutzertastendruck) • <i>inputData</i> – <i>optional/nur bei opMode = Input</i> (Zifferneingabe des Benutzers)
Nachbedingungen	Wenn Mode=OutputKeep bleibt Data auf dem Display des KT stehen
Standardablauf	<p>Setze CT = CTM_CT_LIST(ctId)</p> <ol style="list-style-type: none"> 1. <i>opMode=</i> <ol style="list-style-type: none"> a. <u>Input:</u> Der Konnektor MUSS via SICCT INPUT am CT zur Eingabe auffordern. Dabei MUSS die KT-Ansteuerung so erfolgen, dass: <ul style="list-style-type: none"> • <i>displayMessage</i> zur Anzeige gebracht wird • maximal <i>inputLength</i> Ziffern akzeptiert werden. Bei <i>inputLength=0</i> werden 1-n Zeichen akzeptiert (n=Maximalwert, definiert durch KT) • die eingegebenen Zeichen am Display angezeigt werden • die Eingabe explizit mit OK oder ABBRUCH beendet werden muss b. <u>OutputWait:</u> Der Konnektor MUSS via SICCT OUTPUT am CT <i>displayMessage</i> zur Anzeige bringen. Nach einer Wartezeit von <i>waitTimer</i> Sekunden MUSS der Konnektor die Anzeige des KT leeren. c. <u>OutputConfirm:</u> Der Konnektor MUSS via SICCT INPUT am CT <i>displayMessage</i> zur Anzeige bringen und auf eine Bestätigung durch den Nutzer warten (zulässig: OK, ABBRUCH) d. <u>OutputKeep:</u> Der Konnektor MUSS via SICCT OUTPUT am CT <i>displayMessage</i> zur Anzeige bringen. Die Anzeige

	bleibt erhalten, bis das KT neue Informationen am Display darstellen muss/soll. e. <u>OutputErase</u> : Der Konnektor MUSS via SICCT OUTPUT am CT die Anzeige leeren.
Varianten/ Alternativen	<ul style="list-style-type: none"> Ist das Kartenterminal-Display durch einen anderen, zeitgleich im Konnektor ablaufenden Vorgang reserviert, so muss der Konnektor zunächst maximal 10 Sekunden lang versuchen, Zugriff auf das Display zu erhalten (und somit parallele Zugriffe auf das Display zu serialisieren). Erst nach Ablauf der Wartezeit wird Fehler 4039 geworfen.
Fehlerfälle	Fehler in den folgenden Schritten des Ablaufs führen zum Aufruf von TUC_KON_256 { topic = "CT/ERROR"; eventType = \$ErrorType; severity = \$Severity; parameters = („CtID=\$ctId, Name=\$CT.HOSTNAME, Error=\$Fehlercode, Bedeutung=\$Fehlertext") } (→1) Display und PinPad des Kartenterminals sind aktuell belegt (PIN, Eingabe, andere Ausgabe etc.), Fehlercode: 4039 (→1) Kartenterminal antwortet mit einer spezifischen Fehlermeldung, Fehlercode <gemäß [SICCT]>
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 38: TAB_KON_114 Fehlercodes TUC_KON_051 „Mit Anwender über Kartenterminal interagieren“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4039	Technical	Error	Kartenterminal durch andere Nutzung aktuell belegt

[<=]

4.1.4.4.2 TUC_KON_056 „Karte anfordern“

TIP1-A_5409 - TUC_KON_056 „Karte anfordern“

Der Konnektor MUSS den technischen Use Case „Karte anfordern“ gemäß TUC_KON_056 umsetzen.

2636 **Tabelle 39: TAB_KON_723 - TUC_KON_056 „Karte anfordern“**

Element	Beschreibung
Name	TUC_KON_056 „Karte anfordern“
Beschreibung	Der TUC ermöglicht es, die Aufforderung zum Karte-Stecken an das Kartenterminal zu senden und dabei eine Meldung zum Anzeigen im Display des Kartenterminals mitzugeben.
Auslöser	Fachmodul im Konnektor oder Operation RequestCard ruft diesen Use Case auf.
Vorbedingungen	
Eingangsdaten	<ul style="list-style-type: none"> - ctId (Kartenterminalidentifikator) - slotId (Nummer des Kartenslots) - cardType - <i>optional</i> - displayMessage - <i>optional</i> (Text zur Darstellung am Kartenterminal, Länge durch KT begrenzt) - timeOut (Wartezeit in Sekunden)
Komponenten	Konnektor, Kartenterminal
Ausgangsdaten	<ul style="list-style-type: none"> • cardObject (Informationsobjekt der Karte)
Nachbedingungen	Im Erfolgsfall enthält die CM_CARD_LIST ein neues CARD-Objekt des geforderten Typs.
Standardablauf	<p>Setze CT = CTM_CT_LIST(ctId)</p> <ol style="list-style-type: none"> 1. Falls displayMessage nicht explizit angegeben ist, MUSS sie gemäß Anforderung [TIP1-A_5408] erstellt werden. 2. Der Konnektor MUSS das Kommando SICCT REQUEST ICC an das Kartenterminal CT senden. Die verfügbaren Optionen (Optical Signal, Acoustic Signal) können herstellerspezifisch sein bzw. über die Konfigurationsschnittstelle des Konnektors eingestellt werden. displayMessage wird als Eingabeaufforderung mitgegeben. Der übergebene timeOut-Wert wird dem SICCT-Kommando als Parameter übergeben.

	<p>3. Falls die Karte noch nicht gesteckt war, wird durch das Stecken der Karte das Ereignis „Karte gesteckt“ ausgelöst, worauf der Konnektor reagiert [TIP1-A_4563].</p> <p>4. Die Verarbeitung wird fortgesetzt, wenn eines der Ereignisse eingetreten ist:</p> <ul style="list-style-type: none"> a. SICCT REQUEST ICC kehrt mit '6201' zurück (eine aktivierte Karte steckte bereits) b. SICCT REQUEST ICC kehrt mit '9000' oder '9001' zurück und das Ereignis "Karte gesteckt" wurde gemäß [TIP1-A_4563] verarbeitet c. SICCT REQUEST ICC kehrt mit '9000' oder '9001' zurück und das Ereignis "Karte gesteckt" wurde nicht empfangen (eine deaktivierte Karte steckte bereits), die Karte wurde durch Rufe TUC_KON_001 { ctId; slotId } geöffnet. <p>In allen Fällen liegt in CM_CARD_LIST ein neues CARD-Objekt vor.</p> <p>5. Falls cardType angegeben ist, wird nach erfolgreicher Ausführung von SICCT REQUEST ICC der AID des MF der gesteckten Karte gelesen und mit dem gewünschten Kartentyp in cardType verglichen. Bei fehlender Übereinstimmung wird der Ablauf mit dem Fehler 4051 abgebrochen.</p> <p>6. Es wird cardObject (ein Informationsobjekt der Karte, die sich in dem Slot mit der Nummer slotId befindet) zurückgegeben.</p>
Varianten/ Alternativen	Die Ausgabe einer Display-Nachricht entfällt, wenn der adressierte Slot bereits eine gesteckte Karte enthält.
Fehlerfälle	<p>Fehler in den folgenden Schritten des Ablaufs führen zu Aufruf von TUC_KON_256 { topic = "CT/ERROR"; eventType = \$ErrorType; severity = \$Severity; parameters = („CtID=\$ctId, Name=\$CT.HOSTNAME, Error=\$Fehlercode, Bedeutung=\$Fehlertext“) }</p> <p>(→2) Display des Kartenterminals ist aktuell belegt, Fehlercode: 4039 (→2) Fehler beim Zugriff auf das Kartenterminal, Fehlercode: 4044 (→2) Ungültige Kartenterminal-ID: Fehlercode: 4007 (→2) Ungültige Kartenslot-ID: Fehlercode: 4097 (→2) Kartenterminal nicht aktiv, Fehlercode: 4221 (→2) Kartenterminal ist nicht verbunden, Fehlercode: 4222 (→2) Kartenterminal antwortet mit einer spezifischen</p>

	Fehlermeldung, Fehlercode <gemäß [SICCT]> (→4) Timeout. Es wurde keine Karte innerhalb der angegebenen Zeitspanne gesteckt, Fehlercode: 4202 (→5) Falscher Kartentyp, Fehlercode: 4051
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

2637 **Tabelle 40: TAB_KON_724 Fehlercodes TUC_KON_056 „Karte anfordern“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4039	Technical	Error	Kartenterminal durch andere Nutzung aktuell belegt
4044	Technical	Error	Fehler beim Zugriff auf das Kartenterminal
4051	Technical	Error	Falscher Kartentyp
4007	Technical	Error	Ungültige Kartenterminal-ID
4097	Technical	Error	Ungültige Kartenslot-ID
4202	Technical	Error	Timeout. Es wurde keine Karte innerhalb der angegebenen Zeitspanne gesteckt.
4221	Technical	Error	Kartenterminal nicht aktiv
4222	Technical	Error	Kartenterminal ist nicht verbunden

2638
2639 **[<=]**

2640 **4.1.4.4.3 TUC_KON_057 „Karte auswerfen“**

2641 TIP1-A_5410 - TUC_KON_057 „Karte auswerfen“

2642 Der Konnektor MUSS den technischen Use Case „Karte auswerfen“ gemäß TUC_KON_057
2643 umsetzen.

2644
2645 **Tabelle 41: TAB_KON_725 – TUC_KON_057 „Karte auswerfen“**

Element	Beschreibung
Name	TUC_KON_057 „Karte auswerfen“
Beschreibung	Der TUC ermöglicht es, das SICCT-Kommando zum Auswerfen der Karte an das Kartenterminal zu senden und dabei eine Meldung zum Anzeigen im Display des Kartenterminals

	mitzugeben, die den Benutzer zum Entnehmen der Karte auffordert.
Auslöser	Fachmodul im Konnektor oder Operation EjectCard ruft diesen Use Case auf.
Vorbedingungen	
Eingangsdaten	<ul style="list-style-type: none"> • ctId (Kartenterminalidentifikator) • slotId (Nummer des Kartenslots) • displayMessage – <i>optional</i> (Text zur Darstellung am Kartenterminal, Länge durch KT begrenzt) • timeOut (Wartezeit in Sekunden)
Komponenten	Konnektor, Kartenterminal
Ausgangsdaten	keine
Nachbedingungen	Durch das Entfernen der Karte wird das Ereignis „Karte entfernt“ ausgelöst, worauf der Konnektor reagiert [TIP1-A_4562].
Standardablauf	<p>Setze CT = CTM_CT_LIST(ctId)</p> <ol style="list-style-type: none"> 1. Der Konnektor prüft, dass entweder die Karte nicht reserviert ist oder der Aufrufer im Besitz des Karten-Locks ist. 2. Falls displayMessage nicht explizit angegeben ist, MUSS sie gemäß Anforderung [TIP1-A_5408] erstellt werden. 3. Der Konnektor MUSS das Kommando SICCT EJECT ICC an das Kartenterminal CT senden. Der Aufruf MUSS mit der Option „Delivery: Mechanical Throwout“ erfolgen. Die anderen Optionen (Optical Signal, Acoustic Signal) können herstellerspezifisch eingestellt werden bzw. können über die Konfigurationsschnittstelle des Konnektors eingestellt werden. Der übergebene Wert timeOut wird dem SICCT-Kommando als Parameter übergeben.
Varianten/ Alternativen	Auch im Falle, dass nach der internen Buchführung des Konnektors in dem angegebenen Slot des Kartenterminals keine Karte steckt, MUSS der Konnektor das SICCT-Kommando SICCT EJECT ICC an das Kartenterminal senden. Meldet das Kartenterminal keinen Fehler, so meldet auch der Konnektor keinen Fehler und es kann davon ausgegangen werden, dass sich keine Karte mehr in dem Slot befindet.
Fehlerfälle	Fehler in den folgenden Schritten des Ablaufs führen zu Aufruf von TUC_KON_256 { topic = "CT/ERROR"; eventType = \$ErrorType;

	<pre>severity = \$Severity; parameters = („CtID=\$CtID, Name=\$CT.HOSTNAME, Error=\$Fehlercode, Bedeutung=\$Fehlertext“) }</pre> <p>(→1) Die Karte ist fremdreserviert, Fehlercode 4093 (→3) Display des Kartenterminals ist aktuell belegt, Fehlercode: 4039 (→3) Fehler beim Zugriff auf das Kartenterminal, Fehlercode: 4044 (→3) Karte deaktiviert, aber nicht entnommen, Fehlercode: 4203 (→3) Ungültige Kartenterminal-ID: Fehlercode: 4007 (→3) Ungültige Kartenslot-ID: Fehlercode: 4097 (→3) Kartenterminal nicht aktiv, Fehlercode: 4221 (→3) Kartenterminal ist nicht verbunden, Fehlercode: 4222 (→3) Kartenterminal antwortet mit einer spezifischen Fehlermeldung, Fehlercode <gemäß [SICCT]></p>
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

2646 **Tabelle 42: TAB_KON_796 Fehlercodes TUC_KON_057 „Karte auswerfen“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4039	Technical	Error	Kartenterminal durch andere Nutzung aktuell belegt
4044	Technical	Error	Fehler beim Zugriff auf das Kartenterminal
4203	Technical	Error	Karte deaktiviert, aber nicht entnommen
4093	Technical	Error	Karte wird in einer anderen Kartensitzung exklusiv verwendet
4007	Technical	Error	Ungültige Kartenterminal-ID
4097	Technical	Error	Ungültige Kartenslot-ID
4221	Technical	Error	Kartenterminal nicht aktiv
4222	Technical	Error	Kartenterminal ist nicht verbunden

2647
2648 **[<=]**

2649 **4.1.4.4.4 TUC_KON_058 „Displaygröße ermitteln“**

2650 **A_17473 - TUC_KON_058 „Displaygröße ermitteln“**

2651 Der Konnektor MUSS den technischen Use Case „Displaygröße ermitteln“ gemäß
2652 TUC_KON_058 umsetzen.

2653

Tabelle 43: TAB_KON_854 – TUC_KON_058 „Displaygröße ermitteln“

Element	Beschreibung
Name	TUC_KON_058 „Displaygröße ermitteln“
Beschreibung	Der TUC liefert den Inhalt der Variable CT.DISPLAY_CAPABILITIES zurück.
Auslöser	Fachmodul im Konnektor ruft diesen Use Case auf.
Vorbedingungen	
Eingangsdaten	<ul style="list-style-type: none"> ctId (Kartenterminalidentifikator)
Komponenten	Konnektor
Ausgangsdaten	CT.DISPLAY_CAPABILITIES
Nachbedingungen	Keine
Standardablauf	Setze CT = CTM_CT_LIST(ctId) <ol style="list-style-type: none"> Der Konnektor prüft, ob CT.DISPLAY_CAPABILITIES belegt ist. Falls CT.DISPLAY_CAPABILITIES belegt ist, wird der Inhalt der Variable zurückgegeben.
Varianten/ Alternativen	Keine
Fehlerfälle	Fehler in den folgenden Schritten des Ablaufs führen zu Aufruf von TUC_KON_256 { <pre> topic = "CT/ERROR"; eventType = \$ErrorType; severity = \$Severity; parameters = („CtID=\$CtID, Name=\$CT.HOSTNAME, Error=\$Fehlercode, Bedeutung=\$Fehlertext") } (→2) CT.DISPLAY_CAPABILITIES ist nicht belegt, Fehlercode 4254 </pre>
Nichtfunktionale Anforderungen	Keine

Zugehörige Diagramme	Keine
----------------------	-------

2654 **Tabelle 44: TAB_KON_855 Fehlercodes TUC_KON_058 „Displaygröße ermitteln“**

Fehlercode	ErrorType	Severity	Fehlertext
4254	Technical	Error	Keine Displaygröße für das Kartenterminal definiert

2655
2656
2657

[<=]

2658 4.1.4.5 Operationen an der Außenschnittstelle

2659 TIP1-A_5411 - Basisdienst Kartenterminaldienst

2660 Der Konnektor MUSS Clientsystemen den Basisdienst Kartenterminaldienst anbieten.

2661

2662 **Tabelle 45: TAB_KON_722 Basisdienst Kartenterminaldienst**

Name	CardTerminalService	
Version (KDV)	Siehe Anhang D (WSDL-Version)	
Namensraum	Siehe Anhang D	
Namensraum-Kürzel	CT für Schema und CTW für WSDL	
Operationen	Name	Kurzbeschreibung
	RequestCard	Karte anfordern
	EjectCard	Karte auswerfen
WSDL	CardTerminalService.wsdl	
Schema	CardTerminalService.xsd	

2663
2664

[<=]

2665 4.1.4.5.1 RequestCard

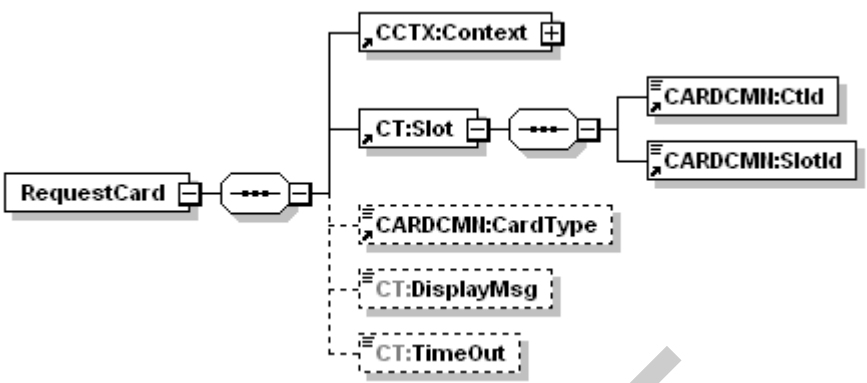
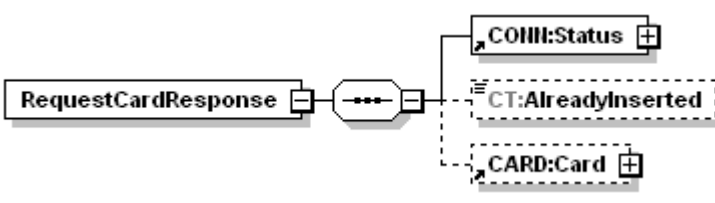
2666 TIP1-A_5412 - Operation RequestCard

2667 Der Konnektor MUSS an der Außenschnittstelle eine Operation RequestCard, wie in
2668 Tabelle TAB_KON_716 Operation RequestCard beschrieben, anbieten.

2669

2670 **Tabelle 46: TAB_KON_716 Operation RequestCard**

Name	RequestCard
Beschreibung	Liefert die Information zu einer Karte, die in dem Slot eines Kartenterminals steckt oder innerhalb einer bestimmten Zeit (Timeout) gesteckt wird.

Aufruf- parameter		
	Name	Beschreibung
	CCTX:Context	MandantId, CsId, WorkplaceId verpflichtend
	CT:Slot	Adressiert den Slot eines Kartenterminals über die Identifikation des Kartenterminal CARDCMN:CtId und die Nummer des Slots CARDCMN:SlotId
	CARDCMN:CardType	Ein Kartentyp aus {EGK, KVK, HBAX, SM-B} als optionaler Filter. Wenn angegeben, werden nur Karten vom spezifizierten Typ zurückgegeben.
	CT:DisplayMsg	Diese Nachricht wird am Display des Kartenterminals angezeigt, um den Nutzer zum Stecken der Karte aufzufordern.
	CT:TimeOut	Die Zeit in sec, die maximal gewartet wird bis zum Stecken einer Karte. Wird dieser Parameter nicht übergeben, SOLL der Konnektor den Wert 20 sec verwenden. Optional KANN dieser Default-Wert im Konnektor konfigurierbar sein.
Rückgabe		
	Name	Beschreibung
	CONN:Status	Enthält den Ausführungsstatus der Operation (siehe 3.5.2)
	CT:AlreadyInserted	Dieses optionale Flag gibt an, ob die Karte bereits vor der Anfrage steckte (Wert true) oder erst auf Anforderung dieses Aufrufs gesteckt wurde (Wert false oder Element nicht vorhanden).

	CARD:Card	Falls eine Karte gesteckt ist, werden Information zur Karte zurückgegeben (siehe 4.1.6.5.2)
Vorbedingung	keine	
Nachbedingung	keine	

2671 Der Ablauf der Operation RequestCard ist in Tabelle TAB_KON_717 Ablauf RequestCard
 2672 beschrieben.
 2673

2674 **Tabelle 47: TAB_KON_717 Ablauf RequestCard**

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab. Wird die Operation für einen nicht unterstützten Kartentypen aufgerufen, so bricht die Operation mit Fehler 4058 ab.
2.	TUC_KON_000 „Prüfe Zugriffs- berechtigung“	Prüfung der Zugriffsberechtigung durch den Aufruf TUC_KON_000 { mandantId = \$context.mandantId; clientSystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; ctId = \$Slot.CtId; needCardSession=false; allWorkplaces=false } Tritt bei der Prüfung ein Fehler auf, so bricht die Operation mit dem Fehlercode aus TUC_KON_000 ab.
3.	TUC_KON_056 „Karte anfordern“	Anforderung der Karte vom Kartenterminal durch Aufruf TUC_KON_056(ctId = \$Slot.CtId; slotId = \$Slot.SlotId; \$cardType; displayMessage = \$DisplayMsg; \$timeout)

2675 **Tabelle 48: TAB_KON_718 Fehlercodes „RequestCard“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler
4058	Security	Error	Aufruf nicht zulässig

2676
2677
2678 [\leq]

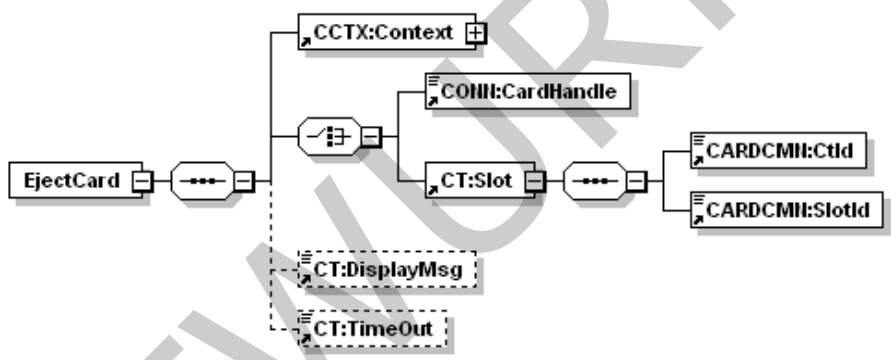
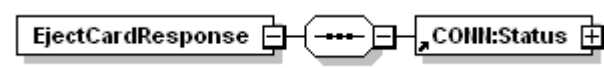
2679 4.1.4.5.2 EjectCard

2680 TIP1-A_5413 - Operation EjectCard

2681 Der Konnektor MUSS an der Außenschnittstelle eine Operation EjectCard, wie in Tabelle
2682 TAB_KON_719 Operation EjectCard beschrieben, anbieten.

2683

2684 **Tabelle 49: TAB_KON_719 Operation EjectCard**

Name	EjectCard	
Beschreibung	Beendet die Kommunikation mit der Karte und wirft sie aus, falls das Kartenterminal eine solche mechanische Funktion hat.	
Aufruf- parameter		
	Name	Beschreibung
	Context	MandantId, CsId, WorkplaceId verpflichtend
	CONN: CardHandle	Adressiert die Karte, die ausgeworfen werden soll.
	CT:Slot	Adressiert alternativ den Slot eines Kartenterminals, aus dem die Karte ausgeworfen werden soll. Die Adressierung erfolgt über die Identifikation des Kartenterminal <code>CARDCMN:CtId</code> und die Nummer des Slots <code>CARDCMN:SlotId</code> .
	CT: DisplayMsg	Diese Nachricht wird am Display des Kartenterminals angezeigt, um den Nutzer zum entnehmen der Karte aufzufordern.
	CT:TimeOut	Die Zeit in msec, die maximal gewartet wird bis eine Karte gezogen ist. Wird dieser Parameter nicht übergeben, SOLL der Konnektor den Wert 20 sec verwenden. Optional KANN dieser Default-Wert im Konnektor konfigurierbar sein.
Rückgabe		

	Name	Beschreibung
	Status	Enthält den Ausführungsstatus der Operation (siehe 3.5.2)
Vorbedingung	keine.	
Nachbedingung	keine.	

Der Ablauf der Operation EjectCard ist in Tabelle TAB_KON_720 Ablauf EjectCard beschrieben.

Tabelle 50: TAB_KON_720 Ablauf EjectCard

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	TUC_KON_000 „Prüfe Zugriffsberechtigung“	<p>Ist \$cardHandle vorgegeben, so wird \$ctId als Id des Kartenterminals bestimmt, in dem die Karte steckt. Prüfung der Zugriffsberechtigung durch den Aufruf TUC_KON_000 {</p> <pre> mandantId = \$Context.MandantId; clientSystemId = \$Context.ClientSystemId; workplaceId = \$Context.WorkplaceId; ctId = \$Slot.CtId bzw. ctId = CM_CARD_LIST(\$CardHandle).CTID; needCardSession = false; allWorkplaces = false } </pre> <p>Tritt bei der Prüfung ein Fehler auf, bricht die Operation mit Fehlercode aus TUC_KON_000 ab.</p>
3.	TUC_KON_057 „Karte auswerfen“	<p>Wurde EjectCard mit dem Parameter Slot aufgerufen: Veranlassen des Kartenauswurfs am Kartenterminal durch Aufruf TUC_KON_057 {</p> <pre> ctId = \$Slot.CtId; slotId = \$Slot.Slotid; displayMessage = \$DisplayMsg; \$timeOut } </pre> <p>Wurde EjectCard mit dem Parameter CardHandle aufgerufen: Veranlassen des Kartenauswurfs am Kartenterminal durch Aufruf TUC_KON_057 {</p> <pre> ctId = CM_CARD_LIST(\$CardHandle).CTID; slotId = CM_CARD_LIST(\$CardHandle).SLOTNO; ; displayMessage = \$DisplayMsg; \$timeOut } </pre>

2689 **Tabelle 51: TAB_KON_721 Fehlercodes Operation „EjectCard“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler
4203	Technical	Error	Karte deaktiviert, aber nicht entnommen
4101	Technical	Error	Karten-Handle ungültig

2690
2691
2692

[<=]

2693 4.1.4.6 Betriebsaspekte

2694 4.1.4.6.1 Allgemeine Betriebsaspekte

2695 TIP1-A_4549 - Initialisierung Kartenterminaldienst

2696 Während des Bootvorgangs, nach dem Einlesen der persistierten Informationen des
2697 Kartenterminaldienstes MUSS der Konnektor für jedes Kartenterminal CT in
2698 CTM_CT_LIST:

- 2699 • die zugehörigen Attribute CT.SLOTS_USED, CT.VALID_VERSION und ggf. (bei
2700 dynamischer Adressvergabe) CT.IP_ADRESS aktualisieren
- 2701 • für jedes CT mit CT.CORRELATION = „aktiv“:
 - 2702 • Wenn CT.VALID_VERSION = True: TUC_KON_050 „Beginne
2703 Kartenterminalsitzung“ {ctId=CT.CtID; role=„User“} aufrufen
 - 2704 • Wenn CT.VALID_VERSION = False: CT.CORRELATION=„gepairt“
2705 setzen

2706 [≤]

2707 Hinweis: Bei der Initialisierung des Kartenterminaldienstes liest der Konnektor noch nicht
2708 die Karten, um zu ermitteln, welche Karten gesteckt sind. Dies erfolgt erst bei
2709 Initialisierung des Kartendienstes.

2710 TIP1-A_4550 - Konfigurationsparameter des Kartenterminaldienstes

2711 Die Managementschnittstelle MUSS es einem Administrator ermöglichen
2712 Konfigurationsänderungen gemäß Tabelle TAB_KON_527 vorzunehmen:
2713

2714 **Tabelle 52: TAB_KON_527 Konfigurationswerte eines Kartenterminalobjekts**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
CTM_SERVICE_DISCO VERY_PORT	Portnummer	Der Administrator MUSS die Portnummer eingeben können, auf der die KTs im lokalen Netz auf Dienstanfragen hören. Default-Wert=4742

CTM_SERVICE_DISCOVERY_TIMEOUT	X Sekunden	Der Administrator MUSS die Anzahl Sekunden eingeben können, die der Konnektor auf Antworten zu Service-Discovery-Anfragen wartet. Default-Wert=3
CTM_SERVICE_ANNOUNCEMENT_PORT	Portnummer	Der Administrator MUSS die Portnummer eingeben können, auf der der Konnektor auf Dienstbeschreibungspakete hört. Default-Wert=4742
CTM_SERVICE_DISCOVERY_CYCLE	X Minuten	Der Administrator MUSS die Anzahl Minuten einstellen können, in denen der Konnektor wiederholt Service Discovery Nachrichten absetzt. Default-Wert=10, 0=Deaktiviert
CTM_KEEP_ALIVE_INTERVAL	X Sekunden	Intervall in Sekunden in den Keep-Alive-Nachrichten an das Kartenterminal gesendet werden Der Administrator MUSS diesen Wert im vorgegebenen Bereich anpassen können. Wertebereich: 1-10 Default-Wert=10
CTM_KEEP_ALIVE_TRY_COUNT	Anzahl der Versuche	Anzahl von aufeinander folgenden, nicht beantworteten Keep-Alive-Nachrichten, nach denen ein Timeout der TLS-Verbindung festgestellt wird Der Administrator MUSS diesen Wert im vorgegebenen Bereich anpassen können. Wertebereich: 3-10 Default-Wert=3
CTM_TLS_HS_TIMEOUT	X Sekunden	Der Administrator MUSS die Anzahl Sekunden eingeben können, die der Konnektor auf den TLS-Verbindungsaufbau zum Kartenterminal wartet (Handshake-Timeout). Wertebereich: 1-60 Default-Wert=10

2715
2716

[<=]

2717 TIP1-A_4986 - Informationsparameter des Kartenterminaldienstes
2718 Die Managementschnittstelle MUSS es einem Administrator ermöglichen die
2719 Informationsparameter gemäß Tabelle TAB_KON_528 einzusehen:
2720

2721 **Tabelle 53: TAB_KON_528 Informationsparameter des Kartenterminaldienstes**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
CTM_SUPPORTED_KT_VERSIONS	Liste von EHEALTH-	Der Administrator MUSS die Liste der vom Konnektor unterstützten modellunabhängigen

	Interface-Versionen	EHEALTH-Interface-Versionen einsehen können.
--	---------------------	--

2722

2723 [**<=**]2724 **4.1.4.6.2 Kartenterminals pflegen**

2725 Im Folgenden werden die Administratorinteraktionen beschrieben, die zum Hinzufügen,
 2726 Pairen, Bearbeiten und Löschen von Kartenterminals innerhalb der CTM_CT_LIST
 2727 angeboten werden müssen. Eine Aktualisierung der Kartenterminals mit neuer Firmware
 2728 wird in Kapitel 4.3.9 beschrieben.

2729 TIP1-A_4551 - Einsichtnahme von Kartenterminaleinträgen

2730 Die Managementschnittstelle MUSS es einem Administrator ermöglichen die Liste der
 2731 verwalteten und neu entdeckten Kartenterminals einzusehen (CTM_CT_LIST).

2732 [**<=**]

2733 TIP1-A_4552 - Manueller Verbindungsversuch zu Kartenterminals

2734 Die Managementschnittstelle MUSS es einem Administrator ermöglichen zu jedem CT-
 2735 Object-Eintrag in CTM_CT_LIST mit CT.CONNECTED=Nein und CT.CORRELATION=aktiv
 2736 einen manuellen Verbindungsaufbau über TUC_KON_050 {ctId=CtID; role=„User“}
 2737 auszulösen.

2738 [**<=**]

2739 TIP1-A_4553 - Einsichtnahme in und Aktualisierung der Kartenterminaleinträge

2740 Die Managementschnittstelle MUSS es einem Administrator ermöglichen zu jedem CT-
 2741 Object-Eintrag in CTM_CT_LIST die Werte gemäß Tabelle TAB_KON_529 einsehen zu
 2742 können:

2743 Zu jedem Eintrag MUSS der Administrator TUC_KON_055 „Befülle CT-Object“ auslösen
 2744 können.

2745

2746 **Tabelle 54: TAB_KON_529 Anzeigewerte zu einem Kartenterminalobjekt**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
Geräte kenndaten		
CT.CTID	Identifizier	Eindeutige, statische Identifikation des Kartenterminals
CT.IS_PHYSICAL	Ja/Nein	Kennzeichnung, ob es sich um ein logisches oder physisches Kartenterminal handelt (siehe auch TAB_KON_522 Parameterübersicht des Kartenterminaldienstes)
CT.MAC_ADRESS	MAC-Adresse	die MAC-Adresse des Kartenterminals
CT.HOSTNAME	String	SICCT-Terminalname des Kartenterminals, auch als FriendlyName bezeichnet
CT.IP_ADRESS	IP-Adresse	die IP-Adresse des Kartenterminals
CT.TCP_PORT	Portnummer	der TCP-Port des SICCT-Kommandointerpreters des Kartenterminals

CT.SLOTCOUNT	Nummer	Anzahl der Slots des Kartenterminals
CT.SLOTS_USED	Liste	Liste der mit Karten belegten Slots
CT.PRODUCT INFORMATION	Inhalt Product Information.xsd	die Herstellerinformationen zum Kartenterminal gemäß [gemSpec_OM]
CT.EHEALTH_ INTERFACE_ VERSION	Version	Die EHEALTH-Interface-Version des Kartenterminals, die mittels des SICCT- Kommandos GET STATUS aus dem Element VER des Discretionary Data Objects ermittelt wurde
CT.VALID_ VERSION	Boolean	True, wenn die Version des Kartenterminals (CT.EHEALTH_INTERFACE_VERSION) durch den Konnektor unterstützt wird, d.h. zu den in CTM_SUPPORTED_KT_VERSIONS passt
Pairingdaten		
CT.SMKT_AUT	X.509-Cert	C.SMKT.AUT-Zertifikat des Kartenterminals, gespeichert im Rahmen des Pairings
Verbindungs daten		
CT. CORRELATION	bekannt zugewiesen gepairt aktiv aktualisierend	Der Korrelationsstatus zum Konnektor: <ul style="list-style-type: none"> • bekannt (über Service Announcement/Service Discovery gelernte Kartenterminals), • zugewiesen (durch den Administrator aus dem Bereich der bekannten Kartenterminals oder manuell konfigurierte Kartenterminals), • gepairt (Pairing erfolgreich aber noch nicht zum Verbindungsaufbau freigegeben) • aktiv (durch Administrator zum Verbindungsaufbau freigegeben), • aktualisierend (ein laufender Updatevorgang, ausgelöst durch den Konnektor; Der Zustand tritt ein, wenn der Kartenterminaldienst das Event „KSR/UPDATE/START“ fängt und endet mit dem Event „KSR/UPDATE/END“),
CT.CONNECTED	Ja/Nein	Der Verfügbarkeitsstatus des Kartenterminals (Ja = nach Aufbau der TLS- Verbindung und erfolgter zweiter Authentifizierung)
CT.ACTIVEROLE	User/Admin	Benutzerrolle, die für die aktuelle Session verwendet wird

KT-Admin-Credentials		
CT.ADMIN_USERNAME	String	Username des Administrators am KT

2747
2748

[<=]

2749 TIP1-A_4554 - Bearbeitung von Kartenterminaleinträgen
 2750 Die Managementschnittstelle MUSS es einem Administrator ermöglichen zu jedem CT-
 2751 Object-Eintrag in CTM_CT_LIST die Werte gemäß Tabelle TAB_KON_530 ändern zu
 2752 können:
 2753 Zur Überprüfung der veränderten Parameter auf Korrektheit MUSS nach Änderung von
 2754 CT.IP_ADRESS, TCP_PORT oder HOSTNAME TUC_KON_054 mit Mode= ManuallyModified
 2755 und allen vorhandenen CT-Parametern aufgerufen werden. Endet der Aufruf von
 2756 TUC_KON_054 mit einem Fehler, MUSS der Konnektor die geänderten
 2757 Konfigurationswerte auf ihren Ausgangswert zurücksetzen.
 2758

2759 **Tabelle 55: TAB_KON_530 Konfigurationswerte eines Kartenterminalobjekts**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
CT.IP_ADRESS	IP-Adresse	Der Administrator MUSS für KTs mit CT.IS_PHYSICAL=Ja die IPv4-Adresse des Kartenterminals eingeben können.
CT.TCP_PORT	Portnummer	Der Administrator MUSS für KTs mit CT.IS_PHYSICAL=Ja den TCP-Port des SICCT-Kommandointerpreters des Kartenterminals eingeben können.
CT.HOSTNAME	String	Der Administrator MUSS den SICCT-Terminalnamen (Hostname) - auch als FriendlyName bezeichnet - des Kartenterminals eingeben können.
CT.ADMIN_USERNAME	String	Der Administrator MUSS für KTs mit CT.IS_PHYSICAL=Ja den Username des KT-Administrators des Kartenterminals eingeben können.
CT.ADMIN_PASSWORD	String	Der Administrator MUSS für KTs mit CT.IS_PHYSICAL=Ja das Password des KT-Administrators des Kartenterminals eingeben können.

2760
2761

[<=]

2762 TIP1-A_6477 - Manuelles Service Discovery
 2763 Die Managementschnittstelle MUSS es einem Administrator ermöglichen, ein Service
 2764 Discovery entsprechend [SICCT] auszulösen, um neue Kartenterminals hinzuzufügen.
 2765 **[<=]**

2766 TIP1-A_4555 - Manuelles Hinzufügen eines Kartenterminals
 2767 Die Managementschnittstelle MUSS es einem Administrator ermöglichen für neue
 2768 Kartenterminals CT-Objects manuell in CTM_CT_LIST aufzunehmen.

- 2769 Hierzu MUSS der Administrator für das neue Kartenterminal folgende Werte eingeben
2770 können:
- 2771 • IP-Adresse (Eingabe verpflichtend)
 - 2772 • TCP-Port (Eingabe optional)
 - 2773 • MAC-Adresse (Eingabe optional)
 - 2774 • Hostname (Eingabe optional)
- 2775 Bestätigt der Administrator seine Eingaben, MUSS TUC_KON_054 mit
2776 Mode=ManuallyAdded und allen eingegebenen Parametern aufgerufen werden.
2777 [**<=**]
- 2778 Als Sicherung gegen den unbemerkten Austausch von Kartenterminals oder deren
2779 Identitäten wird das gSMC-KT über den Konnektor logisch an das eHealth-Kartenterminal
2780 gebunden. Dieser Vorgang wird als Pairing von Kartenterminal und gSMC-KT bezeichnet
2781 und ist ausführlich in [gemSpec_KT] beschrieben.
- 2782 TIP1-A_4556 - Pairing mit Kartenterminal durchführen
2783 Die Managementschnittstelle MUSS es einem Administrator ermöglichen alle
2784 Kartenterminals mit CT.CORRELATION = „zugewiesen“ in einer Liste einzusehen und für
2785 einen ausgewählten Eintrag mit CT.VALID_VERSION=True TUC_KON_053 auslösen zu
2786 können.
2787 [**<=**]
- 2788 TIP1-A_4557 - Ändern der Korrelationswerte eines Kartenterminals
2789 Die Managementschnittstelle MUSS es einem Administrator ermöglichen zu einem
2790 Kartenterminal aus CTM_CT_LIST für KT's mit CT.IS_PHYSICAL=Ja den Wert für
2791 CT.CORRELATION nach folgenden Mustern zu ändern:
- 2792 • CT.CORRELATION = „bekannt“
2793 Das Kartenterminal gilt als nicht durch den Konnektor verwaltet.
 - 2794 • → „zugewiesen“:
2795 Ein (per Service Announcement entdecktes) Kartenterminal dem Konnektor
2796 zuweisen.
2797 Folgende Schritte MUSS der Konnektor für diesen Zustandswechsel zuvor
2798 erfolgreich durchlaufen:
2799 - Rufe TUC_KON_055 „Befülle CT-Object“
2800 - Prüfen, ob CT.HOSTNAME bereits für ein anderes
2801 Kartenterminal in CTM_CT_LIST verwendet wird. Wenn ja
2802 MUSS dieser Änderungsversuch fehlschlagen (Prinzip der
2803 Eindeutigkeit verletzt). Der Administrator MUSS eine
2804 entsprechende Fehlermeldung erhalten.
 - 2805 • CT.CORRELATION = „zugewiesen“
2806 Das Kartenterminal gilt als durch den Konnektor verwaltet.
 - 2807 • → „bekannt“
 - 2808 • → „gepairt“:
2809 Das Pairing wurde erfolgreich durchgeführt; die Werte
2810 CT.SMKT_AUT, CT.SHARED_SECRET sind im CT-Objekt
2811 eingetragen.
 - 2812 • CT.CORRELATION = „gepairt“
2813 Verbundenheit zwischen Kartenterminal und gesteckter gSMC-KT wurde
2814 nachgewiesen

- 2815 • → „zugewiesen“:
- 2816 Die Werte CT.SMKT_AUT, CT.SHARED_SECRET werden gelöscht
- 2817 • → „aktiv“:
- 2818 Wechsel nur möglich, wenn CT.VALID_VERSION=True. Dann Aufruf
- 2819 von TUC_KON_050 „Beginne Kartenterminalsitzung“ {ctId=CT.CtID;
- 2820 role=„User“}
- 2821 • CT.CORRELATION = „aktiv“
- 2822 Das Kartenterminal kann fachlich genutzt werden
- 2823 • → „gepairt“:
- 2824 Eventuelle TLS-Verbindung wird beendet, CT.CONNECTED auf Nein
- 2825 gesetzt.

2826 [**<=**]

2827 TIP1-A_5698 - Löschen von Kartenterminaleinträgen
 2828 Die Managementschnittstelle MUSS einem Administrator die Möglichkeit bieten,
 2829 Kartenterminals aus der Liste der Kartenterminals (CTM_CT_LIST) zu entfernen.
 2830 [**<=**]

2831 4.1.4.6.3 Import der Kartenterminal-Informationen

2832 Im Rahmen des Konnektormanagements müssen die Konfigurationsdaten des Konnektors
 2833 ex- und importiert werden können (siehe Kapitel 4.3.3). Eine Sonderstellung nimmt
 2834 dabei der Import von Kartenterminalinformationen ein, da hier im Rahmen des Imports
 2835 folgende Interaktion mit dem Administrator erforderlich ist:

2836

2837 TIP1-A_5011 - Import von Kartenterminal-Informationen
 2838 Der Konnektor MUSS vor der endgültigen Aktivierung der importierten
 2839 Kartenterminalkonfiguration folgende zusätzliche Schritte ausführen:

- 2840 1. Die Liste der zu importierenden Kartenterminals MUSS dem Administrator
 2841 angezeigt werden. Er MUSS die Möglichkeit erhalten, einzelne Kartenterminals aus
 2842 dieser Liste zu löschen.
- 2843 2. Erst nach Bestätigung durch den Administrator werden die
 2844 Kartenterminalinformationen in die Kartenterminalverwaltung übernommen.
- 2845 3. Sofern die Kartenterminal-Konfiguration in einen Konnektor mit neuer Identität
 2846 importiert werden soll (neuer Konnektor oder neuer privater Schlüssel und neues
 2847 Zertifikat C.SAK.AUT auf der gSMC-K), muss die neue Identität des Konnektors
 2848 allen importierten Kartenterminals bekannt gemacht werden (Wartungs-Pairing,
 2849 siehe auch [gemSpec_KT#2.5.2.4]).
- 2850 a. Dazu baut der Konnektor unter der Nutzung von C.SAK.AUT eine temporäre
 2851 TLS-Verbindung auf und sendet das eHealth-Kartenterminal-Kommando
 2852 EHEALTH TERMINAL AUTHENTICATE in der Variante „ADD“ an jedes in der
 2853 Liste aufgeführte Kartenterminal. Mit dem Kommando und P2=03 holt sich der
 2854 Konnektor eine Challenge.
- 2855 b. Der eigentliche Austausch bzw. die Aufnahme des neuen Zertifikates erfolgt im
 2856 KT erst, nachdem diese Challenge mit dem Kommando EHEALTH TERMINAL
 2857 AUTHENTICATE im Modus P2=04 vom Konnektor korrekt beantwortet wurde.
 2858 Dieses Kommando sowie die Erzeugung der Challenge-Antwort wird in
 2859 [gemSpec_KT#3.7.2.4] und [gemSpec_KT#3.7.2] beschrieben.

- c. Nach erfolgreicher Abarbeitung des Kommandos wird der Eintrag in die interne Liste der gepairten Kartenterminals übernommen und die temporäre Verbindung zum Kartenterminal abgebaut. Kann ein Kartenterminal nicht erreicht werden, so MUSS die Befehlskette nachgeholt werden, sobald das Kartenterminal vom Konnektor wieder als verfügbar erkannt wird.

4. Zur abschließenden Kontrolle und zur weiteren fachlichen Nutzung baut der Konnektor zu jedem der neu konfigurierten und aktiv gesetzten Kartenterminals via TUC_KON_050 eine Verbindung auf.

[<=]

4.1.5 Kartendienst

Innerhalb des Kartendienstes werden folgende Präfixe für Bezeichner verwendet:

- Events (Topic Ebene 1): „CARD“
- Konfigurationsparameter: „CM_“

Der Konnektor verwaltet eine Liste aller Karten (CM_CARD_LIST), die in die vom Konnektor verwalteten Kartenterminals gesteckt sind (CTM_CT_LIST). Alle Ereignisse und Operationen, die sich auf Karten beziehen, werden durch diesen Basisdienst gekapselt.

Für jede gesteckte Karte vergibt er einen eindeutigen Identifikator (im weiteren Text CardHandle bezeichnet), mit dem diese Karte adressiert werden kann, um zu diesen oder mit diesen Karten Operationen auszuführen. Dieses Handle ist gültig bis zum Entfernen der Karte aus dem Kartenterminal.

Um die in [gemSpec_Perf] geforderten Zeiten für kartenbezogene Operationen erreichen zu können, kann es erforderlich sein, dass der Konnektor möglichst viele Informationen der Karten cached. Hierzu gehören Steuerdaten wie Extended Length, Version etc. aber auch Zertifikate der Karte (X.509 und CVC). Da es sich bei Caching um einen internen Mechanismus handelt, der sich nicht auf das funktionale Außenverhalten von TUCs oder Operationen auswirkt, wird das Caching nicht weiter beschrieben oder explizit gefordert. Es kann aber Anforderungen aus Sicherheitsicht bezüglich des Cachings geben (insbesondere hinsichtlich der erlaubten Caching-Dauer). Die Einhaltung dieser Vorgaben wird im Rahmen der CC-Evaluierung geprüft werden.

Der Kartendienst verwaltet mindestens die in der informativen Tabelle TAB_KON_531 ausgewiesenen Parameter, weitere herstellerepezifische Parameter sind möglich. Die normative Festlegung wann welche Parameter wie belegt werden, erfolgt in den folgenden Abschnitten und Unterkapiteln.

Tabelle 56: TAB_KON_531 Parameterübersicht des Kartendienstes

ReferenzID	Belegung	Zustandswerte
CM_CARD_LIST	Liste von Card-Objekten	Eine Liste von Repräsentanzen (CardObjects) der dem Konnektor bekannten Karten. Die Attribute der Card-Objekte sind im Folgenden gelistet.
CARD.CARDHANDLE		vom Konnektor vergebenen eindeutigen Identifikator (Handle).

CARD.CTID		Kartenterminal, in dem die Karte steckt
CARD.SLOTNO		Slot, in dem die Karte steckt
CARD.ICCSN		ICCSN der Karte (sofern auslesbar),
CARD.TYPE		Typ der Karte gemäß Tabelle TAB_KON_500 Wertetabelle Kartentypen
CARD.CARDVERSION		die Versionsinformationen zum Produkttyp der Karte und den gespeicherten Datenstrukturen gemäß [gemSpec_Karten_Fach_TIP].
CARD.CARDVERSION.COSVERSION		Produkttypversion des COS
CARD.CARDVERSION.OBJECTSYSTEMVERSION		Produkttypversion des Objektsystems
CARD.CARDVERSION.CARDPTPERSVERSION		Produkttypversion der Karte bei Personalisierung
CARD.CARDVERSION.DATASTRUCTUREVERSION		Version der Speicherstrukturen (aus EF.Version)
CARD.CARDVERSION.LOGGINGVERSION		Version der Befüllvorschrift für EF.Logging
CARD.CARDVERSION.ATRVERSION		Version der Befüllvorschrift für EF.ATR
CARD.CARDVERSION.GDOVERSION		Version der Befüllvorschrift für EF.GDO
CARD.CARDVERSION.KEYINFOVERSION		Version der Befüllvorschrift für KeyInfo
CARD.INSERTTIME	Timestamp	Zeitpunkt, an dem die Karte gesteckt wurde
CARD.CARDHOLDERNAME	String	Name des Karteninhabers bzw. der Institution/Organisation (subject.commonName)
CARD.KVNR	String	Versicherten-ID (unveränderbarer Teil der KVNR)
CARD.CERTEXPIRATIONDATE		Ablaufdatum des AUT-Zertifikats der Karte
CARD.CARDSESSION_LIST	Liste von CardSession-Objekten	Eine Liste von Repräsentanzen (CardSession-Objects) der pro Karte vorhandenen Kartensitzungen. Die Attribute der CardSession-Objekte sind im Folgenden gelistet. Das Tripel aus MandantID, CSID und

		UserID bildet den Kontext ab, in welchem diese Kartensitzung initiiert wurde.
CARDSESSION.AUTHSTATE	Liste von Einträgen aus a) C2C:KeyRef, Role oder b) CHV: PINRef	Liste von erreichten Sicherheitszuständen. Jeder einzelne Sicherheitszustand kann entweder über C2C gegen KeyRef (mit einer bestimmten Rolle gemäß [gemSpec_PKI_TI#Tab_PKI_918]) oder Card Holder Verification (CHV) gegen eine referenzierte PIN erreicht worden sein. Für eGK G2.0 wird der Zustand der MRPINs nicht in AuthState gespeichert.
CARDSESSION.MANDANTID		Mandant-ID
CARDSESSION.CSID		Clientsystem-ID
CARDSESSION.USERID		Nutzer-ID
CARDSESSION.AUTHBY	Referenz auf CardSession	Kartensitzung, über die diese Karte freigeschaltet wurde (nur für eGK belegt)
CARDSESSION.SIGNMODE	„PIN“ oder „Comfort“	Signaturmodus „PIN“: Komfortsignaturmodus ist für die Karte ausgeschaltet „Comfort“: Komfortsignaturmodus ist eingeschaltet Default-Wert=„PIN“ Nur relevant für den HBA

4.1.5.1 Funktionsmerkmalweite Aspekte

TIP1-A_4988 - Unterstützung von Gen1 und Gen2 Karten

Der Konnektor MUSS eGKs der Generation 1+ unterstützen.

Der Konnektor DARF eGKs der Generation 1 NICHT unterstützen. eGKs der Generation 1 werden im Konnektor als CARD.TYPE = UNKNOWN geführt.

Der Konnektor MUSS für eGK, HBA, SMC-B, gSMC-KT und gSMC-K Karten der Generation 2 unterstützen. Karten der Generation 2 sind alle Karten, deren Version des dem aktiven Objektsystem zugrundeliegenden Produkttyps (Tag 'C1' in EF.Version2) den Wert 4.x.x hat, wobei x in {0, ..., 255}.

Bei Karten der Generation 2

- MUSS der Konnektor die ECC-basierten Geräte-CV-Zertifikate unterstützen.

[<=]

Es kann notwendig sein, Karten der Generation 2 (G2) näher zu bezeichnen. In diesem Fall wird in G2.0- und G2.1-Karten unterschieden. Wird von Karten der Generation 2 gesprochen, so gilt die Festlegung für G2.x (G2.0, G2.1 und höher) des betrachteten Kartentyps.

TIP1-A_4558 - Caching-Dauer von Kartendaten im Konnektor

2913 Sofern der Konnektor Daten gesteckter Karten cached, so DÜRFEN diese Daten von HBAX
 2914 und SM-B NICHT länger als 24 Stunden gecached werden.
 2915 Der Konnektor DARF Daten der eGK NICHT über den Steckzyklus der Karte hinaus
 2916 cachen.
 2917 Ausnahme: Eine Cachingdauer über den Steckzyklus der eGK hinaus wird von einer
 2918 Fachanwendung gefordert und durch die Fachmodulspezifikation dieser Fachanwendung
 2919 definiert.
 2920 [**<=**]

2921 TIP1-A_6031 - Kein selbsttätiges Zurücksetzen der SM-B
 2922 Der Konnektor DARF NICHT selbsttätig die SM-B und deren Sicherheitszustände
 2923 zurücksetzen, auch nicht, wenn die Daten der SM-B nach Ablauf der 24-Stunden-Frist
 2924 neu in den Cache eingelesen werden.
 2925 [**<=**]

2926 TIP1-A_4559 - Konnektorzugriffsverbot auf DF.KT
 2927 Der Konnektor DARF NICHT auf das DF.KT einer gSMC-KT zugreifen.
 2928 [**<=**]

2929 TIP1-A_4560 - Rahmenbedingungen für Kartensitzungen
 2930 Der Konnektor MUSS alle Zugriffe auf Karten aus CM_CARD_LIST, die den
 2931 Sicherheitszustand der Karte erhöhen können oder einen erhöhten Sicherheitszustand
 2932 der Karte voraussetzen, im Kontext einer Kartensitzung zu dieser Karte durchführen
 2933 (CARD.CARDESESSION). Ausgenommen hiervon ist der Zugriff durch das CMS (bzw.
 2934 VSDD) auf die eGK.
 2935 Der Konnektor MUSS sicherstellen, dass in einer Kartensitzung nur dann auf einen
 2936 erhöhten Sicherheitszustand einer Karte zugegriffen werden kann, wenn die zur
 2937 Erreichung dieses Sicherheitszustandes erforderlichen Authentisierungen (PIN-
 2938 Verifikation, C2C-Rollen-Authentisierung etc.) in dieser verwendeten Kartensitzung
 2939 erfolgreich durchgeführt wurden.
 2940 Der Konnektor MUSS Authentisierungen in einer Kartensitzung so durchführen, dass in
 2941 anderen Kartensitzungen vorhandene Sicherheitszustände nicht beeinflusst werden. (Eine
 2942 falsche PIN-Eingabe in einer Kartensitzung darf den erhöhten Sicherheitszustand einer
 2943 anderen Sitzung nicht zurücksetzen etc.).
 2944 Der Konnektor SOLL die Verwaltung der Sicherheitsstatus der Kartensitzungen so über
 2945 die Nutzung logischer Kartenkanäle umsetzen, dass PIN-Verifikationen, die für die Dauer
 2946 der Kartensitzung Gültigkeit haben, nicht unnötig wiederholt werden müssen.
 2947 [**<=**]

2948 Für die TUCs zur PIN-Eingabe, Änderung und Entsperrung sind Festlegungen hinsichtlich
 2949 der auf dem Kartenterminal anzuzeigenden Meldungen erforderlich. Die folgende Tabelle
 2950 definiert diese Terminalanzeigen gemäß [SICCT#5.5.10.19].

2951 TIP1-A_4561-02 - Terminal-Anzeigen für PIN-Operationen
 2952 Der Konnektor MUSS im Rahmen des interaktiven PIN-Handlings die folgenden
 2953 Displaymessages für die Anzeige im Kartenterminal verwenden:

2954 **Tabelle 57: TAB_KON_090 Terminalanzeigen beim Eingeben der PIN am Kartenterminal**

Karte/ Kontext	PIN-Referenz	I/ O	Terminal-Anzeige	ANW (max.Anz Zeichen)
eGK /PIN-Eingabe	PIN.AMTS_REP	I	Vertreter- PIN • 0x0B für • 0x0BANW 0x0F Vertr-PIN:	22

für Vertreter-PIN				
eGK /PIN-Eingabe für Vertreter-PIN ändern	PIN.AMTS_REP	I	Vertreter-PIN • 0x0Bändern 0x0FPIN.eGK:	
eGK /PIN-Eingabe für Vertreter-PIN entsperren	PIN.AMTS_REP	I	Vertreter-PIN • 0x0entsperren 0x0FPIN.eGK:	
eGK /PIN-Eingabe für PIN-Schutz einschalten	MRPIN.NFD, MRPIN.DPE, MRPIN.AMTS, MRPIN.GDD	I	PIN-Schutz • 0x0BANW • 0x0Beinschalten 0x0FPIN.eGK:	16
eGK /PIN-Eingabe für PIN-Schutz abschalten	MRPIN.NFD, MRPIN.DPE, MRPIN.AMTS, MRPIN.GDD	I	PIN-Schutz • 0x0BANW • 0x0Babschalten 0x0FPIN.eGK:	16
eGK /Sonstige	ALLE (außer PIN.AMTS_REP)	I	PIN • 0x0Bfür • 0x0BANW 0x0FPIN.eGK:	32
HBax	PIN.CH	I	Eingabe • 0x0BFreigabe-PIN • 0x0BHBA 0x0FPIN.HBA:	
	PIN.QES (Signatur auslösen)	I	#UVW-XYZ • 0x0BEingabe • 0x0BSignatur-PIN • 0x0BHBA 0x0FPIN.QES:	
HBA	PIN.QES (Komfortsignatur aktivieren)	I	Komfortsignatur • 0x0Baktivieren • 0x0BHBA 0x0FPIN.QES:	
SMC-B	PIN.SMC	I	Eingabe • 0x0BPIN • SMC-B • 0x0BSLOT:X 0x0FPIN.SMC:	
ANDERE	BELIEBIG	I	Herstellerspezifisch	
Erfolgreiche PIN-Eingabe	ALLE	O	PIN • 0x0BERfolgreich • 0x0Bverifiziert!	
Fehlerhafte PIN-Eingabe	ALLE	O	PIN • 0x0Bfalsch • 0x0Boder • 0x0Bgesperrt!	
PUK-Eingabe	eGK PUK.CH	I	Eingabe • 0x0BVersicherten • 0x0BPUK 0x0FPUK.eGK:	
	HBax PUK.CH	I	Eingabe • 0x0BFreigabe-PUK • 0x0BHBA 0x0FPUK.HBA:	
	HBax PUK.QES	I	Eingabe • 0x0BSignatur-PUK • 0x0BHBA 0x0FPUK.QES:	
	SMC-B PUK.SMC	I	Eingabe • 0x0BPUK • SMC-B • 0x0BSLOT:X 0x0FPUK.SMC:	

Erfolgreiche PUK-Eingabe	ALLE	O	PIN • 0x0B erfolgreich • 0x0B entsperrt!
Fehlerhafte PUK-Eingabe	ALLE	O	PUK • 0x0B falsch • 0x0B oder • 0x0B gesperrt!
Eingabe einer neuen PIN	eGK ALLE (außer PIN.AMTS_REP)	I	Eingabe • 0x0B neue • 0x0B Versicherten - 0x0B PIN • 0x0B (6-8 • Ziffern) 0x0F PIN.eGK:
	eGK PIN.AMTS_REP	I	Eingabe • 0x0B neue • 0x0B Vertreter-PIN • 0x0B (6-8 • Ziffern) 0x0F Vertr-PIN:
	HBAX PIN.CH	I	Eingabe • 0x0B neue • 0x0B Freigabe- PIN • 0x0B HBA • 0x0B (6-8 • Ziffern) 0x0F PIN.HBA:
	HBAX PIN.QES	I	Eingabe • 0x0B neue • 0x0B Signatur- PIN • 0x0B HBA • 0x0B (6-8 • Ziffern) 0x0F PIN.QES:
	SMC-B PIN.SMC	I	Eingabe • 0x0B neue • 0x0B PIN • SMC-B • 0x0B SLOT: X • 0x0B (6-8 • Ziffern) 0x0F PIN.SMC:
Eingabe einer Transport-PIN	eGK PIN.CH	I	Eingabe • 0x0B Transport - 0x0B Versicherten - 0x0B PIN 0x0F T-PIN.eGK:
	HBAX PIN.CH	I	Eingabe • 0x0B Transport - 0x0B PIN • 0x0B HBA 0x0F T-PIN.HBA:
	HBAX PIN.QES	I	Eingabe • 0x0B Transport - 0x0B PIN • 0x0B HBA 0x0F T-PIN.QES:
	SMC-B PIN.SMC	I	Eingabe • 0x0B Transport - 0x0B PIN • SMC- B • 0x0B SLOT: X 0x0F T-PIN.SMC:
Wiederholung einer neuen PIN	eGK PIN.CH	I	Eingabe • 0x0B Versicherten - 0x0B PIN • 0x0B wiederholen! 0x0F PIN.eGK:
	eGK PIN.AMTS_REP	I	Eingabe • 0x0B neue • 0x0B Vertreter-PIN • 0x0B wiederholen! 0x0F Vertr-PIN:
	HBAX PIN.CH	I	Eingabe • 0x0B für • HBA • 0x0B wiederholen! 0x0F PIN.HBA:
	HBAX PIN.QES	I	Eingabe • 0x0B für • HBA • 0x0B wiederholen! 0x0F PIN.QES:
	SMC-B PIN.SMC	I	Eingabe • 0x0B PIN.SMC • 0x0B SLOT: X • 0x0B wiederholen! 0x0F PIN.SMC:

Ungleichheit bei der Wiederholung der Eingabe der neuen PIN	ALLE	0	PINs • 0x0B nicht • 0x0B identisch! • 0x0B Abbruch!
Erfolgreiche PIN-Änderung	ALLE	0	PIN • 0x0B erfolgreich • 0x0B geändert!
Anzeigen am lokalen Terminal beim Remote-PIN-Verfahren für das Ergebnis der Verschlüsselung durch die gSMC-KT			
Erfolgreiche Verschlüsselung	ALLE	0	Eingabe • 0x0B wird • 0x0B bearbeitet.
Fehler bei der Verschlüsselung	ALLE	0	Eingabe • 0x0B fehlgeschlagen.

[<=]

Hinweise zu den Terminalanzeigen bei PIN-Eingaben und zu obiger Tabelle:

- ANW kennzeichnet den Anwendungsfall und wird durch den vom Aufrufer übergebenen String ersetzt (siehe z. B. TUC_KON_012 „PIN verifizieren“)
- Zu PIN.SMC: "Slot:X" im PIN-Prompt gibt die Slot-Nummer im Kartenterminal an, in der die SMC steckt, da in einem Kartenterminal mehr als eine SMC stecken kann.
- Variable Teile der Terminalanzeige (Job- und Slot-Nummer) sind kursiv formatiert.
- Zeichensatz gemäß ISO 646DE-/DIN 66003-Codierung
- max. 48 Zeichen Text + 10 Zeichen PIN-Prompt bei Input
- max. 48 Zeichen bei Output
- Leerzeichen werden als "•" dargestellt
- UVW-XYZ: zeigt die Jobnummer an (siehe Kapitel 4.1.8.1.4)
- #: Beginn der Jobnummer zur Verifizierung des korrekten Kartenterminals
- Weitere Details zur Gestaltung der Jobnummer finden sich im Kapitel 4.1.8.1.4.
- Die Zeilenumbrüche in der Spalte "Terminal-Anzeige" sind editorisch bedingt.
- 0x0B und 0x0F (Sollbruchstellen bzw. Trennung zwischen Nachricht und PIN-Prompt) sind Trennzeichen gemäß [SICCT#5.6.1].

In den Technischen Use Cases TUC_KON_012 „PIN verifizieren“, TUC_KON_019 „PIN ändern“, TUC_KON_021 „PIN entsperren“ wird das Remote-PIN-Verfahren verwendet, sofern die Zielkarte in einem als für den Arbeitsplatz entfernt definiertem Kartenterminal steckt (siehe Kap. 4.1.1.1, Relation [7]). In diesem Fall erfolgt die Nutzerinteraktion am Remote-PIN-KT von workplaceId (PinInputKT). Dabei wendet der Konnektor das folgende Verfahren an:

2983 TIP1-A_5012 - Remote-PIN-Verfahren
 2984 Der Konnektor MUSS das Remote-PIN Verfahren im Sinne der BSI TR-03114
 2985 unterstützen. Abweichend von der TR-03114 MUSS statt der SMC-A eine gSMC-KT
 2986 verwendet werden.
 2987 Der Konnektor MUSS für die PIN-Objekte: HBA.PIN.CH, HBA.PUK.CH, HBA.PIN.QES,
 2988 HBA.PUK.QES, SM-B.PIN.SMC und SM-B.PUK.SMC das Remote-PIN Verfahren
 2989 unterstützen. Für alle anderen Karten und PIN-Objekte DARF das Verfahren NICHT
 2990 verwendet werden.
 2991 Für die Interaktion mit dem Anwender MÜSSEN die Display Messages entsprechend
 2992 TAB_KON_090 Terminalanzeigen beim Eingeben der PIN am Kartenterminal verwendet
 2993 werden.
 2994 Der Ablauf für eine PIN-Operation gegen eine Zielkarte MUSS in diesen logischen
 2995 Schritten erfolgen:

- 2996 1. Aufruf TUC_KON_005 „Card-to-Card authentisieren“ mit eigens für diesen
 2997 Zweck erzeugten Cardsession sowohl für die „Sendekarte“ im PinInputKT (gSMC-
 2998 KT) sowie der Zielkarte. AuthMode ist „gegenseitig+TC“
- 2999 2. Der Benutzer wird mit dem SICCT-Kommando PERFORM VERIFICATION bzw.
 3000 MODIFY VERIFICATION DATA zur Eingabe der PIN am PinInputKT aufgefordert.
 3001 Als Display Messages für die erfolgreiche Bearbeitung bzw. Fehler in der
 3002 Bearbeitung dieser Kommandos müssen die Texte mitgesendet werden, die in
 3003 TAB_KON_090 für die Ergebnisse der Verschlüsselung durch die gSMC-KT
 3004 festgelegt sind.
- 3005 3. Im PinInputKT verschlüsselt die gSMC-KT die eingegebene PIN mit dem zuvor
 3006 erzeugten Sessionkey.
- 3007 4. Die verschlüsselte PIN wird in das zur intendierten PIN-Operation passende
 3008 Kommando eingebettet (PIN verifizieren, ändern oder entsperren - wird durch den
 3009 eigentlichen PIN-TUC festgelegt) und das Kommando vom Konnektor an die
 3010 Zielkarte zur Entschlüsselung und Verifikation übergeben. Dabei MUSS die
 3011 Übertragung im gleichen Logischen Kanal wie die SM Vereinbarung erfolgen.
- 3012 5. Der Konnektor zeigt das Resultat der Zielkarte mittels SICCT OUTPUT am
 3013 lokalen Kartenterminal an. Er verwendet dabei den in TAB_KON_090 für die
 3014 aktuelle PIN-Operation spezifizierten Ausgabetexte.
- 3015 6. Das Result der Zielkarte wird an den Aufrufer zurückgegeben

3016 Fehlermeldung: Ein Fehler in der Verarbeitung führt zum Abbruch mit Fehlercode 4053
 3017 „Remote-PIN nicht möglich“ (Security, Error).
 3018 [**<=**]

3019 *Hinweis: Derzeit schlägt die Freischaltung der SMC-B durch Card-2-Card-Authentisierung*
 3020 *ohne Fehlermeldung fehl. Der Sicherheitszustand der SMC-B wird nicht verändert. Diese*
 3021 *Einschränkung betrifft TUC_KON_005 „Card-to-Card authentisieren“ (TAB_KON_096).*

3022 4.1.5.2 Durch Ereignisse ausgelöste Reaktionen

3023 TIP1-A_4562 - Reaktion auf „Karte entfernt“
 3024 Empfängt der Kartendienst das Ereignis „CT/SLOT_FREE“, so MUSS der Konnektor:

- 3025 • das über die im Ereignis gemeldeten Parameter CtID und SlotNo in
 3026 CM_CARD_LIST adressierte CardObject CARD identifizieren
- 3027 • für dieses CardObject folgendes Ereignis absetzen:
 3028 TUC_KON_256{
 3029 topic = „CARD/REMOVED“;

3030 eventType = Op;
 3031 Severity = Info;
 3032 parameters = <Params>}
 3033 wobei <Params> mit folgenden Werten belegt werden MUSS:

- 3034 • „CardHandle=\$CARD.CARDHANDLE,
- 3035 • Type=\$CARD.TYP,
- 3036 • CardVersion=\$CARD.VER,
- 3037 • ICCSN=\$CARD.ICCSN,
- 3038 • CtID=\$CARD.CTID,
- 3039 • SlotID=\$CARD.SLOTID,
- 3040 • InsertTime=\$CARD.INSERTTIME,
- 3041 • CardHolderName=\$CARD.CARDHOLDERNAME,
- 3042 • KVNVR=\$CARD.KVNVR“
- 3043 • das zugehörige CardObject aus CM_CARD_LIST entfernen.

3044
 3045 [**<=**]

3046 TIP1-A_4563 - Reaktion auf „Karte gesteckt“
 3047 Empfängt der Kartendienst das Ereignis „CT/SLOT_IN_USE“, so MUSS der Konnektor für
 3048 die Karte, die über die im Ereignis gemeldeten Parameter CtID und SlotNo adressiert ist,
 3049 über TUC_KON_001 ein neues CardObject in CM_CARD_LIST anlegen.
 3050 [**<=**]

3051 4.1.5.3 Interne TUCs, nicht durch Fachmodule nutzbar

3052 4.1.5.3.1 TUC_KON_001 „Karte öffnen“

3053 TIP1-A_4565 - TUC_KON_001 „Karte öffnen“
 3054 Der Konnektor MUSS den technischen Use Case „Karte öffnen“ gemäß TUC_KON_001
 3055 umsetzen.
 3056

3057 **Tabelle 58: TAB_KON_734 – TUC_KON_001 „Karte öffnen“**

Element	Beschreibung
Name	TUC_KON_001 „Karte öffnen“
Beschreibung	Der TUC initialisiert ein Card-Object basierend auf einer physikalischen Karte und fügt es CM_CARD_LIST zu. Die Karte kann erst im Anschluss unter Verwendung des erzeugten CardHandles verwendet werden.
Auslöser	Der Kartenterminaldienst meldet das Belegen eines KT-Slots
Vorbedingungen	<ul style="list-style-type: none"> • In ctId/slotId steckt eine Karte

Eingangsdaten	<ul style="list-style-type: none"> ctId (Kartenterminalidentifikator) slotId (Nummer des Kartenslots)
Komponenten	Karte, Kartenterminal, Konnektor
Ausgangsdaten	Keine
Standardablauf	<p>1. Prüfe, ob unter ctId und slotId ein Eintrag in CM_CARD_LIST vorhanden ist. Wenn bereits ein Eintrag vorhanden ist, lösche diesen.</p> <p>2. Erzeuge neuen Card-Object-Eintrag in CM_CARD_LIST und</p> <p>a) Generiere CARD.CARDHANDLE. mit folgenden Anforderungen:</p> <ul style="list-style-type: none"> - Das CardHandle MUSS innerhalb CM_CARD_LIST eindeutig sein. - Ein ungültig gewordenes CardHandle DARF innerhalb von 48h NICHT als neues CardHandle vergeben werden. <p>b) Befülle CARD.CTID und CARD.SLOTNO mit den Eingangsdaten</p> <p>c) Ermittle und befülle (soweit durch Karte unterstützt) die folgenden Daten:</p> <ul style="list-style-type: none"> - CARD.ICCSN - CARD.TYPE (mögliche Werte siehe Tabelle TAB_KON_500 Wertetabelle Kartentypen) - CARD.CARDVERSION - CARD.INSERTTIME (=aktuelle Systemzeit) - CARD.CARDHOLDERNAME (aus X.509-AUT-Zertifikat) - CARD.KVNR (nur für eGK, aus C.CH.AUT: unveränderbarer Teil der KVNR) - CARD.CERTEXPIRATIONDATE (=validity aus X.509-AUT-Zertifikat) <p>X.509-AUT-Zertifikat bezeichnet für eGK das C.CH.AUT-Zertifikat, für HBAX das C.HP.AUT-Zertifikat und für SMC-B das C.HCI.AUT-Zertifikat.</p> <p>3. Rufe TUC_KON_256{ topic = „CARD/INSERTED“; eventType = Op; severity = Info; parameters = <Params>} mit <Params> belegt aus dem CARD-Object: „CardHandle=\$, CardType=\$, CardVersion=\$, ICCSN=\$,CtID=\$,</p>

	<p>SlotID=\$, InsertTime=\$, CardHolderName=\$, KVN=\$, CertExpirationDate=\$"</p> <p>In CardVersion sind die Werte</p> <ul style="list-style-type: none"> - COSVERSION und - OBJECTSYSTEMVERSION <p>aus CARD.CARDVERSION einzutragen. Für eGK G1+ ist zusätzlich die</p> <ul style="list-style-type: none"> - DATASTRUCTUREVERSION <p>aus CARD.CARDVERSION einzutragen. CardVersion kann weitere Werte aus CARD.CARDVERSION enthalten.</p>
Varianten/ Alternativen	<p>Im Falle der KVK gibt es kein EF.ATR, EF.GDO und EF.DIR. Es wird daher lediglich der ATR ausgewertet, den das Kartenterminal beim Stecken der Karte liefert.</p>
Fehlerfälle	<p>(-> 2c) Karte/Kartenterminal antwortet mit einer spezifischen Fehlermeldung, Fehlercode <gemäß [gemSpec_COS]/[SICCT]> Auch im Fehlerfall wird Schritt 3 durchlaufen. Wenn nicht alle zu einem Kartentyp notwendigen Daten von der Karte gelesen werden konnten, dann wird Schritt 3 mit CardType=UNKNOWN ausgeführt.</p> <p>Auch im Fehlerfall wird Schritt 3 durchlaufen. Wenn nicht alle zu einem Kartentyp notwendigen Daten von der Karte gelesen werden konnten, dann wird Schritt 3 mit CardType=UNKNOWN ausgeführt.</p>
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

3058

3059 [\leq]

3060 4.1.5.4 Interne TUCs, auch durch Fachmodule nutzbar

3061 4.1.5.4.1 TUC_KON_026 „Liefere CardSession“

3062 TIP1-A_4566 - TUC_KON_026 „Liefere CardSession“

3063 Der Konnektor MUSS den technischen Use Case „Liefere CardSession“ gemäß

3064 TUC_KON_26 umsetzen.

3065 **Tabelle 59: TAB_KON_735 - TUC_KON_026**

Element	Beschreibung
Name	TUC_KON_026 „Liefere CardSession“
Beschreibung	Dieser Use Case gibt auf Grund der übergebenen Parameter die zugehörige CardSession zurück. Ist für die Parameterkombination noch keine CardSession vorhanden, wird eine neue erzeugt und im zugehörigen Card-Object hinterlegt.
Auslöser	<ul style="list-style-type: none"> • Indirekter Aufruf über durch Clientsysteme ausgeführte Operationen. • Aufruf durch Fachmodul
Vorbedingungen	Keine
Eingangsdaten	<ul style="list-style-type: none"> • mandantId • clientSystemId • cardHandle • userId - <i>optional/verpflichtend, wenn cardType = HBAX</i>
Komponenten	Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> • cardSession
Standardablauf	<ol style="list-style-type: none"> 1. Ermittle Card in CM_CARD_LIST über cardHandle 2. Prüfe dass der Karte entweder kein Lock zugeordnet ist oder der Aufrufer das Karten-Lock besitzt. 3. Ermittle cardSession in Card.CARDSESSION_LIST über mandantId, clientSystemId und userId

Varianten/ Alternativen	(→3) Wenn keine CardSession für diese Parameter vorhanden: 1. erzeuge neue CardSession in Card. CARDSESSION_LIST 2. Befülle CARDSESSION.MANDANTID, .CSID und .USERID mit Übergabeparametern
Fehlerfälle	(→2) Karte bereits reserviert, Fehlercode 4093
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

3066 **Tabelle 60: TAB_KON_824 Fehlercodes TUC_KON_026 „Liefere CardSession“**

Fehlercode	ErrorType	Severity	Fehlertext
4093	Technical	Error	Karte wird in einer anderen Kartensitzung exklusiv verwendet

3067
3068 **[<=]**
3069 *Hinweis zu TAB_KON_735 - TUC_KON_026: Die WorkplaceId wird als Eingangsparameter*
3070 *nicht benötigt. Bereits TUC_KON_000 stellt sicher, dass eine eGK jeweils nur von einem*
3071 *einzigem Arbeitsplatz aus angesprochen werden kann.*

3072 **4.1.5.4.2 TUC_KON_012 „PIN verifizieren“**

3073 **TIP1-A_4567 - TUC_KON_012 „PIN verifizieren“**

3074 Der Konnektor MUSS den technischen Use Case „PIN verifizieren“ gemäß TUC_KON_012
3075 umsetzen.

3076

3077 **Tabelle 61: TAB_KON_087 – TUC_KON_012 „PIN verifizieren“**

Element	Beschreibung
Name	TUC_KON_012 „PIN verifizieren“
Beschreibung	Dieser Use Case führt die Verifikation einer PIN einer Karte durch. Dabei wird der Anwender am Display des Kartenterminals aufgefordert, die PIN einzugeben. Dies erfolgt am PIN-Pad des Kartenterminals. Remote-PIN-Eingabe wird dabei automatisch unterstützt.
Auslöser	<ul style="list-style-type: none"> Aufruf des Use Case durch Basisdienste des Konnektors Aufruf des Use Cases durch ein Fachmodul im Konnektor

	<ul style="list-style-type: none"> Aufruf der Operation VerifyPin des CardService (siehe 4.1.5.5.1) durch das Clientsystem.
Vorbedingungen	Karte unterstützt die übergebene pinRef
Eingangsdaten	<ul style="list-style-type: none"> cardSession (Kartensitzung der Karte, deren PIN verifiziert werden soll) workplaceId pinRef (Referenz auf die zu verifizierende PIN, gemäß der Objektsystem-Spezifikation des jeweiligen Kartentyps.) actionName – <i>optional/verpflichtend, wenn cardType = eGK</i> (Zeichenkette, max. 32 bzw. 22 Zeichen PIN.AMTS_REP mit dem Namen der zugreifenden Fachanwendung bzw. des zu nutzenden Datenobjekts und der Zugriffsart, die mit dieser PIN freigeschaltet werden soll, z. B. für MRPIN.NFD: actionName = „Notfalldaten schreiben“; Positionen in der Zeichenkette, an denen ein Zeilenumbruch bei der Ausgabe am Kartenterminal erlaubt ist, werden mit `0x0B` gekennzeichnet. `0x0B` zählt bei der Länge der Zeichenkette nicht.) verificationType [Mandatorisch Sitzung] (Art der PIN-Verifikation: <ul style="list-style-type: none"> Mandatorisch: PIN wird immer verifiziert. Sitzung: PIN wird nicht erneut verifiziert, falls dies für die cardSession zuvor bereits geschehen ist und der dadurch erreichte Sicherheitszustand nicht zurückgesetzt wurde.)
Komponenten	Karte, Kartenterminal, Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> pinResult [PinResult] (Ergebnis der PIN-Verifikation) leftTries – <i>optional/verpflichtend, wenn pinResult = REJECTED</i> (Anzahl der verbleibenden Versuche)
Standardablauf	<ol style="list-style-type: none"> Ermittle Card = CM_CARD_LIST(CardSession) Prüfe, dass der Karte entweder kein Lock zugeordnet ist oder der Aufrufer das Karten-Lock besitzt. Wenn PinTyp(pinRef) = PIN.QES oder VerificationType = Mandatorisch 6. Wenn pinRef in CARDSESSION.AUTHSTATE vorhanden: pinResult = OK; Prüfe TUC_KON_022 „Liefere PIN-Status“ <ol style="list-style-type: none"> „VERIFYABLE“; „DISABLED“: pinResult = OK; Ermittle PinInputKT: Wenn Card.ctId ein dem Arbeitsplatz(workplaceId) lokal zugeordnetes Kartenterminal ist

	<p>(siehe Relation [6], Kapitel 4.1.1.1)</p> <ol style="list-style-type: none"> a. Setze PinInputKT = Card.CtID b. sonst „lokales Kartenterminal, das für die Remote-PIN-Eingabe zu verwenden ist“: PinInputKT = Arbeitsplatz(workplaceId).remote-PIN-KT(mandantId) <p>7. Atomare Operation: PIN verifizieren inkl. Eventing und Ergebnisvermerk</p> <ol style="list-style-type: none"> a. Rufe TUC_KON_256 { topic = „CARD/PIN/VERIFY_STARTED“; eventType = Op; severity = Info; parameters = („CardHandle=\$, CardType=\$, ICCSN=\$, CtID=\$, SlotID=\$, PinRef=\$, PinInputCtID=\$PinInputKT“, doLog=false)} b. Pin-Verifikation über „Perform Verification“ ([SICCT]) mit Display Messages gemäß Kontext in TAB_KON_090 Terminalanzeigen beim Eingeben der PIN am Kartenterminal, bei eGK ersetze „ANW“ durch actionName in Display Message. Wenn PinInputKT=Card.CtID dann PIN Verifikation direkt an Card.CtID, ansonsten Remote-PIN-Eingabe gemäß (TIP1-A_5012) c. Setze pinResult in Abhängigkeit von Ergebnis Perform Verification: <ul style="list-style-type: none"> - pinResult = OK für erfolgreiche Prüfung - pinResult = ERROR für Nutzer-Abbruch oder Bearbeitungsfehler (siehe Fehlerfälle) - pinResult = REJECTED für falsche PIN; - leftTries = x (bei Kartenantwort '63 Cx', x > 0) - pinResult = BLOCKED für gesperrte PIN (bei Kartenantwort '63 C0') d. Rufe TUC_KON_256 { topic = „CARD/PIN/VERIFY_FINISHED“; eventType = Op; severity = Info; parameters = („CardHandle=\$, CardType=\$, ICCSN=\$, CtID=\$, SlotID=\$, PinRef=\$, PinInputCtID=\$PinInputKT, Result=\$pinResult“); doLog = false } e. befülle CARDSESSION.AUTHSTATE mit pinRef und Ergebnis der PIN-Prüfung <p>8. Liefere pinResult zurück</p>
Varianten/ Alternativen	Schritt 7e: Für eGK G2.0 wird der Zustand der MRPINs nicht in AuthState gespeichert.
Fehlerfälle	Schritt 7 wird mit allen Teilschritten durchlaufen. Ein als Fehler ausgewiesener Zustand führt erst nach Schritt 7e zum Abbruch des TUCs. Fehleingaben zählen explizit nicht zu den Fehlerzuständen, sondern werden auf das Ergebnis REJECTED

	<p>oder BLOCKED abgebildet.</p> <ul style="list-style-type: none"> * Karte antwortet nicht innerhalb von CARD_TIMEOUT_CARD Sekunden, Fehlercode 4094 (→2) Karte ist fremd reserviert, Fehlercode 4093 (→5) Rückgabewert= <ul style="list-style-type: none"> - VERIFIED, Fehlercode 4001 - TRANSPORT_PIN oder EMPTY_PIN, Fehlercode 4065 - BLOCKED, Fehlercode 4063 (→6b) kein Remote-PIN-KT zugeordnet, Fehlercode 4092 (->6b) Card.TYP=eGK und Card.CtID ist nicht dem durch workplaceId bezeichneten Arbeitsplatz lokal zugeordnet: Fehlercode 4053 (→7) Timeout bei PIN Eingabe: Fehlercode 4043 (→7) Abbruch durch Nutzer: Fehlercode 4049 (→7) Sind das für die PIN-Eingabe benötigte Kartenterminal oder benötigte Teile davon (PIN Pad, Display) durch einen anderen zeitgleich im Konnektor ablaufenden Vorgang reserviert, so bricht der Use Case mit Fehler 4060 ab. (→7) Rückgabewert= <ul style="list-style-type: none"> - transportgeschützt (Transport-PIN oder Leer-PIN), Fehlercode 4065 (→7b) Ungültige PIN-Referenz; Fehlercode 4072 (→7b) Karte/Kartenterminal antwortet mit einer spezifischen Fehlermeldung, Fehlercode <gemäß [gemSpec_COS]/[SICCT]> <p>Zusätzliche Fehlerfälle ergeben sich aus der Remote-PIN-Eingabe gemäß (TIP1-A_5012)</p>
Nichtfunktionale Anforderungen	
Zugehörige Diagramme	Abbildung PIC_KON_111 Aktivitätsdiagramm zu „PIN verifizieren“

4001	Technical	Error	Interner Fehler
4043	Technical	Warning	Timeout bei der PIN-Eingabe
4049	Technical	Error	Abbruch durch den Benutzer
4053	Security	Error	Remote-PIN nicht möglich
4060	Technical	Error	Ressource belegt
4063	Security	Error	PIN bereits gesperrt (BLOCKED)
4065	Technical	Warning	PIN ist transportgeschützt, Änderung erforderlich
4072	Technical	Error	Ungültige PIN-Referenz <code>pinRef</code>
4092	Technical	Error	Remote-PIN-KT benötigt aber für diesen Arbeitsplatz nicht definiert
4093	Technical	Error	Karte wird in einer anderen Kartensitzung exklusiv verwendet
4094	Technical	Error	Timeout beim Kartenzugriff aufgetreten

3081
3082
3083
3084

[<=]

3085 4.1.5.4.3 TUC_KON_019 „PIN ändern“

3086 TIP1-A_4568 - TUC_KON_019 „PIN ändern“

3087 Der Konnektor MUSS den technischen Use Case „PIN ändern“ gemäß TUC_KON_019
3088 umsetzen.

3089

3090 **Tabelle 63: TAB_KON_736 – TUC_KON_019 „PIN ändern“**

Element	Beschreibung
Name	TUC_KON_019 „PIN ändern“
Beschreibung	Dieser Use Case führt die Änderung einer PIN einer Karte durch. Dabei wird der Anwender am Display des Kartenterminals aufgefordert, alte und neue PIN einzugeben. Remote-PIN-Eingabe wird dabei automatisch unterstützt.
Auslöser	<ul style="list-style-type: none"> Aufruf der Operation <code>ChangePin</code> des <code>CardService</code> (siehe 4.1.5.5.2) durch das Clientsystem. Aufruf durch Fachmodul
Vorbedingungen	Karte unterstützt die übergebene <code>pinRef</code>
Eingangsdaten	<ul style="list-style-type: none"> <code>cardSession</code> <code>workplaceId</code> (Arbeitsplatz-Identifikator)

	<ul style="list-style-type: none"> • pinRef (Referenz auf die zu ändernde PIN, gemäß der Objektsystem-Spezifikation des jeweiligen Kartentyps) • sourceCardSession – <i>optional/verpflichtend, wenn C2C erforderlich ist</i> (CardSession der Karte, die für die Card-to-Card-Authentisierung bei Änderung der PIN einer eGK der Generation 1+ verwendet werden soll.)
Komponenten	Karte, Kartenterminal, Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> • pinResult [PinResult] (Ergebnis der PIN-Verifikation) • leftTries – <i>optional/verpflichtend, wenn pinStatus = REJECTED</i> (verbleibende Versuche)
Standardablauf	<ol style="list-style-type: none"> 1. Ermittle Card = CM_CARD_LIST(CardSession) 2. Prüfe, dass der Karte entweder kein Lock zugeordnet ist oder der Aufrufer das Karten-Lock besitzt. 3. Prüfe TUC_KON_022 „Liefere PIN-Status“ {cardSession; pinRef}<>BLOCKED 4. Wenn pinRef=PIN.AMTS_REP, dann rufe TUC_KON_012 „PIN verifizieren“ { cardSession; workplaceId; pinRef=PIN.CH; actionName= „“; mandatorisch} 5. Wenn Card.TYP=eGK UND Card.Version=Generation1+, dann Aufruf TUC_KON_005 „Card-to-Card authentisieren“{ sourceCardSession; targetCardSession=cardSession; AuthMode =einseitig}. <p>Falls keine sourceCardSession angegeben ist, kann die CardSession der für den Mandanten verwalteten SMC-B verwendet werden.</p> <ol style="list-style-type: none"> 6. Ermittle PinInputKT: Wenn Card.ctId ein dem Arbeitsplatz (workplaceId) lokal zugeordnetes Kartenterminal ist (siehe Relation [6], Kapitel 4.1.1.1) <ol style="list-style-type: none"> a. Setze PinInputKT = Card.CtID b. sonst „lokales Kartenterminal, das für die Remote-PIN-Eingabe zu verwenden ist“: PinInputKT = Arbeitsplatz(workplaceId).remote-PIN-KT(mandantId) 7. Atomare Operation: PIN ändern inkl. Eventing und Ergebnisvermerk <ol style="list-style-type: none"> a. Rufe TUC_KON_256 { topic = „CARD/PIN/CHANGE_STARTED“;

	<pre> eventType = Op; severity = Info; parameters = („CardHandle=\$, CardType=\$, ICCSN=\$, CtID=\$, SlotID=\$, PinRef=\$, PinInputCtID=\$PinInputKT“); doLog = false } </pre> <p>b. Pin-Änderung über „MODIFY VERIFICATION DATA“ ([SICCT]) mit Display Messages entsprechend TAB_KON_090 Terminalanzeigen beim Eingeben der PIN am Kartenterminal. Bei Änderung der Versicherten-PIN der eGK ist dabei der Platzhalter „ANW“ durch den String „Änderung“ zu ersetzen. Der Platzhalter „#UVW-XYZ“ entfällt für die PIN.QES des HBA.</p> <p>Wenn PinInputKT=Card.CtID, dann PIN-Änderung direkt an Card.CtID, ansonsten Remote-PIN-Eingabe gemäß (TIP1-A_5012)</p> <p>Dabei sowohl Unterstützung normaler PIN-Änderung als auch Umsetzens eines Transportschutzes (alle Varianten gemäß Kartenspec sind zu unterstützen)</p> <p>c. Setze pinResult in Abhängigkeit von Ergebnis MODIFY VERIFICATION DATA:</p> <ul style="list-style-type: none"> - pinResult = OK für erfolgreiche Änderung - pinResult = ERROR für Nutzer-Abbruch oder Bearbeitungsfehler (siehe Fehlerfälle) <p>pinResult = REJECTED für falsche PIN-Eingaben; leftTries = x (bei Kartenantwort '63 Cx', x > 0)</p> <ul style="list-style-type: none"> - pinResult = BLOCKED für gesperrte PIN (bei Kartenantwort '63 C0') <p>d. Rufe TUC_KON_256 { topic = „CARD/PIN/CHANGE_FINISHED“; eventType = Op; severity = Info; parameters = („CardHandle=\$, CardType=\$, ICCSN=\$;CtID=\$, SlotID=\$, PinRef=\$, PinInputCtID=\$PinInputKT, Result=pinStatus“); doLog = false}</p> <p>e. Wenn Result = REJECTED oder BLOCKED , dann entferne PinRef aus CARDSESSION.AUTHSTATE</p> <p>8. Liefere pinResult und ggf. leftTries zurück</p>
Varianten/ Alternativen	<p>Schritt 4: Für eGK G2.0 gilt:</p> <p>Wenn pinRef=PIN.AMTS_REP, dann rufe TUC_KON_012 „PIN verifizieren“ { cardSession; workplaceId; pinRef=MRPIN.AMTS; actionName= „“; mandatorisch}</p>

	Schritt 7e: Für eGK G2.0 wird der Zustand der MRPINs nicht in AuthState gespeichert.
Fehlerfälle	<p>Schritt 7 wird mit allen Teilschritten durchlaufen. Ein als Fehler ausgewiesener Zustand führt erst nach Schritt 7e zum Abbruch des TUCs.</p> <p>* Karte antwortet nicht innerhalb von CARD_TIMEOUT_CARD Sekunden,</p> <p>Fehlercode 4094</p> <p>(→2) Karte ist fremd reserviert, Fehlercode 4093</p> <p>(→3) pinStatus=BLOCKED: Fehlercode 4063</p> <p>(→5) sourceCardSession benötigt aber leer, Fehlercode 4071</p> <p>(→6b) kein Remote-PIN-KT zugeordnet, Fehlercode 4092</p> <p>(→6b) Card.TYP=eGK und Card.CtID ist nicht dem durch workplaceId bezeichneten Arbeitsplatz lokal zugeordnet: Fehlercode 4053</p> <p>(→7b) neue PIN zu kurz/lang: Fehlercode 4068</p> <p>(→7b) zweite neue PIN<> erste neue PIN: Fehlercode 4067</p> <p>(→7b) Timeout bei PIN-Eingabe: Fehlercode 4043.</p> <p>(→7b) Abbruch durch Nutzer: Fehlercode 4049.</p> <p>(→7b) Ist das Kartenterminal oder Teile davon (PIN-Pad, Display) durch einen anderen Vorgang reserviert: Fehlercode 4060</p> <p>(→7b) kein PIN-Pad am Kartenterminal verfügbar: Fehlercode 4066</p> <p>(→7b) Ungültige PIN-Referenz; Fehlercode 4072</p> <p>(→7b) Karte antwortet mit einer spezifischen Fehlermeldung, Fehlercode</p> <p><Kartenfehlercode gemäß [gemSpec_COS]></p> <p>Zusätzliche Fehlerfälle ergeben sich aus der Remote-PIN-Eingabe gemäß (TIP1-A_5012)</p>
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

3091

Tabelle 64: TAB_KON_093 Fehlercodes TUC_KON_019 „PIN ändern“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4043	Technical	Warning	Timeout bei der PIN-Eingabe
4049	Technical	Error	Abbruch durch den Benutzer
4053	Security	Error	Remote-PIN nicht möglich
4060	Technical	Error	Ressource belegt

4063	Security	Error	PIN bereits blockiert (BLOCKED)
4066	Technical	Error	PIN Pad nicht verfügbar
4067	Security	Error	neue PIN nicht identisch
4068	Security	Error	neue PIN zu kurz/zu lang
4071	Technical	Error	keine Karte für C2C-Auth gesetzt
4072	Technical	Error	ungültige PIN-Referenz <code>PinRef</code>
4092	Technical	Error	Remote-PIN-KT benötigt aber für diesen Arbeitsplatz nicht definiert
4093	Technical	Error	Karte wird in einer anderen Kartensitzung exklusiv verwendet
4094	Technical	Error	Timeout beim Kartenzugriff aufgetreten

3092

3093 [\leq]

3094 4.1.5.4.4 TUC_KON_021 „PIN entsperren“

3095 TIP1-A_4569-02 - TUC_KON_021 „PIN entsperren“

3096 Der Konnektor MUSS den technischen Use Case „PIN entsperren“ gemäß TUC_KON_021
3097 umsetzen.

3098

3099 **Tabelle 65: TAB_KON_236 – TUC_KON_021 „PIN entsperren“**

Element	Beschreibung
Name	TUC_KON_021 „PIN entsperren“
Beschreibung	Dieser Use Case setzt den Fehlbedienungs­zähler für diese PIN in der Karte auf seinen Anfangswert zurück und es wird optional eine neue PIN gesetzt. Remote-PIN-Eingabe wird dabei automatisch unterstützt.
Auslöser	<ul style="list-style-type: none"> Aufruf der Operation UnblockPin des CardService (siehe 4.1.5.5.4) durch das Clientsystem.
Vorbedingungen	Karte unterstützt die übergebene pinRef
Eingangsdaten	<ul style="list-style-type: none"> cardSession CardSession der Karte, deren PIN entsperret werden soll) workplaceId

	<ul style="list-style-type: none"> pinRef (Referenz auf die zu entsperrende PIN, gemäß der Objektsystem-Spezifikation des jeweiligen Kartentyps) <p>setNewPin (true/false) - Angabe, ob eine neue PIN gesetzt oder die aktuelle weiterverwendet werden soll. Default = false</p> <p>sourceCardSession - <i>optional/wenn eGK G1+</i> (CardSession der Karte, die für die Card-to-Card-Authentisierung bei Entsperrung der PIN einer eGK der Generation 1+ verwendet werden soll)</p>
Komponenten	Karte, Kartenterminal, Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> result [PukResult]) (Ergebnis der PIN-Entsperrung durch PUK-Eingabe) leftTries - <i>optional/verpflichtend, wenn pukStatus = REJECTED</i> (verbleibende Versuche des PUKs)
Standardablauf	<ol style="list-style-type: none"> Ermittle Card = CM_CARD_LIST(Target.CardHandle) Prüfe, dass der Karte entweder kein Lock zugeordnet ist oder der Aufrufer das Karten-Lock besitzt. Wenn TUC_KON_022 „Liefere PIN-Status“ { cardSession; pinRef } <> („BLOCKED“ oder "TRANSPORT_PIN") dann beende TUC erfolgreich. Wenn pinRef=PIN.AMTS_REP, dann <ol style="list-style-type: none"> setNewPin = true rufe TUC_KON_012 „PIN verifizieren“ { cardSession; workplaceId; pinRef=PIN.CH; actionName= „“; mandatorisch} Wenn Card.TYP=eGK UND Card.Version=Generation1+, dann Aufruf TUC_KON_005 „Card-to-Card authentisieren“ { sourceCardSession; targetCardSession=cardSession; AuthMode =einseitig }. Falls keine sourceCardSession angegeben ist, kann die CardSession der für den Mandanten verwalteten SMC-B verwendet werden. Ermittle PinInputKT: Wenn Card.ctId ein dem Arbeitsplatz(workplaceId) lokal zugeordnetes Kartenterminal ist (siehe Relation [6], Kapitel 4.1.1.1) <ol style="list-style-type: none"> Setze PinInputKT = Card.CtID

	<p>b. sonst „lokales Kartenterminal, das für die Remote-PIN-Eingabe zu verwenden ist“: PinInputKT = Arbeitsplatz(workplaceId).remote-PIN-KT(mandantId)</p> <p>7. Atomare Operation: PIN entsperren inkl. Eventing und Ergebnisvermerk</p> <p>a. Rufe TUC_KON_256 { topic = „CARD/PIN/CHANGE_STARTED“; eventType = Op; severity = Info; parameters = („CardHandle=\$, CardType=\$, ICCSN=\$, CtID=\$; SlotID=\$, PinRef=\$, PinInputCtID=\$PinInputKT“); doLog=false}</p> <p>b. PIN-Entsperrung mit Display Messages entsprechend TAB_KON_090 Terminalanzeigen beim Eingeben der PIN am Kartenterminal. Wenn PinInputKT=Card.CtID, dann PIN-Änderung direkt an Card.CtID, ansonsten Remote-PIN-Eingabe gemäß (TIP1-A_5012)</p> <ul style="list-style-type: none"> Für pinRef == PIN.QES über „PERFORM VERIFICATION“ [SICCT] mit dem eingebetteten Kommando Reset Retry Counter in der Variante P1=1 (keine neue PIN setzen). Für pinRef<>PIN.QES wenn setNewPin = false, dann über PERFORM VERIFICATION“ [SICCT], sonst über „MODIFY VERIFICATION DATA“ [SICCT]. Das mit dem SICCT-Kommando als Command-To-Perform mitgesandte „Reset Retry Counter“ wird entsprechend dem Wert von setNewPIN parametrisiert. <p>c. Setze result in Abhängigkeit von Ergebnis Perform Verification bzw. Modify VerificationData:</p> <ul style="list-style-type: none"> result = OK für erfolgreiche Entsperrung result = ERROR für Nutzer-Abbruch oder Bearbeitungsfehler (siehe Fehlerfälle) result = REJECTED für falsche PUK; result = BLOCKED für gesperrte PUK; (bei Kartenantwort '63 C0') <p>d. Rufe TUC_KON_256 { topic=„CARD/PIN/CHANGE_FINISHED“; eventType=Op; severity=Info; parameters = („CardHandle=\$; CardType=\$; ICCSN=\$;CtID=\$; SlotID=\$; PinRef=\$; PinInputCtID=\$PinInputKT; Result=\$“); doLog=false }</p> <p>8. Liefere result und ggf. leftTries zurück</p>
--	---

Varianten/ Alternativen	Schritt 4: Für eGK G2.0 gilt: Wenn pinRef=PIN.AMTS_REP, dann rufe TUC_KON_012 „PIN verifizieren“ { cardSession; workplaceId; pinRef=MRPIN.AMTS; actionName= „“; mandatorisch}
Fehlerfälle	Schritt 7 wird mit allen Teilschritten durchlaufen. Ein als Fehler ausgewiesener Zustand führt erst nach Schritt 7d zum Abbruch des TUCs. * Karte antwortet nicht innerhalb von CARD_TIMEOUT_CARD Sekunden, Fehlercode 4094 (→2) Karte wird in einer anderen Kartensitzung exklusiv verwendet, Fehlercode 4093 (→5) sourceCardSession benötigt aber leer, Fehlercode 4071 (→6b) kein Remote-PIN-KT zugeordnet, Fehlercode 4092 (→6b) Card.TYP=eGK und Card.CtID ist nicht dem durch workplaceId bezeichneten Arbeitsplatz lokal zugeordnet: Fehlercode 4053 (→7b) blockierte PUK: Fehlercode 4064 (→7b) neue PIN zu kurz/lang: Fehlercode 4068 (→7b) zweite neue PIN<> erste neue PIN: Fehlercode 4067 (→7b) Timeout bei PIN Eingabe: Fehlercode 4043. (→7b) Abbruch durch Nutzer: Fehlercode 4049. (→7b) Ist das Kartenterminal oder Teile davon (PIN-Pad, Display) durch einen anderen Vorgang reserviert: Fehlercode 4060 (→7b) Karte/Kartenterminal antwortet mit einer spezifischen Fehlermeldung, Fehlercode <gemäß [gemSpec_COS]/[SICCT]> (→7b) Ungültige PIN-Referenz; Fehlercode 4072. Zusätzliche Fehlerfälle ergeben sich aus der Remote-PIN-Eingabe gemäß (TIP1-A_5012)
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

3100

Tabelle 66: TAB_KON_193 Fehlercodes TUC_KON_021 „PIN entsperren“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			

4043	Technical	Warning	Timeout bei der PIN-Eingabe
4049	Technical	Error	Abbruch durch den Benutzer
4053	Security	Error	Remote-PIN nicht möglich
4060	Technical	Error	Ressource belegt
4064	Security	Error	alte PIN bereits blockiert (hier: PUK)
4067	Security	Error	neue PIN nicht identisch
4068	Security	Error	neue PIN zu kurz/zu lang
4072	Technical	Error	ungültige PIN-Referenz <code>PinRef</code>
4092	Technical	Error	Remote-PIN-KT benötigt aber für diesen Arbeitsplatz nicht definiert
4093	Technical	Error	Karte wird in einer anderen Kartensitzung exklusiv verwendet
4094	Technical	Error	Timeout beim Kartenzugriff aufgetreten

3101

3102

3103 [\leq]

3104

3105 4.1.5.4.5 TUC_KON_022 „Liefere PIN-Status“

3106 TIP1-A_4570 - TUC_KON_022 „Liefere PIN-Status“

3107 Der Konnektor MUSS den technischen Use Case „Liefere PIN-Status“ gemäß
3108 TUC_KON_022 umsetzen.3109 **Tabelle 67 TAB_KON_532 – TUC_KON_022 „Liefere PIN-Status“**

Element	Beschreibung

Name	TUC_KON_022 „Liefere PIN-Status“
Beschreibung	Dieser Use Case prüft den Zustand eines PIN-Objekts einer Karte im Kontext einer CardSession.
Auslöser	<ul style="list-style-type: none"> • Aufruf des Use Case im Rahmen von technischen Use Cases der Basisdienste des Konnektors • Aufruf des Use Cases durch ein Fachmodul im Konnektor • Aufruf der Operation GetPinStatus des CardService (siehe 4.1.5.5.1) durch das Clientsystem.
Vorbedingungen	Karte unterstützt die übergebene pinRef
Eingangsdaten	<ul style="list-style-type: none"> • cardSession • pinRef (Pin-Referenz der angefragten PIN, gemäß der Objektsystem-Spezifikation des jeweiligen Kartentyps)
Komponenten	Karte, Kartenterminal, Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> • pinStatus [PinStatus] • leftTries – <i>optional/verpflichtend, wenn pinStatus = VERIFYABLE</i> (Anzahl der verbleibenden Versuche für die Verifikation der PIN)
Standardablauf	<ol style="list-style-type: none"> 1. Ermittle Card = CM_CARD_LIST(cardSession) 2. Prüfe, dass der Karte entweder kein Lock zugeordnet ist oder der Aufrufer das Karten-Lock besitzt. 3. pinRef in CardSession.AUTHSTATE vorhanden: <ol style="list-style-type: none"> a) Ja: Setze pinStatus = VERIFIED oder DISABLED (wie in AUTHSTATE) b) Nein: Aufruf der Kartenoperation „GET PIN STATUS“, Antwort der Karte wird ausgewertet: <ol style="list-style-type: none"> a. '90 00': (NoError: Verifiziert): pinStatus = VERIFYABLE (da nicht in dieser CardSession verifiziert) b. '62 C1': pinStatus = TRANSPORT_PIN c. '62 C7': pinStatus = EMPTY_PIN (Leer-PIN) d. '63 Cx': pinStatus = VERIFYABLE (mit $1 \leq x \leq 3$); LeftTries=x e. '63 C0': pinStatus = BLOCKED; leftTries=0 f. '62 D0': pinStatus = DISABLED (Verifikation nicht erforderlich, da PIN-Schutz ausgeschaltet); cardSession.AUTHSTATE aktualisieren g. Antwortet die Karte mit einer Fehlermeldung, bricht der TUC ab.

	Liefere leftTries nur in den Fällen d und e zurück.
Varianten/ Alternativen	
Fehlerfälle	* Karte antwortet nicht innerhalb von CARD_TIMEOUT_CARD Sekunden, Fehlercode 4094 (→3b) pinRef nicht gefunden: Fehlercode 4072
Zugehörige Diagramme	keine

3110 **Tabelle 68: TAB_KON_091 Fehlercodes TUC_KON_022 „Liefere PIN-Status“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4072	Technical	Error	ungültige PIN-Referenz <code>PinRef</code>
4094	Technical	Error	Timeout beim Kartenzugriff aufgetreten

3111
3112 [**<=**]

3113 4.1.5.4.6 TUC_KON_027 „PIN-Schutz ein-/ausschalten“

3114 TIP1-A_5486 - TUC_KON_027 „PIN-Schutz ein-/ausschalten“

3115 Der Konnektor MUSS den technischen Use Case TUC_KON_027 „PIN-Schutz ein-
3116 /ausschalten“ umsetzen.

3117 **Tabelle 69: TAB_KON_240 - TUC_KON_027 „PIN-Schutz ein-/ausschalten“**

Element	Beschreibung
Name	TUC_KON_027 „PIN-Schutz ein-/ausschalten“
Beschreibung	Schaltet das Erfordernis, die PIN zu verifizieren, ein bzw. aus. Diese Operation wird nur unterstützt für PINs der EGK G2 gemäß [gemSpec_eGK_ObjSys]; für sie können folgende Kommandos auf das Passwortobjekt angewendet werden: <ul style="list-style-type: none"> DISABLE VERIFICATION REQUIREMENT ENABLE VERIFICATION REQUIREMENT
Auslöser	<ul style="list-style-type: none"> Aufruf durch ein Fachmodul Aufruf der Operationen EnablePin und DisablePin des CardService durch das Clientsystem.
Vorbedingungen	Karte unterstützt die übergebene pinRef

Eingangsdaten	<ul style="list-style-type: none"> cardSession (CardSession einer EGK G2) pinRef (PIN-Referenz der ab-/anzuschaltenden PIN, gemäß der Objektsystem-Spezifikation des jeweiligen Kartentyps) enable [Boolean] (enable = true: Erfordernis der Benutzerverifikation einschalten; enable = false: Erfordernis der Benutzerverifikation abschalten)
Komponenten	Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> pinResult [PinResult] (Ergebnis von PIN-Schutz ein-/ausschalten durch PIN-Eingabe) leftTries – <i>optional/verpflichtend nach fehlerhafter PIN</i> (verbleibende Versuche)
Standardablauf	<ol style="list-style-type: none"> 1. Ermittle Card = CM_CARD_LIST(cardSession) 2. Prüfe, dass der Karte entweder kein Lock zugeordnet ist oder der Aufrufer im Besitz des Karten-Locks ist. 3. Prüfe Card.Type = EGK und Generation ≥ 2 4. Prüfe pinRef = MRPIN.AMTS und Card.Type = EGK und Generation > 2.0 5. Wenn enable A: =true: Atomare Operation: PIN bearbeiten inkl. Eventing und Ergebnisvermerk <ol style="list-style-type: none"> a. Rufe TUC_KON_256 { topic = „CARD/PIN/ENABLE_STARTED“; eventType = Op; severity = Info; parameters = („CardHandle=\$, CardType=\$, ICCSN=\$, CtID=\$, SlotID=\$, PinRef=\$, PinInputCtID=\$PinInputKT“); doLog = false } b. Aufruf des Kartenterminalkommandos „SICCT PERFORM VERIFICATION“ mit der Kartenoperation „ENABLE VERIFICATION REQUIREMENT“ als Command-To-Perform. Es ist der Parameter P1='00' (mit Benutzerverifikation) zu verwenden. Die Anzeige am KT erfolgt entsprechend TAB_KON_090 Terminalanzeigen beim Eingeben der PIN am Kartenterminal. Ersetze in displayMessage „ANW“ entsprechend ANW(pinRef) gemäß Tabelle TAB_KON_838. c. Setze pinResult in Abhängigkeit von Ergebnis Perform Verification: <ul style="list-style-type: none"> - pinResult = OK für erfolgreiche Änderung - pinResult = ERROR für Nutzer-Abbruch oder Bearbeitungsfehler (siehe Fehlerfälle) - pinResult = REJECTED für falsche PIN; leftTries = x (bei Kartenantwort '63 Cx', x > 0)

	<ul style="list-style-type: none"> - pinResult = BLOCKED für gesperrte PIN (bei Kartenantwort '63 C0') <p>d. Rufe TUC_KON_256 { topic = „CARD/PIN/ENABLE_FINISHED“; eventType = Op; severity = Info; parameters = („CardHandle=\$, CardType=\$, ICCSN=\$, CtID=\$, SlotID=\$, PinRef=\$, PinInputCtID=\$PinInputKT“); doLog = false }</p> <p>B: =false: Atomare Operation: PIN bearbeiten inkl. Eventing und Ergebnisvermerk</p> <p>a. Rufe TUC_KON_256 { topic = „CARD/PIN/DISABLE_STARTED“; eventType = Op; severity = Info; parameters = („CardHandle=\$, CardType=\$, ICCSN=\$, CtID=\$, SlotID=\$, PinRef=\$, PinInputCtID=\$PinInputKT“); doLog = false }</p> <p>b. Aufruf des Kartenterminalkommandos „SICCT PERFORM VERIFICATION“ mit der Kartenoperation „DISABLE VERIFICATION REQUIREMENT“ als Command-To-Perform. Es ist der Parameter P1='00' (mit Benutzerverifikation) zu verwenden. Die Anzeige am KT erfolgt entsprechend TAB_KON_090 Terminalanzeigen beim Eingeben der PIN am Kartenterminal. Ersetze in displayMessage „ANW“ entsprechend ANW(pinRef) gemäß Tabelle TAB_KON_838.</p> <p>c. Setze pinResult in Abhängigkeit von Ergebnis Perform Verification: <ul style="list-style-type: none"> - pinResult = OK für erfolgreiche Änderung - pinResult = ERROR für Nutzer-Abbruch oder Bearbeitungsfehler (siehe Fehlerfälle) - pinResult = REJECTED für falsche PIN; leftTries = x (bei Kartenantwort '63 Cx', x > 0) - pinResult = BLOCKED für gesperrte PIN </p> <p>d. Rufe TUC_KON_256 { topic = „CARD/PIN/DISABLE_FINISHED“; eventType = Op; severity = Info; parameters = („CardHandle=\$, CardType=\$, ICCSN=\$;CtID=\$, SlotID=\$, PinRef=\$, PinInputCtID=\$PinInputKT“); doLog=false}</p> <p>6. Liefere pinResult und leftTries zurück</p>
--	--

Varianten/ Alternativen	(->3) zur Optimierung kann vor Schritt 5 der PIN-Schutz geprüft werden: a. pinStatus=TUC_KON_022 „Liefere PIN-Status“ { cardSession; pinRef } b. Wenn pinStatus<>DISABLED und enable=true, dann pinResult=OK und -> weiter in Schritt 6 c. Wenn pinStatus=DISABLED und enable=false, dann pinResult=OK und -> weiter in Schritt 6
Fehlerfälle	(→2) Karte ist fremd reserviert: Fehlercode 4093 (→3) Karte ist keine eGK der Generation 2 oder höher: Fehlercode 4209 (→4) PIN nicht gefunden; Karte ist eGK G2.0: Die Operation „PIN-Schutz ein-/ausschalten“ wird für MRPIN.AMTS nicht unterstützt: Fehlercode 4072 (→5) Karte antwortet nicht innerhalb von CARD_TIMEOUT_CARD Sekunden: Fehlercode 4094 (→5) PIN nicht gefunden: Fehlercode 4072 (→5) PIN gesperrt: Fehlercode 4063 (→5) Zugriffsbedingung nicht erfüllt (PIN nicht abschaltbar): Fehlercode 4085
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	keine

3118 **Tabelle 70: TAB_KON_838 Mapping von pinRef auf ANW**

pinRef	ANW (max. 16 Zeichen)
MRPIN.NFD	Notfalldaten
MRPIN.DPE	Pers.Erklärungen
MRPIN.AMTS	Medikationsdaten
MRPIN.GDD	PIN•GDD

3119
3120 Hinweis zu TAB_KON_838: Leerzeichen werden als "•" dargestellt.

3121 **Tabelle 71: TAB_KON_241 Fehlercodes TUC_KON_027 „PIN-Schutz ein/ausschalten“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			

4063	Security	Error	PIN bereits blockiert (BLOCKED)
4072	Technical	Error	ungültige PIN-Referenz <code>PinRef</code>
4085	Security	Error	Zugriffsbedingung nicht erfüllt
4093	Technical	Error	Karte wird in einer anderen Kartensitzung exklusiv verwendet
4094	Technical	Error	Timeout beim Kartenzugriff aufgetreten
4209	Technical	Error	Kartentyp <code>%CardType%</code> wird durch diese Operation nicht unterstützt.

3122
3123
3124

[<=]

3125 4.1.5.4.7 TUC_KON_023 „Karte reservieren“

3126 TIP1-A_4571 - TUC_KON_023 „Karte reservieren“

3127 Der Konnektor MUSS den technischen Use Case „Karte reservieren“ gemäß
3128 TUC_KON_023 umsetzen.

3129

3130 **Tabelle 72: TAB_KON_533 - TUC_KON_023 „Karte reservieren“**

Element	Beschreibung
Name	<p>TUC_KON_023 „Karte reservieren“</p> <p>Dem Aufrufer des TUC_KON_023 wird beim Reservieren (DoLock=Ja) der Karte zur ausschließlichen Nutzung ein Lock zugeordnet. Wird der TUC-KON_023 mit diesem Lock zum Freigeben der Reservierung (DoLock=Nein) aufgerufen, dann erlischt das Lock und die ausschließliche Nutzung wird beendet. Der Scope der Kartenreservierung wird vom Aufrufer des TUC_KON_023 gesteuert. Das Lock ist Konnektor-intern. Es darf nicht außerhalb des Konnektors referenzierbar sein. Zwei verschiedene Operationsaufrufe am Konnektor dürfen nie ein identisches Lock haben.</p> <p>Der Konnektor MUSS sicherstellen, dass auch im Fehlerfall die Reservierung zu einem Lock aufgehoben wird. Ein Lock darf nicht dauerhaft bestehen.</p>
Beschreibung	Reservierung der Karte
Auslöser	<ul style="list-style-type: none"> Aufruf des Use Case im Rahmen von technischen Use Cases der Basisdienste des Konnektors Aufruf des Use Cases durch ein Fachmodul im Konnektor
Vorbedingungen	Keine
Eingangsdaten	<ul style="list-style-type: none"> <code>cardSession</code>

	<ul style="list-style-type: none"> doLock [Boolean] (Zielzustand der Karte; true = reserviert, false = freigegeben)
Komponenten	Konnektor
Ausgangsdaten	Keine
Standardablauf	1. Ermittle Card = CM_CARD_LIST(cardSession) 2. Wenn doLock A: = true: i. Prüfe, dass der zur cardSession gehörenden Karte kein Lock zugeordnet ist ii. Dem Aufrufer wird ein Lock auf die zur cardSession gehörende Karte zugeordnet. Es wird nicht explizit als Ausgangsdatum modelliert, sondern der Aufrufer hat das Lock durch die Zuordnung, muss es aber nicht verwalten. B: = false: i. Prüfe, dass der Aufrufer für die zur cardSession gehörende Karte ein Lock hat. ii. Das der Karte zugeordnete Lock wird gelöscht.
Varianten/ Alternativen	Keine
Fehlerfälle	(→2Ai) Karte bereits reserviert, Fehlercode 4093 (→2Bi) Karte nicht durch Aufrufer reserviert, Fehlercode 4001
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

3131 **Tabelle 73: TAB_KON_534 Fehlercodes TUC_KON_023 „Karte reservieren“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4001	Technical	Error	interner Fehler
4093	Technical	Error	Karte bereits reserviert

3132
3133 **[<=]**

3134 **4.1.5.4.8 TUC_KON_005 „Card-to-Card authentisieren“**

3135 Die C2C-Authentisierung erfolgt konform zu den in [gemSpec_COS#15] festgelegten
3136 Authentisierungsprotokollen.

3137 **Definition Quellkarte/Zielkarte:**

3138 Bei einseitiger Card-to-Card-Authentisierung ohne Aushandlung eines Session Key ist die
 3139 Quellkarte diejenige, die die Rolle des Karteninhabers bzw. der Organisation gemäß
 3140 [gemSpec_PKI_TI#Tab_PKI_254] gegenüber der anderen Karte nachweist, z. B. der HBA
 3141 bei der Freischaltung einer eGK.

3142 Bei gegenseitiger Card-to-Card-Authentisierung ohne Aushandlung eines Session Key
 3143 erfolgen nach einander zwei einseitige Card-to-Card-Authentisierungen mit vertauschten
 3144 Rollen. Quell- und Zielkarte habe daher für den Gesamtablauf keine nähere Bedeutung.

3145 Bei Card-to-Card-Authentisierung mit Aushandlung eines Session Key ist die Quellkarte
 3146 diejenige, die die SM-APDUs produzieren kann, also die SMC (-KT oder -K).

3147 Die Zielkarte ist jeweils die Karte, die nicht die Quellkarte ist.

3148

3149 TIP1-A_4572 - TUC_KON_005 „Card-to-Card authentisieren“

3150 Der Konnektor MUSS den technischen Use Case „Card-to-Card authentisieren“ gemäß
 3151 TUC_KON_005 umsetzen.

3152 Die Card-to-Card-Authentisierung zwischen zwei Karten, bei der eine Karte der
 3153 Generation 1+ angehört MUSS das RSA-Verfahren verwenden.

3154 Die Card-to-Card-Authentisierung zwischen zwei Karten der Generation 2 MUSS das
 3155 Verfahren der elliptischen Kurven verwenden.

3156

3157 **Tabelle 74: TAB_KON_096 – TUC_KON_005 „Card-to-Card authentisieren“**

Element	Beschreibung
Name	TUC_KON_005 „Card-to-Card authentisieren“
Beschreibung	Durchführung einer Card-to-Card-Authentisierung
Auslöser	<ul style="list-style-type: none"> • Aufruf des Use Case im Rahmen von technischen Use Cases der Basisdienste des Konnektors • Aufruf des Use Cases durch ein Fachmodul im Konnektor
Vorbedingungen	Wert von Source_CARDSESSION.AUTHSTATE: wenn Quellkarte a) ein HBA ist: CHV; PIN.CH, verifiziert b) eine SMC-B ist: CHV; PIN.SMC verifiziert
Eingangsdaten	<ul style="list-style-type: none"> • sourceCardSession (Quellkarte) • targetCardSession (Zielkarte) • authMode (gemäß Tabelle TAB_KON_673)
Komponenten	Karten, Konnektor, Kartenterminal
Ausgangsdaten	Keine
Standardablauf	<ol style="list-style-type: none"> 1. Ermittle sCard = CM_CARD_LIST(sourceCardSession) 2. Ermittle tCard = CM_CARD_LIST(targetCardSession) 3. Prüfe, dass der <u>Quell</u>karte entweder kein Lock zugeordnet ist oder der Aufrufer im Besitz auf das Lock der Quellkarte ist. Prüfe, dass der <u>Ziel</u>karte entweder kein Lock zugeordnet

	<p>ist oder der Aufrufer im Besitz auf das Lock der Zielkarte ist.</p> <ol style="list-style-type: none"> 4. Prüfe Aufrufparameter auf erlaubte Kombination gemäß Tabelle TAB_KON_674 5. Wenn das zu verwendende CV-Zertifikat der Quellkarte ein CV-Zertifikat der Generation 2 oder höher ist, dann prüfe sein Ausstellungsdatum (CED) gegen die aktuelle Zeit 6. Wenn Card.TYP=eGK UND Card.Version=Generation1+, dann prüfe, ob aktuelles System-Datum < 01.01.2019 ist 7. Wähle Key-Referenzen gemäß Tabelle TAB_KON_674 8. Prüfe pinRef/keyRef in sCard.CARDSESSION.AUTHSTATE und tCard.CARDSESSION.AUTHSTATE für adressierte Schlüssel wie in Zugriffsbedingung der Karten definiert vorhanden 9. Durchführung der Authentisierung gemäß Tabelle TAB_KON_673 mit Key-Referenzen gemäß Tabelle TAB_KON_674 10. Ergänze targetCardSession.AUTHSTATE mit tKeyRef und Rolle aus sKeyRef (CHA bzw. CHAT aus dem EndEntity-CV-Zertifikat der Quellkarte)
Varianten/ Alternativen	<p>(→9) Wenn der für die CA-Zertifikatsprüfung zu selektierende CVC-Root-Key auf der Zielkarte nicht vorhanden ist (Returncode des Kartenkommandos „MANAGE SECURITY ENVIRONMENT“ ist '6A 88'), dann muss der Konnektor:</p> <ol style="list-style-type: none"> a) das oder die passenden Cross-CV-Zertifikate aus dem Truststore auswählen b) mit dem Kartenkommando „PSO Verify Certificate“ jedes ausgewählte Cross-CV-Zertifikat durch die Zielkarte prüfen lassen. Dadurch wird der im Cross-CV-Zertifikat enthaltene öffentliche Schlüssel an die Zielkarte übertragen. Die Zielkarte speichert den darin enthaltenen neuen CVC-Root-Key. c) den neuen CVC-Root-Key auf der Zielkarte selektieren d) den Standardablauf der C2C-Authentisierung fortsetzen <p>(→9) Wenn tCard.TYPE=EGK und AuthMode=gegenseitig, dann Echtheitsprüfung der eGK durch den Konnektor:</p> <ol style="list-style-type: none"> a) Freischaltung der EGK durch den HBA/die SMC-B: Durchführen der Authentisierung gemäß Tabelle TAB_KON_673 mit Key-Referenzen gemäß Tabelle TAB_KON_674 aber mit AuthMode=einseitig b) Konnektor liest das CA-Zertifikat EF.C.CA_eGK.CS (G1+) bzw. C.CA_eGK.CS.E256 (G2) c) Konnektor liest das End-Entity-Zertifikat der EGK EF.C.eGK.AUT_CVC (G1+) bzw. EF.C.eGK.AUT_CVC.E256 (G2) d) Konnektor prüft das CVC-EE-Zertifikat mit TUC_KON_042

	<p>„CV-Zertifikat prüfen“ { certificate = C.eGK.AUT_CVC/C.eGK.AUT_CVC.E256; caCertificate = C.CA_eGK.CS/C.CA_eGK.CS.E256 } e) Konnektor erzeugt Zufallszahl f) Konnektor selektiert den PrK.eGK.AUT_CVC (G1+) bzw. PrK.eGK.AUT_CVC.E256 (G2) und stellt abhängig von der Version der eGK den Algorithmus auf der eGK ein (MSE Set) g) Konnektor sendet Konkatenation aus Zufallszahl und CARD.ICCSN mit dem Befehl „INTERNAL AUTHENTICATE“ an die eGK h) Konnektor wertet das von der Karte erhaltene Chifftrat aus</p>
Fehlerfälle	<p>* Karte antwortet nicht innerhalb von CARD_TIMEOUT_CARD Sekunden, Fehlercode 4094 (→3) Eine Karte ist fremd reserviert, Fehlercode 4093 (→5) Zertifikat der Quellkarte fehlerhaft. Ausstellungsdatum liegt in der Zukunft; Fehlercode 4233 (→6) eGK G1+ ausgealtert, Fehlercode 4192 (→8) Nötige PIN, bzw. KeyRef ist nicht verifiziert, Fehlercode 4085 (→9) Je nachdem, welche Karte den Fehler verursachte, wird zum ursprünglichen Fehler (Fehlercode gemäß [gemSpec_COS]) im Error-Trace (welcher an erster Stelle im Falle des HBA z. B. bereits ein Fehler bezüglich PIN-Verifikation enthalten kann) noch ein weiterer mit Code 4056 oder 4057 hinzugefügt. Kann der Fehler nicht eindeutig einer der beiden Karten zugeordnet so wird Error-Code 4048 verwendet.</p>
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	Keine

3158

Tabelle 75: TAB_KON_673 AuthMode für C2C

AuthMode	Definition des Ablaufs
einseitig	Externe oder Interne Authentisierung ([gemSpec_COS#15.1] oder [gemSpec_COS#15.2], passend zu den Zugriffsregeln der beteiligten CVC)
gegenseitig	Card-2-Card-Authentisierung ohne Sessionkey-Aushandlung ([gemSpec_COS#15.3])
gegenseitig+TC	Card-2-Card-Authentisierung mit Sessionkey-Aushandlung zur Etablierung eines Trusted Channels ([gemSpec_COS#15.4])

3159 **Tabelle 76: TAB_KON_674 Erlaubte Parameterkombinationen und resultierende CV-**
 3160 **Zertifikate für C2C**

Quellkarte	Zielkarte	AuthMode	sKeyRef	tKeyRef	Fachlicher UseCase
HBA oder SM-B	eGK G1+	einseitig	{HPC.AUTR_ CVC.R2048 SMC.AUTR_ CVC.R2048}		Freischaltung eGK
HBA oder SM-B	eGK G1+	gegen seitig	{HPC.AUTR_ CVC.R2048 SMC.AUTR_ CVC.R2048}	eGK.AUT_ CVC.R2048	Freischaltung eGK mit Echtheits prüfung eGK
HBA oder SM-B	eGK G2	einseitig	{HPC.AUTR_ CVC.E256 SMC.AUTR_ CVC.E256}		Freischaltung eGK
HBA oder SM-B	eGK G2	gegen seitig	{HPC.AUTR_ CVC.E256 SMC.AUTR_ CVC.E256}	eGK.AUT_ CVC.E256	Freischaltung eGK mit Echtheits prüfung eGK
SMC-K	HBA	gegen seitig+TC	SAK.AUTD_ CVC.E256	HPC.AUTD_ SUK_CVC.E256	DTBS- Übertragung bei QES
SMC-KT	HBA	gegen seitig+TC	SMC.AUTD_ RPS_CVC.E256	HPC.AUTD_ SUK_CVC.E256	Remote-PIN
SMC-KT	SM-B	gegen seitig+TC	SMC.AUTD_ RPS_CVC.E256	SMC.AUTD_ RPE_CVC.E256	Remote-PIN

3161 **Tabelle 77: TAB_KON_535 Fehlercodes TUC_KON_005 „Card-to-Card authentisieren“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4048	Technical	Error	Fehler bei der C2C-Authentisierung
4056	Technical	Error	Fehler bei der C2C-Authentisierung, Quellkarte
4057	Technical	Error	Fehler bei der C2C-Authentisierung, Zielkarte
4085	Security	Error	Zugriffsbedingungen nicht erfüllt
4093	Technical	Error	Karte wird in einer anderen Kartensitzung exklusiv verwendet
4094	Technical	Error	Timeout beim Kartenzugriff aufgetreten
4192	Security	Error	C2C mit eGK G1+ ab 01.01.2019 nicht mehr gestattet
4233	Security	Error	Ausstellungsdatum des Zertifikats liegt in der Zukunft;

3162
3163 [\leq]

3164 4.1.5.4.9 TUC_KON_202 „LeseDatei“

3165 TIP1-A_4573 - TUC_KON_202 „LeseDatei“

3166 Der Konnektor MUSS den technischen Use Case „LeseDatei“ gemäß TUC_KON_202
3167 umsetzen.

3168

3169 **Tabelle 78: TAB_KON_218 – TUC_KON_202 „LeseDatei“**

Element	Beschreibung
Name	TUC_KON_202 „LeseDatei“
Beschreibung	Transparente Datei oder Teile davon lesen
Auslöser	<ul style="list-style-type: none"> • Aufruf des Use Case im Rahmen von technischen Use Cases der Basisdienste des Konnektors • Aufruf des Use Cases durch ein Fachmodul im Konnektor
Vorbedingungen	Die Karte MUSS den nötigen Sicherheitszustand für den Zugriff besitzen
Eingangsdaten	<ul style="list-style-type: none"> • cardSession • fileIdentifier – <i>optional/verpflichtend, wenn kein sfid angegeben ist</i> (FID der zu lesenden Datei) • sfid – <i>optional/verpflichtend, wenn kein fileIdentifier angegeben ist</i> (Short File Identifier der zu lesenden Datei) • folder (Verzeichnis/Applikation auf der Karte, in dem sich die Datei befindet) • offset – <i>optional/nur verwendbar, wenn fileIdentifier angegeben ist</i> (Startposition innerhalb der Datei) • length – <i>optional</i> (Längenangabe, um den Zugriff auf Teile einer Datei einzuschränken)
Komponenten	Karte, Kartenterminal, Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> • content (Gelesene Daten)

Standardablauf	<ol style="list-style-type: none"> 1. Ermittle Card = CM_CARD_LIST(cardSession) 2. Prüfe, dass der Karte entweder kein Lock zugeordnet ist oder der Aufrufer das Karten-Lock besitzt. 3. Prüfe PinRef/KeyRef in CARDSESSION.AUTHSTATE für adressierte Datei wie in Zugriffsbedingung der Karte definiert vorhanden 4. Selektiere Verzeichnis und Datei 5. Lies Daten über Kartenkommando „READ BINARY“ unter Berücksichtigung von Offset- und Längenangaben 6. Die gelesenen Daten werden an den Aufrufer zurückgegeben
Varianten/ Alternativen	Wenn Card.TYPE = KVK, sendet der Konnektor in diesem Fall ein "Read Binary" im Sinne von SICCT 1.2.1, 5.5.8.1 "Kommandos für synchrone Chipkarten".
Fehlerfälle	<p>* Karte antwortet nicht innerhalb von CARD_TIMEOUT_CARD Sekunden, Fehlercode 4094 (→2) Karte ist fremd reserviert, Fehlercode 4093 (→3) Nötige PIN ist nicht verifiziert, Fehlercode 4085 (→5) Verzeichnis deaktiviert, Fehlercode 4086 (→4-5) Karte antwortet mit einer spezifischen Fehlermeldung, Fehlercode <Kartenfehlercode gemäß [gemSpec_COS]></p>
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

3170 **Tabelle 79: TAB_KON_536 Fehlercodes TUC_KON_202 „LeseDatei“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4085	Security	Error	Zugriffsbedingungen nicht erfüllt
4086	Technical	Error	Verzeichnis deaktiviert
4093	Technical	Error	Karte wird in einer anderen Kartensitzung exklusiv verwendet
4094	Technical	Error	Timeout beim Kartenzugriff aufgetreten

3171
 3172
 3173 **[<=]**

3174 **4.1.5.4.10 TUC_KON_203 „SchreibeDatei“**
 3175 **TIP1-A_4574 - TUC_KON_203 „SchreibeDatei“,**

3176 Der Konnektor MUSS den technischen Use Case „SchreibeDatei“ gemäß TUC_KON_203
 3177 umsetzen.
 3178

3179 **Tabelle 80: TAB_KON_219 – TUC_KON_203 „SchreibeDatei“**

Element	Beschreibung
Name	TUC_KON_203 „SchreibeDatei“
Beschreibung	Daten in transparente Datei schreiben
Auslöser	<ul style="list-style-type: none"> Aufruf durch Fachmodul
Vorbedingungen	Die Karte MUSS den nötigen Sicherheitszustand für den Zugriff besitzen.
Eingangsdaten	<ul style="list-style-type: none"> cardSession fileIdentifier – <i>optional/verpflichtend, wenn kein sfid angegeben ist</i> (FID der zu lesenden Datei) sfid – <i>optional/verpflichtend, wenn kein fileIdentifier angegeben ist</i> (Short File Identifier der zu lesenden Datei) folder (Verzeichnis/Applikation auf der Karte, in dem sich die Datei befindet) offset – <i>optional</i> (Startposition innerhalb der Datei, default: 0) length – <i>optional</i> (Längenangabe, um den Zugriff auf Teile einer Datei einzuschränken; default: alles ab offset) dataToBeWritten (Zu schreibende Daten)
Komponenten	Karte, Kartenterminal, Konnektor
Ausgangsdaten	Keine

Standardablauf	<ol style="list-style-type: none"> 1. Ermittle Card = CM_CARD_LIST(cardSession) 2. Prüfe Card.TYPE <> KVK 3. Prüfe, dass der Karte entweder kein Lock zugeordnet ist oder der Aufrufer das Karten-Lock besitzt. 4. Prüfe PinRef/KeyRef in CARDSESSION.AUTHSTATE für adressierte Datei wie in Zugriffsbedingung der Karte definiert vorhanden 5. Selektiere Verzeichnis 6. Selektiere Datei mittels SELECT mit P2='04' (Selektieren einer Datei, Antwortdaten mit FCP) 7. Ermittle size (Größe der selektierten Datei in Byte) mit size = numberOfOctet aus FCP 8. Wenn size - offset >= Größe von dataToBeWritten in Byte, dann schreibe dataToBeWritten mittels Kartenkommando "UPDATE BINARY" unter Berücksichtigung von Offset- und Längenangaben
Varianten/ Alternativen	keine
Fehlerfälle	<p>* Karte antwortet nicht innerhalb von CARD_TIMEOUT_CARD Sekunden, Fehlercode 4094 (→2) Schreibzugriff auf KVK nicht gestattet, Fehlercode 4085 (→3) Karte ist fremd reserviert, Fehlercode 4093 (→4) Nötige PIN ist nicht verifiziert, Fehlercode 4085 (→5) Verzeichnis oder Datei existiert nicht, Fehlercode 4087 (→4-5) Karte antwortet mit einer spezifischen Fehlermeldung, Fehlercode <Kartenfehlercode gemäß [gemSpec_COS]> (→6) Ausgewählte Datei ist nicht transparent, Fehlercode 4089 (→6) Verzeichnis deaktiviert, Fehlercode 4086 (→8) dataToBeWritten sind größer als der zur Verfügung stehende Speicherplatz, Fehlercode 4247</p>
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

3180

Tabelle 81: TAB_KON_537 Fehlercodes TUC_KON_203 „Schreibe Datei“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4085	Security	Error	Zugriffsbedingungen nicht erfüllt

4086	Technical	Error	Verzeichnis deaktiviert
4087	Technical	Error	Datei nicht vorhanden
4089	Technical	Error	Datei ist vom falschen Typ
4093	Technical	Error	Karte wird in einer anderen Kartensitzung exklusiv verwendet
4094	Technical	Error	Timeout beim Kartenzugriff aufgetreten
4247	Technical	Error	Speicherplatz auf der Karte nicht ausreichend

3181

3182

3183 [\leq]

3184 4.1.5.4.11 TUC_KON_204 „LöscheDateiInhalt“

3185 TIP1-A_5476 - TUC_KON_204 „LöscheDateiInhalt“

3186 Der Konnektor MUSS den technischen Use Case „LöscheDateiInhalt“ gemäß
 3187 TUC_KON_204 umsetzen.

3188

3189 **Tabelle 82: TAB_KON_204 – TUC_KON_204 „LöscheDateiInhalt“**

Element	Beschreibung
Name	TUC_KON_204 „LöscheDateiInhalt“
Beschreibung	Inhalt einer transparenten Datei löschen
Auslöser	<ul style="list-style-type: none"> Aufruf des Use Cases durch ein Fachmodul im Konnektor
Vorbedingungen	Die Karte MUSS den nötigen Sicherheitszustand für den Zugriff besitzen
Eingangsdaten	<ul style="list-style-type: none"> cardSession fileIdentifier – <i>optional/verpflichtend, wenn kein sfid angegeben ist</i> (FID der zu bearbeitenden Datei) sfid – <i>optional/verpflichtend, wenn kein fileIdentifier angegeben ist</i> (Short File Identifier der zu bearbeitenden Datei) folder (Verzeichnis/Applikation auf der Karte, in dem sich die Datei befindet) offset – <i>optional</i> (Position, ab der der Inhalt gelöscht werden soll. Default: 0)
Komponenten	Karte, Kartenterminal, Konnektor

Ausgangsdaten	keine
Standardablauf	<ol style="list-style-type: none"> 1. Ermittle Card = CM_CARD_LIST(cardSession) 2. Prüfe Card.TYPE <> KVK 3. Prüfe, dass der Karte entweder kein Lock zugeordnet ist oder der Aufrufer im Besitz des Karten-Locks ist. 4. Prüfe PinRef/KeyRef in CARDESSION.AUTHSTATE für adressierte Datei wie in Zugriffsbedingung der Karte definiert vorhanden 5. Selektiere Verzeichnis und Datei 6. Lösche Inhalt der selektierten Datei über Kartenkommando „ERASE BINARY“, ggf. ab angegebenem Offset, sonst ab Anfang
Varianten/ Alternativen	keine
Fehlerfälle	<p>* Karte antwortet nicht innerhalb von CARD_TIMEOUT_CARD Sekunden, Fehlercode 4094 (→2) Karte ist keine eGK der Generation 2 oder höher: Fehlercode 4209 (→3) Karte ist fremd reserviert, Fehlercode 4093 (→4) Nötige PIN ist nicht verifiziert, Fehlercode 4085 (→5) Verzeichnis oder Datei existiert nicht, Fehlercode 4087 (→6) Ausgewählte Datei ist nicht transparent, Fehlercode 4089 (→6) Verzeichnis deaktiviert, Fehlercode 4086 (→5-6) Karte antwortet mit einer spezifischen Fehlermeldung, Fehlercode <Kartenfehlercode gemäß [gemSpec_COS]></p>
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

3190 **Tabelle 83: TAB_KON_785 Fehlercodes TUC_KON_204 „LöscheDateiInhalt“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4085	Security	Error	Zugriffsbedingungen nicht erfüllt
4086	Technical	Error	Verzeichnis deaktiviert
4087	Technical	Error	Datei nicht vorhanden
4089	Technical	Error	Datei ist vom falschen Typ

4093	Technical	Error	Karte wird in einer anderen Kartensitzung exklusiv verwendet
4094	Technical	Error	Timeout beim Kartenzugriff aufgetreten
4209	Technical	Error	Kartentyp %CardType% wird durch diese Operation nicht unterstützt.

3191
3192
3193 [**<=**]

3194 4.1.5.4.12 TUC_KON_209 „LeseRecord“

3195 TIP1-A_4575 - TUC_KON_209 „LeseRecord“

3196 Der Konnektor MUSS den technischen Use Case „LeseRecord“ gemäß TUC_KON_209
3197 umsetzen.

3198

3199 **Tabelle 84: TAB_KON_538 – TUC_KON_209 „LeseRecord“**

Element	Beschreibung
Name	TUC_KON_209 „LeseRecord“
Beschreibung	Daten aus strukturierter Datei lesen
Auslöser	<ul style="list-style-type: none"> Aufruf durch Fachmodul
Vorbedingungen	Die Karte MUSS den nötigen Sicherheitszustand für den Zugriff besitzen
Eingangsdaten	<ul style="list-style-type: none"> cardSession fileIdentifier – <i>optional/verpflichtend, wenn kein sfid angegeben ist</i> (FID der zu lesenden Datei) sfid – <i>optional/verpflichtend, wenn kein fileIdentifier angegeben ist</i> (Short File Identifier der zu lesenden Datei) folder (Verzeichnis/Applikation auf der Karte, in dem sich die Datei befindet) recordNumber
Komponenten	Karte, Kartenterminal, Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> content (Inhalt des Records)

Standardablauf	<ol style="list-style-type: none"> 1. Ermittle Card = CM_CARD_LIST(cardSession) 2. Prüfe, dass der Karte entweder kein Lock zugeordnet ist oder der Aufrufer das Karten-Lock besitzt 3. Prüfe PinRef/KeyRef in CARDSESSION.AUTHSTATE für adressierte Datei wie in Zugriffsbedingung der Karte definiert vorhanden 4. Selektiere Verzeichnis und ggf. Datei 5. Lies Daten über Kartenkommando „READ RECORD“ unter Berücksichtigung von recordNumber 6. Rückgabe der Daten an den Aufrufer
Varianten/ Alternativen	keine
Fehlerfälle	<p>* Karte antwortet nicht innerhalb von CARD_TIMEOUT_CARD Sekunden, Fehlercode 4094 (→2) Karte ist fremd reserviert, Fehlercode 4093 (→3) Nötige PIN ist nicht verifiziert, Fehlercode 4085 (→4) Verzeichnis oder Datei oder Record existiert nicht, Fehlercode 4087 (→5) Wenn Karte WrongFileType liefert, Fehlercode 4089 (→5) Verzeichnis deaktiviert, Fehlercode 4086 (→4-5) Karte antwortet mit einer spezifischen Fehlermeldung, Fehlercode <Kartenfehlercode gemäß [gemSpec_COS]>.</p>
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

3200

Tabelle 85: TAB_KON_539 Fehlercodes TUC_KON_209 „LeseRecord“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4085	Security	Error	Zugriffsbedingungen nicht erfüllt
4086	Technical	Error	Verzeichnis deaktiviert
4087	Technical	Error	Datei nicht vorhanden
4089	Technical	Error	Datei ist vom falschen Typ
4093	Technical	Error	Karte wird in einer anderen Kartensitzung exklusiv verwendet
4094	Technical	Error	Timeout beim Kartenzugriff aufgetreten

3201
3202
3203 [\leq]

3204 4.1.5.4.13 TUC_KON_210 „SchreibeRecord“

3205 TIP1-A_4576 - TUC_KON_210 „SchreibeRecord“

3206 Der Konnektor MUSS den technischen Use Case „SchreibeRecord“ gemäß TUC_KON_210
3207 umsetzen.

3208

3209 **Tabelle 86: TAB_KON_224 – TUC_KON_210 „SchreibeRecord“**

Element	Beschreibung
Name	TUC_KON_210 „SchreibeRecord“
Beschreibung	Daten in lineare Datei schreiben
Auslöser	<ul style="list-style-type: none"> Aufruf durch Fachmodul
Vorbedingungen	Die Karte MUSS den nötigen Sicherheitszustand für den Zugriff besitzen
Eingangsdaten	<ul style="list-style-type: none"> cardSession fileIdentifier – <i>optional/verpflichtend, wenn kein sfid angegeben ist</i> (FID der zu bearbeitenden Datei) sfid – <i>optional/verpflichtend, wenn kein fileIdentifier angegeben ist</i> (Short File Identifier der zu bearbeitenden Datei) folder (Verzeichnis/Applikation auf der Karte, in dem sich die Datei befindet) recordNumber dataToBeWritten (Zu schreibende Daten)
Komponenten	Karte, Kartenterminal, Konnektor
Ausgangsdaten	keine

Standardablauf	<ol style="list-style-type: none"> 1. Ermittle Card = CM_CARD_LIST(cardSession) 2. Prüfe Card.TYPE <> KVK 3. Prüfe, dass der Karte entweder kein Lock zugeordnet ist oder der Aufrufer das Karten-Lock besitzt. 4. Prüfe PinRef/KeyRef in CARDSESSION.AUTHSTATE für adressierte Datei wie in Zugriffsbedingung der Karte definiert vorhanden 5. Selektiere Verzeichnis und ggf. Datei 6. Schreibe Daten über Kartenkommando „UPDATE RECORD“ unter Berücksichtigung von recordNumber
Varianten/ Alternativen	keine
Fehlerfälle	<p>* Karte antwortet nicht innerhalb von CARD_TIMEOUT_CARD Sekunden, Fehlercode 4094 (→2) Schreibzugriff auf KVK nicht gestattet, Fehlercode 4085 (→3) Karte ist fremd reserviert, Fehlercode 4093 (→4) Nötige PIN ist nicht verifiziert, Fehlercode 4085 (→5) Verzeichnis, Datei existiert nicht, Fehlercode 4087 (→5-6) Verzeichnis deaktiviert, Fehlercode 4086 (→4-6) Karte antwortet mit einer spezifischen Fehlermeldung, Fehlercode <Kartenfehlercode gemäß [gemSpec_COS]></p>
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

3210 **Tabelle 87: TAB_KON_540 Fehlercodes TUC_KON_210 „SchreibeRecord“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4085	Security	Error	Zugriffsbedingungen nicht erfüllt
4086	Technical	Error	Verzeichnis deaktiviert
4087	Technical	Error	Datei nicht vorhanden
4088	Technical	Error	Datensatz zu groß

4093	Technical	Error	Karte wird in einer anderen Kartensitzung exklusiv verwendet
4094	Technical	Error	Timeout beim Kartenzugriff aufgetreten

3211
3212
3213 **[<=]**

3214 4.1.5.4.14 TUC_KON_211 „LöscheRecordInhalt“

3215 TIP1-A_5477 - TUC_KON_211 „LöscheRecordInhalt“

3216 Der Konnektor MUSS den technischen Use Case „LöscheRecordInhalt“ gemäß
3217 TUC_KON_211 umsetzen.

3218

3219 **Tabelle 88: TAB_KON_211 – TUC_KON_211 „LöscheRecordInhalt“**

Element	Beschreibung
Name	TUC_KON_211 „LöscheRecordInhalt“
Beschreibung	Inhalt eines Records einer strukturierten Datei löschen
Auslöser	<ul style="list-style-type: none"> • Aufruf des Use Case im Rahmen von technischen Use Cases der Basisdienste des Konnektors • Aufruf des Use Cases durch ein Fachmodul im Konnektor
Vorbedingungen	Die Karte MUSS den nötigen Sicherheitszustand für den Zugriff besitzen
Eingangsdaten	<ul style="list-style-type: none"> • cardSession • fileIdentifier – <i>optional/verpflichtend, wenn kein sfid angegeben ist</i> (FID der zu bearbeitenden Datei) • sfid – <i>optional/verpflichtend, wenn kein fileIdentifier angegeben ist</i> (Short File Identifier der zu bearbeitenden Datei) • folder (Verzeichnis/Applikation auf der Karte, in dem sich die Datei befindet) • recordNumber
Komponenten	Karte, Kartenterminal, Konnektor
Ausgangsdaten	keine

Standardablauf	<ol style="list-style-type: none"> 1. Ermittle Card = CM_CARD_LIST(cardSession) 2. Prüfe Card.TYPE <> KVK 3. Prüfe, dass der Karte entweder kein Lock zugeordnet ist oder der Aufrufer im Besitz des Karten-Locks ist. 4. Prüfe PinRef/KeyRef in CARDSESSION.AUTHSTATE für adressierte Datei wie in Zugriffsbedingung der Karte definiert vorhanden 5. Selektiere Verzeichnis und Datei 6. Lösche Recordinhalt (identifiziert durch recordNumber) der selektierten Datei über Kartenkommando „ERASE RECORD“
Varianten/ Alternativen	keine
Fehlerfälle	<p>* Karte antwortet nicht innerhalb von CARD_TIMEOUT_CARD Sekunden, Fehlercode 4094 (→2) Karte ist keine eGK der Generation 2 oder höher: Fehlercode 4209 (→3) Karte ist fremd reserviert, Fehlercode 4093 (→4) Nötige PIN ist nicht verifiziert, Fehlercode 4085 (→5) Verzeichnis, Datei oder Record existiert nicht, Fehlercode 4087 (→6) Verzeichnis deaktiviert, Fehlercode 4086 (→6) Record nicht vorhanden, Fehlercode 4091 (→5-6) Karte antwortet mit einer spezifischen Fehlermeldung, Fehlercode <Kartenfehlercode gemäß [gemSpec_COS]></p>
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

3220

Tabelle 89: TAB_KON_786 Fehlercodes TUC_KON_211 „LöscheRecordInhalt“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4085	Security	Error	Zugriffsbedingungen nicht erfüllt
4086	Technical	Error	Verzeichnis deaktiviert
4087	Technical	Error	Datei nicht vorhanden
4091	Technical	Error	Record nicht vorhanden
4093	Technical	Error	Karte wird in einer anderen Kartensitzung exklusiv verwendet
4094	Technical	Error	Timeout beim Kartenzugriff aufgetreten

4209	Technical	Error	Kartentyp %CardType% wird durch diese Operation nicht unterstützt.
------	-----------	-------	--

3221
3222
3223

[<=]

3224 4.1.5.4.15 TUC_KON_214 „FügeHinzuRecord“

3225 TIP1-A_4577 - TUC_KON_214 „FügeHinzuRecord“

3226 Der Konnektor MUSS den technischen Use Case „FügeHinzuRecord“ gemäß
3227 TUC_KON_214 umsetzen.

3228

3229 **Tabelle 90: TAB_KON_228 – TUC_KON_214 „FügeHinzuRecord“**

Element	Beschreibung
Name	TUC_KON_214 „FuegeHinzuRecord“
Beschreibung	Daten in lineare Datei anfügen
Auslöser	<ul style="list-style-type: none"> • Aufruf durch Fachmodul • TUC_KON_006
Vorbedingungen	Die Karte MUSS den nötigen Sicherheitszustand für den Zugriff besitzen
Eingangsdaten	<ul style="list-style-type: none"> • cardSession • fileIdentifier – <i>optional/verpflichtend, wenn kein sfid angegeben ist</i> (FID der zu bearbeitenden Datei) • sfid – <i>optional/verpflichtend, wenn kein fileIdentifier angegeben ist</i> (Short File Identifier der zu bearbeitenden Datei) • folder (Verzeichnis/Applikation auf der Karte, in dem sich die Datei befindet) • dataToBeWritten (Zu schreibende Daten)
Komponenten	Karte, Kartenterminal, Konnektor
Ausgangsdaten	keine

Standardablauf	<ol style="list-style-type: none"> 1. Ermittle Card = CM_CARD_LIST(cardSession) 2. Prüfe Card.TYPE <> KVK 3. Prüfe, dass der Karte entweder kein Lock zugeordnet ist oder der Aufrufer das Karten-Lock besitzt. 4. Prüfe PinRef/KeyRef in CARDSESSION.AUTHSTATE für adressierte Datei wie in Zugriffsbedingung der Karte definiert vorhanden 5. Selektiere Verzeichnis und ggf. Datei 6. Schreibe Daten über Kartenkommando „APPEND RECORD“
Varianten/ Alternativen	keine
Fehlerfälle	<p>* Karte antwortet nicht innerhalb von CARD_TIMEOUT_CARD Sekunden, Fehlercode 4094 (→2) Schreibzugriff auf KVK nicht gestattet, Fehlercode 4085 (→3) Karte ist fremd reserviert, Fehlercode 4093 (→4) Nötige PIN ist nicht verifiziert, Fehlercode 4085 (→5-6) Verzeichnis, Datei existiert nicht, Fehlercode 4087 (→6) Verzeichnis deaktiviert, Fehlercode 4086 (→5-6) Karte antwortet mit einer spezifischen Fehlermeldung, Fehlercode <Kartenfehlercode gemäß [gemSpec_COS]></p>
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

3230 **Tabelle 91: TAB_KON_541 Fehlercodes TUC_KON_214 „FügeHinzuRecord“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4085	Security	Error	Zugriffsbedingungen nicht erfüllt
4086	Technical	Error	Verzeichnis deaktiviert
4087	Technical	Error	Datei nicht vorhanden
4093	Technical	Error	Karte wird in einer anderen Kartensitzung exklusiv verwendet
4094	Technical	Error	Timeout beim Kartenzugriff aufgetreten

3231
 3232
 3233 [**<=**]

3234 4.1.5.4.16 TUC_KON_215 „SucheRecord“

3235 TIP1-A_4578 - TUC_KON_215 „SucheRecord“

3236 Der Konnektor MUSS den technischen Use Case „SucheRecord“ gemäß TUC_KON_215
3237 umsetzen.
3238

3239 **Tabelle 92: TAB_KON_229 – TUC_KON_215 „SucheRecord“**

Element	Beschreibung
Name	TUC_KON_215 „SucheRecord“
Beschreibung	Daten in linearer Datei suchen
Auslöser	<ul style="list-style-type: none"> Aufruf durch Fachmodul
Vorbedingungen	Die Karte MUSS den nötigen Sicherheitszustand für den Zugriff besitzen
Eingangsdaten	<ul style="list-style-type: none"> cardSession fileIdentifier – <i>optional/verpflichtend</i>, wenn kein sfid angegeben ist (FID der zu bearbeitenden Datei) sfid – <i>optional/verpflichtend</i>, wenn kein fileIdentifier angegeben ist (Short File Identifier der zu bearbeitenden Datei) folder (Verzeichnis/Applikation auf der Karte, in dem sich die Datei befindet) pattern (SuchMuster) recordNumber – <i>optional; default = 1</i> (Recordnummer, bei der Suche beginnen soll) ()
Komponenten	Karte, Kartenterminal, Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> numbersFound (Liste: Nummern der Records, die dem SuchMuster entsprechen)

Standardablauf	<ol style="list-style-type: none"> 1. Ermittle Card = CM_CARD_LIST(cardSession) 2. Prüfe, dass der Karte entweder kein Lock zugeordnet ist oder der Aufrufer das Karten-Lock besitzt. 3. Prüfe PinRef/KeyRef in CARDSESSION.AUTHSTATE für adressierte Datei wie in Zugriffsbedingung der Karte definiert vorhanden 4. Selektiere Verzeichnis und ggf. Datei 5. Sende Kartenkommando „SEARCH RECORD“ mit SuchMuster <i>pattern</i> unter Berücksichtigung von recordNumber 6. Liefere Antwort der Karte zurück
Varianten/ Alternativen	Keine
Fehlerfälle	<p>* Karte antwortet nicht innerhalb von CARD_TIMEOUT_CARD-Sekunden, Fehlercode 4094 (→2) Karte ist fremd reserviert, Fehlercode 4093 (→3) Nötige PIN ist nicht verifiziert, Fehlercode 4085 (→4-5) Verzeichnis, Datei existiert nicht, Fehlercode 4087 (→5) Verzeichnis deaktiviert, Fehlercode 4086 (→4-5) Karte antwortet mit einer spezifischen Fehlermeldung, Fehlercode <Kartenfehlercode gemäß [gemSpec_COS]></p>
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

3240 **Tabelle 93: TAB_KON_542 Fehlercodes TUC_KON_215 „SucheRecord“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4085	Security	Error	Zugriffsbedingungen nicht erfüllt
4086	Technical	Error	Verzeichnis deaktiviert
4087	Technical	Error	Datei nicht vorhanden
4093	Technical	Error	Karte wird in einer anderen Kartensitzung exklusiv verwendet
4094	Technical	Error	Timeout beim Kartenzugriff aufgetreten

3241
3242
3243 [**<=**]

3244 4.1.5.4.17 TUC_KON_018 „eGK-Sperrung prüfen“

3245 TIP1-A_4579 - TUC_KON_018 „eGK-Sperrung prüfen“

3246 Der Konnektor MUSS den technischen Use Case „eGK-Sperrung prüfen“ gemäß

3247 TUC_KON_018 umsetzen.

3248

3249 **Tabelle 94: TAB_KON_110 - TUC_KON_018 „eGK-Sperrung prüfen“**

Element	Beschreibung
Name	TUC_KON_018 „eGK-Sperrung prüfen“
Beschreibung	Es wird geprüft, dass DF.HCA (Health Care Application) der eGK nicht gesperrt ist und optional, dass das AUT-Zertifikat im DF.ESIGN gültig ist. Für eine Karte ab der Generation G2.1 wird das AUT-Zertifikat (ECC) geprüft. Für eine Karte der Generation G2.0 wird das AUT-Zertifikat (RSA) geprüft.
Auslöser	Aufruf durch Fachmodul im Konnektor
Vorbedingungen	keine
Eingangsdaten	<ul style="list-style-type: none"> cardSession checkHcaOnly [Boolean] - <i>optional; default = false</i> (Prüfung auf die Frage beschränken, ob auf DF.HCA zugegriffen werden kann)
Komponenten	Konnektor, Kartenterminal, eGK
Ausgangsdaten	<ul style="list-style-type: none"> Karte gesperrt: true false Status – <i>optional/wenn checkHcaOnly = false</i> <ul style="list-style-type: none"> DF.HCA gesperrt: true false Ergebnis der Offline-Prüfung des C.CH.AUT-Zertifikats: gültig ungültig Sperrstatus des C.CH.AUT-Zertifikats: gut gesperrt nicht ermittelbar
Standardablauf	<ol style="list-style-type: none"> 1. Ermittle Card = CM_CARD_LIST(cardSession) 2. Prüfe, dass der Karte entweder kein Lock zugeordnet ist oder der Aufrufer das Karten-Lock besitzt. 3. Selektiere DF.HCA : <ol style="list-style-type: none"> a. Wenn die Karte '90 00' zurückmeldet, war das Selektieren möglich: DF.HCA gesperrt = false b. In allen anderen Fällen war das Selektieren nicht fehlerfrei möglich: DF.HCA gesperrt = true 4. Wenn checkHcaOnly = true Beende TUC, liefere Status. 5. Ermittle Zertifikatsobjekt (fileIdentifier und folder) für C.AUT der Karte unter Berücksichtigung des kryptographischen Verfahrens crypt

	<p>gemäß TAB_KON_858. Für eine Karte ab der Generation G2.1 setze crypt=ECC. Für eine Karte der Generation G2.0 setze crypt=RSA. Rufe Cert = TUC_KON_216 „LeseZertifikat“ {cardSession; fileIdentifier; folder}</p> <p>6. Bestimme per Aufruf von TUC_KON_037 „Zertifikat prüfen“</p> <p>a. das Ergebnis der Offline-Prüfung des C.CH.AUT-Zertifikats (gültig ungültig) sowie</p> <p>b. den Sperrstatus des C.CH.AUT-Zertifikats (gut gesperrt nicht ermittelbar).</p> <p>7. Die Karte ist gesperrt = true, wenn</p> <p>a. DF.HCA gesperrt = true oder</p> <p>b. Ergebnis der Offline-Prüfung des C.CH.AUT-Zertifikats = ungültig oder</p> <p>c. Sperrstatus des C.CH.AUT-Zertifikats = gesperrt.</p> <p>In allen anderen Fällen ist die Karte gesperrt = false.</p>
Varianten/ Alternativen	keine
Fehlerfälle	(→2) Karte ist fremd reserviert, Fehlercode 4093
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

3250 **Tabelle 95: TAB_KON_239 Fehlercodes TUC_KON_018 „eGK-Sperrung prüfen“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4093	Technical	Error	Karte wird in einer anderen Kartensitzung exklusiv verwendet

3251
3252 **[<=]**

3253 **4.1.5.4.18 TUC_KON_006 „Datenzugriffsaudit eGK schreiben“**

3254 TIP1-A_4580 - TUC_KON_006 „Datenzugriffsaudit eGK schreiben“

3255 Der Konnektor MUSS den technischen Use Case „Datenzugriffsaudit eGK schreiben“
3256 gemäß TUC_KON_006 umsetzen.

3257

3258

Tabelle 96: TAB_KON_108 - TUC_KON_006 „Datenzugriffsaudit eGK schreiben“

Element	Beschreibung
Name	TUC_KON_006 „Datenzugriffsaudit eGK schreiben“
Beschreibung	Zugriff auf eGK in EF.Logging protokollieren.
Auslöser	Aufruf durch ein Fachmodul
Vorbedingungen	Keine
Eingangsdaten	<ul style="list-style-type: none"> cardSession (CardSession einer eGK) sourceCardSession (HBA/SMC-B, der/die für den eGK-Zugriff verwendet wird) dataType (zugreifende Anwendung, siehe [gem_Spec_Karten_Fach_TIP#4.1 – Tabelle Tab_Karten_Fach_TIP_010 _StrukturEF.Logging – Struktur der Rekords der Datei EF.Logging]) accessType (Zugriffsart, siehe ebenda)
Komponenten	eGK, HBA/SMC, Konnektor, Kartenterminal
Ausgangsdaten	Keine
Standardablauf	<ol style="list-style-type: none"> 1. Ermittle Card = CM_CARD_LIST(cardSession) 2. Prüfe Card.TYPE = EGK 3. Prüfe, dass der Karte entweder kein Lock zugeordnet ist oder der Aufrufer das Karten-Lock besitzt. 4. Wenn KeyRef in CARDESESSION.AUTHSTATE für DF.HCA.EF.LOGGING nicht mit passender Rolle vorhanden: Rufe TUC_CON_005 „Card-to-Card authentisieren“ { sourceCardSession; targetCardSession = cardSession; authMode = einseitig} 5. Erzeuge Loggingdaten gemäß [gem_Spec_Karten_Fach_TIP#4.1 – Tabelle Tab_Karten_Fach_TIP_010 _StrukturEF.Logging – Struktur der Rekords der Datei EF.Logging] 6. Rufe TUC_KON_214 „FügeHinzRecord“ { cardSession = \$cardSession; folder = MF; fileIdentifier = DF.HCA/EF.Logging; dataToBeWritten = Loggingdaten }
Varianten/ Alternativen	Keine
Fehlerfälle	(→2) Protokoll nur für eGK gestattet, Fehlercode 4251 (→3) Karte ist fremd reserviert, Fehlercode 4093

Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

Tabelle 97: TAB_KON_238 Fehlercodes TUC_KON_006 „Datenzugriffsaudit eGK schreiben“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4093	Technical	Error	Karte wird in einer anderen Kartensitzung exklusiv verwendet
4251	Technical	Error	Protokoll nur für eGK gestattet

[<=]

4.1.5.4.19 TUC_KON_218 „Signiere“

TIP1-A_4581 - TUC_KON_218 „Signiere“

Der Konnektor MUSS den technischen Use Case „Signiere“ gemäß TUC_KON_218 umsetzen.

Tabelle 98: TAB_KON_231 – TUC_KON_218 „Signiere“

Element	Beschreibung
Name	TUC_KON_218 „Signiere“
Beschreibung	Dieser Use Case beschreibt das Anwenden eines privaten Schlüssels einer Karte zur Signatur oder Authentisierung.
Auslöser	<ul style="list-style-type: none"> Aufruf einer der Operationen SignDocument des Signaturdienstes oder ExternalAuthenticate des Authentifizierungsdienstes durch das Clientsystem. Aufruf durch Fachmodul
Vorbedingungen	Zugriffsbedingung für referenzierten Schlüssel MUSS erfüllt sein

Eingangsdaten	<ul style="list-style-type: none"> • cardSession • pinRef (PIN-Referenz, gemäß der Objektsystem-Spezifikation des jeweiligen Kartentyps) • keyRef (Referenz auf den privaten Schlüssel, mit dem signiert werden soll, gemäß der Objektsystem-Spezifikation des jeweiligen Kartentyps) • algorithmusId (einer der laut Objektspezifikation für diesen Schlüssel zulässigen algorithmIdentifier) • dataToBeSigned (Zu signierende Daten, Hashwert)
Komponenten	Karte, Kartenterminal, Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> • chiffrat (Signatur)
Standardablauf	<ol style="list-style-type: none"> 1. Ermittle Card = CM_CARD_LIST(cardSession) 2. Prüfe, dass der Karte entweder kein Lock zugeordnet ist oder der Aufrufer das Karten-Lock besitzt. 3. Prüfe pinRef in CARDESESSION.AUTHSTATE vorhanden: 4. Setze keyRef und algorithmusId der Karte 5. Sende „PSO: COMPUTE DS“ mit dataToBeSigned an Karte 6. Gib chiffrat an den Aufrufer zurück
Varianten/ Alternativen	Keine
Fehlerfälle	<p>* Karte antwortet nicht innerhalb von CARD_TIMEOUT_CARD Sekunden, Fehlercode 4094 (→2) Karte ist fremd reserviert, Fehlercode 4093 (→3) Nötige PIN ist nicht verifiziert, Fehlercode 4085 (→5) Karte antwortet mit einer spezifischen Fehlermeldung, Fehlercode <Kartenfehlercode gemäß [gemSpec_COS]></p>
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

3269 **Tabelle 99: TAB_KON_543 Fehlercodes TUC_KON_218 „Signiere“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4085	Security	Error	Zugriffsbedingungen nicht erfüllt
4093	Technical	Error	Karte wird in einer anderen Kartensitzung exklusiv verwendet
4094	Technical	Error	Timeout beim Kartenzugriff aufgetreten

3270
3271
3272

[<=]

3273 **4.1.5.4.20 TUC_KON_219 „Entschlüssele“**

3274 TIP1-A_4582 - TUC_KON_219 „Entschlüssele“

3275 Der Konnektor MUSS den technischen Use Case „Entschlüssele“ gemäß TUC_KON_219
3276 umsetzen.

3277 **Tabelle 100: TAB_KON_232 – TUC_KON_219 „Entschlüssele“**

Element	Beschreibung
Name	TUC_KON_219 „Entschlüssele“
Beschreibung	Dieser Use Case beschreibt das Anwenden eines privaten Schlüssels einer Karte zur Entschlüsselung.
Auslöser	<ul style="list-style-type: none"> Aufruf durch Fachmodul
Vorbedingungen	Zugriffsbedingung für referenzierten Schlüssel muss erfüllt sein
Eingangsdaten	<ul style="list-style-type: none"> cardSession pinRef (Referenz auf die PIN, mit der der Entschlüsselungsschlüssel freigeschaltet werden kann, gemäß der Objektsystem-Spezifikation des jeweiligen Kartentyps) keyRef (Referenz auf den privaten Schlüssel, mit dem entschlüsselt werden soll, gemäß der Objektsystem-Spezifikation des jeweiligen Kartentyps.) algorithmusId (einer der für diesen Schlüssel zulässigen algorithmIdentifizier) encryptedData (Zu entschlüsselnde Daten, Chiffrat)
Komponenten	Karte(n), Kartenterminal, Konnektor

Ausgangsdaten	<ul style="list-style-type: none"> plainData (Entschlüsselte Daten)
Standardablauf	<ol style="list-style-type: none"> 1. Ermittle Card = CM_CARD_LIST(cardSession) 2. Prüfe, dass der Karte entweder kein Lock zugeordnet ist oder der Aufrufer das Karten-Lock besitzt. 3. Prüfe pinRef in CARDESESSION.AUTHSTATE vorhanden: 4. Selektiere DF, in dem der private Schlüssel (keyRef) liegt, falls er noch nicht selektiert ist. 5. Setze Schlüssel (keyRef) und algorithmusId. 6. Sende encryptedData mittels Kommandos PSO: DECIPHER. 7. gib plainData an den Aufrufer zurück
Varianten/ Alternativen	Keine
Fehlerfälle	<p>* Karte antwortet nicht innerhalb von CARD_TIMEOUT_CARD Sekunden, Fehlercode 4094 (→2) Karte ist fremd reserviert, Fehlercode 4093 (→3) Nötige PIN ist nicht verifiziert, Fehlercode 4085 (→5) Schlüssel nicht vorhanden, Fehlercode 4079 (→6) Fehler im Chifftrat: Fehlercode 4069 (→4, 6) Karte antwortet mit einer spezifischen Fehlermeldung, Fehlercode <Kartenfehlercode gemäß [gemSpec_COS]></p>
Varianten/ Alternativen	Keine
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

3278

Tabelle 101: TAB_KON_210 Fehlercodes TUC_KON_219 „Entschlüssele“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4069	Technical	Error	korruptes Chifftrat bei asymmetrischer Entschlüsselung
4079	Technical	Error	Schlüsseldaten fehlen
4085	Security	Error	Zugriffsbedingungen nicht erfüllt

4093	Technical	Error	Karte wird in einer anderen Kartensitzung exklusiv verwendet
4094	Technical	Error	Timeout beim Kartenzugriff aufgetreten

3279
3280
3281

[<=]

3282 4.1.5.4.21 TUC_KON_200 „SendeAPDU“

3283 TIP1-A_4583 - TUC_KON_200 „SendeAPDU“

3284 Der Konnektor MUSS den technischen Use Case „SendeAPDU“ gemäß TUC_KON_200
3285 umsetzen.

3286

3287 **Tabelle 102: TAB_KON_215 TUC_KON_200 „SendeAPDU“**

Element	Beschreibung
Name	TUC_KON_200 „SendeAPDU“
Beschreibung	Dieser Use Case beschreibt das Senden einer APDU an eine Chipkarte bzw. an ein Kartenterminal und das Empfangen der Antwort.
Auslöser	<ul style="list-style-type: none"> Aufruf durch Fachmodul
Vorbedingungen	Zugriffsbedingungen für das Kommando müssen in der Karte erfüllt sein und Karte muss für exklusiven Zugriff reserviert worden sein
Eingangsdaten	<ul style="list-style-type: none"> cardSession – <i>optional/verpflichtend</i>, wenn die APDU an die Karte gerichtet ist ctId – <i>optional/verpflichtend</i>, wenn die APDU an das Kartenterminal gerichtet ist (Kartenterminalidentifikator für Kommandos an das Kartenterminal) commandAPDU (versandfertige APDU (Bytefolge), in dem die Parameter {CLA, INS, P1,P2, Data (<i>optional</i>) Le(<i>optional</i>) } gesetzt sind.)
Komponenten	Karte(n), Kartenterminal, Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> responseAPDU (Antwort der Chipkarte oder des Kartenterminals, Bytefolge)
Standardablauf	<p>A. cardSession ist gegeben</p> <ol style="list-style-type: none"> Ermittle Card = CM_CARD_LIST(cardSession) Prüfe, dass der Aufrufer für die zur cardSession gehörenden Karte ein Lock hat. commandAPDU wird über das Kartenterminal an die Zielkarte gesendet

	4. die Antwort (responseAPDU) der Zielkarte wird an den Aufrufer zurückgegeben. B. ctId ist gegeben 1. Sende commandAPDU an das Kartenterminal ctId 2. gib die Antwort responseAPDU des Kartenterminals an den Aufrufer zurück
Varianten/Alternativen	<ul style="list-style-type: none"> Soll Secure Messaging verwendet werden, MUSS vorher TUC_KON_023 „Karte reservieren“ aufgerufen werden
Fehlerfälle	* Karte antwortet nicht innerhalb von CARD_TIMEOUT_CARD Sekunden, Fehlercode 4094 (→2) Der Aufrufer ist nicht im Besitz des Karten-Locks, Fehlercode 4232 (→3) Kommunikationsfehler mit dem Kartenterminal: Fehlercode 4044. (→3) Karte antwortet mit einer spezifischen Fehlermeldung, Fehlercode <Kartenfehlercode gemäß [gemSpec_COS]>
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

Tabelle 103: TAB_KON_216 Fehlercodes TUC_KON_200 „SendeAPDU“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4044	Technical	Error	Fehler beim Zugriff auf das Kartenterminal
4094	Technical	Error	Timeout beim Kartenzugriff aufgetreten
4232	Technical	Error	der Aufrufer besitzt nicht das Karten-Lock

[<=]

4.1.5.4.22 TUC_KON_024 „Karte zurücksetzen“

TIP1-A_4584 - TUC_KON_024 „Karte zurücksetzen“

Der Konnektor MUSS den technischen Use Case „Karte zurücksetzen“ gemäß TUC_KON_024 umsetzen.

Tabelle 104: TAB_KON_737 – TUC_KON_024 „Karte zurücksetzen“

Element	Beschreibung
Name	TUC_KON_024 „Karte zurücksetzen“
Beschreibung	Der technische Use Case setzt die gewählte Karte zurück (alle erreichten Sicherheitszustände werden auf der Karte und in der

	Verwaltung des Konnektors zurückgesetzt; auf der Karte wird MF selektiert). Ein eventuell laufendes C2C wird dabei abgebrochen.
Auslöser	Fachmodul
Vorbedingungen	keine
Eingangsdaten	<ul style="list-style-type: none"> ctId – <i>optional/verpflichtend, wenn keine cardSession angegeben ist</i> (Kartenterminalidentifikator) slotId – <i>optional/verpflichtend, wenn keine cardSession angegeben ist</i> (Nummer des Slots, in dem die Karte steckt) cardSession – <i>optional/verpflichtend, wenn ctId und slotId nicht angegeben sind</i> (Angabe der CardSession alternativ zur Angabe von ctId und slotId)
Komponenten	Karte, Kartenterminal, Konnektor
Ausgangsdaten	Keine
Standardablauf	<ol style="list-style-type: none"> 1. Wenn cardSession gegeben, dann ermittle ctId und slotId 2. Der Konnektor prüft, dass entweder die Karte nicht reserviert ist oder der Aufrufer im Besitz des Karten-Locks ist. 3. Brich eventuell parallel laufenden TUC_KON_005 ab 4. Sende SICCT RESET ICC für slotId an das Kartenterminal CtID, um einen Warm Reset auszulösen 5. Lösche alle Sicherheitszustände aus CARDSESSION.AUTHSTATE und den Inhalt von CARDSESSION.AUTHBY.
Varianten/ Alternativen	Keine
Fehlerfälle	<p>* Karte antwortet nicht innerhalb von CARD_TIMEOUT_CARD Sekunden, Fehlercode 4094 (→2) Der Aufrufer ist nicht im Besitz des Karten-Locks, Fehlercode 4232 (→4) Karte antwortet mit einer spezifischen Fehlermeldung, Fehlercode <Kartenfehlercode gemäß [gemSpec_COS]></p>
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

3298

Tabelle 105: TAB_KON_544 Fehlercodes TUC_KON_024 „Karte zurücksetzen“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			

4094	Technical	Error	Timeout beim Kartenzugriff aufgetreten
4232	Technical	Error	der Aufrufer ist nicht im Besitz des Karten-Locks

3299

3300 [\leq]

3301 4.1.5.4.23 TUC_KON_216 „LeseZertifikat“

3302 TIP1-A_4585 - TUC_KON_216 „LeseZertifikat“

3303 Der Konnektor MUSS den technischen Use Case „LeseZertifikat“ gemäß TUC_KON_216
3304 umsetzen.

3305

3306 **Tabelle 106: TAB_KON_230 – TUC_KON_216 „LeseZertifikat“**

Element	Beschreibung
Name	TUC_KON_216 „LeseZertifikat“
Beschreibung	Dieser Use Case beschreibt das Lesen eines Zertifikates von einer Karte
Auslöser	<ul style="list-style-type: none"> • Aufruf der Operation ReadCardCertificate des Zertifikatsdienstes durch das Clientsystem. • Aufruf durch Fachmodul • Aufruf im Rahmen von technischen Use Cases der Basisdienste des Konnektors
Vorbedingungen	Keine
Eingangsdaten	<ul style="list-style-type: none"> • cardSession • fileIdentifizier – <i>optional/verpflichtend, wenn kein sfid angegeben ist</i> (FID der zu lesenden Datei) • sfid – <i>optional/verpflichtend, wenn kein fileIdentifizier angegeben ist</i> (Short File Identifier der zu lesenden Datei) • folder (Verzeichnis/Applikation auf der Karte, in dem sich das Zertifikat befindet)
Komponenten	Karte, Kartenterminal, Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> • certificate (gelesenes Zertifikat)

Standardablauf	<ol style="list-style-type: none"> 1. Ermittle Card = CM_CARD_LIST(cardSession) 2. Prüfe, dass der Karte entweder kein Lock zugeordnet ist oder der Aufrufer das Karten-Lock besitzt. 3. Prüfe CARDSESSION.AUTHSTATE für adressierte Datei wie in Zugriffsbedingung der Karte definiert vorhanden 4. Rufe TUC_KON_202 „LeseDatei“ { cardSession; fileIdentifier; folder } oder TUC_KON_202 „LeseDatei“ { cardSession; sfid; folder } 5. Das Zertifikat wird an den Aufrufer zurückgegeben.
Varianten/ Alternativen	Keine
Fehlerfälle	(→2) Karte ist fremd reserviert, Fehlercode 4093 (->4) Es wurde versucht, ein Zertifikat von der Karte zu lesen, welches auf der Karte nicht vorhanden ist (Fehlercode 4256). Hierbei kann es sich um ein fehlendes Zertifikatsobjekt (z.B. adressiertes ECC-Zertifikat auf HBA G2.0) oder ein leeres Zertifikatsobjekt (z.B. adressiertes ECC-Zertifikat auf gSMC-K G2.0, welches aber nicht personalisiert wurde) handeln.
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

3307 **Tabelle 107: TAB_KON_209 Fehlercodes TUC_KON_216 „LeseZertifikat“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4093	Technical	Error	Karte wird in einer anderen Kartensitzung exklusiv verwendet
4256	Technical	Warning	Zertifikat auf Karte nicht vorhanden

3308
3309 **[<=]**

3310 4.1.5.4.24 TUC_KON_036 „LiefereFachlicheRolle“

3311 TIP1-A_5478 - TUC_KON_036 „LiefereFachlicheRolle“

3312 Der Konnektor MUSS den technischen Use Case TUC_KON_036 „LiefereFachlicheRolle“
3313 umsetzen.
3314

3315 **Tabelle 108: TAB_KON_827 TUC_KON_036 „LiefereFachlicheRolle“**

Element	Beschreibung
Name	TUC_KON_036 „LiefereFachlicheRolle“
Beschreibung	Dieser TUC liefert die fachliche Rolle, die der OID aus dem X.509Zertifikat der gesteckten Karte zugeordnet ist. Es werden nur folgende Karten unterstützt: HBAX, SM-B, EGK, KVK Es werden nur die AUT-Zertifikate ausgelesen. Für eine Karte ab der Generation G2.1 wird das AUT-Zertifikat (ECC) geprüft. Für eine Karte der Generation G2.0 wird das AUT-Zertifikat (RSA) geprüft.
Auslöser	<ul style="list-style-type: none"> Aufruf durch ein Fachmodul oder eine Basisanwendung des Konnektors
Vorbedingungen	Keine
Eingangsdaten	<ul style="list-style-type: none"> cardSession
Komponenten	Konnektor, Karte
Ausgangsdaten	<ul style="list-style-type: none"> role (fachliche Rolle gemäß [gemSpec_PKI#Tab_PKI_254 Zugriffsprofile für eine Rollenauthentisierung])
Nachbedingungen	Keine
Standardablauf	<ol style="list-style-type: none"> Ermittle Card = CM_CARD_LIST(cardSession) Prüfe, dass der Karte entweder kein Lock zugeordnet ist oder der Aufrufer im Besitz des Karten-Locks ist. Wenn CARD.TYPE = KVK, dann setze fachliche Rolle = „Versicherter“ und springe zu Schritt 8. Ermittle <i>fileIdentifier</i> und folder des C.AUT-Zertifikates unter Berücksichtigung des kryptographischen Algorithmus crypt für die Karte, die durch die cardSession referenziert wird. Für eine Karte ab der Generation G2.1 setze crypt=ECC. Für eine Karte der Generation G2.0 setze crypt=RSA. Welches Zertifikat gelesen wird, ist in TAB_KON_858 beschrieben. Lies Zertifikat: Rufe TUC_KON_216 "LeseZertifikat" { cardSession; <i>fileIdentifier</i> = <i>fileIdentifier</i> (AUT-Zertifikat); folder = folder(AUT-Zertifikat)} Ermittle ProfessionOIDs aus Extension Admission des Zertifikates: Rufe TUC_PKI_009 „Rollenermittlung“ {certificate}

	<p>7. Ermittle die fachliche Rolle, die den ProfessionOIDs entspricht, gemäß [gemSpec_PKI# Tab_PKI_254 Zugriffsprofile für eine Rollenauthentisierung].</p> <p>8. Rückgabe \$role (fachliche Rolle) an den Aufrufer</p>
Varianten/ Alternativen	Keine
Fehlerfälle	<p>* Karte antwortet nicht innerhalb von CARD_TIMEOUT_CARD Sekunden, Fehlercode 4094 (→2) Karte ist fremd reserviert, Fehlercode 4093 (→7) ProfessionOIDs mappen nicht auf die gleiche Rolle, Fehlercode 4210</p>
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

Tabelle 109: TAB_KON_829 Fehlercodes TUC_KON_036 „LiefereFachlicheRolle“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4093	Technical	Error	Karte wird in einer anderen Kartensitzung exklusiv verwendet
4094	Technical	Error	Timeout beim Kartenzugriff aufgetreten
4210	Technical	Error	ProfessionOIDs nicht eindeutig auf eine Rolle abbildbar

[<=]

4.1.5.5 Operationen an der Außenschnittstelle

TIP1-A_4586 - Basisanwendung Kartendienst

Der Konnektor MUSS für Clients eine Basisanwendung Kartendienst mit den Operationen VerifyPin, ChangePin, UnblockPin, GetPinStatus an der Außenschnittstelle anbieten.

Tabelle 110: TAB_KON_038 Basisanwendung Karten- und Kartenterminaldienst

Name	CardService
Version (KDV)	<p>8.1.0 (WSDL- und XSD-Version) 8.1.1 (WSDL- und XSD-Version) 8.1.2 (WSDL-Version) 8.1.3 (XSD-Version) Siehe Anhang D (WSDL-Version)</p>

Namensraum	Siehe Anhang D	
Namensraum-Kürzel	CARD für Schema und CARDW für WSDL	
Operationen	Name	Kurzbeschreibung
	VerifyPin	PIN prüfen
	ChangePin	PIN ändern
	UnblockPin	PIN entsperren
	GetPinStatus	PIN-Status ermitteln
	EnablePin	Erfordernis der PIN-Verifikation einschalten
	DisablePin	Erfordernis der PIN-Verifikation abschalten
WSDL	CardService.wsdl	
Schema	CardService.xsd	

3327

3328 [**<=**]3329 4.1.5.5.1 *VerifyPin*

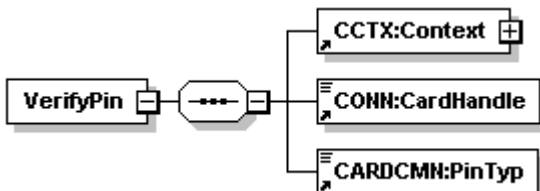
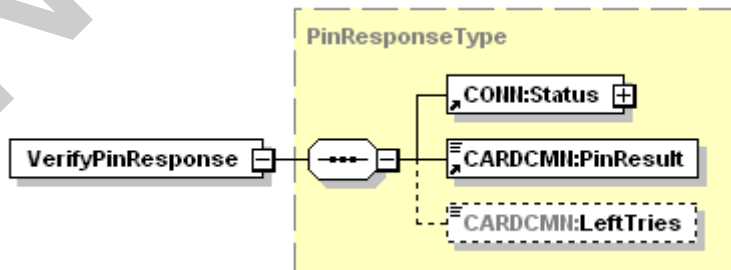
3330 TIP1-A_4587 - Operation VerifyPin

3331 Der Konnektor MUSS an der Außenschnittstelle eine Operation VerifyPin, wie in Tabelle
 3332 TAB_KON_047 Operation VerifyPin beschrieben, anbieten.

3333

3334 **Tabelle 111: TAB_KON_047 Operation VerifyPin**

Name	VerifyPin
Beschreibung	<p>Stößt die sichere Eingabe einer PIN am PIN-Pad des Kartenterminals für eine Karte an.</p> <p>Das Ergebnis der PIN-Prüfung gibt Auskunft darüber, ob die PIN richtig oder falsch war oder aufgrund zu vieler Fehlversuche blockiert ist.</p> <p>Eine Karte kann potentiell mehrere PINs haben. Insbesondere für die qualifizierte elektronische Signatur existiert eine separate PIN. Diese PIN darf nur über das PIN-Pad eingegeben werden. Die PIN-Verifikation und die damit verbundene Änderung des Sicherheitsstatus der Karte erfolgt nur für die durch den Aufrufkontext adressierte Kartensitzung. Falls die Karte in einem zentralen Kartenterminal steckt, auf das der Arbeitsplatz Zugriff hat, erfolgt eine Remote-PIN-Eingabe. Das Kartenterminal für die PIN-Eingabe ergibt sich dabei aus der im Aufrufkontext angegebenen Mandanten-ID und Arbeitsplatz-ID</p> <p>Diese Operation entspricht dem Aufruf von TUC_KON_012 „PIN verifizieren“. Dort sind auch die Display Messages definiert, die bei PIN-Eingabe am Kartenterminal anzuzeigen sind (TAB_KON_090 Terminalanzeigen beim Eingeben der PIN am Kartenterminal). Die beim Aufruf von TUC_KON_012 anzugebende PIN-Art lautet „mandatorisch“. Die PIN-Verifikation</p>

	wird also unabhängig vom erreichten Sicherheitsstatus in der Karte immer durchgeführt.		
Aufrufparameter			
	Name	Beschreibung	
	Context	MandantId, CsId, WorkplaceId verpflichtend; UserId verpflichtend für HBAX	
	CardHandle	Adressiert die Karte, für die die PIN verifiziert werden soll. Die Operation DARF die PIN-Verifikation mit der eGK NICHT unterstützen. Unterstützt werden die Kartentypen HBAX und SM-B. Wird die Operation mit einem nicht unterstützten Kartentypen aufgerufen, so MUSS der Konnektor die Bearbeitung mit dem Fehler 4209 abbrechen.	
	PinTyp	Gibt an, welche PIN der Karte verifiziert werden soll. Erlaubte Belegung von PinTyp in Abhängigkeit der durch Cardhandle referenzierten Karte: <ul style="list-style-type: none">• HBAX: PIN.CH• SM-B: PIN.SMC	
Rückgabe			
	Name	Beschreibung	
	Status	Enthält den Ausführungsstatus der Operation (siehe 3.5.2)	
	PinResult	Wert	Bedeutung
		OK	Prüfung war erfolgreich
	REJECTED	PIN war falsch. Die Anzahl der verbleibenden Versuche ist im Element LeftTries	

		ERROR	Ein Bearbeitungsfehler ist aufgetreten. Fehlerursache im Feld <code>Error</code>
		WASBLOCKED	PIN war zum Aufrufzeitpunkt bereits gesperrt
		NOWBLOCKED	PIN ist durch aktuellen Fehlversuch gesperrt
		TRANSPORT _PIN	PIN ist mit Transportschutz versehen
	LeftTries	Im Falle von <code>Result=REJECTED</code> wird hier die Anzahl der verbleibenden möglichen Versuche zurückgegeben.	
Vorbedingung	Keine		
Nachbedingung	keine		

3335 Der Ablauf der Operation VerifyPin ist in Tabelle TAB_KON_738 Ablauf VerifyPin
 3336 beschrieben.
 3337

3338 **Tabelle 112: TAB_KON_738 Ablauf VerifyPin**

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	TUC_KON_000 „Prüfe Zugriffs-berechtigung“	Prüfung der Zugriffsberechtigung durch den Aufruf TUC_KON_000 { mandantId = \$context.mandantId; clientSystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; userId = \$context.userId; cardHandle } Tritt bei der Prüfung ein Fehler auf, bricht die Operation mit Fehlercode aus TUC_KON_000 ab.
3.	TUC_KON_026 „Liefere CardSession“	Ermittle cardSession über TUC_KON_026 { mandatId = \$context.mandantId; clientsystemId = \$context.clientsystemId; userId = \$context.userId; cardHandle }
4.	TUC_KON_012 „PIN verifizieren“	Verifiziere PIN über TUC_KON_012 { cardSession; workplaceId = \$context.workplaceId;

		pinRef = PinRef(PinTyp); appName = „“ (Leerstring); verificationType = Mandatorisch }
5.	Verifikationsergebnis auswerten	Wenn TUC_KON_012 mit Fehler 4065 abbricht, wird dies als erfolgreicher Operationsdurchlauf mit PinResult= TRANSPORT_PIN abgefangen. Wenn TUC_KON_012 den Returncode BLOCKED liefert, wird dies als erfolgreicher Operationsdurchlauf mit PinResult= NOWBLOCKED zurückgegeben. Wenn TUC_KON_012 mit Fehler 4063 abbricht, wird dies als erfolgreicher Operationsdurchlauf mit PinResult= WASBLOCKED zurückgegeben

 3339 **Tabelle 113: TAB_KON_545 Fehlercodes „VerifyPin“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler
4078	Security	Error	PIN-Eingabe über das Clientsystem ist nicht zugelassen
4209	Technical	Error	Kartentyp %CardType% wird durch diese Operation nicht unterstützt.

 3340
 3341
 3342 **[<=]**

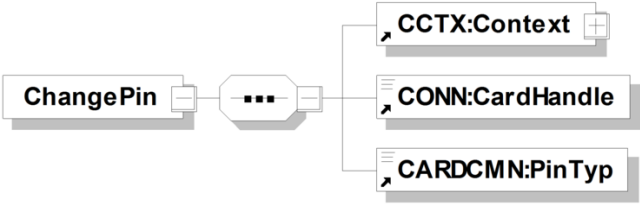
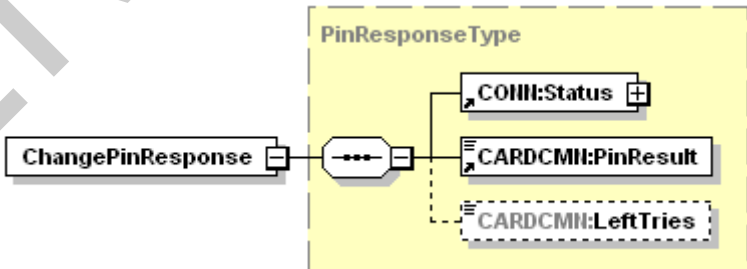
 3343 **4.1.5.5.2 ChangePin**

3344 TIP1-A_4588 - Operation ChangePin

 3345 Der Konnektor MUSS an der Außenschnittstelle eine Operation ChangePin, wie in Tabelle
 3346 TAB_KON_049 Operation ChangePin beschrieben, anbieten.

 3347 **Tabelle 114: TAB_KON_049 Operation ChangePin**

Name	ChangePin
Beschreibung	Ändert eine PIN einer Karte. Alte und neue PIN werden dabei am PIN-Pad des Kartenterminals eingegeben. Falls die Karte in einem zentralen Kartenterminal steckt, auf das der im Aufrufkontext angegebene Arbeitsplatz Zugriff hat, erfolgt eine Remote-PIN-Eingabe. Diese Operation entspricht dem Aufruf TUC_KON_019 „PIN ändern“ .

Aufrufparameter		
	Name	Beschreibung
	Context	MandantId, CsId, WorkplaceId verpflichtend; UserId optional (verpflichtend beim HBA)
	CardHandle	Adressiert die Karte, für die die PIN geändert werden soll. Unterstützt werden die Kartentypen EGK, HBAX und SM-B. Wird die Operation mit einem nicht unterstützten Kartentypen aufgerufen, so MUSS der Konnektor die Bearbeitung mit dem Fehler 4209 abbrechen.
	PinTyp	<p>Gibt an, welche PIN der Karte geändert werden soll.</p> <p>Erlaubte Belegung von PinTyp in Abhängigkeit der durch CardHandle referenzierten Karte:</p> <ul style="list-style-type: none"> • eGK G1+: PIN.CH, • eGK G2: PIN.CH, MRPIN.NFD, MRPIN.NFD_READ, MRPIN.DPE, MRPIN.GDD, MRPIN.OSE, MRPIN.AMTS, PIN.AMTS_REP • zusätzlich eGK G2.0: MRPIN.DPE_READ • HBAX: PIN.CH, PIN.QES • SM-B: PIN.SMC
Rückgabe		
	Name	Beschreibung
	LeftTries	Im Falle von REJECTED wird hier die Anzahl der verbleibenden möglichen Versuche zurückgegeben.
	Status	Enthält den Ausführungsstatus der Operation, siehe 3.5.2

	PinResult	Wert	Bedeutung
		OK	PIN-Änderung war erfolgreich
		ERROR	Ein Bearbeitungsfehler ist aufgetreten. Fehlerursache im Feld <code>Error</code>
		REJECTED	OldPIN war falsch Die Anzahl der verbleibenden Versuche ist im Element <code>LeftTries</code>
		WASBLOCKED	PIN war zum Aufrufzeitpunkt bereits gesperrt
		NOWBLOCKED	PIN ist durch aktuellen Fehlversuch gesperrt
Vorbedingung	Keine		
Nachbedingung	keine		

3348 **Tabelle 115: TAB_KON_546 Ablauf ChangePin**

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	TUC_KON_000 „Prüfe Zugriffs- berechtigung“	Prüfung der Zugriffsberechtigung durch den Aufruf TUC_KON_000 { mandantId = \$context.mandantId; clientSystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; userId = \$context.userId; cardHandle } Tritt bei der Prüfung ein Fehler auf, bricht die Operation mit Fehlercode aus TUC_KON_000 ab.
3.	TUC_KON_026 „Liefere CardSession“	Ermittle cardSession über TUC_KON_026 { mandantId = \$context.mandantId; clientsystemId = \$context.clientsystemId; cardHandle; userId = \$context.userId }

4.	TUC_KON_019 „PIN ändern“	Ändere PIN über TUC_KON_019 { cardSession; workplaceId = \$context.workplaceId; pinRef = PinRef(PinTyp) }
5.	Verifikationsergebnis auswerten	Wenn TUC_KON_019 den Returncode BLOCKED liefert, wird dies als erfolgreicher Operationsdurchlauf mit PinResult= NOWBLOCKED zurückgegeben. Wenn TUC_KON_019 mit Fehler 4063 abbricht, wird dies als erfolgreicher Operationsdurchlauf mit PinResult= WASBLOCKED zurückgegeben.

Tabelle 116: TAB_KON_547 Fehlercodes „ChangePin“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler
4072	Technical	Error	Ungültige PIN-Referenz <code>PinRef</code>
4209	Technical	Error	Kartentyp <code>%CardType%</code> wird durch diese Operation nicht unterstützt.

[<=]

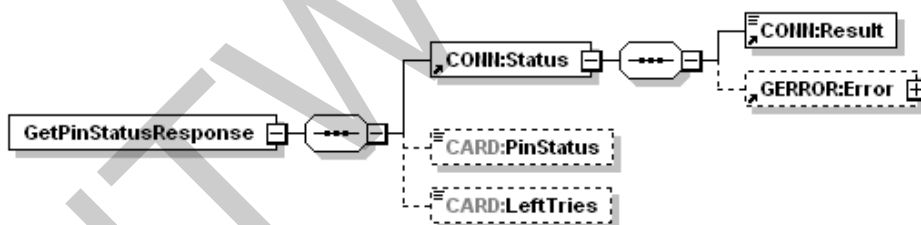
4.1.5.5.3 *GetPinStatus*

TIP1-A_4589 - Operation GetPinStatus

Der Konnektor MUSS an der Außenschnittstelle eine Operation GetPinStatus, wie in Tabelle TAB_KON_051 Operation GetPinStatus beschrieben, anbieten.

Tabelle 117: TAB_KON_051 Operation GetPinStatus

Name	GetPinStatus	
Beschreibung	<p>Diese Operation gibt Auskunft über den PIN-Zustand einer Karte. Für transportgeschützte PIN gibt die Operation die Art des Transportschutzes an.</p> <p>Für Echt-PINs kann mit dieser Operation die Anzahl der noch verbleibenden Versuche für PIN-Verifikationen ermittelt werden oder ob die PIN bereits verifiziert wurde.</p>	
Aufrufparameter	<pre> sequenceDiagram participant Caller participant GetPinStatus participant Params as ... participant CCTX as CCTX:Context participant CONN as CONN:CardHandle participant CARDCMN as CARDCMN:PinTyp Caller->>GetPinStatus Params->>GetPinStatus CCTX->>GetPinStatus CONN->>GetPinStatus CARDCMN->>GetPinStatus </pre>	
	Name	Beschreibung

	Context	MandantId, CsId, WorkplaceId; UserId	
	CardHandle	Adressiert die Karte, für die der PIN-Status ermittelt werden soll. Unterstützt werden die Kartentypen EGK, HBax und SM-B. Eine KVK ist nicht zulässig. Wird die Operation mit einem nicht unterstützten Kartentypen aufgerufen, so MUSS der Konnektor die Bearbeitung mit dem Fehler 4209 abbrechen.	
	PinTyp	Gibt an, für welche PIN der Karte der PIN-Status ermittelt werden soll. Erlaubte Belegung von PinTyp in Abhängigkeit der durch Cardhandle referenzierten Karte: <ul style="list-style-type: none">• eGK G1+: PIN.CH• eGK G2: PIN.CH, MRPIN.NFD, MRPIN.NFD_READ, MRPIN.DPE, MRPIN.GDD, MRPIN.OSE, MRPIN.AMTS, PIN.AMTS_REP• zusätzlich eGK G2.0: MRPIN.DPE_READ• HBax: PIN.CH, PIN.QES• SM-B: PIN.SMC	
Rückgabe			
	Name	Beschreibung	
	Status	Enthält den Ausführungsstatus der Operation siehe 3.5.2	
	PinStatus	Status der PIN. Die folgenden Werte sind verpflichtend:	
		Wert	Bedeutung
		VERIFIED	Bereits verifiziert (in CARDSESSION.AUTHSTATE vorhanden)
		TRANSPORT_PIN	Transport-PIN
		EMPTY_PIN	Leer-PIN
BLOCKED		gesperrt	
VERIFIABLE		Echt-PIN, noch nicht verifiziert	

		DISABLED	PIN-Schutz ausgeschaltet (Verifikation nicht erforderlich)
	LeftTries	Bei einer Echt-PIN wird hier bei PinStatus = VERIFIABLE die Anzahl der verbleibenden möglichen Versuche für die Verifikation der PIN zurückgegeben, bei einer gesperrten PIN 0.	
Vorbedingung	keine		
Nachbedingung	keine		

3359 **Tabelle 118: TAB_KON_548 Ablauf GetPinStatus**

Nr .	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	TUC_KON_000 „Prüfe Zugriffsberechtigung“	Prüfung der Zugriffsberechtigung durch den Aufruf TUC_KON_000 { mandantId = \$context.mandantId; clientSystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; userId = \$context.userId; // falls angegeben cardHandle } Tritt bei der Prüfung ein Fehler auf, so bricht die Operation mit dem Fehlercode aus TUC_KON_000 ab.
3.	TUC_KON_026 „Liefere CardSession“	Ermittle cardSession über TUC_KON_026 { mandantId = \$context.mandantId; clientSystemId = \$context.clientsystemId; userId = \$context.userId; // falls angegeben ; cardHandle }
4.	TUC_KON_022 „Liefere PIN-Status“	Ermittle PinStatus über TUC_KON_022 { cardSession; pinRef = PinRef(PinTyp) }

3360 **Tabelle 119: TAB_KON_549 Fehlercodes „GetPinStatus“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			

4000	Technical	Error	Syntaxfehler
4001	Technical	Error	interner Fehler
4072	Technical	Error	ungültige PIN-Referenz <code>PinRef</code>
4209	Technical	Error	Kartentyp <code>%CardType%</code> wird durch diese Operation nicht unterstützt.

3361
3362
3363

[<=]

3364 4.1.5.5.4 UnblockPin

3365 TIP1-A_4590 - Operation UnblockPin

3366 Der Konnektor MUSS an der Außenschnittstelle eine Operation UnblockPin, wie in Tabelle
3367 TAB_KON_053 Operation UnblockPin beschrieben, anbieten.

3368

3369 **Tabelle 120: TAB_KON_053 Operation UnblockPin**

Name	UnblockPin						
Beschreibung	<p>Mit diesem Kommando kann eine blockierte PIN wieder freigeschaltet werden. Dabei wird der Wiederholungszähler für diese PIN in der Karte auf seinen Anfangswert zurückgesetzt und es KANN eine neue PIN gesetzt werden. Um diese Aktion durchführen zu können, muss eine PUK (auch als Resetting Code bezeichnet) präsentiert werden.</p> <p>PIN und PUK werden am PIN-Pad des Kartenterminals eingegeben. Falls die Karte in einem zentralen Kartenterminal steckt, auf das der im Aufrufkontext angegebene Arbeitsplatz Zugriff hat, erfolgt eine Remote-PIN-Eingabe. Das Kartenterminal für die PIN-Eingabe ergibt sich dabei aus der im Aufrufkontext angegebenen Mandanten-ID und Arbeitsplatz-ID.</p> <p>Diese Operation entspricht dem Aufruf von TUC_KON_021 „PIN entsperren“.</p>						
Aufruf- parameter	<pre> sequenceDiagram participant UnblockPin UnblockPin->>CCTX:Context CCTX:Context->>CONN:CardHandle CONN:CardHandle->>CARDCMN:PinTyp CARDCMN:PinTyp-->>CARD:SetNewPin style CARD:SetNewPin stroke-dasharray: 5 5 </pre> <table> <thead> <tr> <th>Name</th><th>Beschreibung</th></tr> </thead> <tbody> <tr> <td>Context</td><td>MandantId, CsId, WorkplaceId verpflichtend; UserId (optional, für HBA verpflichtend)</td></tr> <tr> <td>CardHandle</td><td>Adressiert die Karte, für die die Blockierung der PIN aufgehoben werden soll. Unterstützt werden die Kartentypen EGK, HBAX und SM-B. Wird die Operation mit einem nicht unterstützten</td></tr> </tbody> </table>	Name	Beschreibung	Context	MandantId, CsId, WorkplaceId verpflichtend; UserId (optional, für HBA verpflichtend)	CardHandle	Adressiert die Karte, für die die Blockierung der PIN aufgehoben werden soll. Unterstützt werden die Kartentypen EGK, HBAX und SM-B. Wird die Operation mit einem nicht unterstützten
Name	Beschreibung						
Context	MandantId, CsId, WorkplaceId verpflichtend; UserId (optional, für HBA verpflichtend)						
CardHandle	Adressiert die Karte, für die die Blockierung der PIN aufgehoben werden soll. Unterstützt werden die Kartentypen EGK, HBAX und SM-B. Wird die Operation mit einem nicht unterstützten						

		Kartentypen aufgerufen, so MUSS der Konnektor die Bearbeitung mit dem Fehler 4209 abbrechen.	
	PinTyp	<p>Gibt an, für welche PIN der Karte die Blockierung aufgehoben werden soll.</p> <p>Erlaubte Belegung von PinTyp in Abhängigkeit der durch Cardhandle referenzierten Karte:</p> <ul style="list-style-type: none">- eGK G1+: PIN.CH- eGK G2: PIN.CH, MRPIN.NFD, MRPIN.NFD_READ, MRPIN.DPE, MRPIN.GDD, MRPIN.OSE, MRPIN.AMTS, PIN.AMTS_REP- zusätzlich eGK G2.0: MRPIN.DPE_READ- HBAX: PIN.CH, PIN.QES- SM-B: PIN.SMC	
	SetNewPin	<p>Dieses Flag zeigt an, ob eine neue PIN gesetzt werden soll. Wird dieses Flag nicht angegeben, so wird FALSE angenommen.</p> <p>Das Flag ist notwendig, um bei Eingabe am PIN-Pad eindeutig festzulegen, ob eine neue PIN gesetzt werden soll.</p>	
Rückgabe			
	Name	Beschreibung	
	LeftTries	Im Falle von REJECTED wird hier die Anzahl der verbleibenden möglichen Versuche für die Eingabe der PUK zurückgegeben.	
	Status	Enthält den Ausführungsstatus der Operation siehe 3.5.2	
	PinResult	Wert	Bedeutung
		OK	Prüfung war erfolgreich.
ERROR		Ein Bearbeitungsfehler ist aufgetreten. Fehlerursache im Feld Error.	
	REJECTED	PUK war falsch. Die Anzahl der verbleibenden Versuche ist im Element LeftTries.	

		WASBLOCKED	PUK war zum Aufrufzeitpunkt bereits gesperrt
		NOWBLOCKED	PUK ist durch aktuellen Fehlversuch gesperrt
Vorbedingungen	keine		
Nachbedingungen	keine		

3370

Tabelle 121: TAB_KON_550 Ablauf UnblockPIN

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	TUC_KON_000 „Prüfe Zugriffsberechtigung“	Prüfung der Zugriffsberechtigung durch den Aufruf TUC_KON_000 { mandantId = \$context.mandantId; clientSystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; userId = \$context.userId; // falls angegeben cardHandle }
3.	TUC_KON_026 „Liefere CardSession“	Ermittle cardSession über TUC_KON_026 { mandantId = \$context.mandantId; clientSystemId = \$context.clientsystemId; userId = \$context.userId; // falls angegeben cardHandle }
4.	TUC_KON_021 „PIN entsperren“	Rücksetzen des Fehlbedienungszählers über TUC_KON_021 { cardSession; workplaceId = \$context.workplaceId; pinRef = pinRef(PinTyp); setNewPIN = SetNewPIN }
5.	Verifikationsergebnis auswerten	Wenn TUC_KON_021 den Returncode BLOCKED liefert, wird dies als erfolgreicher Operationsdurchlauf mit PinResult= NOWBLOCKED zurückgegeben. Wenn TUC_KON_021 mit dem Fehlercode 4064 abbricht, wird dies als erfolgreicher Operationsdurchlauf mit PinResult= WASBLOCKED zurückgegeben.

3371 **Tabelle 122: TAB_KON_551 Fehlercodes „UnblockPin“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler
4209	Technical	Error	Kartentyp %CardType% wird durch diese Operation nicht unterstützt.

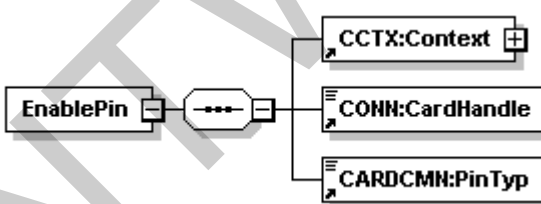
3372
3373
3374 [**<=**]

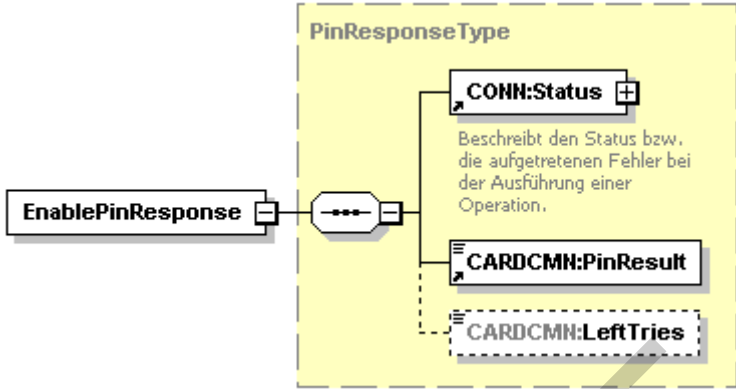
3375 **4.1.5.5.5 EnablePin**

3376 TIP1-A_5487 - Operation EnablePin

3377 Der Konnektor MUSS an der Außenschnittstelle eine Operation EnablePin, wie in Tabelle
3378 TAB_KON_242 Operation EnablePin beschrieben, anbieten.

3379 **Tabelle 123: TAB_KON_242 Operation EnablePin**

Name	EnablePin	
Beschreibung	Schaltet für eine Multireferenz-PIN das Erfordernis, das Nutzergeheimnis zu verifizieren, <u>ein</u> , so dass der Sicherheitszustand nur durch eine erfolgreiche Benutzerverifikation gesetzt werden kann.	
Aufrufparameter		
	Name	Beschreibung
	Context	MandantId, ClientSystemId, WorkplaceId verpflichtend;
	CardHandle	Adressiert die Karte, deren MRPIN bearbeitet werden soll. Es werden nur eGKs ab Generation 2 unterstützt.
	PinTyp	Gibt an, auf welche MRPIN der Karte die Operation angewendet werden soll. Erlaubte Werte: <ul style="list-style-type: none"> eGK G2: MRPIN.NFD, MRPIN.DPE, MRPIN.GDD zusätzlich ab eGK G2.1: MRPIN.AMTS

Rückgabe			
	Name	Beschreibung	
	Status	Enthält den Ausführungsstatus der Operation, siehe 3.5.2	
	PinResult	Wert	Bedeutung
		OK	Aktivierung war erfolgreich
		REJECTED	PIN war falsch. Die Anzahl der verbleibenden Versuche ist im Element LeftTries
		ERROR	Ein Bearbeitungsfehler ist aufgetreten. Fehlerursache im Feld Error
		WASBLOCKED	PIN war zum Aufrufzeitpunkt bereits gesperrt
		NOWBLOCKED	PIN ist durch aktuellen Fehlversuch gesperrt
		TRANSPORT_PIN	Dieser Wert wird nicht verwendet
LeftTries	Im Falle von Result=REJECTED wird hier die Anzahl der verbleibenden möglichen Versuche zurückgegeben.		
Vorbedingung	keine		
Nachbedingung	Für das Erreichen des Sicherheitszustands der MRPIN ist eine Nutzereingabe erforderlich		

3380

3381

Tabelle 124: TAB_KON_243 Ablauf EnablePin

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung

1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	TUC_KON_000 „Prüfe Zugriffsberechtigung“	Prüfung der Zugriffsberechtigung durch den Aufruf TUC_KON_000 { mandantId = \$context.mandantId; clientSystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; userId = \$context.userId; cardHandle } Tritt bei der Prüfung ein Fehler auf, so bricht die Operation mit dem Fehlercode aus TUC_KON_000 ab.
3.	TUC_KON_026 „Liefere CardSession“	Ermittle cardSession über TUC_KON_026 { mandantId = \$context.mandantId; clientSystemId = \$context.clientsystemId; userId = \$context.userId; cardHandle }
4.	TUC_KON_027 „PIN-Schutz ein-/ausschalten“	Aktiviere das Erfordernis der Benutzerverifikation der MRPIN durch Aufruf des TUC_KON_027 „PIN-Schutz ein-/ausschalten“ { cardSession; pinRef = PinRef(PinType); enable = true}
5.	Verifikationsergebnis auswerten	Als erfolgreicher Operationsdurchlauf wird nur PinResult=OK gewertet. Alle anderen Resultate sind Fehlerfälle, und neben dem Status ist auch PinResult entsprechend zu setzen. Dabei gelten folgende Regeln: Wenn TUC_KON_027 den PIN-Status BLOCKED liefert, wird auf PinResult=NOWBLOCKED abgebildet. Wenn TUC_KON_027 mit Fehler 4063 abbricht, wird dies auf PinResult=WASBLOCKED abgebildet.

3382

3383

Tabelle 125: TAB_KON_244 Fehlercodes „EnablePin“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler
4072	Technical	Error	Ungültige PIN-Referenz <code>PinRef</code>
4209	Technical	Error	Kartentyp <code>%CardType%</code> wird durch diese Operation nicht unterstützt.

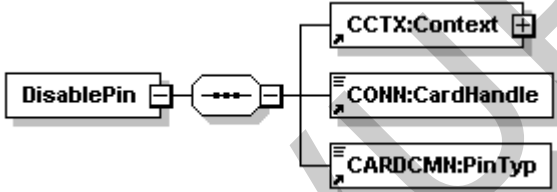
3384
3385
3386 [\leq]

3387 4.1.5.5.6 DisablePin

3388 TIP1-A_5488 - Operation DisablePin

3389 Der Konnektor MUSS an der Außenschnittstelle eine Operation DisablePin, wie in Tabelle
3390 TAB_KON_245 Operation DisablePin beschrieben, anbieten.

3391 **Tabelle 126: TAB_KON_245 Operation DisablePin**

Name	DisablePin	
Beschreibung	Schaltet für eine Multireferenz-PIN das Erfordernis, das Nutzergeheimnis zu verifizieren, <u>ab</u> . Die MRPIN verhält sich danach bei allen Zugriffen auf die durch sie geschützten Objekte, als wäre sie freigeschaltet.	
Aufrufparameter		
	Name	Beschreibung
	Context	MandantId, ClientSystemId, WorkplaceId verpflichtend;
	CardHandle	Adressiert die Karte, deren MRPIN bearbeitet werden soll. Es werden nur eGKs ab Generation 2 unterstützt.
	PinTyp	Gibt an, auf welche MRPIN der Karte die Operation angewendet werden soll. Erlaubte Werte: <ul style="list-style-type: none"> eGK G2: MRPIN.NFD, MRPIN.DPE, MRPIN.GDD zusätzlich ab eGK G2.1: MRPIN.AMTS

Rückgabe			
	Name	Beschreibung	
	Status	Enthält den Ausführungsstatus der Operation siehe 3.5.2	
	PinResult	Wert	Bedeutung
		OK	Aktivierung war erfolgreich
		REJECTED	PIN war falsch. Die Anzahl der verbleibenden Versuche ist im Element LeftTries
		ERROR	Ein Bearbeitungsfehler ist aufgetreten. Fehlerursache im Feld Error
		WASBLOCKED	PIN war zum Aufrufzeitpunkt bereits gesperrt
		NOWBLOCKED	PIN ist durch aktuellen Fehlversuch gesperrt
TRANSPORT_PIN		Dieser Wert wird nicht verwendet	
LeftTries	Im Falle von Result=REJECTED wird hier die Anzahl der verbleibenden möglichen Versuche zurückgegeben.		
Vorbedingung	keine		
Nachbedingung	Der Sicherheitszustand der PIN ist dauerhaft (bis zur expliten Aktivierung mit EnablePin) gesetzt, ohne dass eine Nutzereingabe erforderlich wäre		

3392 Tabelle 127: TAB_KON_246 Ablauf DisablePin

Nr.	Aufruf Technischer Use Case oder Interne	Beschreibung
-----	---	--------------

	Operation	
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	TUC_KON_000 „Prüfe Zugriffs- berechtigung“	Prüfung der Zugriffsberechtigung durch den Aufruf TUC_KON_000 { mandantId = \$context.mandantId; clientSystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; userId = \$context.userId; cardHandle } Tritt bei der Prüfung ein Fehler auf, so bricht die Operation mit dem Fehlercode aus TUC_KON_000 ab.
3.	TUC_KON_026 „Liefere CardSession“	Ermittle cardSession über TUC_KON_026 { mandantId = \$context.mandantId; clientSystemId = \$context.clientSystemId; userId = \$context.userId; cardHandle }
4.	TUC_KON_027 „PIN-Schutz ein- /ausschalten“	Deaktiviere das Erfordernis der Benutzerverifikation der MRPIN durch Aufruf des TUC_KON_027 „PIN-Schutz ein- /ausschalten“ { cardSession; pinRef = PinRef(PinType); enable = false}
5.	Verifikations- ergebnis auswerten	Als erfolgreicher Operationsdurchlauf wird nur PinResult=OK gewertet. Alle anderen Resultate sind Fehlerfälle, und neben dem Status ist auch PinResult entsprechend zu setzen. Dabei gelten folgende Regeln: Wenn TUC_KON_027 den PIN-Status BLOCKED liefert, wird auf PinResult=NOWBLOCKED abgebildet. Wenn TUC_KON_027 mit Fehler 4063 abbricht, wird dies auf PinResult=WASBLOCKED abgebildet.

3393

3394

Tabelle 128: TAB_KON_247 Fehlercodes „DisablePin“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler
4072	Technical	Error	ungültige PIN-Referenz PinRef

4209	Technical	Error	Kartentyp %CardType% wird durch diese Operation nicht unterstützt.
------	-----------	-------	--

[<=]

4.1.5.6 Betriebsaspekte

TIP1-A_4592 - Konfigurationswerte des Kartendienstes

Der Konnektor MUSS es einem Administrator ermöglichen, Konfigurationsänderungen gemäß Tabelle TAB_KON_554 vorzunehmen.

Tabelle 129: TAB_KON_554 Konfiguration des Kartendienstes

ReferenzID	Belegung	Bedeutung
CARD_TIMEOUT_CARD	Sekunden	Maximale Zeit, die ein Aufruf einer Kartenoperation dauern darf, bevor der Aufruf abgebrochen wird. Der Konnektor MUSS sicherstellen, dass dieser Parameter einen Wert besitzt, mit dem ein reibungsloser Betrieb gewährleistet ist, und MUSS dem Administrator die Möglichkeit bieten, diesen Parameter zu konfigurieren.

[<=]

4.1.5.6.1 TUC_KON_025 "Initialisierung Kartendienst"

TIP1-A_4593 - TUC_KON_025 „Initialisierung Kartendienst“

Der Konnektor MUSS den technischen Use Case „Initialisierung Kartendienst“ gemäß TUC_KON_025 umsetzen.

Tabelle 130: TAB_KON_555 - TUC_KON_025 „Initialisierung Kartendienst“

Element	Beschreibung
Name	TUC_KON_025 „Initialisierung Kartendienst“
Beschreibung	Nach dem Start des Kartendienstes MUSS der Konnektor für alle gesteckten Karten den TUC_KON_001 {ctId, slotId } aufrufen und CM_CARD_LIST befüllen.
Auslöser	der Kartendienst wird gestartet
Vorbedingungen	Kartenterminaldienst wurde gestartet
Eingangsdaten	CTM_CT_LIST
Komponenten	Karte, Kartenterminal, Konnektor
Ausgangsdaten	Aktuelle CM_CARD_LIST
Standardablauf	<ol style="list-style-type: none"> 1. Rufe TUC_KON_001 „Karte öffnen“ 2. Wiederhole, bis für alle gesteckten Karten ein Eintrag in CM_CARD_LIST existiert.

Varianten/Alternativen	keine
Fehlerfälle	keine
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

3411

3412 **[<=]**3413 *4.1.5.6.2 Kartenübersicht und PIN-Management*

3414 TIP1-A_5110 - Übersicht über alle verfügbaren Karten

3415 Die Administrationsoberfläche MUSS dem Administrator eine Übersichtsseite anbieten,
3416 die alle in CM_CARD_LIST enthaltenen Karten listet.

3417 In dieser Übersichtsseite muss zu jeder Karte dargestellt werden:

- 3418 • CARD.CTID
- 3419 • CT(CARD.CTID).HOSTNAME
- 3420 • CARD.SLOTNO
- 3421 • CARD.TYPE
- 3422 • CARD.INSERTTIME
- 3423 • CARD.CARDHOLDERNAME

3424 Ferner MÜSSEN auf Verlangen des Administrators zu jeder Karte neben den obigen
3425 Informationen auch folgende Details angezeigt werden:

- 3426 • CARD.ICCSN
- 3427 • CARD.CARDVERSION
- 3428 • CARD.CERTEXPIRATIONDATE

3429 **[<=]**

3430 TIP1-A_5111 - PIN-Management der SM-Bs für den Administrator

3431 Über die Administrationsoberfläche MUSS der Administrator für jede in der
3432 Übersichtsseite angezeigte Karte vom Typ SM-B die folgenden TUCs für die PIN.SMC
3433 auslösen können.3434 Für diese MUSS er einen der gemäß Kapitel 4.1.1.6 [TIP1-A_4526] definierten
3435 Mandanten auswählen können:

- 3436 • TUC_KON_012 „PIN verifizieren“
- 3437 • TUC_KON_019 „PIN ändern“
- 3438 • TUC_KON_021 „PIN entsperren“
- 3439 • TUC_KON 022 „Liefere PIN-Status“

3440 Die Eingabe der PIN SOLL von jedem vom Informationsmodell her zulässigen
3441 Kartenterminal aus möglich sein.3442 **[<=]**3443 Der Konnektor kann den Administrator zur Laufzeit entscheiden lassen, an welchem
3444 Kartenterminal die PIN eingegeben werden soll, indem er ihn wählen lässt, ob er die PIN

3445 am Kartenterminal eingibt, in dem die betroffene SM-B steckt, oder ihn den Arbeitsplatz
3446 wählen lässt, von dem aus er die Remote-PIN eingibt.

3447 **4.1.6 Systeminformationsdienst**

3448 Der Systeminformationsdienst stellt Basisdiensten, Fachmodulen und Clientsystemen
3449 sowohl aktiv (Push-Mechanismus) wie passiv (Pull-Mechanismus) Informationen zur
3450 Verfügung. Dabei erhebt er selbst keine Daten, sondern dient nur als zentraler
3451 Mechanismus, der von anderen Basisdiensten und Fachmodulen zur Verteilung und
3452 Bereitstellung derer Informationen verwendet werden kann.

3453 Innerhalb des Systeminformationsdienstes werden folgende Präfixe für Bezeichner
3454 verwendet:

- 3455 • Events (Topic Ebene 1): „EVT“
- 3456 • Konfigurationsparameter: „EVT_“

3457 **Push-Mechanismus**

3458 Der Push-Mechanismus des Systeminformationsdienstes hat die Aufgabe, Ereignisse von
3459 internen Ereignisquellen im Konnektor (z. B. von anderen Basisdiensten wie
3460 Kartendienst, Kartenterminaldienst oder Fachmodulen) an alle Basisdienste und
3461 Fachmodule sowie an die bei ihm registrierten Ereignisempfänger (Clientsysteme)
3462 weiterzuleiten.

3463 Die Namen der Ereignisse, die Topics, sind als Baumstruktur organisiert und werden
3464 mittels „/“-getrennter Liste angegeben (z. B. „Auslöser/Ereigniskategorie1/.../Ereignis1“).
3465 Die konkreten Topics werden innerhalb der einzelnen Funktionsmerkmale
3466 kontextbezogen definiert und im Anhang in einer zentralen Liste übersichtlich dargestellt.

3467 Clientsysteme können sich für den Empfang bestimmter Ereigniskategorien (Topics)
3468 anmelden. Der Systeminformationsdienst übernimmt dementsprechend bei der
3469 Verteilung der Ereignisse auch eine Filterfunktion für die weiterzuleitenden Ereignisse.

3470 Die Zustellung der Ereignisse erfolgt unidirektional über eine Netzschnittstelle, deren
3471 Kommunikationsendpunkt („Ereignissenke“) vom Clientsystem realisiert werden muss.
3472 Zur Übertragung der Daten wird ein konnektoreigenes Protokoll cetp (Connector Event
3473 Transport Protocol) verwendet.

3474 **Pull-Mechanismus**

3475 Der Pull-Mechanismus des Systeminformationsdienstes hat die Aufgabe sowohl
3476 Zustandswerte als auch statische Informationen des Konnektors selbst als auch von den
3477 über ihn verwalteten Ressourcen durch Fachmodule und Clientsysteme abrufbar zu
3478 machen. Dabei können entweder Listen von Ressourcen oder Details zu einzelnen
3479 Ressourcen abgerufen werden.

3480 Die folgenden Unterkapitel regeln:

- 3481 • Das Kommunikationsprotokoll cetp
- 3482 • Die Struktur der Ereignisnachricht
- 3483 • Die TUCs für die Ereignisverteilung (PUSH)
- 3484 • Die TUCs und Operationen der Außenschnittstelle für den Abruf von
3485 Informationen (PULL)
- 3486 • Einstellungen, die der Administrator zur Steuerung des Verhaltens vornehmen
3487 kann.

4.1.6.1 Funktionsmerkmalweite Aspekte

TIP1-A_4594 - Richtung bei Verbindungsaufbau des Systeminformationsdienstes
Der Konnektors MUSS zur Übertragung von Ereignissen eine cetp-Verbindung zu der Ereignissenke des Clientsystems aufbauen, die das Clientsystem beim Operationsaufruf Subscribe per `EventTo` angegeben hatte.

[<=]

TIP1-A_5536 - Connector Event Transport Protocol über TCP

Der Konnektor MUSS das Anwendungsprotokoll cetp (Connector Event Transport Protocol) ausschließlich über das Transportprotokoll TCP (gegebenfalls TLS gesichert) anbieten.

[<=]

TIP1-A_4595 - Gesicherte Übertragung von Ereignissen

Der Konnektor MUSS zur Übertragung der Ereignisse eine gesicherte Verbindung (TLS) verwenden, die vom Konnektor als TLS-Client initiiert wurde, wenn `ANCL_TLS_MANDATORY=Enabled`.

Der Konnektor muss sich beim Aufbau der TLS-Sitzung gegenüber dem Clientsystem authentisieren, wenn dieses eine Authentisierung im Rahmen des TLS-Handshakes anfordert.

Die Schalter `ANCL_CAUT_MODE` und `ANCL_CAUT_MANDATORY` wirken für die Übertragung der Ereignisse nicht.

[<=]

Für die Übermittlung der Ereignisse wurde ein leichtgewichtiges Protokoll gewählt, da vom Clientsystem keine Antwort auf Anwendungsebene erwartet wird.

TIP1-A_4596 - Nachrichtenaufbau und -kodierung des Systeminformationsdienstes
Der Konnektors MUSS Ereignisse an Ereignissenken mittels Nachrichten verteilen, die gemäß `TAB_KON_030` „Ereignisnachricht“ aufgebaut sind. Der Konnektor MUSS die Nachrichten mit der Zeichenkette „CETP“ beginnen, gefolgt von der Länge der folgenden Ereignisnachricht in Anzahl Bytes. Das vier Byte lange Längenfeld MUSS in der Byte-Reihenfolge Big-Endian codiert werden (das hochwertigste Byte wird als erstes übertragen).

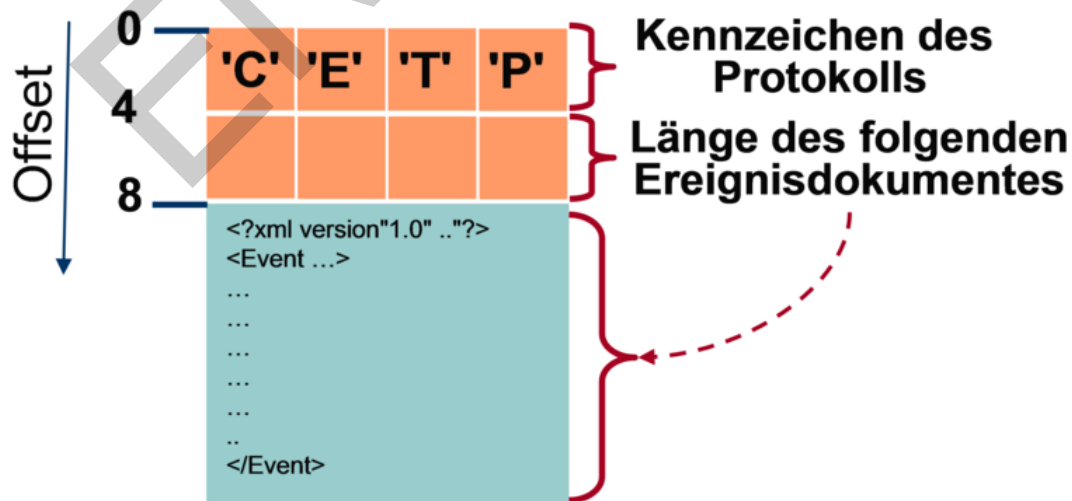
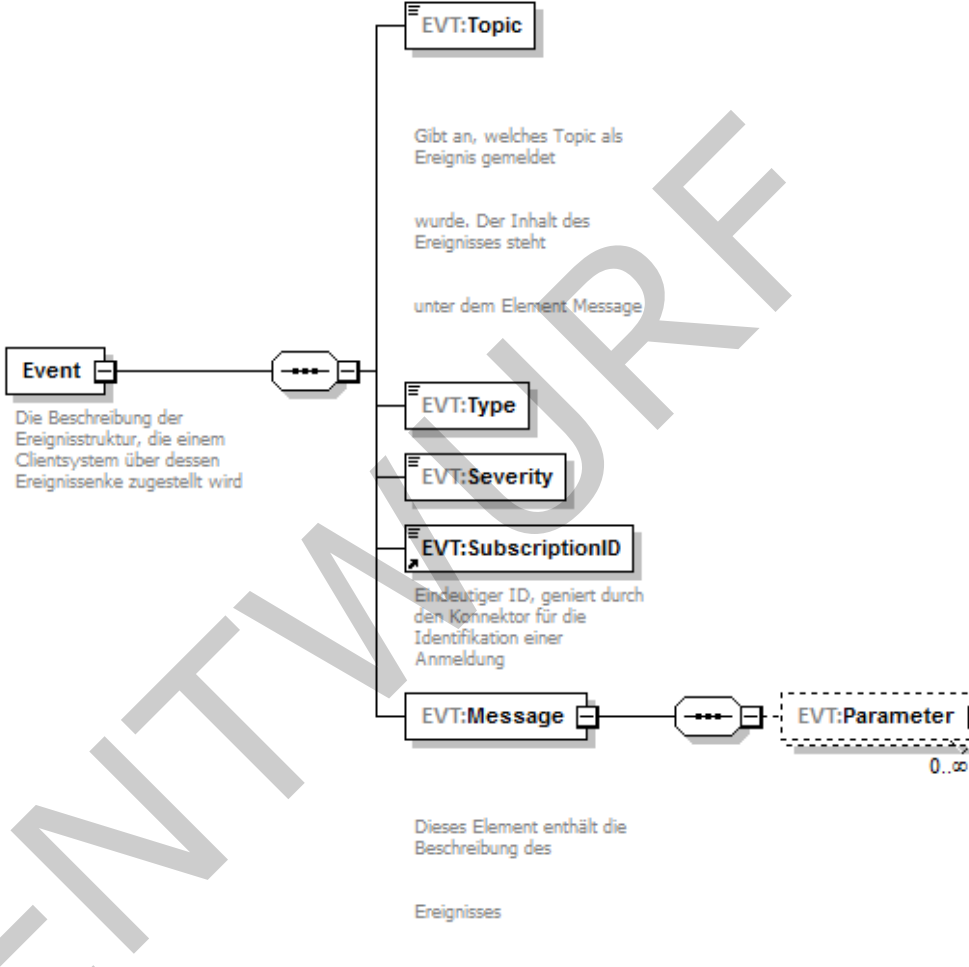


Abbildung 11: PIC_KON_022 Grundsätzlicher Aufbau der Ereignisnachricht

3522 **Tabelle 131: TAB_KON_030 Ereignisnachricht**

Beschreibung g	<p>Die Ereignisnachricht, die zur Ereignissenke gesendet wird, ist ein XML-Dokument. Die Ereignisnachricht wird in den „Umschlag“ Event gepackt. Wenn ein mandantenfähiges Clientsystem mehrere Anwendungskonnektoren verwendet, dann kann es die erhaltenen Ereignisbenachrichtigungen anhand der Subscription-ID einem Mandanten zuordnen.</p>  <p>Die Beschreibung der Ereignisstruktur, die einem Clientsystem über dessen Ereignissenke zugestellt wird</p> <p>Gibt an, welches Topic als Ereignis gemeldet wurde. Der Inhalt des Ereignisses steht unter dem Element Message</p> <p>Eindeutiger ID, geniert durch den Konnektor für die Identifikation einer Anmeldung</p> <p>Dieses Element enthält die Beschreibung des Ereignisses</p> <p>0..∞</p> <p>0..∞</p>
Topic	Topic der Ereignisnachricht
Type	Typ der Ereignisnachricht (Security, Operation, Infrastructure)
Severity	Schwere der Ereignisnachricht (Info, Warning, Error, Fatal)

	SubscriptionID	Identifikator der Anmeldung, der vom Konnektor bei der Operation <code>Subscribe</code> für die Anmeldung des jeweiligen Clientsystems vergeben wurde.
	Message	Dieses Element enthält die Ereignisnachricht. Der Inhalt ist abhängig vom Topic und wird mittels „Key-Value“-Parametern übertragen.
	Message/Parameter/Key	Name des Parameters (String), case sensitiv
	Message/Parameter/Value	Wert des Parameters (String)
Hinweise	Das XML-Dokument MUSS UTF-8-codiert sein.	

3523
3524
3525

[<=]

3526 4.1.6.2 Durch Ereignisse ausgelöste Reaktionen

3527 Keine.

3528 4.1.6.3 Interne TUCs, nicht durch Fachmodule nutzbar

3529 Keine.

3530 4.1.6.4 Interne TUCs, auch durch Fachmodule nutzbar

3531 4.1.6.4.1 TUC_KON_256 „Systemereignis absetzen“

3532 TIP1-A_4598 - TUC_KON_256 „Systemereignis absetzen“

3533 Der Konnektor MUSS für den PUSH-Mechanismus des Systeminformationsdienstes den
3534 technischen Use Case TUC_KON_256 „Systemereignis absetzen“ umsetzen.

3535

3536 Tabelle 132: TAB_KON_556 - TUC_KON_256 „Systemereignis absetzen“

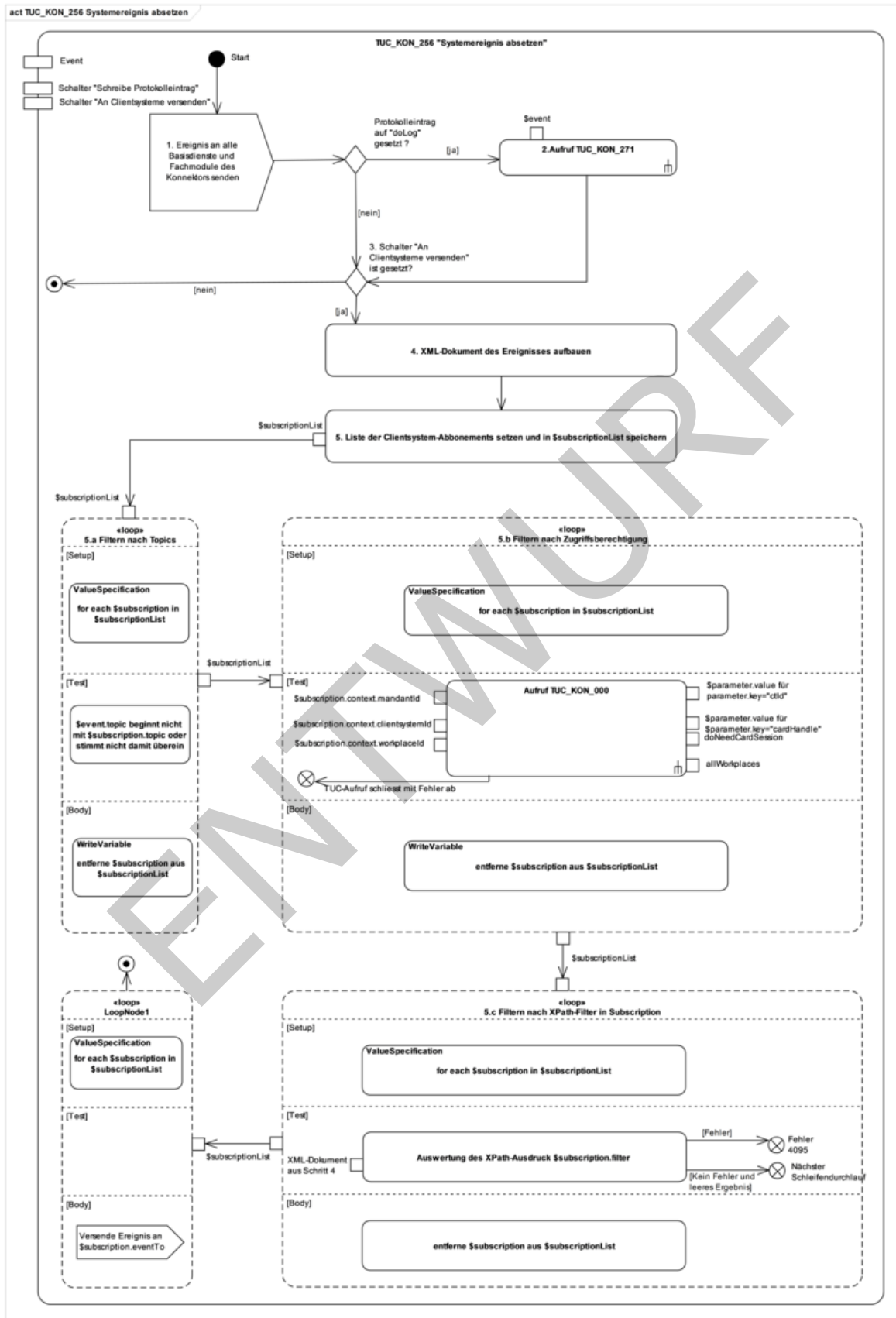
Element	Beschreibung
Name	TUC_KON_256 „Systemereignis absetzen“
Beschreibung	Dieser TUC verteilt ein Ereignis im Konnektor intern (d.h. an Basisdienste und Fachmodule) sowie an Clientsysteme, die sich für den Empfang angemeldet haben (Operation <code>Subscribe</code>). Zusätzlich wird, bei gesetztem Flag, das Ereignis durch den Protokollierungsdienst protokolliert.
Auslöser	Aufruf durch Basisdienst oder Fachmodul
Vorbedingungen	Fall Topic = „BOOTUP/BOOTUP_COMPLETE“: Zu allen URLs von clientseitigen Endpunkten, wie sie bei der <code>Subscribe</code> -Operation angegeben wurden, ist in der Subscription-

	<p>Verwaltung des Konnektors eine TerminationTime gespeichert. Sie wird jeweils auf den Wert der TerminationTime der am längsten gültigen Subscription zu dem jeweiligen Endpunkt gesetzt. Die URLs von clientseitigen Endpunkten müssen bis zum Ablauf ihrer TerminationTime auch über Bootups hinweg gespeichert werden. Vor dem Versenden des BOOTUP_COMPLETE-Events werden sämtliche Subscriptions, jedoch nicht die URLs gelöscht. Bei Ablauf ihrer TerminationTime werden nach dem Versenden des BOOTUP_COMPLETE-Events auch die URLs gelöscht.</p>
Eingangsdaten	<p>Attribute des zu versendenden Ereignisses:</p> <ul style="list-style-type: none"> • topic (Name des Ereignisses) • eventType [EventType] (Wenn statt eines EventType ein ErrorType übergeben wird, so wird der EventType daraus abgeleitet. Typ des Events: Op = Operation, Sec = Security, Infra = Infrastructure) • severity [EventSeverity] (Schwere des Ereignisses: Info = Information, Warn = Warning, Err = Error, Fatal) • parameters (weitere Parameter als key-value-Paare) <p>Arbeitsanweisungen:</p> <ul style="list-style-type: none"> • doLog [Boolean] – <i>optional; default = true</i> (Schalter „Schreibe Protokolleintrag“) • doDisp [Boolean] – <i>optional; default = true</i> (Schalter „An Clientsysteme versenden“) <p>Die Bezeichnungen Op, Sec, Infra, Info, Warning, Err, Fatal werden nur in diesem Dokument verwendet und sind als Abkürzungen für die Werte Operation, Security, Infrastructure, Information, Warning, Error, Fatal in den jeweiligen Ereignisnachrichten gemäß Schema EventService.xsd zu verstehen.</p>
Komponenten	Konnektor
Ausgangsdaten	Keine
Nachbedingungen	
Standardablauf	<p>Für das übergebene Ereignis werden folgende Schritte durchgeführt:</p> <ol style="list-style-type: none"> 1. Das Ereignis wird an alle Basisdienste und Fachmodule des Konnektors gesendet. 2. Wenn doLog = true, erfolgt der Aufruf von TUC_KON_271 { eventType = \$Event.eventType (mit eventType = „Op“, wenn \$Event.eventType in {„Op“, „Infra“} mit eventType = „Sec“, wenn \$Event.eventType gleich

	<p>"Sec")</p> <pre> severity=\$Event.severity; parameters= (\$Event.topic, \$Event.parameters) } </pre> <p>Die Einschränkungen zur Protokollierung personenbezogener Daten gemäß TIP1-A_4710 müssen beim Aufruf von TUC_KON_271 beachtet werden.</p> <ol style="list-style-type: none"> 3. Falls doDisp = false ist, wird an dieser Stelle abgebrochen. 4. Das für den Versand an Clientsysteme benötigte XML-Dokument des Ereignisses wird aufgebaut (Element „Event“ gemäß EventService.XSD). 5. Setze \$subscriptionList = Liste der Clientsystem-Abonnements, die durch die Operationen Subscribe/Unsubscribe gepflegt werden und deren TerminationTime > Systemzeit. <p>Im Folgenden durchläuft diese Liste der Reihe nach drei Filter. Nach dem letzten Filterschritt enthält \$subscriptionList nur noch die Abonnements, an die das Ereignis versendet werden soll.</p> <ol style="list-style-type: none"> a. Filtern nach Topics: für jede \$subscription in \$subscriptionList { wenn \$event.topic nicht mit \$subscription.topic beginnt oder übereinstimmt (case insensitive Vergleich), dann entferne \$subscription aus \$subscriptionList } b. Filtern nach Zugriffsberechtigung: für jede \$subscription in \$subscriptionList { wenn TUC_KON_000 mit einem Fehler abgeschlossen wird, dann entferne \$subscription aus \$subscriptionList. Wenn cardHandle in parameters übergeben wurde, dann TUC_KON_000 { mandantId = \$subscription.context.mandantId; clientSystemId = \$subscription.context.clientsystemId; workplaceId = \$subscription.context.workplaceId; ctId = \$parameters.value für \$parameters.key = „ctId“ cardHandle = \$parameters.value für \$parameters.key = „cardHandle“; needCardSession = false; allWorkplaces = false } oder im Fall nicht gegebenes cardHandle TUC_KON_000 { mandantId = \$subscription.context.mandantId; clientSystemId = \$subscription.context.clientsystemId; workplaceId = \$subscription.context.workplaceId; ctId = \$parameters.value für \$parameters.key = „ctId“ needCardSession = false; allWorkplaces = false
--	---

	<pre> } } c. Filtern nach XPath-Filter in Subscription ([XPATH]): für jede \$subscription in \$subscriptionList { wenn der XPath-Ausdruck \$subscription.filter angewandt auf das als XML-Dokument dargestellte Ereignis ein leeres Ergebnis liefert, dann entferne \$subscription aus \$subscriptionList } 6. Versenden: für jede \$subscription in \$subscriptionList { versende das Ereignis an \$subscription.eventTo } Für das versendete Ereignis wird keine Antwort durch das Clientsystem erwartet. </pre>
Varianten/ Alternativen	<p>Fall Topic = „BOOTUP/BOOTUP_COMPLETE“:</p> <p>4. Das für den Versand an Clientsysteme benötigte XML-Dokument des Ereignisses wird aufgebaut (Element „Event“ gemäß EventService.XSD, SubscriptionID als leeres Element).</p> <p>5. Setze \$urlList = Liste der URLs von clientseitigen Endpunkten, wie sie bei der <u>Subscribe</u>-Operation angegeben wurden. Clientsysteme, deren Subscription-URL beim Einschalten des Konnektors noch nicht gelöscht waren, müssen benachrichtigt werden, auch wenn dann bereits deren TerminationTime < Systemzeit ist.</p> <p>Versenden: für jede \$url in \$urlList { versende das Ereignis an \$url }</p> <p>Für das versendete Ereignis wird keine Antwort durch das Clientsystem erwartet. Dadurch wird bei einer Nichtzustellung auch kein erneuter Versand des Ereignisses angestoßen, da der Konnektor keine Kenntnis über den Erfolg einer Ereignisübermittlung hat.</p>
Fehlerfälle	<p>Fehler in den folgenden Schritten des Standardablaufs führen zum Abbruch mit den ausgewiesenen Fehlercodes:</p> <p>(→5c) Fehler bei der Auswertung des XPath-Ausdrucks: Fehlercode: 4095, nur für die jeweilige Abonnement-Prüfung.</p>
Fachliche Fehlermeldung	Keine
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Abbildung PIC_KON_112 Aktivitätsdiagramm zu „Systemereignis absetzen“

3537



3538

Abbildung 12: PIC_KON_112 Aktivitätsdiagramm zu „Systemereignis absetzen“

Tabelle 133: TAB_KON_557 Fehlercodes TUC_KON_256 „Systemereignis absetzen“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4095	Technical	Error	Fehler bei der Auswertung eines XPath-Ausdruck

[<=]

4.1.6.4.2 TUC_KON_252 „Liefere KT_Liste“

TIP1-A_4599 - TUC_KON_252 „Liefere KT_Liste“

Der Konnektor MUSS den technischen Use Case TUC_KON_252 „Liefere KT_Liste“ umsetzen.

Tabelle 134: TAB_KON_558 – TUC_KON_252 „Liefere KT_Liste“

Element	Beschreibung
Name	TUC_KON_252 „Liefere KT_Liste“
Beschreibung	Dieser TUC liefert eine Liste der Kartenterminals, die unter Beachtung der Eingangsdaten verfügbar/erreichbar sind.
Auslöser	Aufruf durch ein Clientsystem (Operation <code>GetCardTerminals</code>) oder ein Fachmodul
Vorbedingungen	Keine
Eingangsdaten	<ul style="list-style-type: none"> workplaceId - <i>optional</i> (Arbeitsplatz ID) clientSystemId (Clientssystem ID) mandantId (Mandanten ID)
Komponenten	Konnektor, Kartenterminal
Ausgangsdaten	<ul style="list-style-type: none"> cardTerminals (Liste der Kartenterminals, die den angegebenen Arbeitsplätzen, Mandanten und Clientsystemen zugeordnet sind bzw. auf die diese zugreifen dürfen (siehe Zugriffsberechtigungsdienst), sowie deren aktuelle Verfügbarkeit. Verfügbarkeit bedeutet im Falle eines eHealth-Kartenterminals, dass der Konnektor eine Verbindung zum Kartenterminal aktuell hält.)
Nachbedingungen	<ul style="list-style-type: none"> Der Zustand der Kartenterminals bleibt unverändert

Standardablauf	<ol style="list-style-type: none"> Erstellen der Liste aller Kartenterminals, auf die der angegebene Mandant und das angegebene Clientsystem zugreifen dürfen (siehe Zugriffsberechtigungsdienst) <ol style="list-style-type: none"> Wurde der optionale Parameter workplaceId ID übergeben, so werden nur die Kartenterminals in die Liste aufgenommen, die diesem Arbeitsplatz zugeordnet sind (siehe Zugriffsberechtigungsdienst). Dazu zählen insbesondere nicht die als entfernte Kartenterminals bezeichneten KT. Fehlt dieser Parameter, so werden alle Kartenterminals in die Liste aufgenommen, die sowohl dem Clientsystem als auch dem Mandanten zugeordnet sind. Rückgabe der Liste cardTerminals (der in Schritt 1 erstellten Liste) mit Angaben zu jedem Kartenterminal gemäß Schema „Eventservice.xsd“.
Varianten/Alternativen	Keine
Fehlerfälle	Keine
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

3550

3551 [\leq]

3552 4.1.6.4.3 TUC_KON_253 „Liefere Karten_Liste“

3553 TIP1-A_4600 - TUC_KON_253 „Liefere Karten_Liste“

3554 Der Konnektor MUSS den technischen Use Case TUC_KON_253 „Liefere Karten_Liste“
3555 umsetzen.

3556

3557 **Tabelle 135: TAB_KON_559 – TUC_KON_253 „Liefere Karten_Liste“**

Element	Beschreibung
Name	TUC_KON_253 „Liefere Karten_Liste“
Beschreibung	Dieser TUC liefert eine Liste der gesteckten Karten, die unter Beachtung der Eingangsdaten verfügbar/erreichbar sind.
Auslöser	Aufruf durch ein Clientsystem (Operation GetCards) oder ein Fachmodul
Vorbedingungen	Keine
Eingangsanforderung	Keine
Eingangsdaten	<ul style="list-style-type: none"> workplaceId – <i>optional</i> (Arbeitsplatz-ID)

	<ul style="list-style-type: none"> • clientSystemId (Clientssystem ID) • cardTerminalId - <i>optional; verpflichtend, wenn slotId übergeben wird</i> (Kartenterminalidentifikator) • slotId - <i>optional</i> (Nummer des Slots, beginnend bei 1) • mandantId (Mandanten ID) • cardType - <i>optional</i> (Kartentyp gemäß Tabelle TAB_KON_500)
Komponenten	Konnektor, Kartenterminal, Karte
Ausgangsdaten	<ul style="list-style-type: none"> • cards (Liste der gesteckten Karten einschließlich der Informationen für CARD:card, auf die der Mandant und das Clientssystem von dem Arbeitsplatz aus zugreifen dürfen (siehe Zugriffsberechtigungsdienst)). Wird workplaceId nicht übergeben, so werden alle vom Clientssystem und dem Mandant erreichbaren Kartenterminals in die Liste aufgenommen. Die Eingangsdaten dienen als Filter, welche Karten in cards zurückgegeben werden. Beispiel: Falls cardTerminalId angegeben ist, werden nur Karten in die Liste aufgenommen, die im entsprechenden Kartenterminal stecken.)
Nachbedingungen	<ul style="list-style-type: none"> • Der Zustand der Kartenterminals und der Karten bleibt unverändert
Standardablauf	<ol style="list-style-type: none"> 1. Erstellen der Liste aller Karten, auf die der angegebene Mandant und das angegebene Clientssystem zugreifen dürfen (siehe Zugriffsberechtigungsdienst). <ol style="list-style-type: none"> a. Wurde cardTerminalId übergeben, dann nur Karten berücksichtigen, die dem dadurch referenziertem Kartenterminal zugeordnet sind. b. Wurde außer cardTerminalId auch slotId übergeben, so ist nur die Karte zu berücksichtigen, die in dem angegebenen Slot steckt. c. Wurde workplaceId übergeben, so werden nur die Karten in die Liste aufgenommen, auf die von diesem Arbeitsplatz aus zugegriffen werden darf (siehe „Zugriffsberechtigung Ressourcen“). d. Wurde cardType übergeben, so werden nur die Karten in die Liste aufgenommen, die dem Kartentyp in CardType entsprechen.

	2. Rückgabe cards, der in Schritt 1 erstellten Liste mit Angaben zu jeder Karte gemäß Schema „Eventservice.xsd“.
Varianten/ Alternativen	Keine
Fehlerfälle	Fehler in den folgenden Schritten des Standardablaufs führen zum Abbruch mit den ausgewiesenen Fehlercodes: (→1 a) Ungültige Kartenterminal-ID: Fehlercode: 4007
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

3558

3559

Tabelle 136: TAB_KON_560 Fehlercodes TUC_KON_253 „Liefere Karten_Liste“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4007	Technical	Error	ungültige Kartenterminal-ID

3560

3561 [\leq]

3562 4.1.6.4.4 TUC_KON_254 „Liefere Ressourcendetails“

3563 TIP1-A_4602 - TUC_KON_254 „Liefere Ressourcendetails“

3564 Der Konnektor MUSS den technischen Use Case TUC_KON_254 „Liefere
 3565 Ressourcendetails“ umsetzen.
 3566

Tabelle 137: TAB_KON_561 - TUC_KON_254 „Liefere Ressourcendetails“

Element	Beschreibung
Name	TUC_KON_254 „Liefere Ressourcendetails“
Beschreibung	Dieser TUC liefert Detailinformationen zu einer Ressource (KT, Karte) oder dem Konnektor
Auslöser	Aufruf durch ein Clientsystem (Operation <code>GetResourceInformation</code>) oder ein Fachmodul
Vorbedingungen	Keine
Eingangsanforderung	Keine
Eingangsdaten	<ul style="list-style-type: none"> clientSystemId (Clientsystem ID) mandantId (Mandanten ID) workplaceId – <i>optional</i> (Arbeitsplatz ID)

	<ul style="list-style-type: none"> • cardTerminalId – <i>optional</i> (Kartenterminal ID) • slotId – <i>optional/zulässig nur, wenn auch cardTerminalId angegeben ist</i> (Kartenslot-Nummer) • cardHandle – <i>optional</i> • iccsn – <i>optional</i>
Komponenten	Konnektor, Kartenterminal, Karte, HSM
Ausgangsdaten	<ul style="list-style-type: none"> • resource (Informationsobjekt einer Ressource (Kartenterminal, Karte, HSM))
Nachbedingungen	<ul style="list-style-type: none"> • Der Zustand der Kartenterminals, Karten und HSM bleibt unverändert
Standardablauf	<ol style="list-style-type: none"> 1. Falls cardTerminalId und slotId übergeben wurde oder in den Eingangsparametern iccsn oder cardHandle enthalten ist, wird ein Informationsobjekt der Karte, die sich in dem angegebenen Slot befindet bzw. die über die Iccsn oder das CardHandle identifiziert werden kann, zurückgegeben. 2. Falls cardTerminalId, aber keine slotId übergeben wurde, wird ein Informationsobjekt des Kartenterminals zurückgegeben. 3. Wurde weder iccsn, cardHandle, cardTerminalId noch eine slotId übergeben, so wird ein Informationsobjekt des Konnektors zurückgegeben. Für das Element ErrorCondition ist aus der Tabelle TAB_KON_503 Betriebszustand_Fehlerzustandsliste der Text aus der Spalte ErrorCondition zu übernehmen, ggf. mit den in dieser Spalte angegebenen Parameterwerten. Vor der Rückgabe der Informationen über eine Ressource wird geprüft, ob der angegebene Mandant und das angegebene Clientsystem darauf zugreifen dürfen (siehe Zugriffsberechtigungsdiens). Wurde zusätzlich der optionale Parameter workplaceId übergeben, so wird auch geprüft, ob die Ressource diesem Arbeitsplatz zugeordnet ist. Die Rückgabe der Informationen erfolgt gemäß dem Schema „Eventservice.xsd“.
Varianten/ Alternativen	Keine
Fehlerfälle	Fehler in den folgenden Schritten des Standardablaufs führen zum Abbruch mit den ausgewiesenen Fehlercodes: (→1) Ungültige Kartenterminal-ID: Fehlercode: 4007 (→1) Ungültige Kartenslot-ID: Fehlercode: 4097 (→1) Keine Karte im angegebenen Slot: Fehlercode: 4098 (→1) Keine Karte mit angegebener Iccsn gefunden: Fehlercode: 4099

	(→1) Karten-Handle ungültig: Fehlercode: 4101 (→2) Ungültige Kartenterminal-ID: Fehlercode: 4007
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

3568 **Tabelle 138: TAB_KON_562 Fehlercodes TUC_KON_254 „Liefere Ressourcendetails“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4007	Technical	Error	ungültige Kartenterminal-ID
4097	Technical	Error	ungültige Kartenslot-ID
4098	Technical	Error	keine Karte im angegebenen Slot gefunden
4099	Technical	Error	keine Karte zur angegebenen Iccsn gefunden
4101	Technical	Error	Karten-Handle ungültig

3569

3570 [**<=**]

3571 **4.1.6.5 Operationen an der Außenschnittstelle**

3572 TIP1-A_4603 - Basisanwendung Systeminformationsdienst

3573 Der Konnektor MUSS für Clients eine Basisanwendung Systeminformationsdienst
3574 anbieten.

3575

3576 **Tabelle 139 TAB_KON_029 Basisanwendung Systeminformationsdienst**

Name	EventService	
Version	7.2.0 Siehe Anhang D (WSDL-Version)	
Namensraum	Siehe Anhang D	
Namensraum-Kürzel	EVT für Schema und EVTW für WSDL	
Operationen	Name	Kurzbeschreibung
	GetCardTerminals	Auflistung der verfügbaren Kartenterminals
	GetCards	Auflistung der gesteckten Karten

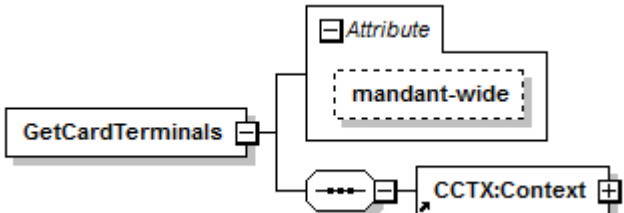
	GetResourceInformation	Liefert Details zu einer Ressource (Kartenterminal, Karte, HSM)
	Subscribe	Anmeldung der Zustellung von Ereignissen
	Unsubscribe	Abmelden von der Zustellung von Ereignissen
	RenewSubscriptions	Gültigkeit bestehender Subscriptions verlängern
	GetSubscriptions	Abfrage der angemeldeten Zustellungen von Ereignissen
WSDL	EventService.wsdl	
Schema	EventService.xsd	

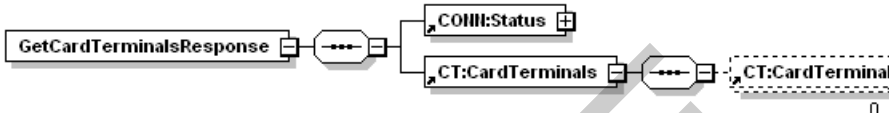
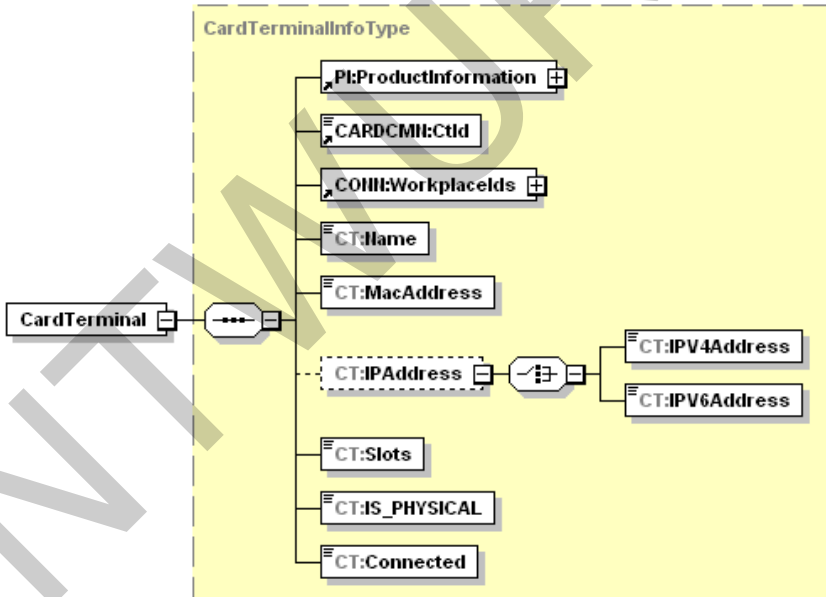
3577
3578
3579 [\leq]

3580 4.1.6.5.1 GetCardTerminals

3581 TIP1-A_4604 - Operation GetCardTerminals
3582 Der Konnektors MUSS an der Außenschnittstelle eine Operation GetCardTerminals, wie in
3583 Tabelle TAB_KON_563 „Operation GetCardTerminals“ beschrieben, anbieten.
3584

3585 **Tabelle 140: TAB_KON_563 Operation GetCardTerminals**

Name	GetCardTerminals	
Beschreibung	Liefert die Liste der Kartenterminals, auf die der aufrufende Mandant und das aufrufende Clientsystem zugreifen dürfen (siehe Zugriffsberechtigungsdiens) sowie deren aktuelle Verfügbarkeit. Verfügbarkeit bedeutet im Falle eines eHealth-Kartenterminals, dass der Konnektor eine Verbindung zum Kartenterminal aktuell hält.	
Aufrufparameter		
	Name	Beschreibung

	@mandant-wide	Wenn „true“, werden alle Kartenterminals zurückgegeben, auf die der Mandant und das aufrufende Clientsystem zugreifen dürfen. Wenn „false“ (Standardbelegung), werden nur Kartenterminals zurückgegeben, auf die von dem im Aufrufkontext spezifizierten Arbeitsplatz zugegriffen werden darf.
	Context	Aufrufkontext
Rückgabe		
	Name	Beschreibung
	Status	Ergebnis der Operation
		
	Die Liste der Kartenterminals	
	Name	Beschreibung
	Product Information	Produktinformationen gemäß [gemSpec_OM] und dem Schema „ProductInformation.xsd“ zu formatieren.
	CtId	Eindeutige Identifikation des Kartenterminals
	WorkplaceIds	Die Liste der Arbeitsplätze, denen das Kartenterminal als lokales Kartenterminal zugeordnet ist. Insbesondere für Entfernte Kartenterminals kann diese Liste leer sein (siehe TUC_KON_252).
	Name	Sprechender Name des Kartenterminals

	MacAddress	MAC-Adresse des Kartenterminals
	IPAddress	IP-Adresse des Kartenterminals
	Slots	Anzahl der Slots des Kartenterminals
	IS_PHYSICAL	Attribut des Kartenterminals das anzeigt ob es sich um ein physisches oder logisches Kartenterminal handelt (siehe auch TAB_KON_522 Parameterübersicht des Kartenterminaldienstes)
	Connected	Zeigt an, ob dieses Kartenterminal aktuell verfügbar ist. TRUE – ist verfügbar FALSE – ist nicht verfügbar
Vorbedingungen	Keine	
Nachbedingungen	Der Zustand der Kartenterminals bleibt unverändert.	
Hinweise	Der Aufruf DARF nur den im Konnektor verwalteten, aktuellen Zustand des Kartenterminals liefern und DARF NICHT Abfragen an die Kartenterminals absetzen.	

Der Ablauf der Operation GetCardTerminals ist in Tabelle TAB_KON_564 Ablauf GetCardTerminals beschrieben:

Tabelle 141: TAB_KON_564 Ablauf GetCardTerminals

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	TUC_KON_000 „Prüfe Zugriffsberechtigung“	Prüfung der Zugriffsberechtigung durch den Aufruf TUC_KON_000 { mandantId = \$context.mandantId; clientSystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; needCardSession = false; allWorkplaces = @mandant-wide } Tritt bei der Prüfung ein Fehler auf, bricht die Operation mit Fehlercode aus TUC_KON_000 ab.
3.	TUC_KON_252 „Liefere KT_Liste“	Die Liste der Kartenterminals wird erstellt und zurückgegeben. Tritt hierbei ein Fehler auf, so bricht die Operation mit dem Fehler des TUCs ab. Wenn @mandant-wide=true dann ermittle die Liste der Kartenterminals für alle Arbeitsplätze des Mandanten für das angegebene Clientsystem durch den Aufruf von TUC_KON_252{ clientSystemId = \$context.ClientSystemId; mandantId = \$context.mandantId }

		Wenn @mandant-wide=false dann ermittle die Liste der Kartenterminals für den Arbeitsplatz des Mandanten für das angegebene Clientsystem entsprechend \$context durch den Aufruf von TUC_KON_252{ workplaceId = \$context.workplaceId; clientSystemId = \$context.ClientSystemId; mandantId = \$context.mandantId }
--	--	---

3590

3591 **Tabelle 142: TAB_KON_823 Fehlercodes „GetCardTerminals“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler

3592

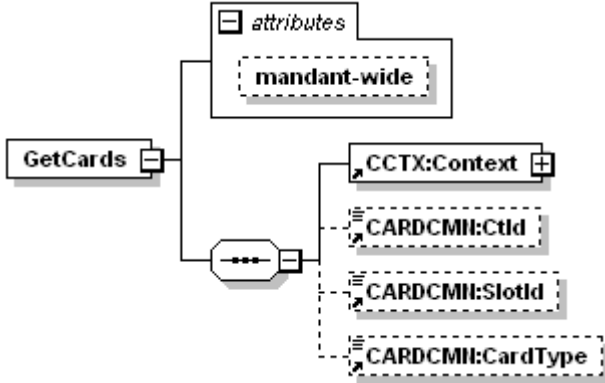
3593

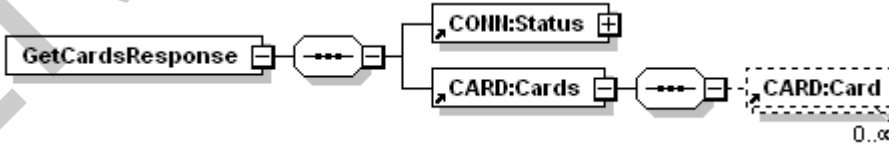
3594 [**<=**]3595 **4.1.6.5.2 GetCards**

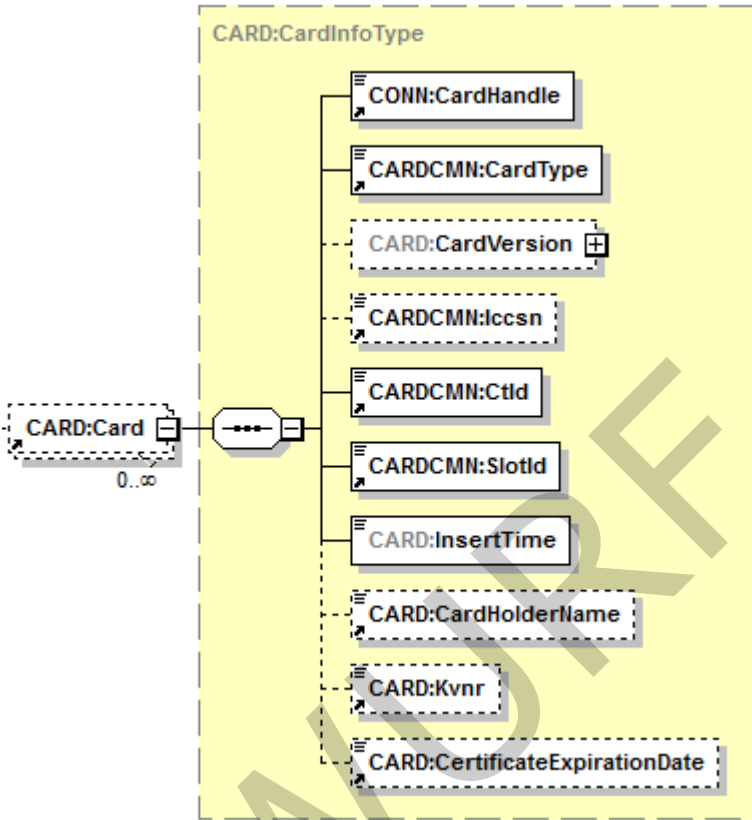
3596 TIP1-A_4605 - Operation GetCards

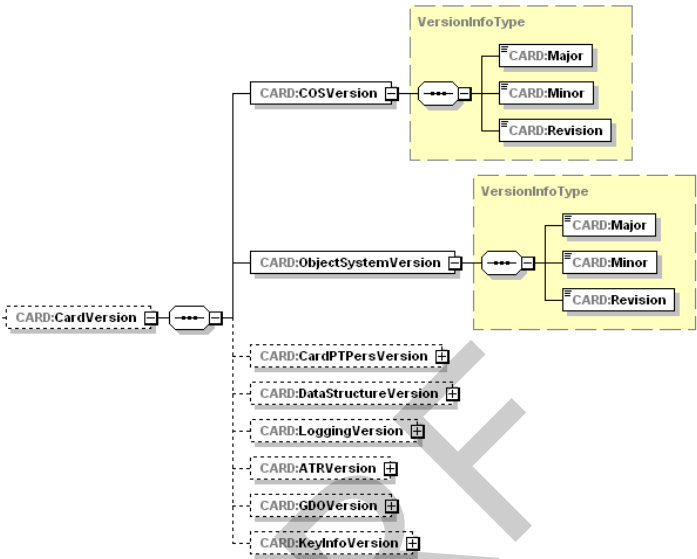
3597 Der Konnektors MUSS an der Außenschnittstelle eine Operation GetCards, wie in Tabelle
 3598 TAB_KON_565 „Operation GetCards“ beschrieben, anbieten und MUSS dabei Kartentypen
 3599 aus Tabelle TAB_KON_500 Wertetabelle Kartentypen unterscheiden.

3600 **Tabelle 143: TAB_KON_565 Operation GetCards**

Name	GetCards
Beschreibung	Liefert Informationen zu den in den Kartenterminals verfügbaren Karten zurück, die in Kartenterminals stecken, auf die Mandant und Clientsystem zugreifen dürfen. Insbesondere umfasst die Information die sog. Karten-Handles. Die Karten-Handles können bei anderen Konnektoraufrufen zur Adressierung von Karten genutzt werden.
Aufrufparameter	

	Name	Beschreibung
	@mandant-wide	Wenn „true“, werden alle Karten zurückgegeben, auf die der Mandant und das aufrufende Clientsystem zugreifen dürfen. Wenn „false“ (Standardbelegung), werden nur Karten zurückgegeben, auf die von dem im Aufrufkontext spezifizierten Arbeitsplatz zugegriffen werden darf.
	Context	Aufrufkontext
	CtId	Identifikation des Kartenterminals. Wenn angegeben, werden nur die Karten zurückgeliefert, die in diesem Kartenterminal verfügbar sind.
	SlotId	Nummer des Slots, beginnend bei 1. Wird zusätzlich zur CtId auch SlotId übergeben, so wird die Karte zurückgegeben, die in dem angegebenen Slot des mit CtId adressierten Kartenterminals steckt.
	CardType	Ein Kartentyp gemäß Tabelle TAB_KON_500 „Wertetabelle Kartentypen“ als optionaler Filter. Wenn angegeben, werden nur Karten vom spezifizierten Typ zurückgegeben. Unterstützt werden die Kartentypen EGK, KVK, HBAX, SM-B, SMC-KT und UNKNOWN.
Antwort		
	Name	Beschreibung
	Status	Ergebnis der Operation
	Im Element <code>Cards</code> wird die Liste der gesteckten Karten zurückgegeben. Für jede Karte wird dabei ein <code>Card</code> -Element angegeben. Leere Slots der Kartenterminals sind in dieser Liste nicht enthalten.	

	
Name	Beschreibung
Card Handle	<p>Handle, mit dem die Karte in Folgeaufrufen adressiert werden kann. Der Konnektor garantiert, dass dieses Handle die gesteckte Karte eindeutig identifiziert und bei Entfernen der Karte aus dem Kartenterminal ungültig wird.</p> <p>Auch für nicht erkannte Karten (z. B. bei falscher Steckrichtung der Karte) SOLL der Konnektor gültige Handles liefern (sofern das Kartenterminal in diesem Fall in der Lage ist, das entsprechende Ereignis „Karte wurde gesteckt“ zu liefern), damit diese Karten z. B. zum Auswurf adressiert werden können.</p>
CardType	<p>Erkannter Typ der Karte. Siehe Tabelle TAB_KON_500 Wertetabelle Kartentypen,</p>

	Card Version	 <p>Der Konnektor MUSS in CardVersion bei eGK, HBA und SM-B/SMC-KT der Generation 2 die Versionsinformationen gemäß [gemSpec_Karten_Fach_TIP] übergeben, für G1+ aus /MF/EF.Version. Bei KVK, HBA-VK und unbekannten Karten MUSS das Element weggelassen werden.</p>
	Iccsn	Falls auslesbar, die ICC-Serial-Number der Karte. Im Fall der KVK wird das optionale Element Iccsn nicht zurückgegeben.
	CtId	Identifikation des Kartenterminals, in dem die Karte steckt.
	SlotId	Nummer des Slots (beginnend bei 1), in dem die Karte steckt.
	InsertTime	Gibt den Zeitpunkt an, zu dem der Konnektor die Karte erkannt hat. Die Zeit wird mit dem Datentyp <code>DateTime</code> in folgendem Format angegeben: <code>yyyy-mm-ddThh:mm:ss+hh:mm</code> Es ist also – gemäß ISO 8601 [ISO8601] – die lokale Zeit und die Differenz zur UTC anzugeben.
	CardHolder Name	Name des Karteninhabers bzw. der Institution/Organisation (subject.commonName). Bei KVK und unbekannten Karten MUSS das Element weggelassen werden.

	Kvnr	KVNR (Unveränderbarer Teil) MUSS bei eGK belegt werden. Bei allen anderen Karten MUSS das Element weggelassen werden.
	Certificate Expiration Date	Ablaufdatum des Zertifikates (AUT bzw. OSIG). Bei KVK und unbekannten Karten MUSS das Element weggelassen werden.
Vorbedingungen	Keine.	
Nachbedingungen	Der Zustand der Karten und der Kartenterminals bleibt unverändert.	
Hinweise	Der Aufruf darf nur den im Konnektor verwalteten aktuellen Zustand der Karte liefern und keine Abfragen an die Kartenterminals absetzen.	

3601 Der Ablauf der Operation GetCards ist in Tabelle TAB_KON_566 Ablauf GetCards
 3602 beschrieben:
 3603

3604 **Tabelle 144: TAB_KON_566 Ablauf GetCards**

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	TUC_KON_000 „Prüfe Zugriffsberechtigung“	Die Prüfung erfolgt durch den Aufruf TUC_KON_000 { mandantId = \$context.mandantId; clientSystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; needCardSession = false; allWorkplaces = @mandant-wide} Tritt bei der Prüfung ein Fehler auf, bricht die Operation mit Fehlercode aus TUC_KON_000 ab.
3.	TUC_KON_253 „Liefere Karten_Liste“	Die Liste der Karten wird erstellt und zurückgegeben. Tritt hierbei ein Fehler auf, so bricht die Operation mit dem Fehler des TUCs ab. Wenn @mandant-wide=true dann ermittle die Liste der Karten für alle Arbeitsplätze des Mandanten für das angegebene Clientsystem durch den Aufruf TUC_KON_253 „Liefere Karten_Liste“ { clientSystemId = \$context.clientsystemId; cardTerminalId = CtId; slotId = SlotId;

		<pre> mandantId = \$context.mandantId; cardType = CardType } Wenn @mandant-wide=false dann ermittle die Liste der Karten für den Arbeitsplatz des Mandanten für das angegebene Clientsystem entsprechend \$context durch den Aufruf TUC_KON_253 „Liefere Karten_Liste“ { workplaceId= \$context.workplaceId; clientSystemId = \$context.clientsystemId; cardTerminalId = CtId; slotId = SlotId; mandantId = \$context.mandantId; cardType = CardType } </pre>
--	--	---

3605 Die Fehlerfälle der Operation GetCards sind in Tabelle TAB_KON_567 Fehlercodes
 3606 „GetCards dargestellt:
 3607

3608 **Tabelle 145: TAB_KON_567 Fehlercodes „GetCards“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weiteren Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler

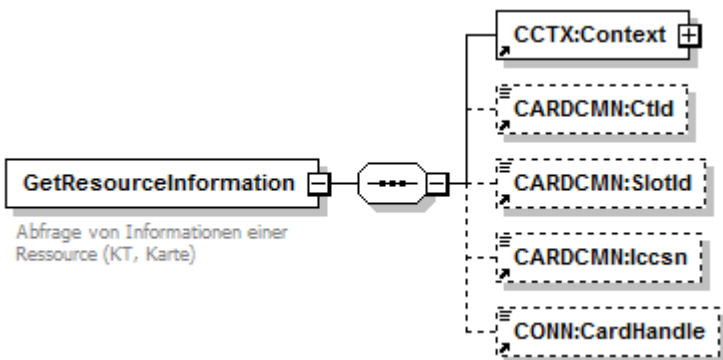
3609 [\leq]

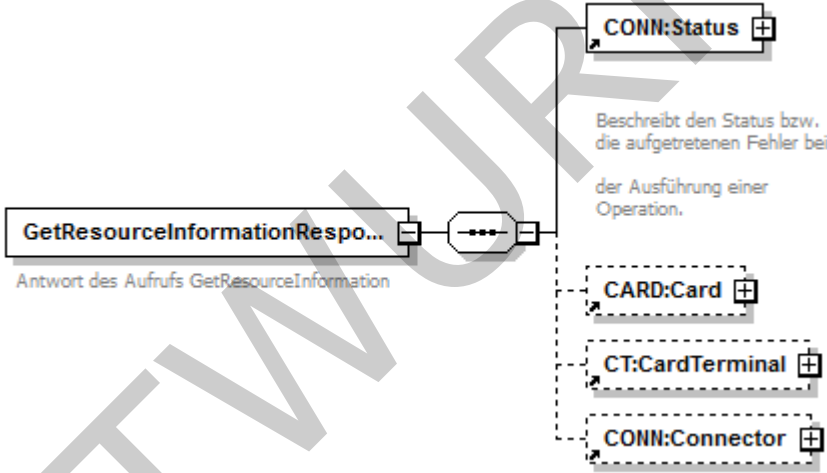
3610 4.1.6.5.3 GetResourceInformation

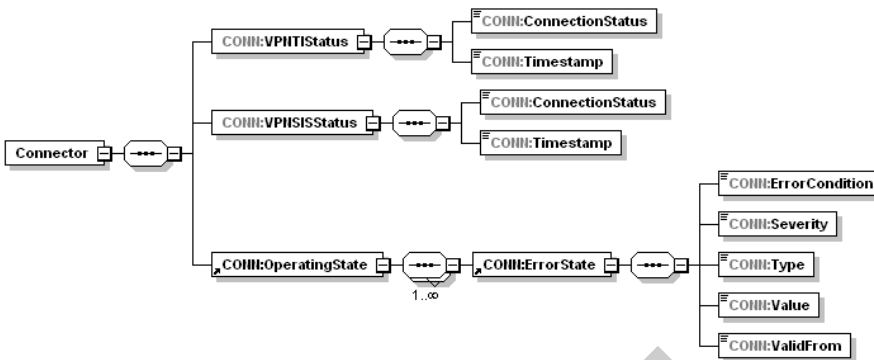
3611 TIP1-A_4607 - Operation GetResourceInformation

3612 Der Konnektor MUSS an der Außenschnittstelle eine Operation GetResourceInformation,
 3613 wie in Tabelle TAB_KON_568 „Operation GetResourceInformation“ beschrieben, anbieten.
 3614

3615 **Tabelle 146: TAB_KON_568 Operation GetResourceInformation**

Name	GetResourceInformation		
Beschreibung	Gibt Informationen zu einer Ressource (Karte, KT) oder dem Konnektor selbst zurück		
Aufrufparameter			
	Name	Beschreibung	

	Context	Aufrufkontext
	CtId	Identifikator eines Kartenterminals
	SlotId	Kartenslot-Nummer (in Kombination mit CtId)
	Iccsn	Iccsn einer Karte
	CardHandle	CardHandle einer Karte. Unterstützt werden die Kartentypen EGK, KVK, HBAX, SM-B, SMC-KT und UNKNOWN.
	Wurde keines der Elemente CtId, SlotId, Iccsn übergeben, so wird davon ausgegangen, dass der Aufrufer Informationen zum Konnektor selbst abfragen möchte.	
Rückgabe	 <p>Antwort des Aufrufs GetResourceInformation</p> <p>Beschreibt den Status bzw. die aufgetretenen Fehler bei der Ausführung einer Operation.</p>	
	Name	Beschreibung
	Status	Ergebnis der Operation
	Card	Informationen einer Karte (siehe GetCards)
	CardTerminal	Informationen eines Kartenterminals (siehe GetCardTerminals)
	Connector	Informationen zum Konnektor

	
VPNTISStatus	
VPNTISStatus/ ConnectionStatus	Status der VPN-Verbindung zur TI (Online oder Offline)
VPNTISStatus/ Timestamp	Zeitstempel der letzten Statusänderung
VPNSISStatus	
VPNSISStatus/ ConnectionStatus	Status der VPN-Verbindung des SIS (Online oder Offline)
VPNSISStatus/ Timestamp	Zeitstempel der letzten Statusänderung
OperatingState	Betriebszustand (siehe Kapitel 3.3)
OperatingState/ ErrorState	Eine Zeile der Fehlerzustandsliste gemäß Tabelle TAB_KON_503 Betriebszustand_Fehlerzustandsliste
OperatingState/ ErrorState/ ErrorCondition	ErrorCondition gemäß Tabelle TAB_KON_503 Betriebszustand_Fehlerzustandsliste
OperatingState/ ErrorState/Severity	Schwere des Fehlerzustandes gemäß Tabelle TAB_KON_503 Betriebszustand_Fehlerzustandsliste
OperatingState/ ErrorState/Type	Fehlertyp gemäß Tabelle TAB_KON_503 Betriebszustand_Fehlerzustandsliste
OperatingState/ ErrorState/Value	Fehlerzustandswert
OperatingState/ ErrorState/ValidFrom	Zeitstempel der letzten Änderung des Fehlerzustands
Vorbedingung	
Nachbedingung	Der Zustand der Ressource bleibt unverändert.

Hinweise

Der Ablauf der Operation GetResourceInformation ist in Tabelle TAB_KON_569 Ablauf GetResourceInformation beschrieben:

Tabelle 147: TAB_KON_569 Ablauf GetResourceInformation

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Insbesondere wird geprüft, dass eine SlotId nur in Verbindung mit einer CtId übergeben werden kann (Abfrage einer Karte). Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	TUC_KON_000 „Prüfe Zugriffs- berechtigung“	<p>Die Prüfung erfolgt,</p> <p>falls die Ressource der Konnektor ist, durch den Aufruf</p> <pre>TUC_KON_000 { mandantId = \$context.mandantId; clientSystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; ctId = null; cardHandle = null; needCardSession = false; allWorkplaces = true }</pre> <p>falls die Ressource ein Kartenterminal ist, durch den Aufruf</p> <pre>TUC_KON_000 { mandantId = \$context.mandantId; clientSystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; ctId = \$ctId; cardHandle = null; needCardSession = false; allWorkplaces = true }</pre> <p>falls die Ressource eine Karte ist, durch den Aufruf</p> <pre>TUC_KON_000 { mandantId = \$context.mandantId; clientSystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; ctId = null; cardHandle = \$cardHandle; needCardSession = false; allWorkplaces = false }</pre>

		Tritt bei der Prüfung ein Fehler auf, bricht die Operation mit Fehlercode aus TUC_KON_000 ab.
3.	TUC_KON_254 „Liefere Ressourcendetails“	Die Informationen zu der Ressource werden zusammengetragen und zurückgegeben. Tritt hierbei ein Fehler auf, so bricht die Operation mit dem Fehler des TUCs ab.

3620 Die Fehlerfälle der Operation GetResourceInformation sind in Tabelle TAB_KON_570
 3621 Fehlercodes „GetResourceInformation dargestellt:
 3622

3623 **Tabelle 148: TAB_KON_570 Fehlercodes „GetResourceInformation“**

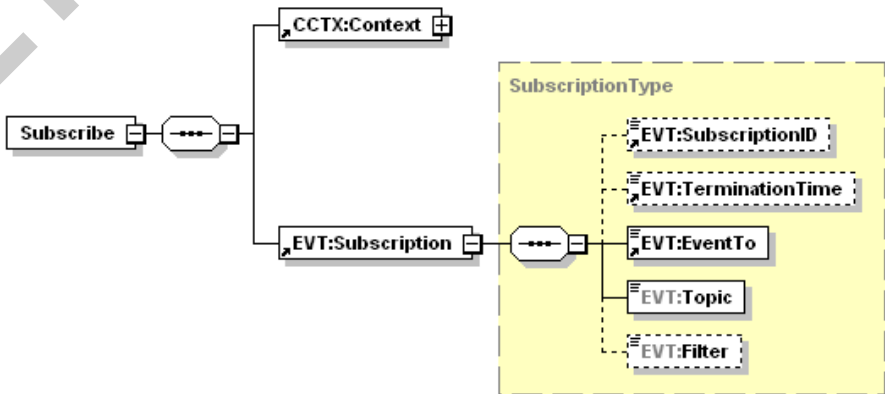
Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weiteren Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler

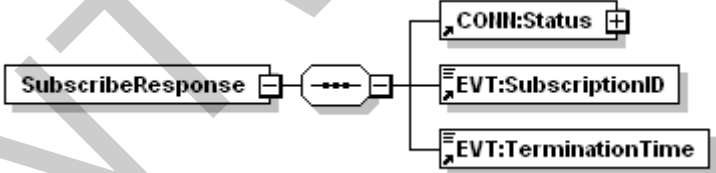
3624
 3625
 3626 [<=]

3627 4.1.6.5.4 Subscribe

3628 TIP1-A_4608 - Operation Subscribe
 3629 Der Konnektors MUSS an der Außenschnittstelle eine Operation Subscribe, wie in Tabelle
 3630 TAB_KON_571 Operation Subscribe beschrieben, anbieten.
 3631

3632 **Tabelle 149: TAB_KON_571 Operation Subscribe**

Name	Subscribe	
Beschreibung	Clientsysteme melden mit dieser Operation ihr Interesse an bestimmten Topics (Ereignissen) an.	
Aufrufparameter		
	Name	Beschreibung
	Context	Aufrufkontext

	SubscriptionID	Darf nicht verwendet werden
	TerminationTime	Darf nicht verwendet werden
	EventTo	URL des Endpunkts, wo die Ereignisse zugestellt werden sollen. Syntax: <i>cetp://host:port</i> <i>host</i> : IP-Adresse oder FQDN des Clientsystems. <i>port</i> : Portnummer des Kommunikationsendpunkts, an dem das Clientsystem auf die Zustellung der Ereignisse wartet.
	Topic	Ein Topic, für das das Clientsystem sein Interesse anmeldet.
	Filter	Filter für die Ereignisnachricht (X-Path Ausdruck im Kontext mit Default Namespace gleich "http://ws.gematik.de/conn/EventService/v7.2" " ohne Verwendung eines Namespace-Präfixes sowie Namensraum mit Präfix EVT gleich "http://ws.gematik.de/conn/EventService/v7.2", der beim Versand von Ereignissen in TUC_KON_256 ausgewertet wird. Ermöglicht die Filterung auf Basis der Elemente einer XML-Ereignisnachricht)
Rückgabe		
	Name	Beschreibung
	Status	Ergebnis der Operation
	SubscriptionID	Ein Identifikator, der die Anmeldung für die Topics eindeutig identifiziert. Bei den Operationen Unsubscribe, GetSubscription und RenewSubscriptions MUSS dieser SubscriptionID angegeben werden.
	TerminationTime	Maximaler Gültigkeitszeitpunkt der Subscription. Sie MUSS auf Systemzeit + 25 h gesetzt werden.
Vorbedingung	Das Clientsystem muss die Ereignissenke realisieren.	
Nachbedingung	Nach erfolgreicher Anmeldung vermerkt der Konnektor das angemeldete Topic unter dem SubscriptionID. Der Konnektor muss die Anmeldungen so lange als gültig behandeln, bis entweder das Clientsystem diese explizit abmeldet	

	<p>oder der Konnektor das Clientsystem als nicht mehr erreichbar erkennt (siehe nächsten Punkt) oder der Konnektor neu gestartet oder ausgeschaltet wird oder die TerminationTime kleiner als die Systemzeit ist.</p> <p>Der Konnektor muss die Anmeldung aus seiner Verwaltung entfernen („Auto-Unsubscribe“), wenn EVT_MAX_TRY Verbindungsaufbauversuche oder zählbare Zustellungsversuche (z.B. durch Zählung beim Absenden der Zustellversuche) in Folge fehlgeschlagen sind. Wenn die Ereignissenke Zustellungen grundsätzlich nicht beantwortet, so sind nur die Verbindungsaufbauversuche zu zählen.</p>
Hinweise	

3633 Der Ablauf der Operation Subscribe ist in Tabelle TAB_KON_572 Ablauf Subscribe
 3634 beschrieben:
 3635

3636 **Tabelle 150: TAB_KON_572 Ablauf Subscribe**

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	TUC_KON_000 „Prüfe Zugriffs- berechtigung“	<p>Die Prüfung erfolgt durch den Aufruf TUC_KON_000_000 { mandantId = \$context.mandantId; clientsystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; needCardSession = false; allWorkplaces = true } Tritt bei der Prüfung ein Fehler auf, so bricht die Operation mit dem Fehlercode aus TUC_KON_000 ab.</p>
3.	saveSubscription	<p>Die Anmeldung wird im Konnektor hinterlegt. Vorgehalten werden folgende Daten:</p> <ul style="list-style-type: none"> • SubscriptionId (wird generiert) • TerminationTime (Systemzeit + 25h) • MandantId • ClientsystemId • WorkplaceId • Ereignissenke (Feld EventTo) • Abonnierter Topic (Feld Topic) • Filterausdruck (Feld Filter) <p>Bei der Übernahme wird eine eindeutige SubscriptionId generiert, die dem aufrufenden System</p>

		zurückgegeben wird, falls die Subscription noch nicht existiert. Existiert sie bereits, wird die bestehende SubscriptionID zurückgegeben.
--	--	---

3637 Die Fehlerfälle der Operation Subscribe sind in Tabelle TAB_KON_573 Fehlercodes
 3638 „Subscribe dargestellt:
 3639

3640 **Tabelle 151 TAB_KON_573 Fehlercodes „Subscribe“**

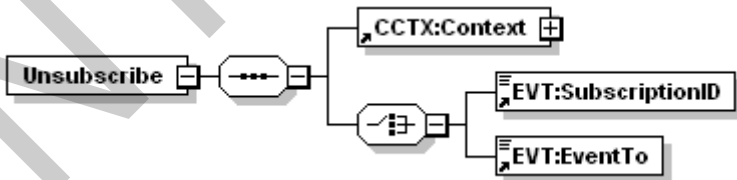

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weiteren Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler

3641
 3642
 3643 [\leq]

3644 4.1.6.5.5 Unsubscribe

3645 TIP1-A_4609 - Operation Unsubscribe
 3646 Der Konnektors MUSS an der Außenschnittstelle eine Operation Unsubscribe, wie in
 3647 Tabelle TAB_KON_574 Operation Unsubscribe beschrieben, anbieten.
 3648

3649 **Tabelle 152: TAB_KON_574 Operation Unsubscribe**

Name	Unsubscribe		
Beschreibung	Löscht eine Anmeldung mit dem angegebenen SubscriptionID oder alle Anmeldungen zu einem Endpunkt EventTo.		
Aufrufparameter			
	Name	Beschreibung	
	Context	Aufrufkontext	
	SubscriptionID	Der Identifikator, der bei der Subscribe-Operation geliefert wurde.	
	EventTo	URL des clientseitigen Endpunkts, wie er bei der Subscribe-Operation angegeben wurde.	
Rückgabe			
	Name	Beschreibung	
	Status	Ergebnis der Operation	

Vorbedingung	Die Anmeldung <code>Subscribe</code> muss vor dieser Operation aufgerufen worden sein.
Nachbedingung	Der Konnektor entfernt aus seiner Verwaltung die Subscription zur <code>Subscription-ID</code> bzw. alle Subscriptions zur clientseitigen URL des Endpunkts <code>EventTo</code> .
Hinweise	Keine

Der Ablauf der Operation `Unsubscribe` ist in Tabelle TAB_KON_575 Ablauf `Unsubscribe` beschrieben:

Tabelle 153: TAB_KON_575 Ablauf Unsubscribe

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	<code>checkArguments</code>	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	TUC_KON_000 „Prüfe Zugriffs- berechtigung“	Die Prüfung erfolgt durch den Aufruf <pre>TUC_KON_000 { mandantId = \$context.mandantId; clientsystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; needCardSession = false; allWorkplaces = true } </pre> Tritt bei der Prüfung ein Fehler auf, bricht die Operation mit Fehlercode aus TUC_KON_000 ab.
3.	<code>removeSubscription</code>	Entfernen der Subscriptions aus der Liste aller Subscriptions.

Die Fehlerfälle der Operation `Unsubscribe` sind in Tabelle TAB_KON_576 Fehlercodes „Unsubscribe“ dargestellt:

Tabelle 154: TAB_KON_576 Fehlercodes „Unsubscribe“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weiteren Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler
4102	Technical	Error	ungültige SubscriptionId

[<=]

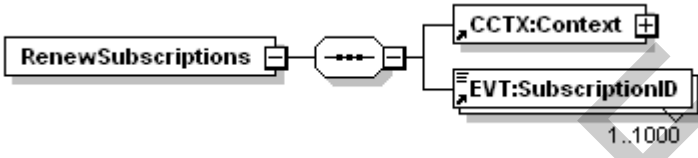
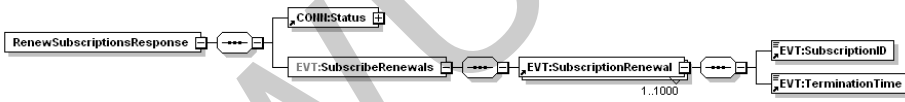
4.1.6.5.6 *RenewSubscriptions*

TIP1-A_5112 - Operation `RenewSubscriptions`

3663 Der Konnektors MUSS an der Außenschnittstelle eine Operation RenewSubscriptions, wie
 3664 in Tabelle TAB_KON_792 Operation RenewSubscriptions beschrieben, anbieten.

3665

3666 **Tabelle 155: TAB_KON_792 Operation RenewSubscriptions**

Name	RenewSubscriptions	
Beschreibung	Verlängert die Gültigkeit einer Liste von Anmeldungen, die jeweils per SubscriptionID identifiziert werden.	
Aufrufparameter		
	Name	Beschreibung
	Context	Aufrufkontext
	Subscription ID	Der Identifikator, der bei der Subscribe-Operation geliefert wurde.
Rückgabe		
	Name	Beschreibung
	Status	Ergebnis der Operation
	Subscription ID	Ein Identifikator, der die Anmeldung für die Topics eindeutig identifiziert. Bei den Operationen Unsubscribe, GetSubscription und RenewSubscriptions MUSS diese SubscriptionID angegeben werden.
	Termination Time	Maximaler Gültigkeitszeitpunkt der Subscription. Sie MUSS auf Systemzeit + 25 h gesetzt werden.
Vorbedingung		
Nachbedingung	Der Konnektor speichert jede neu vergebene TerminationTime in seiner Verwaltung der Subscriptions.	
Hinweise	Keine	

3667 Der Ablauf der Operation RenewSubscriptions ist in Tabelle TAB_KON_793 Ablauf
 3668 RenewSubscriptions beschrieben:

3669

3670 **Tabelle 156: TAB_KON_793 Ablauf RenewSubscriptions**

Nr.	Aufruf Technischer Use Case oder	Beschreibung
-----	--	--------------

	Interne Operation	
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	TUC_KON_000 „Prüfe Zugriffs- berechtigung“	Die Prüfung erfolgt durch den Aufruf TUC_KON_000 { mandantId = \$context.mandantId; clientsystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; needCardSession = false; allWorkplaces = true } Tritt bei der Prüfung ein Fehler auf, bricht die Operation mit Fehlercode aus TUC_KON_000 ab.
3.	renewSubscriptions	Es wird eine neue <code>SubscribeRenewals</code> -Liste angelegt. Alle Subscriptions, deren <code>TerminationTime</code> kleiner als die Systemzeit sind, muss der Konnektor aus der Verwaltung entfernen. Für jede <code>SubscriptionID</code> , die in der Verwaltung der Subscriptions existiert und deren <code>TerminationTime</code> größer als die Systemzeit ist, wird eine neue <code>TerminationTime = Systemzeit + 25h</code> bestimmt. Diese wird zusammen mit der <code>SubscriptionID</code> als <code>SubscribeRenewal</code> der <code>SubscribeRenewals</code> -Liste hinzugefügt. Kommt es zu keiner Subscription-Verlängerung, weil nur ungültige SubscriptionIDs im Aufruf angegeben waren, wird der Fehler 4102 zurückgeliefert. Kommt es zu mindestens einer Subscription-Verlängerung, sind aber auch ungültige SubscriptionIDs im Aufruf, wird eine <code>RenewSubscriptionsResponse</code> zurückgeliefert, mit <code>CONN:Status/CONN:Result = "Warning"</code> , <code>GERROR:Trace</code> mit {Fehlercode: 4102, ErrorType: Technical, Severity: Error, Fehlertext: "Ungültige SubscriptionId"}, und der Information, welche SubscriptionsIDs ungültig waren.

3671 Die Fehlerfälle der Operation `RenewSubscriptions` sind in Tabelle TAB_KON_794
 3672 Fehlercodes „RenewSubscriptions dargestellt:

3673

3674 **Tabelle 157: TAB_KON_794 Fehlercodes „RenewSubscriptions“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weiteren Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler
4102	Technical	Error	Ungültige SubscriptionId

3675

3676

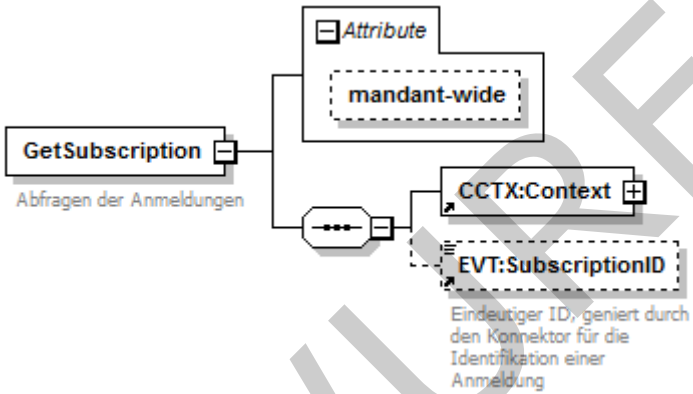
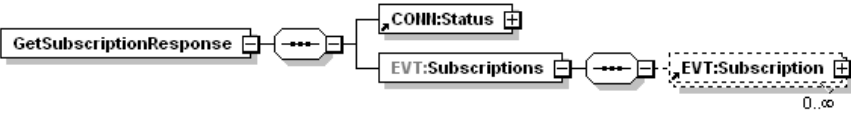
3677 [**<=**]

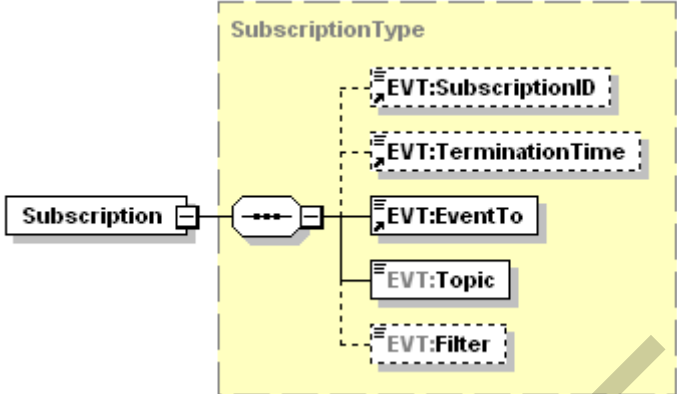
3678 4.1.6.5.7 GetSubscription

3679 TIP1-A_4610 - Operation GetSubscription

3680 Der Konnektor MUSS an der Außenschnittstelle eine Operation GetSubscription, wie in
 3681 Tabelle TAB_KON_577 Operation GetSubscription beschrieben, anbieten.
 3682

3683 **Tabelle 158: TAB_KON_577 Operation GetSubscription**

Name	GetSubscription	
Beschreibung	Gibt die Liste der angemeldeten Topics zurück	
Aufrufparameter		
	Name	Beschreibung
	@mandant-wide	Wenn „true“, werden alle Subscriptions zurückgegeben, die Mandant und Clientsystem zugeordnet sind. Wenn „false“ (Standardbelegung) werden alle Subscriptions zurückgegeben, die dem im Aufrufkontext spezifizierten Tripel aus Clientsystem, Mandanten und Arbeitsplatz zugeordnet sind.
	Context	Aufrufkontext
	SubscriptionID	Der Identifikator, der bei der Subscribe-Operation geliefert wurde.
Rückgabe		
	Name	Beschreibung
	Status	Ergebnis der Operation
	Subscriptions	Die Liste Subscriptions (vgl. Operation Subscribe)

		
	Subscription	Angefordertes Subscription-Element
	Subscription/ SubscriptionID	Identifikator der Subscription
	Subscription/ TerminationTime	Maximaler Gültigkeitszeitpunkt der Subscription.
	Subscription/ EventTo	URL des Endpunkts, wo die Ereignisse zugestellt werden sollen (Ereignissenke)
	Subscription/ Topic	Angemeldeter Topic
	Subscription/ Filter	Filterausdruck (falls vorhanden)
Vorbedingung	Keine	
Nachbedingung	Die Liste der Subscriptions bleibt unverändert	
Hinweise	Keine	

3684 Der Ablauf der Operation GetSubscription ist in Tabelle TAB_KON_578 Ablauf
 3685 GetSubscription beschrieben:
 3686

3687 **Tabelle 159: TAB_KON_578 Ablauf GetSubscription**

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	TUC_KON_000 „Prüfe Zugriffs- berechtigung“	Die Prüfung erfolgt durch den Aufruf TUC_KON_000 { mandantId = \$context.mandantId; clientsystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; needCardSession = false; allWorkplaces = @mandant-wide }

		Tritt bei der Prüfung ein Fehler auf, bricht die Operation mit Fehlercode aus TUC_KON_000 ab.
3.	getSubscriptions	Rückgabe der Subscription, die durch <code>SubscriptionId</code> identifiziert wird. Wurde keine <code>SubscriptionId</code> angegeben und <code>@mandant-wide="true"</code> , werden alle Subscriptions zurückgegeben, die dem angegebenen Clientsystem und Mandanten zugeordnet werden können. Wurde keine <code>SubscriptionId</code> angegeben und <code>@mandant-wide="false"</code> , werden alle Subscriptions zurückgegeben, die dem angegebenen Clientsystem, Mandanten und Arbeitsplatz zugeordnet werden können.

Die Fehlerfälle der Operation GetSubscription sind in Tabelle TAB_KON_579 Fehlercodes „GetSubscription dargestellt:

Tabelle 160: TAB_KON_579 Fehlercodes „GetSubscription“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weiteren Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler
4102	Technical	Error	ungültige SubscriptionId

[<=]

4.1.6.5.8 GetLeCards

4.1.6.6 Betriebsaspekte

TIP1-A_4611 - Konfigurationswerte des Systeminformationsdienstes
Die Managementschnittstelle MUSS es einem Administrator ermöglichen Konfigurationsänderungen gemäß Tabelle TAB_KON_580 vorzunehmen:

Tabelle 161: TAB_KON_580 Konfigurationswerte des Systeminformationsdienstes (Administrator)

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
EVT_MAX_TRY	Nummer	Der Administrator MUSS über diesen Konfigurationsparameter die Anzahl der Fehlversuche bzgl. Verbindungsversuche bzw. Ereigniszustellungen festlegen können. Ist diese maximal zulässige Anzahl der Fehlversuche überschritten, muss der Konnektor automatisch ein „Auto-Unsubscribe“ (analog Operation

		„Unsubscribe“ mit „EventTo gleich der URL des clientseitigen Endpunkts“) durchführen.
--	--	---

3703

3704 [\leq]

3705 TIP1-A_4612 - Maximale Anzahl an Subscriptions

3706 Der Konnektor MUSS eine Mindestmenge von 999 Subscriptions insgesamt unterstützen.

3707 Der Konnektorhersteller kann jedoch die Anzahl der maximal möglichen Subscriptions
3708 (insgesamt und/oder pro Ziel) festlegen.3709 [\leq]

3710 TIP1-A_4613 - Initialisierung Subscriptions-Liste beim Bootup

3711 Der Konnektor MUSS beim Bootup mit einer leeren Liste an Subscriptions starten.

3712 [\leq]3713 **4.1.7 Verschlüsselungsdienst**3714 Der Verschlüsselungsdienst bietet Schnittstellen zum hybriden und symmetrischen Ver-
3715 und Entschlüsseln von Dokumenten an.3716 Der Verschlüsselungsdienst bietet für alle `Alle_DocFormate` die hybride und
3717 symmetrische Ver- und Entschlüsselung nach dem Cryptographic Message Syntax (CMS)
3718 Standard an [RFC5652].3719 Darüber hinaus werden folgende formaterhaltende Ver-/Entschlüsselungsmechanismen
3720 unterstützt:

- 3721 • hybride Ver-/Entschlüsselung von XML-Dokumenten nach der W3C
- 3722 Recommendation „XML Encryption Syntax and Processing“ [XMLEnc]
- 3723 • hybride Ver-/Entschlüsselung von MIME-Dokumenten nach dem S/MIME-Standard
- 3724 [S/MIME]

3725 Der Konnektor muss bezüglich der zur Ver- und Entschlüsselung von Dokumenten
3726 verwendeten Verfahren und Algorithmen die Vorgaben in [gemSpec_Krypt#3.1.4] sowie
3727 in [gemSpec_Krypt#3.1.5] und hinsichtlich ECC-Migration die Vorgaben aus
3728 [gemSpec_Krypt#5] erfüllen.

3729 **4.1.7.1 Funktionsmerkmalweite Aspekte**

3730 TIP1-A_4614 - Missbrauchserkennung Verschlüsselungsdienst

3731 Der Konnektors MUSS zur Unterstützung von Missbrauchserkennungen die in Tabelle
3732 TAB_KON_581 gelisteten Operationen als Einträge in EVT_MONITOR_OPERATIONS
3733 berücksichtigen.

3734

3735 **Tabelle 162: TAB_KON_581 Verschlüsselungsdienst-Operationen für**
3736 **EVT_MONITOR_OPERATIONS**

Operationsname	OK_Val	NOK_Val	Alarmwert (Default-Grenzwert 10 Minuten- Σ)
EncryptDocument	1	5	101
DecryptDocument	1	5	101

3737

3738 [\leq]

3739 TIP1-A_5434 - Verschlüsselung/Entschlüsselung eines XML Dokuments ergibt
3740 unverändertes XML-Dokument
3741 Der Konnektor MUSS das Operationspaar Verschlüsselung/Entschlüsselung so
3742 implementieren, dass Dokumente vom Typ XML unverändert bleiben, wobei zwei XML-
3743 Dokumente als identisch zu betrachten sind, wenn sie gemäß Canonical XML 1.1 gleich
3744 sind [CanonXML1.1].[<=]

3745

3746 A_17746 - Einsatzbereich und Vorgaben für Ver- und Entschlüsselung (ECC-Migration)
3747 Der Konnektor MUSS für die kartenbasierte Ver- und Entschlüsselung die Zertifikate und
3748 Schlüssel in Abhängigkeit vom kryptographischen Verfahren unter Berücksichtigung des
3749 Einsatzbereiches aus TAB_KON_747 ermitteln.[<=]

3750

3751 **Tabelle 163: TAB_KON_747 KeyReference für Encrypt-/DecryptDocument**

Karte	KeyReference	Crypt	Zertifikat (Encrypt) ...in DF.ESIGN	Schlüssel (Decrypt) ...in DF.ESIGN	Einsatzbereich	
					Außen- schnittste lle	Fachmod ul- schnittste lle
HBA	C.ENC	RSA_E CC	EF.C.HP.ENC.R20 48 EF.C.HP.ENC.E25 6	PrK.HP.ENC.R20 48 PrK.HP.ENC.E25 6	Ja	Ja
		ECC	EF.C.HP.ENC.E25 6	PrK.HP.ENC.E25 6	Ja	Ja
		RSA	EF.C.HP.ENC.R20 48	PrK.HP.ENC.R20 48	Ja	Ja
SM- B	C.ENC	RSA_E CC	EF.C.HCI.ENC.R2 048 EF.C.HCI.ENC.E2 56	PrK.HCI.ENC.R2 048 PrK.HP.ENC.E25 6	Ja	Ja
		ECC	EF.C.HCI.ENC.E2 56	PrK.HP.ENC.E25 6	Ja	Ja
		RSA	EF.C.HCI.ENC.R2 048	PrK.HCI.ENC.R2 048	Ja	Ja
HBA -VK	C.ENC	RSA_E CC RSA	EF.C.HP.ENC	PrK.HP.ENC	Ja	Ja
eGK	C.ENC	ECC	C.CH.ENC.E256	PrK.CH.ENC.E25 6	Nein	Ja

	C.ENC	RSA	C.CH.ENC.R2048	PrK.CH.ENC.R2048	Nein	Ja
--	-------	-----	----------------	------------------	------	----

3752

3753

3754

Tabelle 164: TAB_KON_859 Werteliste und Defaultwert des Parameters crypt bei hybrider Verschlüsselung

Typname	Werteliste	Defaultwert	Bedeutung
ENC_CRYPT	RSA ECC RSA_ECC	RSA	Werteliste des Parameters crypt bei der hybriden Verschlüsselung RSA: Es wird RSA-2048 basiert verschlüsselt. ECC: Es wird ECC-256 basiert verschlüsselt. RSA_ECC: Es wird dual RSA-2048 basiert und ECC-256 basiert verschlüsselt. Es wird als Fehlerfall gewertet, wenn weder RSA- noch ECC-Zertifikat von der Karte geladen werden konnten, und als Warnung, wenn nur ein Zertifikat geladen werden konnte.

3755

4.1.7.2 Durch Ereignisse ausgelöste Reaktionen

3756

Keine.

3757

4.1.7.3 Interne TUCs, nicht durch Fachmodule nutzbar

3758

Keine.

3759

4.1.7.4 Interne TUCs, auch durch Fachmodule nutzbar

3760

Die in diesem Kapitel beschriebenen TUCs zur hybriden Ver- und Entschlüsselung werden den Fachmodulen und Außenoperationen angeboten. Die TUCs zur symmetrischen Ver-/Entschlüsselung werden den Fachmodulen angeboten. Es gibt keine Aufrufhierarchie innerhalb der hier beschriebenen TUCs zur hybriden und symmetrischen Ver-/Entschlüsselung.

3761

3762

3763

3764

3765

4.1.7.4.1 TUC_KON_070 „Daten hybrid verschlüsseln“

3766

TIP1-A_4616 - TUC_KON_070 „Daten hybrid verschlüsseln“

3767

Der Konnektor MUSS den technischen Use Case TUC_KON_070 „Daten hybrid verschlüsseln“ umsetzen.

3768

3769

3770

Tabelle 165: TAB_KON_739 - TUC_KON_070 „Daten hybrid verschlüsseln“

Element	Beschreibung
Name	TUC_KON_070 „Daten hybrid verschlüsseln“

Beschreibung	<p>Dieser TUC verschlüsselt ein Dokument oder Teile eines Dokumentes. Die Verschlüsselung erfolgt zweistufig, d. h. die Daten werden symmetrisch mit einem generierten Schlüssel verschlüsselt und anschließend wird dieser Schlüssel mit einem asymmetrischen Verfahren verschlüsselt.</p> <p>Die asymmetrische Verschlüsselung des symmetrischen Schlüssels kann für mehrere Identitäten, repräsentiert durch X.509-Zertifikate oder öffentliche Schlüssel, erfolgen. Das Ergebnis sind entsprechend viele Verschlüsselungen desselben symmetrischen Schlüssels.</p> <p>Es werden die folgenden formaterhaltenden Verschlüsselungsverfahren für die genannten Dokumententypen unterstützt:</p> <ul style="list-style-type: none"> • XML mit [XMLEnc] • MIME mit [S/MIME] <p>Des Weiteren ist für alle unterstützten Dokumentformate (Alle_DocFormate) die Verschlüsselung mit CMS [RFC5652] möglich.</p>
Auslöser	Aufruf durch einen Fachmodul-TUC oder durch die Operation EncryptDocument des Verschlüsselungsbasisdienstes
Vorbedingungen	Falls mit einem öffentlichen Schlüssel auf einer Karte verschlüsselt werden soll, muss die Karte gesteckt sein.
Eingangsdaten	<ul style="list-style-type: none"> • documentToBeEncrypted (Zu verschlüsselndes Dokument) • encryptionCertificates – <i>optional/entfällt, wenn encryptionKeys übergeben wird</i> (X.509v3-Zertifikate) • encryptionKeys – <i>optional/entfällt, wenn encryptionCertificates übergeben wird</i> (öffentliche Schlüssel; unterstützte Karten sind SM-B, HBAX und eGK) • encryptionType [EncryptionType] (Angaben zum einzusetzenden Verschlüsselungsverfahren (CMS, XMLEnc oder S/MIME)). • cardSession – <i>optional/verpflichtend, wenn ein Zertifikat von einer Karte gelesen werden soll</i> (Kartensitzung; unterstützte Karten sind SM-B, HBAX und eGK.) • certificateReference – <i>optional/verpflichtend, wenn ein Zertifikat von einer Karte gelesen werden soll</i> (Zertifikatsreferenz; unterstützte Karten sind SM-B, HBAX und eGK). • crypt [ENC_CRYPT] - <i>optional; default und Wertebereich siehe TAB_KON_859</i> (Wenn das Verschlüsselungszertifikat von einer Karte

	<p><i>kommt, steuert <code>crypt</code>, mit welchen kryptographischen Verfahren die Verschlüsselung der Hybridschlüssel erfolgt.)</i></p> <ul style="list-style-type: none"> • <code>xmlElements</code> – <i>optional/verpflichtend, wenn <code>encryptionType</code> = <code>XMLEnc</code></i> (Festlegung der zu verschlüsselnden Teile des Dokumentes durch Spezifikation eines Xpath-Ausdruckes (XML-Elements). • <code>keyInfoMode</code> [embedded separate] – <i>optional/verpflichtend, wenn <code>encryptionType</code> = <code>XMLEnc</code></i> (Angabe, ob die <code>KeyInfo</code> in das XML-Dokument eingebettet oder separat an den Aufrufer zurückgegeben werden soll)
Komponenten	Konnektor, Kartenterminal, Karte
Ausgangsdaten	<ul style="list-style-type: none"> • <code>encryptedDocument</code> (Verschlüsseltes Dokument) • <code>encryptedKeys</code> – <i>optional/verpflichtend, wenn diese nicht im verschlüsselten Dokument enthalten sind</i> (Verschlüsselte symmetrische Schlüssel) • <code>keyInfo</code> – <i>optional/verpflichtend, wenn <code>encryptionType</code> = <code>XMLEnc</code> und <code>keyInfoMode</code> = <code>separate</code></i> (<code>KeyInfo</code>, falls nicht ins Dokument eingebettet)
Standardablauf	<ol style="list-style-type: none"> 1. Das Verschlüsselungsverfahren wird anhand des Eingangsparameters <code>EncryptionType</code> gewählt. 2. <u>Nur für <code>XMLEnc</code>:</u> Die zu verschlüsselnden XML-Elemente werden lokalisiert. Falls kein zu verschlüsselndes XML-Element gefunden wurde, wird Fehler 4103 gemeldet. Die zu verschlüsselnden XML-Elemente dürfen nicht ineinander verschachtelt sein. Sind die zu verschlüsselnden XML-Elemente ineinander verschachtelt, so wird Fehler 4104 gemeldet. 3. Für jedes von der Karte zu lesende Zertifikat, wird <code>TUC_KON_216</code> „Lese Zertifikat“ aufgerufen. Welches Zertifikat von der Karte gelesen werden soll, wird durch den Parameter <code>crypt</code> über Tabelle <code>TAB_KON_747</code> gesteuert. In den Fällen <code>crypt</code> = <code>RSA</code> und <code>crypt</code> = <code>ECC</code> bricht der TUC ab, wenn dabei ein Fehler auftritt. Im Fall <code>crypt</code> = <code>RSA_ECC</code> bricht der TUC im Fehlerfall dann ab, wenn weder <code>RSA</code>- noch <code>ECC</code>-Zertifikat geladen werden konnte, und läuft mit einer Warnung durch, wenn nur ein Zertifikat geladen werden konnte. 4. Falls Zertifikate übergeben oder von der Karte gelesen wurden, werden diese durch Aufruf von <code>TUC_KON_037</code> „Zertifikat prüfen“ geprüft. Als Parameter des TUC-Aufrufs gilt für Zertifikate, die mit

	<p>Zertifikaten aus CERT_IMPORTED_CA_LIST geprüft werden:</p> <pre>TUC_KON_037 „Zertifikat prüfen“ { certificate = Zertifikat; qualifiedCheck = not_required; offlineAllowNoCheck = true; intendedKeyUsage= intendedKeyUsage(Zertifikate aus CERT_IMPORTED_CA_LIST); validationMode = NONE }</pre> <p>Für alle anderen Zertifikate gilt: {</p> <pre> certificate = [C.CH.ENC]; qualifiedCheck=not_required; offlineAllowNoCheck=false; policyList =[oid_egk_enc]; intendedKeyUsage= intendedKeyUsage(C.CH.ENC); validationMode=OCSP }</pre> <p>oder</p> <pre>{ certificate = [C.CH.ENCV]; qualifiedCheck=not_required; offlineAllowNoCheck=false; policyList =[oid_egk_encv]; intendedKeyUsage= intendedKeyUsage(C.CH.ENCV); validationMode=OCSP }</pre> <p>oder</p> <pre>{ certificate = [C.HCI.ENC]; qualifiedCheck=not_required; offlineAllowNoCheck=false; policyList =[oid_smc_b_enc]; intendedKeyUsage= intendedKeyUsage(C.HCI.ENC); validationMode=OCSP }</pre> <p>oder</p> <pre>{ certificate = [C.HP.ENC]; qualifiedCheck=not_required; offlineAllowNoCheck=false; policyList =[oid_hba_enc]; intendedKeyUsage= intendedKeyUsage(C.HP.ENC); validationMode=OCSP }</pre> <ol style="list-style-type: none"> Die öffentlichen Schlüssel werden aus den Zertifikaten extrahiert, falls sie nicht direkt übergeben wurden. Falls ein Schlüssel keinen der zugelassenen Verschlüsselungsalgorithmen gemäß [gemSpec_Krypt#3.5.2] bzw. [gemSpec_Krypt#5.8] erlaubt, wird Fehler 4200 gemeldet. Der Konnektor generiert einen symmetrischen Schlüssel. Dabei muss der symmetrische Schlüssel den Kriterien aus [gemSpec_Krypt#2.4] entsprechen.
--	---

	<p>7. Der Konnektor verschlüsselt das Dokument oder Teile des Dokuments mit dem generierten symmetrischen Schlüssel.</p> <p>a. <u>CMS:</u> Es MÜSSEN die Vorgaben aus [gemSpec_Krypt#3.5.1] beachtet werden.</p> <p>b. <u>XMLEnc:</u> Alle zu verschlüsselnden XML-Elemente werden mit demselben symmetrischen Schlüssel verschlüsselt. Dabei MÜSSEN die Vorgaben aus [gemSpec_Krypt#3.1.4] beachtet werden.</p> <p>8. Der symmetrische Schlüssel wird asymmetrisch für die einzelnen Identitäten verschlüsselt. Dabei müssen die Vorgaben aus [gemSpec_Krypt#3.1.5; 3.5.2; 5.8] beachtet werden.</p> <p>9. Das Zieldokument wird erstellt. <u>XMLEnc</u> Format und Inhalt des verschlüsselten Dokuments SOLLEN dem XML Encryption Format in [COMMON_PKI#Part 8] folgen. Zum Format des verschlüsselten XML-Dokumentes siehe auch Tabelle TAB_KON_073 Vorgaben zum Format verschlüsselter XML-Dokumente. Die verschlüsselten Datenelemente (EncryptedData) werden erstellt. EncryptedData ersetzt jeweils das zu verschlüsselnde Element des XML-Dokuments. In [COMMON_PKI] wird die Verwendung des Attributs Type in EncryptedData ausgeschlossen; diese Spezifikation sieht jedoch dessen Verwendung für verschlüsselte XML-Bestandteile (element, content) wie in [XMLEnc] beschrieben vor. Der Namespace von EncryptedData ist als http://www.w3.org/2001/04/xmlenc# anzugeben.</p> <p>Für das Element EncryptedData wird das Sub-Element EncryptionMethod mit Angaben zum Verschlüsselungsalgorithmus als obligatorisch vorgegeben, ebenso die Elemente KeyInfo und CipherData. Das Element EncryptedData/KeyInfo hat den Namespace "http://www.w3.org/2000/09/xmldsig#". Es muss pro Hybridschlüssel ein Element EncryptedKey enthalten. In jedem EncryptedKey-Element wird neben dem eigentlichen Hybridschlüssel ein Element zur EncryptionMethod der asymmetrischen Verschlüsselung und ein KeyInfo-Element mit dem Zertifikat angelegt, das für die Verschlüsselung des symmetrischen Schlüssels verwendete wurde. Das Zertifikat wird jeweils im Element EncryptedKey/KeyInfo/X509Data/X509Certificate base64-kodiert und darin DER-kodiert abgelegt. Hybridschlüssel (RSA): Das Element EncryptedData/KeyInfo/EncryptedKey muss</p>
--	---

	<p>die Verschlüsselungsmethode im Element EncryptionMethod angeben, den hybridSchlüssel im Element CipherData speichern und das Zertifikat, mit dem der symmetrische Schlüssel zum Hybridschlüssel verschlüsselt wurde, im Element EncryptedKey/KeyInfo/X509Data/X509Certificate base64-kodiert und darin DER-kodiert ablegen.</p> <p>Hybridschlüssel (ECC): Es gelten die Vorgaben aus [gemSpec_Krypt#5.8]</p> <p><u>CMS:</u></p> <p>Es ist CMS mit Authenticated-Enveloped-Data Content Type gemäß [RFC-5083] und der AES-GCM-Encryption gemäß [RFC-5084] zu verwenden. Bei der Verschlüsselung des „content-encryption key“ wird die Technik „key transport“ eingesetzt. Pro Empfänger wird eine Instanz vom Typ KeyTransRecipientInfo erzeugt. Dabei ist für RecipientIdentifier die Option IssuerAndSerialNumber zu wählen.</p> <p>ContentType = OID {... authEnvelopedData} = 1.2.840.113549.1.9.16.1.23</p> <p>Im Fall ECC sind die Vorgaben aus [gemSpec_Krypt#5.8] zur Erzeugung des Hybridschlüssels zu beachten.</p> <p>Im Fall RSA sind die Vorgaben aus [gemSpec_Krypt#3.5.2] zur Erzeugung des Hybridschlüssels zu beachten.</p> <p>10. Der symmetrische Schlüssel wird aktiv gelöscht (überschrieben).</p>
Varianten/ Alternativen	<p><u>Zur Rückgabe der Hybridschlüssel</u> MUSS auch die Variante vorgesehen werden, dass die Hybridschlüssel („KeyInfo“) nicht eingebettet im Zieldokument zurückgegeben werden, sondern separat.</p> <p><u>Im Fall des Verschlüsselungsverfahrens S/MIME</u> wird der Standardablauf des CMS Verschlüsselungsverfahrens durch einen vorgelagerten S/MIME-Vorbereitungsschritt und einen nachgelagerten S/MIME-Nachbereitungsschritt ergänzt. Das S/MIME-Verfahren MUSS konform [S/MIME] und SOLL konform [COMMON_PKI#Part 3] erfolgen.</p> <p>Der S/MIME-Vorbereitungsschritt bereitet das übergebene MIME-Dokument gemäß [S/MIME#3.1] auf die nachfolgende CMS-Verschlüsselung durch eine Kanonisierung für Text [S/MIME#3.1.1] vor. Eine weitere Kanonisierung oder eine Anpassung des Transfer Encodings [S/MIME#3.1.2] erfolgt nicht.</p> <p>Im S/MIME-Nachbereitungsschritt wird das im Standardablauf erzeugt CMS-Objekt in eine MIME-Nachricht vom Typ „application/pkcs7-mime“ eingebettet.</p> <p>Sämtliche Header-Felder der Nachricht MÜSSEN in die Header-Felder der S/MIME-Nachricht übernommen werden. Die im Folgenden explizit zu setzenden Header-Felder überschreiben die betroffenen Header-Felder.</p> <p>Es MUSS ein neues message-id Element für den S/MIME-Header generiert werden.</p> <p>"MIME-Version: 1.0" MUSS definiert sein.</p>

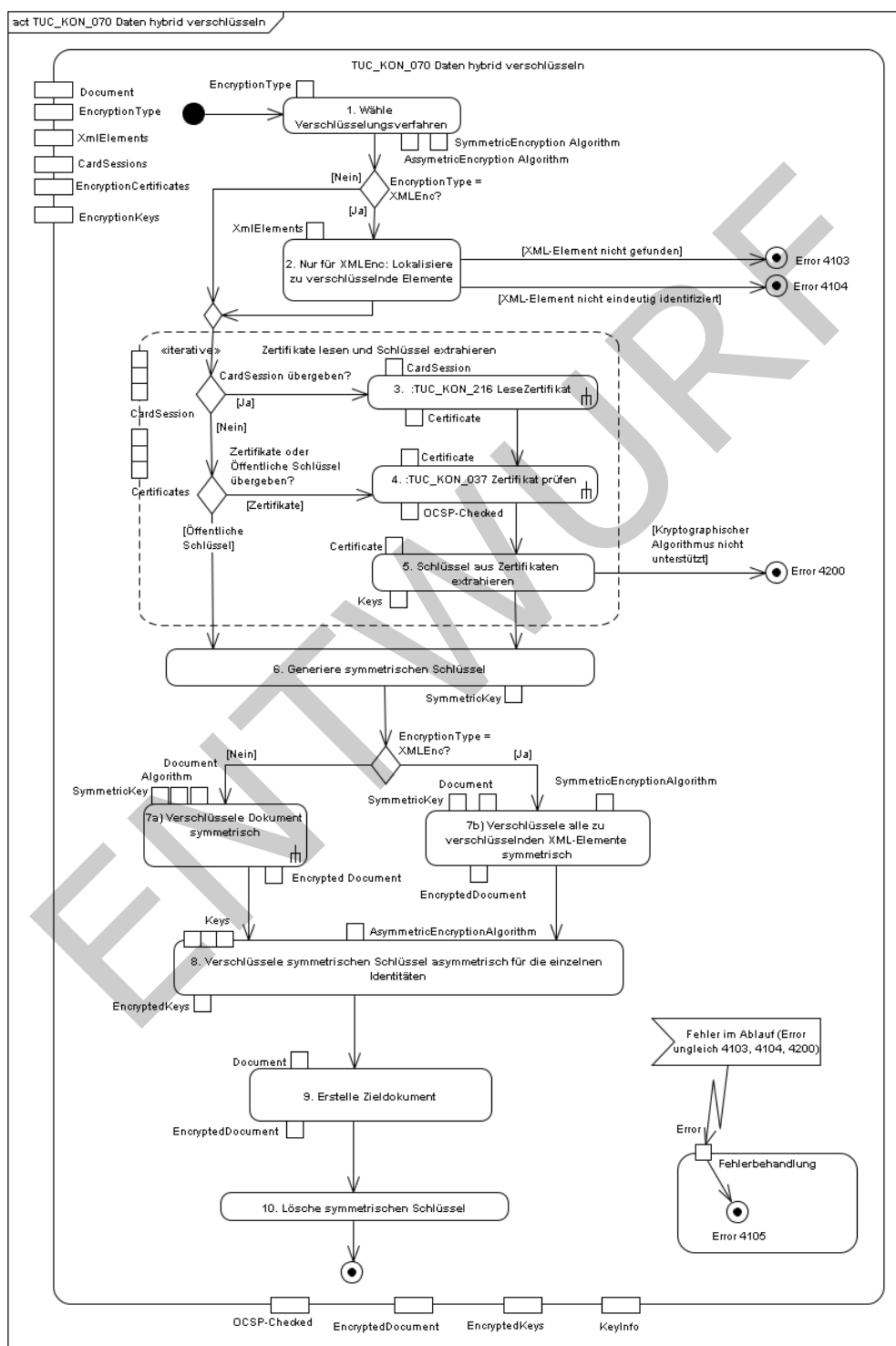
	<p>Das Feld "Subject" MUSS mit "Subject: Verschlüsselte Nachricht" überschrieben werden.</p> <p>Die Codierung des verschlüsselten Inhalts der Nachricht MUSS in "base64" erfolgen. Entsprechend ist das zugehörige Header-Feld zu füllen: "Content-Transfer-Encoding: base64".</p> <p>Das Feld "Content-Type:" ist als "application/pkcs7-mime" zu definieren. Die weiteren Attribute dieses Feldes sind:</p> <ul style="list-style-type: none"> "smime-type=enveloped-data;" "name=\$dateiname", wobei \$dateiname auf ".p7m" endet. <p>Das Feld "Content-Disposition" definiert den Inhalt der Nachricht als Dateianhang: "Content-Disposition: attachment; filename=\$dateiname"</p> <p><u>Zu Schritten 5 und 8 für TI-fremde X.509-Zertifikate</u></p> <p>Der Konnektor MUSS beim asymmetrischen Anteil der hybriden Verschlüsselung auch TI-fremde X.509-Zertifikate unterstützen, wenn diese von einem CA-Zertifikat aus CERT_IMPORTED_CA_LIST ausgestellt wurden und die kryptographischen Vorgaben aus Tabelle [gemSpec_Krypt#Tab_KRYPT_002] erfüllen.</p> <p>Der Konnektor MUSS Anfragen zur Hybridverschlüsselung mit einer Fehlermeldung (Fehler 4200) abweisen, wenn hierfür TI-fremde X509-Zertifikate vorgegeben werden, die nicht die kryptographischen Vorgaben aus Tabelle [gemSpec_Krypt#Tab_KRYPT_002] oder [gemSpec_Krypt#Tab_KRYPT_002a] erfüllen.</p>
Fehlerfälle	<p>Siehe Tabelle TAB_KON_740 Fehlercodes TUC_KON_070 „Daten hybrid verschlüsseln“. Wenn im Ablauf des TUCs ein anderer Fehler als die in Tabelle TAB_KON_740 beschriebenen Fehler auftritt, wird Fehler 4105 gemeldet.</p> <p>(->4) Schritt 4 – Zertifikatsprüfung „für alle anderen Zertifikate“</p> <p>Für MGM_LU_ONLINE=Enabled gilt:</p> <p>Liefert die Zertifikatsprüfung (OCSP-Abfrage) mdt. eine der folgenden Warnungen gemäß [gemSpec_PKI#Tab_PKI_274]</p> <ul style="list-style-type: none"> CERT_REVOKED CERT_UNKNOWN <p>dann wird der TUC mit Fehler 4105 abgebrochen,</p> <p>Ausnahme: Falls im Falle crypt=RSA_ECC der Hybridschlüssel nur für eines der beiden Zertifikate erzeugt werden konnte, dann wird die Warnung 4259 mit <Zertifikat> gemäß TAB_KON_747 in der Response zurückgegeben.</p>
Nichtfunktionale Anforderungen	keine

Zugehörige
Diagramme

Abbildung PIC_KON_058 Aktivitätsdiagramm „Daten hybrid verschlüsseln“

Das Diagramm dient nur der Veranschaulichung und ist nicht vollständig. Beispielsweise enthält es nicht die Steuerung durch den Parameter `crypt`.

3771



3772

3773

Abbildung 13: PIC_KON_058 Aktivitätsdiagramm „Daten hybrid verschlüsseln“

3774

3775 **Tabelle 166: TAB_KON_073 Vorgaben zum Format verschlüsselter XML-Dokumente**

#	Beschreibung
	xenc:EncryptedData MUSS ein ds:KeyInfo Element enthalten, welches wiederum ein xenc:EncryptedKey Element enthält.
	Der xenc:EncryptedKey MUSS [XMLEnc] konform sein.
	Die xenc:EncryptionMethod für den Schlüssel MUSS gemäß [gemSpec_Krypt#3.1.5] gewählt werden
	Der xenc:EncryptedKey MUSS ein ds:KeyInfo Element mit ds:X509Data und ds:X509Certificate Subelement enthalten, in dem das X.509-Zertifikat hinterlegt wird.

3776

3777 **Tabelle 167: TAB_KON_740 Fehlercodes TUC_KON_070 „Daten hybrid verschlüsseln“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4103	Technical	Error	XML-Element nicht gefunden
4104	Technical	Error	XML-Element nicht eindeutig identifiziert. (Überschneidung)
4105	Technical	Error	hybride Verschlüsselung konnte nicht durchgeführt werden
4200	Security	Error	Schlüssel erlaubt keinen zugelassenen Verschlüsselungsalgorithmus
4259	Technical	Warning	Verschlüsselung für Zertifikat <Zertifikat> nicht möglich

3778

3779 **[<=]**3780 **4.1.7.4.2 TUC_KON_071 „Daten hybrid entschlüsseln“**3781 **TIP1-A_4617-02 - TUC_KON_071 „Daten hybrid entschlüsseln“**

3782 Der Konnektor MUSS den technischen Use Case TUC_KON_071 „Daten hybrid
 3783 entschlüsseln“ umsetzen.

3784

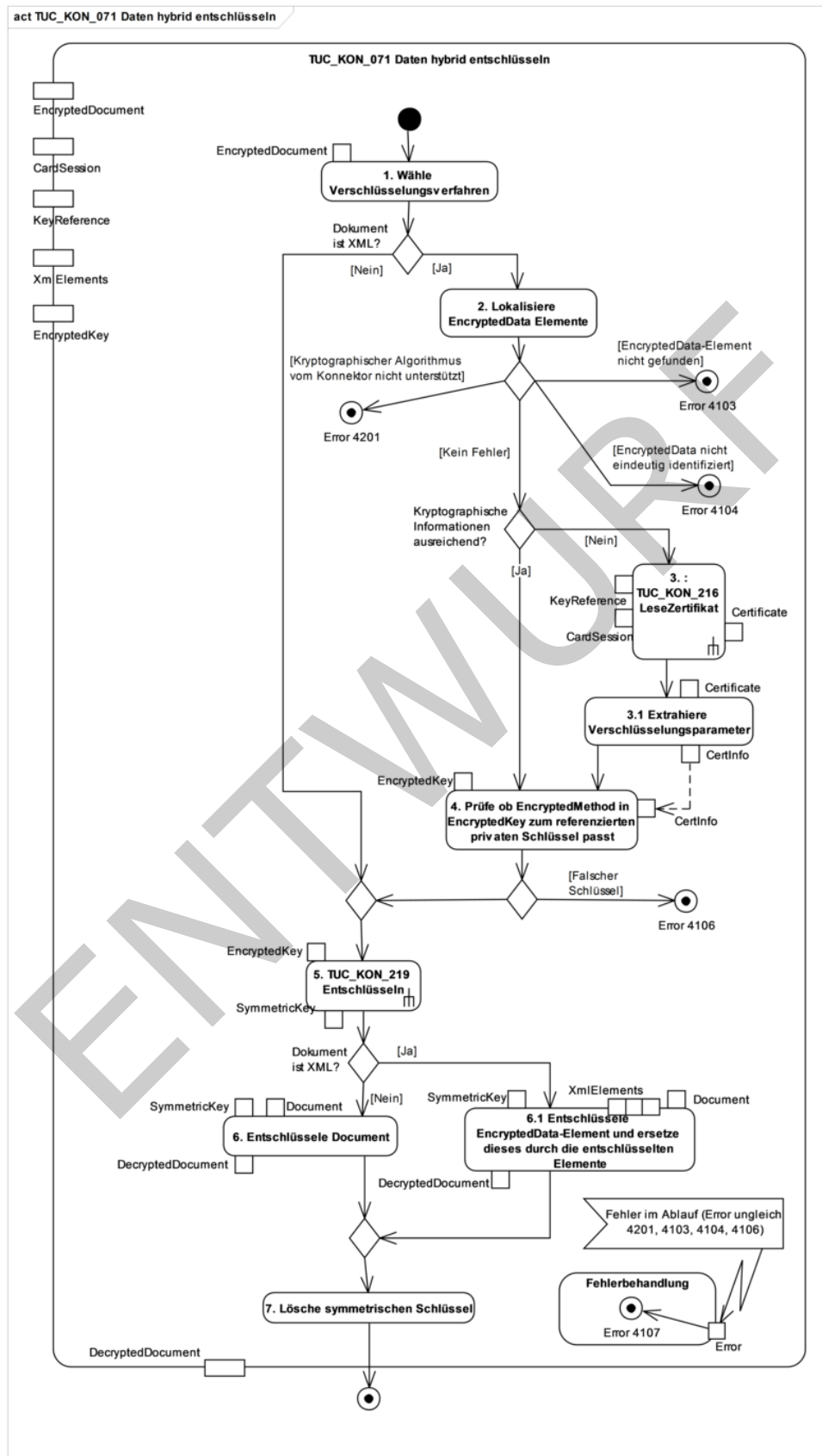
3785 **Tabelle 168: TAB_KON_140 – TUC_KON_071 „Daten hybrid entschlüsseln“**

Element	Beschreibung
Name	TUC_KON_071 „Daten hybrid entschlüsseln“
Beschreibung	Ein hybrid verschlüsseltes Dokument, das konform zu TUC_KON_070 erstellt wurde, wird entschlüsselt. Es muss eine asymmetrische Verschlüsselung vorliegen, zu der der Schlüssel auf einer Karte vorliegt.
Auslöser	Aufruf in einem fachlichen Use Case oder des Verschlüsselungsbasisdienstes.
Vorbedingungen	Die Karte mit dem privaten Schlüssel muss gesteckt sein und der Sicherheitszustand zur Nutzung des privaten Schlüssels muss gesetzt sein. Ein konform zu TUC_KON_070 hybrid verschlüsseltes Dokument liegt vor. Bei XML-Dokumenten: Das Dokument enthält EncryptedData Elemente. Falls mehrere Elemente des Dokumentes zu entschlüsseln sind, müssen diese alle mit demselben symmetrischen Schlüssel verschlüsselt sein.
Eingangsdaten	<ul style="list-style-type: none"> • encryptedDocument (Zu entschlüsselndes Dokument) • cardSession (Kartensitzung; unterstützt werden SM-B, HBAX und eGK mit der jeweiligen C.ENC-KeyReference). • privateKeyReference (Referenz auf den privaten Schlüssel; unterstützt werden SM-B, HBAX und eGK mit der jeweiligen C.ENC-KeyReference). • encryptionCertificate – <i>optional</i> (Verschlüsselungszertifikat passend zur Schlüsselreferenz). • encryptionCertificateReference – <i>optional</i> (Referenz auf das Zertifikat auf obiger Karte passend zur Schlüsselreferenz). • encryptedKey – <i>optional, falls nicht in encryptedDocument enthalten</i> (asymmetrisch verschlüsselter symmetrischer Schlüssel) Darüber hinaus werden die folgenden, vom Dokumentformat und dem Verschlüsselungsverfahren abhängigen Eingangsdaten benötigt: Bei XML-Dokumenten:

	<ul style="list-style-type: none"> xmlElements – <i>optional/verpflichtend, wenn encryptionType = XMLEnc</i> (bei XML-Dokumenten Angabe der zu entschlüsselnden Teile des XML-Dokuments)
Komponenten	Konnektor, Kartenterminal, Karte
Ausgangsdaten	<ul style="list-style-type: none"> plainDocument (Unverschlüsseltes Dokument. Bei XML-Dokumenten: Das EncryptedData-Element ist durch das entschlüsselte ersetzt.)
Standardablauf	<ol style="list-style-type: none"> Das Verfahren zum Entschlüsseln wird entsprechend dem Format des übergebenen zu entschlüsselnden Dokuments (EncryptedDocument) gewählt. Der Konnektor MUSS beim asymmetrischen Anteil der Entschlüsselung hybrid verschlüsselter Dokumente die in [gemSpec_Krypt] beschriebenen Verfahren unterstützen. XMLEnc: Das EncryptedData Element (oder mehrere Elemente) werden im Dokument lokalisiert. Falls sie nicht oder nicht eindeutig gefunden werden können wird Fehler 4103 bzw. 4104 gemeldet. Ist in einem EncryptedData Element ein vom Konnektor nicht unterstützter Mechanismus spezifiziert, wird Fehler 4201 gemeldet. Falls erforderlich, wird TUC_KON_216 „Lese Zertifikat“ aufgerufen, um das Zertifikat von der Karte zu lesen. 3.1 Die Kenntnis des Zertifikats kann erforderlich sein, um im Zertifikat kodierte Verschlüsselungsparameter auszulesen. (Zur Zeit der Erstellung dieser Spezifikation werden zur Laufzeit keine zusätzlichen Parameter aus dem Zertifikat benötigt, da alle nötigen Informationen aus den PKI- und Kartenspezifikationen abgeleitet werden können.) XMLEnc: Es wird geprüft, ob die Verschlüsselungsparameter (EncryptionMethod in EncryptedKey) zum referenzierten privaten Schlüssel auf der Karte passen. Ist dies nicht der Fall, bricht der Use Case mit Fehler 4106 ab. Es wird TUC_KON_219 „Entschlüssele“ aufgerufen, um den symmetrischen Schlüssel mit Hilfe des angegebenen privaten Schlüssels zu entschlüsseln. Mit dem symmetrischen Schlüssel wird der unverschlüsselte Dateninhalt wiederhergestellt. 6.1 XMLEnc: Das EncryptedData Element wird durch die entschlüsselten Daten ersetzt. Der symmetrische Schlüssel wird aktiv gelöscht (überschrieben).
Varianten/Alternativen	Zu 6.: Zur Unterstützung von Bestandssystemen werden, neben den für den symmetrischen Teil der hybriden Verschlüsselung

	<p>vorgeschriebenen kryptographischen Algorithmen, für den symmetrischen Teil der hybriden Entschlüsselung auch folgende Algorithmen unterstützt (siehe [gemSpec_Krypt#3.5.1]):</p> <ul style="list-style-type: none"> • AES-128 GCM • AES-192 GCM <p>RSA- und ECC-basierter Hybridschlüssel: Wenn sowohl ein RSA- als auch ein ECC-basierter Hybridschlüssel vorliegen, muss zuerst die Entschlüsselung des ECC-basierten Hybridschlüssels erfolgen. Falls dabei ein Fehler auftritt, muss der Fehler protokolliert werden, und dann - ohne Abbruch - mit der Entschlüsselung des RSA-basierten Hybridschlüssels fortgefahren werden.</p>
Fehlerfälle	<p>Siehe Tabelle TAB_KON_142 Fehlercodes TUC_KON_071 „Daten hybrid entschlüsseln“.</p> <p>Wenn im Ablauf des TUCs ein anderer Fehler als die in Tabelle TAB_KON_142 Fehlercodes TUC_KON_071 „Daten hybrid entschlüsseln“ beschriebenen Fehler auftritt, wird Fehler 4107 gemeldet.</p>
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	Abbildung PIC_KON_059 Aktivitätsdiagramm „Daten hybrid entschlüsseln“

3786



3787

Abbildung 14: PIC_KON_059 Aktivitätsdiagramm „Daten hybrid entschlüsseln“

Tabelle 169: TAB_KON_142 Fehlercodes TUC_KON_071 „Daten hybrid entschlüsseln“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4106	Technical	Error	falscher Schlüssel
4107	Technical	Error	hybride Entschlüsselung konnte nicht durchgeführt werden
4103	Technical	Error	XML-Element nicht gefunden
4104	Technical	Error	XML-Element nicht eindeutig identifiziert
4201	Technical	Error	kryptographischer Algorithmus vom Konnektor nicht unterstützt

[<=]

4.1.7.4.3 TUC_KON_072 „Daten symmetrisch verschlüsseln“

TIP1-A_4618 - TUC_KON_072 „Daten symmetrisch verschlüsseln“

Der Konnektor MUSS den technischen Use Case TUC_KON_072 „Daten symmetrisch verschlüsseln“ umsetzen.

Tabelle 170: TAB_KON_741 – TUC_KON_072 „Daten symmetrisch verschlüsseln“

Element	Beschreibung
Name	TUC_KON_072 „Daten symmetrisch verschlüsseln“
Beschreibung	Es wird ein Dokument symmetrisch verschlüsselt. Dabei kann der zu verwendende symmetrische Schlüssel optional übergeben werden.
Auslöser	Aufruf durch ein Fachmodul in einem fachlichen Use Case
Vorbedingungen	keine
Eingangsdaten	<ul style="list-style-type: none"> documentToBeEncrypted (zu verschlüsselndes Dokument.) symmetricKey – <i>optional</i> (zu verwendender symmetrischer Schlüssel)
Komponenten	Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> encryptedDocument (Verschlüsseltes Dokument) symmetricKey – <i>optional/verpflichtend, wenn Schlüssel durch den TUC erzeugt wurde</i> (erzeugter symmetrischer Schlüssel)
Standardablauf	1. Wurde kein symmetrischer Schlüssel übergeben, so wird ein Schlüssel erzeugt. Die Qualität des

	<p>Schlüssels muss den Vorgaben in [gemSpec_Krypt#2.2] genügen.</p> <p>2. Das Dokument wird mit dem erzeugten oder übergebenen symmetrischen Schlüssel verschlüsselt. Als Verfahren zum Verschlüsseln wird CMS gewählt ([RFC5652]). Die Content Type Option „Encrypted-data Content Type“ ist zu verwenden. Content Type = OID{... pkcs-7 encryptedData} = 1.2.840.113549.1.7.6 Die symmetrische Verschlüsselung binärer Daten erfolgt nach den Vorgaben gemäß [gemSpec_Krypt#GS-A 5016]. Falls die Verschlüsselung fehlschlägt, wird Fehler 4108 gemeldet.</p> <p>3. Das verschlüsselte Dokument und der symmetrische Schlüssel (falls dieser erzeugt wurde) werden zurückgeliefert.</p>
Varianten/Alternativen	keine
Fehlerfälle	Siehe Standardablauf.
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

3798

3799

3800

Tabelle 171: TAB_KON_742 Fehlercodes TUC_KON_072 „Daten symmetrisch verschlüsseln“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4108	Technical	Error	Symmetrische Verschlüsselung konnte nicht durchgeführt werden

3801

3802 [**<=**]

3803 4.1.7.4.4 TUC_KON_073 „Daten symmetrisch entschlüsseln“

3804 TIP1-A_4619 - TUC_KON_073 „Daten symmetrisch entschlüsseln“

3805 Der Konnektor MUSS den technischen Use Case TUC_KON_073 „Daten symmetrisch
3806 entschlüsseln“ umsetzen.

3807

3808 **Tabelle 172: TAB_KON_743 - TUC_KON_073 „Daten symmetrisch entschlüsseln“**

Element	Beschreibung
Name	TUC_KON_073 „Daten symmetrisch entschlüsseln“

Beschreibung	Es wird ein Dokument symmetrisch entschlüsselt. Der zu verwendende symmetrische Schlüssel wird übergeben.
Auslöser	Aufruf durch ein Fachmodul in einem fachlichen Use Case
Vorbedingungen	keine
Eingangsdaten	<ul style="list-style-type: none"> encryptedDocument (Verschlüsseltes Dokument) symmetricKey (zu verwendender symmetrischer Schlüssel)
Komponenten	Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> plainDocument (Entschlüsseltes Dokument)
Standardablauf	Das verschlüsselte Dokument wird mit dem symmetrischen Schlüssel entschlüsselt. Als Verfahren zum Entschlüsseln wird CMS gewählt ([RFC5652]). Das entschlüsselte Dokument wird zurückgeliefert.
Varianten/Alternativen	keine
Fehlerfälle	Bei Auftreten eines Fehlers im Standardablauf wird Fehlercode 4109 gemeldet.
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

Tabelle 173: TAB_KON_744 Fehlercodes TUC_KON_073 „Daten symmetrisch entschlüsseln“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4109	Technical	Error	symmetrische Entschlüsselung konnte nicht durchgeführt werden

[<=]

4.1.7.4.5 TUC_KON_075 „Symmetrisch verschlüsseln“

A_18001 - TUC_KON_075 „Symmetrisch verschlüsseln“

Der Konnektor MUSS den technischen Use Case TUC_KON_075 „Symmetrisch verschlüsseln“ umsetzen.

Tabelle 174: TAB_KON_860 – TUC_KON_075 „Symmetrisch verschlüsseln“

Element	Beschreibung
---------	--------------

Name	TUC_KON_075 „Symmetrisch verschlüsseln“
Beschreibung	Es werden binäre Daten symmetrisch verschlüsselt. Optional können der zu verwendende symmetrische Schlüssel und AssociatedData für Authenticated Encryption with Associated Data (AEAD) übergeben werden.
Auslöser	Aufruf durch ein Fachmodul in einem fachlichen Use Case
Vorbedingungen	keine
Eingangsdaten	<ul style="list-style-type: none"> • dataToBeEncrypted (zu verschlüsselnde Daten) • symmetricKey – optional (zu verwendender symmetrischer Schlüssel) • associatedData – optional (Parameter für den Verschlüsselungsalgorithmus)
Komponenten	Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> • encryptedData (Verschlüsselte Daten mit der Struktur gemäß Punkt 2 aus A_18004) • symmetricKey – optional/verpflichtend, wenn Schlüssel durch den TUC erzeugt wurde (erzeugter symmetrischer Schlüssel)
Standardablauf	<ol style="list-style-type: none"> 1. Wurde kein symmetrischer Schlüssel übergeben, so wird ein Schlüssel erzeugt. Die Qualität des Schlüssels muss den Vorgaben in GS-A_4367 genügen. 2. dataToBeEncrypted wird mit dem erzeugten oder übergebenen symmetrischen Schlüssel unter Berücksichtigung der optional übergebenen associatedData verschlüsselt. Die symmetrische Verschlüsselung binärer Daten erfolgt nach den Vorgaben gemäß A_17872. 3. encryptedData wird erzeugt mit der Struktur gemäß Punkt 2 aus A_18004. 4. Das verschlüsselte Dokument und der symmetrische Schlüssel (falls dieser erzeugt wurde) werden zurückgeliefert.
Varianten/Alternativen	keine
Fehlerfälle	-> 2: Falls die Verschlüsselung fehlschlägt, wird Fehler 4108 gemäß TAB_KON_742 gemeldet.

Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

3820 [\leq]

3821 4.1.7.4.6 TUC_KON_076 „Symmetrisch entschlüsseln“

3822 A_18002 - TUC_KON_076 „Symmetrisch entschlüsseln“

3823 Der Konnektor MUSS den technischen Use Case TUC_KON_076 „Symmetrisch entschlüsseln“ umsetzen.

3825

3826 **Tabelle 175: TAB_KON_861 - TUC_KON_076 „Symmetrisch entschlüsseln“**

Element	Beschreibung
Name	TUC_KON_076 „Symmetrisch entschlüsseln“
Beschreibung	Es werden verschlüsselte Daten symmetrisch entschlüsselt. Für Authenticated Encryption with Associated Data (AEAD) kann AssociatedData optional übergeben werden. Der zu verwendende symmetrische Schlüssel wird übergeben.
Auslöser	Aufruf durch ein Fachmodul in einem fachlichen Use Case
Vorbedingungen	keine
Eingangsdaten	<ul style="list-style-type: none"> • encryptedData (Verschlüsselte Daten mit der Struktur gemäß Punkt 2 aus A_18004) • symmetricKey (zu verwendender symmetrischer Schlüssel) • associatedData - optional (Parameter für den Verschlüsselungsalgorithmus)
Komponenten	Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> • plainData (Entschlüsselte Daten)
Standardablauf	Das verschlüsselte Dokument wird mit dem symmetrischen Schlüssel und associatedData unter Verwendung der kryptographischen Verfahren aus A_17872 entschlüsselt. Die entschlüsselten Daten werden zurückgeliefert.

Varianten/Alternativen	keine
Fehlerfälle	Bei Auftreten eines Fehlers im Standardablauf wird Fehlercode 4109 gemäß TAB_KON_744 gemeldet.
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

[<=]

4.1.7.5 Operationen an der Außenschnittstelle

TIP1-A_4620-02 ~~TIP1-A_4620~~ - Basisdienst Verschlüsselungsdienst

Der Konnektor MUSS für Clients einen Basisdienst Verschlüsselungsdienst anbieten.

Tabelle 176: TAB_KON_745 Basisdienst Verschlüsselungsdienst

Name	EncryptionService	
Version (KDV)	6.1.0 (WSDL-Version) , 6.1.1 (XSD-Version) 6.1.1 (WSDL-Version) , 6.1.2 (XSD-Version)	
Namensraum	Siehe Anhang D	
Namensraum-Kürzel	CRYPT für Schema und CRYPTW für WSDL	
Operationen	Name	Kurzbeschreibung
	EncryptDocument	Dokument hybrid verschlüsseln
	DecryptDocument	Dokument hybrid entschlüsseln
WSDL	EncryptionService.wsdl (WSDL-Version 6.1.0) EncryptionService_v6_1_1.wsdl	
Schema	EncryptionService.xsd (XSD-Version 6.1.1) EncryptionService_v6_1_2.xsd	

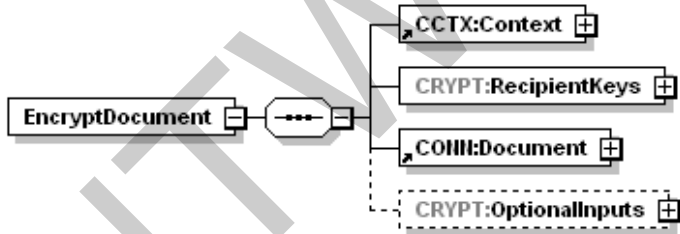
[<=]

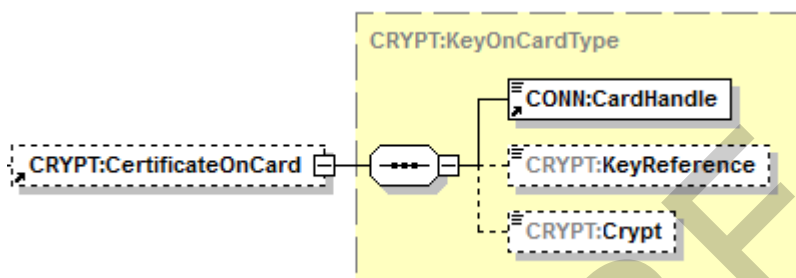
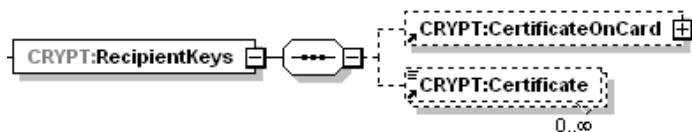
4.1.7.5.1 EncryptDocument

TIP1-A_4621-02 - Operation EncryptDocument

Der Basisdienst Verschlüsselungsdienst des Konnektors MUSS an der Clientschnittstelle eine Operation EncryptDocument anbieten.


3841 **Tabelle 177: TAB_KON_071 Operation EncryptDocument**

Name	EncryptDocument
Beschreibung	<p>Diese Operation verschlüsselt ein übergebenes Dokument hybrid. Es werden die Dokumententypen <code>Alle_DocFormate</code> unterstützt. Für die hybride Verschlüsselung wird ein asymmetrischer Schlüssel aus einem X.509v3-Zertifikat genutzt. Dieses Zertifikat kann von einer Karte kommen oder als Parameter übergeben werden. Pro Operationsaufruf können mehrere Hybridschlüssel erzeugt werden. Übergibt der Aufrufer die Zertifikate beim Aufruf, steuert er durch die Wahl der Zertifikate, ob RSA-basierte oder ECC-basierte Hybridschlüssel erzeugt werden. Wenn das Verschlüsselungszertifikat von einer Karte kommt, kann der Aufrufer durch Angabe des Kryptoverfahrens <code>crypt</code> steuern, ob Hybridschlüssel für RSA oder für ECC oder beide erzeugt werden. Das Defaultverhalten ist die Hybridschlüsselerzeugung für RSA und entspricht dem Verhalten aus der Version 6.1.0 der Schnittstelle.</p> <p>Es werden die folgenden Karten unterstützt: HBAX und SM-B. Die Operation EncryptDocument DARF das Verschlüsseln mit der eGK NICHT unterstützen.</p> <p>Für alle Dokumententypen wird immer das gesamte Dokument verschlüsselt.</p>
	
Name	Beschreibung
Context	Aufrufkontext: <ul style="list-style-type: none"> • MandantID, ClientSystemID, WorkplaceId verpflichtend • UserID verpflichtend bei HBAX, bei SM-B nicht ausgewertet



Das RecipientKeys-Element identifiziert die Empfänger der zu verschlüsselnden Nachricht über X.509-Zertifikate (öffentliche Schlüssel). Quelle für die Zertifikate kann eine gesteckte Karte sein, die per CertificateOnCard-Element referenziert wird, oder der Aufrufer, der X.509-Zertifikate im Certificate-Element übergibt.

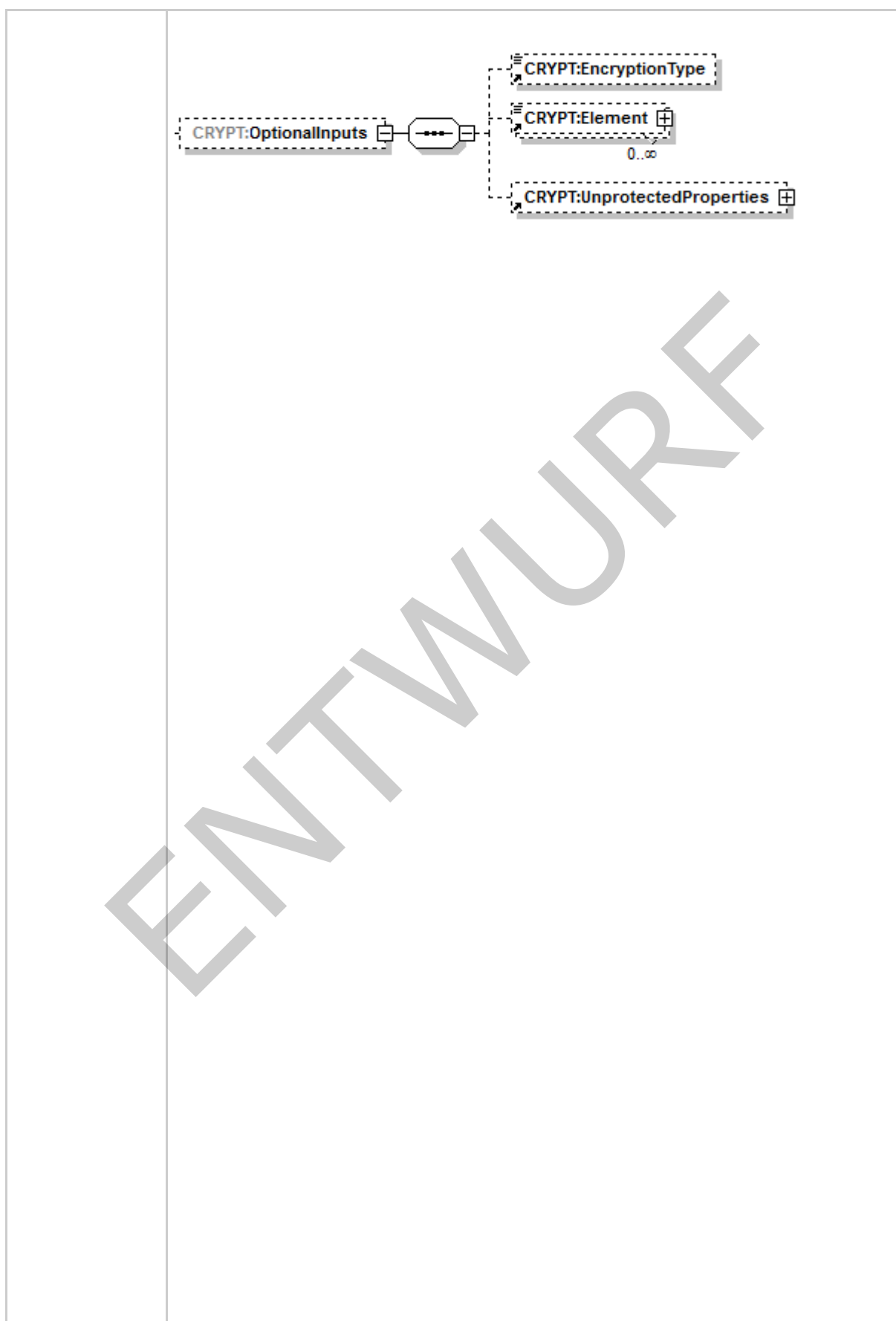
	Card Handle	Identifiziert die zu verwendende Karte mit dem (öffentlichen) Schlüssel. Ist das Element nicht vorhanden, so werden nur Zertifikate per Element <code>Certificate</code> übergeben.
	KeyRef erence	Der Wert dieses Parameters ist in Tabelle TAB_KON_747 KeyReference für Encrypt-/DecryptDocument spezifiziert. Ist der Parameter nicht angegeben, gilt der Default-Wert C.ENC.
	Crypt	Optional; Default: siehe TAB_KON_859 Wertebereich: [ENC_CRYPT] Gibt den Typ von Zertifikaten vor, die von der per CardHandle referenzierten Karte für die Erzeugung der Hybridschlüssel gemäß Tabelle TAB_KON_747 verwendet werden.
	Certifi cate	<code>Certificate</code> ist ein Base64-kodiertes XML-Element, in dem das Zertifikat, das den asymmetrischen Schlüssel enthält (öffentlicher Schlüssel), DER-kodiert übergeben wird. Es kann eine Liste von Zertifikaten übergeben werden. Kommt das Zertifikat ausschließlich von einer Karte, dann kann dieser Parameter weggelassen werden.

Document 

ENTWURF

	CONN: Document	Dieses entsprechend [OASIS-DSS] Section 2.4.2 spezifizierte Element enthält das zu verschlüsselnde Dokument, wobei die Kindelemente <code>CONN:Base64XML</code> und <code>dss:Base64Data</code> verwendet werden. Im Fall <code>dss:Base64Data</code> wird ein etwaig übergebenes MIME-Type- Attribut nicht ausgewertet.
--	-------------------	---

ENTWURF




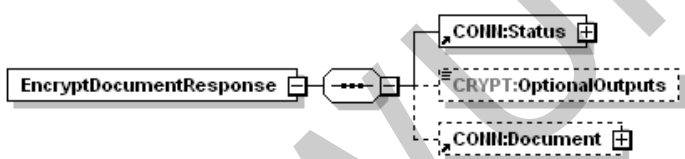
	CRYPT: Optional Inputs	Enthält eine Auswahl der folgenden unten näher erläuterten (optionalen) Eingabeparameter:
--	------------------------------	---

ENTWURF

	<div data-bbox="435 309 639 353" data-label="Text"> <p>EncryptionType</p> </div> <div data-bbox="316 629 1214 1585" data-label="Text"> <p>ENTWURF</p> </div>
--	--

	Encryption Type	<p>Zu wählendes Verschlüsselungsverfahren, wobei folgende URI vorgesehen sind:</p> <ul style="list-style-type: none"> • XMLEnc: „http://www.w3.org/TR/xmlenc-core/“ • CMS: „urn:ietf:rfc:5652“ • S/MIME: „urn:ietf:rfc:5751“ <p>Im Fall XMLEnc wird ein Base64-codiertes XML-Dokument im Element <code>CONN:Document/CONN:Base64XML</code> übergeben. In den Fällen CMS und S/MIME wird ein Base64-codiertes Binär-Dokument im Element <code>CONN:Document/dss:Base64Data</code> übergeben .</p> <p>Ist der Parameter EncryptionType nicht gesetzt, dann gilt folgendes Default-Verhalten: Für ein im Element <code>CONN:Document/CONN:Base64XML</code> übergebenes XML-Dokument wird als Verschlüsselungsverfahren [XMLEnc] angewandt, und für ein im Element <code>CONN:Document/dss:Base64Data</code> übergebenes Dokument wird das Verschlüsselungsverfahren CMS angewandt. XML-Dokumente werden nach <code>Type=http://www.w3.org/2001/04/xmlenc#Element</code> verschlüsselt. Im Fall S/MIME ist das in <code>CONN:Document/dss:Base64Data</code> übergebene Dokument eine MIME-Nachricht.</p>
--	--------------------	---

	<div data-bbox="435 309 563 353"> Element</div>
<div data-bbox="319 627 1212 1590">ENTWURF</div>	

	Element	Der Parameter wird nicht ausgewertet.
		
	CRYPT:UnprotectedProperties	<p>Dieses optionale Element wird im CMS-Fall (EncryptionType = urn:ietf:rfc:5652) ausgewertet. Die Elemente <code>./UnprotectedProperties/Property/Value/CMSAttribute</code> müssen base64/DER-kodiert ein vollständiges ASN.1-Attribute enthalten, definiert in [CMS# 9.1.AuthenticatedData Type]. Es muss bei der Erstellung des CMS-Containers unter "unauthAttrs" aufgenommen werden. Das zugehörige Element <code>./UnprotectedProperties/Property/Identifier</code> wird nicht ausgewertet.</p>
Rückgabe		
	Status	Enthält den Ausführungsstatus der Operation.
	CRYPT:OptionalOutputs	Kann – in zukünftigen Versionen der Spezifikation – optionale Ausgabeparameter enthalten.
	CONN:Document	<p>Enthält das verschlüsselte Dokument in base64-codierter Form, wenn die Verschlüsselung erfolgreich durchgeführt wurde.</p> <p>Im Fall XMLEnc wird das Base64-codierte verschlüsselte XML-Dokument im Element <code>CONN:Document/CONN:Base64XML</code> zurückgegeben.</p> <p>Im Fall CMS wird das Base64-codierte Binär-Dokument im Element <code>CONN:Document/dss:Base64Data</code> zurückgegeben.</p> <p>Im Fall S/MIME wird die Base64-codierte S/MIME-Nachricht im Element <code>CONN:Document/dss:Base64Data</code> zurückgegeben. Das Attribut <code>CONN:Document/dss:Base64Data/@MimeType</code> wird auf „application/pkcs7-mime“ gesetzt. Die S/MIME-Nachricht hat Content-Transfer-Encoding: base64.</p>
Fehler	Bei Auftreten eines Fehlers im Standardablauf werden Fehlercodes entsprechend TAB_KON_141 gemeldet.	

Vorbedingungen	Keine
Nachbedingungen	Keine

3842

3843 Der Ablauf der Operation EncryptDocument ist in Tabelle TAB_KON_746 Ablauf
 3844 EncryptDocument beschrieben:

3845

3846 **Tabelle 178: TAB_KON_746 Ablauf EncryptDocument**

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab. Wird die Operation für einen nicht unterstützten Kartentypen aufgerufen, so bricht die Operation mit Fehler 4058 ab.
2.	TUC_KON_000 „Prüfe Zugriffs- berechtigung“	Die Prüfung erfolgt durch den Aufruf TUC_KON_000 { mandantId = \$context.mandantId; clientsystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; userId = \$context.userId; cardHandle = \$cardHandle } Tritt bei der Prüfung ein Fehler auf, bricht die Operation mit Fehlercode aus TUC_KON_000 ab.
3.	TUC_KON_026 „Liefere CardSession“	Ermittle CardSession über TUC_KON_026 { mandatId = \$context..mandantId; clientSystemId = \$context.clientSystemId; cardHandle = \$context..cardHandle; userId = \$context.userId }
4.	TUC_KON_070 „Daten hybrid verschlüsseln“	Die hybride Verschlüsselung wird durchgeführt. Tritt hierbei ein Fehler auf, bricht die Operation ab. Die KeyInfo, d.h. die Liste der Hybridschlüssel inklusive des bei ihrer Erzeugung verwendeten Zertifikates, sind dabei in das Dokument einzubetten.

3847

Tabelle 179: TAB_KON_141 Fehlercodes „EncryptDocument“

Fehlercode	ErrorType	Severity	Fehlertext
------------	-----------	----------	------------

Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:

4000	Technical	Error	Syntaxfehler
4001	Security	Error	Interner Fehler
4058	Security	Error	Aufruf nicht zulässig

3848

3849 [\leq]

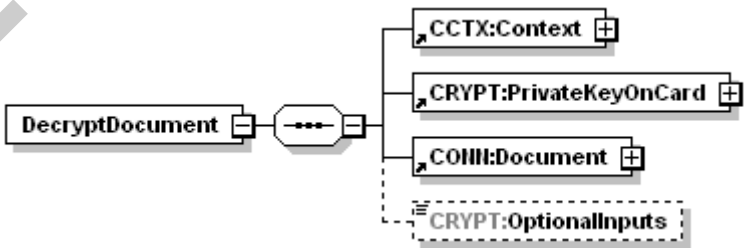
3850 4.1.7.5.2 DecryptDocument

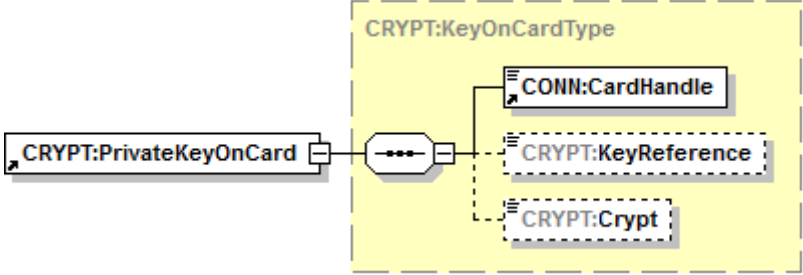
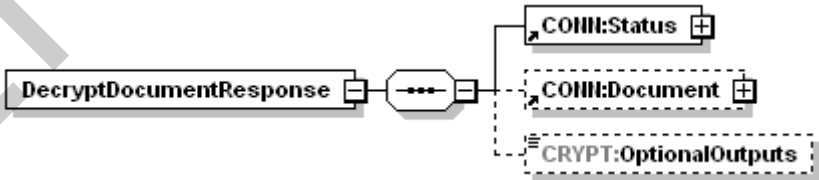
3851 TIP1-A_4622-02 - Operation DecryptDocument

3852 Der Basisdienst Verschlüsselungsdienst des Konnektors MUSS an der Clientschnittstelle
 3853 eine Operation DecryptDocument anbieten.

3854

3855 **Tabelle 180: TAB_KON_075 Operation DecryptDocument**

Name	DecryptDocument		
Beschreibung	<p>Die Operation entschlüsselt alle hybrid verschlüsselten Dokumente, die mit der Operation EncryptDocument erzeugt wurden. Es werden die Dokumententypen <code>Alle_DocFormate</code> unterstützt.</p> <p>Für die Entschlüsselung wird ein asymmetrischer Schlüssel zu einem X.509v3-Zertifikat genutzt. Dieses Zertifikat und der Schlüssel müssen von einer Karte kommen.</p> <p>Das bei der Entschlüsselung verwendete Kryptoverfahren (RSA oder ECC) wird durch den Hybridschlüssel bestimmt, der durch die Karte entschlüsselt werden soll. Sind sowohl RSA- als auch ECC-Hybridschlüssel für die referenzierte Karte vorhanden, versucht der Konnektor die Entschlüsselung des ECC-Hybridschlüssels, und wenn das nicht erfolgreich war, die Entschlüsselung des RSA-Hybridschlüssels.</p>		
Aufrufparameter			
	Name	Beschreibung	
	Context	Aufrufkontext: <ul style="list-style-type: none"> MandantId, ClientSystemId, WorkplaceId verpflichtend UserId verpflichtend bei HBAX, bei SM-B nicht ausgewertet 	

		
	PrivateKeyOnCard	Identifiziert die zu verwendende Karte mit dem (privaten) Schlüssel. Es werden die folgenden Karten unterstützt: HBAX und SM-B. Die Operation DecryptDocument DARF das Entschlüsseln mit der eGK NICHT unterstützen.
	CardHandle	Identifiziert die gesteckte Karte.
	KeyReference	Der Wert dieses Parameters ist in der Tabelle TAB_KON_747 KeyReference für Encrypt-/DecryptDocument spezifiziert. Ist der Parameter nicht angegeben, gilt der Default-Wert C.ENC.
	Crypt	Ist nicht enthalten.
	CONN:Document	Enthält das base64-codierte Dokument, das entschlüsselt werden soll.
	CRYPT:OptionalInputs	Kann – in zukünftigen Versionen der Spezifikation – optionale Aufrufparameter enthalten.
Rückgabe		
	Status	Enthält den Ausführungsstatus der Operation.
	CRYPT:OptionalOutputs	Kann – in zukünftigen Versionen der Spezifikation – optionale Ausgabeparameter enthalten.
	CONN:Document	Enthält das entschlüsselte Dokument in base64-codierter Form
Fehler	Bei Auftreten eines Fehlers im Standardablauf werden Fehlercodes entsprechend TAB_KON_145 gemeldet.	

Vorbedingungen	Keine
Nachbedingungen	Keine

Der Ablauf der Operation DecryptDocument ist in Tabelle TAB_KON_076 Ablauf DecryptDocument beschrieben:

Tabelle 181: TAB_KON_076 Ablauf DecryptDocument

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1. 2.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab. Wird die Operation für einen nicht unterstützten Kartentypen aufgerufen, so bricht die Operation mit Fehler 4058 ab.
2. 1.	TUC_KON_000 „Prüfe Zugriffs- berechtigung“	Die Prüfung erfolgt durch den Aufruf TUC_KON_000 { mandantId = \$context.mandantId; clientsystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; userId = \$context.userId; cardHandle = \$cardHandle } Tritt bei der Prüfung ein Fehler auf, bricht die Operation mit Fehlercode aus TUC_KON_000 ab.
3.	TUC_KON_026 „Liefere CardSession“	Ermittle CardSession über 026 { mandatId = \$context.mandantId; clientsystemId = \$context.clientsystemId; cardHandle = \$context.cardHandle; userId = \$context.userId }
4. 4.	TUC_KON_071 Daten hybrid entschlüsseln	Die Entschlüsselung wird durchgeführt. Im Fall eines XML-Dokuments mit mehreren verschlüsselten Elementen sind alle mit dem angegebenen Schlüssel entschlüsselbaren Elemente zu entschlüsseln.

Tabelle 182: TAB_KON_145 Fehlercodes „DecryptDocument“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler
4001	Security	Error	interner Fehler
4058	Security	Error	Aufruf nicht zulässig

3861 [\leq]

3862 4.1.7.6 Betriebsaspekte

3863 keine

3864 4.1.8 Signaturdienst

3865 Der Signaturdienst bietet Clientsystemen und Fachmodulen eine Schnittstelle zum
3866 Signieren von Dokumenten und Prüfen von Dokumentensignaturen

3867 Innerhalb des Signaturdienstes werden folgende Präfixe für Bezeichner verwendet:

- 3868 • Events (Topic Ebene 1): keine Events vorhanden
- 3869 • Konfigurationsparameter: „SAK_“

3870 4.1.8.1 Funktionsmerkmalweite Aspekte

3871 4.1.8.1.1 Dokumentensignatur

3872 Der Signaturdienst umfasst die Funktionalität der nicht-qualifizierten elektronischen
3873 Signatur (nonQES) mit der SM-B, sowie die qualifizierte elektronische Signatur (QES) mit
3874 dem HBA und den HBA-Vorläuferkarten HBA-qSig und ZOD_2.0 (=HBAx).

3875 In der Abbildung fachlicher Abläufe kann es nötig sein, ein Dokument mehrfach parallel
3876 zu signieren, oder existierende Signaturen gegenzusignieren. Der Konnektor unterstützt
3877 **parallele Signaturen** (QES und nonQES). Ebenso unterstützt er Gegensignaturen (QES
3878 und nonQES), die jeweils alle bestehenden Signaturen gegensignieren. Die angebotene
3879 Möglichkeit des Gegensignierens bezieht sich dabei auf das Signieren aller vorhandenen
3880 parallelen Signaturen, während ein Gegensignieren von Gegensignaturen nicht
3881 angeboten wird. Der Konnektor unterstützt ausschließlich
3882 eine **dokumentexkludierende Gegensignatur**, bei der alle Signaturen gegensigniert
3883 werden, aber nicht der fachliche Inhalt des Dokumentes selbst.

3884 TIP1-A_4623 - Unterstützte Signaturverfahren nonQES

3885 Der Signaturdienst MUSS für die Erstellung und Prüfung von nicht-qualifizierten
3886 elektronischen Signaturen (nonQES) für die `nonQES_DocFormate` die Signaturverfahren
3887 entsprechend Tabelle TAB_KON_582 – Signaturverfahren unterstützen.

3888 [\leq]

3889 TIP1-A_4627 - Unterstützte Signaturverfahren QES

3890 Der Signaturdienst MUSS für die Erstellung und Prüfung von qualifizierten elektronischen
3891 Signaturen (QES) für die `QES_DocFormate` die Signaturverfahren entsprechend Tabelle
3892 TAB_KON_582 – Signaturverfahren unterstützen.

3893 [\leq]

3894

3895 Tabelle 183: TAB_KON_582 – Signaturverfahren Dokumentensignatur

Signaturformat	Standard	Dokumentformate	QES/ nonQES	Bemerkung
XMLDSig (XAdES)	[RFC3275] [XMLDSig]	XML	QES, nonQES	Hierdurch können abgesetzte (detached), umschließende

	[XAdES] [RFC6931]			(enveloping) und eingebettete (enveloped) Signaturen erzeugt werden.
CMS (CAAdES)	[RFC5652] [CAAdES]	QES_DocFormate nonQES_DocFormate	QES, nonQES	Hierdurch können abgesetzte (detached) und umschließende (enveloping) Signaturen erzeugt werden.
PDF/A (PAdES)	[PAdES-3]	PDF/A	QES, nonQES	Hierdurch können CMS-basierte Signaturen in PDF/A-Dokumente eingefügt und dadurch eingebettete Signaturen erzeugt werden.
S/MIME	[RFC5751]	nonQES_DocFormate	nonQES	Es werden MIME-Nachrichten signiert.

3896 Zu den Begriffen detached, enveloping und enveloped Signaturen siehe beispielsweise
3897 auch [HüKo06#Abs. 4.3.3. und 4.3.1.5].

3898 TIP1-A_5446 - Zusätzliche Signaturverfahren für Dokumentensignaturprüfung
3899 Der Signatordienst MUSS für die Signaturprüfung zusätzlich zu den in „TAB_KON_582 –
3900 Signaturverfahren Dokumentensignatur“ geforderten Signaturverfahren auch die
3901 Signaturverfahren in „TAB_KON_585 – Zusätzliche Signaturverfahren für
3902 Dokumentensignaturprüfung“ unterstützen.
3903 Der Signatordienst MUSS die Prüfung basierend auf folgenden Aufrufparametern der
3904 Operation VerifyDocument vornehmen:

- 3905 • Das Signaturformat PKCS#1 (V2.1) wird durch den Wert „urn:ietf:rfc:3447“, das
3906 Signaturformat ECDSA wird durch den Wert „urn:bsi:tr:03111:ecdsa“ im
3907 folgenden Parameter identifiziert:
3908 /VerifyDocument/dss:SignatureObject/@Type
- 3909 • Der binäre Signaturstring wird in folgendem Parameter übergeben:
3910 /VerifyDocument/dss:SignatureObject/dss:Base64Signature
- 3911 • Das Dokument wird übergeben in:
3912 /VerifyDocument/SIG:Document
3913 Es werden Alle_DocFormate unterstützt.
- 3914 • Das Zertifikat wird übergeben in:
3915 /VerifyDocument/SIG:OptionalInputs/dss:AdditionalKeyInfo/ds:KeyInfo/ds:X509D
3916 ata/ds:X509Certificate

3917 Für die Prüfung von Signaturformat PKCS#1 gilt:

- 3918 • Für die kryptografische Prüfung der Signatur nach [RFC3447] ist das Dokument
3919 als Octetstring die zu prüfende „message M“.

- Nach der Rekonstruktion der „encoded message“ wird die Codierungsvariante PSS an Hand des Prüfschritts [RFC3447], Abschnitt 9.1.2, Schritt 4, identifiziert.
- Im Falle des Signaturverfahrens RSASSA-PKCS1-v1_5 ermittelt der Konnektor aus dem DigestInfo-Datenfeld in der „encoded message“ das verwendete Hashverfahren. Der Konnektor beginnt die Ausführung der Methode EMSA-PKCS1-v1_5-ENCODE nach [RFC3447], Abschnitt 9.2, mit Schritt 1, Erzeugung des Hashwertes.

Im Falle des Signaturverfahrens RSASSA-PSS geht der Konnektor von der Hashfunktionen SHA-256, einer Saltlänge von 256 bit und der Mask Generation Funktion MGF1 with SHA-256 aus. Der Konnektor beginnt die Ausführung der Methode EMSA-PSS-VERIFY nach [RFC3447], Abschnitt 9.1.2, mit Schritt 1.

Für die Prüfung von Signaturformat ECDSA gilt:

- Der Konnektor MUSS die Prüfung der Signatur gemäß [BSI-TR-03111] durchführen.

[<=]

Tabelle 184: TAB_KON_585 – Zusätzliche Signaturverfahren für Dokumentensignaturprüfung

Signaturformat (signatureType)	Standard	SignatureScheme	QES/nonQES
PKCS#1 (V2.1)	[RFC3447]	RSASSA-PSS RSASSA-PKCS1-v1_5	QES, nonQES
ECDSA	[BSI-TR-03111]		QES, nonQES

TIP1-A_5447 - Einsatzbereich der Signaturvarianten
Der Signaturdienst MUSS für die Erstellung und Prüfung von nicht-qualifizierten elektronischen Signaturen (nonQES) und qualifizierten elektronischen Signaturen (QES) die Vorgaben zum Einsatzbereich gemäß Tabelle TAB_KON_778 umsetzen.

Tabelle 185: TAB_KON_778 – Einsatzbereich der Signaturvarianten für XAdES, CAdES und PAdES

Signaturvarianten				Einsatzbereich		
Signaturverfahren	Signaturvariante	WAS wird signiert?	WO wird die Signatur abgelegt?	nonQES	QES Außen-schnittstelle	QES Fachmodul - schnittstelle
XAdES	detached	beliebiges (Binär)-Dokument	außerhalb des Dokuments in der SignResponse	Nein	Nein	Nein

XAdES	detached	gesamtes Input XML-Dokument (= Root-Element mit Subelementen)	außerhalb des Dokuments in der SignResponse	Nein	Nein	Nein
XAdES	detached	ausgewähltes nicht Root-Element mit Subelementen im Input XML-Dokument	außerhalb des Dokuments in der SignResponse	Nein	Nein	Nein
XAdES	detached	ausgewähltes nicht Root-Element mit Subelementen im Input XML-Dokument	Innerhalb des Dokuments, aber außerhalb des signierten Subbaums	Nein	Bedingt	Bedingt
XAdES	enveloped	gesamtes Input XML-Dokument (= Root-Element mit Subelementen)	Als direktes Child des Root-Elements	Ja	Bedingt	Bedingt
XAdES	enveloped	ausgewähltes nicht Root-Element mit Subelementen im Input XML-Dokument	Als direktes Child des ausgewählten Elements	Nein	Nein	Bedingt
XAdES	enveloping	gesamtes Input XML-Dokument (= Root-Element mit Subelementen)	Im Dokument, das Root-Element umschließend	Ja	Bedingt	Bedingt
XAdES	enveloping	ausgewähltes nicht Root-Element mit Subelementen im Input XML-Dokument	Im Dokument, das ausgewählte Element umschließend	Nein	Nein	Nein

CAdES	detached	gesamtes Binärdokument	außerhalb des Dokuments in der SignResponse	Ja	Ja	Ja
CAdES	enveloping	gesamtes Binär-Dokument	innerhalb des CMS-Dokuments	Ja	Ja	Ja
PAdES	-	gesamtes PDF-Dokument	Im PDF-Dokument	Ja	Ja	Ja

Legende:

Ja: Die Signaturvariante ist für den Einsatzbereich erlaubt.

Nein: Die Signaturvariante ist für den Einsatzbereich nicht erlaubt.

Bedingt: Die Signaturvariante ist für den Einsatzbereich nicht erlaubt, es sei denn es wird durch eine im Konnektor integrierte Signaturreichtlinie explizit gefordert.

Die Spalten mit gelber Kopfzeile definieren die Signaturvarianten, die mit grauer, den Einsatzbereich. Beim Einsatzbereich wird zwischen nonQES und QES unterschieden und im Fall QES nach der Bereitstellung an der Außenschnittstelle oder intern für Fachmodule.

Die benötigten Signaturvarianten werden für XAdES über die Aufrufparameter

IncludeObject und SignaturePlacement gemäß [OASIS-DSS] gesteuert.

Für CAdES erfolgt die Steuerung welche Signaturvariante gewählt wird, über den Aufrufparameter IncludeEContent.

[<=]

A_18756 - Optionalität von nonQES-XAdES Signatur

Der Konnektor KANN alle Aufrufe zu Signaturerstellung einer nonQES-XAdES Signatur mit Fehler 4111 und alle Aufrufe zur Signaturprüfung einer nonQES-XAdES Signatur mit Fehler 4112 beantworten. Die Signaturvarianten aus TAB_KON_778 werden damit weiter eingeschränkt. Wird die nonQES-XAdES Signatur umgesetzt, so ist diese in der Sicherheitszertifizierung zu betrachten.[<=]

TIP1-A_5402 - Baseline-Profilierung der AdES-EPES-Profile

Der Konnektor MUSS von den AdES-Profilen die AdES-EPES-Profile umsetzen, ergänzt um

- RevocationValues gemäß AdES-X-L,
- SignatureTimeStamp (für Signaturprüfung, nicht für Signaturerstellung) gemäß AdES-T

Dabei MUSS der Konnektor die Baseline-Profilierung gemäß Kapitel 6 in [XAdES Baseline Profile] für XAdES, Kapitel 6 in [CAdES Baseline Profile] für CAdES und Kapitel 6 in [PAdES Baseline Profile] für PAdES umsetzen.

[<=]

Durch die Baseline-Profilierung der AdES-BES-Profile wird festgelegt, wie der Signaturzeitpunkt, gemessen als Systemzeit des Konnektors, in die Signatur eingebracht wird.

TIP1-A_5403 - Common PKI konforme Profile

Der Konnektor SOLL die signierten Dokumente konform zu [COMMON_PKI#Part 3] und [COMMON_PKI#Part 8] erstellen.

[<=]

3982 TIP1-A_4624 - Default-Signaturverfahren nonQES
 3983 Bei fehlender expliziter Angabe durch den Aufrufer MUSS der Signaturdienst bei der
 3984 Erstellung von nicht-qualifizierten elektronischen Signaturen (nonQES) die Default-
 3985 Signaturverfahren entsprechend TAB_KON_583 Default-Signaturverfahren wählen.
 3986 [\leq]

3987 TIP1-A_4628 - Default-Signaturverfahren QES
 3988 Bei fehlender expliziter Angabe durch den Aufrufer MUSS der Signaturdienst bei der
 3989 Erstellung von qualifizierten elektronischen Signaturen (QES) die Default-
 3990 Signaturverfahren entsprechend TAB_KON_583 – Default-Signaturverfahren wählen.
 3991 [\leq]

3992

3993 **Tabelle 186: TAB_KON_583 – Default-Signaturverfahren**

Dokument- Format	Signaturverfahren (und -variante)			
	Signaturverfahren	Signaturvariante	WAS wird signiert?	WO wird die Signatur abgelegt?
XML	XAdES	enveloped	gesamtes Input XML-Dokument (= Root-Element mit Subelementen)	als direktes Child des Root-Elements
PDF/A	PADES	-	gesamtes PDF-Dokument	im PDF-Dokument
alle anderen	CADES	detached	gesamtes Binärdokument	außerhalb des Dokuments in der SignResponse

3994 TIP1-A_5387 - Erweiterte Nutzung der AdES-Profile
 3995 Der Konnektor MUSS auf eine vollständige Nutzung der AdES-Profile erweiterbar sein.
 3996 [\leq]

3997 TIP1-A_5033 - Missbrauchserkennung Signaturdienst (nonQES)
 3998 Der Konnektor MUSS zur Unterstützung von Missbrauchserkennungen die in Tabelle
 3999 TAB_KON_584 gelisteten Operationen als Einträge in EVT_MONITOR_OPERATIONS
 4000 berücksichtigen.
 4001

4002 **Tabelle 187: TAB_KON_584 nonQES-Operationen für EVT_MONITOR_OPERATIONS**

Operationsname	OK_Val	NOK_Val	Alarmwert (Default-Grenzwert 10 Minuten-Σ)
SignDocument (nonQES)	1	5	41
VerifyDocument (nonQES)	1	5	61

4003

4004 [\leq]

4005 TIP1-A_4629 - Unterstützte Karten QES-Erstellung

- 4006 Der Signatordienst MUSS für die QES-Erstellung die Kartentypen HBA, HBA-qSig und
4007 ZOD_2.0 unterstützen.
4008 [\leq]
- 4009 TIP1-A_5436 - XML Dokument nach Entfernen der Signatur unverändert
4010 Der Konnektor MUSS die Operation SignDocument für XML-Dokumente so
4011 implementieren, dass das Dokument nach Entfernen der Signatur, insbesondere auch
4012 einer Teilsignatur, als Ganzes unverändert ist, wobei zwei XML-Dokumente als identisch
4013 zu betrachten sind, wenn sie gemäß Canonical XML 1.1 gleich sind [CanonXML1.1].
4014 [\leq]
- 4015 TIP1-A_5682 - XML Nicht geeignete Algorithmen im VerificationReport
4016 Der Konnektor MUSS im VerificationReport einer QES-Signaturprüfung ausweisen, wenn
4017 die für die Signatur verwendeten Algorithmen nach dem Algorithmenkatalog [ALGCAT]
4018 als nicht geeignet eingestuft werden.
4019 [\leq]
- 4020 A_17768 - Zertifikate und Schlüssel für Signaturerstellung und Signaturprüfung (QES
4021 und nonQES)
4022 Der Konnektor MUSS bei der Signaturerstellung und Signaturprüfung (QES und nonQES) die
4023 Zertifikate und Schlüssel gemäß den Vorgaben in TAB_KON_900 ermitteln.
4024 **Tabelle 188: TAB_KON_900 Zertifikate und private Schlüssel für Signaturerstellung und**
4025 **Signaturprüfung (QES und nonQES)**

Karte	Crypt	Zertifikat (Verify)	Schlüssel (Sign)	Einsatzbereich	
				Außen-schnittstelle	Fachmodul-schnittstelle
QES		...in DF.QES			
HBA	RSA	EF.C.HP.QES.R2048	PrK.HP.QES.R2048	ja	ja
	ECC	EF.C.HP.QES.E256	PrK.HP.QES.E256	ja	ja
	RSA_ECC	[ab G2.1]: EF.C.HP.QES.E256 [G2.0]: EF.C.HP.QES.R2048	[ab G2.1]: PrK.HP.QES.E256 [G2.0]: PrK.HP.QES.R2048	ja	ja
HBA-VK	RSA	EF.C.HP.QES	PrK.HP.QES	ja	ja
nonQES		...in DF.ESIGN			
SM-B	RSA	EF.C.HCI.OSIG.R2048	PrK.HCI.OSIG.R2048	ja	ja
	ECC	EF.C.HCI.OSIG.E256	PrK.HCI.OSIG.E256	ja	ja

	RSA_E CC	[ab G2.1]: EF.C.HCI.OSI G.E256 [G2.0]: EF.C.HCI.OSIG.R 2048	[ab G2.1]: PrK.HCI.OSI G.E256 [G2.0]: PrK.HCI.OSIG.R 2048	ja	ja
eGK	RSA	EF.C.CH.AUT.R2048	PrK.CH.AUT.R2048	nein	ja
	ECC	EF.C.CH.AUT.E256	PrK.CH.AUT.E256	nein	ja
	RSA_E CC	[ab G2.1]: EF.C.CH.AUT. E256 [G2.0]: EF.C.CH.AUT.R2 048	[ab G2.1]: PrK.CH.AUT. E256 [G2.0]: PrK.CH.AUT.R20 48	nein	ja

[<=]

Tabelle 189: TAB_KON_862 Werteliste und Defaultwert des Parameters crypt bei QES-Erzeugung

Typname	Werteliste	Defaultwert	Bedeutung
SIG_CRYPT_QES	RSA ECC RSA_ECC	RSA_ECC	Werteliste des Parameters crypt bei der bei der Erzeugung einer QES-Signatur RSA: Es wird eine RSA-2048 Signatur erzeugt. ECC: Es wird eine ECC-256 Signatur erzeugt. RSA_ECC: In Abhängigkeit von der Kartengeneration wird eine RSA-2048 bzw. eine ECC-256 Signatur erzeugt (siehe TAB_KON_900).

Tabelle 190: TAB_KON_863 Werteliste und Defaultwert des Parameters crypt bei nonQES-Erzeugung

Typname	Werteliste	Defaultwert	Bedeutung
SIG_CRYPT_nonQES	RSA ECC RSA_ECC	RSA	Werteliste des Parameters crypt bei der bei der Erzeugung einer nonQES-Signatur RSA: Es wird eine RSA-2048 Signatur erzeugt. ECC: Es wird eine ECC-256 Signatur erzeugt. RSA_ECC: In Abhängigkeit von der Kartengeneration wird eine RSA-2048 bzw. eine ECC-256 Signatur erzeugt (siehe TAB_KON_900).

4034 4.1.8.1.2 Signaturreichtlinien

4035 Signaturreichtlinien dienen der Profilierung von Signaturerstellung und -prüfung. Beim
4036 Aufruf der Operation SignDocument kann eine URI übergeben werden, die eine im
4037 Konnektor hinterlegte Signaturreichtlinie referenziert. Die Plattform des Konnektors stellt
4038 selbst keine Signaturreichtlinien bereit. Fachanwendungen, die Signaturreichtlinien
4039 erfordern, definieren diese im Fachmodul des Konnektors. Für XML-Dokumentenformate
4040 aus der Menge von QES_DocFormate können die nachfolgenden Aspekte über eine
4041 Signaturreichtlinie gekapselt festgelegt werden:

- 4042 • XML-Schemas für die Typkonformitätsprüfung (im Konnektor zu hinterlegen)
- 4043 • Constraints für den Aufruf der Schnittstelle SignDocument und VerifyDocument,
4044 die zur Profilierung der Schnittstelle dienen.

4045 TIP1-A_5538 - Signaturreichtlinien bei QES für XML-Dokumentenformate
4046 Der Konnektor MUSS Signaturreichtlinien für XML-Dokumentenformate aus der Menge von
4047 QES_DocFormate bei der Signaturerstellung und -prüfung umsetzen.
4048 Der Konnektor MUSS den für jede Signaturreichtlinie definierten Bezeichner (URI) bei der
4049 Signatur als SigPolicyId im Feld SignaturePolicyIdentifier einbetten. Bei der
4050 Signaturprüfung MUSS der Konnektor über eine etwaig vorhandene SigPolicyId die
4051 Signaturreichtlinie identifizieren.
4052 Die gemäß AdES erforderliche Hash-Referenz über die Policy (SigPolicyHash) MUSS
4053 Schema-konform leer gelassen werden. Bei der Signaturprüfung DARF die Hash-Referenz
4054 über die Policy NICHT geprüft werden.
4055 [**<=**]

4056 4.1.8.1.3 Signaturzeitpunkt

4057 Bezogen auf den vom Konnektor für die Signaturprüfung anzunehmenden
4058 Signaturstellungszeitpunkt werden in dieser Spezifikation die Bezeichner
4059 Ermittelter_Signaturzeitpunkt und Benutzerdefinierter_Zeitpunkt verwendet.

4060 **Ermittelter_Signaturzeitpunkt:** Vom Konnektor ermittelter Zeitpunkt, zu dem eine
4061 Signatur geprüft wird. Es werden folgende Signaturzeitpunkte ermittelt:

- 4062 1. Ermittelter_Signaturzeitpunkt_Eingebettet:
4063 in der Signatur eingebetteter Zeitpunkt (falls vorhanden)
- 4064 2. Ermittelter_Signaturzeitpunkt_System:
4065 Systemzeit des Konnektors bei Signaturprüfung

4066 Anmerkung: Bei vom Konnektor selbst erstellten Signaturen ist immer ein in der Signatur
4067 eingebetteter Zeitpunkt vorhanden, jedoch kein qualifizierter Zeitstempel, da in der TI
4068 keine qualifizierten Zeitstempel ausgestellt werden. Sollte ein Dokument mit einem
4069 qualifizierten Zeitstempel versehen sein, so wird dieser nicht für die Ermittlung des
4070 Signaturzeitpunktes herangezogen.

4071 **Benutzerdefinierter_Zeitpunkt:** Vom Benutzer beim Aufruf der Signaturprüfoperation
4072 als Parameter an den Konnektor übergebener Zeitpunkt, zu dem eine Signatur geprüft
4073 werden soll.

4074 4.1.8.1.4 Jobnummer

4075 Da die eHealth-Kartenterminals dezentral über eine Netzwerkschnittstelle am Konnektor
4076 betrieben werden, fehlt die Möglichkeit zur direkten physischen und vom Anwender
4077 kontrollierbaren Zuordnung eines solchen Terminals zu einem Arbeitsplatz, auf dem sich
4078 das Clientsystem befindet.

4079 Daher ist es bei einer fehlerhaften Zuordnung eines eHealth-Kartenterminals zu einem
4080 Arbeitsplatz möglich, dass die PIN-Eingabeaufforderung – beispielsweise zu einem
4081 Signaturauftrag – an ein entferntes Kartenterminal weitergeleitet wird. Diese fehlerhafte
4082 Zuordnung kann durch einen Fehler des Clientsystems oder den Versuch eines Angriffes
4083 hervorgerufen werden.

4084 Die Jobnummern werden vom Konnektor erzeugt und können durch Clientsystem oder
4085 Signaturproxy abgerufen werden. Der Konnektor stellt jedoch keine Verbindung zwischen
4086 erzeugten und verwendeten Jobnummern her. Es wird also nicht geprüft, ob nur
4087 Jobnummern verwendet werden, die vorher vom Konnektor erzeugt wurden, oder ob alle
4088 Jobnummern verwendet werden, die vom Konnektor erzeugt wurden.

4089 TIP1-A_4639 - Generierung von Jobnummern für PIN-Eingaben
4090 Um Fehler- und Angriffsmöglichkeiten auszuschließen, MUSS der Konnektor bei
4091 bestimmten PIN-Verifikationen vor der Aufforderung zur PIN-Eingabe an einem eHealth-
4092 Kartenterminal eine hinreichend eindeutige Nummer – die Jobnummer – generieren,
4093 welche den Auftrag kennzeichnet, für dessen Verarbeitung die PIN-Eingabe erfolgen soll.
4094 Bei welchen PIN-Verifikationen dies der Fall ist, kann den PIN-Prompts in TAB_KON_090
4095 Terminalanzeigen beim Eingeben der PIN am Kartenterminal entnommen werden.

4096 [**<=**]

4097 TIP1-A_4640 - Anzeige der Jobnummern für PIN-Eingaben
4098 Diese Jobnummer MUSS vom Konnektor im Display des eHealth-Kartenterminals neben
4099 der PIN-Eingabeaufforderung angezeigt werden.

4100 [**<=**]

4101 TIP1-A_4992 - Guidance zur Jobnummer
4102 Das Handbuch des Konnektors MUSS den Benutzer über den korrekten Gebrauch der
4103 Jobnummer informieren. Es MUSS ihm verdeutlichen, dass er seine PIN über die Tastatur
4104 des eHealth-Kartenterminals nur eingeben darf, wenn am Signaturproxy bzw.
4105 Primärsystem und am Display des Kartenterminals die gleiche Jobnummer angezeigt
4106 wird. Stimmen die beiden Nummern nicht überein, so soll der Benutzer seine PIN nicht
4107 eingeben und stattdessen weitergehende Schritte zur Klärung des aufgetretenen
4108 Fehlverhaltens einleiten.

4109 [**<=**]

4110 TIP1-A_4642 - Ableitung der Jobnummer von einem Zufallswert
4111 Zur hinreichend eindeutigen Kennzeichnung des Vorganges MUSS eine Jobnummer von
4112 einem Zufallswert abgeleitet sein, wobei die Vorgaben an einen solchen Zufallswert
4113 beachtet werden MÜSSEN [gemSpec_Krypt#2.2].

4114 [**<=**]

4115 TIP1-A_4643 - Beschaffenheit der Jobnummer
4116 Zur Wahrung der Benutzerfreundlichkeit MUSS eine Reduzierung der Jobnummer auf eine
4117 Länge von sechs Zeichen erfolgen. Diese sechs Zeichen MÜSSEN in zwei Zeichengruppen
4118 mit je drei Zeichen, getrennt durch einen Bindestrich (0x2D), dargestellt werden. Die
4119 erste Zeichengruppe MUSS ausschließlich die Zeichen "A-Z" beinhalten, die zweite
4120 Zeichengruppe MUSS aus Ziffern "0-9" bestehen. Die Länge der resultierenden,
4121 reduzierten Jobnummer ist sieben und wird durch den Umfang der darstellbaren Zeichen
4122 auf dem Display des eHealth-Kartenterminals beschränkt.

4123 [**<=**]

4124 TIP1-A_4644 - Jobnummer über 1.000 Vorgänge eindeutig
4125 Der Konnektor MUSS die Eindeutigkeit einer Jobnummer sicherstellen:

- 4126 • Bei Aufruf der Operation GetJobnumber MUSS der Konnektor innerhalb von 1000
- 4127 Aufrufen eine eindeutige Jobnummer generieren. Die Zählung der Aufrufe erfolgt
- 4128 dabei unabhängig vom Aufrufkontext.

- Wird die Operation SignDocument mit einer Jobnummer aufgerufen, die innerhalb der vorangegangenen 1.000 Vorgänge verwendet wurde, so MUSS der Konnektor die Bearbeitung mit dem Fehler 4252 abbrechen. Die Zählung der Aufrufe erfolgt dabei unabhängig vom Aufrufkontext.

4133 [**<=**]

4134 TIP1-A_4645 - Zeichen der Jobnummer

4135 Die einzelnen Zeichen der Jobnummer MÜSSEN für die Anzeige am Kartenterminal gemäß dem Zeichensatz ISO 646DE/DIN66003, bzw. ISO 646 US codiert werden. Aus diesem Zeichensatz dürfen nur die Zeichen „A-Z“ (0x41 bis 0x5A) und die Ziffern „0-9“ (0x30 bis 0x39) für die Anzeige der Jobnummer verwendet werden.

4139 [**<=**]

4140 Beispiele für eine Jobnummer sind ABC-475 und HZF-696.

4141 Die Einbettung der Jobnummer in den Nachrichtentext für den Bildschirm des Kartenlesers wird in TAB_KON_090 Terminalanzeigen beim Eingeben der PIN am Kartenterminal beschrieben.

4144 4.1.8.1.5 Komfortsignatur

4145 Für die QES unterstützt der Konnektor die Komfortsignaturfunktion. In diesem Modus können für ein- und denselben HBA mehrere vom Clientsystem initiierte Signaturaufträge (Einzel- oder Stapelsignatur) abgearbeitet werden, ohne dass der Inhaber des HBA für jeden einzelnen dieser Signaturaufträge die PIN.QES am Kartenterminal eingeben muss.

4150 Im Auslieferungszustand ist die Komfortsignaturfunktion ausgeschaltet (SAK_COMFORT_SIGNATURE = Disabled), d. h. mit dem Konnektor können zunächst keine Komfortsignaturen durchgeführt werden. Die Komfortsignaturfunktion kann vom Administrator eingeschaltet werden. Dies ist nur möglich, wenn an der Clientsystemschnittstelle des Konnektors verpflichtend TLS mit Clientauthentisierung (Konfigurationsvariante SOAP1 und SOAP2 in TAB_KON_852) konfiguriert ist. Das Einschalten der Komfortsignaturfunktion im Konnektor hat zur Folge, dass alle Operationen an der Clientsystemschnittstelle nur über TLS mit Clientauthentisierung angesprochen werden können (außer ggf. Dienstverzeichnisdienst).

4159 Bei eingeschalteter Komfortsignaturfunktion können potentiell alle HBAs in der Umgebung, in der der Konnektor eingesetzt ist, Komfortsignaturen durchführen. Die eigentliche Aktivierung der Komfortsignatur muss separat für jeden einzelnen HBA erfolgen.

4163 Durch Aufruf der Operation ActivateComfortSignature des Konnektors durch das Primärsystem wird die Nutzung der Komfortsignatur für einen HBA (Komfortsignaturmodus) aktiviert. Dazu muss der HBA-Inhaber die PIN.QES eingeben.

4166 Der Konnektor merkt sich für die Cardsession des HBA, dass die Komfortsignatur aktiviert wurde. Bei den folgenden Aufrufen von SignDocument werden dann Komfortsignaturen ausgeführt, solange bis eines der folgenden Abbruchkriterien eintritt:

- Die vom HBA (entsprechend Personalisierung) oder die vom Konnektor (entsprechend Konfiguration SAK_COMFORT_SIGNATURE_MAX) durchgesetzte maximale Anzahl von Signaturen wurde erreicht.
- Das konfigurierte Zeitintervall für die Komfortsignatur (entsprechend Konfiguration SAK_COMFORT_SIGNATURE_TIMER) ist für die Cardsession abgelaufen.
- Der Komfortsignaturmodus wurde für die betroffene Cardsession deaktiviert.

- 4175 • Der HBA wurde gezogen.
- 4176 • Der Sicherheitszustand des HBA wurde zurückgesetzt.
- 4177 • Die Komfortsignaturfunktion wurde für den Konnektor durch den Administrator deaktiviert.
- 4178 A_19945 - Unterstützte Signaturvarianten bei Komfortsignatur
- 4179 Der Signatordienst MUSS bei der Komfortsignatur die Signaturvarianten für die QES
- 4180 gemäß TAB_KON_778 unterstützen.【<=】
- 4181 A_18597 - Sicherheitszustand der PIN.QES bei Komfortsignatur
- 4182 Bei der Komfortsignatur DARF der Konnektor den Sicherheitszustand der PIN.QES NICHT
- 4183 selbsttätig zurücksetzen, außer wenn dies explizit spezifikatorisch gefordert wird.【<=】
- 4184 A_18597 kann z. B. umgesetzt werden, indem
- 4185 • ein dedizierter logischer Kanal des HBA für die Komfortsignatur verwendet
- 4186 wird und
- 4187 • im dedizierten logischen Kanal des HBA die Selektion von DF.QES solange
- 4188 beibehalten wird, bis ein Verlassen von DF.QES durch die Spezifikation explizit
- 4189 gefordert wird.
- 4190 A_18686 - Komfortsignatur-Timer
- 4191 Der Konnektor MUSS für jede HBA-Kartensitzung mit eingeschalteter Komfortsignatur
- 4192 einen Komfortsignatur-Timer gemäß konfiguriertem Zeitintervall
- 4193 SAK_COMFORT_SIGNATURE_TIMER einrichten und nach Erreichen des Maximalwerts den
- 4194 Sicherheitszustand des HBA zurücksetzen.【<=】
- 4195 A_19100 - Komfortsignatur-Zähler
- 4196 Der Konnektor MUSS für jeden gesteckten HBA mit eingeschalteter Komfortsignatur die an
- 4197 die Karte gesendeten Signaturaufträge zählen und nach Erreichen des Maximalwerts den
- 4198 Sicherheitszustand des HBA zurücksetzen.【<=】
- 4199 A_19258 - Secure Messaging bei Komfortsignatur
- 4200 Bei der Komfortsignatur MUSS der Signatordienst die zu signierenden Daten (DTBS) über
- 4201 Secure Messaging vom Konnektor zum HBA übertragen. Dieser Secure Messaging-Kanal
- 4202 MUSS über die gSMC-K zum HBA mittels C.SAK.AUTD_CVC aufgebaut werden.【<=】
- 4203 A_20073 - Prüfung der Länge der UserId
- 4204 Der Konnektor MUSS die beim Aktivieren des Komfortsignaturmodus vom PS übermittelte
- 4205 UserId für die Kartensitzung des HBA, für den der Modus aktiviert wird, auf die
- 4206 ausreichende Länge von 128 Bit prüfen und die Aktivierung mit Fehler 4272 ablehnen,
- 4207 wenn die UserId nicht ausreichend lang ist.【<=】
- 4208 A_20074 - UserId über 1.000 Vorgänge eindeutig
- 4209 Der Konnektor MUSS die Eindeutigkeit der UserId sicherstellen. Wird die Operation
- 4210 ActivateComfortSignature mit einer UserId im Aufrufkontext aufgerufen, die innerhalb
- 4211 der vorangegangenen 1.000 Vorgänge bereits verwendet wurde, so MUSS der Konnektor
- 4212 die Bearbeitung mit dem Fehler 4270 abbrechen. Die Zählung der Aufrufe erfolgt dabei
- 4213 unabhängig vom Aufrufkontext.【<=】
- 4214 A_19101 - Handbuch-Hinweis zu Nutzerauthentisierung am Clientsystem bei
- 4215 Komfortsignatur
- 4216 Das Handbuch des Konnektors MUSS einen Hinweis enthalten, dass die Authentifizierung
- 4217 des HBA-Inhabers für die Komfortsignatur vom Clientsystem vorgenommen wird und
- 4218 dass die Authentifizierung des Nutzers am Clientsystem einen unverzichtbaren Beitrag
- 4219 zur Sicherheit der Lösung leistet.【<=】
- 4220

4.1.8.2 Durch Ereignisse ausgelöste Reaktionen

keine

4.1.8.3 Interne TUCs, nicht durch Fachmodule nutzbar

Abbildung PIC_KON_103 Use Case Diagramm Signaturdienst (nonQES) beschreibt die Aufrufbeziehungen der nonQES-TUCs des Signaturdienstes. Die TUCs des Signaturdienstes sind weiß dargestellt. Genutzte TUCs anderer Basisdienste sind grau hinterlegt.

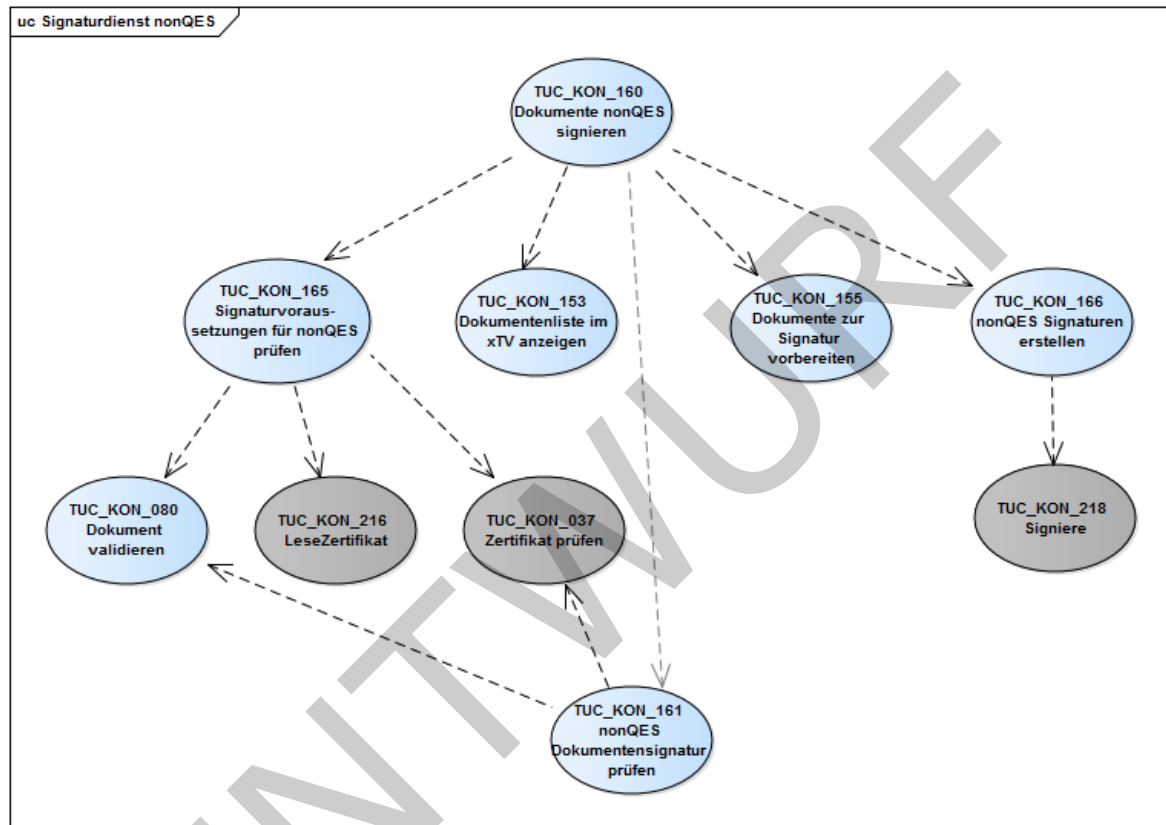


Abbildung 15: PIC_KON_103 Use Case Diagramm Signaturdienst (nonQES)

Abbildung PIC_KON_104 Use Case Diagramm Signaturdienst (QES) beschreibt die Aufrufbeziehungen der QES-TUCs des Signaturdienstes.

4232

4233
42344235 **Abbildung 16: PIC_KON_104 Use Case Diagramm Signatordienst (QES)**

4236 Abbildung PIC_KON_102 Use Case Diagramm Signatordienst (Komfortsignatur)
4237 beschreibt die Aufrufbeziehungen der TUCs des Signatordienstes für die Komfortsignatur.

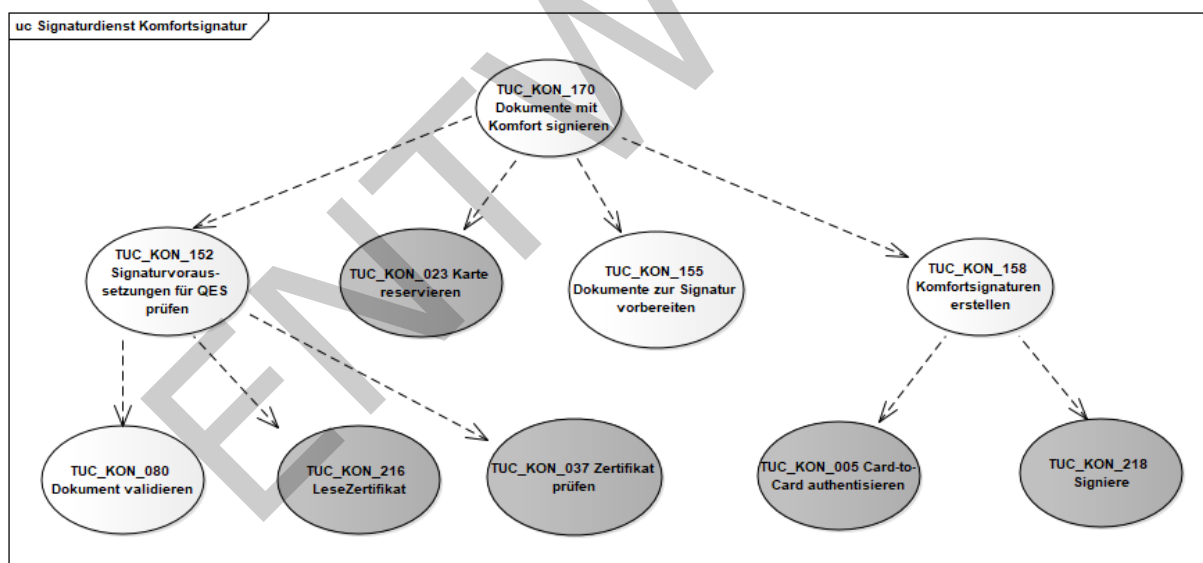
4238
4239

Abbildung 17: PIC_KON_102 Use Case Diagramm Signatordienst (Komfortsignatur)

4240 4.1.8.3.1 TUC_KON_155 „Dokumente zur Signatur vorbereiten“

4241 TIP1-A_4646-02 - ab PTV4: TUC_KON_155 „Dokumente zur Signatur vorbereiten“

4242 Der Konnektor MUSS den technischen Use Case TUC_KON_155 „Dokumente zur Signatur
4243 vorbereiten“ umsetzen.

4244

4245 **Tabelle 191: TAB_KON_748 - TUC_KON_155 „Dokumente zur Signatur vorbereiten“**

Element	Beschreibung
---------	--------------

Name	TUC_KON_155 "Dokumente zur Signatur vorbereiten"
Beschreibung	Die zu signierenden Dokumente werden entsprechend den Erfordernissen der Signaturverfahren für die QES oder nonQES vorbereitet.
Anwendungsumfeld	Erstellung von qualifizierten elektronischen Signaturen (QES) und nicht-qualifizierten elektronischen Signaturen (nonQES)
Auslöser	Aufruf durch TUC_KON_150 „Dokumente QES signieren“ oder TUC_KON_160 „Dokumente nonQES signieren“
Vorbedingungen	keine
Eingangsdaten	<ul style="list-style-type: none"> - signatureMode (Signaturart: QES nonQES) - documentsToBeSigned (Zu signierendes Dokument bzw. zu signierende Dokumente) und pro Dokument: - documentFormat (Formatangabe für das zu signierende Dokument) - optionalInputs (weitere optionale Eingabeparameter zur Steuerung der Details bei der zu erstellenden Signatur (siehe Operation SignDocument, Parameter dss:OptionalInputs), darin u.a. - signatureType (URI für den Signatortyp XML-, CMS-, S/MIME- oder PDF-Signatur) - certificate (Signaturzertifikat) - ocspsResponses – <i>optional</i> (OCSP-Response des EE-Zertifikats, das bei der Signaturerstellung in die Signatur eingebettet wird.)
Komponenten	Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> • preProcessedDocuments (Aufbereitetes zu signierendes Dokument bzw. aufbereitete zu signierende Dokumente)
Standardablauf	signatureType = XMLDSig (XAdES) Entsprechend den Regeln für die QES und die nonQES werden zunächst weitere Signatureigenschaften zum jeweiligen Dokument in Form von <i>QualifyingProperties</i> (siehe [XAdES]) hinzugefügt. Die Systemzeit des Anwendungskonnektors muss in das XML-Element <i>SigningTime</i> (siehe [XAdES]) eingetragen werden. Die Signatur wird anschließend entsprechend [XMLDSig] vorbereitet. D. h., es

	<p>wird je Dokument nach Erzeugung der Reference Elemente das SignedInfo Element aufgebaut. Dessen Inhalt ergibt dann nach erfolgter XML-Kanonisierung und Hashing die DTBS (Data To Be Signed), die später zur Karte gesendet werden.</p> <p>certificate wird im Element <code>ds:KeyInfo/ds:X509Data</code> gespeichert.</p> <p>Im Fall <code>signatureMode = QES</code> können neben den reinen Nutzdaten auch alle weiteren Elemente in die Signatur einbezogen werden, die für die Rekonstruktion der ursprünglich dargestellten Daten in der sicheren Anzeige erforderlich sind. Für XML-Dokumente sind das, falls vorhanden, das/die XML-Schema(ta). Für diese werden Referenzen (Hash + URI) in die Signatur eingebettet.</p> <p>Die URI ist im Fall übergebener XML-Schemata der übergebene <i>signatureType</i> - Parameter. Die URI ist im Fall der im Konnektor im Rahmen einer Signaturreichtlinie hinterlegten XML-Schemata/XSL-Stylesheets die URI der Signaturreichtlinie, ergänzt um den Dateinamen mit Pfad, wie in der Signaturreichtlinie festgelegt.</p> <p>(Beispiel: URI für Schemadatei <code>NFD_Document.xsd</code> der Signaturreichtlinie <code>SR_DF_NFDM_NOTFALLDATEN</code> lautet: <code>urn:gematik:fa:sak:nfdm:r1:v1:NFD_Document.xsd</code>)</p> <p>Das Einbetten der Referenzen erfolgt über das XML-Element <code>ds:object/ds:manifest (XMLDSig)</code> mit eingebetteten XML-Elementen <code>ds:Reference</code>, die eine URI (RefURI) als Identifier für die jeweilige Datei und einen Hash über die jeweilige Resource enthalten. Der ShortTextClientsystem muss in die Signatur in das <code>DataObjectFormat/Description-Element</code> gemäß [XAdES] (Abschnitt 7.2.5) eingebettet werden.</p> <p>Falls durch den Aufrufparameter <code>SIG:IncludeRevocationInfo</code> angefordert, wird die für die Offline-Prüfung notwendige OCSP-Antwort im Sinne vom ES-X-L vom Konnektor in die Signatur eingebettet:</p> <p>Die base-64 kodierte OCSP-Response wird im Feld <code>QualifyingProperties/UnsignedProperties/UnsignedSignatureProperties/RevocationValues/OCSPValues/EncapsulatedOCSPValue</code> (selbst DER-kodiert)</p>
--	---

	<p>gespeichert.</p> <p>signatureType = CMS (CADES) Etwaig einzubettende XML-Schemata werden zunächst wie für XAdES definiert in ein ds:manifest-Element eingebettet. Die so erzeugte Zeichenkette wird als genau ein ASN.1 Character String vom Typ UTF8String verpackt. Dieser wird als contentDescription in einen Content-Hints Attributwert vom Typ ContentHints verpackt, wobei der contentType=id-data gemäß [CADES]. Der ShortTextClientsystem muss in die Signatur in das content-hints.ContentDescription-Attribut gemäß [CADES] (Abschnitt 5.10.3) eingebettet werden.</p> <p>Ist die Einbettung von OCSP-Responses gefordert, wird die für die Offline-Prüfung notwendige OCSP-Antwort des EE-Zertifikats im Attribut SignedData.crls.other abgelegt.</p> <p>signatureType = PDF/A (PAdES) Der ShortTextClientsystem muss bei einer PDF-Signatur in das Reason-Feld eingebettet werden.</p> <p>OCSP-Responses werden bei PAdES nicht eingebettet.</p> <p>Es sind die Vorgaben zum Signaturprofil gemäß Tabelle TAB_KON_779 „Profilierung der Signaturformate“ zu erfüllen.</p> <p>Die aufbereiteten zu signierenden Dokumente werden an den Aufrufer zurückgegeben.</p>
Varianten/ Alternativen	keine
Fehlerfälle	<p>Das Verhalten des TUCs bei einem Fehlerfall ist in TAB_KON_586 Fehlercodes TUC_KON_155 „Dokumente zur Signatur vorbereiten“ „PDF/A (PAdES)“</p> <p>Es ist nicht genügend Speicherplatz im PDF-Dokument verfügbar: 4205</p>
Nichtfunktionale Anforderungen	keine

Zugehörige Diagramme	keine
----------------------	-------

4246

4247 **Tabelle 192: TAB_KON_586 Fehlercodes TUC_KON_155 „Dokumente zur Signatur**
 4248 **vorbereiten“**

Fehlercode	ErrorType	Severity	Fehlertext
4205	Technical	Error	Es ist nicht genügend Speicherplatz im PDF-Dokument verfügbar.

4249

4250 [\leq]

4251

4252 4.1.8.3.2 TUC_KON_165 „Signaturvoraussetzungen für nonQES prüfen“

4253 TIP1-A_4647-02 - TUC_KON 165 „Signaturvoraussetzungen für nonQES prüfen“
 4254 Der Konnektor MUSS den technischen Use Case „Signaturvoraussetzungen für nonQES
 4255 prüfen“ umsetzen.

4256

4257 **Tabelle 193: TAB_KON_749 – TUC_KON_165 „Signaturvoraussetzungen für nonQES**
 4258 **prüfen“**

Element	Beschreibung
Name	TUC_KON_165 „Signaturvoraussetzungen für nonQES prüfen“
Beschreibung	Es werden die Voraussetzungen an die zu signierenden Dokumente und das Signaturzertifikat geprüft. Es werden die nonQES_DocFormate unterstützt.
Auslöser	TUC_KON_160 „Dokumente nonQES signieren“
Vorbedingungen	keine
Eingangsdaten	<ul style="list-style-type: none"> • Zu signierende Dokumente • optionale Eingabeparameter zur Steuerung der Details der Signaturerstellung • cardSession Signaturkarte • zu verwendende Identität (Zertifikatsreferenz)
Komponenten	Konnektor, Kartenterminal, Signaturkarte
Ausgangsdaten	<ul style="list-style-type: none"> • Prüfergebnis • Signaturzertifikat
Standardablauf	1. Abhängig von seinem Typ werden für jedes Dokument die typabhängigen Validierungsschritte (ohne Prüfung auf sichere Anzeigbarkeit) durchgeführt. Dies geschieht durch Aufruf von TUC_KON_080 „Dokument validieren“. Wird der Aufruf von TUC_KON_080 mit einem Fehler

	<p>beendet, wird die Prüfung im laufenden TUC mit diesem Fehler abgebrochen.</p> <p>2. Durch Aufruf von TUC_KON_216 „Lese Zertifikat“ wird das Signaturzertifikat von der Signaturkarte gelesen.</p> <p>3. Das Signaturzertifikat wird durch Aufruf von TUC_KON_037 „Zertifikat prüfen“{ certificate = Zertifikatsreferenz; qualifiedCheck = not_required; offlineAllowNoCheck = true; validationMode = OCSP} geprüft.</p>
Varianten/Alternativen	Keine
Fehlerfälle	Keine
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

Tabelle 194: TAB_KON_587 Fehlercodes TUC_KON_165 „Signaturvoraussetzungen für nonQES prüfen“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können keine weiteren Fehlercodes auftreten.			

[<=]

4.1.8.3.3 TUC_KON_166 „nonQES Signaturen erstellen“

TIP1-A_4648 - TUC_KON_166 „nonQES Signaturen erstellen“

Der Konnektor MUSS den technischen Use Case TUC_KON_166 „nonQES Signaturen erstellen“ umsetzen.

Tabelle 195: TAB_KON_750 – TUC_KON_166 „nonQES Signaturen erstellen“

Element	Beschreibung
Name	TUC_KON_166 „nonQES Signaturen erstellen“
Beschreibung	Die Data To Be Signed (DTBS) werden erzeugt, an die Signaturkarte gesendet und dort signiert.
Auslöser	TUC_KON_160 „Dokumente nonQES signieren“
Vorbedingungen	keine
Eingangsdaten	<ul style="list-style-type: none"> Liste der zu signierenden Dokumente cardSession Signaturkarte zu verwendende Identität (Zertifikatsreferenz) crypt [SIG_CRYPT_nonQES]: <i>optional</i>; <i>default</i> und Wertebereich: SIG_CRYPT_DEFAULT siehe

	TAB_KON_863 (Dieser Parameter steuert, ob RSA-basierte oder ECC-basierte Signaturen erzeugt werden.)
Komponenten	Konnektor, Kartenterminal, Signaturkarte
Ausgangsdaten	<ul style="list-style-type: none"> • Signierte Dokumente
Standardablauf	<p>Die folgenden Schritte werden für jedes Dokument der Liste durchgeführt.</p> <ol style="list-style-type: none"> 1. Das zu signierende Dokument wird, soweit noch nicht erfolgt, für die XML-Signatur vorbereitet. Ein Ergebnis dieser Vorbereitung sind die Data To Be Signed (DTBS): der Hash-Wert (Digest des SignedInfo-Elementes), der zur Signatur an die Karte gesendet werden soll. Für XML-Signaturen müssen die Vorgaben aus [gemSpec_Krypt#3.1.1] beachtet werden. 2. Für das zu signierende Dokument werden die DTBS zur Signatur an die Signaturkarte übermittelt (Aufruf von TUC_KON_218 „Signiere“). Dabei werden der Schlüssel und der Algorithmusidentifizierer über die Tabelle TAB_KON_900 bestimmt. 3. Die erstellte Signatur wird mathematisch geprüft. 4. Der ermittelte Signaturwert wird in die zuvor vorbereitete XML-Signatur eingefügt. 5. Der Konnektor löst TUC_KON_256 {"SIG/SIGNDOC/NEXT_SUCCESSFUL"; Op; Info; „\$Jobnummer“; noLog; \$doInformClients } aus.
Varianten/Alternativen	keine
Fehlerfälle	Fehler in den folgenden Schritten des Standardablaufs führen zum Abbruch mit den ausgewiesenen Fehlercodes: (→3) Fehlgeschlagene mathematische Prüfung der Signatur: 4120
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

4268 **Tabelle 196: TAB_KON_120 Fehlercodes TUC_KON_166 „nonQES Signaturen erstellen“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4120	Security	Error	Kartenfehler

4269
4270 **[<=]**

- 4271 4.1.8.3.4 TUC_KON_152 "Signaturvoraussetzungen für QES prüfen"
- 4272 TIP1-A_4649 - TUC_KON_152 „Signaturvoraussetzungen für QES prüfen“
- 4273 Der Konnektor MUSS den technischen Use Case TUC_KON_152
- 4274 „Signaturvoraussetzungen für QES prüfen“ umsetzen.
- 4275

4276 **Tabelle 197: TAB_KON_751 – TUC_KON_152 „Signaturvoraussetzungen für QES prüfen“**

Element	Beschreibung
Name	TUC_KON_152 „Signaturvoraussetzungen für QES prüfen“
Beschreibung	Es werden die Voraussetzungen an die zu signierenden Dokumente und das Signaturzertifikat geprüft. Es werden die QES_DocFormate unterstützt.
Auslöser	TUC_KON_150 „Dokumente QES signieren“
Vorbedingungen	keine
Eingangsdaten	<ul style="list-style-type: none"> • Zu signierende Dokumente • optionale Eingabeparameter zur Steuerung der Details der Signaturerstellung • cardSession Signaturkarte • zu verwendende Identität (Zertifikatsreferenz) • includeRevocationInfo [Boolean] - optional; Default: true (Dieser Parameter steuert die Einbettung von OCSP-Responses in die Signatur. true: Die Sperrinformationen werden in ocsResponses zurückgegeben.)
Komponenten	Konnektor, Kartenterminal, Signaturkarte
Ausgangsdaten	<ul style="list-style-type: none"> • Prüfergebnis • Signaturzertifikat • ocsResponses - optional/nur wenn includeRevocationInfo = true (OCSP-Response des EE-Zertifikats, die beim Aufruf von TUC_KON_037 „Zertifikat prüfen“ zurückgegeben wird)
Standardablauf	<ol style="list-style-type: none"> 1. Abhängig von seinem Typ werden für jedes Dokument die typabhängigen Dokumentvalidierungsschritte durchgeführt (Aufruf TUC_KON_080 „Dokument validieren“). Wird der Aufruf von TUC_KON_080 mit einem Fehler beendet, wird die Prüfung im laufenden TUC mit diesem Fehler abgebrochen. 2. Durch Aufruf von TUC_KON_216 „Lese Zertifikat“ wird das Signaturzertifikat von der Signaturkarte gelesen. 3. Das Signaturzertifikat wird durch Aufruf von TUC_KON_037 „Zertifikat prüfen“{

	certificate = Zertifikatsreferenz; qualifiedCheck = required; offlineAllowNoCheck = true; validationMode = OCSP; getOCSPResponses = includeRevocationInfo} geprüft.
Varianten/Alternativen	keine
Fehlerfälle	(->3) Für MGM_LU_ONLINE=Enabled gilt: Liefert die Zertifikatsprüfung (OCSP-Abfrage) die Warnung CERT_REVOKED oder CERT_UNKNOWN gemäß [gemSpec_PKI#Tab_PKI_274], dann wird der TUC mit Fehler 4123 abgebrochen.
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

4277

4278

4279

Tabelle 198: TAB_KON_588 Fehlercodes TUC_KON_152 „Signaturvoraussetzungen für QES prüfen“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können keine weiteren Fehlercodes auftreten.			

4280

4281 [\leq]

4282 4.1.8.3.5 TUC_KON_154 "QES Signaturen erstellen"

4283 Der TUC_KON_154 stellt den Standardsignaturfall in der TI, die Stapelsignatur dar (auch
4284 für Stapel der Größe 1). Da die Stapelsignatur auf der Zielkarte passende CVC
4285 voraussetzt, die auf den HBA-Vorläuferkarten nicht vorhanden sind, kann dieser TUC nur
4286 den HBA unterstützen. Für HBA-Vorläuferkarten kann TUC_KON_168 verwendet werden.

4287 TIP1-A_4651 - TUC_KON_154 „QES Signaturen erstellen“

4288 Der Konnektor MUSS den technischen Use Case TUC_KON_154 „QES Signaturen
4289 erstellen“ umsetzen.

4290

4291 **Tabelle 199: TAB_KON_752 – TUC_KON_154 „QES Signaturen erstellen“**

Element	Beschreibung
Name	TUC_KON_154 „QES Signaturen erstellen“
Beschreibung	Die Data To Be Signed (DTBS) werden erzeugt, an die Signaturkarte gesendet und dort signiert.
Auslöser	TUC_KON_150 „Dokumente QES signieren“
Vorbedingungen	Die Ressourcen Signaturkarte und Kartenterminal sind für den Vorgang reserviert.

	<p>DF.QES ist selektiert. PIN.QES ist initial verifiziert</p>
Eingangsdaten	<ul style="list-style-type: none"> • Zu signierendes Dokument bzw. zu signierende Dokumente • cardSession (nur HBA erlaubt) • zu verwendende Identität (Zertifikatsreferenz) • crypt [SIG_CRYPT_QES] - <i>optional</i>; <i>default und Wertebereich</i>: siehe TAB_KON_862 (Dieser Parameter steuert, ob RSA-basierte oder ECC-basierte Signaturen erzeugt werden.) • WorkplaceId
Komponenten	Konnektor, Kartenterminal, Signaturkarte (HBA)
Ausgangsdaten	<ul style="list-style-type: none"> • Signierte Dokumente
Standardablauf	<p>Basierend auf SAK.AUTD_CVC und HPC.AUTD_SUK_CVC und den zugehörigen privaten Schlüsseln wird ein sicherer Kanal zwischen der gSMC-K des Konnektors und dem HBA aufgebaut mittels Aufruf TUC_KON_005 „Card-to-Card authentisieren“ { sourceCardSession = gSMC-K; targetCardSession = CardSession; authMode = „gegenseitig+TC“}</p> <p>Die folgenden Schritte werden für jedes Dokument des Stapels durchgeführt.</p> <ol style="list-style-type: none"> 1. Das zu signierende Dokument wird, soweit noch nicht erfolgt, für die Signatur gemäß des entsprechenden Formats vorbereitet. Ein Ergebnis dieser Vorbereitung sind die Data To Be Signed (DTBS): der Hash-Wert (Digest des SignedInfo-Elementes), der zur Signatur an die Karte gesendet werden soll. 2. Für das zu signierende Dokument werden die DTBS zur Signatur im sicheren Kanal an den HBA übermittelt (Aufruf TUC_KON_218 „Signiere“). Dabei werden der Schlüssel und der Algorithmusidentifizierer über die Tabelle TAB_KON_900 bestimmt. 3. Falls Schritt 3 fehlgeschlagen ist, weil der PIN.QES-Nutzungszähler abgelaufen ist (erkennbar z. B. daran, dass die Karte einen Autorisierungsfehler zurückmeldet), wird die PIN.QES verifiziert (Aufruf TUC_KON_012 „PIN verifizieren“, nachdem der im Konnektor verwaltete Sicherheitszustand (CARDSESSION.AUTHSTATE) aktualisiert wurde). Am Display des Kartenterminals wird dabei die Jobnummer für den Signaturvorgang angezeigt. Aus der WorkplaceId geht hervor, ob es sich um

	<p>eine Remote-PIN-Eingabe handelt. Nach der PIN-Verifikation wird erneut die zuvor fehlgeschlagene Signatur in Schritt 3 ausgeführt.</p> <ol style="list-style-type: none"> 4. Die erstellte Signatur wird mathematisch geprüft. 5. Der ermittelte Signaturwert wird in den zuvor vorbereiteten Signaturprototypen eingefügt. 6. Der Konnektor löst TUC_KON_256 {"SIG/SIGNDOC/NEXT_SUCCESSFUL"; Op; Info; „\$Jobnummer“; noLog; \$doInformClients } aus.
Varianten/ Alternativen	<p>Alternativ zum Standardablauf kann zu Beginn die maximal erlaubte Stapelgröße SSEC durch Auslesen von EF.SSEC ermittelt werden. Der zu signierende Dokumentenstapel wird in Teilstapel von maximaler Größe SSEC zerlegt. Für jeden Teilstapel wird die PIN.QES verifiziert. Die Dokumente des Teilstapels werden wie im Standardablauf beschrieben signiert. Der Nutzer kann den Vorgang der PIN-Eingabe abbrechen.</p>
Fehlerfälle	<p>(->2) Fehler im Signaturvorgang führen zum Abbruch des gesamten Signaturvorgangs, Fehlercode 4123 (->3) Fehler bei der PIN-Eingabe führen zum Abbruch des Signaturvorgangs (->4) Fehler in mathematischer Prüfung der Signatur führen zum Abbruch des Signaturvorgangs, Fehlercode 4120 Das Verhalten des TUCs bei einem Fehlerfall, einem Timeout der PIN-Eingabe oder beim Abbruch durch den Benutzer ist in Tabelle TAB_KON_192 Verhalten des Konnektors beim Abbruch einer Stapelsignatur beschrieben.</p>
Sicherheitsanforderungen	<p>Zum Aufbau des sicheren Kanals bzw. zur Aushandlung des symmetrischen Schlüssels DARF DF.QES NICHT verlassen werden. Benötigte CVCs des HBA MÜSSEN also bereits vor dem Signaturvorgang eingelesen und gecacht werden. Dies KANN bereits beim Stecken des HBA geschehen. Die in [gemSpec_Krypt#3.1.2] angegebenen Festlegungen der zu unterstützenden Algorithmen MÜSSEN berücksichtigt werden.</p>
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	<p>Abbildung PIC_KON_113 Aktivitätsdiagramm zu „QES Signaturen erstellen“ Das Diagramm dient nur der Veranschaulichung und ist nicht vollständig. Beispielsweise enthält es nicht die Steuerung durch den Parameter crypt.</p>

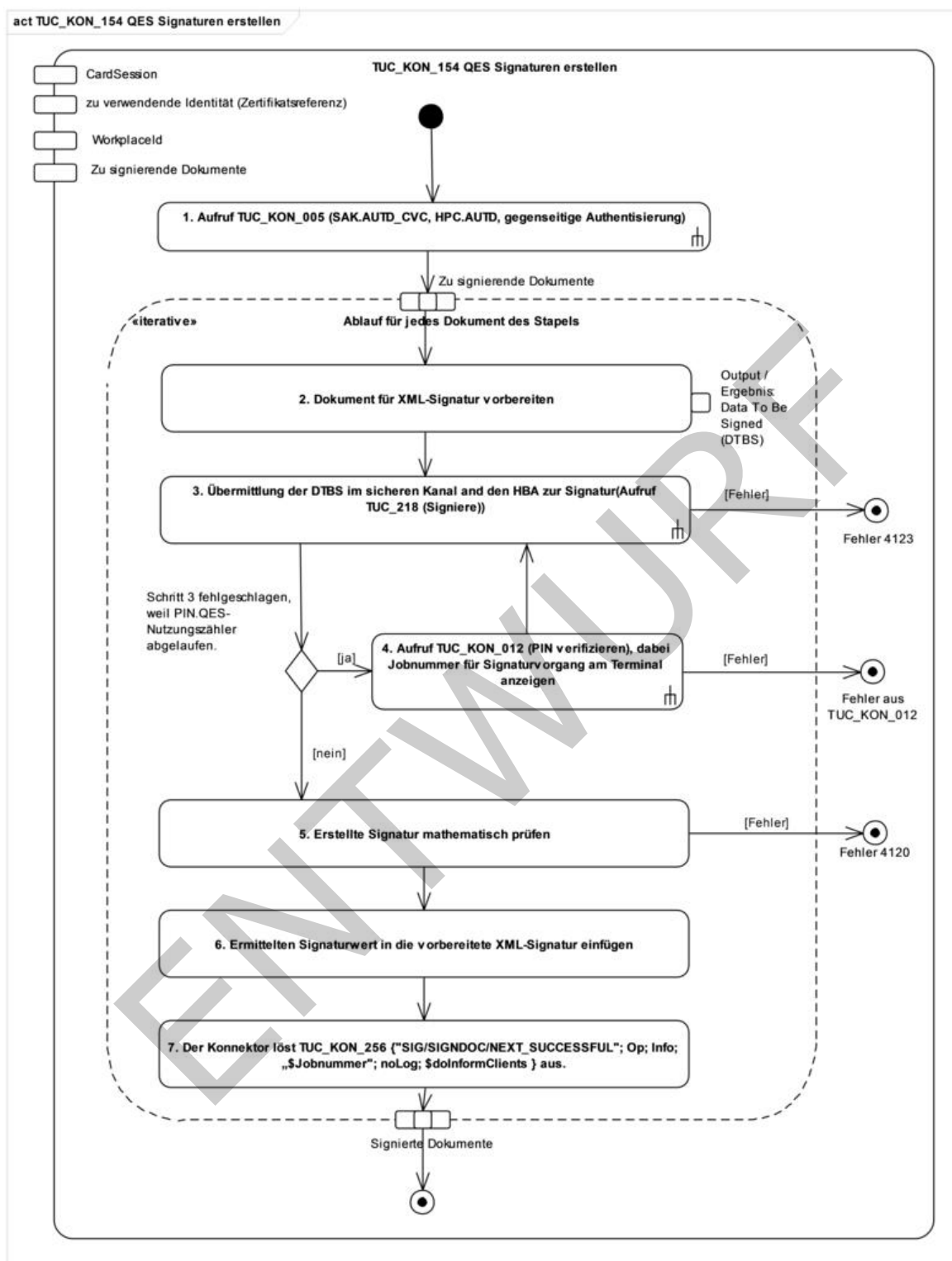


Abbildung 18: PIC_KON_113 Aktivitätsdiagramm zu „QES Signaturen erstellen“

Tabelle 200: TAB_KON_126 Fehlercodes TUC_KON_154 „QES Signaturen erstellen“

Fehlercode	ErrorType	Severity	Fehlertext
------------	-----------	----------	------------

Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:

4120	Security	Error	Kartenfehler
4123	Security	Error	Fehler bei Signaturerstellung

4297 [\leq]

4298 4.1.8.3.6 TUC_KON_168 „Einzelsignatur QES erstellen“

4299 TIP1-A_4652 - TUC_KON_168 „Einzelsignatur QES erstellen“

4300 Der Konnektor MUSS den technischen Use Case TUC_KON_168 „Einzelsignatur QES erstellen“ umsetzen.

4302

4303 **Tabelle 201: TAB_KON_293 - TUC_KON_168 „Einzelsignatur QES erstellen“**

Element	Beschreibung
Name	TUC_KON_168 "Einzelsignatur QES erstellen"
Beschreibung	Es wird ein Dokument technisch mit einer Signatur versehen. Im Gegensatz zum TUC_KON_154 „QES Signaturen erstellen“ wird hier nur eine einzelne Signatur ohne vorhergehendes C2C erstellt. Die Übertragung der DTBS erfolgt ohne Secure Messaging.
Auslöser	TUC_KON_150 Dokumente QES signieren
Vorbedingungen	Die Ressourcen Signaturkarte und Kartenterminal sind für den Vorgang reserviert. DF.QES ist selektiert.
Eingangsdaten	<ul style="list-style-type: none"> • zu signierendes Dokument • CardSession (HBAX) • zu verwendende Identität (Zertifikatsreferenz) • crypt: [SIG_CRYPT_QES] - <i>optional</i>; <i>default</i> und Wertebereich: siehe TAB_KON_862 Dieser Parameter steuert, ob RSA-basierte oder ECC-basierte Signaturen erzeugt werden. • WorkplaceId
Komponenten	Konnektor, Kartenterminal, Signaturkarte (HBAX)
Ausgangsdaten	<ul style="list-style-type: none"> • Signiertes Dokument
Standardablauf	<ol style="list-style-type: none"> 1. Das zu signierende Dokument wird, soweit noch nicht erfolgt, für die Signatur vorbereitet. Ein Ergebnis dieser Vorbereitung sind die DTBS: der Hash-Wert (Digest des SignedInfo-Elementes), der zur Signatur an die Karte gesendet werden soll. 2. Für das zu signierende Dokument werden die DTBS zur Signatur an den HBAX übermittelt (Aufruf TUC_KON_218 „Signiere“). Dabei werden der Schlüssel und der Algorithmusidentifizierer über die Tabelle TAB_KON_900

	bestimmt. Jeder Fehler führt zum Abbruch des Signaturvorgangs 3. Die erstellte Signatur wird mathematisch geprüft. Der ermittelte Signaturwert wird in den zuvor gemäß des entsprechenden Signaturformates vorbereiteten Signaturprototypen eingefügt.
Varianten/ Alternativen	keine
Fehlerfälle	Das Verhalten des TUCs bei einem Fehlerfall, einem Timeout der PIN-Eingabe oder beim Abbruch durch den Benutzer ist in Tabelle TAB_KON_192 Verhalten des Konnektors beim Abbruch einer Stapelsignatur beschrieben. (→3) Fehler in mathematischer Prüfung der Signatur: Abbruch mit 4120
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

4304 **Tabelle 202: TAB_KON_590 Fehlercodes TUC_KON_168 „Einzelsignatur QES erstellen“**

Fehlercode	ErrorType	Severit y	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten.			
4120	Security	Error	Kartenfehler

4305
4306 **[<=]**

4307 4.1.8.3.7 TUC_KON_158 "Komfortsignaturen erstellen"

4308 Der TUC_KON_158 führt die Komfortsignatur für ein Dokument oder mehrere Dokumente
4309 eines Stapels aus. Da die Komfortsignatur auf der Zielkarte passende CVC voraussetzt,
4310 die auf den HBA-Vorläuferkarten nicht vorhanden sind, unterstützt dieser TUC nur den
4311 HBA.

4312 A_19102 - TUC_KON_158 „Komfortsignaturen erstellen“

4313 Der Konnektor MUSS den technischen Use Case TUC_KON_158 „Komfortsignaturen
4314 erstellen“ umsetzen.

4315

4316 **Tabelle 203: TAB_KON_870 – TUC_KON_158 „Komfortsignaturen erstellen“**

Element	Beschreibung
Name	TUC_KON_158 „Komfortsignaturen erstellen“
Beschreibung	Die Data To Be Signed (DTBS) werden erzeugt, an die Signaturkarte gesendet und dort signiert. Die Übertragung der DTBS erfolgt mit Secure Messaging. Die Abarbeitung der Signatur erfolgt im SE#2.

Auslöser	TUC_KON_170 „Dokumente mit Komfort signieren“
Vorbedingungen	Die Ressource Signaturkarte ist für den Vorgang reserviert. DF.QES ist selektiert. PIN.QES ist initial verifiziert
Eingangsdaten	<ul style="list-style-type: none"> • Zu signierendes Dokument bzw. zu signierende Dokumente • cardSession (nur HBA erlaubt) • zu verwendende Identität (Zertifikatsreferenz) • crypt [SIG_CRYPT_QES] - <i>optional</i>; <i>default und Wertebereich</i>: siehe TAB_KON_862 (Dieser Parameter steuert, ob RSA-basierte oder ECC-basierte Signaturen erzeugt werden.) • WorkplaceId
Komponenten	Konnektor, Kartenterminal, Signaturkarte (HBA)
Ausgangsdaten	<ul style="list-style-type: none"> • Signierte Dokumente
Standardablauf	<ol style="list-style-type: none"> 1. Wenn noch nicht erfolgt, wird basierend auf SAK.AUTD_CVC und HPC.AUTD_SUK_CVC und den zugehörigen privaten Schlüsseln ein sicherer Kanal zwischen der gSMC-K des Konnektors und dem HBA aufgebaut mittels Aufruf TUC_KON_005 „Card-to-Card authentisieren“ { sourceCardSession = gSMC-K; targetCardSession = CardSession; authMode = „gegenseitig+TC“} Die folgenden Schritte werden für jedes Dokument des Stapels durchgeführt. 2. Das zu signierende Dokument wird, soweit noch nicht erfolgt, für die Signatur gemäß des entsprechenden Formats vorbereitet. Ein Ergebnis dieser Vorbereitung sind die Data To Be Signed (DTBS): der Hash-Wert (Digest des SignedInfo-Elementes), der zur Signatur an die Karte gesendet werden soll. 3. Es wird geprüft, ob der Komfortsignatur-Zähler der cardSession den Wert SAK_COMFORT_SIGNATURE_MAX überschritten hat . 4. Es wird geprüft, ob der Komfortsignatur-Timer der cardSession (SAK_COMFORT_SIGNATURE_TIMER) abgelaufen ist. 5. Für das zu signierende Dokument werden die DTBS zur Signatur im sicheren Kanal an den HBA übermittelt (Aufruf TUC_KON_218 „Signiere“). Dabei werden der Schlüssel und der Algorithmusidentifizierer über die Tabelle TAB_KON_900 bestimmt.

	<p>6. Der Komfortsignatur-Zähler der cardSession wird um 1 erhöht.</p> <p>7. Die erstellte Signatur wird mathematisch geprüft.</p> <p>8. Der ermittelte Signaturwert wird in den zuvor vorbereiteten Signaturprototypen eingefügt.</p> <p>9. Der Konnektor löst TUC_KON_256 {"SIG/SIGND/DOC/NEXT_SUCCESSFUL"; Op; Info; „\$Jobnummer“; noLog; \$doInformClients } aus.</p>
Varianten/ Alternativen	Keine
Fehlerfälle	<p>In den Fehlerfällen, die zum Abbruch des Komfortsignaturmodus mit Fehlercode 4271 führen, wird vor dem Abbruch TUC_KON_172 für das cardHandle des HBA ausgeführt.</p> <p>(->3) Der Komfortsignatur-Zähler der cardSession hat den Maximalwert überschritten: Fehlercode 4271</p> <p>(->4) Der Komfortsignatur-Timer der cardSession ist abgelaufen: Fehlercode 4271</p> <p>(->5) Der PIN.QES-Nutzungszähler der Karte ist abgelaufen (erkennbar z. B. daran, dass die Karte einen Autorisierungsfehler zurückmeldet): Fehlercode 4271</p> <p>(->5) Fehler im Signaturvorgang führen zum Abbruch des gesamten Signaturvorgangs: Fehlercode 4123</p> <p>(->7) Fehler in mathematischer Prüfung der Signatur führen zum Abbruch des Signaturvorgangs: Fehlercode 4120</p> <p>Das weitere Verhalten des TUCs bei einem Fehlerfall oder beim Abbruch durch den Benutzer ist in TAB_KON_192, Verhalten des Konnektors beim Abbruch einer Stapelsignatur, beschrieben.</p>
Sicherheitsanforderungen	<p>Zum Aufbau des sicheren Kanals bzw. zur Aushandlung des symmetrischen Schlüssels DARF DF.QES NICHT verlassen werden. Benötigte CVCs des HBA MÜSSEN also bereits vor dem Signaturvorgang eingelesen und gecached werden. Dies KANN bereits beim Stecken des HBA geschehen.</p> <p>Komfortsignaturen MÜSSEN im SE#2 abgearbeitet werden.</p> <p>Die in [gemSpec_Krypt] angegebenen Festlegungen der zu unterstützenden Algorithmen MÜSSEN berücksichtigt werden.</p>

4317 **Tabelle 204: TAB_KON_873 Fehlercodes TUC_KON_158 „Komfortsignaturen erstellen“**

Fehlercode	ErrorType	Severity	Fehlertext
------------	-----------	----------	------------

Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:

4120	Security	Error	Kartenfehler
4123	Security	Error	Fehler bei Signaturerstellung
4271	Technical	Error	Komfortsignaturmodus abgebrochen

[<=]

4.1.8.4 Interne TUCs, auch durch Fachmodule nutzbar

[A_20478 - Zusätzliche Dokumentformate für nonQES-Signatur](#)
Der Konnektor KANN für die nonQES-Signaturerstellung an der Schnittstelle zu Fachmodulen zusätzliche Dokumentformate unterstützen. [<=]
Die in der obigen Anforderung benannten Signaturen von Dokumentenformaten umfassen beispielsweise die Signatur von Token nach SAML2 für das Fachmodul ePA entsprechend [gemSpec FM ePA#A_14927].

4.1.8.4.1 TUC_KON_160 „Dokumente nonQES signieren“

TIP1-A_4653 - TUC_KON_160 „Dokumente nonQES signieren“

Der Konnektor MUSS den technischen Use Case TUC_KON_160 „Dokumente nonQES signieren“ umsetzen.

Tabelle 205: TAB_KON_753 – TUC_KON_160 „Dokumente nonQES signieren“

Element	Beschreibung
Name	TUC_KON_160 „Dokumente nonQES signieren“
Beschreibung	Im Rahmen von Fachanwendungen werden ein oder mehrere Dokumente mit einer nicht-qualifizierten elektronischen Signatur (nonQES) versehen. Es werden die nonQES_DocFormate unterstützt.
Auslöser	Aufruf durch ein Clientsystem (Operation SignDocument) oder ein Fachmodul.
Vorbedingungen	Die Signaturkarte muss gesteckt sein.
Eingangsdaten	<ul style="list-style-type: none"> cardSession (Kartensitzung; zulässig sind SM-B, oder bei Aufruf durch Fachmodul auch zusätzlich eGK) signRequests (Liste von Signaturaufträgen.) Jeder Signaturauftrag (SignRequest) kapselt: <ul style="list-style-type: none"> documentsToBeSigned (Zu signierendes Dokument bzw. zu signierende

	<p>Dokumente); darin u.a. documentFormat (Formatangabe für das zu signierende Dokument)</p> <ul style="list-style-type: none"> • optionalInputs (weitere optionale Eingabeparameter zur Steuerung der Details bei der zu erstellenden Signatur, siehe Operation SignDocument, Parameter dss:OptionalInputs); darin u.a. signatureType (URI für den Signatortyp XML-, CMS-, S/MIME-, PDF-Signatur) • includeRevocationInfo: – <i>optional; default: true</i> (Dieser optionale Parameter steuert die Einbettung von OCSP-Antworten in die Signatur: nur wirksam bei der Prüfung von enthaltenen Parallelsignaturen, wenn eine Gegensignatur erstellt werden soll. Die OCSP-Antworten werden in die jeweils geprüfte Parallelsignatur eingebettet.) • workplaceId (Identifikator des Arbeitsplatzes)
Komponenten	Konnektor, Kartenterminal, Signaturkarte bzw. HSM-B
Ausgangsdaten	<ul style="list-style-type: none"> • signedDocuments (Liste der signierten Dokumente)
Standardablauf	<p>Der Konnektor KANN die Schritte 1 bis 4 in einer beliebigen Reihenfolge durchführen.</p> <ol style="list-style-type: none"> 1. Der signatureType und die Signaturvariante werden für jedes Dokument der Liste entsprechend SignatureType und SignatureVariant festgelegt. Wenn signatureType oder SignatureVariant nicht übergeben wurden (als Element von optionalInputs), wird das dem dokumentformat entsprechende Default-Verfahren gewählt (siehe TAB_KON_583 – Default-Signaturverfahren). 2. Für alle Dokumente des Stapels wird die Zulässigkeit des Kartentyps geprüft. Das für die Signatur zu nutzende Zertifikat wird anhand des Kartentyps implizit ausgewählt. 3. Es werden die Voraussetzungen für die Signatur geprüft. Dies erfolgt durch Aufruf von TUC_KON_165 „Signaturvoraussetzungen für nonQES prüfen“. 4. Zum Vorbereiten der Dokumente für die Signatur wird TUC_KON_155 „Dokumente zur Signatur vorbereiten“ mit ocsResponses aufgerufen. 5. Die Signaturen werden durch den Aufruf von TUC_KON_166 erstellt.

	6. Die signierten Dokumente werden an den Aufrufer zurückgegeben.
Varianten/ Alternativen	<p><u>Im Fall signatureType=S/MIME-Signatur</u> wird der Standardablauf des CMS Signaturverfahrens durch einen vorgelagerten S/MIME-Vorbereitungsschritt und einen nachgelagerten S/MIME-Nachbereitungsschritt ergänzt. Das S/MIME-Verfahren MUSS konform [S/MIME] und SOLL konform [COMMON_PKI], Part 3, erfolgen.</p> <p>Der S/MIME-Vorbereitungsschritt bereitet das übergebene MIME-Dokument gemäß [S/MIME], Kapitel 3.1, auf die nachfolgende CMS-Signatur durch eine Kanonisierung für Text [S/MIME], Kapitel 3.1.1, vor. Eine weitere Kanonisierung oder eine Anpassung des Transfer Encodings [S/MIME], Kapitel 3.1.2, erfolgt nicht.</p> <p>Im S/MIME-Nachbereitungsschritt wird das im Standardablauf erzeugte CMS-Objekt in eine MIME-Nachricht vom Typ „application/pkcs7-mime“ eingebettet.</p> <p>Sämtliche Header-Felder der Nachricht MÜSSEN in die Header-Felder der S/MIME-Nachricht übernommen werden.</p> <p>"MIME-Version: 1.0" MUSS definiert sein.</p> <p>Das Feld "Content-Type:" ist als "application/pkcs7-mime" zu definieren. Die weiteren Attribute dieses Feldes sind:</p> <ul style="list-style-type: none"> • "smime-type=signed-data;" • "name=\$dateiname", wobei \$dateiname auf ".p7m" endet. <p>Die Codierung des signierten Inhalts der Nachricht MUSS in "base64" erfolgen. Entsprechend ist das zugehörige Header-Feld zu füllen: "Content-Transfer-Encoding: base64".</p> <p>Das Feld "Content-Disposition" definiert den Inhalt der Nachricht als Dateianhang: "Content-Disposition: attachment; filename=\$dateiname"</p>
Fehlerfälle	<p>Fehler in den folgenden Schritten des Standardablaufs führen zum Abbruch mit den ausgewiesenen Fehlercodes:</p> <p>(→2) Ungültige Angabe des Signaturverfahrens: Fehlercode 4111</p> <p>Übergabe eines für die nonQES nicht unterstützten Dokumentformats: Fehlercode 4110</p> <p>(→3) Kartentyp nicht zulässig für Signatur: Fehlercode 4126</p>
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

4333 **Tabelle 206: TAB_KON_127 Fehlercodes TUC_KON_160 „Dokumente nonQES signieren“**

Fehlercode	ErrorType	Severity	Fehlertext
------------	-----------	----------	------------

Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4110	Technical	Error	ungültiges Dokumentformat (%Format%) Der Parameter Format enthält das übergebene Dokumentformat.
4111	Technical	Error	ungültiger Signatortyp oder Signaturvariante
4126	Security	Error	Kartentyp nicht zulässig für Signatur

4334
4335 [\leq]

4336 TIP1-A_4653-02 - ab PTV4: TUC_KON_160 „Dokumente nonQES signieren“
4337 Der Konnektor MUSS den technischen Use Case TUC_KON_160 „Dokumente nonQES
4338 signieren“ umsetzen.
4339

4340 **Tabelle 207: TAB_KON_753 – TUC_KON_160 „Dokumente nonQES signieren“**

Element	Beschreibung
Name	TUC_KON_160 „Dokumente nonQES signieren“
Beschreibung	Im Rahmen von Fachanwendungen werden ein oder mehrere Dokumente mit einer nicht-qualifizierten elektronischen Signatur (nonQES) versehen. Es werden die nonQES_DocFormate unterstützt.
Auslöser	Aufruf durch ein Clientsystem (Operation SignDocument) oder ein Fachmodul.
Vorbedingungen	Die Signaturkarte muss gesteckt sein.
Eingangsdaten	<ul style="list-style-type: none"> cardSession (Kartensitzung; zulässig sind SM-B, oder bei Aufruf durch Fachmodul auch zusätzlich eGK) crypt [SIG_CRYPT_nonQES] - <i>optional</i>; default und Wertebereich: siehe TAB_KON_863 Dieser Parameter steuert, ob RSA-basierte oder ECC-basierte Signaturen erzeugt werden. signRequests (Liste von Signaturaufträgen. Jeder Signaturauftrag (SignRequest) kapselt: <ul style="list-style-type: none"> documentsToBeSigned (Zu signierendes Dokument bzw. zu signierende Dokumente); darin u.a. documentFormat (Formatangabe für das zu signierende Dokument)

	<ul style="list-style-type: none"> • optionalInputs (weitere optionale Eingabeparameter zur Steuerung der Details bei der zu erstellenden Signatur, siehe Operation SignDocument, Parameter dss:OptionalInputs); darin u.a. signatureType (URI für den Signatortyp XML-, CMS-, S/MIME-, PDF-Signatur) • includeRevocationInfo: – <i>optional; default: true</i> (Dieser optionale Parameter steuert die Einbettung von OCSP-Antworten in die Signatur: nur wirksam bei der Prüfung von enthaltenen Parallelsignaturen, wenn eine Gegensignatur erstellt werden soll. Die OCSP-Antworten werden in die jeweils geprüfte Parallelsignatur eingebettet.) • workplaceId (Identifikator des Arbeitsplatzes)
Komponenten	Konnektor, Kartenterminal, Signaturkarte bzw. HSM-B
Ausgangsdaten	<ul style="list-style-type: none"> • signedDocuments (Liste der signierten Dokumente)
Standardablauf	<p>Der Konnektor KANN die Schritte 1 bis 4 in einer beliebigen Reihenfolge durchführen.</p> <ol style="list-style-type: none"> 1. Der signatureType und die Signaturvariante werden für jedes Dokument der Liste entsprechend SignatureType und SignatureVariant festgelegt. Wenn signatureType oder SignatureVariant nicht übergeben wurden (als Element von optionalInputs), wird das dem dokumentformat entsprechende Default-Verfahren gewählt (siehe TAB_KON_583 – Default-Signaturverfahren). 2. Für alle Dokumente des Stapels wird die Zulässigkeit des Kartentyps geprüft. Das für die Signatur zu nutzende Zertifikat wird anhand des Kartentyps und des Parameters crypt ausgewählt. 3. Es werden die Voraussetzungen für die Signatur geprüft. Dies erfolgt durch Aufruf von TUC_KON_165 „Signaturvoraussetzungen für nonQES prüfen“. 4. Zum Vorbereiten der Dokumente für die Signatur wird TUC_KON_155 „Dokumente zur Signatur vorbereiten“ mit ocsResponses aufgerufen. 5. Die Signaturen werden durch den Aufruf von TUC_KON_166 erstellt. 6. Die signierten Dokumente werden an den Aufrufer zurückgegeben.

Varianten/ Alternativen	<p>Im Fall signatureType=S/MIME-Signatur wird der Standardablauf des CMS Signaturverfahrens durch einen vorgelagerten S/MIME-Vorbereitungsschritt und einen nachgelagerten S/MIME-Nachbereitungsschritt ergänzt. Das S/MIME-Verfahren MUSS konform [S/MIME] und SOLL konform [COMMON_PKI], Part 3, erfolgen.</p> <p>Der S/MIME-Vorbereitungsschritt bereitet das übergebene MIME-Dokument gemäß [S/MIME], Kapitel 3.1, auf die nachfolgende CMS-Signatur durch eine Kanonisierung für Text [S/MIME], Kapitel 3.1.1, vor. Eine weitere Kanonisierung oder eine Anpassung des Transfer Encodings [S/MIME], Kapitel 3.1.2, erfolgt nicht.</p> <p>Im S/MIME-Nachbereitungsschritt wird das im Standardablauf erzeugte CMS-Objekt in eine MIME-Nachricht vom Typ „application/pkcs7-mime“ eingebettet.</p> <p>Sämtliche Header-Felder der Nachricht MÜSSEN in die Header-Felder der S/MIME-Nachricht übernommen werden.</p> <p>"MIME-Version: 1.0" MUSS definiert sein.</p> <p>Das Feld "Content-Type:" ist als "application/pkcs7-mime" zu definieren. Die weiteren Attribute dieses Feldes sind:</p> <ul style="list-style-type: none"> • "smime-type=signed-data;" • "name=\$dateiname", wobei \$dateiname auf ".p7m" endet. <p>Die Codierung des signierten Inhalts der Nachricht MUSS in "base64" erfolgen. Entsprechend ist das zugehörige Header-Feld zu füllen: "Content-Transfer-Encoding: base64".</p> <p>Das Feld "Content-Disposition" definiert den Inhalt der Nachricht als Dateianhang: "Content-Disposition: attachment; filename=\$dateiname"</p>
Fehlerfälle	<p>Fehler in den folgenden Schritten des Standardablaufs führen zum Abbruch mit den ausgewiesenen Fehlercodes:</p> <p>(→2) Ungültige Angabe des Signaturverfahrens: Fehlercode 4111</p> <p>Übergabe eines für die nonQES nicht unterstützten Dokumentformats: Fehlercode 4110</p> <p>(→3) Kartentyp nicht zulässig für Signatur: Fehlercode 4126</p>
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

4341 **Tabelle 208: TAB_KON_127 Fehlercodes TUC_KON_160 „Dokumente nonQES signieren“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			

4110	Technical	Error	ungültiges Dokumentformat (%Format%) Der Parameter Format enthält das übergebene Dokumentformat.
4111	Technical	Error	ungültiger Signaturtyp oder Signaturvariante
4126	Security	Error	Kartentyp nicht zulässig für Signatur

4342

4343

Die zulässigen Zertifikate und Schlüssel sind in TAB_KON_900 aufgelistet.[<=]

4344

4345 4.1.8.4.2 TUC_KON_161 „nonQES Dokumentsignatur prüfen“

4346 TIP1-A_4654-03 - TUC_KON_161 „nonQES Dokumentsignatur prüfen“

4347 Der Konnektor MUSS den technischen Use Case TUC_KON_161 „nonQES

4348 Dokumentsignatur prüfen“ umsetzen.

4349

4350 **Tabelle 209: TAB_KON_121 - TUC_KON_161 „nonQES Dokumentsignatur prüfen“**

Element	Beschreibung
Name	TUC_KON_161 „nonQES Dokumentsignatur prüfen“
Beschreibung	Es wird die nicht-qualifizierte elektronische Signatur (nonQES) eines Dokuments geprüft. Dabei werden die Signaturverfahren laut Tabelle TAB_KON_582 – Signaturverfahren unterstützt. Sind mehrere Signaturen vorhanden, so werden alle geprüft. Auch Parallel- und Gegensignaturen MÜSSEN unterstützt werden.
Auslöser	Aufruf durch ein Clientsystem (Operation VerifyDocument) oder ein Fachmodul
Vorbedingungen	keine
Eingangsdaten	<ul style="list-style-type: none"> signedDocument (Signiertes Document vom Typ nonQES_DocFormate) signature – <i>optional/falls detached Signatur</i> (Signatur. Es werden Parallel- und Gegensignaturen unterstützt.) optionalInputs (optionale Eingabeparameter, siehe Operation VerifyDocument, Parameter SIG:OptionalInputs) certificate – <i>optional/verpflichtend, wenn das Zertifikat nicht im signierten Dokument enthalten ist</i> (X.509-Zertifikat, gegen das die Signatur geprüft werden soll) <p>ocspGracePeriod (OCSP-Grace Period: maximal zulässiger Zeitraum, den die letzte OCSP-Antwort aus dem Cache bezüglich des Referenzzeitpunkts zurückliegen darf)</p>

	<ul style="list-style-type: none"> xmlSchemas – <i>optional/nur für XML-Dokumente</i> (XMLSchema und ggf. weitere vom Hauptschema benutzte Schemata) includeRevocationInfo: – <i>optional; Default = false</i> (Dieser optionale Parameter steuert die Einbettung von OSCP Antworten in die Signatur)
Komponenten	Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> verificationResult [VerificationResult] (Ergebnis der Signaturprüfung) optionalOutput – <i>optional</i> (weitere Ausgabedaten gemäß SIG:OptionalOutput)
Standardablauf	<ol style="list-style-type: none"> „DocumentValidation“: Falls die Signatur im Dokument eingebettet ist, wird das signierte Dokument validiert durch Aufruf TUC_KON_080 „Dokument validieren“ { CheckDisplayability=false; ... } Treten dabei Fehler bei Validierung der Typkonformität auf, wird die Prüfung mit einem Fehler abgebrochen. „CoreValidation“: Es erfolgt die mathematische Prüfung der Signatur bestehend aus der Prüfung der Hash-Kette bis zum signierten Hashwert und der Prüfung der kryptographischen Signatur unter Verwendung des öffentlichen Schlüssels, des Signaturwertes und des signierten Hashwertes. XML-Signatur: Die Core Validation erfolgt entsprechend [XMLDSig] Kapitel 3.2 Core Validation. CMS-Signatur: Die Core Validation erfolgt entsprechend Cryptographic Message Syntax (CMS) Kapitel 5.6 Signature Verification Process [RFC5652]. PDF-Signatur: Die Core Validation erfolgt entsprechend [PADES-3] Kapitel 4.6 Signature Validation aus PADES-BES Part 3. Auch wenn die Validierung fehlschlägt, werden die folgenden Prüfschritte durchgeführt, so dass ein vollständiges Prüfprotokoll erstellt werden kann. „CheckSignatureCertificate“: Teil 1: Signaturzertifikat ermitteln XML-Signatur: Das Signaturzertifikat ist im XMLDSig Element <code>ds:KeyInfo/ds:X509Data</code> gespeichert [XMLDSig] oder wird als Eingangsparameter übergeben.

	<p>CMS-Signatur: Das Signaturzertifikat für CADES ist im Feld <code>certificates</code> im <code>SignedData</code> Container gespeichert [CADES] oder wird als Eingangsparameter übergeben.</p> <p>PDF-Signatur: Das PDF Signaturzertifikat für PAdES ist im Feld <code>SignedData.certificates</code> entsprechend Kapitel 6.1.1 „Placements of the signing certificate“ [PAdES Baseline Profile] gespeichert oder wird als Eingangsparameter übergeben.</p> <p>Teil 2: Signaturzeitpunkt bestimmen Der Signaturzeitpunkt <code>Ermittelter_Signaturzeitpunkt_Eingebettet</code> wird wie folgt selektiert:</p> <p>XML-Signatur: Das XML element <code>SigningTime</code> spezifiziert den Signaturzeitpunkt entsprechend Kapitel 7.2.1 XAdES [XAdES].</p> <p>CMS-Signatur: Das Attribut <code>SigningTime</code> spezifiziert den Signaturzeitpunkt entsprechend Kapitel 11.3 CMS [CMS].</p> <p>PDF-Signatur: Der Signaturzeitpunkt kann dem M Eintrag des Signature Dictionary entnommen werden [PAdES Baseline Profile] Kapitel 6.2.1 Signing time.</p> <p>Der Signaturzeitpunkt <code>Benutzerdefinierter_Zeitpunkt</code> liegt gegebenenfalls als Aufrufparameter vor. Der Signaturzeitpunkt <code>Ermittelter_Signaturzeitpunkt_System</code> wird ermittelt.</p> <p>Teil 3: Signaturzertifikatsprüfung: Bei der folgenden Signaturzertifikatsprüfung sind die Signaturzeitpunkte gemäß [TIP1-A_5545] zu berücksichtigen. Die Signaturzertifikatsprüfung erfolgt durch Aufruf von <code>TUC_KON_037 „Zertifikat prüfen“</code>, und zwar: Wenn es sich um das X.509-Zertifikat einer eGK handelt (<code>PolicyList = oid_egk_aut</code> bzw. <code>oid_egk_autn</code>), dann: <code>TUC_KON_037 „Zertifikat prüfen“ {</code></p>
--	---

	<pre> certificate; qualifiedCheck = not_required; baseTime = Signaturzeitpunkt; offlineAllowNoCheck = true; policyList = [oid_egk_aut oid_egk_autn]; intendedKeyUsage= intendedKeyUsage(C.CH.AUT C.CH.AUTN); intendedExtendedKeyUsage = id-kp-clientAuth; ocspResponses = OCSP-Response; gracePeriod = ocspGracePeriod; validationMode = OCSP; getOCSPResponses = includeRevocationInfo } Wenn es ein X.509-Zertifikat der SM-B ist (PolicyList = oid_smc_b_osig), dann: TUC_KON_037 „Zertifikat prüfen“ { certificate; qualifiedCheck = not_required; baseTime = Signaturzeitpunkt; offlineAllowNoCheck = true; policyList = oid_smc_b_osig; intendedKeyUsage = intendedKeyUsage(C.HCI.OSIG); ocspResponses = OCSP-Response; gracePeriod = ocspGracePeriod; validationMode = OCSP ; getOCSPResponses = includeRevocationInfo } Sind OCSP-Responses in der Signatur eingebettet, ist die jüngste OCSP-Response, die für die Zertifikatsprüfung notwendig ist, beim Aufruf von TUC_KON_037 zu übergeben. Sofern der Aufruf von TUC_KON_037 ocspResponsesRenewed zurückgibt, wird die Liste der OCSP-Responses in die Signatur eingebettet. Auch wenn die Zertifikatsprüfung fehlschlägt, werden die folgenden Prüfungen durchgeführt. </pre> <p>4. “CheckPolicyConstraints”</p> <p>In diesem Schritt wird das signierte Dokument entsprechend der Profilierung der Signaturformate (siehe Anhang B.2) geprüft. Es sind die Vorgaben für die Prüfung von Signaturen aus den Standards für AdES [XAdES], [XAdES Baseline], [CAAdES], [CAAdES Baseline], [PAdES-3] und [PAdES Baseline] umzusetzen. Dabei sind die Vorgaben aus Tabelle TAB_KON_779 „Profilierung der Signaturformate“ und Tabelle TAB_KON_778 „Einsatzbereich der Signaturvarianten“ zu erfüllen. Auch wenn nicht alle Anforderungen an das Format des signierten Dokuments erfüllt werden, wird die Prüfung</p>
--	---

	<p>mit den folgenden Schritten fortgesetzt, um ein vollständiges Prüfungsprotokoll zu erhalten.</p> <p>5. Das Prüfergebnis (verificationResult, optionalOutput wird an den Aufrufer zurückgegeben (siehe TAB_KON_754 Übersicht Status für Prüfung einer Dokumentensignatur).</p>
Varianten/ Alternativen	<p>Im Fall, dass die Online-Prüfung des Sperrzustands des Signaturzertifikats nicht möglich ist und eine möglicherweise gecachte OCSP-Response nicht vorhanden ist oder nicht mehr verwendet werden darf, wird das Prüfergebnis mit der entsprechenden Warnung zurückgegeben.</p> <p>Im Fall einer PKCS#1-Signatur ist das verwendete Signaturverfahren, RSASSA-PSS bzw. RSASSA-PKCS1-v1_5, aus der Signatur zu bestimmen.</p>
Fehlerfälle	<p>Das Verhalten des TUCs bei einem Fehlerfall ist in TAB_KON_124 Fehlercodes TUC_KON_161 „nonQES Dokumentensignatur prüfen“ beschrieben.</p> <p>(->1) keine Signatur in signedDocument und signature vorhanden: 4253</p> <p>(->2 „CoreValidation“)</p> <p>Interner Fehler: 4001, Signatur des Dokument ungültig: 4115.</p> <p>Signatur umfasst nicht das gesamte Dokument: 4262.</p> <p>(->3 „CheckSignatureCertificate“)</p> <p>Interner Fehler: 4001, Signaturzertifikat ermitteln fehlgeschlagen: 4206.</p> <p>(->4 „CheckPolicyConstraints“)</p> <p>Interner Fehler: 4001, Dokument nicht konform zu Regeln für nonQES: 4112.</p>
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

Tabelle 210: TAB_KON_124 Fehlercodes TUC_KON_161 „nonQES Dokumentensignatur prüfen“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weiteren Fehlercodes auftreten.			
4001	Technical	Error	Interner Fehler
4206	Technical	Error	Signaturzertifikat ermitteln ist fehlgeschlagen
4112	Technical	Error	Dokument nicht konform zu Regeln für nonQES

4115	Security	Error	Signatur des Dokuments ungültig. Der SignatureValue des Dokuments ist falsch oder für mindestens eine Reference ist der DigestValue falsch.
4253	Technical	Error	Keine Signatur im Aufruf
4262	Technical	Error	Signatur umfasst nicht das gesamte Dokument
4264	Technical	Warning	Ein oder mehrere Zertifikate ignoriert

4353 Das Gesamtergebnis (VerificationResult) für die Prüfung einer Dokumentensignatur fasst
 4354 die Ergebnisse aller Prüfungsschritte in einem einzelnen Statuswert zusammen.
 4355

4356 **Tabelle 211: TAB_KON_754 Übersicht Status für Prüfung einer Dokumentensignatur**

VerificationResult für gesamtes Dokument (VerificationResult/HighLevelResult)	
Wert	Bedeutung
VALID	Wenn VerificationResult für alle Signaturen zum Dokument VALID
INVALID	Wenn VerificationResult für eine Signatur zum Dokument INVALID
INCONCLUSIVE	in allen anderen Fällen
VerificationResult pro Signatur (VerificationReport/IndividualReport/Result)	
Wert	Bedeutung mögliche Ausprägungen im VerificationReport
VALID	Die Signatur wurde gemäß den Regeln für die nonQES geprüft und für gültig befunden.
	ResultMajor = urn:oasis:names:tc:dss:1.0:resultmajor:Success ResultMinor = urn:oasis:names:tc:dss:1.0:resultminor:valid:signature:OnAllDocuments
	ResultMajor = urn:oasis:names:tc:dss:1.0:resultmajor:Success ResultMinor = urn:oasis:names:tc:dss:1.0:resultminor:valid:signature:HasManifestResults
INVALID	Die Signatur ist ungültig oder aufgrund eines Fehlers konnte die Signaturprüfung nicht durchgeführt werden.

	ResultMajor = urn:oasis:names:tc:dss:1.0:resultmajor:Success ResultMinor = urn:oasis:names:tc:dss:1.0:resultminor:invalid:IncorrectSignature
	ResultMajor = urn:oasis:names:tc:dss:1.0:resultmajor:Success ResultMinor = urn:oasis:names:tc:dss:1.0:resultminor:valid:signature:InvalidSignatureTimestamp
	ResultMajor = urn:oasis:names:tc:dss:1.0:resultmajor:RequesterError
	ResultMajor = urn:oasis:names:tc:dss:1.0:resultmajor:ResponderError
	ResultMajor = urn:oasis:names:tc:dss:1.0:resultmajor:InsufficientInformation ResultMinor = urn:oasis:names:tc:dss:1.0:resultminor:invalid:IncorrectSignature
	ResultMajor = urn:oasis:names:tc:dss:1.0:resultmajor:InsufficientInformation ResultMinor = urn:oasis:names:tc:dss:1.0:resultminor:CertificateChainNotComplete
INCONCLUSIVE	Die Signatur wurde gemäß den Regeln für die nonQES geprüft. Allerdings konnten eine oder mehrere Prüfungen nicht vollständig durchgeführt werden. Einzelheiten finden sich in Result-Detail. Die Prüfungen, die durchgeführt werden konnten, waren erfolgreich.
	ResultMajor = urn:oasis:names:tc:dss:1.0:resultmajor:InsufficientInformation ResultMinor = urn:oasis:names:tc:dss:1.0:resultminor:OcspsNotAvailable Hinweis: Das Erreichen dieses Zustandes hängt davon ab, ob eine OCSP-Abfrage nicht durchgeführt werden konnte, unabhängig davon, ob die Ursache dafür die Offlineschaltung des Konnektors (MGM_LU_ONLINE = Disabled) oder die Nichterreichbarkeit des OCSP-Responders im Online-Betrieb (MGM_LU_ONLINE = Enabled) ist.

4357 [**<=**]

4358 TIP1-A_5545 - nonQES-Signaturprüfergebnis bezogen auf Signaturzeitpunkt
4359 Der Konnektor MUSS zur nonQES-Signaturprüfung ein Prüfergebnis das sich auf genau
4360 einen angenommenen Signaturzeitpunkt bezieht, an den Aufrufer zurückgeben.
4361 Die Auswahl des angenommenen Signaturzeitpunkts, auf den sich das Signaturergebnis
4362 bezieht, erfolgt hierarchisch:

- 4363 • Benutzerdefinierter_Zeitpunkt
- 4364 falls vorhanden, sonst
- 4365 • Ermittelter_Signaturzeitpunkt_Eingebettet
- 4366 falls vorhanden, sonst
- 4367 • Ermittelter_Signaturzeitpunkt_System

4368 [\leq]

4369 4.1.8.4.3 TUC_KON_162 „Kryptographische Prüfung der XML-Dokumentensignatur“

4370 TIP1-A_5505 - TUC_KON_162 „Kryptographische Prüfung der XML-Dokumentensignatur“

4371 Der Konnektor MUSS den technischen Use Case TUC_KON_162 „Kryptographische
4372 Prüfung der XML-Dokumentensignatur“ umsetzen.

4373

4374 **Tabelle 212: TAB_KON_430 – TUC_KON_162 „Kryptographische Prüfung der XML-
4375 Dokumentensignatur“**

Element	Beschreibung
Name	TUC_KON_162 „Kryptographische Prüfung der XML-Dokumentensignatur“
Beschreibung	Es wird die mathematische Korrektheit der elektronischen Signatur eines XML-Dokuments geprüft. Sind mehrere Signaturen vorhanden, so werden alle geprüft.
Auslöser	Aufruf durch ein Fachmodul
Vorbedingungen	<ul style="list-style-type: none"> signedDocument ist ein XML-Dokument signedDocument hat TUC_KON_080 erfolgreich durchlaufen
Eingangsdaten	<ul style="list-style-type: none"> signedDocument – <i>optional</i> (QES-signiertes XML-Dokument -> siehe Definition in Operation VerifyDocument mit SIG:Document) signatureObject – <i>optional</i> (-> siehe Definition in Operation VerifyDocument mit dss:SignatureObject)
Komponenten	Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> result (Ergebnis der Signaturprüfung)
Standardablauf	<p>„CoreValidation“: Es erfolgt die mathematische Prüfung der Signatur, bestehend aus der Prüfung der Hash-Kette bis zum signierten Hashwert und der Prüfung der kryptographischen Signatur unter Verwendung des öffentlichen Schlüssels aus dem Zertifikat, des Signaturwertes und des signierten Hashwertes.</p> <p><u>XML-Signatur:</u> Die Core Validation erfolgt entsprechend [XMLDSig] Kapitel 3.2 Core Validation. a) CoreValidation erfolgreich -> result = true b) CoreValidation fehlerhaft -> result = false</p>
Varianten/Alternativen	keine

Fehlerfälle	Fehler in den folgenden Schritten des Standardablaufs führen zu den ausgewiesenen Fehlercodes: Interner Fehler: 4001
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

4376

4377

4378

Tabelle 213: TAB_KON_431 Fehlercodes TUC_KON_162 „Kryptographische Prüfung der XML-Dokumentensignatur“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weiteren Fehlercodes auftreten.			
4001	Technical	Error	Interner Fehler

4379

4380

[<=]

4381

4.1.8.4.4 TUC_KON_150 „Dokumente QES signieren“

4382

TIP1-A_4655 - TUC_KON_150 „Dokument QES signieren“,

4383

Der Konnektor MUSS den technischen Use Case TUC_KON_150 „Dokumente QES signieren“ umsetzen.

4384

4385

4386

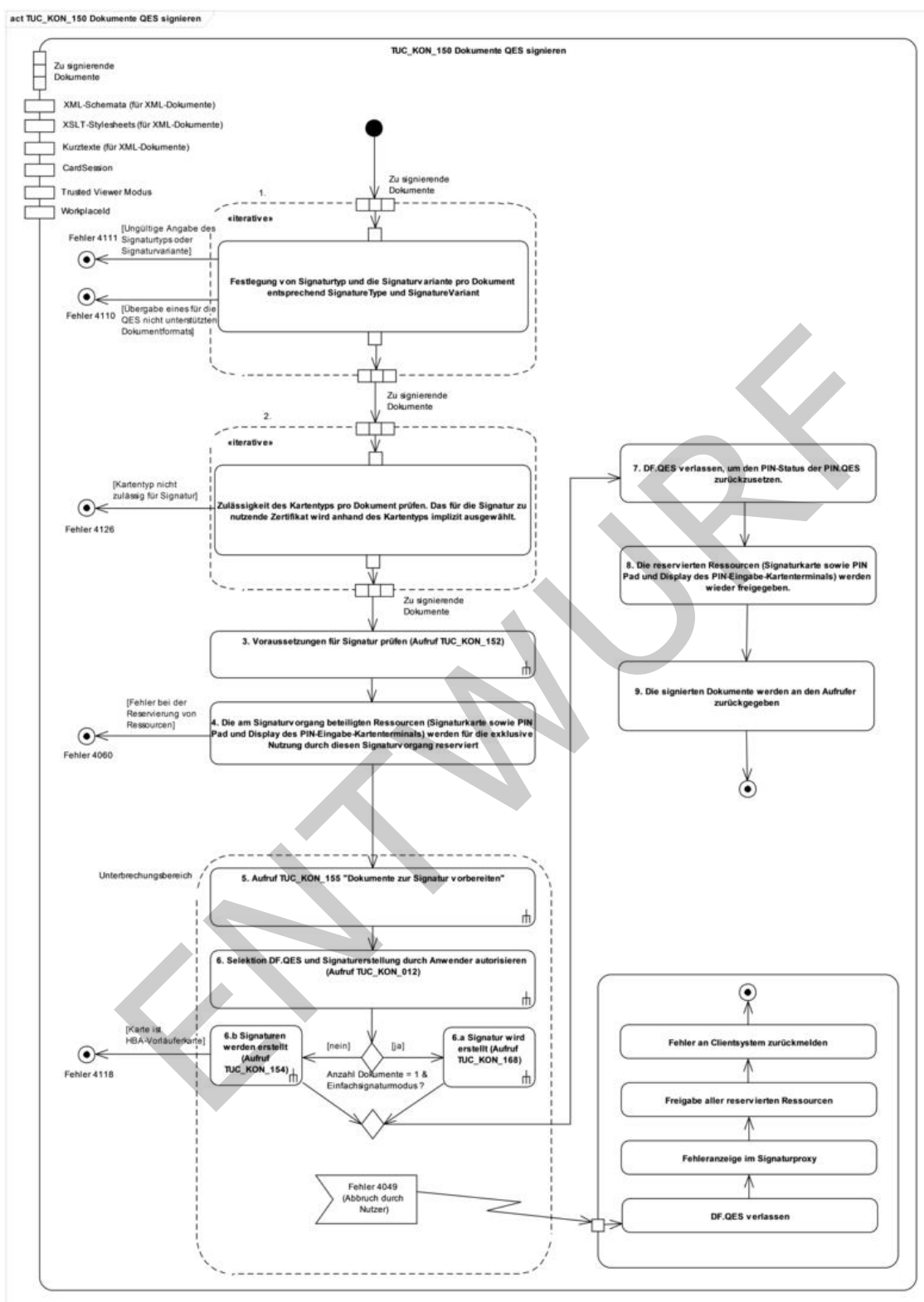
Tabelle 214: TAB_KON_755 – TUC_KON_150 „Dokumente QES signieren“

Element	Beschreibung
Name	TUC_KON_150 "Dokumente QES signieren"
Beschreibung	Im Rahmen von Fachanwendungen werden ein oder mehrere Dokumente mit einer qualifizierten elektronischen Signatur versehen. Es werden die QES_DocFormate unterstützt.
Auslöser	Aufruf durch ein Clientsystem (Operation SignDocument) oder ein Fachmodul.
Vorbedingungen	Die Signaturkarte muss gesteckt sein.
Eingangsdaten	<ul style="list-style-type: none"> signRequests (Liste von Signaturaufträgen) Jeder Signaturauftrag (SignRequest) kapselt: <ul style="list-style-type: none"> documentsToBeSigned (Zu signierendes Dokument bzw. zu signierende Dokumente); darin u.a.

	<p>documentFormat (Formatangabe für das zu signierende Dokument)</p> <ul style="list-style-type: none"> optionalInputs (weitere optionale Eingabeparameter zur Steuerung der Details bei der zu erstellenden Signatur, siehe Operation SignDocument, Parameter dss:OptionalInputs); darin u.a. signatureType (URI für den Signaturtyp XML-, CMS-, S/MIME-, PDF-Signatur) includeRevocationInfo [Boolean]: – optional; Default: true (Dieser optionale Parameter steuert die Einbettung von OCSP Antworten in die Signatur; siehe Operation SignDocument, Parameter SIG:IncludeRevocationInfo) cardSession (Kartensitzung. Unterstützte Kartentypen: HBAX) crypt [SIG_CRYPT_QES] - <i>optional</i>; default und Wertebereich: siehe TAB_KON_862 (Dieser Parameter steuert, ob RSA-basierte oder ECC-basierte Signaturen erzeugt werden.) workplaceId
Komponenten	Konnektor, Kartenterminal, Signaturkarte (HBAX)
Ausgangsdaten	<ul style="list-style-type: none"> signedDocuments (Liste der signierten Dokumente)
Standardablauf	<p>Der Konnektor KANN die Schritte 1 bis 4 in einer beliebigen Reihenfolge durchführen.</p> <ol style="list-style-type: none"> Der Signaturtyp und die Signaturvariante werden für jedes Dokument der Liste entsprechend signatureType und SignatureVariant festgelegt (ggf. in optionalInputs enthalten). Wenn SignatureType oder SignatureVariant nicht übergeben wurden, wird das dem Dokumentformat entsprechende Default-Verfahren gewählt (siehe TAB_KON_583 – Default-Signaturverfahren). Für alle Dokumente des Stapels wird die Zulässigkeit des Kartentyps geprüft. Das für die Signatur zu nutzende Zertifikat wird anhand des Kartentyps und des Parameters crypt ausgewählt. Es werden die Voraussetzungen für die Signatur geprüft. Dies erfolgt im TUC_KON_152 „Signaturvoraussetzungen für QES prüfen“. Wenn includeRevocationInfo=true, dann setze ocsResponses auf Rückgabewert von TUC_KON_152. Die am Signaturvorgang beteiligten Ressourcen (Signaturkarte sowie PIN Pad und Display des PIN-

	<p>Eingabe-Kartenterminals) werden für die exklusive Nutzung durch diesen Signaturvorgang reserviert. Die Reservierung der Signaturkarte erfolgt durch Aufruf von TUC_KON_023 „Karte reservieren“ { cardSession; doLock = true }.</p> <p>5. Zum Vorbereiten der Dokumente für die Signatur wird TUC_KON_155 „Dokumente zur Signatur vorbereiten“ mit ocsResponses aufgerufen. Die Zugriffe auf die Signaturkarte in den Schritten 6 bis 7 müssen im DF.QES erfolgen.</p> <p>6. Die Signaturerstellung wird durch den Anwender autorisiert. Dies erfolgt durch Aufruf von TUC_KON_012 „PIN verifizieren“ { cardSession; workplaceId; pinRef = PIN.QES; verificationType = Mandatorisch }</p> <p>Wenn nur ein zu signierendes Dokument vorhanden ist und der Einfachsignaturmodus aktiviert ist (siehe Konfigurationsparameter SAK_SIMPLE_SIGNATURE_MODE), wird in Schritt 7 Variante a) durchgeführt, ansonsten Variante b).</p> <p>7. Variante a) Die Signatur wird erstellt. Dies erfolgt gemäß TUC_KON_168 „Einzelsignatur QES erstellen“. Variante b) Die Signaturen werden erstellt. Dies erfolgt gemäß TUC_KON_154 „QES-Signaturen erstellen“.</p> <p>8. Es wird DF.QES verlassen, um den PIN-Status der PIN.QES zurückzusetzen. Der im Konnektor verwaltete Sicherheitszustand (CARDSESSION.AUTHSTATE) ist zu aktualisieren.</p> <p>9. Die reservierten Ressourcen (Signaturkarte sowie PIN-Pad und Display des PIN-Eingabe-Kartenterminals) werden wieder freigegeben. Zur Freigabe der Signaturkarte wird TUC_KON_023 „Karte reservieren“ cardSession; doLock = false } aufgerufen.</p> <p>10. Die signierten Dokumente werden an den Aufrufer zurückgegeben.</p>
Varianten/ Alternativen	Der Nutzer kann den Vorgang bei der Autorisierung (Schritt 6) abbrechen. Hierbei sind die gleichen Regeln anzuwenden wie im Fehlerfall (s. Fehlerfälle).
Fehlerfälle	Fehler in den folgenden Schritten des Standardablaufs führen zum Abbruch mit den ausgewiesenen Fehlercodes: (->1) Ungültige Angabe des Signaturtyps oder Signaturvariante: Fehlercode 4111

	<p>Übergabe eines für die QES nicht unterstützten Dokumentformats: Fehlercode 4110 (->2) Kartentyp nicht zulässig für Signatur: Fehlercode 4126 (->5) Fehler bei der Reservierung von Ressourcen: Fehlercode 4060 (->7b) Karte ist kein HBA, sondern HBA-Vorläuferkarte: Fehlercode 4118 Im Fehlerfall, inklusive Timeout bei der PIN-Eingabe, oder bei Abbruch durch den Benutzer (Fehler 4049): a) ... MUSS DF.QES verlassen werden b) ... MÜSSEN alle reservierten Ressourcen freigegeben werden c) ... MUSS der Fehler immer an das Clientsystem zurückgemeldet werden</p>
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	Abbildung PIC_KON_114 Aktivitätsdiagramm zu „Dokument QES signieren“



4387

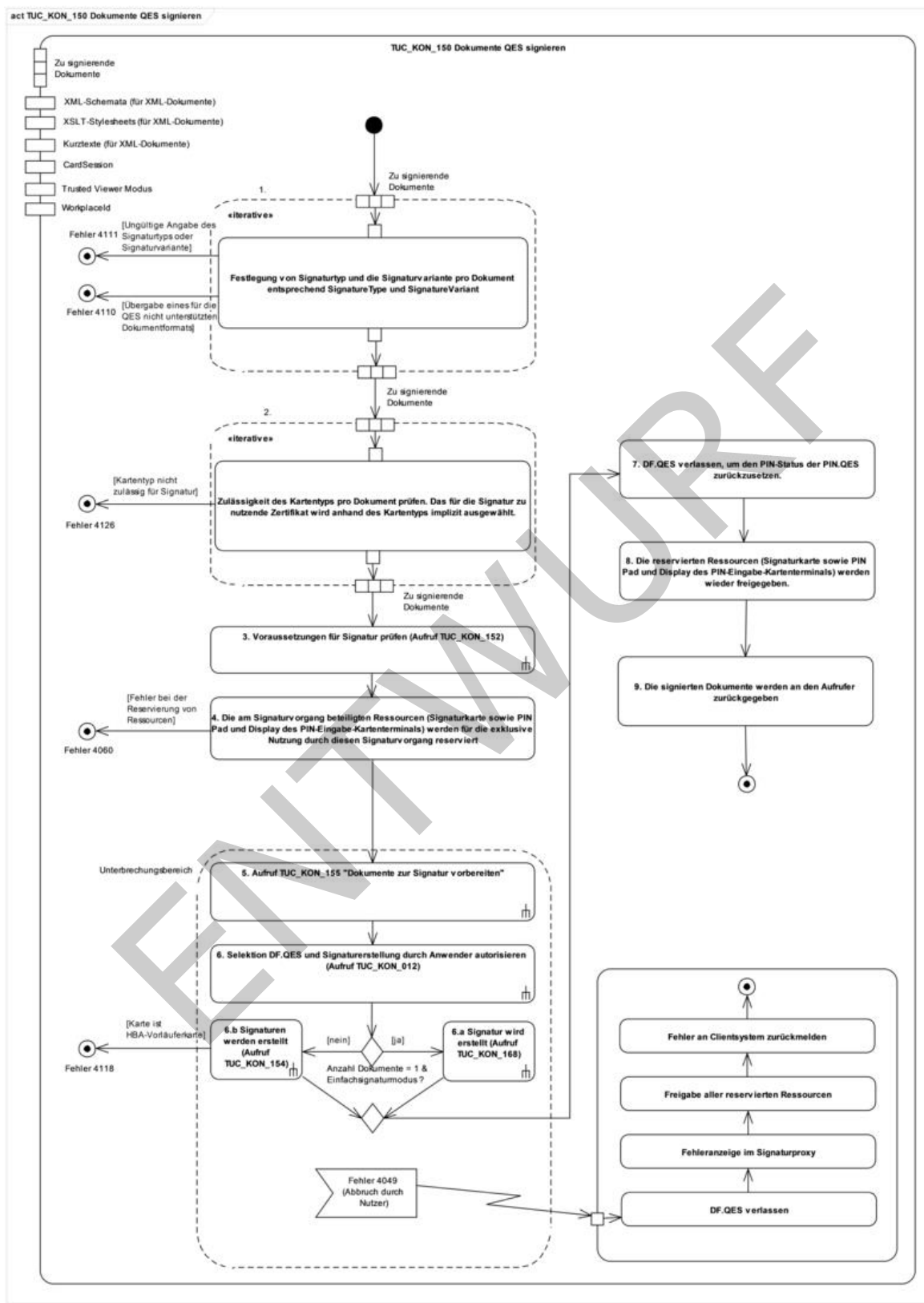


Abbildung 19: PIC_KON_114 Aktivitätsdiagramm zu „Dokument QES signieren“

4392 **Tabelle 215: TAB_KON_128 Fehlercodes TUC_KON_150 „Dokument QES signieren“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4060	Technical	Error	Ressource belegt
4110	Technical	Error	ungültiges Dokumentformat (%Format%) Der Parameter Format enthält das übergebene Dokumentformat.
4111	Technical	Error	ungültiger Signaturtyp oder Signaturvariante
4118	Technical	Error	Stapelsignaturen werden nur für den HBA unterstützt. Mit HBA-Vorläuferkarten sind nur Einzelsignaturen möglich.
4126	Security	Error	Kartentyp nicht zulässig für Signatur
4049	Technical	Error	Abbruch durch den Benutzer

4393 [**<=**]4394 **Anforderungen zur XML-Sicherheit:**

4395 TIP1-A_5113 - Abwehr von XML-Signature-Wrapping Angriffen

4396 Der Konnektor MUSS XML-Signature-Wrapping-Angriffe (XSW) abwehren.

4397 [**<=**]4398 *4.1.8.4.5 Anforderungen an die Stapelsignatur*

4399 Eine Stapelsignatur definiert sich als „Erstellung einer begrenzten Anzahl Signaturen nach
 4400 den zeitlich unmittelbar aufeinander folgenden Prozessen der Anzeige der zu
 4401 signierenden Daten und der einmaligen Authentisierung des Signaturschlüssel-Inhabers
 4402 gegenüber der qualifizierten elektronischen Signaturerstellungseinheit“ (siehe [BSI-
 4403 TR03114]).

4404 TIP1-A_4669 - QES-Stapelsignatur

4405 Der Signatordienst MUSS die Möglichkeit bieten, Dokumente eines Stapels einzeln
 4406 qualifiziert elektronisch zu signieren. Der Signatordienst MUSS als qualifizierte
 4407 elektronische Signaturerstellungseinheit für die Stapelsignatur den HBA unterstützen.

4408 [**<=**]

4409 TIP1-A_5664 - Reihenfolge der Dokumente bei Stapelsignatur

4410 Die zu signierenden Dokumente einer Stapelsignatur MÜSSEN vom Signatordienst im
 4411 Konnektor in derselben Reihenfolge signiert, in der sie im Signaturauftrag vom
 4412 Clientsystem geschickt werden.

4413 [**<=**]

4414 TIP1-A_4670 - Secure Messaging für die DTBS

4415 Bei der Stapelsignatur MUSS der Signatordienst die zu signierenden Daten (DTBS) über
 4416 Secure Messaging vom Konnektor zum HBA übertragen. Dieser Secure Messaging-Kanal
 4417 MUSS über die gSMC-K zum HBA mittels C.SAK.AUTD_CVC aufgebaut werden.

4418 [**<=**]

4419 TIP1-A_4671 - Verhalten des Konnektors beim Abbruch einer Stapelsignatur

4420 Der Signatordienst MUSS dem Benutzer während und nach einer PIN-Eingabe die

4421 Möglichkeit zum Abbruch einer Stapelsignatur anbieten.

4422 Das geforderte Verhalten des Konnektors beim Abbruch einer Stapelsignatur wird in der

4423 folgenden Tabelle beschrieben. Hierbei werden die beiden Punkte „Abbruch, während die
 4424 erneute PIN-Eingabe angefordert wird“ (Nummer 1 bis 4) und „Abbruch, während der
 4425 Vorgang der Signaturerstellung läuft“ (Nummer 5 bis 6) unterschieden. Zeile Nummer 7
 4426 beschreibt alle sonstigen Fehlerfälle.
 4427 Ein Teilstapel einer Stapelsignatur ist durch die maximale Anzahl der Dokumente
 4428 definiert, welche nach der Eingabe der Signatur-PIN durch den Signaturschlüssel-Inhaber
 4429 signiert werden kann.

4430
 4431 **Tabelle 216: TAB_KON_192 Verhalten des Konnektors beim Abbruch einer Stapelsignatur**

Nummer	Problem/Fehler/Ereignis	Verhalten des Konnektors
Während die erneute PIN-Eingabe angefordert wird	1 Timeout bei der PIN-Eingabe am KT	Der Signaturvorgang (Stapel) wird <u>beendet</u> . Kein „Fehler“ Die Signaturen des/der vorherigen Teilstapel(s) bleiben erhalten und werden an das Clientsystem zurückgegeben. Keine weiteren Signaturen des neuen Teilstapels werden erstellt. (Die Weiterverarbeitung bereits erstellter Signaturen des letzten Teilstapels (sofern vorhanden) wird noch abgeschlossen).
	2 PIN gesperrt (nach mehrfacher Fehleingabe)	Siehe Verhalten unter Nummer 1
	3 Abbruchkommando „StopSignature“ zur Jobnummer wird empfangen	Der Signaturvorgang (Stapel) wird <u>beendet</u> . Kein „Fehler“ Keine weiteren Signaturen des neuen Teilstapels werden erstellt. (Die Weiterverarbeitung bereits erstellter Signaturen des letzten Teilstapels (sofern vorhanden) wird noch abgeschlossen).
	4 Abbruchtaste am Kartenterminal wird gedrückt	Siehe Verhalten unter Nummer 1
während der Vorgang der Signaturerstellung läuft	5 Abbruchkommando „StopSignature“ zur Jobnummer wird empfangen	Signaturvorgang (Stapel) wird <u>abgebrochen</u> . Kein „Fehler“ Keine weiteren Signaturen des Stapels werden erstellt. Keine weiteren Signaturen des Teilstapels werden erstellt. Bisher erstellte Signaturen des

			aktuellen Teilstapels werden verworfen.
	6	Abbruchtaste am Kartenterminal wird gedrückt.	Die „Abbruch“-Taste wird nicht vom Signatordienst fortlaufend überwacht → Keine Aktion seitens des Signatordienstes.
	7	Bei allen anderen Fehlerfällen (z. B.: es kommen zu viele Signaturen zurück, der Hash-Wert einer der Signaturen stimmt nicht, Karte gezogen, etc)	Signaturvorgang (Stapel) wird abgebrochen. Schwerer Fehler. Keine weiteren Signaturen des Stapels werden erstellt. Keine weiteren Signaturen des aktuellen Teilstapels werden erstellt. Bisher erstellte Signaturen aller Teilstapel werden verworfen. Es handelt sich um Probleme/Fehlerfälle, die bei typischen Angriffen auftreten können.

4432

4433 [\leq]

4434 4.1.8.4.6 TUC_KON_151 „QES Dokumentensignatur prüfen“

4435 TIP1-A_4672-02 - TUC_KON_151 „QES-Dokumentensignatur prüfen“

4436 Der Konnektor MUSS den technischen Use Case TUC_KON_151 „QES-Dokumentensignatur prüfen“ umsetzen.

4437

4438

4439 **Tabelle 217: TAB_KON_591 - TUC_KON_151 „QES-Dokumentensignatur prüfen“**

Element	Beschreibung
Name	TUC_KON_151 „QES-Dokumentensignatur prüfen“
Beschreibung	Es wird die QES eines Dokuments geprüft. Dabei werden die Signaturverfahren laut Tabelle TAB_KON_582 – Signaturverfahren unterstützt. Sind mehrere Signaturen vorhanden, so werden alle geprüft. Auch Parallel- und Gegensignaturen MÜSSEN unterstützt werden.
Eingangsanforderung	keine
Auslöser	Aufruf durch ein Clientsystem (Operation VerifyDocument) oder durch ein Fachmodul im Konnektor
Vorbedingungen	keine

Eingangsdaten	<ul style="list-style-type: none"> signedDocument – <i>optional</i> (QES-signiertes Dokument vom Typ QES_DocFormate -> siehe Definition in Operation VerifyDocument mit SIG:Document) signatureObject – <i>optional</i> (-> siehe Definition in Operation VerifyDocument mit dss:SignatureObject. Es werden Parallel- und Gegensignaturen unterstützt.) optionalInputParams (optionale Eingabeparameter, siehe Operation VerifyDocument, Parameter SIG:OptionalInputs) certificates – <i>optional/falls diese nicht im signierten Dokument enthalten sind, sondern nur referenziert werden</i> (X.509-Zertifikate). xmlSchemas – <i>optional/nur für XML-Dokumente</i> (XMLSchema und ggf. weitere vom Hauptschema benutzte Schemata) includeRevocationInfo [Boolean]: – <i>optional; Default: false</i> (Dieser optionale Parameter steuert die Einbettung von OCSP Antworten in die Signatur)
Komponenten	Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> verificationResult [VerificationResult] (Ergebnis der Signaturprüfung) optionalOutput – <i>optional</i> (weitere Ausgabedaten gemäß SIG:OptionalOutput)
Standardablauf	<p>1. „DocumentValidation“: Das signierte Dokument wird validiert mit Aufruf TUC_KON_080 „Dokument validieren“{ ... }.</p> <p>Treten Fehler bei der Validierung der Typkonformität auf, wenn die Signatur im Dokument eingebettet ist, wird die Prüfung mit einem Fehler abgebrochen. Treten bei der Typkonformität, wenn die Signatur nicht im Dokument eingebettet ist, Fehler auf, so bricht der TUC nicht ab, sondern führt die folgenden Schritte soweit sinnvoll möglich durch. (Die Entscheidung über das sinnvoll Durchführbare liegt beim Hersteller des Konnektors.)</p> <p>2. „CoreValidation“:</p> <p>Es erfolgt die mathematische Prüfung der Signatur, bestehend aus der Prüfung der Hash-Kette bis zum signierten Hashwert und der Prüfung der Signatur unter Verwendung des öffentlichen Schlüssels, des Signaturwertes und des signierten Hashwertes.</p>

	<p>XML-Signatur: Die Core Validation erfolgt entsprechend [XMLDSig] Kapitel 3.2 Core Validation.</p> <p>CMS-Signatur: Die Core Validation erfolgt entsprechend Cryptographic Message Syntax (CMS) Kapitel 5.6 Signature Verification Process [RFC5652].</p> <p>PDF-Signatur: Die Core Validation erfolgt entsprechend [PAdES-3] Kapitel 4.6 Signature Validation aus PAdES-BES Part 3.</p> <p>Auch wenn die Validierung fehlschlägt, werden die folgenden Prüfschritte durchgeführt, so dass ein vollständiges Prüfprotokoll erstellt werden kann.</p> <p>3. „CheckSignatureCertificate“:</p> <p>Teil 1: Signaturzertifikat ermitteln</p> <p>XML-Signatur: Das Signaturzertifikat ist im XMLDSig Element <code>ds:KeyInfo/ds:X509Data</code> gespeichert [XMLDSig] oder wird als Eingangsparemeter übergeben.</p> <p>CMS-Signatur: Das Signaturzertifikat für CADES ist im Feld <code>certificates</code> im <code>SignedData</code> Container gespeichert [CADES] oder wird als Eingangsparemeter übergeben.</p> <p>PDF-Signatur: Das PDF Signaturzertifikat für PAdES ist im Feld <code>SignedData.certificates</code> entsprechend Kapitel 6.1.1 „Placements of the signing certificate“ [PAdES Baseline Profile] gespeichert oder wird als Eingangsparemeter übergeben.</p> <p>Teil 2: Signaturzeitpunkt bestimmen</p> <p>Der Signaturzeitpunkt <code>Ermittelter_Signaturzeitpunkt_Eingebettet</code> wird wie folgt selektiert:</p> <p>XML-Signatur: Das XML element <code>SigningTime</code> spezifiziert den Signaturzeitpunkt entsprechend Kapitel 7.2.1 XAdES [XAdES].</p> <p>CMS-Signatur: Das Attribut <code>SigningTime</code> spezifiziert den Signaturzeitpunkt entsprechend Kapitel 11.3 CMS [CMS].</p> <p>PDF-Signatur: Der Signaturzeitpunkt kann dem M Eintrag des Signature Dictionary entnommen werden [PAdES Baseline Profile] Kapitel</p>
--	---

	<p>6.2.1 Signing time.</p> <p>Der Signaturzeitpunkt <code>Benutzerdefinierter_Zeitpunkt</code> liegt gegebenenfalls als Aufrufparameter vor. Der Signaturzeitpunkt <code>Ermittelter_Signaturzeitpunkt_System</code> wird ermittelt.</p> <p>Teil 3: Signaturzertifikatsprüfung: Bei der folgenden Signaturzertifikatsprüfung sind die Signaturzeitpunkte gemäß [TIP1-A_5540] zu berücksichtigen. Die Signaturzertifikatsprüfung erfolgt durch Aufruf von TUC_KON_037 „Zertifikat prüfen“ { certificate = C.HP.QES; qualifiedCheck = required; baseTime = Signaturzeitpunkt; offlineAllowNoCheck = true; validationMode = OCSP; ocspResponses = OCSP-Response; getOCSPResponses = includeRevocationInfo }. Sind OCSP-Responses in der Signatur eingebettet, ist die jüngsten OCSP-Response des EE-Zertifikats, die für die Zertifikatsprüfung notwendig ist, beim Aufruf von TUC_KON_037 zu übergeben. Sofern der Aufruf von TUC_KON_037 ocspResponses zurückgibt, wird die OCSP-Response des EE-Zertifikats in die Signatur eingebettet. Auch wenn die Zertifikatsprüfung fehlschlägt, werden die folgenden Prüfungen durchgeführt.</p> <p>4. „CheckPolicyConstraints“:</p> <p>In diesem Schritt wird das signierte Dokument entsprechend der Profilierung der Signaturformate (siehe Anhang B.2) geprüft. Es sind die Vorgaben für die Prüfung von Signaturen aus den Standards für AdES [XAdES], [XAdES Baseline], [CAAdES], [CAAdES Baseline], [PAdES-3] und [PAdES Baseline] umzusetzen. Dabei sind die Vorgaben aus Tabelle TAB_KON_779 „Profilierung der Signaturformate“ und Tabelle TAB_KON_778 „Einsatzbereich der Signaturvarianten“ zu erfüllen.</p> <p>Auch wenn nicht alle Anforderungen an das Format des signierten Dokuments erfüllt werden, wird die Prüfung mit den folgenden Schritten fortgesetzt, um ein vollständiges Prüfungsprotokoll zu erhalten.</p> <p>5. Das Prüfergebnis (VerificationResult, OptionalOutput) wird an den Aufrufer zurückgegeben</p>
--	--

	(siehe TAB_KON_593 Übersicht Status für Prüfung einer Dokumentensignatur).
Varianten/Alternativen	Keine
Fehlerfälle	<p>Das Verhalten des TUCs bei einem Fehlerfall ist in TAB_KON_592 Fehlercodes TUC_KON_151 „QES Dokumentensignatur prüfen“ beschrieben.</p> <p>(->1) keine Signatur in signedDocument und signatureObject vorhanden: 4253.</p> <p>(→ 2 „CoreValidation“) Interner Fehler: 4001, Signatur des Dokuments ungültig: 4115, Signatur umfasst nicht das gesamte Dokument: 4262</p> <p>(→3 „CheckSignatureCertificate“) Interner Fehler: 4001, Signaturzertifikat ermitteln ist fehlgeschlagen: 4206.</p> <p>(→4 „CheckPolicyConstraints“) Interner Fehler: 4001, Dokument nicht konform zu Regeln für QES: 4124, Dokument nicht konform zu Profilierung der Signaturformate: 4208.</p>
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	keine

4440

4441 **Tabelle 218: TAB_KON_592 Fehlercodes TUC_KON_151 „QES Dokumentensignatur prüfen“**

4442

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4001	Technical	Error	interner Fehler
4115	Security	Error	Signatur des Dokuments ungültig. Prüfung der Hashwertkette bzw. Prüfung der kryptographischen Signatur fehlgeschlagen.
4124	Technical	Error	Dokument nicht konform zu Regeln für QES
4206	Technical	Error	Signaturzertifikat ermitteln ist fehlgeschlagen
4208	Technical	Error	Dokument nicht konform zu Profilierung der Signaturformate
4253	Technical	Error	Keine Signatur im Aufruf
4262	Technical	Error	Signatur umfasst nicht das gesamte Dokument
4264	Technical	Warning	Ein oder mehrere Zertifikate ignoriert

4443 Das Gesamtergebnis (VerificationResult) für die Prüfung einer Dokumentensignatur fasst

4444 die Ergebnisse

4445 aller Prüfungsschritte in einem einzelnen Statuswert zusammen.

4446 **Tabelle 219: TAB_KON_593 Übersicht Status für Prüfung einer Dokumentensignatur**

VerificationResult für gesamtes Dokument (VerificationResult/HighLevelResult)	
Wert	Bedeutung
VALID	Wenn VerificationResult für alle Signaturen zum Dokument VALID
INVALID	Wenn VerificationResult für eine Signatur zum Dokument INVALID
INCONCLUSIV E	in allen anderen Fällen
VerificationResult pro Signatur (VerificationReport/IndividualReport/Result)	
Wert	Bedeutung mögliche Ausprägungen im VerificationReport
VALID	Die Signatur wurde gemäß den Regeln für die QES geprüft und für gültig befunden.
	ResultMajor = urn:oasis:names:tc:dss:1.0:resultmajor:Success ResultMinor = urn:oasis:names:tc:dss:1.0:resultminor:valid:signature:OnAllDocuments
	ResultMajor = urn:oasis:names:tc:dss:1.0:resultmajor:Success ResultMinor = urn:oasis:names:tc:dss:1.0:resultminor:valid:signature:HasManifestResults
INVALID	Die Signatur ist ungültig oder aufgrund eines Fehlers konnte die Signaturprüfung nicht durchgeführt werden.
	ResultMajor = urn:oasis:names:tc:dss:1.0:resultmajor:Success ResultMinor = urn:oasis:names:tc:dss:1.0:resultminor:invalid:IncorrectSignature
	ResultMajor = urn:oasis:names:tc:dss:1.0:resultmajor:RequesterError
	ResultMajor = urn:oasis:names:tc:dss:1.0:resultmajor:ResponderError
	ResultMajor = urn:oasis:names:tc:dss:1.0:resultmajor:InsufficientInformation

	ResultMinor = urn:oasis:names:tc:dss:1.0:resultminor:invalid:IncorrectSignature
	ResultMajor = urn:oasis:names:tc:dss:1.0:resultmajor:InsufficientInformation ResultMinor = urn:oasis:names:tc:dss:1.0:resultminor:CertificateChainNotComplete
INCONCLUSIVE	<p>Die Signatur wurde gemäß den Regeln für die QES geprüft. Allerdings konnten eine oder mehrere Prüfungen nicht vollständig durchgeführt werden. Einzelheiten finden sich in Result-Detail. Die Prüfungen, die durchgeführt werden konnten, waren erfolgreich.</p> <p>ResultMajor = urn:oasis:names:tc:dss:1.0:resultmajor:InsufficientInformation ResultMinor = urn:oasis:names:tc:dss:1.0:resultminor:OcspNotAvailable</p> <p>Hinweis: Das Erreichen dieses Zustandes hängt davon ab, ob eine OCSP-Abfrage nicht durchgeführt werden konnte, unabhängig davon, ob die Ursache dafür die Offlineschaltung des Konnektors (MGM_LU_ONLINE = Disabled) oder die Nichterreichbarkeit des OCSP-Responders im Online-Betrieb (MGM_LU_ONLINE = Enabled) ist.</p>

4447

4448 [**<=**]

4449 TIP1-A_5540-01 - QES-Signaturprüfergebnis bezogen auf Signaturzeitpunkt

4450 Der Konnektor MUSS zur QES-Signaturprüfung ein Prüfergebnis, das sich auf genau

4451 einen angenommenen Signaturzeitpunkt bezieht, an den Aufrufer zurückgeben.

4452 Die Auswahl des angenommenen Signaturzeitpunkts, auf den sich das Signaturergebnis

4453 bezieht, erfolgt hierarchisch:

4454 • Benutzerdefinierter_Zeitpunkt

4455 falls vorhanden, sonst

4456 • Ermittelter_Signaturzeitpunkt_Eingebettet

4457 falls vorhanden, sonst

4458 • Ermittelter_Signaturzeitpunkt_System

4459 [**<=**]

4460 4.1.8.4.7 TUC_KON_170 „Dokumente mit Komfort signieren“

4461 A_19103 - TUC_KON_170 "Dokumente mit Komfort signieren"

4462 Der Konnektor MUSS den technischen Use Case TUC_KON_170 „Dokumente mit Komfort
4463 signieren“ umsetzen.

4464

4465 **Tabelle 220: TAB_KON_871 – TUC_KON_170 „Dokumente mit Komfort signieren“**

Element	Beschreibung
Name	TUC_KON_170 "Dokumente mit Komfort signieren"

Beschreibung	Im Rahmen von Fachanwendungen werden ein oder mehrere Dokumente mit einer Komfortsignatur versehen. Es werden die QES_DocFormate unterstützt.
Auslöser	Aufruf durch ein Clientsystem (Operation SignDocument) oder ein Fachmodul.
Vorbedingungen	Die Signaturkarte muss gesteckt sein.
Eingangsdaten	<ul style="list-style-type: none"> signRequests (Liste von Signaturaufträgen) Jeder Signaturauftrag (SignRequest) kapselt: <ul style="list-style-type: none"> documentsToBeSigned (Zu signierendes Dokument bzw. zu signierende Dokumente); darin u.a. documentFormat (Formatangabe für das zu signierende Dokument) optionalInputs (weitere optionale Eingabeparameter zur Steuerung der Details bei der zu erstellenden Signatur, siehe Operation SignDocument, Parameter dss:OptionalInputs); darin u.a. signatureType (URI für den Signatortyp XML-, CMS-, PDF-Signatur) includeRevocationInfo [Boolean]: – optional; Default: true (Dieser optionale Parameter steuert die Einbettung von OCSP Antworten in die Signatur; siehe Operation SignDocument, Parameter SIG:IncludeRevocationInfo) cardSession (Kartensitzung. Unterstützte Kartentypen: HBA) crypt [SIG_CRYPT_QES] - <i>optional</i>; default und Wertebereich: siehe TAB_KON_862 (Dieser Parameter steuert, ob RSA-basierte oder ECC-basierte Signaturen erzeugt werden.) workplaceId
Komponenten	Konnektor, Kartenterminal, Signaturkarte (HBA)
Ausgangsdaten	<ul style="list-style-type: none"> signedDocuments (Liste der signierten Dokumente)
Standardablauf	<p>Der Konnektor KANN die Schritte 1 bis 4 in einer beliebigen Reihenfolge durchführen.</p> <ol style="list-style-type: none"> 1. Prüfe SAK_COMFORT_SIGNATURE = Enabled 2. Der Signatortyp und die Signaturvariante werden für jedes Dokument der Liste entsprechend signatureType und SignatureVariant festgelegt (ggf. in optionalInputs enthalten). Wenn SignatureType oder SignatureVariant nicht übergeben wurden, wird das dem Dokumentformat entsprechende Default-

	<p>Verfahren gewählt (siehe TAB_KON_583 – Default-Signaturverfahren).</p> <p>3. Für alle Dokumente des Stapels wird die Zulässigkeit des Kartentyps geprüft. Das für die Signatur zu nutzende Zertifikat wird anhand des Kartentyps und des Parameters crypt ausgewählt.</p> <p>4. Es werden die Voraussetzungen für die Signatur geprüft. Dies erfolgt im TUC_KON_152 „Signaturvoraussetzungen für QES prüfen“.</p> <p>Wenn includeRevocationInfo=true, dann setze ocsResponses auf Rückgabewert von TUC_KON_152.</p> <p>5. Die am Signaturvorgang beteiligte Ressource Signaturkarte wird für die exklusive Nutzung durch diesen Signaturvorgang reserviert. Die Reservierung der Signaturkarte erfolgt durch Aufruf von TUC_KON_023 „Karte reservieren“ { cardSession; doLock = true }.</p> <p>6. Zum Vorbereiten der Dokumente für die Signatur wird TUC_KON_155 „Dokumente zur Signatur vorbereiten“ mit ocsResponses aufgerufen.</p> <p>Die Zugriffe auf die Signaturkarte im Schritt 7 müssen im DF.QES erfolgen. DF.QES darf am Ende des TUCs nicht verlassen werden.</p> <p>7. Die Signaturen werden erstellt. Dies erfolgt gemäß TUC_KON_158 „Komfortsignaturen erstellen“.</p> <p>8. Die reservierte Ressource Signaturkarte wird wieder freigegeben. Zur Freigabe der Signaturkarte wird TUC_KON_023 „Karte reservieren“ cardSession; doLock = false } aufgerufen.</p> <p>9. Die signierten Dokumente werden an den Aufrufer zurückgegeben.</p>
Varianten/ Alternativen	keine
Fehlerfälle	<p>Fehler in den folgenden Schritten des Standardablaufs führen zum Abbruch mit den ausgewiesenen Fehlercodes:</p> <p>(->1) Komfortsignaturfunktion im Konnektor nicht aktiviert: Fehlercode 4263</p> <p>(->2) Ungültige Angabe des Signaturtyps oder Signaturvariante: Fehlercode 4111 Übergabe eines für die QES nicht unterstützten Dokumentformats: Fehlercode 4110</p> <p>(->3) Kartentyp nicht zulässig für Signatur: Fehlercode 4126</p> <p>(->5) Fehler bei der Reservierung der Signaturkarte: Fehlercode 4060</p> <p>(->7) Karte ist kein HBA, sondern HBA-Vorläuferkarte: Fehlercode 4118</p>

	Im Fehlerfall: a) ... DARF DF.QES NICHT verlassen werden b) ... MÜSSEN alle reservierten Ressourcen freigegeben werden c) ... MUSS der Fehler immer an das Clientsystem zurückgemeldet werden
Sicherheitsanforderungen	Der Konnektor MUSS sicherstellen, dass der erhöhte Sicherheitszustand der PIN.QES nur für die Komfortsignatur mittels TUC_KON_170 innerhalb einer Kartensitzung nachgenutzt werden darf.

Tabelle 221: TAB_KON_872 Fehlercodes TUC_KON_170 „Dokumente mit Komfort signieren“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4060	Technical	Error	Ressource belegt
4110	Technical	Error	ungültiges Dokumentformat (%Format%) Der Parameter Format enthält das übergebene Dokumentformat.
4111	Technical	Error	ungültiger Signatortyp oder Signaturvariante
4118	Technical	Error	Stapelsignaturen werden nur für den HBA unterstützt.
4126	Security	Error	Kartentyp nicht zulässig für Signatur
4049	Technical	Error	Abbruch durch den Benutzer
4263	Technical	Error	Komfortsignaturfunktion nicht aktiviert

[<=]

4.1.8.4.8 TUC_KON_171 „Komfortsignatur einschalten“

A_19104 - TUC_KON_171 „Komfortsignatur einschalten“

Der Konnektor MUSS den technischen Use Case TUC_KON_171 „Komfortsignatur einschalten“ umsetzen.

Tabelle 222: TAB_KON_883 – TUC_KON_171 „Komfortsignatur einschalten“

Element	Beschreibung
Name	TUC_KON_171 „Komfortsignatur einschalten“
Beschreibung	Zum Einschalten des Komfortsignaturmodus wird die PIN.QES verifiziert und der Signaturmodus „Comfort“ für die cardSession gesetzt.

Auslöser	<ul style="list-style-type: none"> Operation ActivateComfortSignature Aufruf durch ein Fachmodul
Vorbedingungen	Der Karte muss gesteckt sein.
Eingangsdaten	<ul style="list-style-type: none"> cardSession (nur HBA erlaubt)
Komponenten	Konnektor, Kartenterminal, Karte (HBA)
Ausgangsdaten	<ul style="list-style-type: none"> signatureMode
Standardablauf	<ol style="list-style-type: none"> 1. Prüfe <code>SAK_COMFORT_SIGNATURE = Enabled</code> 2. Die am Vorgang beteiligten Ressourcen (Karte sowie PIN-Pad und Display des PIN-Eingabe-Kartenterminals) werden für die exklusive Nutzung durch diesen Vorgang reserviert. Die Reservierung der Karte erfolgt durch Aufruf von TUC_KON_023 „Karte reservieren“ { cardSession; doLock = true } 3. Die Einschaltung der Komfortsignatur wird durch den Anwender autorisiert. Dies erfolgt durch Aufruf von TUC_KON_012 „PIN verifizieren“ { cardSession; workplaceId; pinRef = PIN.QES; verificationType = Mandatorisch } Für die Anzeige am Kartenterminal ist die Displaymessage für „Komfortsignatur aktivieren“ aus TAB_KON_090 zu verwenden. 4. Setze <code>CARDSESSION.SIGNMODE = Comfort</code> 5. Starte Komfortsignatur-Timer für die cardSession bei „0“ 6. Die reservierten Ressourcen (Karte sowie PIN-Pad und Display des PIN-Eingabe-Kartenterminals) werden wieder freigegeben. Zur Freigabe der Karte wird TUC_KON_023 „Karte reservieren“ cardSession; doLock = false } aufgerufen.
Varianten/ Alternativen	Keine
Fehlerfälle	Fehler in den folgenden Schritten des Standardablaufs führen zum Abbruch mit den ausgewiesenen Fehlercodes: (->1) Komfortsignaturfunktion im Konnektor nicht aktiviert: Fehlercode 4263 (->2) Fehler bei der Reservierung von Ressourcen: Fehlercode 4060

	(->4) Fehler beim Setzen des Signaturmodus: Fehlercode 4267 (->5) Fehler beim Starten des Komfortsignatur-Timers: Fehlercode 4267 Im Fehlerfall, inklusive Timeout bei der PIN-Eingabe, oder bei Abbruch durch den Benutzer (Fehler 4049): a) ... MUSS (ab Schritt 3) DF.QES verlassen werden b) ... MÜSSEN alle reservierten Ressourcen freigegeben werden c) ... MUSS der Fehler immer an das Clientsystem zurückgemeldet werden
--	---

 4476 **Tabelle 223: TAB_KON_886 Fehlercodes TUC_KON_171 „Komfortsignatur einschalten“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4049	Technical	Error	Abbruch durch den Benutzer
4060	Technical	Error	Ressource belegt
4263	Technical	Error	Komfortsignaturfunktion nicht aktiviert
4267	Technical	Error	Fehler beim Aktivieren des Komfortsignaturmodus <cardHandle>

 4477 [\leq]

4478

 4479 **4.1.8.4.9 TUC_KON_172 „Komfortsignatur ausschalten“**

4480 A_19105 - TUC_KON_172 „Komfortsignatur ausschalten“

4481 Der Konnektor MUSS den technischen Use Case TUC_KON_172 „Komfortsignatur ausschalten“ umsetzen.

4482

 4484 **Tabelle 224: TAB_KON_884 – TUC_KON_172 „Komfortsignatur ausschalten“**

Element	Beschreibung
Name	TUC_KON_172 „Komfortsignatur ausschalten“
Beschreibung	Zum Ausschalten des Komfortsignaturmodus werden die Sicherheitszustände der Karte(n), die im Konnektor verwalteten Sicherheitszustände und der Signaturmodus der cardSession(s) zurückgesetzt.
Auslöser	<ul style="list-style-type: none"> Operation DeactivateComfortSignature TUC_KON_158 Der Administrator setzt SAK_COMFORT_SIGNATURE = Disabled Aufruf durch ein Fachmodul
Vorbedingungen	Die Karten müssen gesteckt sein.

Eingangsdaten	Bei Auslösen des TUCs durch den Administrator: <ul style="list-style-type: none"> Keine Ansonsten: <ul style="list-style-type: none"> cardHandles : Liste von cardHandles (nur HBA erlaubt)
Komponenten	Konnektor, Kartenterminal, Karte (HBA)
Ausgangsdaten	Keine
Standardablauf	<ol style="list-style-type: none"> Wenn der TUC <u>nicht</u> durch den Administrator ausgelöst wurde: Prüfe <code>SAK_COMFORT_SIGNATURE = Enabled</code> Wenn der TUC durch den Administrator ausgelöst wurde: Ermittle die cardHandles aller gesteckten HBA. Für jedes übergebene bzw. ermittelte cardHandle: Ermittle cardSessions zu cardHandle Für jede ermittelte cardSession: <ol style="list-style-type: none"> Setze den PIN-Status der PIN.QES zurück (z. B. durch Verlassen von DF.QES für alle logischen Kanäle der Karte) Lösche den im Konnektor verwalteten Sicherheitszustand aus <code>CARDSESSION.AUTHSTATE</code> (<code>PINRef=PIN.QES</code>) Setze <code>CARDSESSION.SIGNMODE = PIN</code> Stoppe Komfortsignatur-Timer für die cardSession
Varianten/ Alternativen	Keine
Fehlerfälle	(->1) Komfortsignaturfunktion im Konnektor nicht aktiviert: Fehlercode 4263 Fehler und Warnungen in den folgenden Schritten werden über alle cardHandle akkumuliert und die <komma-separierte Liste von cardHandle> für den jeweiligen Fehlertext erzeugt. (->3) Bei einem ungültigen cardHandle wird mit dem nächsten cardHandle aus cardHandles fortgesetzt. Fehlercode 4265 (->4) Ist zu einem cardHandle keine cardSession vorhanden wird mit dem nächsten cardHandle fortgesetzt. Fehlercode 4266 (->5) Tritt in Schritt 4 ein Fehler auf wird mit dem nächsten cardHandle fortgesetzt. Fehlercode 4268

4485

4486

Tabelle 225: TAB_KON_887 Fehlercodes TUC_KON_172 „Komfortsignatur ausschalten“

Fehlercode	ErrorType	Severity	Fehlertext
4263	Technical	Fehler	Komfortsignaturfunktion nicht aktiviert

4265	Technical	Warning	Karten-Handle ungültig <komma-separierte Liste von cardHandle>
4266	Technical	Warning	Keine Kartensitzung vorhanden <komma-separierte Liste von cardHandle>
4268	Technical	Fehler	Fehler beim Deaktivieren des Komfortsignaturmodus <komma-separierte Liste von cardHandle>

4487 [\leq]

4488

4489 4.1.8.4.10 TUC_KON_173 „Liefere Signaturmodus“

4490 A_19106 - TUC_KON_173 „Liefere Signaturmodus“

4491 Der Konnektor MUSS den technischen Use Case TUC_KON_173 „Liefere Signaturmodus“ umsetzen.

4492

4493

4494 **Tabelle 226: TAB_KON_885 – TUC_KON_173 „Liefere Signaturmodus“**

Element	Beschreibung
Name	TUC_KON_173 „Liefere Signaturmodus“
Beschreibung	Der aktuell konfigurierte Status der Komfortsignaturfunktion im Konnektor und der aktuelle Signaturmodus für alle dem Konnektor bekannten Aufrufkontexte zu den übergebenen HBA-CardHandles wird ermittelt und an den Aufrufer zurückgegeben.
Auslöser	<ul style="list-style-type: none"> • Operation GetSignatureMode • Aufruf durch ein Fachmodul
Vorbedingungen	Keine
Eingangsdaten	<ul style="list-style-type: none"> • Liste von cardHandles (nur HBA erlaubt)
Komponenten	Konnektor, Kartenterminal, Signaturkarte (HBA)
Ausgangsdaten	<ul style="list-style-type: none"> • comfortSignatureStatus • comfortSignatureMax • comfortSignatureTimer • signatureModes: Struktur aus • Liste von cardHandles (nur HBA erlaubt) <ul style="list-style-type: none"> • Liste von Tupeln (signatureContext, signatureMode, countRemaining, timeRemaining)
Standardablauf	<ol style="list-style-type: none"> 1. Ermittle den Status der Komfortsignaturfunktion: comfortSignatureStatus=SAK_COMFORT_SIGNATURE 2. Ermittle comfortSignatureMax=SAK_COMFORT_SIGNATURE_MAX

	<p>3. Ermittle comfortSignatureTimer= SAK_COMFORT_SIGNATURE_Timer</p> <p>4. Für jedes übergebene cardHandle:</p> <p>a. Ermittle cardSession zu cardHandle</p> <p>b. Für jede ermittelte cardSession:</p> <p>i. Ermittle den Kontext (signatureContext) der cardSession aus CARDSESSION.MANDANTID, CARDSESSION.CSID, CARDSESSION.USERID</p> <p>ii. Ermittle den Signaturmodus (signatureMode) aus CARDSESSION.SIGNMODE</p> <p>iii. Ermittle Differenz von SAK_COMFORT_SIGNATURE_MAX und Komfortsignatur-Zähler der cardSession (countRemaining)</p> <p>iv. Ermittle verbleibende Zeit aus SAK_COMFORT_SIGNATURE_TIMER und Komfortsignatur-Timer der cardSession (timeRemaining)</p>
Varianten/ Alternativen	<p>Wenn SAK_COMFORT_SIGNATURE = Disabled (->4 b iii) countRemaining = 0 (->4 b iv) timeRemaining = 0</p>
Fehlerfälle	<p>(->2) Bei einem ungültigen cardHandle wird mit dem nächsten cardHandle aus cardHandles fortgesetzt. Fehlercode 4265 (->2a) Ist zu einem cardHandle keine cardSession vorhanden wird mit dem nächsten cardHandle fortgesetzt. Fehlercode 4266 (->2b) Tritt in Schritt 2b ein Fehler auf wird mit dem nächsten cardHandle fortgesetzt. Fehlercode 4269 Die Fehler und Warnungen werden über alle cardHandle akkumuliert und die <komma-separierte Liste von cardHandle> für den jeweiligen Fehlertext erzeugt.</p>

4495

4496

Tabelle 227: TAB_KON_888 Fehlercodes TUC_KON_173 „Liefere Signaturmodus“

Fehlercode	ErrorType	Severity	Fehlertext
4265	Technical	Warning	Karten-Handle ungültig <komma-separierte Liste von cardHandle>
4266	Technical	Warning	Keine Kartensitzung vorhanden <komma- separierte Liste von cardHandle>
4269	Technical	Error	Fehler beim Ermitteln des Signaturmodus <komma-separierte Liste von cardHandle>

4497 [**<=**]

4498

4.1.8.5 Operationen an der Außenschnittstelle

TIP1-A 4676-04 ~~**TIP1-A-4676-02**~~ - Basisdienst Signaturdienst (nonQES und QES)
Der Konnektor MUSS Clientsystemen den Basisdienst Signaturdienst (nonQES und QES) anbieten.

Tabelle 228: TAB_KON_197 Basisdienst Signaturdienst (nonQES und QES)

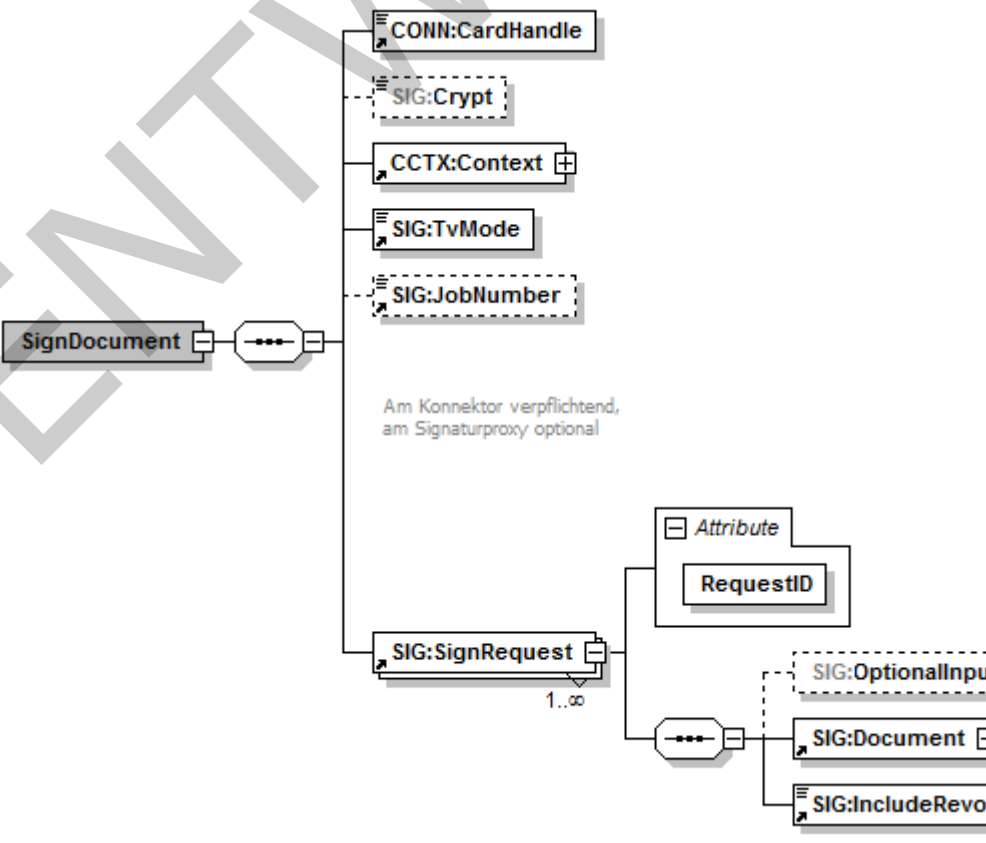
Name	SignatureService	
Version (KDV)	7.4.0 (WSDL-Version), 7.4.2 (XSD-Version) 7.4.1 (WSDL-Version), 7.4.3 (XSD-Version) 7.5.01 (WSDL- und XSD-Version) Siehe Anhang D	
Namensraum	Siehe Anhang D	
Namensraum-Kürzel	SIG für Schema und SIGW für WSDL	
Operationen	Name	Kurzbeschreibung
	SignDocument	Dokument signieren
	VerifyDocument	Signatur verifizieren
	StopSignature	Signieren eines Dokumentenstapels abbrechen
	GetJobNumber	Liefert eine Jobnummer für den nächsten Signiervorgang
	ActivateComfortSignature	Aktiviert die Komfortsignatur für einen HBA
	DeactivateComfortSignature	Deaktiviert die Komfortsignatur für einen oder mehrere HBA
	GetSignatureMode	Liefert den Status der Komfortsignaturfunktion und den Signaturmodus für einen oder mehrere HBA
WSDL	SignatureService_V7_5_01.wsdl SignatureService_V7_4_1.wsdl SignatureService.wsdl (WSDL-Version 7.4.0)	
Schema	SignatureService_V7_5_01.xsd SignatureService_V7_4_3.xsd SignatureService.xsd (XSD-Version 7.4.2)	

[<=]

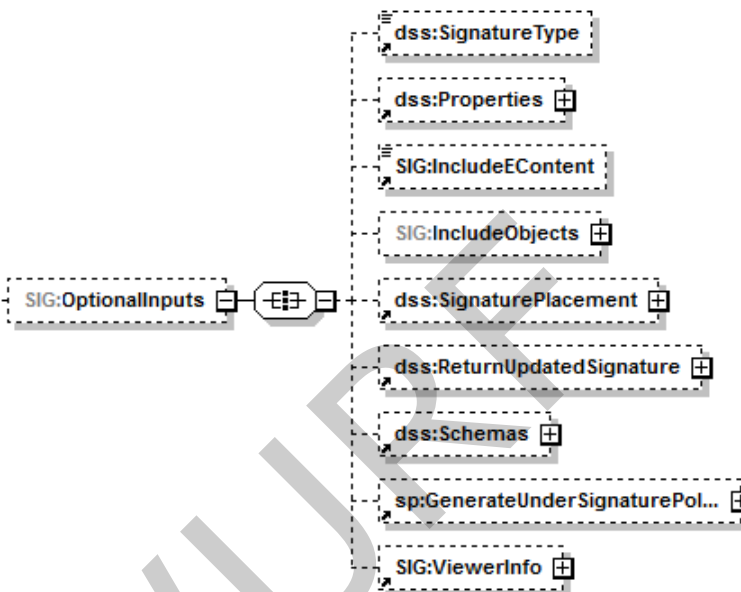
4.1.8.5.1 SignDocument (nonQES und QES)

TIP1-A 5010-04 ~~**TIP1-A-5010-03**~~ - Operation SignDocument (nonQES und QES)
Der Signaturdienst des Konnektors MUSS an der Clientschnittstelle eine an [OASIS-DSS] angelehnte Operation SignDocument anbieten.

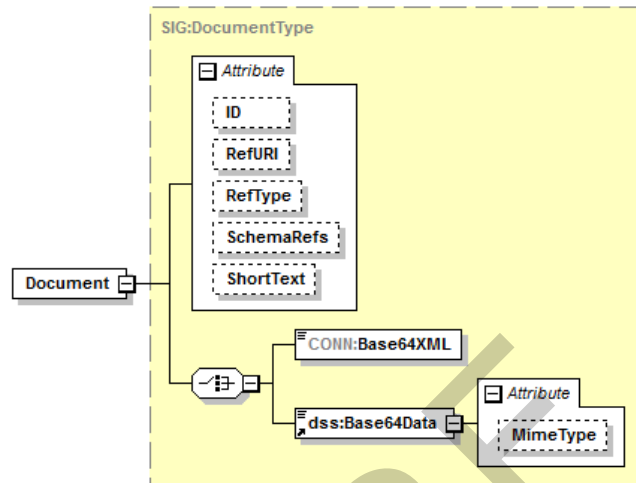
4511 Tabelle 229: TAB_KON_065 Operation SignDocument (nonQES und QES)

Name	SignDocument
Beschreibung	<p>Diese Operation lehnt sich an [OASIS-DSS] an. Sie enthält voneinander unabhängige SignRequests. Jeder SignRequest erzeugt eine Signatur für ein Dokument.</p> <p>Für die qualifizierte elektronische Signatur (QES) werden die QES_DocFormate unterstützt. Für nicht-qualifizierte elektronische Signaturen (nonQES) werden die nonQES_DocFormate unterstützt.</p> <p>Zur Signaturerzeugung werden Schlüssel und Zertifikate einer Chipkarte benutzt.</p> <p>Unterstützte Karten sind für die QES der HBAX mit dem QES-Zertifikat. Für die nonQES wird für die Signaturtypen „XML-Signatur, CMS-Signatur, PDF-Signatur, S/MIME-Signatur“ die SM-B mit dem OSIG-Zertifikat unterstützt.</p> <p>Bei der Erstellung von XML-Signaturen MUSS Canonical XML 1.1 verwendet werden [CanonXML1.1].</p> <p>Es soll der Common-PKI-Standard eingesetzt werden, siehe [Common-PKI].</p> <p>In Summe für die Größe der Dokumente in allen SignRequests innerhalb einer SignDocument-Anfrage MUSS der Konnektor eine Gesamtgröße von ≤ 250 MB unterstützen.</p>
Aufrufparameter	 <p>Am Konnektor verpflichtend, am Signaturproxy optional</p>

Name	Beschreibung
CONN: Card Handle	Identifiziert die zu verwendende Signaturkarte. Die Operation DARF die Signatur mit der eGK NICHT unterstützen. Wird die Operation mit einem nicht unterstützten Kartentypen aufgerufen, so MUSS der Konnektor die Bearbeitung mit dem Fehler 4126 abbrechen.
SIG: Crypt	Der Parameter crypt steuert die Auswahl der Zertifikate und Schlüssel für die Signaturerstellung abhängig von der durch cardHandle adressierten Karte gemäß TAB_KON_900. Defaultwert: <ul style="list-style-type: none"> gemäß TAB_KON_862 für die QES gemäß TAB_KON_863 für die nonQES.
CCTX: Context	<u>Aufrufkontext QES mit HBAX:</u> MandantId, ClientSystemId, WorkplaceId, UserId verpflichtend <u>Aufrufkontext nonQES mit SM-B:</u> MandantId, ClientSystemId, WorkplaceId verpflichtend; UserId nicht ausgewertet
TvMode	Der Parameter wird im Konnektor nicht ausgewertet.
SIG: JobNumber	Die Nummer des Jobs, unter der der nächste Signaturvorgang gestartet wird. Parameter ist verpflichtend.
SIG: Sign Request	Ein SignRequest kapselt den Signaturauftrag für ein Dokument. Das verpflichtende XML-Attribut RequestID identifiziert einen SignRequest innerhalb eines Stapels von SignRequests eindeutig. Es dient der Zuordnung der SignResponse zum jeweiligen SignRequest. Enthält der Aufruf mehr als die unterstützte Anzahl von SignRequests, bricht die Operation mit Fehler 4000 ab. Es sind mindestens 50 SignRequests zu unterstützen.

	SIG: Optional Inputs	<p>Enthält optionale Eingangsparameter (angelehnt an dss:OptionalInputs gemäß [OASIS-DSS] Section 2.7):</p> 
--	----------------------------	---

SIG:
Document



Dieses an das `dss:Document` Element aus [OASIS-DSS] Section 2.4.2 angelehnte Element enthält das zu signierende Dokument, wobei die Kindelemente `CONN:Base64XML` und `dss:Base64Data` auftreten können.

Bei den als `dss:Base64Data` übergebenen Dokumenten werden folgende (Klassen von) MIME-Types unterschieden:

- "application/pdf-a" – für PDF/A-Dokumente,
- "text/plain",
"text/plain; charset=iso-8859-15" oder
"text/plain; charset=utf-8" – für Text-Dokumente,
- "image/tiff" – für TIFF-Dokumente und
- ein beliebiger anderer MIME-Type für nicht näher unterschiedene Binärdaten des spezifizierten Typs.

Der MIME-Type „text/plain“ wird interpretiert als „text/plain; charset=iso-8859-15“.

Das Element enthält ein Attribut `ShortText`. Es muss für QES-Signaturen bei jedem Aufruf vom Clientsystem übergeben werden, für nonQES-Signaturen ist es optional.

Über das Attribut `RefURI` kann gemäß [OASIS-DSS] (Abschnitt 2.4.1) ein zu signierender Teilbaum eines XML-Dokuments ausgewählt werden. Wenn die Signatur eines Teilbaums für die Signaturvariante nicht unterstützt wird, muss der Signaturauftrag mit Fehler 4111 abgelehnt werden.

	SIG: Include Revocation Info	<p>Durch diesen verpflichtenden Schalter kann der Aufrufer die Einbettung von zum Zeitpunkt der Signaturerstellung vorliegenden Sperrinformationen anfordern. Es wird ausschließlich die zu erstellende Signatur betrachtet, d.h. es erfolgt keine Einbettung von Sperrinformationen für bereits enthaltene Signaturen.</p> <p>Für nicht-qualifizierte elektronische Signaturen (nonQES) wird diese Funktionalität nicht unterstützt. Für PDF-Signaturen werden keine Sperrinformationen eingebettet.</p>
--	---------------------------------------	---

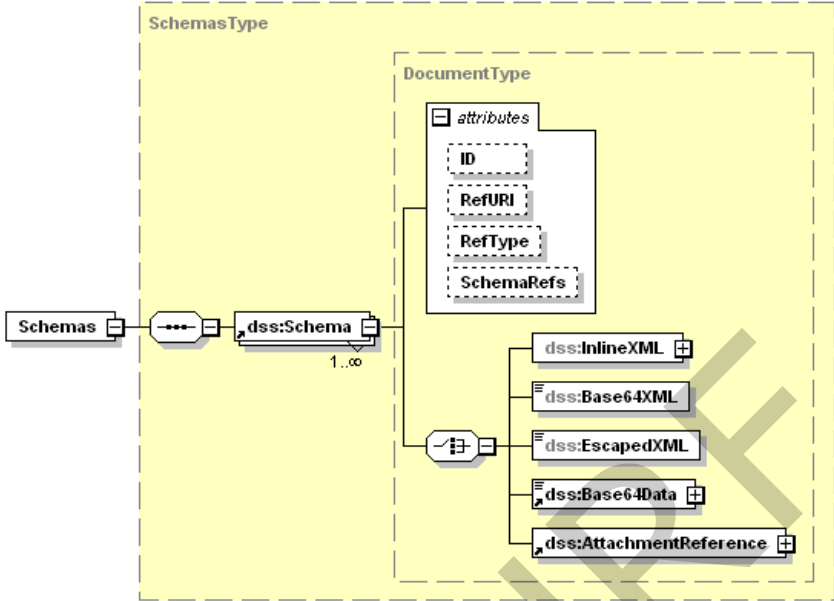
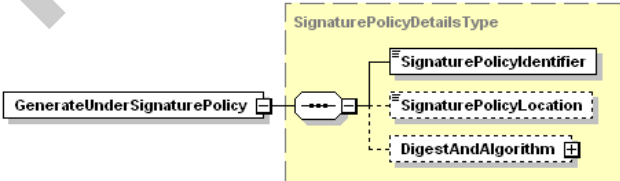
ENTWURF

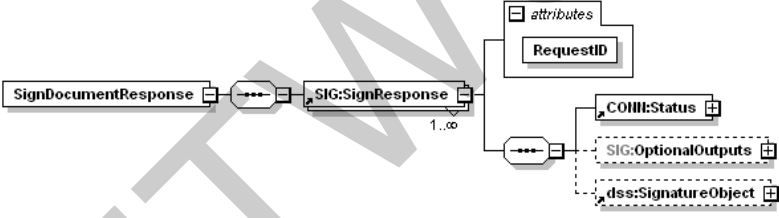
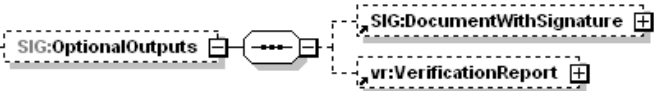
	dss: Signature Type	<p>Durch dieses in [OASIS-DSS] (Abschnitt 3.5.1) beschriebene Element kann der generelle Typ der zu erzeugenden Signaturen spezifiziert werden. Hierbei MÜSSEN folgende Signaturtypen unterstützt werden:</p> <ul style="list-style-type: none"> XML-Signatur Durch Übergabe der URI urn:ietf:rfc:3275 wird die Erstellung von XML-Signaturen gemäß [RFC3275], [XMLDSig] angestoßen. Das zu verwendende Profil ist XAdES-BES ([XAdES]). Die Rückgabe einer solchen Signatur erfolgt als <code>ds:Signature</code>-Element. CMS-Signatur Durch Übergabe der URI urn:ietf:rfc:5652 wird eine CMS-Signatur gemäß [RFC5652] angestoßen. Das zu verwendende Profil ist CAdES-BES ([CAdES]). Die Signatur wird als <code>dss:Base64Signature</code> mit der oben genannten URI als <code>Type</code> zurückgeliefert. S/MIME-Signatur Durch Übergabe der URI „urn:ietf:rfc:5751“ wird eine S/MIME-Signatur gemäß [RFC5751] angestoßen. Die CMS-Signatur der übergebenen MIME-Nachricht erfolgt konform der Vorgaben zur CMS-Signatur. Das Rückgabedokument ist eine MIME-Nachricht vom Typ „application/pkcs7-mime“ mit einer CMS-Struktur vom Typ <code>SignedData</code>. Ist das übergebene Dokument keine MIME-Nachricht, so wie der Fehler 4111 (Ungültiger Signaturtyp oder Signaturvariante) zurückgeliefert. PDF-Signatur Durch Übergabe der URI http://uri.etsi.org/02778/3 wird die Erzeugung einer PAdES-Basic Signatur gemäß [PAdES-3] angestoßen, wobei das Dokument mit der integrierten Signatur als <code>dss:Base64Signature</code> mit der oben genannten URI als <code>Type</code> zurückgeliefert wird. Handelt es sich beim übergebenen Dokument nicht um ein <code>Base64Data</code>-Element mit MIME-Type „application/pdf-a“, so wird ein Fehler 4111 (Ungültiger Signaturtyp oder Signaturvariante) zurückgeliefert. <p>Andere <code>SignatureType</code>-Angaben führen zu einer Fehlermeldung 4111 (Ungültiger Signaturtyp oder Signaturvariante).</p>
--	---------------------------	--

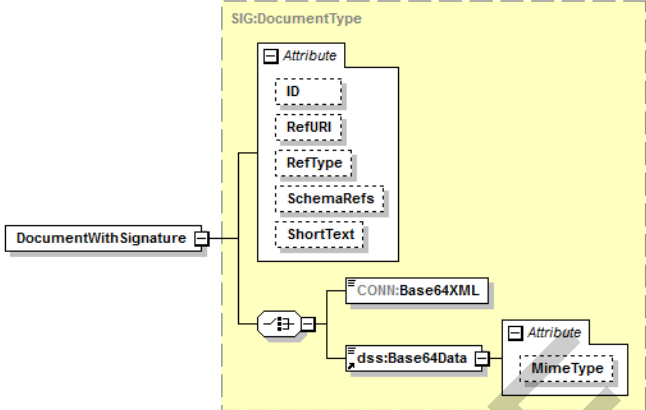
		<p>Die Signaturtypen „XML-Signatur, CMS-Signatur, PDF-Signatur, S/MIME-Signatur“ DÜRFEN für QES der HBAX nur mit dem QES-Zertifikat erfolgen, für nonQES nur mit dem OSIG-Zertifikat der SM-B. In jedem diese Anforderung verletzenden Fall MUSS der Fehler 4058 (Aufruf nicht zulässig) zurückgeliefert werden. Fehlt dieses Element, so wird der Signaturtyp gemäß TAB_KON_583 – Default-Signaturverfahren aus dem Dokumententyp abgeleitet.</p>
--	--	--

dss: Properties	<p>Durch dieses in [OASIS-DSS] (Abschnitt 3.5.5) definierte Element können zusätzliche signierte und unsignierte Eigenschaften (Properties) bzw. Attribute in die Signatur eingefügt werden.</p> <p>Unterstützt werden genau folgende Attribute: Im CMS-Fall (SignatureType = urn:ietf:rfc:5652) kann es XML-Elemente ./SignedProperties/Property/Value/CMSAttribute und ./UnsignedProperties/Property/Value /CMSAttribute enthalten. Ein solches XML-Element CMSAttribute muss ein vollständiges, base64/DER-kodiertes ASN.1-Attribute enthalten, definiert in [CMS#5.3.SignerInfo Type]. Es muss bei der Erstellung des CMS-Containers unverändert unter SignedAttributes bzw. UnsignedAttributes aufgenommen werden.</p> <p><u>Die Übergabe der Attribute</u></p> <ul style="list-style-type: none"> • <u>ContentType</u> • <u>SigningTime</u> • <u>MessageDigest</u> • <u>SigningCertificate und SigningCertificateV2</u> <p><u>wird ignoriert und es wird die Warnung 4273 zurück gegeben.</u></p>
SIG: Include EContent	<p>Durch dieses in [OASIS-DSS] (Abschnitt 3.5.7), definierte Element kann bei einer CMS-basierten Signatur das Einfügen des signierten Dokumentes in die Signatur angefordert werden.</p> <p>Die Verwendung dieses Parameters bei anderen Signaturtypen führt zu einem Fehler 4111 (Ungültiger Signaturtyp oder Signaturvariante).</p>
SIG: Include Object	<p>Dieses Element enthält zum Anfordern einer Enveloping XML Signatur ein dss:IncludeObject-Element gemäß [OASIS-DSS] (Abschnitt 3.5.6). Ist das Element vorhanden und ein anderer Signaturtyp als eine XML-Signatur angefordert, so wird der Fehler 4111 (Ungültiger Signaturtyp oder Signaturvariante) zurückgeliefert.</p>

dss: Signature Placement	<p>Durch dieses in [OASIS-DSS] (Abschnitt 3.5.8) definierte Element kann bei XML-basierten Signaturen gemäß [RFC3275] die Platzierung der Signatur im Dokument angegeben werden.</p> <p>Die in [OASIS-DSS] (Abschnitt 2.5, XPath c) beschriebene Deklaration von Namespace-Prefixes im dss:SignaturePlacement-Element muss nicht unterstützt werden.</p> <p>Bei anderen Signaturtypen wird das Element ignoriert und eine Warnung (Fehlercode 4197, Parameter SignaturePlacement wurde ignoriert) zurückgeliefert.</p> <p>dss:SignaturePlacement darf nur zusammen mit einer unterstützten Signaturrichtlinie verwendet werden (sp:SignaturePolicyIdentifier muss entsprechend gesetzt sein).</p>
dss: Return Updated Signature	<p>Durch dieses in [OASIS-DSS] (Abschnitt 4.5.8) definierte Element kann eine übergegebene XML- oder CMS-Signatur mit zusätzlichen Informationen und Signaturen (Parallel- und Gegensignaturen) versehen werden. Hierbei sind folgende Ausprägungen für das Type-Attribut vorgesehen:</p> <ul style="list-style-type: none"> • http://ws.gematik.de/conn/sig/sigupdate/parallel/ Hierdurch wird eine Parallelsignatur zu einer bereits existierenden Signatur erzeugt und entsprechend zurückgeliefert. • http://ws.gematik.de/conn/sig/sigupdate/counter/documentexcluding Hierdurch wird eine dokumentenexkludierende Gegensignatur für alle vorhandenen parallelen Signaturen erzeugt. <p>Bei anderen Type-Attributen wird der Fehler 4111 (Ungültiger Signaturtyp oder Signaturvariante) zurückgeliefert.</p>
dss: Schemas	<p>Durch das in [OASIS-DSS] (Abschnitt 2.8.5) definierte Element können eine Menge von XML-Schemata übergeben werden, die zur Validierung der übergebenen XML-Dokumente verwendet werden können.</p>

	 <p>The diagram shows a SchemasType container. Inside, there is a DocumentType container. The DocumentType contains an attributes group with ID, RefURI, RefType, and SchemaRefs. It also contains a choice of five elements: dss:InlineXML, dss:Base64XML, dss:EscapedXML, dss:Base64Data, and dss:AttachmentReference. Outside the DocumentType, there is a Schemas element connected to a dss:Schema element (multiplicity 1..∞).</p>
dss:Schema	<p>Dieses Element enthält ein XML-Schema zur Validierung des übergebenen XML-Dokuments. Das Attribut RefURI ist verpflichtend. Es kennzeichnet dabei den Namensraum des XML-Schemas entsprechend [OASIS-DSS] (Abschnitt 2.8.5)</p>
sp:GenerateUnderSignaturePolicy	 <p>The diagram shows a GenerateUnderSignaturePolicy element connected to a SignaturePolicyDetailsType container. The SignaturePolicyDetailsType contains a choice of three elements: SignaturePolicyIdentifier, SignaturePolicyLocation, and DigestAndAlgorithm.</p> <p>Über dieses in [OASIS-SP], Kapitel 2.2.1.1.1 Optional Input <GenerateUnderSignaturePolicy>, definierte Element wird die erforderliche Singnaturrichtlinie ausgewählt. Die im Element sp:SignaturePolicyIdentifier übergebene URI identifiziert die Signaturrichtlinie. Die XML-Elemente SignaturePolicyLocation DigestAndAlgorithm werden nicht verwendet. Wenn eine nach TAB_KON_778 notwendige Signaturrichtlinie fehlt oder die übergebene Signaturrichtlinie unbekannt ist, wird Fehler</p>

		4111 zurückgeliefert.
	SIG: Viewer Info	Enthält optional die vom Konnektor in die Signatur einzubeziehende Referenzen für die Stylesheets zur Anzeige.
Rückgabe		
	SIG: Sign Response	Eine <code>SignResponse</code> kapselt den ausgeführten Signaturauftrag pro Dokument. Die Zuordnung zwischen <code>SignRequest</code> und <code>SignResponse</code> erfolgt über die <code>RequestID</code> .
	CONN: Status	Enthält den Status der ausgeführten Operation pro <code>SignRequest</code> .
	SIG: Optional Outputs	Enthält (angelehnt an <code>dss:OptionalOutputs</code>) optionale Ausgangsparameter: 

	SIG: Document With Signature	 <p>Pro SignResponse wird ein Element <code>SIG:DocumentWithSignature</code> gemäß [OASIS-DSS] (Abschnitt 3.5.8) zurückgeliefert, in dem das Dokument mit Signatur enthalten ist. Dabei werden die XML-Attribute des Elements <code>SIG:Document</code> auf dem zugehörigen <code>SignRequest</code> übernommen.</p> <p>Ist die Signatur nicht im Dokument enthalten, wird ein leeres Element <code>Base64XML</code> oder <code>Base64Data</code> zurückgegeben. Die Signatur wird dann im Element <code>dss:SignatureObject</code> abgelegt.</p> <p>Wenn die Signatur im Dokument enthalten ist, wird das signierte Dokument im Feld <code>Base64XML</code> bzw. <code>Base64Data</code> zurückgeliefert. In diesem Fall MUSS die <code>dss:SignaturePtr</code>-Alternative in <code>dss:SignatureObject</code> (vgl. [OASIS-DSS] Abschnitt 2.5) dazu genutzt werden, auf die in den Dokumenten enthaltenen Signaturen zu verweisen.</p>
	vr: Verifi cation Report	Vom Konnektor nicht befüllt.
	dss: Signature Object	Enthält im Erfolgsfall die erzeugte Signatur pro <code>SignRequest</code> in Form eines <code>dss:SignatureObject</code> -Elementes gemäß [OASIS-DSS] (Abschnitt 3.2).
Vorbe- dingungen	Keine	
Nachbe- dingungen	Keine	

4512 Der Ablauf der Operation SignDocument ist in Tabelle TAB_KON_756 Ablauf Operation
 4513 SignDocument (nonQES und QES) beschrieben:

4514

4515 **Tabelle 230: TAB_KON_756 Ablauf Operation SignDocument (nonQES und QES)**

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Anhand des Kartentyps wird ermittelt, ob eine QES oder eine nonQES erzeugt werden soll. Alle übergebenen Parameterwerte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	TUC_KON_000 „Prüfe Zugriffs- berechtigung“	Die Prüfung erfolgt durch den Aufruf TUC_KON_000 { mandantId = \$context.mandantId; clientsystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; userId = \$context.userId; cardHandle = \$cardHandle } Tritt bei der Prüfung ein Fehler auf, bricht die Operation mit Fehlercode aus TUC_KON_000 ab.
3.	TUC_KON_026 „Liefere CardSession“	Ermittle CardSession über TUC_KON_026 { mandatId = \$context.mandantId; clientsystemId = \$context.clientsystemId; cardHandle = \$context.cardHandle; userId = \$context.userId }
Im Fall QES wird Schritt 4 ausgeführt. Im Fall nonQES wird Schritt 5 ausgeführt.		
4a)	Prüfe Signaturdienst- Modul	Prüfe, ob MGM_LU_SAK=Enabled. Ist dies nicht der Fall, so bricht die Operation mit Fehler 4125 ab.
Wenn für die CardSession die Komfortsignatur aktiviert ist (CARDESSION.SIGNMODE = Comfort) wird Schritt 4 c) ausgeführt. Andernfalls wird Schritt 4 b) ausgeführt.		
4b)	TUC_KON_150 „Dokumente QES signieren“	Die QES wird erzeugt. Tritt hierbei ein Fehler auf, bricht die Operation ab.
4c)	TUC_KON_170 „Dokumente mit Komfort signieren“	Eine Komfortsignatur wird erzeugt. Tritt hierbei ein Fehler auf, bricht die Operation ab.

5)	TUC_KON_160 „Dokumente nonQES signieren“	Die nonQES wird erzeugt. Tritt hierbei ein Fehler auf, bricht die Operation ab.
----	--	--

4516 **Tabelle 231: TAB_KON_757 Fehlercodes „SignDocument (nonQES und QES)“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen TUCs können folgende weiteren Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler
4111	Technical	Error	ungültiger Signaturtyp oder Signaturvariante
4126	Security	Error	Kartentyp nicht zulässig für Signatur
4125	Technical	Error	LU_SAK nicht aktiviert
4197	Technical	Warning	Parameter SignaturePlacement wurde ignoriert
4252	Technical	Error	Jobnummer wurde in den letzten 1.000 Aufrufen bereits verwendet und ist nicht zulässig
4273	Technical	Warning	Attribute im Parameter dss:Properties wurden ignoriert

4517
4518 Die zulässigen Zertifikate und Schlüssel sind in TAB_KON_900 aufgelistet.
4519 [\leq]

4520 4.1.8.5.2 VerifyDocument (nonQES und QES)

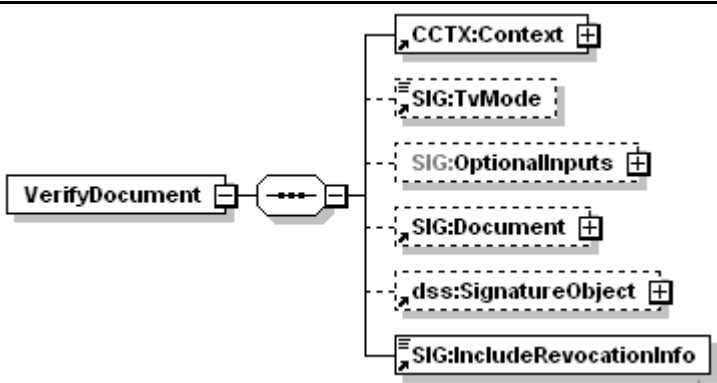
4521 TIP1-A_5034-03 - Operation VerifyDocument (nonQES und QES)

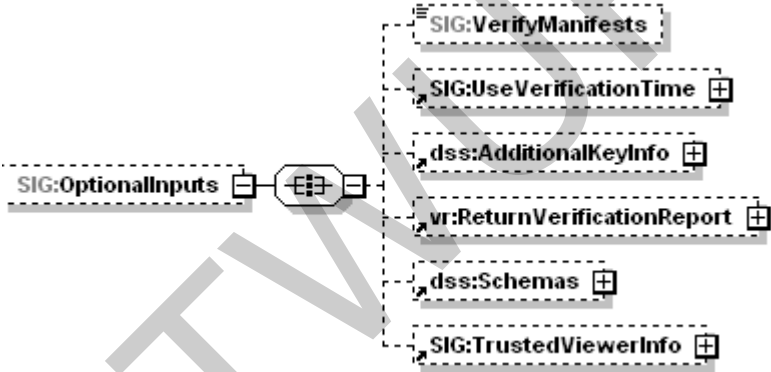
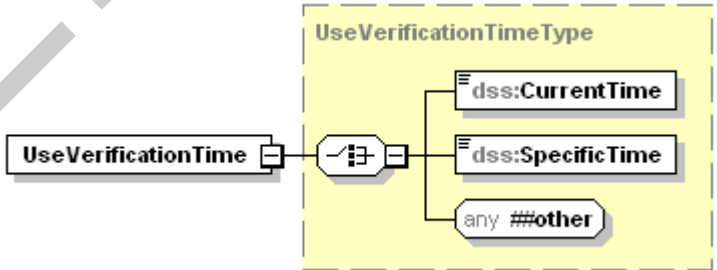
4522 Der Signaturdienst des Konnektors MUSS an der Clientschnittstelle eine an [OASIS-DSS]
4523 angelehnte Operation VerifyDocument (nonQES und QES) anbieten.

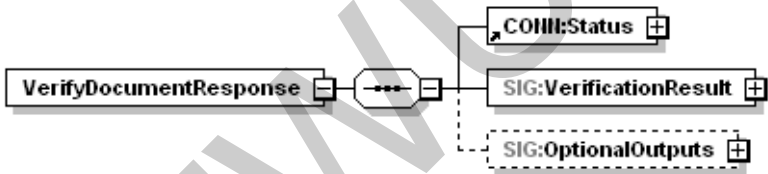
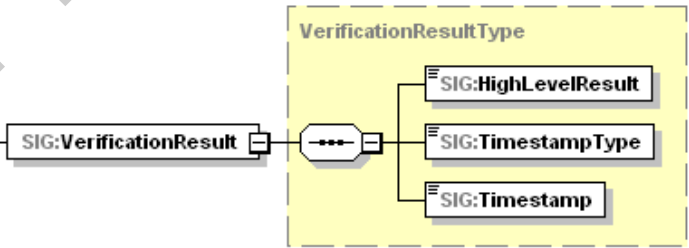
4524

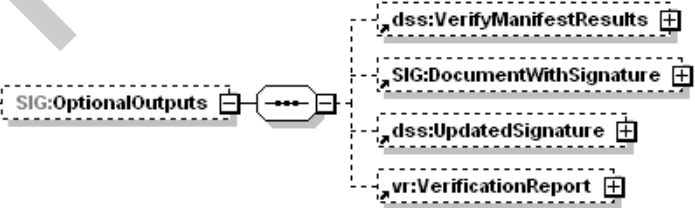
4525 **Tabelle 232: TAB_KON_066 Operation VerifyDocument (nonQES und QES)**

Name	VerifyDocument
Beschreibung	Diese Operation verifiziert die Signatur eines Dokumentes. Der Konnektor MUSS jede konform zur Außenschnittstelle SignDocument erzeugte Signatur durch VerifyDocument prüfen können. Außerdem MÜSSEN die zusätzlich geforderten Signaturverfahren zur Dokumentensignaturprüfung unterstützt werden Das Ergebnis der Prüfung wird, wenn gefordert, in Form eines standardisierten Prüfberichts in einer <i>VerificationReport</i> -Struktur gemäß [OASIS-VR] zurückgeliefert.

Aufruf- parameter		
	Name	Beschreibung
	CCTX: Context	MandantId, ClientSystemId, WorkplaceId verpflichtend; UserId nicht ausgewertet
	TvMode	Der Parameter wird im Konnektor nicht ausgewertet.
	SIG: Optional Inputs	Enthält optionale Eingabeparameter (angelehnt an dss:OptionalInputs gemäß [OASIS-DSS] Section 2.7): Die zulässigen optionalen Eingabeparameter sind unten erläutert.
	SIG: Document	Enthält im Fall der Prüfung von detached oder enveloped Signaturen das zur Signatur gehörende bzw. das diese umschließende Dokument (siehe [OASIS-DSS] Section 2.4.2 und oben).
	dss: Signature Object	Enthält die zu prüfende Signatur, wenn sie nicht im Dokument selbst eingebettet ist ([OASIS-DSS] Kapitel 4.1). Hierbei werden XML-Signaturen als ds:Signature Element und alle anderen Signaturen als dss:Base64Signature mit entsprechend gesetztem Type-Attribut (siehe SignatureType, Operationen SignDocument und ExternalAuthenticate) übergeben, wobei die nachfolgenden Werte unterstützt werden müssen: <ul style="list-style-type: none"> • CMS-Signatur urn:ietf:rfc:5652 • S/MIME-Signatur urn:ietf:rfc:5751 • PDF-Signatur http://uri.etsi.org/02778/3 • PKCS#1-Signatur (siehe Operation ExternalAuthenticate) urn:ietf:rfc:3447

		<ul style="list-style-type: none"> ECC-Signatur (siehe Operation ExternalAuthenticate) urn:bsi:tr:03111:ecdsa
SIG: Include Revocat ionInfo		<p>Durch diesen verpflichtenden Schalter kann der Aufrufer die Einbettung von zum Zeitpunkt der Signaturprüfung vorliegenden Sperrinformationen anfordern.</p> <p>Ist bereits eine Sperrinformation eingebettet, so wird die neue Sperrinformation zusätzlich eingebettet.</p> <p>Für in einer Gegensignatur enthaltene Signaturen erfolgt keine Einbettung von Sperrinformationen. Für PDF-Signaturen erfolgt keine Einbettung von Sperrinformationen. Der Konnektor nimmt die Warnung 4261 in die Antwort auf.</p>
		
SIG: Verify Mani fests		<p>Durch das in [OASIS-DSS] (Abschnitt 4.5.1) definierte Element kann die Prüfung eines ggf. vorhandenen Manifests angefordert werden.</p>
		
SIG: Use Verifi cation Time		<p>Durch das in [OASIS-DSS] (Abschnitt 4.5.2) spezifizierte Element kann die Prüfung der Signatur bezüglich eines durch den Aufrufer bestimmten Zeitpunktes (Benutzerdefinierter_Zeitpunkt) erfolgen.</p>
dss: Addit		<p>Durch das in [OASIS-DSS] (Abschnitt 4.5.4) spezifizierte Element kann zusätzliches, für die</p>

	ional KeyInfo	Prüfung benötigtes, Schlüsselmaterial übergeben werden.
	vr: Return Verifi cation Report	Durch dieses in [OASIS-VR] spezifizierte Element kann die Erstellung eines ausführlichen Prüfberichts angefordert werden. Der Konnektor MUSS die Anforderungen der Konformitätsstufe 2 („Comprehensive“) erfüllen und die Profilierung aus Anhang B3 beachten.
	dss: Schemas	Durch das in [OASIS-DSS] (Abschnitt 2.8.5) definierte Element können eine Menge von XML-Schematas übergeben werden, die zur Validierung des übergebenen XML-Dokumentes verwendet werden können. Zur Struktur dieses Elements siehe Beschreibung des Parameters <code>dss:Schemas</code> der Operation <code>SignDocument</code> .
	SIG: Viewer Info	Der Parameter wird im Konnektor nicht ausgewertet.
Rückgabe		
	Status	Enthält den Ausführungsstatus der Operation.
	SIG: Verifi cation Result	 <p>Das Element <code>Sig:VerificationResult</code> enthält das Ergebnis der Prüfung als Ampel, den Typ des zugehörigen angenommenen Signaturzeitpunkts und der angenommene Signaturzeitpunkt selbst.</p>
	SIG: High Level Result	<p>Das Ergebnis der Prüfung (Ampelschaltung) mit folgenden Werten:</p> <ul style="list-style-type: none"> • VALID: alle Signaturen sind gültig • INVALID: mindestens eine der Signaturen ist ungültig • INCONCLUSIVE: in allen anderen Fällen

	SIG: Time stamp Type	<p>Der Typ des angenommenen Signaturzeitpunkts mit folgenden Werten:</p> <ul style="list-style-type: none"> • SIGNATURE_EMBEDDED_TIMESTAMP: in der Signatur eingebetter Zeitpunkt Ermittelter_Signaturzeitpunkt _Eingebettet • SYSTEM_TIMESTAMP: Systemzeit des Konnektors bei Signaturprüfung Ermittelter_Signaturzeitpunkt _System • USER_DEFINED_TIMESTAMP: benutzerdefinierter Zeitpunkt Benutzerdefinierter_Zeitpunkt <p>Als Format darf jedes zum XML-Typ "dateTime" konforme Format verwendet werden (<element name="Timestamp" type="dateTime"/>). Wenn mehrere Signaturen im Dokument vorhanden sind, wird hier der angenommene Signaturzeitpunkt der jüngsten Signatur angegeben.</p>
	SIG: Time stamp	Im Element SIG:Timestamp wird der zu SIG:TimestampType gehörende Zeitstempel zurückgegeben.
	SIG: Optio nal Outputs	<p>Enthält (angelehnt an dss:OptionalOutputs, wie in Abschnitt 2.7 von [OASIS-DSS] beschrieben) optionale Ausgangselemente:</p> 
	dss: Verify Manifest Results	Dieses in Abschnitt 4.5.1 von [OASIS-DSS] definierte Element enthält Informationen zur Prüfung eines ggf. vorhandenen Signaturmanifests und wird zurückgeliefert, sofern beim Aufruf das dss:VerifyManifest-Element, aber nicht das RequestVerificationReport als optionales Eingabeelement übergeben wurde.
	SIG: Document With Signa ture	Dieses in Abschnitt 4.5.8 von [OASIS-DSS] spezifizierte Element wird zurückgeliefert, falls eine in dem Dokument enthaltene Signatur (Enveloped Signature) in Verbindung mit dem SIG:IncludeRevocationInfo-Element geprüft wurde.

	dss: Updated Signature	Dieses in Abschnitt 4.5.8 von [OASIS-DSS] spezifizierte Element wird zurückgeliefert, falls eine abgesetzte (Detached Signature) oder umschließende (Enveloping Signature) in Verbindung mit dem SIG:IncludeRevocationInfo- Element geprüft wurde.
	vr: Verifi cation Report	Dieses in [OASIS-VR] spezifizierte Element wird zurückgeliefert, falls das ReturnVerificationReport-Element als Eingabeparameter verwendet wurde. Die Profilierung von Anhang B3 MUSS beachtet werden.
Vorbe- dingungen	Keine	
Nachbe- dingungen	Keine	

4526 **Tabelle 233: TAB_KON_760 Ablauf Operation VerifyDocument (nonQES und QES)**

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	TUC_KON_000 „Prüfe Zugriffs- berechtigung“	Die Prüfung erfolgt durch den Aufruf TUC_KON_000 { mandantId = \$context.mandantId; clientsystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; needCardSession= false; } Tritt bei der Prüfung ein Fehler auf, bricht die Operation mit Fehlercode aus TUC_KON_000 ab.
3.	prüfe, ob QES oder nonQES	Ist im jeweiligen Signaturzertifikat mindestens ein QCStatement mit dem OID id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) enthalten, handelt es sich um eine QES-Signatur, andernfalls liegt eine nonQES-Signatur vor.
Für QES-Signaturen wird Schritt 4 ausgeführt. Für nonQES-Signaturen wird Schritt 5 ausgeführt.		
4.a	Prüfe Signaturdienst- Modul	Prüfe, ob MGM_LU_SAK=Enabled. Ist dies nicht der Fall, so bricht die Operation mit Fehler 4125 ab.
4.b	TUC_KON_151 „QES Dokumentensignatur prüfen“	Die QES wird geprüft. Tritt hierbei ein Fehler auf, bricht die Operation ab.

5.	TUC_KON_161 „nonQES Dokumentensignatur prüfen“	Die nonQES wird geprüft. Tritt hierbei ein Fehler auf, bricht die Operation ab.
----	---	--

4527

4528 **Tabelle 234: TAB_KON_761 Fehlercodes „VerifyDocument (nonQES und QES)“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen TUCs (siehe Tabelle TAB_KON_760 Ablauf Operation VerifyDocument) können folgende weiteren Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler
4261	Technical	Warning	Einbettung von Revocation-Informationen nicht unterstützt
4125	Technical	Error	LU_SAK nicht aktiviert

4529

4530

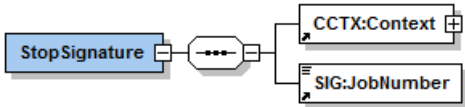
4531 [**<=**]4532 **4.1.8.5.3 StopSignature**

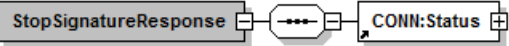
4533 TIP1-A_5666 - Operation StopSignature (nonQES und QES)

4534 Der Signatordienst des Konnektors MUSS an der Clientschnittstelle eine Operation
4535 StopSignature anbieten.

4536

4537 **Tabelle 235: TAB_KON_840 Operation StopSignature**

Name	StopSignature		
Beschreibung	Diese Operation unterbricht die Signatur eines Dokumentenstapels. Der Konnektor MUSS jede Signaturerstellung für ein Dokumentenstapel unterbrechen können.		
Aufrufparameter	 <pre> sequenceDiagram participant StopSignature StopSignature->>CCTX:Context StopSignature->>SIG:JobNumber </pre>		
	Name	Beschreibung	
	CCTX:Context	MandantId, ClientSystemId, WorkplaceId verpflichtend; UserId nicht ausgewertet	
	SIG:JobNumber	Die Nummer des Jobs, der gestoppt werden soll.	

Rückgabe		
	CONN:Status	Enthält den Ausführungsstatus der Operation.
Vorbedingungen	Keine	
Nachbedingungen	Keine	

4538 **Tabelle 236: TAB_KON_841 Ablauf Operation StopSignature**

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	Stoppe die Stapelsignaturverarbeitung	Die Verarbeitung der Stapelsignatur wird abgebrochen

4539

4540 **Tabelle 237: TAB_KON_842 Fehlercodes „StopSignature“**

Fehlercode	ErrorType	Severity	Fehlertext
Folgende Fehlercodes können auftreten:			
4000	Technical	Error	Syntaxfehler
4243	Technical	Error	Jobnummer unbekannt

4541 [**<=**]4542 **4.1.8.5.4 GetJobNumber**


4543 TIP1-A_5667 - Operation GetJobNumber

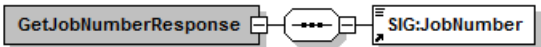
4544 Der Signatordienst des Konnektors MUSS an der Clientschnittstelle eine Operation

4545 GetJobNumber anbieten.

4546

4547 **Tabelle 238: TAB_KON_843 Operation GetJobNumber**

Name	GetJobNumber	
Beschreibung	Diese Operation liefert eine Jobnummer zur Verwendung in der Operation SignDocument. Die Jobnummer MUSS nach den Vorgaben von Kapitel 4.1.8.1.4 erstellt werden.	
Aufrufparameter		
	Name	Beschreibung

	CCTX:Context	MandantId, ClientSystemId, WorkplaceId verpflichtend; UserId nicht ausgewertet
Rückgabe		
	SIG:JobNumber	Jobnummer zur Verwendung in „SignDocument“
Vorbedingungen	Keine	
Nachbedingungen	Keine	

4548 **Tabelle 239: TAB_KON_844 Ablauf Operation GetJobNumber**

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	Generiere und liefere eine Jobnummer	Eine innerhalb von 1000 Aufrufen eindeutige Jobnummer wird generiert und geliefert. Die Zählung der Aufrufe erfolgt dabei unabhängig vom Aufrufkontext.

4549

4550 **Tabelle 240: TAB_KON_845 Fehlercodes „GetJobNumber“**

Fehlercode	ErrorType	Severity	Fehlertext
Folgende Fehlercodes können auftreten:			
4000	Technical	Error	Syntaxfehler

4551

4552 **[<=]**4553 **4.1.8.5.5 ActivateComfortSignature**

4554 A_19107 - Operation ActivateComfortSignature

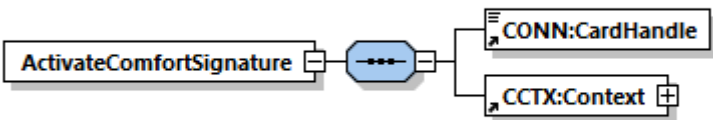
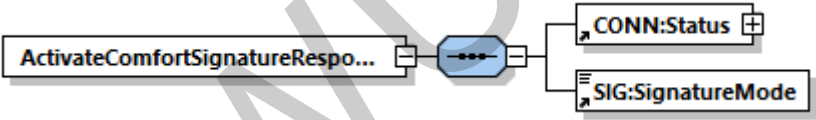
4555 Der Signaturdienst des Konnektors MUSS an der Clientschnittstelle eine Operation

4556 ActivateComfortSignature anbieten.

4557

4558 **Tabelle 241: TAB_KON_874 ActivateComfortSignature**

Name	ActivateComfortSignature
-------------	--------------------------

Beschreibung	Diese Operation aktiviert die Komfortsignatur für einen HBA bezogen auf einen Aufrufkontext.	
Aufrufparameter		
	Name	Beschreibung
	CONN: Card Handle	Identifiziert die zu adressierende Karte. Es wird nur der HBA unterstützt.
	CCTX:Context	MandantId, ClientSystemId, WorkplaceId, UserId verpflichtend zu übergeben; MandantId, WorkplaceId nicht ausgewertet
Rückgabe		
	CONN:Status	Enthält den Ausführungsstatus der Operation.
	SIG: SignatureMode	Signaturmodus des HBA Enthält bei erfolgreicher Ausführung der Operation den Wert „COMFORT“
Vorbedingungen	Keine	
Nachbedingungen	Keine	

4559

Tabelle 242: TAB_KON_877 Ablauf ActivateComfortSignature

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	TUC_KON_000 „Prüfe Zugriffsberechtigung“	Die Prüfung erfolgt durch den Aufruf TUC_KON_000 { mandantId = \$context.mandantId; clientsystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; userId = \$context.userId; cardHandle = \$cardHandle } Tritt bei der Prüfung ein Fehler auf, bricht die Operation mit Fehlercode aus TUC_KON_000 ab.

3.	TUC_KON_026 „Liefere CardSession“	Ermittle CardSession über TUC_KON_026 { mandatId = \$context.mandantId; clientsystemId = \$context.clientsystemId; cardHandle = \$context.cardHandle; userId = \$context.userId }
4.	TUC_KON_171 „Komfortsignatur einschalten“	Der Komfortsignaturmodus wird für das Tupel (CardHandle, CardSession) eingeschaltet. Tritt hierbei ein Fehler auf, bricht die Operation ab.

4560

4561 **Tabelle 243: TAB_KON_879 Fehlercodes ActivateComfortSignature**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen TUCs können folgende weiteren Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler
4270	Technical	Error	UserId wurde in den letzten 1.000 Vorgängen bereits verwendet
4272	Technical	Error	UserId nicht zulässig

4562 [\leq]

4563

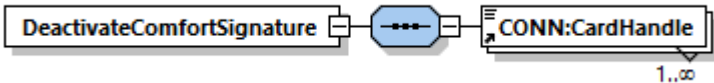
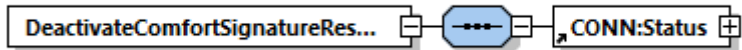
4564 *4.1.8.5.6 DeactivateComfortSignature*

4565 A_19108 - Operation DeactivateComfortSignature

4566 Der Signaturdienst des Konnektors MUSS an der Clientschnittstelle eine Operation DeactivateComfortSignature anbieten.

4568

4569 **Tabelle 244: TAB_KON_875 DeactivateComfortSignature**

Name	DeactivateComfortSignature		
Beschreibung	Diese Operation deaktiviert die Komfortsignatur für einen oder mehrere HBA.		
Aufrufparameter			
	Name	Beschreibung	
	CONN: Card Handle	Identifiziert die zu adressierende Karte. Es wird nur der HBA unterstützt.	
Rückgabe			

	CONN:Status	Enthält den Ausführungsstatus der Operation.
Vorbedingungen	Keine	
Nachbedingungen	Keine	

4570 **Tabelle 245: TAB_KON_878 Ablauf DeactivateComfortSignature**

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	TUC_KON_172 „Komfortsignatur ausschalten“	Der Komfortsignaturmodus wird für alle Karten aus der CardHandle-Liste ausgeschaltet.

4571

4572 **Tabelle 246: TAB_KON_880 Fehlercodes DeactivateComfortSignature**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen TUCs können folgende weiteren Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler

4573 [**<=**]

4574

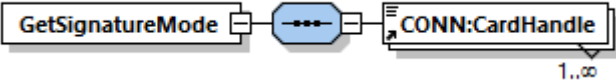
4575 **4.1.8.5.7 GetSignatureMode**

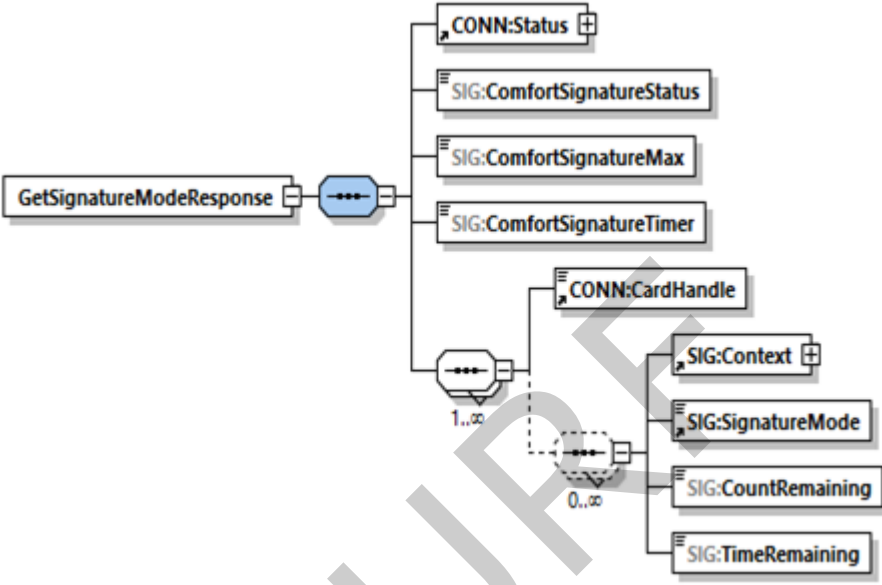
4576 A_19109 - Operation GetSignatureMode

4577 Der Signatordienst des Konnektors MUSS an der Clientschnittstelle eine Operation
 4578 GetSignatureMode anbieten.

4579

4580 **Tabelle 247: TAB_KON_876 GetSignatureMode**

Name	GetSignatureMode	
Beschreibung	Diese Operation liefert den aktuell konfigurierten Status der Komfortsignaturfunktion im Konnektor und die im Konnektor aktuell hinterlegten Signaturmodus zu allen HBA aus der übergebenen CardHandle-Liste.	
Aufrufparameter		
	Name	Beschreibung

	CONN: Card Handle	Identifiziert die zu adressierende Karte. Es wird nur der HBA unterstützt.
Rückgabe	 <p>The diagram shows the structure of the <code>GetSignatureModeResponse</code> message. It is a container message that includes several elements: <code>CONN:Status</code>, <code>SIG:ComfortSignatureStatus</code>, <code>SIG:ComfortSignatureMax</code>, <code>SIG:ComfortSignatureTimer</code>, <code>CONN:CardHandle</code>, <code>SIG:Context</code>, <code>SIG:SignatureMode</code>, <code>SIG:CountRemaining</code>, and <code>SIG:TimeRemaining</code>. The <code>CONN:CardHandle</code> element is a list of <code>CardHandle</code> objects, indicated by a '1..∞' cardinality. The <code>SIG:Context</code>, <code>SIG:SignatureMode</code>, <code>SIG:CountRemaining</code>, and <code>SIG:TimeRemaining</code> elements are grouped together and have a '0..∞' cardinality, indicating they are optional and can occur multiple times.</p>	
	CONN:Status	Enthält den Ausführungsstatus der Operation.
	SIG:ComfortSignatureStatus	Komfortsignatur-Konfigurationsstatus des Konnektors
	SIG:ComfortSignatureMax	Im Konnektor konfigurierte Anzahl von Komfortsignaturen, die ohne erneute PIN-Eingabe ausgeführt werden dürfen,
	SIG:ComfortSignatureTimer	Im Konnektor konfiguriertes Zeitintervall, in dem Komfortsignaturen ohne erneute PIN-Eingabe ausgeführt werden dürfen, Format: "PTnHnMnS" (gemäß Datentyp xsd:duration)
	CONN:CardHandle	Liste von HBA-CardHandles
	SIG:Context	Liste von im Konnektor hinterlegten Aufrufkontexten für das jeweilige HBA-CardHandle MandantId, ClientSystemId, UserId verpflichtend
	SIG:SignatureMode	Im Konnektor hinterlegter Signaturmodus für den jeweiligen Aufrufkontext

	SIG:CountRemaining	Verbleibende Anzahl von Komfortsignaturen, die ohne erneute PIN-Eingabe ausgeführt werden dürfen
	SIG:TimeRemaining	Verbleibende Zeit, in der Komfortsignaturen ohne erneute PIN-Eingabe ausgeführt werden dürfen Format: "PTnHnMnS" (gemäß Datentyp xsd:duration)
Vorbedingungen	Keine	
Nachbedingungen	Keine	

4581 **Tabelle 248: TAB_KON_882 Ablauf GetSignatureMode**

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	TUC_KON_173 „Liefere Signaturmodus“	Der Komfortsignatur-Konfigurationsstatus des Konnektors und die im Konnektor hinterlegten Signaturmodus werden für alle dem Konnektor bekannten Aufrufkontexte der HBA aus der übergebenen CardHandle-Liste zurückgeliefert.

4582

4583 **Tabelle 249: TAB_KON_881 Fehlercodes GetSignatureMode**

Fehlercode	ErrorType	Severity	Fehlertext
Folgende Fehlercodes können auftreten:			
4000	Technical	Error	Syntaxfehler

4584 [**<=**]

4585 **4.1.8.6 Betriebsaspekte**

4586 TIP1-A_4680 - Konfigurationswerte des Signaturdienstes
 4587 Die Managementschnittstelle MUSS es einem Administrator ermöglichen
 4588 Konfigurationsänderungen gemäß Tabelle TAB_KON_596 vorzunehmen:
 4589

4590 **Tabelle 250: TAB_KON_596 Konfigurationswerte des Signaturdienstes (Administrator)**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
------------	----------	---

SAK_SIMPLE_ SIGNATURE_ MODE	SE#1 SE#2	Aktivierung/Deaktivierung des „Einfachsignaturmodus“ für alle HBAX für die Durchführung von Einfachsignaturen im SecurityEnvironment #1 (SE#1) für Dokumentenstapel der Größe 1 anstelle der Verwendung des SE#2. Default-Wert = SE#1
--------------------------------	--------------	--

4591

4592 [\leq]

4593 TIP1-A_4680-02 - Konfigurationswerte des Signaturdienstes

4594 Die Managementschnittstelle MUSS es einem Administrator ermöglichen

4595 Konfigurationsänderungen gemäß Tabelle TAB_KON_596 vorzunehmen:

4596

4597 **Tabelle 251: TAB_KON_596 Konfigurationswerte des Signaturdienstes (Administrator)**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
SAK_SIMPLE_ SIGNATURE_ MODE	SE#1 SE#2	Aktivierung/Deaktivierung des „Einfachsignaturmodus“ für alle HBAX für die Durchführung von Einfachsignaturen im SecurityEnvironment #1 (SE#1) für Dokumentenstapel der Größe 1 anstelle der Verwendung des SE#2. Default-Wert = SE#1 Der Parameter ist nur relevant, wenn die Komfortsignaturfunktion nicht aktiviert ist (SAK_COMFORT_SIGNATURE = Disabled).
SAK_COMFORT_ SIGNATURE	Enabled/ Disabled	Aktivierung/Deaktivierung der Komfortsignaturfunktion im Konnektor Default-Wert = Disabled Die Komfortsignaturfunktion darf nur aktiviert sein, wenn ANCL_TLS_MANDATORY = Enabled und ANCL_CAUT_MANDATORY = Enabled

SAK_COMFORT_SIGNATURE_MAX	[1 - 250]	Anzahl von Komfortsignaturen, die ohne erneute PIN-Eingabe ausgeführt werden dürfen Default-Wert = 100 Der Parameter ist nur relevant, wenn die Komfortsignaturfunktion aktiviert ist (SAK_COMFORT_SIGNATURE = Enabled).
SAK_COMFORT_SIGNATURE_TIMER	[1 - 24 h]	Zeitintervall, in dem Komfortsignaturen ohne erneute PIN-Eingabe ausgeführt werden dürfen Der Timer startet mit Eingabe der PIN.QES für die Komfortsignatur. Default-Wert = 6 h Der Parameter ist nur relevant, wenn die Komfortsignaturfunktion aktiviert ist (SAK_COMFORT_SIGNATURE = Enabled).

4598
4599 [\leq]

4600 4.1.9 Zertifikatsdienst

4601 Der Zertifikatsdienst bietet eine Schnittstelle zur Überprüfung der Gültigkeit von
4602 Zertifikaten an. Dies geschieht auf Grundlage des durch den Vertrauensanker (TSL-CA-
4603 Signer-Zertifikat und eine aktuelle, gültige TSL aufgespannten Vertrauensraums sowie
4604 unter Berücksichtigung von aktuellen Statusinformationen (OCSP, CRL). Die
4605 Zertifikatsprüfung wird sowohl für nonQES- als auch für QES-Zertifikate unterstützt.

4606 Die für die QES-Zertifikatsprüfung notwendigen QES-Signer-Zertifikate werden durch die
4607 Vertrauensliste der Bundesnetzagentur (BNetzA-VL) bereitgestellt. Das Signer-Zertifikat
4608 der BNetzA-VL ist in der TSL enthalten.

4609 Im Rahmen der ECC-Migration muss der Konnektor neben RSA auch ECC unterstützen.
4610 Hierfür wird eine TSL bereitgestellt, die sowohl die neuen ECC-basierten Zertifikate als
4611 auch aus Rückwärtskompatibilitätsgründen die weiterhin benötigten RSA-basierten
4612 Zertifikate enthält. Diese neue TSL wird auch als „TSL(ECC-RSA)“ bezeichnet. In dieser
4613 Spezifikation wird außerhalb der Regelungen zur ECC-Migration nicht zwischen
4614 „TSL(ECC-RSA)“ und „TSL(RSA)“ unterschieden, da die Anforderungslage keine
4615 Unterscheidung erfordert.

4616 Innerhalb des Zertifikatsdienstes werden folgende Präfixe für Bezeichner verwendet:

- 4617 • Events (Topic Ebene 1): „CERT“
- 4618 • Konfigurationsparameter: „CERT_“

4619 4.1.9.1 Funktionsmerkmalweite Aspekte

4620 Bei der Zertifikatsprüfung wird im Rahmen eines Anwendungsfalls u.a. auch der
4621 Verwendungszweck des Zertifikats geprüft. Der Verwendungszweck (intendedKeyUsage)
4622 wird als Parameter an TUC_KON_037 übergeben. Der konkrete Wert

4623 von intendedKeyUsage ist abhängig vom kryptographischen Verfahren, auf welchem das
4624 Zertifikat basiert. Die Parametrisierung von intendedKeyUsage wird in TAB_KON_853
4625 in Abhängigkeit vom zu prüfenden Zertifikat, dem Anwendungsfall und dem
4626 kryptographischen Verfahren definiert.

4627 A_17295 - Verwendung der intendedKeyUsage bei der Zertifikatsprüfung (ECC-Migration)
4628 Der Konnektor MUSS bei der Zertifikatsprüfung die intendedKeyUsage in Abhängigkeit
4629 vom zu prüfenden Zertifikat, dem Anwendungsfall und dem kryptographischen Verfahren
4630 gemäß TAB_KON_853 prüfen.

4631 **Tabelle 252: TAB_KON_853- intendedKeyUsage bei Zertifikatsprüfung**

Zertifikat	Anwendungsfall	intendedKeyUsage bei	
		RSA	ECC
C.SMKT.AUT	TUC_KON_050 „Beginne Kartenterminalsitzung“ TUC_KON_053 „Paire Kartenterminal“	digitalSignature &keyEncipherment	digitalSignature
C.CH.AUT C.CH.AUTN	TUC_KON_161 „nonQES Dokumentsignatur prüfen“	digitalSignature &keyEncipherment	digitalSignature
C.CH.ENC C.CH.ENCV C.HCI.ENC C.HP.ENC Zertifikate aus CERT_IMPORTED_CA_LIST	TUC_KON_070 „Daten hybrid verschlüsseln“	keyEncipherment	keyAgreement
C.HCI.OSIG	TUC_KON_161 „nonQES Dokumentsignatur prüfen“	nonRepudiation	nonRepudiation
C.FD.TLS-S	TUC_KON_110 „Kartenbasierte TLS-Verbindung aufbauen“	digitalSignature&keyEncipherment	digitalSignature
C.ZD.TLS-S	TUC_KON_290 „LDAP-Verbindung aufbauen“	digitalSignature	digitalSignature

C.ZD.TLS-S	TIP1-A_5662 - Gesicherte Übertragung von BNetzA-VL und Hashwert TUC_KON_282 „UpdateInformatio nen beziehen“ TUC_KON_283 Infrastruktur Konfiguration aktualisieren TUC_KON_285 „UpdateInformatio nen für Fachmodul beziehen“ TUC_KON_286 „Paket für Fachmodul laden“	digitalSignature&keyEnciphe rment	digitalSignat ure
C.FD.AUT	A_17225	digitalSignature&keyEnciphe rment	digitalSignat ure

4632 **[<=]**

4633 Bei der Zertifikatsprüfung wird ein übergebenes Zertifikat oder ein Zertifikat einer
 4634 referenzierten Karte geprüft. Das konkrete Zertifikatsobjekt einer Karte ist abhängig vom
 4635 Kartentyp und dem gewählten kryptographischen Verfahren. Die folgende Tabelle führt
 4636 auf, welche Zertifikatsobjekte einer Karte in Abhängigkeit vom kryptographischen
 4637 Verfahren für die jeweilige Zertifikatsreferenz ausgewählt werden.

4638 **Tabelle 253: TAB_KON_858 Kartenobjekt in Abhängigkeit vom kryptographischen**
 4639 **Verfahren**

CertRef	Kartentyp	Objekt der Karte in Abhängigkeit vom kryptographischen Verfahren (Crypt)	
		RSA	ECC
C.AUT	HBA-VK	EF.C.HP.AUT	-
	HBA	EF.C.HP.AUT.R2048	EF.C.HP.AUT.E256
	SM-B	EF.C.HCI.AUT	EF.C.HCI.AUT.E256
	eGK G2	EF.C.CH.AUT.R2048	EF.C.CH.AUT.E256
C.ENC	HBA-VK	EF.C.HP.ENC	-
	HBA	EF.C.HP.ENC.2048	EF.C.HP.ENC.E256

	SM-B	EF.C.HCI.ENC.R2048	EF.C.HCI.ENC.E256
C.SIG	SM-B	EF.C.HCI.OSIG.R2048	EF.C.HCI.OSIG.E256
C.QES	HBA-VK	EF.C.HP.QES	-
	HBA	EF.C.HP.QES.R2048	EF.C.HP.QES.E256

4640

4641 TIP1-A_4682 - Sicheres Einbringen des TI-Vertrauensankers

4642 Der Vertrauensanker der TI MUSS zum Auslieferungszeitpunkt des Konnektors
 4643 integritätsgeschützt im Konnektor hinterlegt sein. Zur Sicherstellung dieser Integrität
 4644 MUSS die Dateiablage EF.C.TSL.CA_1 der Anwendung DF.Sicherheitsanker der gSMC-K
 4645 [gemSpec_gSMC-K_ObjSys#5.7.2] verwendet werden.

4646 [\leq]

4647 TIP1-A_4684 - Regelmäßige Aktualisierung der CRL und der TSL

4648 Falls Parameter MGM_LU_ONLINE=Enabled, MUSS der Zertifikatsdienst einmal täglich die
 4649 Aktualisierung der TSL durch Aufruf von TUC_KON_032 „TSL aktualisieren“ durchführen
 4650 und anschließend TUC_KON_040 „CRL aktualisieren“ aufrufen.

4651 [\leq]

4652 TIP1-A_4685 - Vermeidung von Spitzenlasten bei TSL- und CRL-Download

4653 Der Konnektor MUSS Spitzenlasten durch paralleles Herunterladen der TSL und der CRL
 4654 vermeiden. Dazu MÜSSEN die im Einsatz befindlichen Konnektoren eines Herstellers ihre
 4655 Download-Versuche gleichmäßig über den Tag verteilen.

4656 [\leq]

4657 Dadurch wird gleichzeitig die Spitzenlast bei OCSP-Anfragen begrenzt.

4658 A_17572 - Nutzung der Hash-Datei für TSL (ECC-Migration)

4659 Falls die TSL(ECC-RSA) verwendet wird, MUSS der Konnektor vor deren Aktualisierung
 4660 mit TUC_KON_032 „TSL aktualisieren“ die Hash-Datei der TSL(ECC-RSA) herunterladen,
 4661 um zu prüfen, ob die am TSL-Downloadpunkt verfügbare TSL(ECC-RSA) eine andere ist,
 4662 als die schon zuvor heruntergeladene und bereits ausgewertete TSL(ECC-RSA).

4663 Entspricht der Hash-Wert am Download-Punkt der bereits heruntergeladenen und
 4664 ausgewerteten TSL(ECC-RSA), MUSS der Konnektor auf den Download verzichten. [\leq]

4665 A_17661 - Gesicherte Übertragung der Hash-Datei für TSL (ECC-Migration)

4666 Der Konnektor MUSS für den Download der Hash-Datei der TSL(ECC-RSA) die
 4667 Verbindung zum TSL-Dienst durch TLS absichern. Der Konnektor MUSS das vom TSL-
 4668 Dienst beim TLS-Verbindungsaufbau präsentierte Zertifikat C.ZD.TLS-S prüfen. Die
 4669 Prüfung erfolgt durch Aufruf von TUC_KON_037 „Zertifikat prüfen“ {

```

4670     certificate = C.ZD.TLS-S;
4671     qualifiedCheck = not_required;
4672     offlineAllowNoCheck = true;
4673     policyList = oid_zd_tls_s;
4674     intendedKeyUsage = intendedKeyUsage(C.ZD.TLS-S);
4675     intendedExtendedKeyUsage = id-kp-serverAuth;
4676     validationMode = OCSP } .

```

4677 Falls Fehler im TLS-Verbindungsaufbau bzw. bei der Zertifikatsprüfung auftreten

4678 MUSS der Konnektor den TLS-Verbindungsaufbau mit Fehlercode 4235 gemäß

4679 TAB_KON_825 abbrechen.
4680 [**<=**]

4681 A_17781 - Aktualisierung der TSL ohne Hash-Datei für TSL (ECC-Migration)
4682 Falls im Rahmen der TSL-Aktualisierung beim Download der Hash-Datei der TSL(ECC-
4683 RSA) ein Fehler auftritt MUSS der Konnektor die Aktualisierung der TSL
4684 mit TUC_KON_032 „TSL aktualisieren“ ohne einen ermittelten Hashwert aufrufen. [**<=**]

4685 TIP1-A_6730 - Regelmäßige Aktualisierung der BNetzA-VL
4686 Falls Parameter MGM_LU_ONLINE=Enabled, MUSS der Zertifikatsdienst die
4687 Aktualisierung der BNetzA-VL im Zeitintervall CERT_BNETZA_VL_UPDATE_INTERVAL durch
4688 Aufruf von TUC_KON_031 „BNetzA-VL aktualisieren“ durchführen.
4689 [**<=**]

4690 TIP1-A_6731 - Regelmäßige Prüfung der BNetzA-VL
4691 Der Zertifikatsdienst MUSS einmal täglich die zeitliche Gültigkeit der BNetzA-VL prüfen.
4692 Wenn das Element NextUpdate in der Vergangenheit liegt MUSS der Konnektor den
4693 Betriebszustand EC_BNetzA_VL_not_valid auslösen.
4694 [**<=**]

4695 TIP1-A_6732 - Vermeidung von Spitzenlasten bei BNetzA-VL-Download
4696 Der Konnektor MUSS Spitzenlasten durch Herunterladen der BNetzA-VL vermeiden. Dazu
4697 MÜSSEN die im Einsatz befindlichen Konnektoren den Zeitpunkt für den Download
4698 zufällig wählen unter Beachtung des konfigurierten Zeitintervalls
4699 CERT_BNETZA_VL_UPDATE_INTERVAL.
4700 [**<=**]

4701 TIP1-A_5662 - Gesicherte Übertragung von BNetzA-VL und Hashwert
4702 Der Konnektor MUSS für den Download der BNetzA-VL und deren Hashwert die
4703 Verbindung zum TSL-Dienst durch TLS absichern. Der Konnektor MUSS das vom TSL-
4704 Dienst beim TLS-Verbindungsaufbau präsentierte Zertifikat ID.ZD.TLS_S prüfen. Die
4705 Prüfung erfolgt durch Aufruf von TUC_KON_037 „Zertifikat prüfen“ {

4706 certificate = ID.ZD.TLS_S;
4707 qualifiedCheck = not_required;
4708 offlineAllowNoCheck = true;
4709 policyList = oid_zd_tls_s;
4710 intendedKeyUsage = intendedKeyUsage(C.ZD.TLS-S);
4711 intendedExtendedKeyUsage = id-kp-serverAuth;
4712 validationMode = OCSP } .

4713 Fehler im TLS-Verbindungsaufbau bzw. bei der Zertifikatsprüfung führen zum Abbruch
4714 des TLS-Verbindungsaufbaus mit Fehlercode 4235 gemäß TAB_KON_825.
4715

4716 **Tabelle 254: TAB_KON_825 Fehlercodes „TLS-Verbindungsaufbau zum TSL-Dienst“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4235	Security	Error	TSL-Dienst konnte bei TLS-Verbindungsaufbau nicht authentisiert werden

4717
4718 [**<=**]
4719 TIP1-A_5663 - Prüfung der technischen Rolle bei TLS-Verbindungsaufbau zum TSL-Dienst

4720 Der Konnektor MUSS beim TLS-Verbindungsaufbau zum TSL-Dienst prüfen, dass die vom
4721 TSL-Dienst in ID.ZD.TLS_S übergebene technische Rolle gemäß [gemSpec_OID#GS-
4722 A_4446] dem Wert „oid_tsl_ti“ entspricht.
4723 Ein Fehler bei der Prüfung der technischen Rolle führt zum Abbruch des TLS-
4724 Verbindungsaufbaus mit Fehlercode 4236 gemäß TAB_KON_826.

4725 **Tabelle 255: TAB_KON_826 Fehlercodes „TLS-Verbindungsaufbau zum TSL-Dienst bei**
4726 **Prüfung der technischen Rolle“**

Fehlercode	ErrorType	Severity	Fehlertext
4236	Security	Error	Rollenprüfung bei TLS-Verbindungsaufbau zum TSL-Dienst fehlgeschlagen

4727
4728 [**<=**]

4729 TIP1-A_4686 - Warnung vor und bei Ablauf der TSL
4730 Steht der Ablauf der TSL innerhalb von 7 Tagen an, MUSS der Konnektor den
4731 Betriebszustand EC_TSL_Expiring annehmen.
4732 Mit Ablauf der Gültigkeit der TSL MUSS der Konnektor den Betriebszustand
4733 EC_TSL_Out_Of_Date_Within_Grace_Period annehmen.
4734 Mit Ablauf der Graceperiod der TSL MUSS der Konnektor den kritischen Betriebszustand
4735 EC_TSL_Out_Of_Date_Beyond_Grace_Period annehmen.
4736 [**<=**]

4737 TIP1-A_4687 - Warnung vor und bei Ablauf des TI-Vertrauensankers
4738 Steht der Ablauf der Gültigkeit des TI-Vertrauensankers innerhalb von 30 Tagen an,
4739 MUSS der Konnektor den Betriebszustand EC_TSL_Trust_Anchor_Expiring annehmen.
4740 Mit Ablauf der Gültigkeit des Vertrauensankers MUSS der Konnektor den kritischen
4741 Betriebszustand EC_TSL_Trust_Anchor_Out_Of_Date annehmen.
4742 [**<=**]

4743 TIP1-A_4994 - Warnung vor und bei Ablauf der CRL
4744 Steht der Ablauf der Gültigkeit der CRL innerhalb von 3 Tagen an, MUSS der Konnektor
4745 den Betriebszustand EC_CRL_Expiring annehmen.
4746 Mit Ablauf der Gültigkeit der CRL MUSS der Konnektor den kritischen Betriebszustand
4747 EC_CRL_Out_Of_Date annehmen.
4748 [**<=**]

4749 TIP1-A_4688 - OCSP-Forwarding
4750 Der Konnektor MUSS alle OCSP-Anfragen über den OCSP-Forwarder (HTTP-Proxy) des
4751 Zugangsdienst-Providers schicken, der durch die Konfigurationswerte
4752 (CERT_OCSP_FORWARDER_ADDRESS, CERT_OCSP_FORWARDER_PORT) festgelegt ist.
4753 [**<=**]

4754 TIP1-A_4689 - Caching von OCSP-Antworten
4755 Der Zertifikatsdienst MUSS erhaltene OCSP-Antworten für eine durch
4756 CERT_OCSP_DEFAULT_GRACE_PERIOD_NONQES angegebene Anzahl an Minuten (nonQES-
4757 Zertifikate) zwischenspeichern.
4758 [**<=**]

4759 TIP1-A_4690 - Timeout und Graceperiod für OCSP-Anfragen
4760 Bei Ausführung von TUC_PKI_006 „OCSP-Abfrage“ [gemSpec_PKI#8.3.2.2] MÜSSEN
4761 folgende Parameter verwendet werden:

4762
4763 OCSP-Graceperiod =
4764 CERT_OCSP_DEFAULT_GRACE_PERIOD_NONQES

- 4765 • Timeout-Parameter =
 4766 CERT_OCSP_TIMEOUT_NONQES bzw.
 4767 CERT_OCSP_TIMEOUT_QES

4768 [\leq]

4769 TIP1-A_4691 - Ablauf der gSMC-K und der gesteckten Karten regelmäßig prüfen
 4770 Für die gSMC-K sowie für jede gesteckte Karte außer eGK MUSS der Konnektor im
 4771 Intervall CERT_EXPIRATION_CARD_CHECK_DAYS genau einmal TUC_KON_033 aufrufen.
 4772 Der Konnektor MUSS die Gültigkeitsdauer der Zertifikate prüfen mittels Aufruf von:
 4773 für gSMC-K
 4774 TUC_KON_033{checkSMCK; doInformClients=Ja; crypt = ECC}
 4775 TUC_KON_033{checkSMCK; doInformClients=Ja; crypt = RSA}
 4776 für jede gesteckte G2.0 Karte außer eGK und außer gSMC-K
 4777 TUC_KON_033{cardSession; doInformClients=Ja; crypt = RSA}
 4778 für jede gesteckte ab G2.1 Karte außer eGK
 4779 TUC_KON_033{cardSession; doInformClients=Ja; crypt = ECC}
 4780 TUC_KON_033{cardSession; doInformClients=Ja; crypt = RSA}
 4781 [\leq]

4782 TIP1-A_4692 - Missbrauchserkennung, zu kontrollierende Operationen
 4783 Der Konnektor MUSS zur Unterstützung von Missbrauchserkennungen die in Tabelle
 4784 TAB_KON_597 gelisteten Operationen als Einträge in EVT_MONITOR_OPERATIONS
 4785 berücksichtigen.
 4786

4787 **Tabelle 256: TAB_KON_597 Operationen in EVT_MONITOR_OPERATIONS**

Operationsname	OK_Val	NOK_Val	Alarmwert (Default-Grenzwert 10 Minuten- Σ)
VerifyCertificate	1	5	401

4788
 4789 [\leq]

4790 4.1.9.2 Durch Ereignisse ausgelöste Reaktionen

4791 Keine.

4792 4.1.9.3 Interne TUCs, nicht durch Fachmodule nutzbar

4793 4.1.9.3.1 TUC_KON_032 „TSL aktualisieren“

4794 TIP1-A_4693 - TUC_KON_032 „TSL aktualisieren“
 4795 Der Konnektor MUSS den technischen Use Case TUC_KON_032 „TSL aktualisieren“
 4796 umsetzen.
 4797

4798 **Tabelle 257: TAB_KON_766 TUC_KON_032 „TSL aktualisieren“**

Element	Beschreibung
Name	TUC_KON_032 „TSL aktualisieren“
Beschreibung	Dieser TUC prüft die Aktualität der TSL und initialisiert ggf. den TSL-spezifischen Bereich des TrustStores neu. Zusätzlich wird

	bei einem Wechsel des TI-Vertrauensankers das neue TSL-Signer-CA-Zertifikat in einem sicheren Speicherort im Konnektor hinterlegt. Im Fall der Veröffentlichung eines CVC-Root-CA-Zertifikats werden das CVC-Root-CA-Zertifikat und die Cross-CV-Zertifikate aus der TSL in den Truststore eingestellt.
Auslöser	<ul style="list-style-type: none"> Aufruf durch andere TUCs
Vorbedingungen	<ul style="list-style-type: none"> Ein gültiger TI-Vertrauensanker ist vorhanden Das XML-Schema der TSL-Datei liegt vor
Eingangsdaten	<ul style="list-style-type: none"> importedTSL – <i>optional</i> (TSL aus manuellem Import) (Optional) baseTime – <i>optional; default: aktuelles Datum</i> (Referenzzeitpunkt) () onlineMode [ENABLED DISABLED] (Flag „MGM_LU_ONLINE“ für Offline/Online-Modus) hashTSL – <i>optional</i> (Hashwert-Datei der TSL im System; gilt nur für TSL(ECC-RSA))
Komponenten	Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> result (Status der Prüfung) newHashTSL – <i>optional; verpflichtend für TSL(ECC-RSA)</i> (Hashwert-Datei der TSL im System; gilt nur für TSL(ECC-RSA))
Nachbedingungen	<ul style="list-style-type: none"> Aktuelle TSL-Informationen inkl. des Vertrauensankers der BNetzA VL und sämtlicher CVC-Root-CA- und Cross-CV-Zertifikate liegen im Truststore vor. Ein ggf. gelieferter neuer Vertrauensanker der TI ist in einem sicheren Speicherort gespeichert
Standardablauf	<ol style="list-style-type: none"> Der Konnektor prüft und aktualisiert ggf. die TSL durch Aufruf von TUC_PKI_001. Der durch den dort aufgerufenen TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“ benötigte aktuelle TI-Vertrauensanker befindet sich auf der gSMC-K in der Datei EF.C.TSL_CA_1 oder in einem sicheren Speicherort im Konnektor. Es ist dasjenige Zertifikat zu verwenden, welches zum Referenzzeitpunkt gültig ist und ab dem Aktivierungsdatum (<i>StatusStartingTime</i> des neuen TSL-Signer-CA-Zertifikats) aktiviert ist. Ggf. vorhandene CVC-Root-CA-Zertifikat und Cross-CV-Zertifikate werden genauso wie und zusammen mit den anderen CA-Zertifikaten aus der TSL extrahiert. Alle Informationen aus der TSL werden im TSL-spezifischen Bereich des TrustStores gespeichert

	<p>4. Der Konnektor löst TUC_KON_256 { topic = „CERT/TSL/UPDATED“; eventType = Op; severity = Info; doLog = true; doDisp = false } aus.</p> <p>5. CERT_CRL_DOWNLOAD_ADDRESS wird mit den CRL-Download-Adressen aus der TSL überschrieben.</p>
Varianten/ Alternativen	<p>(→1) Wird die <i>importedTSL</i> manuell übergeben (in den Eingangsdaten), so wird diese statt des Downloads verwendet und an TUC_PKI_001 übergeben. Innerhalb der PKI TUCs findet dann kein Download der TSL statt.</p> <p>(→1) Falls <i>onlineMode</i> = DISABLED, kann der Sperrstatus des TSL-Signer-Zertifikats nicht überprüft werden. In diesem Fall wird die Aktivierung der <i>importedTSL</i> auch ohne Prüfung des Sperrstatus durchgeführt.</p> <p>(→1) Wird durch den von TUC_PKI_001 aufgerufenen TUC_PKI_013 „Import neuer Vertrauensanker“ ein neuer TI-Vertrauensanker (ein neues TSL-Signer-CA-Zertifikat) in der <i>importedTSL</i> gefunden, so wird dieser, wie dort beschrieben, extrahiert und in einem sicheren Speicherort gespeichert. Vor Erreichen des Aktivierungsdatums werden die TSLs ausschließlich mit dem alten TSL-Signer-Zertifikat signiert. Ab dem Aktivierungsdatum werden die TSLs mit einem TSL-Signer-Zertifikat signiert, das von der neuen TSL-Signer-CA ausgestellt wurde.</p>
Fehlerfälle	<p>(→1) Tritt beim manuellen Import der Datei ein Fehler auf, wird TUC_KON_256 { topic = „CERT/TSL/IMPORT“; eventType = Op; severity = Error; parameters = „\$Fehlerbeschreibung“; doLog = true; doDisp = false } ausgelöst. Fehlercode 4128.</p> <p>(→1) Tritt beim periodischen Update der TSL beim Aufruf des TUC_PKI_001 oder eines durch ihn aufgerufenen TUCs ein Fehler auf, geht der Konnektor in den Betriebszustand EC_TSL_Update_Not_Successful. Die vorhandenen TSL-Vertrauensanker werden weiter verwendet. Fehlercode 4127.</p>
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

4799 **Tabelle 258: TAB_KON_598 Fehlercodes TUC_KON_032 „TSL aktualisieren“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4127	Security	Error	Import der TSL-Datei fehlgeschlagen
4128	Technical	Error	der manuelle Import der TSL-Datei schlägt fehl

4800

4801 [**<=**]

4802

4803 **4.1.9.3.2 TUC_KON_031 „BNetzA-VL aktualisieren“**

4804 TIP1-A_6729 - TUC_KON_031 „BNetzA-VL aktualisieren“

4805 Der Konnektor MUSS den technischen Use Case TUC_KON_031 „BNetzA-VL aktualisieren“
4806 umsetzen.

4807

4808 **Tabelle 259: TAB_KON_618 TUC_KON_031 „BNetzA-VL aktualisieren“**

Element	Beschreibung
Name	TUC_KON_031 „BNetzA-VL aktualisieren“
Beschreibung	Dieser TUC prüft die Aktualität der BNetzA-VL. Wenn eine neuere BNetzA-VL vorliegt, wird diese heruntergeladen, geprüft und im Truststore gespeichert.
Auslöser	<ul style="list-style-type: none"> • Aufruf durch andere TUCs • TIP1-A_6728
Vorbedingungen	<ul style="list-style-type: none"> • Aktuell gültige TSL im Truststore vorhanden
Eingangsdaten	<ul style="list-style-type: none"> • BNetzA-VL aus manuellem Import (Optional) • Flag „MGM_LU_ONLINE“ für Offline-/Online-Modus • Flag „MGM_LU_SAK“ für Signaturdienst-Modus
Komponenten	Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> • Status der Prüfung
Nachbedingungen	<ul style="list-style-type: none"> • Aktuelle BNetzA-VL und deren Hashwert liegen im Truststore vor.
Standardablauf	<ol style="list-style-type: none"> 1. Der Konnektor prüft und aktualisiert ggf. die BNetzA-VL durch Aufruf von TUC_PKI_036. 2. Der Konnektor löst TUC_KON_256 {"CERT/BNETZA_VL/UPDATED"; Op; Info; „"; doLog = true; doDisp = false} aus.
Varianten/Alternativen	(→1) Wird eine zu importierende BNetzA-VL manuell übergeben (in den Eingangsdaten), so wird diese statt des Downloads verwendet und an TUC_PKI_036 {BNetzA-VL Datei} übergeben. Innerhalb der PKI TUCs findet dann kein

	Download der BNetzA-VL statt. (→1) Ist MGM_LU_SAK=disabled, so wird der TUC ohne Fehler beendet.
Fehlerfälle	(→1) Tritt beim manuellen Import der Datei ein Fehler auf, wird TUC_KON_256 {„CERT/BNETZA_VL/IMPORT“; Op; Error; „\$Fehlerbeschreibung“; doLog = true; doDisp = false} ausgelöst. Fehlercode 4129. (→1) Tritt beim periodischen Update der BNetzA-VL beim Aufruf des TUC_PKI_036 oder eines durch ihn aufgerufenen TUCs ein Fehler auf, geht der Konnektor in den Betriebszustand EC_BNetzA_VL_Update_Not_Successful. Fehlercode 4133. In beiden Fällen wird eine vorhandene gültige BNetzA-VL weiter verwendet.
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

4809 **Tabelle 260: TAB_KON_619 Fehlercodes TUC_KON_031 „BNetzA-VL aktualisieren“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4129	Technical	Error	der manuelle Import der BNetzA-Vertrauensliste schlägt fehl
4133	Security	Error	Import der BNetzA-Vertrauensliste fehlgeschlagen

4810

4811 [**<=**]

4812 **4.1.9.3.3 TUC_KON_040 „CRL aktualisieren“**

4813 TIP1-A_4694 - TUC_KON_040 „CRL aktualisieren“

4814 Der Konnektor MUSS den technischen Use Case TUC_KON_040 „CRL aktualisieren“
4815 umsetzen.

4816 **Tabelle 261: TAB_KON_767 TUC_KON_040 „CRL aktualisieren“**

Element	Beschreibung
Name	TUC_KON_040 „CRL aktualisieren“
Beschreibung	Dieser TUC aktualisiert die CRL
Auslöser	<ul style="list-style-type: none"> Aufruf durch andere TUCs
Vorbedingungen	<ul style="list-style-type: none"> Ein gültiger Vertrauensraum
Eingangsdaten	<ul style="list-style-type: none"> importedCRL – <i>optional</i> (Manuell importierte CRL)
Komponenten	Konnektor

Ausgangsdaten	Keine
Nachbedingungen	<ul style="list-style-type: none"> Eine aktuelle, gültige CRL liegt vor
Standardablauf	<ol style="list-style-type: none"> Der Konnektor lädt die aktuelle CRL von CERT_CRL_DOWNLOAD_ADDRESS herunter. Die Prüfung der CRL-Signatur mit dem CRL-Signer-Zertifikat setzt sich aus folgenden Teilschritten zusammen <ol style="list-style-type: none"> Prüfung auf zeitliche Gültigkeit des CRL-Signer-Zertifikats mittels TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats" mit Referenzzeitpunkt = aktuelle Systemzeit Auswahl des öffentlichen Schlüssels des CRL-Signer-Zertifikats (CRL-Signer-Zertifikat im Truststore) Die Signatur und der verwendete Algorithmus werden aus der CRL ausgelesen Verifikation der Signatur und Hashwert-Vergleich (Verfahren siehe [RFC5280]). Falls die Prüfung ein negatives Ergebnis erbracht hat, löst der Konnektor das Ereignis TUC_KON_256 { topic = „CERT/CRL/INVALID“; eventType = Op; severity = Error; parameters = „“; doLog = true; doDisp = false } aus. Nach einer erfolgreichen Prüfung speichert der Konnektor die neue CRL und löst das Ereignis TUC_KON_256{ topic = „CERT/CRL/UPDATED“; eventType = Op; severity = Error; parameters = „“; doLog = true; doDisp=false} aus. Falls die aktuelle Systemzeit den Wert NextUpdate aus der CRL erreicht oder überschritten hat, geht der Konnektor in den Betriebszustand EC_CRL_Out_Of_Date.
Varianten/ Alternativen	(→1) Wird eine manuell importierte CRL übergeben, so wird diese verwendet.
Fehlerfälle	(→1) Tritt beim manuellen Import der Datei ein Fehler auf, wird TUC_KON_256 { topic = „CERT/CRL/IMPORT“; eventType = Op; severity = Error;

	parameters = „\${Fehlerbeschreibung}“; doLog = true; doDisp=false} ausgelöst. (→2) Signaturprüfung der CRL fehlgeschlagen: Fehlercode 4130
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

4817 **Tabelle 262: TAB_KON_599 Fehlercodes TUC_KON_040 „CRL aktualisieren“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4130	Security	Error	Signatur- oder Gültigkeitsprüfung der CRL fehlgeschlagen

4818
4819 [\leq]

4820 4.1.9.3.4 TUC_KON_033 „Zertifikatsablauf prüfen“

4821 TIP1-A_4695 - TUC_KON_033 „Zertifikatsablauf prüfen“

4822 Der Konnektor MUSS den technischen Use Case TUC_KON_033 „Zertifikatsablauf prüfen“
4823 umsetzen.

4824

4825 **Tabelle 263: TAB_KON_768 TUC_KON_033 „Zertifikatsablauf prüfen“**

Element	Beschreibung
Name	TUC_KON_033 „Zertifikatsablauf prüfen“
Beschreibung	Dieser TUC prüft und meldet das zeitliche Ablaufen eines X.509-Zertifikats einer Karte.
Auslöser	<ul style="list-style-type: none"> • Aufruf durch andere TUCs des Konnektors oder • über die Managementschnittstelle
Vorbedingungen	Keine
Eingangsdaten	<ul style="list-style-type: none"> • cardSession – <i>optional</i>/für eGK, HBA, SM-B, gSMC-KT • checkSMCK [Boolean] – <i>optional</i>/für gSMC-K; (Referenz auf eine/die gSMC-K, alternativ zu cardSession) • doInformClients [Boolean] (Angabe, ob ein Event an die Clients gesendet werden soll)

	<ul style="list-style-type: none"> • <i>crypt</i> - optional; default = RSA (kryptographischer Algorithmus, für welchen das Zertifikat ermittelt wird; Wertebereich: ECC, RSA)
Komponenten	Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> • <i>expirationDate</i> (Ablaufdatum des untersuchten Zertifikats)
Standardablauf	<ol style="list-style-type: none"> 1. TUC_KON_216 „LeseZertifikat“ für: <ul style="list-style-type: none"> • Bei checkSMCK das Zertifikat der gSMC-K (C.NK.VPN) gemäß TAB_KON_856 • bei CardSession die Zertifikate der identifizierten Karte. <ol style="list-style-type: none"> i. Für die eGK: C.CH.AUT ii. Für den HBAX: C.HP.AUT iii. Für SM-B: C.HCI.AUT • Das konkrete Zertifikatsobjekt der Karte gemäß TAB_KON_858 wird vom Eingangsparameter <i>crypt</i> abgeleitet. 2. Das Ablaufdatum <i>expirationDate</i> wird aus dem Feld <i>validity</i> ausgelesen. 3. Falls das Zertifikat abgelaufen ist, Systemereignis absetzen: <ul style="list-style-type: none"> • gSMC-K: TUC_KON_256 { topic = „CERT/CARD/EXPIRATION“; eventType = Op; severity = Warning; parameters = („CARD_TYPE=gSMC-K, ICCSN=\$ICCSN, Konnektor=\$MGM_KONN_HOSTNAME, ZertName=\$Name des Zertifikatsobjekts gemäß TAB_KON_856, ExpirationDate=\$validity“); doLog = true; doDisp = \$doInformClients } • Sonstige Karten (mit CARD(CardSession)): TUC_KON_256 { topic = „CERT/CARD/EXPIRATION“; eventType = Op; severity = Warning; parameters = („CARD_TYPE=\$Type, ICCSN=\$ICCSN, CARD_HANDLE=\$CardHandle, CardHolderName=\$CardHolderName, ZertName=\$Name des Zertifikatsobjekts aus Schritt 1, ExpirationDate=\$validity“);

	<pre>doLog=false; doDisp = \$doInformClients }</pre> <p>4. Alternativ bei Ablauf des Zertifikats innerhalb von CERT_EXPIRATION_WARN_DAYS Systemereignis absetzen:</p> <ul style="list-style-type: none"> gSMC-K: TUC_KON_256 { topic = „CERT/CARD/EXPIRATION“; eventType = Op; severity = Info; parameters = („CARD_TYPE=gSMC-K, ICCSN=\$ICCSN, Konnektor=\$MGM_KONN_HOSTNAME, ZertName=\$Name des Zertifikatsobjekts gemäß TAB_KON_856, ExpirationDate=\$validity, DAYS_LEFT=\$validity-\$Today“); doLog = false; doDisp = \$doInformClients} Sonstige mit CARD(CardSession)): TUC_KON_256 { topic = „CERT/CARD/EXPIRATION“; eventType = Op; severity = Info; parameters = („CARD_TYPE=\$Type, ICCSN = \$ICCSN, CARD_HANDLE = \$CardHandle, CardHolderName = \$CardHolderName, ZertName=\$Name des Zertifikatsobjekts aus Schritt 1, ExpirationDate = \$validity, DAYS_LEFT = \$validity-\$Today“); doLog = false; doSisp = \$doInformClients} <p>5. expirationDate wird zurückgegeben.</p>
Varianten/ Alternativen	Keine
Fehlerfälle	<p>(→1) Zur angegebenen CardSession keine Karte gefunden: Fehlercode 4131.</p> <p>(→1) Für eGK, HBA, SM-B gilt: Wenn crypt=ECC und Kartengeneration<G2.1, bricht der TUC mit Warnung 4257 ab.</p> <p>(→1) Für gSMC-K gilt: Wenn crypt=ECC und beim Aufruf von TUC_KON_216 wird die Warnung 4256 zurückgegeben, dann wird der TUC nach Schritt 1 beendet und die Warnung 4257 an den Aufrufer zurückgegeben.</p> <p>(→2) Extraktion des Ablaufsdatums fehlgeschlagen: Fehlercode 4132.</p>

Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

4826

4827 **Tabelle 264: TAB_KON_600 Fehlercodes TUC_KON_033 „Zertifikatsablauf prüfen“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4131	Technical	Error	Zum angegebenen CardHandle keine Karte gefunden.
4132	Security	Error	Extraktion des Ablaufsdatums fehlgeschlagen
4257	Technical	Warning	ECC-Zertifikate nicht vorhanden auf Karte: <cardHandle>

4828

4829 [**<=**]4830 **4.1.9.4 Interne TUCs, auch durch Fachmodule nutzbar**4831 **4.1.9.4.1 TUC_KON_037 „Zertifikat prüfen“**

4832 TIP1-A_4696 - TUC_KON_037 „Zertifikat prüfen“

4833 Der Konnektor MUSS den technischen Use Case „Zertifikat prüfen“ gemäß TUC_KON_037 „Zertifikat prüfen“ umsetzen.

4835 [**<=**]

4836

4837 **Tabelle 265: TAB_KON_769 TUC_KON_037 „Zertifikat prüfen“**

Element	Beschreibung
Name	TUC_KON_037 „Zertifikat prüfen“
Beschreibung	Der TUC beschreibt <ul style="list-style-type: none"> die Prüfung eines X.509-Zertifikats gegen den Vertrauensraum
Auslöser	<ul style="list-style-type: none"> Aufruf in einem Fachmodul oder technischen Use Case
Vorbedingungen	<ul style="list-style-type: none"> aktuelle TSL-Informationen im Truststore vorhanden für QES X.509-Prüfung: eine aktuell gültige BNetzA-VL

Eingangsdaten	<ul style="list-style-type: none"> • certificate (ein X.509-Zertifikat (nonQES- oder QES-X.509-Zertifikat)) • EECertificateContainedInTSL - <i>optional; default: false</i> (true: Prüfung, ob ein EE-Zertifikat in der TSL vorhanden und zeitlich gültig ist; EE-Zertifikat wird in der TSL innerhalb eines "TSPService"-Eintrags ServiceTypeIdentifizier "http://uri.etsi.org/TrstSvc/Svctype/unspecified" erwartet. false: vollständige Prüfung eines X.509-Zertifikats mit TUC_PKI_018 bzw. TUC_PKI_030) • qualifiedCheck [not_required required if_QC_present] – (Art der Zertifikatsprüfung) • baseTime – <i>optional/verpflichtend, wenn ein Zeitpunkt zur Prüfung vorgegeben werden soll; default: Verwendung der Systemzeit des Konnektors</i> (Referenzzeitpunkt: Zeitpunkt, für den das Zertifikat geprüft werden soll) • offlineAllowNoCheck [Boolean] – <i>optional; default: false</i> (Angabe, ob es als Fehler (false) oder als Warnung (true) interpretiert werden soll, wenn eine OCSP-Prüfung nicht durchgeführt werden konnte.) • intendedKeyUsage – <i>optional/verpflichtend, wenn certificate ein nonQES-X.509-Zertifikat ist; wird bei QES nicht ausgewertet</i> (Vorgesehene KeyUsage) • nur für nonQES-Zertifikate: <ul style="list-style-type: none"> • policyList (Liste der zugelassenen Zertifikatstyp-OIDs gemäß [gemSpec_OID#GS-A_4445]) • intendedExtendedKeyUsage – <i>optional/verpflichtend, wenn certificate ein nonQES-X.509-Zertifikat ist; wird bei QES nicht ausgewertet</i> (Vorgesehene ExtendedKeyUsage) • gracePeriod – <i>optional/nur für nonQES-X.509-Zertifikat und wenn vom Standard abgewichen werden soll; wird bei QES nicht ausgewertet; default: CERT_OCSP_DEFAULT_GRACE_PERIOD_NONQES</i> (OCSP-GracePeriod: maximal zulässiger Zeitraum, den letzte OCSP-Antwort aus dem Cache bezüglich des Referenzzeitpunkts zurückliegen darf;) • validationMode [OCSP CRL NONE] – <i>optional/verpflichtend, wenn certificate ein nonQES-X.509-Zertifikat ist</i> (Prüfmodus: <ul style="list-style-type: none"> • OCSP: Es wird mittels OCSP geprüft. Dabei wird, falls die OCSP-GracePeriod noch nicht abgelaufen ist, die OCSP-Antwort aus dem Cache des
---------------	---

	<p>Konnektors verwendet. Für QES einzig erlaubter validationMode.</p> <ul style="list-style-type: none"> • CRL: Es wird gegen die aktuelle CRL auf dem Konnektor geprüft. • NONE: Keine Prüfung von Statusinformationen) • ocspResponse – <i>optional</i> (OCSPResponse des EE-Zertifikats) • getOCSPResponses [Boolean]– <i>optional; default: false</i> (true – OCSPResponse des geprüften Zertifikats soll an den Aufrufer zurückgegeben werden)
Komponenten	Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> • Status und Liste von Warnungen/Fehlern bei der Zertifikatsprüfung • role (aus dem Zertifikate ermittelte Rolle oder Berufsgruppe; siehe „Tab_PKI_406 OID-Festlegung technische Rolle in X.509-Zertifikaten“ oder „Tab_PKI_402 OID-Festlegung Rolle im X.509-Zertifikat für Berufsgruppen“ oder Tab_PKI_403 OID-Festlegung Institutionen im X.509-Zertifikat der SMC-B [gemSpec_OID]) • qcStatement – <i>optional/verpflichtend, wenn certificate ein QES-X.509-Zertifikat ist;</i> <i>nicht relevant bei EECertificateContainedInTSL=true.</i> (QCStatements des Zertifikats) • ocspResponsesRenewed – <i>optional/verpflichtend, wenn Eingabeparameter getOCSPResponses = true;</i> <i>nicht relevant bei EECertificateContainedInTSL=true.</i> (OCSP-Response des geprüften Zertifikats)

Standardablauf	<p>1. Falls <code>EECertificateContainedInTSL=false</code>:</p> <ol style="list-style-type: none"> Wenn das X.509-Zertifikat von einem CA-Zertifikat ausgestellt wurde, das in <code>CERT_IMPORTED_CA_LIST</code> enthalten ist, erfolgt eine Zertifikatsprüfung analog zu den Festlegungen in <code>TUC_PKI_018 „Zertifikatsprüfung“</code>. Dabei sind zu prüfen: <ul style="list-style-type: none"> - Zeitliche Gültigkeit, - mathematische Prüfung der Zertifikatssignatur, - die Prüfung der Zweckbindung gemäß der im Zertifikat hinterlegten <code>keyUsage</code> TSL-bezogene Prüfungen im <code>TUC_PKI_018</code> werden in diesem Fall nicht durchgeführt. Ebenso erfolgt keine OCSP-Prüfung. Wenn das zum X.509-Zertifikat gehörende CA-Zertifikat nicht in <code>CERT_IMPORTED_CA_LIST</code> enthalten ist, werden, abhängig vom Parameter <i>qualifiedCheck</i> folgende TUCs unter Weitergabe aller Eingangsparameter sowie der Negation des Werts von <code>MGM_LU_ONLINE</code> als Parameter „Offline-Modus“ aufgerufen: <ol style="list-style-type: none"> Für <code>qualifiedCheck = not_required</code>: <code>TUC_PKI_018 „Zertifikatsprüfung in der TI“</code> Ist der Eingangsparameter <code>ocspResponses</code> mit einer OCSP-Antwort gefüllt, so wird dieser übergeben. Die aktuell aus der OCSP-Abfrage resultierte OCSP-Antwort, falls vorhanden, wird an den Aufrufer weitergegeben. Für <code>qualifiedCheck = required</code>: <code>TUC_PKI_030 „QES-Zertifikatsprüfung“</code> Dabei wird das Basiszertifikat übergeben. Ist Eingangsparameter <code>ocspResponses</code> mit einer OCSP-Response gefüllt, so wird dieser übergeben. Die aktuell aus der OCSP-Abfrage resultierende OCSP-Response, falls vorhanden, wird an den Aufrufer weitergegeben. Für <code>qualifiedCheck = if_QC_present</code>: Ist im jeweiligen Signaturzertifikat mindestens ein <code>QCStatement</code> mit dem OID <code>id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)</code> enthalten, handelt es sich um eine QES-Zertifikatsprüfung mittels <code>TUC_PKI_030 „QES-Zertifikatsprüfung“</code>, sonst um eine nonQES-Zertifikatsprüfung mittels <code>TUC_PKI_018 „Zertifikatsprüfung“</code>. <p>Als Timeout wird beim Aufruf von <code>TUC_PKI_018</code> der Wert von <code>CERT_OCSP_TIMEOUT_NONQES</code> bzw. beim Aufruf von <code>TUC_PKI_030</code> der Wert von <code>CERT_OCSP_TIMEOUT_QES</code> übergeben (siehe auch Eingangsdaten von diesen TUCs in <code>[gemSpec_PKI]</code>).</p>
----------------	--

	<p>Für die QES-Zertifikatsprüfung wird das zu prüfende QES-Zertifikat an TUC_PKI_030 „QES-Zertifikatsprüfung“ übergeben.</p> <p>Wird im Aufruf der Eingangsparameter <code>getOCSPResponses = false</code> mit übergeben, wird keine OCSP-Response an den Aufrufer zurückgegeben.</p> <p>Als <code>TOLERATE_OCSP_FAILURE</code> wird beim Aufruf von TUC_PKI_018 <code>offlineAllowNoCheck</code> verwendet.</p> <p>Wenn der Eingangsparameter <code>validationMode</code> („Prüfmodus“) den Wert <code>NONE</code> hat, werden die TUC_PKI_018-Eingangsparameter</p> <ul style="list-style-type: none"> • „Offline-Modus“ unabhängig von <code>MGM_LU_ONLINE</code> auf „ja“ gesetzt und • „Prüfmodus“ auf „OCSP“. <p>2. Falls <code>EECertificateContainedInTSL=true</code></p> <ol style="list-style-type: none"> a. Prüfe, ob das in <code>certificate</code> übergebene X.509-Zertifikat in der TSL innerhalb eines "TSPService"-Eintrags mit dem <code>ServiceTypeIdentifier</code> "<code>http://uri.etsi.org/TrstSvc/Svctype/unspecified</code>" aufgeführt ist. b. Prüfe zeitliche Gültigkeit von <code>certificate</code> zum Prüfzeitpunkt aktuelle Systemzeit durch Aufruf von TUC_PKI_002. c. Ermittle <code>role</code> von <code>certificate</code> durch Aufruf von TUC_PKI_009. <p>3. Der Status der Prüfung und die ermittelten Ausgangsdaten werden zurückgegeben.</p>
--	--

Varianten/ Alternativen	
Fehlerfälle	TUC_KON_037 im kritischen Betriebszustand EC_TSL_Out_Of_Date_Beyond_Grace_Period aufgerufen: Fehlercode 4002. -> 2a) certificate ist nicht in der TSL enthalten
Nichtfunktionale Anforderungen	Der Konnektor MUSS unter Einhaltung aller anderen Anforderungen an die Zertifikatsprüfung die Anzahl der OCSP- Abfragen minimieren. Dies MUSS durch Caching (unter Berücksichtigung der Grace Period) und DARF NICHT durch Bündelung von OCSP-Anfragen geschehen.
Zugehörige Diagramme	keine

Tabelle 266: TAB_KON_601 Fehlercodes TUC_KON_037 „Zertifikat prüfen“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases treten folgende Fehlercodes auf.			
4002	Security	Fatal	Der Konnektor befindet sich in einem kritischen Betriebszustand
4260	Security	Error	Zertifikat nicht vorhanden in TSL

4.1.9.4.2 TUC_KON_042 „CV-Zertifikat prüfen“

TIP1-A_5482 - TUC_KON_042 „CV-Zertifikat prüfen“

Der Konnektor MUSS den technischen Use Case „CV-Zertifikat prüfen“ gemäß TUC_KON_042 „CV-Zertifikat prüfen“ umsetzen.

[<=]

Tabelle 267: TAB_KON_818 TUC_KON_042 „CV-Zertifikat prüfen“

Element	Beschreibung
Name	TUC_KON_042 „CV-Zertifikat prüfen“
Beschreibung	Die Gültigkeit eines (EndEntity-)CV-Zertifikats wird geprüft. Es werden folgende Prüfungen durchgeführt: Kryptographische Prüfung der Signaturen des End-Entity-CV-Zertifikats und des CVC-CA-Zertifikats <ul style="list-style-type: none"> Zeitliche Gültigkeit nach dem Schalenmodell (nur CV-Zertifikate der Generation 2).
Auslöser	<ul style="list-style-type: none"> Aufruf in einem Fachmodul oder

	<ul style="list-style-type: none"> Technischen Use Case
Vorbedingungen	<ul style="list-style-type: none"> keine
Eingangsdaten	<ul style="list-style-type: none"> eeCertificate (zu prüfendes kartenindividuelles CV-Zertifikat) caCertificate (das CVC-CA-Zertifikat mit dem öffentlichen Schlüssel der zugehörigen ausstellenden CA)
Komponenten	Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> status [Boolean] (Ergebnis der Prüfung; true: CV-Zertifikat ist gültig false: CV-Zertifikat ist ungültig)
Standardablauf	<p>1. Abhängig von der Zertifikats-Generation wird Vorgehen A oder B gewählt.</p> <p>A. Prüfung von CV-Zertifikaten der Generation 1: Die CVC-Prüfung setzt sich gemäß GS-A_4668 [gemSpec_PKI#8.7] aus folgenden Schritten zusammen.</p> <p>i. Prüfe die Signatur des CA-Zertifikats caCertificate mit dem öffentlichen Root-Schlüssel der ausstellenden CVC-Root-CA. Der benötigte Root-Key befindet sich auf der gSMC-K in der Datei EF.PuK.RCA.CS.R2048.</p> <p>ii. Prüfe die Signatur des (EndEntity-)CV-Zertifikats eeCertificate mit dem öffentlichen Schlüssel der ausstellenden CVC-CA (aus dem CVC-CA-Zertifikat extrahiert).</p> <p>B. Prüfung von CV-Zertifikaten der Generation 2: Die CVC-Prüfung setzt sich gemäß GS-A_5009, ... GS-A_5012 [gemSpec_PKI#8.8] aus folgenden Schritten zusammen:</p> <p>i. Prüfe die kryptographische Korrektheit der Signatur des CA-Zertifikats caCertificate mit dem öffentlichen Root-Schlüssel der ausstellenden CVC-Root-CA. Der benötigte Root-Key befindet sich im Truststore des Konnektors.</p> <p>ii. Prüfe die kryptographische Korrektheit der Signatur des (EndEntity-)CV-Zertifikats certificate mit dem öffentlichen Schlüssel der ausstellenden CVC-CA (aus dem CVC-CA-Zertifikat extrahiert).</p> <p>iii. Prüfe die zeitliche Gültigkeit des (EndEntity-)CV-Zertifikates,</p>

	des CVC-CA-Zertifikates und CVC-Root-CA-Zertifikates nach dem Schalenmodell. 2. Der Status <i>status</i> der Prüfung wird zurückgegeben.
Varianten/Alternativen	(→ B.i) Mathematische Korrektheitsprüfung CV-Zertifikate mit Cross-CV-Zertifikat (vgl. Varianten/Alternativen von TUC_KON_005)
Fehlerfälle	(→ A.i) kryptographische (mathematische) Prüfung des CVC-CA-Zertifikats fehlgeschlagen, Fehlercode 4196. (→ A.ii) kryptographische (mathematische) Prüfung des (EndEntity-) CV-Zertifikats fehlgeschlagen, Fehlercode 4196. (→ B.i) das benötigte Cross-CV-Zertifikat ist nicht vorhanden, Fehlercode 4228 (→ B.i) kryptographische (mathematische) Prüfung des CVC-CA-Zertifikats fehlgeschlagen, Fehlercode 4196. (→ B.ii) kryptographische Prüfung des (EndEntity-)CV-Zertifikats fehlgeschlagen, Fehlercode 4196. (→ B.iii) zeitliche Gültigkeit eines der CV-Zertifikate ist abgelaufen, Fehlercode 4196.
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

4851

4852 **Tabelle 268: TAB_KON_819 Fehlercodes TUC_KON_042 „CV-Zertifikat prüfen“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4196	Technical	Error	Fehler bei der CV-Zertifikatsprüfung
4228	Technical	Error	das benötigte Cross-CV-Zertifikat ist nicht vorhanden

4853 **4.1.9.4.3 TUC_KON_034 „Zertifikatsinformationen extrahieren“**

4854 TIP1-A_4697 - TUC_KON_034 „Zertifikatsinformationen extrahieren“

4855 Der Konnektor MUSS den technischen Use Case TUC_KON_034 „Zertifikatsinformationen extrahieren“ umsetzen.

4856

4857 **Tabelle 269: TAB_KON_770 TUC_KON_034 „Zertifikatsinformationen extrahieren“**

Element	Beschreibung
Name	TUC_KON_034 „Zertifikatsinformationen extrahieren“

Beschreibung	Dieser TUC beschreibt die Extraktion der fachlich zentralen Informationen aus bestimmten Zertifikaten einer gesteckten Karte eines Mandanten.
Auslöser	<ul style="list-style-type: none"> Aufruf durch ein Fachmodul oder eine Basisanwendung des Konnektors
Vorbedingungen	Keine
Eingangsdaten	<ul style="list-style-type: none"> cardSession – <i>optional/verpflichtend für den Zugriff auf eGK, HBA, SM-B oder gSMC-KT</i> checkSMCK [Boolean] – <i>optional/verpflichtend für gSMC-K;</i> (Referenz auf eine/die gSMC-K, alternativ zu cardSession) qes [Boolean] - <i>optional; default: false</i> – (Angabe, ob die QES-Identität oder die nonQES-Identität der Karte interessiert) crypt - <i>optional; default = RSA</i> (kryptographischer Algorithmus, für welchen das Zertifikat ermittelt wird; Wertebereich: ECC, RSA)
Komponenten	Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> certType [C.CH.AUT C.HP.AUT C.HCI.AUT C.HP.QES] (Zertifikatstyp) certInfo (Zertifikatsinformationen, bestehend aus SerialNumber, Issuer, Subject, Rollen, registrationNumber und ggf. id-etsi-qcs-QcCompliance, siehe Standardablauf) qcStatements – <i>optional/nur wenn certType = C.HP.QES</i> (QCStatements)
Nachbedingungen	Keine
Standardablauf	<ol style="list-style-type: none"> Je nach Kartentyp wird aus der Karte das passende Zertifikat über TUC_KON_216 "LeseZertifikat" {selektiertes Zertifikat} ausgelesen. Das Zertifikatsobjekt (fileIdentifier und folder)/Zertifikatsbezeichnung wird für die jeweilige Karte unter Berücksichtigung des kryptographischen Verfahrens crypt gemäß TAB_KON_858 bzw. TAB_KON_856 ermittelt. <ol style="list-style-type: none"> Bei qes = false: <ol style="list-style-type: none"> Für die eGK: C.CH.AUT

	<ul style="list-style-type: none"> ii. Für den HBAX: C.HP.AUT iii. Für SM-B: C.HCI.AUT iv. Für gSMC-K: C.NK.VPN <p>b. Bei qes = true:</p> <ul style="list-style-type: none"> i. Für den HBAX: C.HP.QES <p>2. Die Zertifikatsbezeichnung aus Schritt 1 („C.XXX.YYY.ZZZZ“) wird als Ausgangsdatum „certType“ zurückgegeben.</p> <p>3. Zusätzlich werden aus dem Zertifikat folgende Informationen extrahiert und zurückgegeben:</p> <ul style="list-style-type: none"> a. X509SerialNumber b. Issuer (DistinguishedName) nach RFC 2253 c. Subject (DistinguishedName) nach RFC 2253 d. Aus der Extension Admission: <ul style="list-style-type: none"> i. eine Liste von Rollen durch Aufruf von TUC_PKI_009 „Rollenermittlung“ ii. registrationNumber (=Telematik-ID; falls vorhanden) e. id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) in QCStatements, falls vorhanden f. Restriction, falls vorhanden g. validity
Varianten/Alternativen	Keine
Fehlerfälle	<p>(→1) Wenn im Aufrufkontext (also erreichbar durch den Mandanten) zum angegebenen CardHandle keine Karte gefunden werden kann, bricht der TUC mit Fehlercode 4146 ab.</p> <p>(→1b) Ist bei Angabe von QES=true auf der Karte keine QES-Identität zu finden, bricht der TUC mit Fehlercode 4147 ab. Für die Kombination QES=true mit einer eGK bricht der TUC mit Fehlercode 4148 ab (QES-Zertifikate der eGK werden noch nicht unterstützt).</p> <p>(→1) Für eGK, HBA, SM-B gilt: Wenn crypt=ECC und Karte vom Typ <G2.1, bricht der TUC mit Warnung 4257 ab.</p> <p>(→1) Für gSMC-K gilt: Wenn crypt=ECC und TUC_KON_216 Warnung 4256 liefert, bricht der TUC mit Warnung 4257 ab.</p> <p>(→1) Wenn aus anderen Gründen die Extraktion der Zertifikatsinformationen fehlschlägt, bricht der TUC mit Fehlercode 4148 ab.</p>

Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

Tabelle 270: TAB_KON_602 Fehlercodes TUC_KON_034 „Zertifikatsinformationen extrahieren“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4146	Technical	Error	Kartenhandle existiert nicht
4147	Technical	Error	Zertifikat nicht vorhanden (z. B. kein QES-Zertifikat in SM-B)
4148	Technical	Error	Fehler beim Extrahieren von Zertifikatsinformationen
4257	Technical	Warning	ECC-Zertifikate nicht vorhanden auf Karte: <cardHandle>

[<=]

4.1.9.5 Operationen an der Außenschnittstelle

TIP1-A 4698-02 **TIP1-A 4698** - Basisanwendung Zertifikatsdienst

Der Konnektor MUSS Clientsystemen eine Basisanwendung Zertifikatsdienst zur Verfügung stellen

Tabelle 271: TAB_KON_771 Basisanwendung Zertifikatsdienst

Name	CertificateService	
Version (KDV)	6.0.0 (WSDL-Version+), 6.0.1 (XSD-Version) 6.0.1 (WSDL-Version), 6.0.2 (XSD-Version)	
Namensraum	Siehe Anhang D	
Namensraum-Kürzel	CERT für Schema und CERTW für WSDL	
Operationen	Name	Kurzbeschreibung
	ReadCardCertificate	Zertifikat von einer Karte lesen
	CheckCertificateExpiration	Ablaufdatum von Zertifikaten erfragen

	VerifyCertificate	Prüfung des Status eines Zertifikats
WSDL	CertificateService.wsdl (WSDL-Version 6.0.0) CertificateService v6 0 1.wsdl	
Schema	CertificateService.xsd (XSD-Version 6.0.1) CertificateService v6 0 2.xsd	

4869

4870 [**<=**]

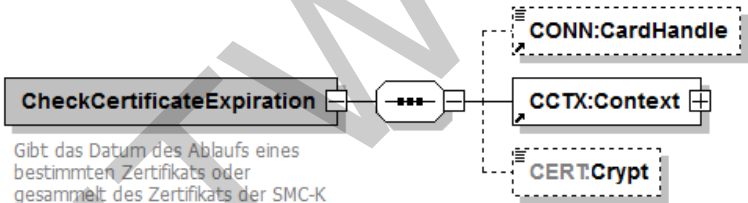
4871 4.1.9.5.1 CheckCertificateExpiration

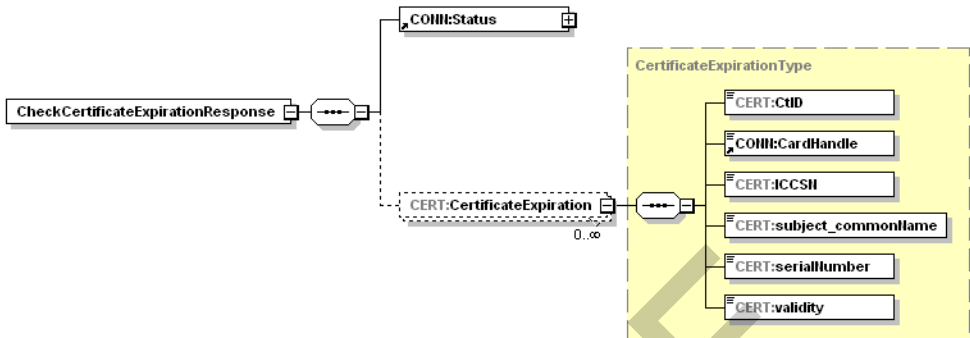
4872 TIP1-A_4699 - Operation CheckCertificateExpiration

4873 Die Basisanwendung Zertifikatsdienst des Konnektors MUSS an der Clientschnittstelle
 4874 eine Operation CheckCertificateExpiration anbieten.

4875

4876 **Tabelle 272: TAB_KON_676 Operation CheckCertificateExpiration**

Name	CheckCertificateExpiration	
Beschreibung	Gibt das Datum des Ablaufs eines bestimmten Zertifikats oder gesammelt des Zertifikats der gSMC-K sowie aller gesteckten HBAX und SM-B des Mandanten zurück.	
Aufruf- parameter		
	Name	Beschreibung
	CardHandle	Optional. Identifiziert die Karte, deren Zertifikate geprüft werden sollen. Wird der Parameter nicht angegeben, so werden alle für den Konnektor erreichbaren Karten (inkl. gSMC-K), die zum Mandanten passen, berücksichtigt. Die Operation CheckCertificateExpiration DARF das Lesen von Zertifikaten der eGK NICHT unterstützen.
	Context	MandantId, CsId, WorkplaceId verpflichtend; UserId optional
	Crypt	Optional; Default: RSA Gibt den kryptographischen Algorithmus vor, für den das Zertifikat ermittelt werden soll. Wertebereich: RSA, ECC

		<ul style="list-style-type: none"> • RSA: Zertifikat für RSA-2048 • ECC: Zertifikat für ECC-256
Rückgabe		
	Status	Enthält den Ausführungsstatus der Operation.
	CertificateExpiration	Eine Liste von Tupeln aus (CtID, CardHandle, ICCSN, subject.CommonName, serialNumber, validity) der Zertifikate der Karten. Für die gSMC-K soll in CertificateExpiration/CtID und CertificateExpiration/CardHandle jeweils ein Leerstring zurückgegeben werden.
Vorbedingungen	Keine	
Nachbedingungen	Keine	

4877 Der Ablauf der Operation CheckCertificateExpiration ist in Tabelle TAB_KON_677
 4878 beschrieben:
 4879

4880 **Tabelle 273: TAB_KON_677 Ablauf CheckCertificateExpiration**

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab. Wird die Operation für einen nicht unterstützten Kartentypen aufgerufen, so bricht die Operation mit Fehler 4058 ab.
2.	TUC_KON_000 „Prüfe Zugriffsberechtigung“	Die Prüfung erfolgt durch den Aufruf TUC_KON_000 { mandantId = \$context.mandantId; clientSystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; userId = \$context.userId;

		<code>cardHandle = \$cardHandle</code> <code>}</code> Tritt bei der Prüfung ein Fehler auf, bricht die Operation mit Fehlercode aus TUC_KON_000 ab.
3.	enumerateCardHandles	Wenn der Parameter CardHandle übergeben wurde, wird dieser als einziges Element in eine Liste gepackt. Wenn der Parameter CardHandle leer war, wird eine Liste der CardHandles aller für den Konnektor erreichbaren Karten (inkl. gSMC-K), die zum Mandanten passen, erstellt.
Für jedes CardHandle der in Schritt 3 erzeugten Liste werden folgende Schritte ausgeführt, für die gSMC-Ks die Schritte 5 und 6: Falls Schritt 5 der TUC_KON_033 die Warnung 4257 zurückgibt, wird Schritt 6 nicht ausgeführt und die Schritte für das CardHandle der in Schritt 3 erzeugten Liste weiter ausgeführt. Die Warnung 4257 wird über alle CardHandle akkumuliert und <komma-separierte List von cardHandle> für den Fehlertext erzeugt.		
4.	TUC_KON_026 „Liefere CardSession“	Ermittle CardSession über TUC_KON_026 { <code>mandatId = MandantId;</code> <code>clientSystemId = ClientSystemId;</code> <code>cardHandle = CardHandle;</code> <code>userId = UserId</code> }
5.	TUC_KON_033 „Zertifikatsablauf prüfen“	Das Gültigkeitsdatum des Zertifikats wird geprüft mit TUC_KON_033 { <code>cardSession;</code> <code>doInformClients = false;</code> <code>Crypt;</code> <code>}</code> bzw. TUC_KON_033 { <code>checkSMCK = true;</code> <code>doInformClients = false;</code> <code>Crypt;</code> <code>}</code>
6.	TUC_KON_034 „Zertifikatsinformationen extrahieren“	Beim Aufruf des TUC_KON_034 ist der Parameter <code>qes = false</code> zu setzen. Aus den jeweiligen Rückgabewerten entsteht eine Liste aus Tupeln (CtID, CardHandle, ICCSN, subject.CommonName, serialNumber, validity). Diese wird von der Operation zurückgegeben.

4881

Tabelle 274: TAB_KON_603 Fehlercodes „CheckCertificateExpiration“

Fehlercode	ErrorType	Severity	Fehlertext
------------	-----------	----------	------------

Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:

4000	Technical	Error	Syntaxfehler
4058	Security	Error	Aufruf nicht zulässig
4257	Technical	Warning	ECC-Zertifikate nicht vorhanden auf Karte: <komma-separierte List von cardHandle>

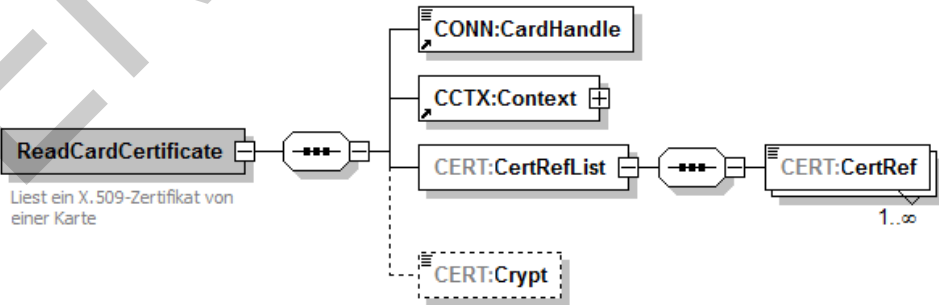
[<=]

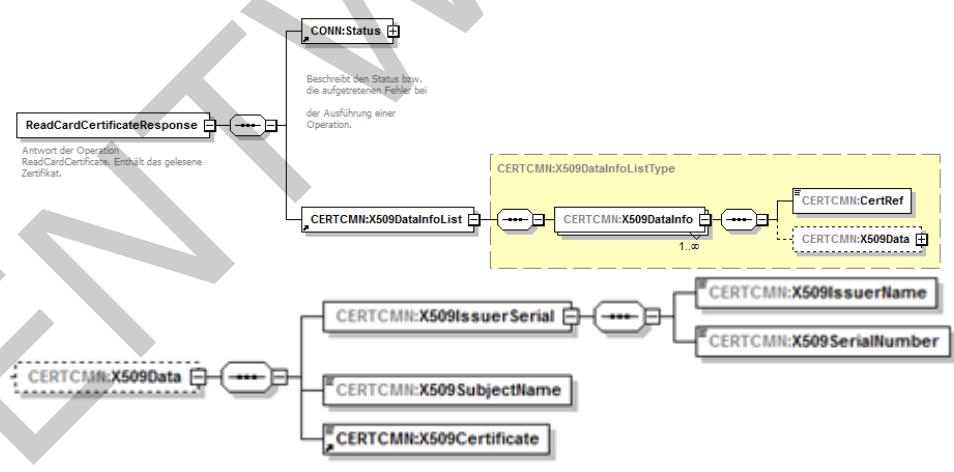
4.1.9.5.2 ReadCardCertificate

TIP1-A_4700 - Operation ReadCardCertificate

Die Basisanwendung Zertifikatsdienst des Konnektors MUSS an der Clientschnittstelle eine Operation ReadCardCertificate wie in Tabelle TAB_KON_678 Operation ReadCardCertificate beschrieben anbieten.

Tabelle 275: TAB_KON_678 Operation ReadCardCertificate

Name	ReadCardCertificate	
Beschreibung	Liest X.509-Zertifikate von einer Karte.	
Aufrufparameter		
	Name	Beschreibung

	CardHandle	Gibt die Karte an, von der das Zertifikat gelesen werden soll. Es können Zertifikate von HBAx (HBA, HBA-VK), SM-B ausgelesen werden. Die Operation ReadCardCertificate DARF das Lesen von Zertifikaten der eGK NICHT unterstützen.
	Context	Aufrufkontext (Mandant)
	CertRefList	Gibt an, welche(s) Zertifikat(e) gelesen werden soll. Mögliche Werte für CertRef sind: C.AUT, C.ENC, C.SIG, C.QES
	Crypt	Optional; Default: RSA Gibt den kryptographischen Algorithmus vor, für den das Zertifikat ermittelt werden soll. Wertebereich: RSA, ECC <ul style="list-style-type: none"> • RSA: Zertifikat für RSA-2048 • ECC: Zertifikat für ECC-256
Rückgabe 		
	Status	Enthält den Ausführungsstatus der Operation.
	CertRef	Dieses Element beinhaltet die Referenz des Zertifikats, welches bei der Anfrage übergeben wurde.

	X509Data	Inhalt des über die CertRef referenzierten Zertifikats. Ist das referenzierte Zertifikat nicht vorhanden, so wird dieses Element nicht vom Konnektor gefüllt.	
		X509Issuer Name	Enthält den Issuer-Name des Zertifikats. Bezüglich des Encodings sind die in [XMLDSig#4.4.4.4.1] angegebenen Regeln zu beachten (Escaping von Sonderzeichen etc.)
		X509Serial Number	Enthält die serialNumber des Zertifikats.
		X509Subject Name	Enthält das Feld subject.CommonName. Bezüglich des Encodings sind die in [XMLDSig#4.4.4.4.1] angegebenen Regeln zu beachten (Escaping von Sonderzeichen etc.)
		X509 Certificate	Enthält das base64-codierte Zertifikat, dessen Binärstruktur wiederum ASN.1-codiert (gemäß [COMMON_PKI]) vorliegt.
Vorbedingungen	Keine		
Nachbedingungen	Keine		

4892 Der Ablauf der Operation ReadCardCertificate ist in Tabelle TAB_KON_679 Ablauf
 4893 ReadCardCertificate beschrieben:
 4894

4895 **Tabelle 276: TAB_KON_679 Ablauf ReadCardCertificate**

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab. Wurde als Zielkarte eine eGK adressiert, wird

		Fehlercode 4090 zurückgeliefert.
2.	TUC_KON_000 „Prüfe Zugriffs- berechtigung“	Die Prüfung erfolgt durch den Aufruf TUC_KON_000 { mandantId = \$context.mandantId; clientsystemId = \$context.clientsystemId; workplaceId = \$context.workplaceId; userId = \$context.userId; cardHandle = \$cardHandle } Tritt bei der Prüfung ein Fehler auf, bricht die Operation mit Fehlercode aus TUC_KON_000 ab.
3.	TUC_KON_026 „Liefere CardSession“	Ermittle CardSession über TUC_KON_026 { mandatId = \$context.mandantId; clientsystemId = \$context.clientsystemId; cardHandle = \$context.cardHandle; userId = \$context.userId } }
4.	getEF	Für jedes Paar von CertRef und CardHandle wird in Abhängigkeit des Parameters Crypt gemäß Tabelle TAB_KON_858 das zu lesende File (EF) bestimmt: Ist die übergebene Zertifikatsreferenz ungültig, wird Fehlercode 4149 zurückgegeben. Das Lesen von Zertifikaten der eGK ist aus Sicherheitsgründen für Clientsysteme nicht zulässig.
	TUC_KON_216 „LeseZertifikat“	Für jedes Paar von CardHandle und EF wird nun durch Aufruf von TUC_KON_216 „LeseZertifikat“ das Zertifikat ausgelesen. Falls TUC_KON_216 die Warnung 4256 zurückgibt, wird die Operation abgebrochen und Fehler 4258 zurückgegeben.
6.	Zertifikatsattribute extrahieren	Aus jedem Zertifikat werden die zu liefernden Attribute extrahiert. Die Ergebnisstruktur wird mit den erhaltenen Rückgabewerten gefüllt.

4896
4897

4898

Tabelle 277: TAB_KON_604 Fehlercodes „ReadCardCertificate“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler
4149	Technical	Error	Ungültige Zertifikatsreferenz
4090	Security	Error	Zugriff auf eGK nicht gestattet

4258	Technical	Error	ECC-Zertifikate nicht vorhanden auf Karte: <cardHandle>
------	-----------	-------	--

4899

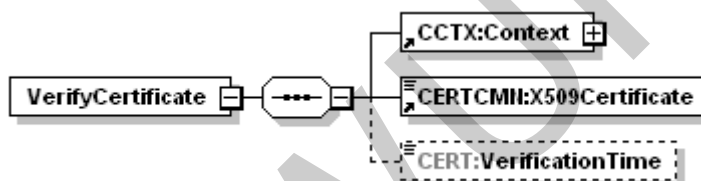
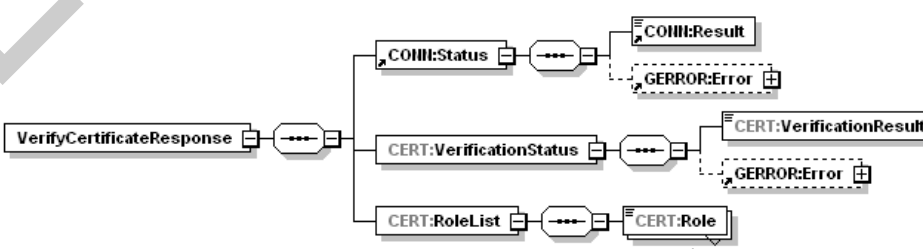
4900 [\leq]

4901 4.1.9.5.3 VerifyCertificate

4902 TIP1-A_5449 - Operation VerifyCertificate

4903 Die Basisanwendung Zertifikatsdienst des Konnektors MUSS an der Clientschnittstelle
 4904 eine Operation VerifyCertificate wie in Tabelle TAB_KON_795 Operation VerifyCertificate
 4905 beschreiben anbieten.
 4906

4907 **Tabelle 278: TAB_KON_795 Operation VerifyCertificate**

Name	VerifyCertificate	
Beschreibung	Prüft den Status eines Zertifikats.	
Aufrufparameter		
	Name	Beschreibung
	CCTX:Context	Aufrufkontext (Mandant)
	CERTCMN:X509Certificate	Zu prüfendes Zertifikat (base64 kodiert), wie in Response zur Operation ReadCardCertificate enthalten.
	CERT:VerificationTime	Der für die Prüfung zu verwendende Referenzzeitpunkt. Falls der Parameter nicht angegeben ist, wird als Referenzzeitpunkt die Systemzeit verwendet.
Rückgabe		
	CONN:Status	Enthält den Ausführungsstatus der Operation.
	CERT:VerificationStatus	Enthält eines der drei möglichen Prüfungsergebnisse in CERT:VerificationResult

		<ul style="list-style-type: none"> • VALID • INCONCLUSIVE • INVALID <p>sowie weiter Details zu den Zuständen „INCONCLUSIVE“ und „INVALID“ in GERROR:Error.</p>
	CERT:RoleList	OIDs der im Zertifikat gespeicherten Rollen.
Vorbedingungen	Keine	
Nachbedingungen	Keine	

4908 Der Ablauf der Operation VerifyCertificate ist in Tabelle TAB_KON_797 Ablauf
 4909 VerifyCertificate beschrieben:
 4910

4911 **Tabelle 279: TAB_KON_797 Ablauf VerifyCertificate**

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Die übergebenen Werte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	TUC_KON_037 „Zertifikat prüfen“	<p>Die Zertifikatsprüfung erfolgt durch Aufruf von TUC_KON_037. Als Parameter des TUC-Aufrufs gilt für Zertifikate aus CERT_IMPORTED_CA_LIST: {</p> <pre> certificate = CERTCMN:X509Certificate qualifiedCheck = not_required; baseTime = CERT:VerificationTime; offlineAllowNoCheck = true; policyList= keine Einschränkung; intendedKeyUsage=empty; intendedExtendedKeyUsage=empty; gracePeriod = empty; validationMode = NONE; ocspResponses (OCSP-Response/Liste von OCSP-Responses = empty } für alle anderen Zertifikate gilt: { certifiacate = CERTCMN:X509Certificate qualifiedCheck =if_QC_present; baseTime = CERT:VerificationTime; offlineAllowNoCheck = true; policyList = alle zugelassenen Zertifikatstyp-OIDs; intendedKeyUsage = empty; intendedExtendedKeyUsage = empty; gracePeriod = empty; </pre>

		validationMode = OCSP; ocspResponses = empty}.
3.		Wenn der Prüfprozess fehlerhaft war und nicht zu einem Ergebnis im Sinne eines VerificationResult führt, wird eine FaultMessage erzeugt. War der Prüfprozess erfolgreich, wird eine VerifyCertificateResponse mit CONN:Status/CONN:Result=OK, dem VerificationStatus (als Ergebnis der Zertifikatsprüfung) und den ermittelten Rollen-OIDs erzeugt. Ein Prüfergebnis „INCONCLUSIVE“ bzw. „INVALID“ wird in CERT:VerificationStatus/GERROR:Error mit den zugehörigen Fehlermeldungen detailliert (in diesem Fall kann CONN:Status/CONN:Result=OK oder CONN:Status/CONN:Result=Warning gesetzt sein).

4912 **Tabelle 280: TAB_KON_800 Fehlercodes „VerifyCertificate“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler

4913
4914
4915

[<=]

4916 **4.1.9.6 Betriebsaspekte**

4917 *4.1.9.6.1 TUC_KON_035 „Zertifikatsdienst initialisieren“*

4918 TIP1-A_4701 - TUC_KON_035 „Zertifikatsdienst initialisieren“

4919 In der Bootup-Phase MUSS der Konnektor den Zertifikatsdienst durch Aufruf des
4920 TUC_KON_035 „Zertifikatsdienst initialisieren“ initialisieren.

4921

4922 **Tabelle 281: TAB_KON_772 TUC_KON_035 „Zertifikatsdienst initialisieren“**

Element	Beschreibung
Name	TUC_KON_035 „Zertifikatsdienst initialisieren“
Beschreibung	Der TUC beschreibt den gesamten Ablauf der Initialisierung des TrustStore im Rahmen der betrieblichen Prozesse: Prüfung der Aktualität, Integrität und Authentizität der Einträge im TrustStore.
Auslöser	<ul style="list-style-type: none"> • Bootup des Konnektors
Vorbedingungen	keine
Eingangsdaten	keine
Komponenten	Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> • Status der Initialisierung des TrustStore

Nachbedingungen	Keine
Standardablauf	<p>Für den übergebenen Status der Initialisierung des TrustStore werden folgende Schritte durchgeführt:</p> <ol style="list-style-type: none"> 1. Durch eine DNS-Anfrage an den DNS-Forwarder zur Auflösung der SRV-RR mit dem Bezeichner "_ocsp._tcp.<DOMAIN_SRVZONE_TI>„ erhält der Konnektor Adressen des http-Forwarders des VPN-Zugangsdienststandortes. 2. Falls in den letzten 24 Stunden keine Aktualisierung der TSL und CRL im Truststore stattgefunden hat, aktualisiert der Konnektor die TSL durch den Aufruf von TUC_KON_032 „TSL aktualisieren“ und die CRL durch den Aufruf von TUC_KON_040 „CRL aktualisieren“. 3. Falls im Zeitraum von CERT_BNETZA_VL_UPDATE_INTERVAL keine Aktualisierung der BNetza VL stattgefunden hat, aktualisiert der Konnektor die BNetza VL durch den Aufruf von TUC_KON_031 „BNetza-VL aktualisieren“. 4. Der Konnektor prüft die Gültigkeitsdauer der Zertifikate aller gesteckten Karten (inkl. gSMC-K) mittels Aufruf von: <u>für gSMC-K</u> TUC_KON_033{checkSMCK; doInformClients=Ja; crypt = ECC} TUC_KON_033{checkSMCK; doInformClients=Ja; crypt = RSA} <u>für jede gesteckte G2.0 Karte</u> TUC_KON_033{cardSession; doInformClients=Ja; crypt = RSA} <u>für jede gesteckte ab G2.1 Karte</u> TUC_KON_033{cardSession; doInformClients=Ja; crypt = ECC} TUC_KON_033{cardSession; doInformClients=Ja; crypt = RSA} 5. Der Konnektor liest von der gSMC-K den öffentlichen Schlüssel des CVC-Root-Zertifikats und speichert diesen im TrustStore [gemSpec_gSMC-K_ObjSys#5.3.10].
Varianten/ Alternativen	Keine
Fehlerfälle	Keine
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

4923 **Tabelle 282: TAB_KON_605 Fehlercodes TUC_KON_035 „Zertifikatsdienst initialisieren“**

Fehlercode	ErrorType	Severity	Fehlertext
------------	-----------	----------	------------

Neben den Fehlercodes der aufgerufenen technischen Use Cases können keine weiteren Fehlercodes auftreten.

4924
4925 **[<=]**

4926 TIP1-A_4702 - Konfigurierbarkeit des Zertifikatsdienstes
4927 Der Administrator MUSS die in TAB_KON_606 aufgelisteten Parameter über die
4928 Managementschnittstelle konfigurieren und die in TAB_KON_733 aufgelisteten Parameter
4929 ausschließlich einsehen können.
4930

4931 **Tabelle 283: TAB_KON_606 Konfiguration des Zertifikatsdienstes**

ReferenzID	Belegung	Bedeutung
CERT_TSL_DEFAULT_ GRACE_PERIOD_DAYS	X Tage	Default Grace Period TSL in Tagen Gibt an, wie viele Tage der Konnektor mit einer zeitlich abgelaufenen TSL weiter betrieben werden kann. Der Wert MUSS zwischen 1 und 30 Tagen liegen. Default-Wert = 30 Tage <i>Hinweis: Vor dem zeitlichen Ablauf einer TSL wird mit ausreichendem Vorlauf eine neue TSL verteilt. Sollte die TSL dennoch ablaufen und der Konfigurationswert überschritten werden, kann eine neue TSL immer noch lokal geladen werden (TIP1-A_4705 „TSL manuell importieren“).</i>
CERT_OCSP_DEFAULT_ GRACE_PERIOD_ NONQES	X Minuten	Default Grace Period OCSP für nonQES in Minuten. Der Wert MUSS zwischen 0 und 20 Minuten liegen. Default-Wert = 10 Minuten
CERT_OCSP_TIMEOUT_ NONQES	X Sekunden	Timeout für OCSP-Abfragen bei der Prüfung von nonQES-Zertifikaten. Der Wert MUSS zwischen 1 und 120 Sekunden liegen. Default-Wert = 10 Sekunden
CERT_OCSP_TIMEOUT_ QES	X Sekunden	Timeout für OCSP-Abfragen bei der Prüfung von QES-Zertifikaten. Der Wert muss zwischen 1 und 120 Sekunden liegen. Default-Wert = 10 Sekunden
CERT_EXPIRATION_ WARN_DAYS	X Tag(e)	Warnung X Tage vor Ablauf von Zertifikaten im Managementinterface und per Ereignis. Der Wert muss zwischen 0 und 180 Tagen (0=keine Warnung) liegen. Default-Wert = 90 Tage
CERT_EXPIRATION_ CARD_CHECK_DAYS	X Tag(e)	Alle X Tage wird der Ablauf aller gesteckten Karten überprüft. Der Wert muss zwischen 0

		und 365 liegen (0=kein Check). Default-Wert = 1 Tag
CERT_IMPORTED_CA_LIST	Liste von manuell importierten CA-Zertifikaten	Der Administrator MUSS CA-Zertifikate importieren, anzeigen und löschen können. Der Konnektor DARF CA-Zertifikate zur Ableitung von QES-Zertifikaten NICHT importieren. Default-Wert = leere Liste
CERT_BNETZA_VL_UPDATE_INTERVAL	X Stunden	Intervall, in dem die BNetzA VL auf Aktualität geprüft werden muss. Der Wert MUSS zwischen 1 Stunde und 168 Stunden (7 Tage) liegen. Default-Wert = 24 Stunden

4932 **Tabelle 284: TAB_KON_733 Einsehbare Konfigurationsparameter des Zertifikatsdienstes**

ReferenzID	Belegung	Bedeutung
CERT_CRL_DOWNLOAD_ADDRESS	2 URIs	Download-Adressen für die CRL
CERT_OCSP_FORWARDER_ADDRESS	2 FQDNs	Adressen der OCSP-Forwarder (HTTPS-Proxy) beim Zugangsdienstprovider Der Administrator muss in geeigneter Weise einen Test auslösen können, ob einer der Server per ICMP-Echo (ping) erreichbar ist und ob ein (beliebiger) OCSP-Request zu einer erhaltenen OCSP-Antwort führt.
CERT_OCSP_FORWARDER_PORT	TCP-Port	TCP-Port des OCSP-Forwarders (HTTPS-Proxy) beim Zugangsdienstprovider

4933
4934 **[<=]**

4937 TIP1-A_4703-01 - Vertrauensraumstatus anzeigen

4938 Das Managementinterface des Konnektors MUSS einem authentisierten Administrator die
4939 Anzeige des Status des Vertrauensraums in Form folgender Daten anbieten:
4940 Sequenznummer der aktuellen TSL, StatusStartingTime (des TSPService (TSL-Signer-CA-
4941 Dienst) zum aktuell gültigen, aktiven TI-Vertrauensanker), NextUpdate, Gültigkeit der
4942 TSL, Typ der TSL (RSA oder ECC-RSA)) sowie optional für den Administrator einsehbar
4943 der Fingerprint des TSL-Signer-Zertifikats. **[<=]**

4944 Der Typ der TSL liefert dem Administrator die Information, ob es sich um eine TSL
4945 handelt, die den TI-Vertrauensraum ausschließlich für Zertifikate mit kryptographischen
4946 Verfahren nach RSA-2048 (TSL(RSA)) oder für Zertifikate mit kryptographischen
4947 Verfahren nach RSA-2048 und ECC-256 (TSL(ECC-RSA)) bereitstellt. Die Information
4948 kann aus der Signatur der TSL ermittelt werden.
4949

4950 TIP1-A_6733 - Aktive BNetzA-VL anzeigen

4951 Das Managementinterface des Konnektors MUSS einem authentisierten Administrator die
 4952 Anzeige des Status der BNetzA-VL in Form folgender Daten anbieten: Sequenznummer,
 4953 NextUpdate, Gültigkeitsstatus und Zeitpunkt der letzten Prüfung der Aktualität durch
 4954 TUC_KON_031.
 4955 [**<=**]

4956 TIP1-A_4704 - Zertifikatsablauf anzeigen
 4957 Der Administrator MUSS einen Prüflauf auf den innerhalb von
 4958 CERT_EXPIRATION_WARN_DAYS Tagen bevorstehenden Ablauf von Zertifikaten aller für
 4959 den Konnektor erreichbaren Karten (inkl. gSMC-K) an zentraler Stelle in der
 4960 Managementschnittstelle auslösen können und das Ergebnis angezeigt bekommen.
 4961 Der Konnektor MUSS die Gültigkeitsdauer der Zertifikate aller gesteckten Karten (inkl.
 4962 gSMC-K) prüfen mittels Aufruf von:
 4963 für gSMC-K
 4964 TUC_KON_033{checkSMCK; doInformClients=Nein; crypt = ECC}
 4965 TUC_KON_033{checkSMCK; doInformClients=Nein; crypt = RSA}
 4966 für jede gesteckte G2.0 Karte außer gSMC-K
 4967 TUC_KON_033{cardSession; doInformClients=Nein; crypt = RSA}
 4968 für jede gesteckte ab G2.1 Karte außer gSMC-K
 4969 TUC_KON_033{cardSession; doInformClients=Nein; crypt = ECC}
 4970 TUC_KON_033{cardSession; doInformClients=Nein; crypt = RSA}[**<=**]

4971 A_18931 - Anzeige Personalisierungs-Status gSMC-K-X.509-Zertifikate
 4972 Der Konnektor MUSS dem Administrator die X.509-Zertifikate der verbauten gSMC-
 4973 Ks gemäß TIP1-A_4506 anzeigen. Aus der Anzeige MUSS der Personalisierungs-Status
 4974 der X.509-Zertifikate ersichtlich sein (dual RSA- und ECC-personalisiert oder nur RSA-
 4975 personalisiert).
 4976 [**<=**]

4977 TIP1-A_4705 - TSL manuell importieren
 4978 Der Konnektor MUSS es dem Administrator ermöglichen, eine TSL manuell von lokaler
 4979 Datenquelle einzuspielen. Dabei MUSS der Konnektor TUC_KON_032{TSL-Datei} mit der
 4980 manuell importierten TSL aufrufen.
 4981 Der Konnektor MUSS den manuellen Import einer TSL auch ermöglichen, wenn er sich im
 4982 kritischen Betriebszustand EC_TSL_Out_Of_Date_Beyond_Grace_Period befindet.
 4983 Der Konnektor MUSS den manuellen Import einer zeitlich abgelaufenen TSL
 4984 zulassen. [**<=**]

4985

4986 TIP1-A_6728 - BNetzA-VL manuell importieren
 4987 Der Konnektor MUSS es dem Administrator ermöglichen, die BNetzA-VL manuell von
 4988 lokaler Datenquelle einzuspielen. Dabei MUSS der Konnektor TUC_KON_031{BNetzA-VL-
 4989 Datei} mit der manuell importierten BNetzA-VL-Datei aufrufen.
 4990 [**<=**]

4991 TIP1-A_4706 - CRL manuell importieren
 4992 Der Konnektor SOLL es dem Administrator ermöglichen, eine CRL manuell von einer
 4993 lokalen Datenquelle einzuspielen. In dem Fall MUSS der Konnektor TUC_KON_040{CRL-
 4994 Datei} mit der manuell importierten CRL aufrufen.[**<=**]

4995 Für die ECC-Migration ist es notwendig den ECC-RSA-Vertrauensraum zu etablieren. Dies
 4996 erfolgt durch das manuelle Einspielen eines TSL-Signer-CA Cross-Zertifikats und das
 4997 neue TSL-Signer-CA-Zertifikat, wodurch der ECC-Vertrauensanker im Konnektor im
 4998 sicheren Datenspeicher gespeichert wird. Die Prüfung des Cross-Zertifikats erfolgt durch
 4999 A_17821 - Wechsel des Vertrauensraumes mittels Cross-Zertifikaten (ECC-Migration).
 5000 Danach kann der Administrator die TSL(ECC-RSA) manuell importieren . Das Ergebnis ist

ein etablierter TI-Vertrauensraum für ECC und RSA.

A_17345 - TSL-Signer-CA Cross-Zertifikat manuell importieren (ECC-Migration)
Der Konnektor MUSS es dem Administrator ermöglichen, ein TSL-Signer-CA Cross-Zertifikat und das TSL-Signer-CA-Zertifikat für den neuen TI-Vertrauensanker manuell von lokaler Datenquelle einzuspielen. [\leq]

A_17837-01 - Nutzung von Cross-Zertifikaten für Vertrauensraum-Wechsel nach ECC-RSA (ECC-Migration)
Um auf Basis des bereits etablierten Vertrauensankers (RSA) in den Vertrauensraum (ECC-RSA) zu wechseln MUSS der Konnektor bei der Initialisierung des neuen Vertrauensankers (ECC-RSA) Cross-Zertifikate verwenden. Das Ergebnis ist ein neuer etablierter TI-Vertrauensanker (ECC-RSA). [\leq]

A_17548 - TSL-Signer-CA Cross-Zertifikat sicher speichern (ECC-Migration)
Der Konnektor MUSS den neuen TI-Vertrauensanker im sicheren Datenspeicher speichern. [\leq]

A_17549 - TSL-Signer-CA Cross-Zertifikat im kritischen Betriebszustand (ECC-Migration)
Der Konnektor MUSS den manuellen Import des TSL-Signer-CA Cross-Zertifikats auch ermöglichen, wenn er sich im kritischen Betriebszustand EC_TSL_Out_Of_Date_Beyond_Grace_Period befindet. [\leq]

A_17550 - TSL-Signer-CA Cross-Zertifikat importieren - Fehler (ECC-Migration)
Falls der manuelle Import des TSL-Signer-CA Cross-Zertifikats nicht erfolgreich durchgeführt werden konnte, MUSS der Konnektor den Vorgang abbrechen und einen Fehler gemäß TAB_KON_857 dem Administrator zur Anzeige bringen und protokollieren.

Tabelle 285: TAB_KON_857 - Fehlercodes beim Import des Cross-Zertifikats für TI-Vertrauensanker ECC

Fehlercode	ErrorType	Severity	Fehlertext
4255	Security	Error	Fehler beim Import des TSL-Signer-CA Cross-Zertifikats

[\leq]

TIP1-A_5700 - Ereignisbasiert http-Forwarder Adressen ermitteln
Beim Auftreten des Events NETWORK/VPN_TI/UP MUSS der Konnektor über DNS die Adressen des http-Forwarders des VPN-Zugangsdienststandortes ermitteln (SRV-RR mit Bezeichner "_ocsp._tcp.<DOMAIN_SRVZONE_TI>").

[\leq]

4.1.10 Protokollierungsdienst

Der Protokollierungsdienst protokolliert system- und sicherheitsrelevante Ereignisse, sowie Ereignisse im Kontext der Performancemessung (siehe [gemSpec_Perf#4.1.2]), innerhalb des Konnektors. Auch Ereignisse von Fachmodulen können protokolliert werden. Im Sicherheitsprotokoll werden alle Ereignisse eingetragen, die Auswirkungen auf Sicherheitsmerkmale des Konnektors haben können (Änderungen an der Firewall-Konfiguration, Authentisierungsfehler etc.). Ereignisse im Kontext der

5041 Performancemessung innerhalb des Konnektors werden in das Konnektor-
 5042 Performanceprotokoll geschrieben. Ereignisse im Kontext der Performancemessung von
 5043 Fachmodulen werden in das Fachmodul-Performanceprotokoll geschrieben. Alle anderen
 5044 Ereignisse werden in das Systemprotokoll oder die Fachmodulprotokolle geschrieben
 5045 (grundsätzlich trifft die Entscheidung über den zu verwendenden Protokollspeicher der
 5046 Aufrufer des Protokolldienstes).

5047 Die Protokolle werden persistiert.

5048 Hinweis:

5049 Ereignisse im Protokollierungsdienst adressieren nicht nur zu protokollierende Events im
 5050 Sinne des Systeminformationsdienstes sondern alles, was zu einem Protokolleintrag
 5051 führen soll (z.B. Fehler, Informationen zu Ablauf, Debug, Performance).

5052 Innerhalb des Protokollierungsdienstes werden folgende Präfixe für Bezeichner
 5053 verwendet:

- 5054 • Events (Topic Ebene 1): „LOG“
- 5055 • Konfigurationsparameter: „LOG_“

5056 **4.1.10.1 Funktionsmerkmalweite Aspekte**

5057 TIP1-A_4708 - Protokollierungsfunktion

5058 Der Konnektor MUSS einen Protokollierungsdienst anbieten. Dabei MUSS der Konnektor
 5059 zwischen System- und Sicherheitsprotokoll, sowie Fachmodulprotokollen unterscheiden.
 5060 Je Fachmodul MUSS ein getrenntes Protokoll vorhanden sein.

5061 Die Protokolleinträge MÜSSEN durch den Konnektor lokal persistiert werden.

5062 [**<=**]

5063 TIP1-A_5654 - Sicherheits-Protokollierung

5064 Der Konnektor MUSS herstellerspezifische Fehler, die Auswirkungen auf
 5065 Sicherheitsmerkmale des Konnektors haben, in das Sicherheitsprotokoll schreiben.

5066 [**<=**]

5067 TIP1-A_4709 - Integrität des Sicherheitsprotokolls

5068 Der Konnektor MUSS sicherstellen, dass Einträge in das Sicherheitsprotokoll nicht von
 5069 außen und nicht durch den Administrator verändert und gelöscht werden können.

5070 [**<=**]

5071 TIP1-A_4710 - Protokollierung personenbezogener und medizinischer Daten

5072 Der Konnektor DARF medizinische Daten NICHT in die Protokolldateien schreiben.

5073 Personenbezogene Daten DÜRFEN NICHT in Protokolleinträgen gespeichert werden.

5074 KVNR, ICCSN und CardHolderName MÜSSEN als personenbezogene Daten behandelt
 5075 werden.

5076 Die ICCSN DARF Im Fehlerfall durch Fachmodule in Protokolleinträgen gespeichert
 5077 werden. Die ICCSN DARF NICHT im Sicherheitsprotokoll gespeichert werden.

5078 [**<=**]

5079 TIP1-A_6479 - Keine Protokollierung vertraulicher Daten

5080 Der Konnektor DARF vertrauliche Daten NICHT in die Protokolldateien schreiben.

5081 [**<=**]

5082 TIP1-A_4711 - Kapazität der Protokolldateien

5083 Der Konnektor MUSS über eine Speichergröße für Protokolldateien verfügen, so dass
 5084 Einträge (protokollierte Ereignisse ab der Schwere „Warning“) über einen Zeitraum von
 5085 bis zu einem Jahr darin vorgehalten werden können.

5086 [**<=**]

5087 Da sich die Menge an Einträgen nach der Größe der Einsatzumgebung richtet, ist die
5088 Speichergröße nach den in [gemSpec_Perf#3.1.1] beschriebenen Einsatzumgebungen
5089 (LE-Ux, x=1,2,3,4) ausreichend zu wählen.

5090 TIP1-A_4712 - Protokollierung erfolgreicher Kryptooperationen

5091 Wenn LOG_SUCCESSFUL_CRYPTO_OPS = Enabled MUSS der Konnektor die folgenden
5092 erfolgreich durchlaufenen Außenoperationen protokollieren:

- 5093 - SignDocument,
- 5094 - VerifyDocument,
- 5095 - ExternalAuthenticate,
- 5096 - EncryptDocument,
- 5097 - DecryptDocument.

5098 Dazu MUSS er

5099

```
5100 TUC_KON_256 {
5101     topic = „LOG/CRYPTO_OP“;
5102     eventType = Sec;
5103     severity = Info;
5104     parameters = („Operation=$Operationsname,
5105                   <für alle betroffenen Schlüssel:>
5106                   Karte=$ICCSN,
5107                   Keyref=<Referenz auf den Schlüssel>,
5108                   CARD_HANDLE=$CardHandle,
5109                   CardHolderName=$CardHolderName“);
5110     doDisp = false}
5111
```

5112 aufrufen.

5113

5114 [**<=**]

5115 TIP1-A_4713 - Herstellerspezifische Systemprotokollierung

5116 Wenn LOG_LEVEL_SYSLOG = Info MUSS der Konnektor herstellerspezifische Informationen
5117 über den laufenden Betrieb in das Systemprotokoll eintragen, um im Bedarfsfall das
5118 Verhalten des Konnektors analysieren zu können (Unterstützung der Fehlersuche etc.).
5119 Die Häufigkeit und der Inhalt der protokollierten Informationen sind herstellerspezifisch.

5120 [**<=**]

5121 TIP1-A_4714 - Art der Protokollierung

5122 Der Konnektor MUSS Protokolleinträge so anlegen, dass eine Analyse der Einträge
5123 unterstützt wird:

- 5124 • Die Protokolleinträge MÜSSEN eine patternbasierte Filterung unterstützen.
5125 Protokollwert/-texte sowie Attribute MÜSSEN in ihren Namensstrukturen hierauf
5126 abgestimmt sein.
- 5127 • „;“ MUSS als Trennzeichen zwischen Key/Value-Paaren verwendet werden.
- 5128 • „=“ MUSS als Trennzeichen zwischen Key und Value in einem Key/Value-Paar
5129 verwendet werden.
- 5130 • Es MUSS durchgängig dasselbe Zeitstempelformat verwendet werden, entweder
5131 „timestamp=%d{dd.MM.yyyy HH:mm:ss.SSS}“ (Beispiel „30.08.2017
5132 13:44:12.436“) und als Wert die gesetzliche Zeit (§4 EinhZeitG)
5133 oder
5134 „timestamp=%d{dd.MM.yyyy HH:mm:ss.SSSZ}“, wobei „Z“ die Zeitzoneangabe
5135 nach RFC 822 mit („+“ / „-“) 4DIGIT bezeichnet (Beispiel „30.08.2017
5136 13:44:12.436+0200“).

5137 [\leq]

5138 **4.1.10.2 Durch Ereignisse ausgelöste Reaktionen**

5139 Keine.

5140 **4.1.10.3 Interne TUCs, nicht durch Fachmodule nutzbar**

5141 Keine.

5142 **4.1.10.4 Interne TUCs, auch durch Fachmodule nutzbar**

5143 *4.1.10.4.1 TUC_KON_271 „Schreibe Protokolleintrag“*

5144 TIP1-A_4715 - TUC_KON_271 „Schreibe Protokolleintrag“

5145 Der Konnektor MUSS den technischen Use Case TUC_KON_271 „Schreibe
5146 Protokolleintrag“ umsetzen.

5147

5148 **Tabelle 286: TAB_KON_607 – TUC_KON_271 „Schreibe Protokolleintrag“**

Element	Beschreibung
Name	TUC_KON_271 „Schreibe Protokolleintrag“
Beschreibung	Dieser TUC schreibt einen Eintrag in ein Protokoll.
Auslöser	Aufruf durch Basisdienst, Fachmodul oder TUC_KON_256 „Systemereignis absetzen“
Vorbedingungen	<p>Im Fall eines zu protokollierenden Ereignisses des Systeminformationsdienstes wird</p> <ul style="list-style-type: none"> • eventType = "Op" gesetzt, wenn Event.Type gleich "Operation", "Infrastructure", "Business" oder "Other" bzw. • eventType = "Sec", wenn Event.Type gleich "Security". Die Schwere entspricht der Event.Severity gemäß Schema EventService.xsd. Im Fall eines zu protokollierenden Fehlers wird • eventType = "Op" gesetzt, wenn ErrorType gleich "Technical", "Business", "Infrastructure" oder "Other" bzw. eventType = "Sec", wenn ErrorType gleich "Security". Die Schwere entspricht der Severity des Fehlers.
Eingangs anforderung	Keine
Eingangsdaten	<ul style="list-style-type: none"> • Zu protokollierendes Ereignis

	<ul style="list-style-type: none"> • <i>fmName</i> – <i>optional/verpflichtend für Aufruf durch Fachmodule</i>; <i>default = ""</i> (Name des aufrufenden Fachmoduls; das Ereignis wird in das entsprechende Konnektor-Protokoll geschrieben) • <i>eventType</i> [<i>EventType</i>] definiert den Protokolltyp, in welchen das Ereignis geschrieben wird; Sec = Security: Ereignis wird in das Securityprotokoll geschrieben Op = Operation: Wenn <i>fmName</i> = "", wird das Ereignis in das Systemprotokoll geschrieben. Wenn <i>fmName</i> gesetzt ist, wird das Ereignis in das durch <i>fmName</i> definierte Fachmodul-Protokoll geschrieben. Perf = Performance: Wenn <i>fmName</i> = "", wird das Ereignis in das Konnektor-Performanceprotokoll geschrieben. Wenn <i>fmName</i> gesetzt ist, wird das Ereignis in das durch <i>fmName</i> definierte Fachmodul-Performanceprotokoll geschrieben. • <i>severity</i> { [<i>EventSeverity</i>] , Debug} (Schwere mit: Debug = Debug Information, Info = Information, Warn = Warning, Err = Error, Fatal) • <i>parameters</i> beinhaltet die Daten des Ereignisses, die im Protokolleintrag geschrieben werden
Komponenten	Konnektor
Ausgangsdaten	Keine
Nachbedingungen	
Standardablauf	<ol style="list-style-type: none"> 1. Wenn <i>eventType</i> = Sec, so wird das Ereignis in das Sicherheitsprotokoll geschrieben. Falls <i>fmName</i> angegeben ist, wird er dem Eintrag hinzugefügt. 2. <i>fmName</i> ist angegeben (durch ein Fachmodul aufgerufen) und <i>eventType</i> = „Op“, so wird das Ereignis in das zugehörige Fachmodulprotokoll geschrieben. <ol style="list-style-type: none"> a. Gemäß den Festlegungen in den jeweiligen Fachmodulspezifikationen (FM_<<i>fmName</i>>_LOG_LEVEL), werden nur Ereignisse in das Fachmodulprotokoll geschrieben, deren <i>severity</i> mindestens dem jeweils dort festgelegten Wert entsprechen. 3. <i>fmName</i> ist nicht angegeben (Aufruf durch ein Fachmodul) und <i>eventType</i> = „Op“, dann wird das Ereignis in das Systemprotokoll geschrieben. <ol style="list-style-type: none"> a. Gemäß den Festlegungen in LOG_LEVEL_SYSLOG werden nur Ereignisse in das Systemprotokoll geschrieben, deren Schwere mindestens dem Wert von LOG_LEVEL_SYSLOG

	<p>entsprechen.</p> <p>4. Wurde der TUC durch ein Fachmodul aufgerufen (fmName ist angegeben) und ist eventType = Perf, so wird das Ereignis in das zugehörige Fachmodul-Performanceprotokoll geschrieben.</p> <p>5. Wurde der TUC nicht durch ein Fachmodul aufgerufen (fmName ist nicht angegeben) und ist eventType = Perf, so wird das Ereignis in das Konnektor-Performanceprotokoll geschrieben. Die geschriebenen Protokolleinträge MÜSSEN mindestens folgende Attribute beinhalten:</p> <ul style="list-style-type: none"> • Datum und Uhrzeit • Übergebenes Ereignis <p>Die Speicherung erfolgt rollierend. Übersteigt die Anzahl der Einträge im Sicherheitsprotokoll SECURITY_LOG_SIZE, so werden ältere Einträge überschrieben. Für die anderen Protokolle beginnt das Überschreiben, wenn der jeweilige Speicherplatz für das Protokoll erschöpft ist. Dabei werden die nach der Reihenfolge der Erstellung ältesten Einträge überschrieben, unabhängig vom Zeitstempel des Logeintrags. Ist der Zeitstempel eines überschriebenen Logeintrags jünger als LOG_DAYS bzw. FM_<fmName>_LOG_DAYS bzw. SECURITY_LOG_DAYS, so wird der Fehlerzustand EC_LOG_OVERFLOW ausgelöst.</p>
Fehlerfälle	<p>Fehler in den folgenden Schritten des Standardablaufs führen zu:</p> <p>a) Aufruf von TUC_KON_256 { topic = „LOG/ERROR“; eventType = \$ErrorType; severity = \$Severity; parameters = („Error=\$Fehlercode, Bedeutung=\$Fehlertext“); doLog = false }</p> <p>b) Abbruch der Verarbeitung mit den ausgewiesenen Fehlercodes</p> <p>(→1) In das Sicherheitsprotokoll kann nicht geschrieben werden: Fehlercode: 4152</p> <p>(→2) In das Fachmodulprotokoll kann nicht geschrieben werden: Fehlercode: 4151</p> <p>(→3) In das Systemprotokoll kann nicht geschrieben werden: Fehlercode: 4150</p> <p>(→4) In das Fachmodul-Performanceprotokoll kann nicht geschrieben werden: Fehlercode: 4217</p> <p>(→5) In das Konnektor-Performanceprotokoll kann nicht geschrieben werden: Fehlercode: 4216</p>
Nichtfunktionale Anforderungen	Keine

Zugehörige Diagramme	Keine
----------------------	-------

5149 **Tabelle 287: TAB_KON_608 Fehlercodes TUC_KON_271 „Schreibe Protokolleintrag“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4150	Technical	Fatal	Fehler beim Schreiben des Systemprotokolls
4151	Technical	Fatal	Fehler beim Schreiben eines Fachmodulprotokolls
4152	Security	Error	Fehler beim Schreiben des Sicherheitsprotokolls
4216	Technical	Fatal	Fehler beim Schreiben des Konnektor-Performanceprotokolls
4217	Technical	Fatal	Fehler beim Schreiben eines Fachmodul-Performanceprotokolls

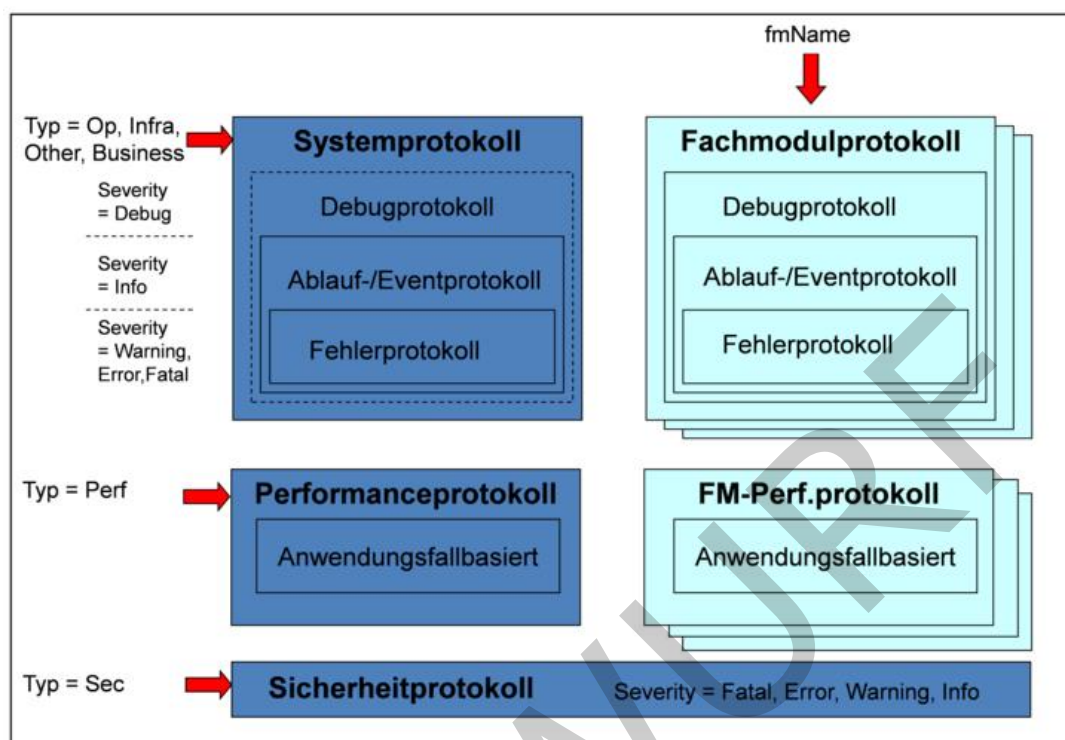
5150

5151 [**<=**]

5152 Die Darstellung PIC_KON_118 veranschaulicht den Aufbau der Protokolle für Plattform
5153 und Fachmodule und die Steuerung der Protokolleinträge in TUC_KON_271 „Schreibe

5154

Protokolleintrag".



5155

5156 **Abbildung 20: PIC_KON_118 Aufbau und Struktur der Protokolldateien für Plattform und**
 5157 **Fachmodule**

5158 4.1.10.5 Operationen an der Außenschnittstelle

5159 Keine

5160 4.1.10.6 Betriebsaspekte

5161 TIP1-A_4716 - Einsichtnahme und Veränderung der Protokolle

5162 Der Administrator MUSS die durch den Protokollierungsdienst geschriebenen Protokolle
 5163 über die Managementschnittstelle einsehen können.

5164 Eine Veränderung des Sicherheitsprotokolls DARF für den Administrator NICHT möglich
 5165 sein.

5166 Das Löschen folgender Protokolle MUSS für den Administrator möglich sein:

- 5167 • Systemprotokoll
- 5168 • das jeweils durch <fmName> spezifizierte Fachmodulprotokoll
- 5169 • Konnektor-Performanceprotokoll
- 5170 • das jeweils durch <fmName> spezifizierte Fachmodul-Performanceprotokoll

5171 Der Konnektor MUSS den Export von Protokolleinträgen oder ganzen Protokolldateien
 5172 unterstützen.

5173 Der Konnektor SOLL das Sortieren und Filtern der Protokolleinträge sowie das Suchen in
 5174 den Protokolleinträgen unterstützen.

5175 [**<=**]

5176 TIP1-A_4996 - Hinweis auf neue Sicherheitsprotokolleinträge
 5177 Nachdem sich der Administrator an der Managementschnittstelle angemeldet hat, MUSS
 5178 der Konnektor ihn automatisch auf Sicherheitsprotokolleinträge hinweisen, die seit dem
 5179 Ausloggen dieses Administrator aufgelaufen sind.

5180 [\leq]

5181 TIP1-A_4717 - Konfigurationswerte des Protokollierungsdienstes
 5182 Die Managementschnittstelle MUSS es einem Administrator ermöglichen
 5183 Konfigurationsänderungen gemäß Tabelle TAB_KON_609 vorzunehmen:
 5184

5185 **Tabelle 288: TAB_KON_609 Konfigurationswerte des Protokollierungsdienstes**
 5186 **(Administrator)**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
LOG_LEVEL_ SYSLOG	Info, Warning, Error, Fatal	Der Administrator MUSS den Detaillierungsgrad des Systemprotokolls durch Festlegung der Mindest-Schwere zu protokollierender Einträge festlegen können. Default-Wert: Warning
FM_<fmName>_ LOG_LEVEL	Debug, Info, Warning, Error, Fatal	Der Administrator MUSS den Detaillierungsgrad des Fachmodulprotokolls durch Festlegung der Mindest-Schwere zu protokollierender Einträge festlegen können. Default-Wert: Warning
SECURITY_LOG_SIZE	X Einträge	Der Administrator MUSS die Größe des Sicherheitsprotokolls angeben können (Anzahl der Einträge im Ringbuffer). Mindestgröße: ≥ 10.000 Maximalgröße: herstellerspezifisch Default-Wert: ≥ 50.000
SECURITY_LOG_DAYS	X Tage	Der Administrator MUSS die erwartete Anzahl der im Sicherheitsprotokoll gespeicherten Tage im Bereich 10 bis 365 konfigurieren können. Default-Wert: 180
LOG_DAYS	X Tage	Der Administrator MUSS die Anzahl der gespeicherten Tage für das Systemprotokoll und das Performanceprotokoll festlegen können. Der Konnektor kann Protokolleinträge, die älter als LOG_DAYS sind, zyklisch löschen. Dabei DARF der eingestellte Wert NICHT unter der Mindestgröße von 10 Tagen oder über der Maximalgröße von einem Jahr (365 Tage) liegen. Default-Wert: 180

FM_<fmName>_ LOG_DAYS	X Tage	Der Administrator MUSS die Anzahl der gespeicherten Tage für die fachmodulspezifischen Protokolle festlegen können. Es kann je Fachmodul einen Konfigurationsparameter für LOG_DAYS geben, der gemeinsam für das Fachmodulprotokoll und das Fachmodul-Performanceprotokoll gilt. Der Konnektor kann Protokolleinträge, die älter als FM_<fmName>LOG_DAYS sind, zyklisch löschen. Dabei DARF der eingestellte Wert NICHT unter der Mindestgröße von 10 Tagen oder über der Maximalgröße von einem Jahr (365 Tage) liegen. Default-Wert: 180 Die Definition des fachmodulspezifischen Konfigurationswertes ist Bestandteil der entsprechenden Fachmodulspezifikation. Ist kein fachmodulspezifischer Konfigurationsparameter spezifiziert, dann gilt LOG_DAYS.
LOG_SUCCESSFUL_ CRYPTO_OPS	Enabled/Disabled	Der Administrator MUSS festlegen können, ob auch erfolgreich ausgeführte Kryptooperationen im Sicherheitslog protokolliert werden sollen. Default-Wert: Disabled

5187

5188 [\leq]

5189 4.1.10.6.1 TUC_KON_272 „Initialisierung Protokollierungsdienst“

5190 TIP1-A_4718 - TUC_KON_272 „Initialisierung Protokollierungsdienst“

5191 Der Konnektor MUSS den technischen Use Case TUC_KON_272 „Initialisierung
5192 Protokollierungsdienst“ umsetzen.

5193

5194 **Tabelle 289: TAB_KON_610 – TUC_KON_272 „Initialisierung Protokollierungsdienst“**

Element	Beschreibung
Name	TUC_KON_272 „Initialisierung Protokollierungsdienst“
Beschreibung	Der Konnektor muss zum Bootup den Protokollierungsdienst starten und die Existenz und Schreibbarkeit der Protokolle sicherstellen.
Eingangs anforderung	Keine
Auslöser und Vorbedingungen	Bootup
Eingangsdaten	Keine
Komponenten	Konnektor

Ausgangsdaten	Keine
Standardablauf	<ol style="list-style-type: none"> 1. Prüfen, ob Schreib-/Lesezugriff auf Sicherheitsprotokoll möglich ist 2. Prüfen, ob Schreib-/Lesezugriff auf Systemprotokoll möglich ist 3. Prüfen, ob Schreib-/Lesezugriff auf Fachmodulprotokolle möglich ist 4. Prüfen, ob Schreib-/Lesezugriff auf Konnektor-Performanceprotokoll möglich ist 5. Prüfen, ob Schreib-/Lesezugriff auf Fachmodul-Performanceprotokolle möglich ist
Varianten/ Alternativen	Keine
Fehlerfälle	<p>Fehler in den folgenden Schritten des Standardablaufs führen zu:</p> <p>a) Aufruf von TUC_KON_256 mit folgenden Parametern { topic = „LOG/ERROR“; eventType = \$ErrorType; severity = \$Severity; parameters = („Error=\$Fehlercode, Bedeutung=\$Fehlertext“); doLog = false }</p> <p>b) Abbruch der Verarbeitung mit den ausgewiesenen Fehlercodes</p> <p>(→1) Zugriff nicht möglich: Fehlercode: 4153 (→2) Zugriff nicht möglich: Fehlercode: 4154 (→3) Zugriff nicht möglich: Fehlercode: 4155 (→4) Zugriff nicht möglich: Fehlercode: 4218 (→5) Zugriff nicht möglich: Fehlercode: 4219</p>
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 290: TAB_KON_611 Fehlercodes TUC_KON_272 „Initialisiere Protokollierungsdienst“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4153	Technical	Fatal	Zugriff auf Sicherheitsprotokoll nicht möglich
4154	Technical	Fatal	Zugriff auf Systemprotokoll nicht möglich
4155	Technical	Fatal	Zugriff auf Fachmodulprotokolle nicht möglich
4218	Technical	Fatal	Zugriff auf Konnektor-Performanceprotokoll nicht möglich
4219	Technical	Fatal	Zugriff auf Fachmodul-Performanceprotokoll nicht möglich

[<=]

5199 4.1.11 TLS-Dienst

5200 Fachmodule müssen gesicherte Verbindungen zu Fachdiensten in der TI aufbauen
 5201 können. Dabei sollen sie sich mit einer Organisationsidentität (einer SM-B) authentisieren
 5202 können. Der TLS-Dienst stellt hierfür TUCs für einen TLS-Verbindungsaufbau und -
 5203 Verbindungsabbau zur Verfügung. Die gesicherte Kommunikation selbst erfolgt dann
 5204 durch das Fachmodul unter Nutzung der etablierten Verbindung.

5205 Die Funktionalität steht nur zur Verfügung, wenn MGM_LU_ONLINE aktiv ist (siehe
 5206 Kapitel 4.3.6)

5207 4.1.11.1 Funktionsmerkmalweite Aspekte

5208 4.1.11.2 Durch Ereignisse ausgelöste Reaktionen

5209 TIP1-A_4719 - TLS-Dienst reagiert auf Veränderung LU_ONLINE
 5210 Tritt das Ereignis „MGM/LU_CHANGED/LU_ONLINE“ ein, so MUSS

- 5211 • wenn „Active=Enabled“ der Dienst bereitgestellt werden
- 5212 • wenn „Active=Disabled“ der Dienst gestoppt werden.
- 5213 Sind TLS-Verbindungen aktiv, so MUSS für jede TUC_KON_111 "Kartenbasierte
- 5214 TLS-Verbindung abbauen" gerufen werden.

5215 [\leq]

5216 4.1.11.3 Interne TUCs, nicht durch Fachmodule nutzbar

5217 Keine.

5218 4.1.11.4 Interne TUCs, auch durch Fachmodule nutzbar

5219 4.1.11.4.1 TUC_KON_110 „Kartenbasierte TLS-Verbindung aufbauen“

5220 TIP1-A_4720 - TUC_KON_110 „Kartenbasierte TLS-Verbindung aufbauen“
 5221 Der Konnektor MUSS den technischen Use Case "Kartenbasierte TLS-Verbindung
 5222 aufbauen" gemäß TUC_KON_110 umsetzen.
 5223

5224 **Tabelle 291: TAB_KON_773 – TUC_KON_110 „Kartenbasierte TLS-Verbindung aufbauen“**

Element	Beschreibung
Name	TUC_KON_110 „Kartenbasierte TLS-Verbindung aufbauen“
Beschreibung	Der TUC_KON_110 „Kartenbasierte TLS-Verbindung aufbauen“ baut eine TLS-Verbindung zur angegebenen Zieladresse auf. Dabei kann für eine gegenseitige Authentisierung eine SM-B verwendet werden.
Auslöser	Aufruf durch ein Fachmodul
Vorbedingungen	Die für die Authentisierung adressierte Karte muss freigeschaltet sein
Eingangsdaten	<ul style="list-style-type: none"> • roleToMatch – <i>optional/verpflichtend, wenn Rollenprüfung durchgeführt werden soll</i>

	<ul style="list-style-type: none"> cardSession – <i>optional/verpflichtend, wenn Clientauthentisierung durchgeführt werden soll</i> (CardSession einer SM-B) targetUri (URI des Verbindungsziels)
Komponenten	Konnektor, eHealth-Kartenterminal, Karte, Server des Fachdienstes
Ausgangsdaten	<ul style="list-style-type: none"> tlsConnectionId (ConnectionIdentifier der TLS-Verbindung)
Standardablauf	<p>Der Konnektor MUSS folgende Schritte durchlaufen:</p> <ol style="list-style-type: none"> Auflösen des FQDN im targetUri per 'TUC_KON_361 „DNS Namen auflösen“ TLS-Verbindung mit ermittelter Adresse aufbauen: <ol style="list-style-type: none"> Prüfe Server-Zertifikat mittels TUC_KON_037 „Zertifikat prüfen“ { <pre>certificate = C.FD.TLS-S; qualifiedCheck = not_required; offlineAllowNoCheck = true; policyList = oid_fd_tls_s; intendedKeyUsage= intendedKeyUsage(C.FD.TLS-S); intendedExtendedKeyUsage = id-kp-serverAuth; validationMode = OCSP}</pre> Das Server-Zertifikat MUSS C.FD.TLS-S sein Prüfe in a) zurückgegebene Rolle („ermittelte Rolle“) == roleToMatch Wenn cardSession übergeben: Clientauthentisierung mittels ID.HCI.AUT tlsConnectionId der erzeugten Verbindung zurückgeben
Varianten/ Alternativen	<ul style="list-style-type: none"> Keine
Fehlerfälle	<p>Fehler in den folgenden Schritten des Ablaufs führen zu einem Abbruch der Verarbeitung mit den ausgewiesenen Fehlercodes</p> <p>(→1) Der Name der Gegenstelle kann nicht aufgelöst werden</p> <p>(→2b) Rollenprüfung fehlgeschlagen: Fehlercode 4220</p> <p>(→2) Server konnte nicht authentisiert werden: Fehlercode 4156</p> <p>(→2) Clientauthentisierung fehlgeschlagen: Fehlercode 4157</p>
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

5225
5226**Tabelle 292: TAB_KON_612 Fehlercodes TUC_KON_110 „Kartenbasierte TLS-Verbindung aufbauen“**

Fehlercode	ErrorType	Severity	Fehlertext
------------	-----------	----------	------------

Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4156	Security	Error	Server konnte bei TLS-Verbindungsaufbau nicht authentisiert werden
4157	Security	Error	Clientauthentisierung bei TLS-Verbindungsaufbau fehlgeschlagen
4220	Security	Error	Rollenprüfung bei TLS-Verbindungsaufbau fehlgeschlagen

5227

5228 [\leq]

5229 4.1.11.4.2 TUC_KON_111 „Kartenbasierte TLS-Verbindung abbauen“

5230 TIP1-A_4721 - TUC_KON_111 „Kartenbasierte TLS-Verbindung abbauen“

5231 Der Konnektor MUSS den technischen Use Case "Kartenbasierte TLS-Verbindung abbauen" gemäß TUC_KON_111 umsetzen.

5232

5233

5234 **Tabelle 293: TAB_KON_774 - TUC_KON_111 „Kartenbasierte TLS-Verbindung abbauen“**

Element	Beschreibung
Name	TUC_KON_111 „Kartenbasierte TLS-Verbindung abbauen“
Beschreibung	Der TUC_KON_111 „Kartenbasierte TLS-Verbindung abbauen“ dient der geregelten Beendigung einer TLS-Verbindung, die zuvor über TUC_KON_110 aufgebaut wurde.
Auslöser	Aufruf durch ein Fachmodul
Vorbedingungen	Mittels TUC_KON_110 wurde eine TLS-Verbindung aufgebaut
Eingangsdaten	<ul style="list-style-type: none"> tlsConnectionId (ConnectionIdentifier der TLS-Verbindung)
Komponenten	Konnektor, Server des Fachdienstes
Ausgangsdaten	Keine
Standardablauf	Der Konnektor MUSS folgende Schritte durchlaufen: <ol style="list-style-type: none"> 1. Trennen der über tlsConnectionId adressierten TLS-Verbindung
Varianten/Alternativen	keine
Fehlerfälle	Fehler in den folgenden Schritten des Ablaufs führen zu einem Abbruch der Verarbeitung mit den ausgewiesenen Fehlercodes: (→1) Keine Verbindung mit angegebenem TLSConnectionIdentifier vorhanden: Fehlercode 4158
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

5235

5236 **Tabelle 294: TAB_KON_613 Fehlercodes TUC_KON_111 „Kartenbasierte TLS-Verbindung**
 5237 **abbauen“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4158	Technical	Error	Adressierte TLS-Verbindung nicht vorhanden

5238

5239 [\leq]

5240 **4.1.11.5 Operationen an der Außenschnittstelle**

5241 Keine.

5242 **4.1.11.6 Betriebsaspekte**

5243 TIP1-A_4722 - TLS-Dienst initialisieren

5244 Wenn MGM_LU_ONLINE = „Enabled“, MUSS der Basisdienst TLS-Dienst nach dem Bootup zur Nutzung zur Verfügung stehen.

5246 Wenn MGM_LU_ONLINE = „Disabled“, DARF der Basisdienst TLS-Dienst nach dem Bootup NICHT zur Nutzung zur Verfügung stehen.

5248 [\leq]

5249 **4.1.12 LDAP-Proxy**

5250 Der Konnektor ermöglicht es Clientsystemen und Fachmodulen durch Nutzung des LDAP-
 5251 Proxies Daten aus dem Verzeichnisdienst der TI-Plattform (VZD) abzufragen. Die
 5252 Kommunikation erfolgt über das LDAPv3 Protokoll.

5253 Die Funktionalität steht nur zur Verfügung, wenn MGM_LU_ONLINE=Enabled ist (siehe
 5254 Kapitel 4.3.6)

5255 **4.1.12.1 Funktionsmerkmalweite Aspekte**

5256 Keine.

5257 **4.1.12.2 Durch Ereignisse ausgelöste Reaktionen**

5258 TIP1-A_5516 - LDAP-Proxy reagiert auf Veränderung LU_ONLINE

5259 Tritt das Ereignis „MGM/LU_CHANGED/LU_ONLINE“ ein, so MUSS

5260 • wenn „Active=Enabled“ der Dienst bereitgestellt werden

5261 • wenn „Active=Disabled“ der Dienst gestoppt werden.

5262 Ist eine Verbindung zum VZD aktiv, so MUSS diese abgebaut werden.

5263 [\leq]

5264 **4.1.12.3 Interne TUCs, nicht durch Fachmodule nutzbar**

5265 Keine.

5266 4.1.12.4 Interne TUCs, auch durch Fachmodule nutzbar

5267 4.1.12.4.1 TUC_KON_290 „LDAP-Verbindung aufbauen“

5268 TIP1-A_5517-02 - Konnektor, TUC_KON_290 „LDAP-Verbindung aufbauen“
 5269 Der Konnektor MUSS den technischen Use Case TUC_KON_290 „LDAP-Verbindung
 5270 aufbauen“ gemäß TAB_KON_805 umsetzen.

5271

5272 **Tabelle 295: TAB_KON_805 - TUC_KON_290 „LDAP-Verbindung aufbauen“**

Element	Beschreibung
Name	TUC_KON_290 „LDAP-Verbindung aufbauen“
Beschreibung	Initiiert durch einen Verbindungsaufbau des LDAP-Clients zum Konnektor baut der Konnektor eine TLS-gesicherte Verbindung zum VZD auf.
Auslöser	LDAP (oder LDAPS wenn ANCL_TLS_MANDATORY=Enabled) Verbindungsaufbau von einem Fachmodul oder einem Clientsystem ist abgeschlossen. Bei Verwendung von LDAPS authentisiert sich der Konnektor beim LDAP-Client mit der Identität ID.AK.AUT.
Vorbedingungen	<ul style="list-style-type: none"> MGM_LU_ONLINE=Enabled
Eingangsdaten	keine
Komponenten	Konnektor, VZD
Ausgangsdaten	keine
Standardablauf	<ol style="list-style-type: none"> Der Konnektor ermittelt den FQDN und Port des VZD durch eine DNS-SD Namensauflösung gemäß [RFC6763] mit dem Bezeichner "_ldap._tcp.vzd.<DNS_TOP_LEVEL_DOMAIN_TI>." Der Konnektor baut eine LDAPS-Verbindung zum VZD auf. Dabei wird das Serverzertifikat des Verzeichnisdienst C.ZD.TLS-S nach TUC_PKI_018 geprüft (PolicyList: oid_zd_tls_s (gemäß gemSpec_OID), intendedKeyUsage: intendedKeyUsage(C.ZD.TLS-S), ExtendedKeyUsages: serverAuth (1.3.6.1.5.5.7.3.1), Offlinemodus: nein, TOLERATE_OCSP_FAILURE: false , Prüfmodus: OCSP)
Varianten/Alternativen	keine
Fehlerfälle	
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

5273

5274 [**<=**]

5275

5276 4.1.12.4.2 TUC_KON_291 „Verzeichnis abfragen“

5277 TIP1-A_5518 - Konnektor, TUC_KON_291 „Verzeichnis abfragen“

5278 Der Konnektor MUSS den technischen Use Case TUC_KON_291 „Verzeichnis abfragen“
5279 gemäß TAB_KON_815 umsetzen.

5280

5281 **Tabelle 296: TAB_KON_815 – TUC_KON_291 „Verzeichnis abfragen“**

Element	Beschreibung
Name	TUC_KON_291 „Verzeichnis abfragen“
Beschreibung	Der Konnektor leitet als LDAP-Proxy einen Search Request des LDAP-Clients an den VZD weiter. Vom VZD empfängt der Konnektor eine Search Response und leitet diese an den LDAP-Client weiter.
Auslöser	Aufruf durch einen LDAPv3 Search Request von einem Fachmodul-TUC oder einem Clientsystem
Vorbedingungen	<ul style="list-style-type: none"> MGM_LU_ONLINE=Enabled Eine LDAPv3-Verbindung LDAP-Client sowie eine LDAPv3 Verbindung vom Konnektor zum VZD wurden aufgebaut (TUC_KON_290 „LDAP-Verbindung aufbauen“)
Eingangsdaten	<ul style="list-style-type: none"> LDAPv3 Search Request gemäß [RFC4511]#4.5.1
Komponenten	Konnektor, VZD
Ausgangsdaten	<ul style="list-style-type: none"> LDAPv3 Search Response gemäß [RFC4511]#4.5.2
Standardablauf	1. Der Konnektor führt TUC_VZD_0001 „search_Directory“ mit dem vom LDAP-Client empfangenen Search Request als Eingangsdaten aus und empfängt die LDAPv3 Search Response vom VZD (entspricht den Ausgangsdaten).
Varianten/Alternativen	keine
Fehlerfälle	Auftretende Fehler werden gemäß [RFC4511]# Appendix A behandelt.
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

5282 [**<=**]

5283 4.1.12.4.3 TUC_KON_292 „LDAP-Verbindung trennen“

5284 TIP1-A_5519 - Konnektor, TUC_KON_292 „LDAP-Verbindung trennen“

5285 Der Konnektor MUSS den technischen Use Case „LDAP-Verbindung trennen“ gemäß
5286 TAB_KON_816 umsetzen.

5287

5288 **Tabelle 297: TAB_KON_816 – TUC_KON_292 „LDAP-Verbindung trennen“**

Element	Beschreibung
Name	TUC_KON_292 „LDAP-Verbindung trennen“
Beschreibung	Der Konnektor beendet die Verbindung zum VZD und zum LDAP-Client.
Auslöser	Aufruf durch einen LDAPv3 Unbind Request von einem Fachmodul-TUC oder einem Clientsystem
Vorbedingungen	<ul style="list-style-type: none"> • MGM_LU_ONLINE=Enabled • Eine LDAPv3-Verbindung LDAP-Client sowie eine LDAPv3 Verbindung vom Konnektor zum VZD wurden aufgebaut (TUC_KON_290 „Verbindungsaufbau zum VZD“)
Eingangsdaten	keine
Komponenten	Konnektor, VZD
Ausgangsdaten	keine
Standardablauf	<ol style="list-style-type: none"> 1. Der Konnektor empfängt vom LDAP-Client einen Unbind Request gemäß [RFC4511]#4.3. 2. Der Konnektor sendet zum VZD einen Unbind Request. 3. Der Konnektor beendet die Verbindung zum VZD und zum LDAP Client gemäß [RFC4511]#5.3.
Varianten/Alternativen	keine
Fehlerfälle	Auftretende Fehler werden gemäß [RFC4511]# Appendix A behandelt.
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

5289
5290 **[<=]**

5291 **4.1.12.4.4 TUC_KON_293 „Verzeichnisabfrage abbrechen“**

5292 **TIP1-A_5520 - Konnektor, TUC_KON_293 „Verzeichnisabfrage abbrechen“**

5293 Der Konnektor MUSS den technischen Use Case TUC_KON_293 „Verzeichnisabfrage
5294 abbrechen" gemäß TAB_KON_817 umsetzen.

5295

5296 **Tabelle 298: TAB_KON_817 – TUC_KON_293 „Verzeichnisabfrage abbrechen"**

Element	Beschreibung
Name	TUC_KON_293 „Verzeichnisabfrage abbrechen"
Beschreibung	Der Konnektor bricht einen unbeantworteten Search Request ab.
Auslöser	Aufruf durch einen LDAPv3 Abandon Request von einem Fachmodul-TUC oder einem Clientsystem
Vorbedingungen	<ul style="list-style-type: none"> • MGM_LU_ONLINE=Enabled • Ein Search Request wurde vom Konnektor empfangen und an den VZD weitergeleitet (TUC_KON_291 „Verzeichnis Abfragen"). Der Request wurde vom VZD noch nicht beantwortet.
Eingangsdaten	keine
Komponenten	Konnektor, VZD
Ausgangsdaten	keine
Standardablauf	<ol style="list-style-type: none"> 1. Der Konnektor empfängt vom LDAP-Client einen Abandon Request gemäß [RFC4511]#4.11. 2. Der Konnektor sendet zum VZD einen Abandon Request gemäß [RFC4511]#4.11
Varianten/Alternativen	keine
Fehlerfälle	Auftretende Fehler werden gemäß [RFC4511]# Appendix A behandelt.
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

5297

5298 [\leq]

5299 4.1.12.5 Operationen an der Außenschnittstelle

5300 4.1.12.5.1 Unterstützte LDAPv3 Operationen

5301 TIP1-A_5521 - Konnektor, LDAPv3 Operationen

5302 Der Konnektor MUSS an der Client-Schnittstelle die folgenden LDAPv3 Operationen
5303 gemäß [RFC4511] anbieten.

5304

- Bind Operation

5305

- Unbind Operation

5306

- Search Operation

- 5307 • Abandon Operation

5308 Andere LDAPv3 Operationen werden mit dem LDAP-Fehler unwillingToPerform (53)
5309 beantwortet.

5310 Wenn ANCL_TLS_MANDATORY=Enabled, muss der Konnektor sicherstellen, dass nur
5311 über eine LDAPS-Verbindung (Voreinstellung TCP Port 636) Daten abgefragt werden
5312 können.

5313 Wenn ANCL_TLS_MANDATORY=Disabled, muss der Konnektor sicherstellen, dass über
5314 eine LDAP-Verbindung (Voreinstellung TCP Port 389) und über eine LDAPS-Verbindung
5315 (Voreinstellung TCP Port 636) Daten abgefragt werden können.

5316 Fehler müssen gemäß [RFC4511]#Appendix A behandelt werden.

5317 [\leq]

5318 **4.1.12.6 Betriebsaspekte**

5319 keine

5320 **4.1.13 Authentifizierungsdienst**

5321 Der Authentifizierungsdienst bietet Clientsystemen und Fachmodulen eine Schnittstelle
5322 zum Signieren von Binärstrings zum Zweck der externen Authentisierung.

5323 Innerhalb des Authentifizierungsdienstes werden folgende Präfixe für Bezeichner
5324 verwendet:

- 5325 • Events (Topic Ebene 1): *keine Events vorhanden*
5326 • Konfigurationsparameter: *keine Konfigurationsparameter vorhanden*

5327 Eine Prüfung der Signatur bietet der Authentifizierungsdienst nicht an. Sie wird im
5328 Rahmen der Operation VerifyDocument des Signaturdienstes angeboten.

5329 **4.1.13.1 Funktionsmerkmalweite Aspekte**

5330 *4.1.13.1.1 Externe Authentisierung*

5331 TIP1-A_5437 - Signaturverfahren für externe Authentisierung

5332 Der Signaturdienst MUSS Signaturverfahren entsprechend TAB_KON_780 -
5333 Signaturverfahren Externe Authentisierung unterstützen.

5334 **Tabelle 299: TAB_KON_780 – Signaturverfahren Externe Authentisierung**

Signaturformat	Standard	Dokument formate	QES/ nonQES	Bemerkung
PKCS#1 (V2.1)	[RFC3447]	Binär	nonQES	Dieses Signaturformat DARF NUR in Verbindung mit dem zur Authentisierung vorgesehenen Schlüssel des HBAX und des SM-B genutzt werden. Die Nutzung ist auf Dokumente (Hash) von maximal 512 bit
ECDSA	[BSI-TR-03111]	Binär	nonQES	

				Länge beschränkt.
--	--	--	--	-------------------

5335

5336 [\leq]

5337 TIP1-A_5149 - PKCS#1-Schnittstelle nur für Authentisierung mit HBAX und SM-B nutzen

5338 Der Hersteller des Konnektors MUSS den Anwender (Clientsystem) im Handbuch des

5339 Konnektors geeignet und ausreichend darüber informieren, dass das Signaturformat

5340 PKCS#1 nur zu Authentisierungszwecken mit dem Authentisierungsschlüssel des HBAX

5341 und des SM-B verwendet werden darf. [\leq]

5342 A_17750 - ECDSA-Schnittstelle nur für Authentisierung mit HBAX und SM-B nutzen

5343 Der Hersteller des Konnektors MUSS den Anwender (Clientsystem) im Handbuch des

5344 Konnektors geeignet und ausreichend darüber informieren, dass das Signaturformat

5345 ECDSA (erzeugt mit Operation ExternalAuthenticate) nur zu Authentisierungszwecken mit

5346 dem Authentisierungsschlüssel des HBAX und des SM-B verwendet werden darf.

5347 [\leq]5348 **4.1.13.2 Durch Ereignisse ausgelöste Reaktionen**

5349 keine

5350 **4.1.13.3 Interne TUCs**

5351 keine

5352 **4.1.13.4 Operationen an der Außenschnittstelle**

5353 TIP1-A_5665 - Basisdienst Authentifizierungsdienst

5354 Der Konnektor MUSS Clientsystemen den Basisdienst Authentifizierungsdienst anbieten.

5355

5356 **Tabelle 300: TAB_KON_839 Basisdienst Authentifizierungsdienst**

Name	AuthSignatureService	
Version (KDV)	WSDL-Version: 7.4.1	
Namensraum	Siehe Anhang D	
Namensraum-Kürzel	SIG für Schema und SIGW für WSDL	
Operationen	Name	Kurzbeschreibung
	ExternalAuthenticate	Binärstring signieren (nonQES)
WSDL	AuthSignatureService.wsdl	
Schema	Kein	

5357

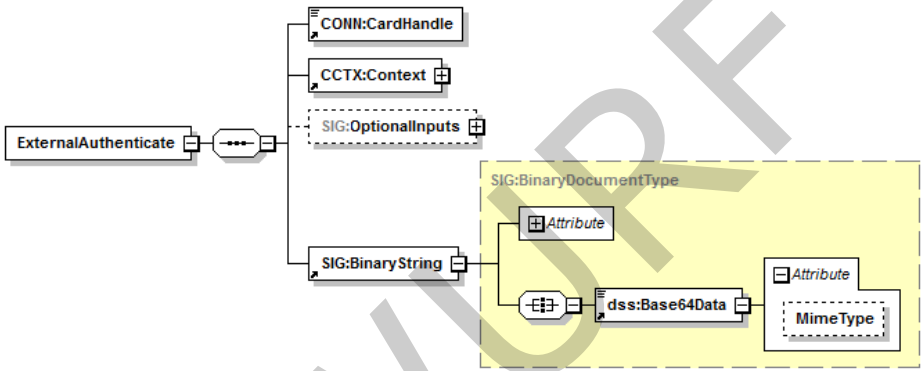
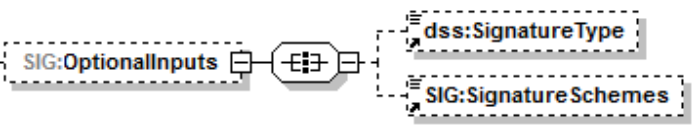
5358 [\leq]5359 **4.1.13.4.1 ExternalAuthenticate**

5360 TIP1-A_5439 - Operation ExternalAuthenticate

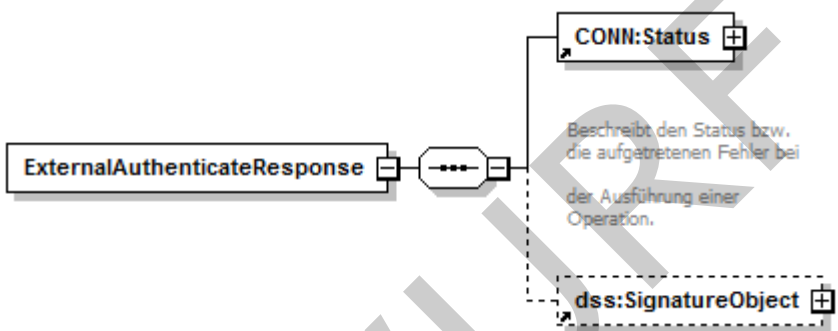
5361 Der Authentifizierungsdienst des Konnektors MUSS an der Clientschnittstelle eine
 5362 Operation ExternalAuthenticate anbieten.

5363

5364 **Tabelle 301: TAB_KON_781 Operation ExternalAuthenticate**

Name	ExternalAuthenticate	
Beschreibung	Diese Operation versieht einen Binärstring der maximalen Länge 512 Bit mit einer nicht-qualifizierten elektronischen Signatur (nonQES). Dazu wird das Signaturverfahren PKCS#1 oder ECDSA verwendet. Das AUT-Zertifikat der SM-B und das AUT-Zertifikat des HBAX werden unterstützt.	
Aufrufparameter		
	Name	Beschreibung
	CONN: CardHandle	Identifiziert die zu verwendende Signaturkarte. Die Operation unterstützt HBAX und SM-B.
	CCTX: Context	<u>Aufrufkontext für HBAX:</u> MandantId, ClientSystemId, WorkplaceId, UserId verpflichtend <u>Aufrufkontext für SM-B:</u> MandantId, ClientSystemId, WorkplaceId verpflichtend; UserId nicht ausgewertet
	SIG: Optional Inputs	Enthält optionale Eingangsparameter: 
	SIG: Binary String	Dieses Element enthält im Kindelement dss:Base64Data den zu signierenden Binärstring. Das XML Attribut SIG:BinaryString/dss:Base64Data/@MimeType MUSS den Wert "application/octet-stream" haben. Die maximale Länge des Binärstrings beträgt 512 Bit entsprechend der maximal zu erwartenden Hash-Größe. Aus der Länge des Binärstrings wird auf das verwendete Hashverfahren geschlossen. Es werden folgende Längen unterstützt:

		<ul style="list-style-type: none"> • 256 Bit: SHA-256 (OID 2.16.840.1.101.3.4.2.1) • 384 Bit: SHA-384 (OID 2.16.840.1.101.3.4.2.2) • 512 Bit: SHA-512 (OID 2.16.840.1.101.3.4.2.3) <p>Im Falle des Signaturverfahrens RSASSA-PKCS1-v1_5 werden SHA-256, SHA-384 und SHA-512 unterstützt.</p> <p>Im Falle des Signaturverfahrens RSASSA-PSS wird SHA-256 unterstützt.</p> <p>Im Falle des Signaturverfahrens ECDSA wird SHA-256 unterstützt.</p> <p>Für die Signaturerstellung gilt:</p> <ul style="list-style-type: none"> • Im Falle des Signaturverfahrens RSASSA-PKCS1-v1_5 beginnt der Konnektor die Ausführung der Methode EMSA-PKCS1-v1_5-ENCODE nach [RFC3447], Abschnitt 9.2, mit Schritt 2, Erstellung des DigestInfo-Datenfeldes. • Im Falle des Signaturverfahrens RSASSA-PSS beginnt der Konnektor die Ausführung der Methode EMSA-PSS-ENCODE nach [RFC3447], Abschnitt 9.1.1, mit Schritt 3. • Im Falle des Signaturverfahrens ECDSA erfolgt die Signaturerstellung gemäß [BSI-TR-03111]#4.2.1. Als Eingangsparameter wird der Hash vom Aufrufer in SIG: BinaryString übergeben.
	dss: Signature Type	<p>Durch dieses in [OASIS-DSS] (Abschnitt 3.5.1) beschriebene Element wird der Typ der zu erzeugenden Signatur bestimmt. Als Signatortyp wird unterstützt :</p> <ul style="list-style-type: none"> • PKCS#1-Signatur Durch Übergabe der URI urn:ietf:rfc:3447 wird eine PKCS#1 (Version 2.1) Signatur gemäß [RFC3447] erzeugt, die als <code>dss:Base64Signature</code> mit der oben genannten URI zurückgeliefert wird. • ECDSA-Signatur Durch Übergabe der URI urn:bsi:tr:03111:ecdsa wird eine ECDSA-Signatur gemäß [BSI-TR-03111]#4.2.1 erzeugt, die als <code>dss:Base64Signature</code> mit der oben genannten URI zurückgeliefert wird. <p>Andere <code>SignatureType</code>-Angaben führen zu einer Fehlermeldung 4111 (Ungültiger Signatortyp oder Signaturvariante).</p>

		Fehlt dieses Element, so wird ebenfalls der Signaturtyp PKCS#1-Signatur verwendet.
	SIG: Signature Schemes	<p>Durch dieses Element wird für PKCS#1-Signaturen zwischen den folgenden SignatureScheme-Optionen unterschieden:</p> <ul style="list-style-type: none"> • RSASSA-PSS • RSASSA-PKCS1-v1_5 <p>Fehlt dieses Element, so wird als Default-SignatureScheme RSASSA-PSS gewählt.</p>
Rückgabe	 <p>The diagram shows a sequence of elements: ExternalAuthenticateResponse, followed by an ellipsis, then CONN:Status, and finally dss:SignatureObject. A dashed line connects the CONN:Status element to a text box that reads: 'Beschreibt den Status bzw. die aufgetretenen Fehler bei der Ausführung einer Operation.'</p>	
	CONN: Status	Enthält den Status der ausgeführten Operation.
	dss: Signature Object	<p>Enthält im Erfolgsfall die erzeugte Signatur in Form eines <code>dss:SignatureObject</code>-Elements gemäß [OASIS-DSS] (Abschnitt 3.2).</p> <p>Der Signaturwert wird im XML-Element <code>dss:SignatureObject/dss:Base64Signature</code> übergeben. Die Signatur wird binär gemäß [BSI-TR-03111]#5.2.2 in der ASN.1 Struktur ECDSA-Sig-Value zurückgegeben.</p> <p>Das XML-Attribut <code>dss:SignatureObject/dss:Base64Signature/@Type</code> kennzeichnet durch den Wert:</p> <ul style="list-style-type: none"> • urn:ietf:rfc:3447 den Signatur-Typ PKCS#1 bzw. • urn:bsi:tr:03111:ecdsa den Signatur-Typ ECDSA. <p>Die XML-Elemente <code>dss:SignatureObject/ds:Signature</code>, <code>dss:SignatureObject/dss:Timestamp</code>, <code>dss:SignatureObject/dss:SignaturePtr</code>, <code>dss:SignatureObject/dss:Other</code> werden nicht verwendet.</p>
Vorbeding ungen	Keine	

Nachbedingungen	Keine
------------------------	-------

5365 Der Ablauf der Operation ExternalAuthenticate ist in Tabelle TAB_KON_782 beschrieben:

5366 **Tabelle 302: TAB_KON_782 Ablauf Operation ExternalAuthenticate**

Nr.	Aufruf Technischer Use Case oder Interne Operation	Beschreibung
1.	checkArguments	Alle übergebenen Parameterwerte werden auf Konsistenz und Gültigkeit überprüft. Treten hierbei Fehler auf, so bricht die Operation mit Fehler 4000 ab.
2.	TUC_KON_000 „Prüfe Zugriffs- berechtigung“	Die Prüfung erfolgt durch den Aufruf TUC_KON_000 { \$context.mandantId; \$context.clientsystemId; \$context.workplaceId; \$context.userId; \$cardHandle } Tritt bei der Prüfung ein Fehler auf, bricht die Operation mit Fehlercode aus TUC_KON_000 ab.
3.	TUC_KON_026 „Liefere CardSession“	Ermittle CardSession über TUC_KON_026 { MandantId, CsId, CardHandle, UserId }
4.	TUC_KON_218 „Signiere“	Signaturberechnung durch Aufruf des TUC_KON_218 { PinRef = PIN.CH bzw. PIN.SMC; KeyRef = PrK.HP.AUT bzw. PrK.HCI.AUT; AlgorithmusID = signPKCS1_V1_5 oder signPSS oder signECDSA; DTBS = Binärstring }

5367 **Tabelle 303: TAB_KON_783 Übersicht Fehler Operation ExternalAuthenticate**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen TUCs können folgende weitere Fehlercodes auftreten:			
4000	Technical	Error	Syntaxfehler
4058	Security	Error	Aufruf nicht zulässig

5368 Die folgende Tabelle führt die zulässigen privaten Schlüssel für die Operation
5369 ExternalAuthenticate auf:

5370 **Tabelle 304: TAB_KON_784 Privater Schlüssel je Karte für ExternalAuthenticate**

Karte	Schlüssel
SM-B	PrK.HCI.AUT in DF.ESIGN
HBAx	PrK.HP.AUT in DF.ESIGN

5371 [**<=**]

5372 **4.1.13.5 Betriebsaspekte**

5373 Keine

5374 4.2 Netzkonnektor

5375 4.2.1 Anbindung LAN/WAN

5376 Unter Anbindung LAN/WAN werden die Mechanismen beschrieben, mit denen der
5377 Konnektor auf der einen Seite in das lokale Netz der Einsatzumgebung, auf der anderen
5378 Seite in die TI bzw. die Bestandsnetze angebunden wird. Diese wesentlichen Aspekte
5379 betreffen Routing und Firewall.

5380 Innerhalb des Kapitels Anbindung LAN/WAN werden folgende Präfixe für Bezeichner
5381 verwendet:

- 5382 • Events (Topic Ebene 1): „ANLW“
- 5383 • Konfigurationsparameter: „ANLW_“

5384 4.2.1.1 Funktionsmerkmalweite Aspekte

5385 TIP1-A_4723 - Verhalten als IPv4 Router

5386 Der Konnektor MUSS sich nach den in [RFC1812#1.1.3] definierten Rahmenbedingungen
5387 als IP Version 4 (IPv4) Router verhalten.

5388 Hiervon ausgenommen sind die in den folgenden Kapiteln aufgeführten Anforderungen
5389 des [RFC1812]:

- 5390 • 7.2 INTERIOR GATEWAY PROTOCOLS
- 5391 • 7.3 EXTERIOR GATEWAY PROTOCOLS
- 5392 • 7.5 FILTERING OF ROUTING INFORMATION
- 5393 • 7.6 INTER-ROUTING-PROTOCOL INFORMATION EXCHANGE
- 5394 • 8. APPLICATION LAYER - NETWORK MANAGEMENT PROTOCOLS
- 5395 • 9. APPLICATION LAYER - MISCELLANEOUS PROTOCOLS
- 5396 • 10. OPERATIONS AND MAINTENANCE

5397 Die in [RFC2644] geforderten Aktualisierungen zum [RFC1812] müssen vom Konnektor
5398 umgesetzt werden.

5399 [\leq]

5400 TIP1-A_5406 - IP-Pakete mit Source Route Option

5401 Der Konnektor DARF NICHT IP-Pakete mit gesetzter Source Route Option gemäß
5402 [RFC791] erzeugen oder weiterleiten.

5403 [\leq]

5404 In der folgenden Anforderung wird die Terminologie gemäß [RFC2663] verwendet.

5405 TIP1-A_5407 - NAT-Umsetzung im Konnektor

5406 Der Konnektor MUSS für die Kommunikation aus den Adressbereichen NET_LEKTR-
5407 Umgebung mit den Adressbereichen NET_TI_OFFENE_FD und ANLW_BESTANDSNETZE
5408 eine Network Address Port Translation (NAPT) gemäß [RFC3022#2.2, 3, 4.1-4.3]
5409 vornehmen.

5410 Für die Umsetzung der Private Local Address aus den Adressbereichen der
5411 Einsatzumgebung MUSS die IP-Adresse VPN_TUNNEL_TI_INNER_IP als Global Address
5412 genutzt werden.

5413 Der Konnektor MUSS für die Kommunikation aus den Adressbereichen der NET_LEKTR-
5414 Umgebung mit dem Internet über den VPN-Tunnel SIS eine Network Address Port
5415 Translation (NAPT) gemäß RFC3022#2.2, 3, 4.1-4.3 vornehmen. Für die Umsetzung der
5416 Local Address MUSS die IP-Adresse VPN_TUNNEL_SIS_INNER_IP als Global Address

5417 genutzt werden.

5418 [**<=**]

5419 TIP1-A_4724 - LAN-Adapter

5420 Der Konnektor MUSS sicherstellen, dass nur über den LAN-Adapter (Adressen aus
5421 ANLW_LAN_NETWORK_SEGMENT oder Adressen aus einem der Netzwerksegmente in
5422 ANLW_LEKTR_INTRANET_ROUTES) mit den Clientsystemen und den Kartenterminals
5423 kommuniziert werden kann.

5424 [**<=**]

5425 TIP1-A_4725 - WAN-Adapter

5426 Für den Betrieb in Reihe (ANLW_ANBINDUNGS_MODUS=InReihe) MUSS der Konnektor
5427 den WAN-Adapter für den Zugang zum Internet über das IAG der Einsatzumgebung
5428 verwenden.

5429 [**<=**]

5430 TIP1-A_4726 - Internet Anbindung nur bei MGM_LU_ONLINE

5431 Der Hersteller des Konnektors MUSS sicherstellen, dass eine Anbindung an das
5432 Transportnetz/Internet nur möglich ist, wenn (MGM_LU_ONLINE=Enabled) gesetzt ist.

5433 [**<=**]

5434 TIP1-A_4728 - Nur IPv4. IPv6 nur hardwareseitig vorbereitet

5435 Der Konnektor MUSS IP Version 4 (IPv4) für alle seine IP-Schnittstellen unterstützen.

5436 Die Hardware des Konnektors MUSS für den Einsatz von IPv4 und IPv6 im Dual-Stack-
5437 Mode geeignet sein.

5438 Bis zu einer Migration von IPv4 auf IPv6 MUSS der Konnektor sämtliche empfangene IP-
5439 Pakete der Version 6 (IPv6) verwerfen.

5440 [**<=**]

5441 TIP1-A_4728-01 - IPv4 und IPv6 (Option IPv6)

5442 Der Konnektor MUSS IP Version 4 (IPv4) und IP Version 6 (IPv6) für alle seine
5443 physikalischen Adapter unterstützen.

5444 Die Hardware des Konnektors MUSS für den Einsatz von IPv4 und IPv6 im Dual-Stack-
5445 Mode geeignet sein.

5446 [**<=**]

5447 TIP1-A_4729 - Es darf kein dynamisches Routing verwendet werden

5448 Dynamische Routing-Protokolle dürfen vom Konnektor nicht eingesetzt werden. Wird in
5449 einem der an den Konnektor angeschlossenen Netzwerke ein dynamisches Routing
5450 genutzt, so DÜRFEN Routing Updates vom Konnektor NICHT akzeptiert werden und keine
5451 Routen eingetragen werden.

5452 [**<=**]

5453 TIP1-A_5152 - Aktualisieren der Infrastrukturinformationen aus der TI

5454 Falls Parameter MGM_LU_ONLINE=Enabled, MUSS der Konnektor einmal täglich
5455 TUC_KON_283 „Infrastruktur Konfiguration aktualisieren“ aufrufen.

5456 [**<=**]

5457 4.2.1.1.1 Netzwerksegmentierung

5458 In Anlehnung an die in der [gemSpec_Net#2.3.3] definierten Netzwerksegmente werden
5459 in der Konnektorspezifikation die folgenden Bezeichner verwendet:

5460

5461 **Tabelle 305: TAB_KON_680 Mapping der Netzwerksegmente**

ReferenzID im Konnektor	Adressbereich für die TI-Produktivumgebung	Adressbereich für die TI-Testumgebung	Adressbereich für die TI-Referenzumgebung
NET_SIS	TI_Dezentral_SIS - Konnektoren	TI_Test_Dezentral_SIS - Konnektoren	Ist durch den Testbetriebsverantwortlichen zu definieren.
NET_TI_DEZENTRAL	TI_Dezentral - Konnektoren	TI_Test_Dezentral - Konnektoren	Ist durch den Testbetriebsverantwortlichen zu definieren.
NET_TI_ZENTRAL	TI_Zentral - Zentrale Dienste	TI_Test_Zentral - Zentrale Dienste	Ist durch den Testbetriebsverantwortlichen zu definieren.
NET_TI_OFFENE_FD	Anwendungsdienste - Offene Fachdienste - aAdG und aAdG-NetG-TI	Test_Anwendungsdienste - Offene Fachdienste - aAdG und aAdG-NetG-TI	Ist durch den Testbetriebsverantwortlichen zu definieren.
NET_TI_GESICHERTE_FD	Anwendungsdienste - Gesicherte Fachdienste	Test_Anwendungsdienste - Gesicherte Fachdienste	Ist durch den Testbetriebsverantwortlichen zu definieren.
NET_LEKTR	Liste der Netzwerke die in der Einsatzumgebung über den Konnektor erreichbar sind. Ein Eintrag der Liste enthält die Netzwerkadresse und den Netzwerkprefix.		
ANLW_BESTANDS_NETZE	Liste der an die TI angeschlossenen Bestandsnetze (u. a. das Sichere Netz der KVen). Ein Eintrag der Liste enthält die Netzwerkadresse und den Netzwerkprefix.		
ANLW_AKTIVE_BESTANDS_NETZE	Liste der an die TI angeschlossenen und aktivierten Bestandsnetze		

5462

5463 **Tabelle 306: TAB_KON_681 Definition der vom Konnektor verwendeten VPN-Tunnel**

ReferenzID	Bedeutung/Belegung
VPN_TI	Logischer Adapter des VPN-Tunnel zur TI mit dessen VPN_TUNNEL_TI_INNER_IP aus dem Adresssegment NET_TI_DEZENTRAL
VPN_SIS	Logischer Adapter des VPN-Tunnel zur SIS mit dessen VPN_TUNNEL_SIS_INNER_IP aus dem Adresssegment NET_SIS

5464

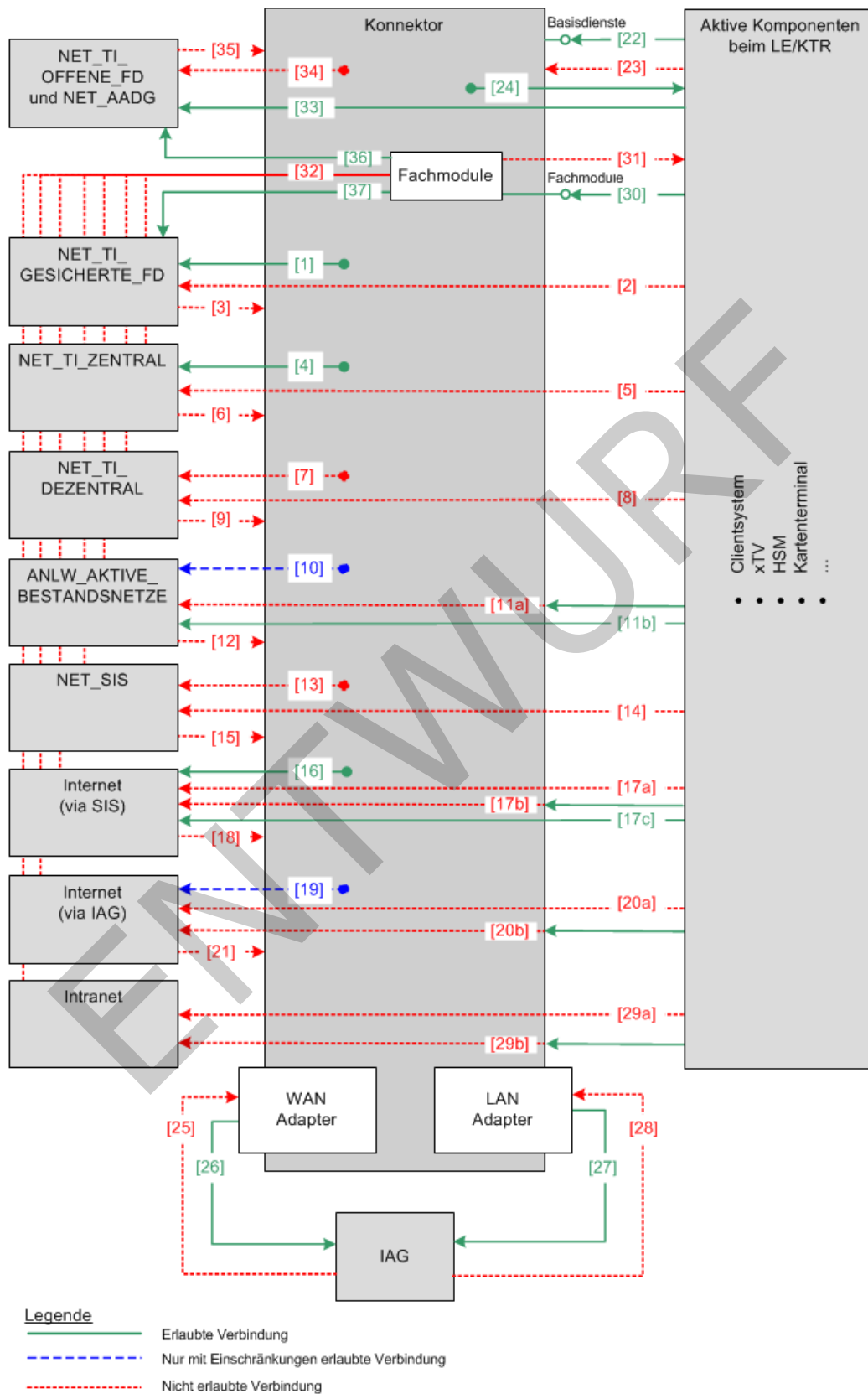
5465 **Tabelle 307: TAB_KON_682 Definition der Konnektor IP-Adressen**

ReferenzID	Bedeutung/Belegung
ANLW_LAN_IP_ADDRESS	Dies ist die IP-Adresse des LAN-Adapters. Aus dem Netz der Einsatzumgebung (ANLW_LAN_NETWORK_SEGMENT) die vom Konnektor verwendete IP-Adresse. Unter dieser Adresse werden die Dienste des Konnektor im lokalen Netzwerk bereitgestellt. Diese Adresse entspricht dem in Tabelle TAB_KON_683 LAN-Adapter IP-Konfiguration definierten Parameter ANLW_LAN_IP_ADDRESS.
ANLW_WAN_IP_ADDRESS	Dies ist die IP-Adresse des WAN-Adapters.

5466 *4.2.1.1.2 Routing und Firewall*5467 **Darstellung der Kommunikationsregeln des Konnektors**

5468 Diese Abbildung dient der Veranschaulichung der im Konnektor verwendeten
 5469 Kommunikationsregeln welche in den nachfolgenden Afo definiert werden.

5470



5471

5472

Abbildung 21: PIC_KON_115 Kommunikationsregeln Konnektor

- 5473 TIP1-A_4730 - Kommunikation mit NET_TI_GESICHERTE_FD
5474 Der Konnektor MUSS sicherstellen, dass IP-Pakete mit einer Absenderadresse aus dem
5475 Adressbereich NET_TI_GESICHERTE_FD verworfen werden, wenn sie nicht aus dem VPN-
5476 Tunnel der TI (VPN_TI) stammen.
5477 Der Konnektor MUSS die Kommunikation mit Systemen des Netzwerksegments
5478 NET_TI_GESICHERTE_FD für folgende Fälle unterstützen:
- 5479 • [1] vom Konnektor kommend
 - 5480 • [37] wenn (MGM_LU_ONLINE=Enabled) vom Fachmodul kommend
- 5481 Der Konnektor MUSS insbesondere die Kommunikation an seinen Außenschnittstellen mit
5482 Systemen des Netzwerksegments NET_TI_GESICHERTE_FD für folgende Fälle blockieren:
- 5483 • [2] von „Aktive Komponenten“ kommend
 - 5484 • [3] in Richtung Konnektor gehend
- 5485 Der Konnektor MUSS sicherstellen, dass die aus einer unterstützten Kommunikation mit
5486 Systemen aus dem Netzwerksegment NET_TI_GESICHERTE_FD bestimmten IP-Pakete
5487 ausschließlich in den VPN-Tunnel der TI (VPN_TI) geleitet werden.
5488 [\leq]
- 5489 TIP1-A_5530 - Kommunikation mit NET_TI_OFFENE_FD
5490 Der Konnektor MUSS sicherstellen, dass IP-Pakete mit einer Absenderadresse aus dem
5491 Adressbereich NET_TI_OFFENE_FD verworfen werden, wenn sie nicht aus dem VPN-
5492 Tunnel der TI (VPN_TI) stammen.
5493 Der Konnektor MUSS die Kommunikation mit Systemen des Netzwerksegments
5494 NET_TI_OFFENE_FD für folgende Fälle unterstützen:
- 5495 • [33] von „Aktive Komponenten“ kommend
 - 5496 • [36] vom Fachmodul kommend
- 5497 Der Konnektor MUSS insbesondere die Kommunikation an seinen Außenschnittstellen mit
5498 Systemen des Netzwerksegments NET_TI_OFFENE_FD für folgende Fälle blockieren:
- 5499 • [34] vom Konnektor kommend
 - 5500 • [35] in Richtung Konnektor gehend
- 5501 Der Konnektor MUSS sicherstellen, dass die aus einer unterstützten Kommunikation mit
5502 Systemen aus dem Netzwerksegment NET_TI_OFFENE_FD bestimmten IP-Pakete
5503 ausschließlich in den VPN-Tunnel der TI (VPN_TI) geleitet werden.
5504 [\leq]
- 5505 TIP1-A_4731 - Kommunikation mit NET_TI_ZENTRAL
5506 Der Konnektor MUSS sicherstellen, dass IP-Pakete mit einer Absenderadresse aus dem
5507 Adressbereich NET_TI_ZENTRAL verworfen werden, wenn sie nicht aus dem VPN-Tunnel
5508 der TI (VPN_TI) stammen.
5509 Der Konnektor MUSS die Kommunikation mit Systemen des Netzwerksegments
5510 NET_TI_ZENTRAL für folgende Fälle unterstützen:
- 5511 • [4] vom Konnektor kommend
- 5512 Der Konnektor MUSS insbesondere die Kommunikation an seinen Außenschnittstellen mit
5513 Systemen des Netzwerksegments NET_TI_ZENTRAL für folgende Fälle blockieren:
- 5514 • [5] von „Aktive Komponenten“ kommend
 - 5515 • [6] in Richtung Konnektor gehend
- 5516 Der Konnektor MUSS sicherstellen, dass die aus einer unterstützten Kommunikation mit
5517 Systemen aus dem Netzwerksegment NET_TI_ZENTRAL bestimmten IP-Pakete

- 5518 ausschließlich in den VPN-Tunnel der TI (VPN_TI) geleitet werden.
5519 **[<=]**
- 5520 TIP1-A_4732 - Kommunikation mit NET_TI_DEZENTRAL
5521 Der Konnektor MUSS sicherstellen, dass die Adressen aus dem Adressbereich
5522 NET_TI_DEZENTRAL nur für die Kommunikation mit der TI/den weiteren Anwendungen
5523 des Gesundheitswesens in Form der inner IP (VPN_TUNNEL_TI_INNER_IP) des VPN-
5524 Tunnel der TI (VPN_TI) verwendet wird.
5525 Der Konnektor MUSS die Kommunikation mit Systemen des Netzwerksegments
5526 NET_TI_DEZENTRAL für folgende Fälle unterstützen:
- 5527 • keine
- 5528 Der Konnektor MUSS insbesondere die Kommunikation an seinen Außenschnittstellen mit
5529 Systemen des Netzwerksegments NET_TI_DEZENTRAL für folgende Fälle blockieren:
- 5530 • [7] vom Konnektor kommend (zur Verhinderung des Zugriffs auf fremde
5531 Konnektoren)
- 5532 • [8] von „Aktive Komponenten“
- 5533 • [9] in Richtung Konnektor gehend
- 5534 **[<=]**
- 5535 TIP1-A_4733 - Kommunikation mit ANLW_AKTIVE_BESTANDSNETZE
5536 Der Konnektor MUSS sicherstellen, dass IP-Pakete mit einer Absenderadresse aus dem
5537 Adressbereich ANLW_AKTIVE_BESTANDSNETZE verworfen werden, wenn sie nicht aus
5538 dem VPN-Tunnel der TI (VPN_TI) stammen.
5539 Der Konnektor MUSS die Kommunikation mit Systemen des Netzwerksegments
5540 ANLW_AKTIVE_BESTANDSNETZE für folgende Fälle unterstützen:
- 5541 • [10] wenn (MGM_LU_ONLINE=Enabled) vom Konnektor kommend nur für die
5542 DNS-Namensauflösung mittels DNS_SERVERS_BESTANDSNETZE
- 5543 • [11b] wenn (MGM_LU_ONLINE=Enabled) von „Aktive Komponenten“ kommend
- 5544 Der Konnektor MUSS insbesondere die Kommunikation an seinen Außenschnittstellen mit
5545 Systemen des Netzwerksegments ANLW_AKTIVE_BESTANDSNETZE für folgende Fälle
5546 blockieren:
5547
- 5548 • [11a] für nicht freigegebene angeschlossene Netze des Gesundheitswesens mit
5549 aAdG-NetG (ANLW_BESTANDSNETZE abzüglich ANLW_AKTIVE_BESTANDSNETZE)
5550 von „Aktive Komponenten“ kommend;
- 5551 • [12] in Richtung Konnektor gehend (und den dahinterliegenden „Aktive
5552 Komponenten“)
- 5553 Der Konnektor MUSS sicherstellen, dass die aus einer unterstützten Kommunikation mit
5554 Systemen aus dem Netzwerksegment ANLW_AKTIVE_BESTANDSNETZE bestimmten IP-
5555 Pakete ausschließlich in den VPN-Tunnel der TI (VPN_TI) geleitet werden.
5556 **[<=]**
- 5557 TIP1-A_4734 - Kommunikation mit NET_SIS
5558 Der Konnektor MUSS sicherstellen, dass eine Adresse aus dem Adressbereich NET_SIS
5559 nur für die Kommunikation mit dem Internet (via SIS) in Form der inner IP
5560 (VPN_TUNNEL_SIS_INNER_IP) des VPN-Tunnel der SIS (VPN_SIS) verwendet wird.
5561 Der Konnektor MUSS insbesondere die Kommunikation mit Systemen des
5562 Netzwerksegments NET_SIS für folgende Fälle unterstützen:
- 5563 • keine

5564 Der Konnektor MUSS die Kommunikation an seinen Außenschnittstellen mit NET_SIS für
5565 folgende Fälle blockieren:

- 5566 • [13] vom Konnektor kommend
- 5567 • [14] von „Aktive Komponenten“ kommend
- 5568 • [15] in Richtung Konnektor gehend (und den dahinterliegenden „Aktiven
5569 Komponenten“)

5570 [**<=**]

5571 TIP1-A_4735 - Kommunikation mit dem Internet (via SIS)

5572 Der Konnektor MUSS sicherstellen, dass IP-Pakete mit einer Absenderadresse aus dem
5573 Adressbereich NET_TI_ZENTRAL, NET_TI_GESICHERTE_FD; NET_TI_OFFENE_FD,
5574 NET_TI_DEZENTRAL, ANLW_AKTIVE_BESTANDSNETZE,
5575 ANLW_LAN_ADDRESS_SEGMENT, aus einem der Netzwerksegmente in
5576 ANLW_LEKTR_INTRANET_ROUTES oder ANLW_WAN_NETWORK_SEGMENT verworfen
5577 werden, wenn sie aus dem VPN-Tunnel der SIS (VPN_SIS) stammen.

5578 Der Konnektor MUSS die Kommunikation mit Systemen des Netzwerksegments Internet
5579 (via SIS) für folgende Fälle unterstützen:

- 5580 • [16] wenn (MGM_LU_ONLINE=Enabled und ANLW_INTERNET_MODUS=SIS)
5581 vom Konnektor kommend
- 5582 • [17c] wenn (MGM_LU_ONLINE=Enabled und ANLW_INTERNET_MODUS=SIS)
5583 von „Aktive Komponenten“ kommend

5584 Der Konnektor MUSS insbesondere die Kommunikation an seinen Außenschnittstellen mit
5585 Internet (via SIS) für folgende Fälle blockieren oder umleiten:

- 5586 • [17a] blockieren, wenn (MGM_LU_ONLINE=Enabled und
5587 ANLW_INTERNET_MODUS=KEINER) von „Aktive Komponenten“ kommend
- 5588 • [17b] umleiten, wenn (MGM_LU_ONLINE=Enabled und
5589 ANLW_INTERNET_MODUS=IAG) von „Aktive Komponenten“ kommend;
5590 ➔ Der Konnektor MUSS an Hosts im Internet gerichtete IP-Pakete gemäß
5591 [RFC792] umleiten (ICMP Redirect).
- 5592 • [18] blockieren, wenn von SIS kommend in Richtung Konnektor (und die
5593 dahinterliegenden „Aktive Komponenten“)

5594 Der Konnektor MUSS sicherstellen, dass die für die Kommunikation mit dem
5595 Internet (via SIS) bestimmten IP-Pakete ausschließlich in den VPN-Tunnel des SIS
5596 (VPN_SIS) geleitet werden.

5597 [**<=**]

5598 TIP1-A_4736 - Kommunikation mit dem Internet (via IAG)

5599 Der Konnektor MUSS sicherstellen, dass eingehende IP-Pakete von der Kommunikation
5600 mit dem Internet mit der Empfängeradresse ungleich (ANLW_LAN_IP_ADDRESS oder aus
5601 einem der Netzwerksegmente in ANLW_LEKTR_INTRANET_ROUTES wenn
5602 ANLW_WAN_ADAPTER_MODUS=DISABLED) oder (ANLW_WAN_IP_ADDRESS wenn
5603 ANLW_WAN_ADAPTER_MODUS=ENABLED) verworfen werden.

5604 Der Konnektor MUSS sicherstellen, dass ausgehende IP-Pakete für die Kommunikation
5605 mit dem Internet mit der Absenderadresse ungleich (ANLW_LAN_IP_ADDRESS oder aus
5606 einem der Netzwerksegmente in ANLW_LEKTR_INTRANET_ROUTES wenn
5607 ANLW_WAN_ADAPTER_MODUS=DISABLED) oder (ANLW_WAN_IP_ADDRESS wenn
5608 ANLW_WAN_ADAPTER_MODUS=ENABLED) verworfen werden.

5609 Der Konnektor MUSS die Kommunikation mit Systemen des Netzwerksegments Internet
5610 (via IAG) für folgende Fälle unterstützen:

- 5611 • [19] vom Konnektor kommend zu den folgenden Systemen für das Protokoll IPsec
- 5612 • VPN_KONZENTRATOR_TI_IP_ADDRESS
- 5613 • VPN_KONZENTRATOR_SIS_IP_ADDRESS
- 5614 • [19] vom Konnektor kommend zu den folgenden Systemen für HTTP und HTTPS
- 5615 • CERT_CRL_DOWNLOAD_ADDRESS
- 5616 • hash&URL-Server
- 5617 • Registrierungsserver
- 5618 • Remote-Managementserver
- 5619 • DNS_ROOT_ANCHOR_URL (benötigte IP-Adressen um den DNSSEC Trust
- 5620 Anchor im Namensraum Internet zu verifizieren)
- 5621 • [19] vom Konnektor kommend zu den folgenden Systemen für das Protokoll DNS
- 5622 • beliebige Hosts

5623 Der Konnektor MUSS insbesondere die Kommunikation an seinen Außenschnittstellen mit
 5624 Internet (via IAG) für folgende Fälle blockieren oder umleiten:

- 5625 • [20a] blockieren, wenn (ANLW_INTERNET_MODUS=KEINER oder
- 5626 MGM_LU_ONLINE=Disabled) von „Aktive Komponenten“ kommend
- 5627 • [20b] mittels ICMP Redirect gemäß [RFC792] zum Default Gateway umleiten,
- 5628 wenn die Zieladresse des IP-Pakets nicht innerhalb der Adressbereiche
- 5629 (NET_TI_ZENTRAL, NET_TI_OFFENE_FD, NET_TI_GESICHERTE_FD und
- 5630 ANLW_AKTIVE_BESTANDSNETZE) ist und ANLW_INTERNET_MODUS=IAG und von
- 5631 „Aktive Komponenten“ kommend.
- 5632 • [21] blockieren, wenn von IAG kommend in Richtung Konnektor (und die
- 5633 dahinterliegenden „Aktive Komponenten“)

5634 [**<=**]

5635

5636

5637

5638 TIP1-A_4737 - Kommunikation mit „Aktive Komponenten“

5639 Der Konnektor MUSS sicherstellen, dass ausgehende IP-Pakete für die Kommunikation
 5640 mit „Aktive Komponenten“ mit einer Absenderadresse ungleich ANLW_LAN_IP_ADDRESS,
 5641 einer Adresse aus einem Netzwerksegment in ANLW_LEKTR_INTRANET_ROUTES oder
 5642 0.0.0.0 verworfen werden.

5643 Der Konnektor MUSS die Kommunikation mit „Aktive Komponenten“ für folgende Fälle
 5644 unterstützen:

- 5645 • [22] auf den Konnektor (mittels der Schnittstelle Basisdienste)
- 5646 • [24] vom Konnektor kommend

5647 Der Konnektor MUSS insbesondere die Kommunikation an seinen Außenschnittstellen mit
 5648 „Aktive Komponenten“ für folgende Fälle blockieren:

- 5649 • [23] zum Konnektor eingehend (direkt – ohne eine der Schnittstellen Fachmodule
- 5650 oder Basisdienste zu nutzen)

5651 [**<=**]

5652 TIP1-A_4738 - Route zum IAG

5653 Der Konnektor MUSS die Kommunikation mit dem IAG der Einsatzumgebung für folgende
5654 Fälle unterstützen:

- 5655 • [26] wenn (ANLW_WAN_ADAPTER_MODUS=ENABLED) vom WAN-Adapter
5656 kommend
- 5657 • [27] wenn (ANLW_WAN_ADAPTER_MODUS=DISABLED) vom LAN-Adapter
5658 kommend

5659 Der Konnektor MUSS insbesondere die Kommunikation an seinen Außenschnittstellen mit
5660 dem IAG der Einsatzumgebung für folgende Fälle blockieren:

- 5661 • [25] wenn (ANLW_WAN_ADAPTER_MODUS=ENABLED) zum WAN-Adapter
5662 eingehend
- 5663 • [28] wenn (ANLW_WAN_ADAPTER_MODUS=DISABLED) zum LAN-Adapter
5664 eingehend

5665 [**<=**]

5666 TIP1-A_4740 - Admin Defined Firewall Rules

5667 Die Firewall des Konnektor MUSS alle vom Administrator in
5668 ANLW_FW_SIS_ADMIN_RULES definierten Firewall-Regeln als zusätzliche Einschränkung
5669 übernehmen.

5670 [**<=**]

5671 TIP1-A_4741 - Kommunikation mit dem Intranet

5672 Der Konnektor MUSS die Kommunikation mit Systemen aus einem Intranet-VPN (einem
5673 der Netzwerksegmente ANLW_LEKTR_INTRANET_ROUTES) für folgende Fälle
5674 unterstützen:

- 5675 • [22] wenn von Aktive Komponenten aus dem Netzwerksegment
5676 ANLW_LEKTR_INTRANET_ROUTES kommend zum Konnektor mittels der
5677 Schnittstelle Basisdienste
- 5678 • [24] wenn vom Konnektor kommend zu ANLW_LEKTR_INTRANET_ROUTES
- 5679 • Der Konnektor MUSS insbesondere die Kommunikation an seinen
5680 Außenschnittstellen mit einem der Intranet Netzwerksegmente für folgende Fälle
5681 blockieren bzw. umleiten:
 - 5682 • [29a] blockieren, wenn (ANLW_INTRANET_ROUTES_MODUS=BLOCK) vom „Aktive
5683 Komponenten“ kommend;
 - 5684 • [29b] umleiten, wenn (ANLW_INTRANET_ROUTES_MODUS=REDIRECT) vom
5685 „Aktive Komponenten“ kommend;
5686 ➔ Der Konnektor MUSS an ANLW_LEKTR_INTRANET_ROUTES gerichtete IP-
5687 Pakete gemäß [RFC792] umleiten (ICMP Redirect).

5688 [**<=**]

5689 TIP1-A_4742 - Kommunikation mit den Fachmodulen

5690 Der Konnektor MUSS die Kommunikation mit den Fachmodulen für folgende Fälle
5691 unterstützen:

- 5692 • [30] von „Aktive Komponenten“ über Schnittstelle Fachmodule

5693 Der Konnektor MUSS insbesondere die Kommunikation an seinen Außenschnittstellen mit
5694 den Fachmodulen für folgende Fälle blockieren:

- 5695 • [31] zu „Aktive Komponenten“

- 5696 • [32] zu den Netzwerksegmenten, NET_TI_ZENTRAL, NET_TI_DEZENTRAL,
5697 ANLW_AKTIVE_BESTANDSNETZE, Internet (via SIS), Internet (via IAG) und
5698 Intranet
- 5699 [**<=**]
- 5700 TIP1-A_4744 - Firewall - Drop statt Reject
- 5701 Die Firewall des Konnektor MUSS alle abgelehnten IP-Pakete verwerfen (DROP) ohne ein
5702 ICMP-Destination-Unreachable (Type 3) zu schicken.
- 5703 [**<=**]
- 5704 TIP1-A_4746 - Firewall – Abwehr von IP-Spoofing, DoS/DDoS-Angriffe und Martian
5705 Packets
- 5706 Der Konnektor MUSS geeignete technische Funktionen zur Abwehr von IP-Spoofing und
5707 DoS/DDoS-Angriffen implementieren.
- 5708 Der Konnektor MUSS Martian Packets (Absender- oder Empfängeradressen aus den von
5709 der IETF als Special-Purpose definierten Netzbereichen), mindestens jedoch aus
5710 folgenden Netzbereichen 0.0.0.0/8, 127.0.0.0/8, 169.254.0.0/16, 192.0.0.0/24,
5711 192.0.2.0/24, 198.18.0.0/15, 198.51.100.0/24, 203.0.113.0/24, 224.0.0.0/4,
5712 240.0.0.0/4 verwerfen. Die in [RFC1918] und [RFC 6598] definierten Netzbereiche sind
5713 hiervon ausgenommen.
- 5714 [**<=**]
- 5715 TIP1-A_4745 - Eingeschränkte Nutzung von „Ping“
- 5716 Die Firewall des Konnektor MUSS TCP-Port-7(Echo)-Pakete verwerfen.
- 5717 Die Firewall des Konnektor MUSS ICMP-Echo-Request (Typ 8) und ICMP-Echo-Response
5718 (Typ 0) ausschließlich für die folgenden Kommunikationen zulassen:
- 5719 • vom Konnektor zu den VPN-Konzentratoren für SIS und TI über das Transportnetz
5720 (via IAG)
- 5721 • vom Konnektor zu dem CRL-Webservern (im Transportnetz) über das Internet
5722 (via SIS) und das Transportnetz (via IAG)
- 5723 • vom Konnektor zu dem IAG der Einsatzumgebung
- 5724 • vom Konnektor zu NET_TI_ZENTRAL
- 5725 • vom Konnektor zu NET_TI_GESICHERTE_FD
- 5726 • vom Konnektor zu NET_TI_OFFENE_FD
- 5727 • vom Konnektor zum lokalen Netzwerk (Adressen aus
5728 ANLW_LAN_NETWORK_SEGMENT oder Adressen aus einem der
5729 Netzwerksegmente in ANLW_LEKTR_INTRANET_ROUTES)
- 5730 • vom lokalen Netzwerk (Adressen aus ANLW_LAN_NETWORK_SEGMENT (jedoch
5731 ohne die ANLW_LAN_IP_ADDRESS) oder Adressen aus einem der
5732 Netzwerksegmente in ANLW_LEKTR_INTRANET_ROUTES) zum Konnektor
- 5733 • vom lokalen Netzwerk in ANLW_AKTIVE_BESTANDSNETZE (die freigegebenen
5734 angeschlossenen Netze des Gesundheitswesens mit aAdG-NetG)
- 5735 • vom lokalen Netzwerk in das Internet (via SIS)
- 5736 Die Firewall des Konnektors MUSS für alle anderen Kommunikationen ein ICMP-
5737 Echo-Request (Typ 8) verwerfen.
- 5738 [**<=**]
- 5739 TIP1-A_4747 - Firewall – Einschränkungen der IP-Protokolle
- 5740 Der Konnektor MUSS alle IP-Protokolle außer 1 (ICMP), 4 (IP in IP (encapsulation)), 17
5741 (UDP), 6 (TCP), 50 (ESP) und 108 (IPComp) für alle ein- oder ausgehenden Pakete an

5742 allen seinen Adaptern verwerfen.
5743 **[<=]**

5744 TIP1-A_4748 - Firewall – Routing-Regeln
5745 Der Konnektor DARF seine Routing-Regeln NICHT durch IP-Kommunikation beeinflussen
5746 lassen, weder mittels eines Routing-Protokolls (wie BGP oder RIP) noch mittels ICMP-
5747 Kommandos (wie Redirect (5), Router Advertisement (9/10) oder auch Mobile Host
5748 Redirect (32)) sondern MUSS diese ausschließlich durch TUC_KON_304 „Netzwerk-
5749 Routen einrichten“ setzen.
5750 Die Firewall des Konnektor MUSS alle aus einem der Tunnel (VPN_TI oder VPN_SIS)
5751 kommenden DHCP-Pakete verwerfen.
5752 Die Firewall des Konnektors MUSS an den Konnektor gerichtete IPsec-Pakete (IKE, ESP
5753 und IPsec NAT-T) verwerfen, sofern sie nicht einer vom Konnektor initiierten IPsec-
5754 Verbindung (VPN_TI und VPN_SIS) zugeordnet werden können.
5755 **[<=]**

5756 TIP1-A_4749 - Firewall Restart
5757 Der Konnektor MUSS gewährleisten, dass unmittelbar nach einer Änderung der
5758 Parameter eines Adapters (LAN-Adapter, WAN-Adapter, virtueller Adapter VPN_TI oder
5759 virtueller Adapter VPN_SIS) die Firewall des Konnektor neu erstellt und geladen wird.
5760 Wenn der WAN-Adapter verwendet wird (ANLW_WAN_ADAPTER_MODUS=ENABLED)
5761 DARF die Firewall des Konnektor bei einer Änderung der ANLW_WAN_IP_ADDRESS
5762 NICHT die Verbindungen über den LAN-Adapter durch einen Restart der Firewall
5763 beeinflussen.
5764 Wenn der WAN-Adapter verwendet wird (ANLW_WAN_ADAPTER_MODUS=ENABLED),
5765 DARF die Firewall des Konnektor bei einer Änderung der ANLW_LAN_IP_ADDRESS NICHT
5766 die Verbindungen über die Adapter WAN, VPN_TI oder VPN_SIS durch einen Restart der
5767 Firewall beeinflussen.
5768 **[<=]**

5769 Umsetzungshinweis für den Hersteller: Es können zwei getrennten Firewall-Regelsets für
5770 den LAN- bzw. für den WAN-Adapter verwendet werden.

5771 TIP1-A_4750 - Firewall-Protokollierung
5772 Der Konnektor MUSS bei Start und Stopp der Firewall einen Protokolleintrag mit der
5773 Schwere „Warning“ und dem Typ „Operations“ sowie mindestens folgenden
5774 Informationen generieren:

- 5775 • Zeitstempel, Aktion (Start/Stop), Ergebnis (Erfolg/Fehler), Auslöser
5776 (Prozess/User)

5777 Der Konnektor MUSS bei Konfigurationsänderungen der Firewall einen Protokolleintrag
5778 mit der Schwere „Warning“ und dem Typ „Operations“ sowie mindestens folgenden
5779 Informationen generieren:

- 5780 • Zeitstempel, Aktion (Add/Delete/Change), Details (Beschreibung der Änderung),
5781 Auslöser (Prozess/User)

5782 Der Konnektor MUSS für alle vom Konnektor ausgehenden, nicht zugelassenen
5783 Kommunikationsversuche einen Protokolleintrag mit der Schwere „Warning“ und dem Typ
5784 „Security“ sowie mindestens folgenden Informationen generieren:

- 5785 • Zeitstempel, Aktion (Drop, Reject), Absender-IP-Adresse, Empfänger-IP-Adresse,
5786 Protokoll, Absender-Port und Empfänger-Port, Interface über das das Paket
5787 empfangen wurde

5788 Der Konnektor MUSS für alle verworfenen IP-Spoofing- und Martian-Packets einen
5789 Protokolleintrag mit der Schwere „Warning“ und dem Typ „Security“ sowie mindestens
5790 folgenden Informationen generieren:

5791 • Zeitstempel, Aktion (Drop, Reject), Absender-IP-Adresse, Empfänger-IP-Adresse,
5792 Protokoll, Absender-Port und Empfänger-Port, Interface über das das Paket
5793 empfangen wurde

5794 Der Konnektor MUSS für alle von der Firewall verworfenen IP-Pakete einen
5795 Protokolleintrag mit der Schwere „Info“ und dem Typ „Security“ sowie mindestens
5796 folgenden Informationen generieren, wobei Layer 3 Broadcasts von der Protokollierung
5797 ausgenommen werden können:

5798 • Zeitstempel, Aktion (Drop, Reject), Absender-IP-Adresse, Empfänger-IP-Adresse,
5799 Protokoll, Absender-Port und Empfänger-Port, Interface über das das Paket
5800 empfangen wurde

5801 Der Konnektor MUSS für die Firewall-Protokollierung den TUC_KON_271 „Schreibe
5802 Protokolleintrag“ nutzen.
5803 [\leq]

5804 4.2.1.2 Durch Ereignisse ausgelöste Reaktionen

5805 TIP1-A_4751 - Reagiere auf LAN_IP_Changed
5806 Beim Auftreten eines der nachfolgenden Events MUSS der Konnektor den TUC_KON_305
5807 „LAN-Adapter initialisieren“ starten.

5808 • Event ANLW/LAN/IP_CHANGED
5809 • Event DHCP/LAN_CLIENT/RENEW

5810 [\leq]

5811 TIP1-A_4752 - Reagiere auf WAN_IP_Changed
5812 Beim Auftreten eines der nachfolgenden Events MUSS der Konnektor TUC_KON_306
5813 „WAN-Adapter initialisieren“ starten.

5814 • Event ANLW/WAN/IP_CHANGED
5815 • Event DHCP/WAN_CLIENT/RENEW

5816 [\leq]

5817 TIP1-A_4753 - Ereignisbasiert Netzwerkrouen einrichten
5818 Beim Auftreten eines der nachfolgenden Events MUSS der Konnektor den TUC_KON_304
5819 „Netzwerk-Routen einrichten“ aufrufen.

5820 • Event NETWORK/VPN_TI/UP
5821 • Event NETWORK/VPN_TI/DOWN
5822 • Event NETWORK/VPN_SIS/UP
5823 • Event NETWORK/VPN_SIS/DOWN
5824 • Event MGM/LU_CHANGED/LU_ONLINE

5825 [\leq]

5826 4.2.1.3 Interne TUCs, nicht durch Fachmodule nutzbar

5827 4.2.1.3.1 TUC_KON_305 „LAN-Adapter initialisieren“

5828 TIP1-A_4754 - TUC_KON_305 „LAN-Adapter initialisieren“

5829 Der Konnektor MUSS den technischen Use Case TUC_KON_305 „LAN-Adapter
5830 initialisieren“ umsetzen.

5831

5832 **Tabelle 308: TAB_KON_614 - TUC_KON_305 „LAN-Adapter initialisieren“**

Element	Beschreibung
Name	TUC_KON_305 LAN-Adapter initialisieren
Beschreibung	Initialisieren der LAN-Netzwerkschnittstelle
Auslöser	<ul style="list-style-type: none"> • Event ANLW/LAN/IP_CHANGED • Event DHCP/LAN_CLIENT/RENEW; BOOTUP
Vorbedingungen	<ul style="list-style-type: none"> • Wenn die IP-Konfiguration des LAN-Adapters statisch (DHCP_CLIENT_LAN_STATE=Disabled) gesetzt wird, MUSS der Konnektor gewährleisten, dass alle Konfigurationsparameter gemäß „Tabelle TAB_KON_683 LAN-Adapter IP-Konfiguration“, vorab über die Managementschnittstelle gesetzt wurden. • Wenn die IP-Konfiguration des LAN-Adapters dynamisch per DHCP (DHCP_CLIENT_LAN_STATE=Enabled) gesetzt wird, MUSS der DHCP-Client diese vorab gesetzt haben.
Eingangsdaten	Keine
Komponenten	Konnektor
Ausgangsdaten	Keine
Standardablauf	<p>1) Die in „Tabelle TAB_KON_683 LAN-Adapter IP-Konfiguration“, und „Tabelle TAB_KON_684 LAN-Adapter Erweiterte Parameter“, gesetzten Werte sind zur Konfiguration des LAN-Adapter zu verwenden.</p> <p>2) Rufe TUC_KON_304 „Netzwerk-Routen einrichten“</p> <p>3) Wenn (ANLW_WAN_ADAPTER_MODUS = DISABLED) und MGM_LU_ONLINE = ENABLED:</p> <ul style="list-style-type: none"> • Rufe TUC_KON_321 „Verbindung zu dem VPN-Konzentrator der TI aufbauen“. • Rufe TUC_KON_322 „Verbindung zu dem VPN-Konzentrator des SIS aufbauen“ <p>4) Firewall-Regeln aktualisieren und aktivieren. Tritt der Fehler 4164 auf, geht der Konnektor in den Betriebszustand EC_Firewall_Not_Reliable über.</p>
Varianten/ Alternativen	Keine

Fehlerfälle	(→ 1) Fehlerhafte LAN IP-Konfiguration; 4162 (→ 4) Beim Aktualisieren oder Aktivieren der Firewall-Regeln ist es zu einem Fehler gekommen; 4164
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

5833 **Tabelle 309: TAB_KON_615 Fehlercodes TUC_KON_305 „LAN-Adapter initialisieren“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4162	Technical	Error	Es liegt eine fehlerhafte LAN IP-Konfiguration vor.
4164	Technical	Fatal	Beim Aktualisieren oder Aktivieren der Firewall-Regeln ist es zu einem Fehler gekommen.

5834 [\leq]

5835 4.2.1.3.2 TUC_KON_306 „WAN-Adapter initialisieren“

5836 TIP1-A_4755 - TUC_KON_306 „WAN-Adapter initialisieren“

5837 Der Konnektor MUSS den technischen Use Case TUC_KON_306 „WAN-Adapter
5838 initialisieren“ umsetzen.

5839

5840 **Tabelle 310: TAB_KON_616 - TUC_KON_306 „WAN-Adapter initialisieren“**

Element	Beschreibung
Name	TUC_KON_306 WAN-Adapter initialisieren
Beschreibung	Initialisieren der WAN-Netzwerkschnittstelle
Auslöser	<ul style="list-style-type: none"> • Event ANLW/WAN/IP_CHANGED • Event DHCP/WAN_CLIENT/RENEW; BOOTUP
Vorbedingungen	
Eingangsdaten	Keine
Komponenten	Konnektor
Ausgangsdaten	Keine

Standardablauf	<p>1) Wenn ANLW_WAN_ADAPTER_MODUS = DISABLED oder MGM_LU_ONLINE = Disabled:</p> <p>a) Aktive VPN-Tunnel TI oder SIS (VPN_TI oder VPN_SIS) müssen gestoppt werden,</p> <p>2) Wenn ANLW_WAN_ADAPTER_MODUS = ENABLED und MGM_LU_ONLINE = ENABLED:</p> <p>a) Der WAN-Adapter wird abhängig von DHCP_CLIENT_WAN_STATE statisch oder dynamisch über DHCP konfiguriert. Die in „Tabelle TAB_KON_685 WAN-Adapter IP-Konfiguration,“ und „Tabelle TAB_KON_686 WAN-Adapter Erweiterte Parameter,“ gesetzten Werte sind zur Konfiguration des WAN-Adapter zu verwenden.</p> <p>b) Rufe TUC_KON_304 „Netzwerk-Routen einrichten“</p> <p>c) Rufe TUC_KON_321 „Verbindung zu dem VPN-Konzentrator der TI aufbauen“.</p> <p>d) Rufe TUC_KON_322 „Verbindung zu dem VPN-Konzentrator des SIS aufbauen“</p> <p>e) Firewall-Regeln aktualisieren und aktivieren. Tritt der Fehler 4164 auf, geht der Konnektor in den Betriebszustand EC_Firewall_Not_Reliable über.</p>
Varianten/ Alternativen	Keine
Fehlerfälle	<p>(→ 1) Fehlerhafte WAN IP-Konfiguration; 4163</p> <p>(→ 2) Beim Aktualisieren oder Aktivieren der Firewall-Regeln ist es zu einem Fehler gekommen; 4164</p>
Nichtfunktionale Anforderungen	Keine

5841 **Tabelle 311: TAB_KON_617 Fehlercodes TUC_KON_306 „WAN-Adapter initialisieren“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4163	Technical	Error	Es liegt eine fehlerhafte WAN-IP-Konfiguration vor.
4164	Technical	Fatal	Beim Aktualisieren oder Aktivieren der Firewall-Regeln ist es zu einem Fehler gekommen.

5842 [**<=**]

5843 4.2.1.3.3 TUC_KON_304 „Netzwerk-Routen einrichten“

5844 TIP1-A_4758 - TUC_KON_304 „Netzwerk-Routen einrichten“

5845 Der Konnektor MUSS den technischen Use Case TUC_KON_304 „Netzwerk-Routen
5846 einrichten“ umsetzen.

5847

5848

Tabelle 312: TAB_KON_622 - TUC_KON_304 „Netzwerk-Routen einrichten“

Element	Beschreibung
Name	TUC_KON_304 Netzwerk-Routen einrichten
Beschreibung	Anpassen der Routing-Tabelle
Auslöser	<ul style="list-style-type: none"> • TUC_KON_305 „LAN-Adapter initialisieren“ • TUC_KON_306 „WAN-Adapter initialisieren“ • Event NETWORK/VPN_TI/UP • Event NETWORK/VPN_TI/DOWN • Event NETWORK/VPN_SIS/UP • Event NETWORK/VPN_SIS/DOWN • Event MGM/LU_CHANGED/LU_ONLINE
Vorbedingungen	keine
Eingangsdaten	<ul style="list-style-type: none"> • IP-Konfiguration des LAN-Interface (gemäß Tabelle TAB_KON_683 LAN-Adapter IP-Konfiguration) • IP-Konfiguration des WAN-Interface (gemäß Tabelle TAB_KON_685 WAN-Adapter IP-Konfiguration) • ANLW_IAG_ADDRESS (IP-Adresse des IAG der Einsatzumgebung) • DNS_SERVERS_INT
Komponenten	Konnektor
Ausgangsdaten	Keine
Nachbedingungen	<ul style="list-style-type: none"> • Die Routing-Einträge im Konnektor wurden gesetzt.
Standardablauf	<p>Alle bestehenden Routen MÜSSEN vollständig durch die in diesem TUC ermittelten Routen ersetzt werden.</p> <p>1) Wenn (MGM_LU_ONLINE=Enabled) Der Konnektor MUSS die nachfolgenden Routen bereitstellen</p> <p>a)</p> <ul style="list-style-type: none"> i. Ziel: Lokale Netze der Einsatzumgebung gemäß ANLW_LEKTR_INTRANET_ROUTES Next Hop: gemäß ANLW_LEKTR_INTRANET_ROUTES <p>b) Wenn die VPN-Tunnel zur TI und zum SIS nicht aufgebaut sind:</p> <ul style="list-style-type: none"> i. Ziel: Default Route Next Hop: ANLW_IAG_ADDRESSc) Wenn der VPN-Tunnel zur TI aufgebaut und der VPN-Tunnel zum SIS nicht aufgebaut sind: i. Ziel: Default Route Next Hop: ANLW_IAG_ADDRESS ii. Ziel: TI (NET_TI_OFFENE_FD,

	<p>NET_TI_GESICHERTE_FD und NET_TI_ZENTRAL) Next Hop: Innere Tunnel IP-Adresse des VPN-Konzentrators TI</p> <p>iii. Ziel: ANLW_AKTIVE_BESTANDSNETZE Next Hop: Innere Tunnel IP-Adresse des VPN-Konzentrators TI</p> <p>iv. Ziel: VPN-Konzentrator TI Next Hop: ANLW_IAG_ADDRESS</p> <p>d) Wenn die VPN-Tunnel zur TI und zum SIS aufgebaut sind:</p> <p>i. Ziel: Default Route Next Hop: Innere Tunnel IP-Adresse des VPN-Konzentrators SIS</p> <p>ii. Ziel: TI (NET_TI_OFFENE_FD, NET_TI_GESICHERTE_FD und NET_TI_ZENTRAL) Next Hop: Innere Tunnel IP-Adresse des VPN-Konzentrators TI</p> <p>iii. Ziel: ANLW_AKTIVE_BESTANDSNETZE Next Hop: Innere Tunnel IP-Adresse des VPN-Konzentrators TI</p> <p>iv. Ziel: VPN-Konzentrator TI Next Hop: ANLW_IAG_ADDRESS</p> <p>v. Ziel: VPN-Konzentrator SIS Next Hop: ANLW_IAG_ADDRESS</p> <p>Hinweis: Wenn der VPN-Tunnel zur TI nicht existiert, kann auch kein VPN-Tunnel zum SIS existieren, da die Default Route zum IAG zeigen muss, um einen VPN-Tunnel zur TI aufbauen zu können.</p> <p>2) Wenn (MGM_LU_ONLINE=Disabled)</p> <p>1. Der Konnektor MUSS die nachfolgenden Routen bereitstellen.</p> <p>i. Ziel: Lokale Netze der Einsatzumgebung gemäß ANLW_LEKTR_INTRANET_ROUTES Next Hop: gemäß ANLW_LEKTR_INTRANET_ROUTES</p> <p>3) Firewall aktualisieren: Die Firewall des Konnektors MUSS die neu eingerichteten Routen berücksichtigen und seine Regeln entsprechend aktualisieren und aktivieren. Tritt der Fehler 4164 auf, geht der Konnektor in den Betriebszustand EC_Firewall_Not_Reliable über.</p>
Varianten/Alternativen	Keine
Fehlerfälle	<p>(→ 1-2) Eine oder mehrere Variablen enthalten eine ungültige oder keine IP; 4167</p> <p>(→ 3) Beim Aktualisieren oder Aktivieren der Firewall-Regeln ist es zu einem Fehler gekommen; 4164</p>
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

5849 **Tabelle 313: TAB_KON_623 Fehlercodes TUC_KON_304 „Netzwerk-Routen einrichten“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4167	Technical	Fatal	CreateRoutes: Ein oder mehrere Adressen sind ungültig.
4164	Technical	Fatal	Beim Aktualisieren oder Aktivieren der Firewall-Regeln ist es zu einem Fehler gekommen.

5850

5851 [\leq]

5852 **4.2.1.4 Interne TUCs, auch durch Fachmodule nutzbar**

5853 Keine.

5854 **4.2.1.5 Operationen an der Außenschnittstelle**

5855 Keine

5856 **4.2.1.6 Betriebsaspekte**

5857 TIP1-A_5414 - Initialisierung „Anbindung LAN/WAN“

5858 Der Konnektor MUSS in der Bootup-Phase zur Initialisierung des Funktionsmerkmals
5859 „Anbindung LAN/WAN“:

- 5860 • den LAN-Adapter initialisieren (TUC_KON_305)
- 5861 • den WAN-Adapter initialisieren (TUC_KON_306)
- 5862 • die Infrastrukturdaten vom KSR einlesen (TUC_KON_283)

5863 [\leq]

5864 TIP1-A_4759 - Konfiguration LAN-Interface

5865 Der Konnektor MUSS gewährleisten, dass die Konfiguration nur dann gespeichert wird,
5866 wenn alle Parameter der nachfolgenden Tabellen den dazugehörigen Bedingungen
5867 entsprechen, sowie grundsätzlich zulässige Werte darstellen (gemäß RFCs).

5868 Wenn die Konfiguration per Managementschnittstelle geändert wurde, MUSS das
5869 folgende Systemereignis ausgelöst werden:

```
5870 TUC_KON_256 {
5871     topic = "ANLW/LAN/IP_CHANGED";
5872     eventType = Op;
5873     severity = Info;
5874     parameters = („IP=$dieNeueIP“);
5875     doDisp = false}
```

5876 Wenn (DHCP_CLIENT_LAN_STATE=Disabled) gesetzt ist, MUSS der Administrator des
5877 Konnektor die Werte der folgenden Tabelle über die Managementschnittstelle setzen
5878 können.

5879 Wenn (DHCP_CLIENT_LAN_STATE=Enabled) gesetzt ist, MUSS der Administrator des
5880 Konnektor die Werte der folgenden Tabelle angezeigt bekommen, kann diese jedoch
5881 nicht ändern.

5882

5883

5884 **Tabelle 314: TAB_KON_683 LAN-Adapter IP-Konfiguration**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
ANLW_LAN_IP_ADDRESS	IP-Adresse	Dies ist die IP-Adresse des LAN-Adapters. Nur wenn DHCP_CLIENT_LAN_STATE=Disabled MUSS der Administrator die LAN-seitige IP-Adresse des Konnektors setzen können. Diese IP-Adresse MUSS innerhalb des ANLW_LAN_NETWORK_SEGMENT liegen.
ANLW_LAN_SUBNETMASK	Subnetzmaske	Dies ist die zu ANLW_LAN_IP_ADDRESS gehörende Subnetzmaske. Der Administrator MUSS die Subnetzmaske setzen können. Der Konnektor MUSS gewährleisten das nur eine gültige Subnetzmaske gespeichert werden kann.
ANLW_LAN_NETWORK_SEGMENT	IP-Adresse / Subnetzmaske	ANLW_LAN_NETWORK_SEGMENT ist ein Zustandswert, der sich aus den Werten von ANLW_LAN_IP_ADDRESS und ANLW_LAN_SUBNETMASK ergibt. Der Wert bezeichnet ein lokales Netzwerk in der Umgebung des Anwenders an das der LAN-Adapter des Konnektors angeschlossen ist. Der Konnektor MUSS gewährleisten, das das Netzwerksegment NICHT mit einem der folgenden Netzwerksegmente überlappt: 1. NET_TI_DEZENTRAL 2. NET_TI_ZENTRAL 3. NET_TI_OFFENE_FD 4. NET_TI_GESICHERTE_FD 5. NET_SIS 6. ANLW_BESTANDSNETZE 7. ANLW_AKTIVE_BESTANDSNETZE 8. ANLW_WAN_NETWORK_SEGMENT 9. ANLW_LEKTR_INTRANET_ROUTES

5885 Der Administrator des Konnektor MUSS die Werte der folgenden Tabelle über die
5886 Managementschnittstelle setzen können.
5887

5888 **Tabelle 315: TAB_KON_684 LAN-Adapter Erweiterte Parameter**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
ANLW_LAN_MTU	Nummer	Der Administrator MUSS Maximum Transmission Unit (MTU) setzen können. Der Konnektor MUSS sicherstellen, das der konfigurierte Wert in den Grenzen von

		576 bis 9000 liegt. Default-Wert: 1400
ANLW_LAN_PARAMETER	Liste von IP, UDP und/oder TCP Parametern	Der Administrator SOLL weitere Konfigurationsparameter gemäß [gemSpec_Net#2.2.2.1,2.5] konfigurieren können.

5889
5890

[<=]

5891 TIP1-A_4760 - Konfiguration WAN-Interface
 5892 Der Konnektor MUSS gewährleisten, dass die Konfiguration nur dann gespeichert wird,
 5893 wenn alle Parameter der nachfolgenden Tabellen den dazugehörigen Bedingungen
 5894 entsprechen.
 5895 Wenn die Konfiguration per Managementschnittstelle geändert wurde, MUSS das
 5896 folgende Systemereignis ausgelöst werden:
 5897 TUC_KON_256 {
 5898 topic = "ANLW/WAN/IP_CHANGED";
 5899 eventType = Op;
 5900 severity = Info;
 5901 parameters = („IP=\$dieNeueIP“);
 5902 doDisp = false}
 5903 Wenn (DHCP_CLIENT_WAN_STATE=Disabled) gesetzt ist, MUSS der Administrator des
 5904 Konnektors die Werte der folgenden Tabelle über die Managementschnittstelle setzen
 5905 können.
 5906 Wenn (DHCP_CLIENT_WAN_STATE=Enabled) gesetzt ist, MUSS der Administrator des
 5907 Konnektors die Werte der folgenden Tabelle angezeigt bekommen, kann diese jedoch
 5908 nicht ändern.

5909

5910 **Tabelle 316: TAB_KON_685 WAN-Adapter IP-Konfiguration**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
ANLW_WAN_IP_ADDRESS	IP-Adresse	Dies ist die IP-Adresse des WAN-Adapters. Nur wenn DHCP_CLIENT_WAN_STATE=Disabled und ANLW_WAN_ADAPTER_MODUS=ENABLED MUSS der Administrator die WAN-seitige IP-Adresse des Konnektors setzen können. Diese IP-Adresse MUSS innerhalb des ANLW_WAN_NETWORK_SEGMENT liegen.
ANLW_WAN_SUBNETMASK	Subnetzmaske	Dies ist die zu ANLW_WAN_IP_ADDRESS gehörende Subnetzmaske. Der Administrator MUSS die Subnetzmaske setzen können. Der Konnektor MUSS gewährleisten, dass nur eine gültige Subnetzmaske gespeichert werden kann.

ANLW_WAN_NETWORK_SEGMENT	IP-Adresse / Subnetzmaske	<p>ANLW_WAN_NETWORK_SEGMENT ist ein Zustandswert, der sich aus den Werten von ANLW_WAN_IP_ADDRESS und ANLW_WAN_SUBNETMASK ergibt. Der Wert bezeichnet ein lokales Netzwerk in der Umgebung des Anwenders an das der WAN-Adapter des Konnektors angeschlossen ist. Der Konnektor MUSS gewährleisten, dass das Netzwerksegment nicht mit einem der folgenden Netzwerksegmente überlappt:</p> <ol style="list-style-type: none"> 1. NET_TI_DEZENTRAL 2. NET_TI_ZENTRAL 3. NET_TI_OFFENE_FD 4. NET_TI_GESICHERTE_FD 5. NET_SIS 6. ANLW_BESTANDSNETZE 7. ANLW_AKTIVE_BESTANDSNETZE 8. ANLW_LAN_NETWORK_SEGMENT 9. ANLW_LEKTR_INTRANET_ROUTES
--------------------------	---------------------------	--

5911 Der Administrator des Konnektor MUSS die Werte der folgenden Tabelle über die
 5912 Managementschnittstelle setzen können.
 5913

5914 **Tabelle 317: TAB_KON_686 WAN-Adapter Erweiterte Parameter**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
ANLW_WAN_MTU	Nummer	<p>Der Administrator MUSS Maximum Transmission Unit (MTU) setzen können.</p> <p>Der Konnektor MUSS sicherstellen, dass der konfigurierte Wert in den Grenzen von 576 bis 9000 liegt. Default-Wert: 1400</p>
ANLW_WAN_PARAMETER	Liste von IP, UDP und/oder TCP Parametern	<p>Der Administrator SOLL weitere Konfigurationsparameter gemäß [gemSpec_Net#2.2.2.1,2.5] konfigurieren können.</p>

5915
 5916 **[<=]**

5917 TIP1-A_4761 - Konfiguration Anbindung LAN/WAN
 5918 Die Managementschnittstelle MUSS es einem Administrator ermöglichen
 5919 Konfigurationsänderungen gemäß Tabelle TAB_KON_624 – „Konfigurationsparameter der
 5920 Anbindung LAN/WAN vorzunehmen.
 5921 Wenn (ANLW_INTRANET_ROUTES_MODUS = REDIRECT) gesetzt ist, MUSS der
 5922 Konnektor jedes Paket aus einem konfigurierten Intranet mit einem ICMP-Redirect mit
 5923 dem hinterlegten Next Hop beantworten und der Konnektor MUSS gewährleisten, dass
 5924 keine IP-Pakete in eines oder mehrere der konfigurierten Intranet geroutet werden.
 5925 Wenn (ANLW_INTRANET_ROUTES_MODUS = BLOCK) gesetzt ist, MUSS der Konnektor

5926 alle IP-Pakete für ein Intranet (gemäß ANLW_LEKTR_INTRANET_ROUTES) ablehnen.

5927

5928 **Tabelle 318: TAB_KON_624 – „Konfigurationsparameter der Anbindung LAN/WAN“**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
ANLW_ ANBINDUNGS_ MODUS	InReihe	Der Konnektor ist in Reihe zu dem IAG der Einsatzumgebung geschaltet. Wenn ANLW_WAN_ADAPTER_MODUS=ENABLED befindet sich der Konnektor in diesem Anbindungsmodus. Der Administrator MUSS diesen Wert einsehen und DARF ihn NICHT ändern können.
	Parallel	Der Konnektor ist parallel (zu allen bestehenden Systemen) ins Netzwerk der Einsatzumgebung angebunden. Wenn ANLW_WAN_ADAPTER_MODUS=DISABLED befindet sich der Konnektor in diesem Anbindungsmodus. Der Administrator MUSS diesen Wert einsehen und DARF ihn NICHT ändern können.
ANLW_ INTERNET_ MODUS	SIS	Der (am Konnektor LAN-seitig ankommende) Internet-Traffic wird per VPN an den SIS geschickt.
	IAG	Bei Anfragen ins Internet wird der Aufrufer per ICMP-Redirect (Type 5) auf die Route zum IAG verwiesen. Wenn (ANLW_ANBINDUNGS_MODUS = InReihe) DARF dieser Wert NICHT auswählbar sein - statt dessen MUSS dann der Wert SIS verwendet werden.
	KEINER	Es wird kein Traffic ins Internet geroutet
ANLW_ INTRANET_ ROUTES_ MODUS	REDIRECT	Der Konnektor MUSS sicherstellen, dass dieser Wert nur gesetzt werden kann, wenn der Administrator zuvor ein oder mehrere Intranet (ANLW_LEKTR_INTRANET_ROUTES) definiert hat.
	BLOCK	Der Konnektor MUSS alle IP-Pakete für ein Intranet (gemäß ANLW_LEKTR_INTRANET_ROUTES) ablehnen.

ANLW_WAN_ADAPTER_MODUS	ENABLED	Dieser Parameter ändert den Interface-Status des WAN-Adapters. Der Administrator MUSS diesen Wert einsehen können. Der Administrator MUSS diesen Wert ändern können.
	DISABLED	Dieser Parameter ändert den Interface-Status des WAN-Adapters. Der Administrator MUSS diesen Wert einsehen können. Der Administrator MUSS diesen Wert ändern können.
ANLW_LEKTR_INTRANET_ROUTES	Tupel aus Netzwerksegment und dazugehörigem Next-Hop	Der Administrator MUSS in diese Liste Einträge hinzufügen, editieren und löschen können. Liste von Routen zur Erreichung der Clientsysteme und Kartenterminals vom Konnektor; jeweils mit IP-Netzwerk dazugehörigem Next Hop. Die Netzwerksegmente DÜRFEN NICHT mit den Netzbereichen <ul style="list-style-type: none"> • NET_SIS • NET_TI_DEZENTRAL • NET_TI_ZENTRAL • NET_TI_OFFENE_FD • NET_TI_GESICHERTE_FD • ANLW_BESTANDSNETZE kollidieren.
ANLW_IAG_ADDRESS	IP Adresse	ANLW_IAG_ADDRESS ist die Adresse des Default Gateways. Diese IP-Adresse MUSS innerhalb des ANLW_WAN_NETWORK_SEGMENT liegen. Die Adresse wird entweder über DHCP automatisch (DHCP_CLIENT_WAN_STATE=ENABLED oder DHCP_CLIENT_LAN_STATE=ENABLED) oder anderenfalls manuell durch den Administrator konfiguriert. Bei automatischer Konfiguration per DHCP MUSS der Administrator den Wert von ANLW_IAG_ADDRESS ausschließlich einsehen können.

ANLW_ AKTIVE_ BESTANDS NETZE	Liste von IP- Address- Segmenten	Der Administrator MUSS manuell aus der empfangenen Liste der zur Verfügung stehenden angeschlossene Netze des Gesundheitswesens mit aAdG-NetG (gemäß TUC_KON_283 „Infrastruktur Konfiguration aktualisieren“) einzelne deaktivieren, bzw. nach vorheriger Deaktivierung, freischalten können. Nur die freigegeben Netze werden in dieser Variablen erfasst und sind aus den Netzwerken der Einsatzumgebung erreichbar. Wird eine Änderung an der Liste der freigegebenen Netze vorgenommen, so MUSS der Konnektor für jedes dieser freigegebenen Netz in DNS_SERVERS_BESTANDSNETZE ein DNS-Referer-Eintrag für jede der dazugehörigen Domains mit allen zugehörigen DNS-Servern im Konnektor hinterlegen. Die Werte hierzu werden der via TUC_KON_283 aktualisierten Bestandsnetze.xml entnommen. Für hier „nicht freigegebene“ oder zwischenzeitlich gelöschte Netze DARF der Konnektor NICHT Referer-Einträge in DNS_SERVERS_BESTANDSNETZE enthalten. Die Einträge in DHCP_AKTIVE_BESTANDSNETZE_ROUTES sind entsprechend zu aktualisieren. Der Konnektor MUSS nach jeder Änderung dieser Variablen durch den Administrator den TUC_KON_304 „Netzwerk-Routen einrichten“ aufrufen.
ANLW_ IA_ BESTANDSNETZE	AN	Der Konnektor MUSS alle über TUC_KON_283 übermittelten angeschlossenen Netze des Gesundheitswesens mit aAdG-NetG aktivieren. Eine spätere manuelle Deaktivierung über das Management-Interface durch den Administrator ist möglich. Dieses Verhalten ist als Standardverhalten zu konfigurieren.
	AUS	Der Konnektor MUSS alle über TUC_KON_283 übermittelten angeschlossenen Netze des Gesundheitswesens mit aAdG-NetG anbieten, diese aber nicht aktivieren. Eine spätere manuelle Aktivierung erfolgt über das Management-Interface durch den Administrator.

5929
5930
5931

[<=]

5932 TIP1-A_5537 - Anzeige IP-Routinginformationen
5933 Der Konnektor MUSS über die Managementschnittstelle die konfigurierten IP-Routen und
5934 die aktuelle IP-Routingtabelle mit mindestens folgenden Informationen anzeigen:

- 5935 • Forwarding Status
- 5936 • Zieladresse/Prefix
- 5937 • Gateway (Next-Hop)
- 5938 • Routing Typ
- 5939 • Routing Protocol
- 5940 • Routing Preference.

5941 [\leq]

5942 TIP1-A_4762 - Konfigurationsparameter Firewall-Schnittstelle

5943 Im Anschluss an eine Anpassung der ANLW_FW_SIS_ADMIN_RULES MUSS der
5944 Konnektor die Firewall neu erstellen und laden.

5945

5946 **Tabelle 319: TAB_KON_625 - Konfigurationsparameter Firewall-Schnittstelle**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
ANLW_FW_SIS_ADMIN_RULES	Firewall Regelset	Der Administrator MUSS Firewall-Regeln (für den einschränkenden Zugriff auf die SIS), auf Grundlage der Parameter Absender-IP-Adresse, Empfänger-IP-Adresse, Protokoll (ggf. mit Absender-Port und Empfänger-Port) und Verbindungsrichtung, einfügen, editieren und löschen können.

5947

5948 [\leq]

5949 **4.2.2 DHCP-Server**

5950 Innerhalb des Kapitels DHCP-Servers werden folgende Präfixe für Bezeichner verwendet:

- 5951 • Events (Topic Ebene 1): „DHCP“
- 5952 • Konfigurationsparameter: „DHCP_SERVER_“

5953 **4.2.2.1 Funktionsmerkmalweite Aspekte**

5954 TIP1-A_4763 - DHCP-Server des Konnektors

5955 Der Konnektor MUSS an seiner LAN-Schnittstelle einen DHCP-Server gemäß [RFC2131]
5956 und [RFC2132] anbieten.

5957 [\leq]

5958 **4.2.2.2 Durch Ereignisse ausgelöste Reaktionen**

5959 Keine.

5960 **4.2.2.3 Interne TUCs, nicht durch Fachmodule nutzbar**

5961 Keine.

5962 **4.2.2.4 Interne TUCs, auch durch Fachmodule nutzbar**

5963 Keine.

5964 **4.2.2.5 Operationen an der Außenschnittstelle**

5965 *4.2.2.5.1 Liefere Netzwerkinformationen über DHCP*

5966 TIP1-A_4765 - Liefere Netzwerkinformationen über DHCP

5967 Der DHCP-Server des Konnektors MUSS an der Client-Schnittstelle eine Operation zur
5968 Lieferung von Netzwerkinformationen über DHCP anbieten.

5969

5970 **Tabelle 320: TAB_KON_626 „Liefere Netzwerkinformationen über DHCP“**

Name	Liefere Netzwerkinformationen über DHCP
Beschreibung	Der Konnektor MUSS anfragenden Clients per DHCP die konfigurierten Netzerkinformationen liefern (siehe Tabelle TAB_KON_628 und Tabelle TAB_KON_629).
Aufrufparameter	gemäß [RFC2131], [RFC2132]
Rückgabe	gemäß [RFC2131], [RFC2132]
Standardablauf	<p>Die an den aufrufenden Client zu übergebenden Parameter ergeben sich aus Tabelle TAB_KON_628 und Tabelle TAB_KON_629:</p> <p>Falls DHCP_SERVER_STATE = Enabled:</p> <ul style="list-style-type: none"> Anhand der MAC-Adresse des anfragenden Client wird die Clientgruppe aus DHCP_SERVER_CLIENTGROUPS bzw. DHCP_SERVER_DEFAULT_CLIENTGROUP ausgewählt. DHCP_OWNDNS_ENABLED <ul style="list-style-type: none"> Enabled: DNS-Server = <konnektoreigene Adresse> Disabled: DNS-Server = DHCP_DNS_ADDR DHCP_NTP <ul style="list-style-type: none"> Enabled: NTP-Server = <konnektoreigene Adresse> Disabled: Keine Wertübermittlung DHCP_OWNDGW_ENABLED <ul style="list-style-type: none"> Enabled: DGW = <konnektoreigene Adresse> Disabled: DGW = DHCP_DGW_ADDR Falls Client-MAC-Adresse in DHCP_STATIC_LEASE <ul style="list-style-type: none"> IP_Address = die in der Static Lease konfigurierte Adresse. Falls Client IP-Adresse = 0.0.0.0 oder innerhalb DHCP_SERVER_DYNAMIC_RANGE <ul style="list-style-type: none"> IP_Address = IP_Address aus DHCP_SERVER_DYNAMIC_RANGE

	<ul style="list-style-type: none"> • Sonst: keine Zuweisung (Empfehlung: DHCPNAK an den Client) • Netzmaske = DHCP_IP_NETMASK • Domainname = DHCP_DOMAINNAME • Hostname = DHCP_HOSTNAME • Lease Dauer = DHCP_LEASE_TTL • Routen bestehend aus <ul style="list-style-type: none"> • DHCP_AKTIVE_BESTANDSNETZE_ROUTES • DHCP_INTRANET_ROUTES • DHCP_ROUTES • Weitere DHCP-Optionen = DHCP_OPTIONS • MTU = ANLW_LAN_MTU
Fehlercodes	Vgl. [RFC2131], [RFC2132]
Vorbedingungen	Der DHCP-Server des Konnektors MUSS aktiviert und konfiguriert sein.
Nachbedingungen	Der DHCP-Server MUSS die DHCP-Antwort geliefert haben. Die Statusinformationen (z.B. Client Lease) müssen gemäß [RFC2131] gespeichert werden.
Hinweise	Keine

5971
5972 [\leq]

5973 4.2.2.6 Betriebsaspekte

5974 TIP1-A_4766 - Deaktivierbarkeit des DHCP-Servers
5975 Der DHCP- Server des Konnektors MUSS durch den Administrator über die
5976 Managementschnittstelle aktivierbar und deaktivierbar sein (gemäß TAB_KON_627). Der
5977 DHCP-Server MUSS bei der Auslieferung deaktiviert sein.
5978 Bei der Aktivierung MUSS der Konnektor den TUC_KON_343 "Initialisierung DHCP-
5979 Server" durchlaufen.
5980 Sobald DHCP_SERVER_STATE geändert wurde, muss
5981 TUC_KON_256{"DHCP/SERVER/STATECHANGED"; Op; Info;
5982 "STATE=\$DHCP_SERVER_STATE "} aufgerufen werden.
5983

5984 **Tabelle 321: TAB_KON_627 „Aktivierung des DHCP-Servers“**

Referenz ID	Belegung	Bedeutung
DHCP_SERVER_STATE	Enabled / Disabled	Der DHCP-Server MUSS durch den Administrator aktivierbar und deaktivierbar sein.

5985
5986 [\leq]

5987 TIP1-A_4767 - Konfiguration des DHCP-Servers

5988 Der Konnektor MUSS die Möglichkeit bieten die in Tabelle TAB_KON_628 und Tabelle
 5989 TAB_KON_629 beschriebenen Parameter des DHCP-Servers über die
 5990 Managementschnittstelle zu konfigurieren.
 5991

5992 **Tabelle 322: TAB_KON_628 „Basiskonfiguration des DHCP-Servers“**

Referenz ID	Belegung	Bedeutung
DHCP_SERVER_NETWORK	IP-Adresse	IP-Netzwerk der Einsatzumgebung.
DHCP_SERVER_BROADCAST	IP-Adresse	Die Broadcast-Adresse des Konnektors am LAN-Interface
DHCP_SERVER_DYNAMIC_RANGE	von – bis IP-Adresse	Adressbereich für Adressen die dynamisch vergeben werden dürfen.
DHCP_SERVER_CLIENTGROUPS	Name der Clientgruppe; Liste an MAC-Adressen	Der Konnektor MUSS dem Administrator über die Managementschnittstelle die Möglichkeit bieten mindestens zwei Client-Gruppen zu verwalten.
DHCP_SERVER_DEFAULT_CLIENTGROUP	Client-Gruppe	Standardmäßig eingestellte Client-Gruppe. Wird verwendet falls DHCP-Anfrage keiner anderen Client-Gruppe zugeordnet werden kann.

5993 **Tabelle 323: TAB_KON_629 „Client-Gruppenspezifische Konfigurationsoptionen des**
 5994 **Konnektor-DHCP-Servers“**

ReferenzID	Belegung	Bedeutung
Die gesamte Parameterliste ist für jede Client-Gruppe getrennt konfigurierbar		
DHCP_OWNDNS_ENABLED	Enabled/Disabled	Der Administrator MUSS konfigurieren können, ob der konnektoreigene DNS-Server als Parameter übergeben wird. Default-Wert: Disabled
DHCP_DNS_ADDR	IP-Adressen der DNS-Server	Falls der konnektoreigene DNS-Server nicht übergeben werden soll, müssen die Adressen externer aus dem Netz der Einsatzumgebung erreichbaren DNS-Server als Parameter übergeben werden. Der Administrator MUSS diese Adressen konfigurieren können.
DHCP_NTP	Enabled/Disabled	Der Administrator MUSS konfigurieren können, ob der Konnektor die Adresse des Konnektor internen NTP-Servers

		per DHCP an die Clients sendet. Default-Wert: Enabled
DHCP_ OWNDBGW_ ENABLED	Enabled/Disabled	Der Administrator MUSS konfigurieren können, ob der Konnektor beim Client als Default-Gateway gesetzt werden soll. Default-Wert: Disabled
DHCP_DGW_ ADDR	IP-Adresse des DGW	Falls der Konnektor nicht als Default Gateway gesetzt werden soll, muss die Adresse des zu verwendenden DGW als Parameter übergeben werden. Der Administrator MUSS die Adresse des DGW konfigurieren können.
DHCP_IP_ NETMASK	Netzmaske	Der Administrator MUSS die Netmask des Clients konfigurieren können.
DHCP_ DOMAINNAME	Domainname	Der Administrator MUSS den Domainnamen des Clients konfigurieren können.
DHCP_ HOSTNAME	Liste von Tupel aus Hostname und Mac-Adresse	Der Administrator MUSS eine Liste von Hostname der Clients konfigurieren können (Einträge einfügen, ändern, löschen).
DHCP_ STATIC_LEASE	Liste von Tupel aus IP- und Mac-Adresse	Der Administrator MUSS für jede MAC-Adresse Static Lease konfigurieren können.
DHCP_ LEASE_TTL	X Minuten	Der Administrator MUSS Lease-Dauer der dynamischen Adressen konfigurieren können.
DHCP_ AKTIVE_ BESTANDS NETZE_ ROUTES	Liste von Tupel: Netzwerksegment je INTRANET und Adresse für Next Hop je freigegebenem angeschlossenen Netze des Gesundheitswesens mit aAdG-NetG	Der Administrator MUSS je freigegebenem angeschlossenen Netze des Gesundheitswesens mit aAdG-NetG (aus ANLW_AKTIVE_BESTANDSNETZE) den an den Client zu übermittelnden Routen-Eintrag aktivieren oder deaktivieren können.

DHCP_ INTRANET_ ROUTES	Liste von Tupel: Netzwerksegment je INTRANET und Adresse für Next Hop in die definierten Intranets	Der Administrator MUSS je Intranet-Tupel (aus ANLW_LEKTR_INTRANET_ROUTES) den an den Client zu übermittelnden Routen-Eintrag aktivieren oder deaktivieren können.
DHCP_ ROUTES	Tupel Netzwerksegment und Adresse für Next Hop	Der Administrator MUSS Routen zur Verteilung an die Clients frei konfigurieren können. Der Konnektor MUSS sicherstellen, diese Listeneinträge keine Überschneidungen mit folgenden Netzsegmenten haben: - dem Netzwerksegment ANLW_LAN_NETWORK_SEGMENT - dem Netzwerksegment ANLW_WAN_NETWORK_SEGMENT - jedes Netzsegmente in ANLW_BESTANDSNETZE ANLW_AKTIVE_BESTANDSNETZE ANLW_LEKTR_INTRANET_ROUTES Die Routen SOLLEN über DHCP Option 121 (Windows Vista oder höher) bzw. DHCP Option 249 (Windows XP und darunter) verteilt werden.
DHCP_ OPTIONS	Liste an weiteren DHCP-Optionen.	Vom Administrator konfigurierbare Liste an weiteren DHCP-Options gemäß [RFC2132]. Die Umsetzung dieser Konfigurationsmöglichkeit KANN entfallen.

5995

5996 [\leq]

5997 4.2.2.6.1 TUC_KON_343 „Initialisierung DHCP-Server“

5998 TIP1-A_4768 - TUC_KON_343 „Initialisierung DHCP-Server“

5999 Der Konnektor MUSS in der Bootup-Phase TUC_KON_343 "Initialisierung DHCP-Server"

6000 durchlaufen.

6001

6002 **Tabelle 324: TAB_KON_630 - TUC_KON_343 „Initialisierung DHCP-Server“**

Element	Beschreibung
Name	TUC_KON_343 "Initialisierung DHCP-Server"

Beschreibung	Falls DHCP-Server Konfiguration aktiv ist, muss der Konnektor in der Bootup-Phase oder bei einer Aktivierung des Servers den DHCP-Server starten.
Anwendungsumfeld	Bereitstellen der Netzwerkkonfiguration für den Betrieb
Eingangsanforderung	Keine
Auslöser und Vorbedingungen	Bootup oder Ereignis DHCP/SERVER/STATECHANGED
Eingangsdaten	Keine
Komponenten	Konnektor
Ausgangsdaten	Keine
Standardablauf	Falls DHCP_SERVER_STATE = enabled - den DHCP-Server starten Falls DHCP_SERVER_STATE = disabled - den DHCP-Server stoppen
Varianten/Alternativen	Keine
Fehlerfälle	4168: DHCP-Server konnte nicht gestartet werden
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

6003 **Tabelle 325: TAB_KON_631 Fehlercodes TUC_KON_343 „Initialisierung DHCP-Server“**

Fehlercode	ErrorType	Severity	Fehlertext
4168	Technical	Error	Der DHCP-Server des Konnektors konnte nicht gestartet werden.

6004
6005 [\leq]

6006 4.2.3 DHCP-Client

6007 Innerhalb des Kapitels DHCP-Client werden folgende Präfixe für Bezeichner verwendet:

- 6008 • Events (Topic Ebene 1): „DHCP“
- 6009 • Konfigurationsparameter: „DHCP_CLIENT_“

6010 4.2.3.1 Funktionsmerkmalweite Aspekte

6011 TIP1-A_4769 - DHCP Client Funktionalität des Konnektors

6012 Der Konnektor MUSS an seiner LAN- und WAN-Schnittstelle die Möglichkeit bieten jeweils
6013 DHCP zu nutzen.

6014 Der DHCP-Client des Konnektors MUSS die empfangenen Parameter wie folgt verwenden:

- 6015 • Die IP-Adresse und Subnetzmaske müssen dem Interface zugewiesen und in den
6016 Variablen ANLW_LAN_IP_ADDRESS bzw. ANLW_WAN_IP_ADDRESS und
6017 ANLW_LAN_SUBNETMASK gespeichert werden.

- 6018 • Der für das Interface, auf Anfrage, gelieferte Wert der MTU Size KANN
- 6019 übernommen werden.
- 6020 • Das Default Gateway (DGW) muss in der Variable ANLW_IAG_ADDRESS
- 6021 gespeichert werden.
- 6022 • DNS-Server muss in der Variable DNS_SERVERS_INT gespeichert werden.
- 6023 Weitere DHCP-Parameter DÜRFEN nicht übernommen werden.
- 6024 [\leq]

6025 4.2.3.2 Durch Ereignisse ausgelöste Reaktionen

- 6026 TIP1-A_4771 - Reagieren auf DHCP/LAN_CLIENT/ STATECHANGED- und
- 6027 DHCP/WAN_CLIENT/ STATECHANGED-Ereignisse
- 6028 Wenn das Ereignis DHCP/LAN_CLIENT/STATECHANGED oder
- 6029 DHCP/WAN_CLIENT/STATECHANGED empfangen wird, MUSS TUC_KON_341 „DHCP-
- 6030 Informationen beziehen“ aufgerufen werden.
- 6031 [\leq]

6032 4.2.3.3 Interne TUCs, nicht durch Fachmodule nutzbar

6033 4.2.3.3.1 TUC_KON_341 „DHCP-Informationen beziehen“

- 6034 TIP1-A_4772 - TUC_KON_341 „DHCP-Informationen beziehen“
- 6035 Der Konnektor MUSS den technischen Use Case TUC_KON_341 „DHCP-Informationen
- 6036 beziehen“ umsetzen.
- 6037

6038 **Tabelle 326: TAB_KON_632 – TUC_KON_341 „DHCP Informationen beziehen“**

Element	Beschreibung
Name	TUC_KON_341 DHCP-Informationen beziehen
Beschreibung	Der Konnektor muss seine WAN- und/oder LAN-Schnittstelle individuell über einen DHCP-Server aus dem Netz der Einsatzumgebung beziehen können.
Anwendungsumfeld	Netzwerkconfiguration für den Betrieb des Konnektors
Eingangsanforderung	Der Konnektor muss zur Netzwerk-Interface-Konfiguration DHCP nutzen sofern keine statischen Informationen vorhanden sind.
Auslöser	Bootup, Ablauf einer DHCP-Lease, manuell angestoßenes DHCP-Renew, Aktivierung der DHCP-Client-Funktionalität.
Vorbedingung	aktivierte DHCP-Client Funktion über die Variablen DHCP_CLIENT_LAN_STATE bzw. DHCP_CLIENT_WAN_STATE
Eingangsdaten	Netzwerk-Adapter (LAN oder WAN) für den DHCP-Informationen bezogen werden sollen
Komponenten	Konnektor
Ausgangsdaten	DHCP-Informationen vom DHCP-Server der Einsatzumgebung

Standardablauf	<ul style="list-style-type: none"> Ermitteln von DHCP-Informationen (DHCPDISCOVER und DHCPREQUEST) gemäß [RFC2131], [RFC2132] Übernahme der ermittelten Werte, ausschließlich für die in Tabelle TAB_KON_683 LAN-Adapter IP-Konfiguration bzw. Tabelle TAB_KON_685 WAN-Adapter IP-Konfiguration aufgeführten Variablen Wenn DHCP Client LAN-Adapter, nur bei IP-Adressen-Wechsel: Erzeugen eines Events durch den Aufruf von TUC_KON_256{"DHCP/LAN_CLIENT/RENEW"; Op; Info; "IP_ADDRESS=\$Belegung"} Wenn DHCP Client WAN-Adapter, nur bei IP-Adressen-Wechsel: Erzeugen eines Events durch den Aufruf von TUC_KON_256{"DHCP/WAN_CLIENT/RENEW"; Op; Info; "IP_ADDRESS=\$Belegung"}
Varianten/Alternativen	Keine
Fehlerfälle	4169: Konnektor erhält keine DHCP-Informationen 4170: Konnektor besitzt identische IP-Adressen am WAN- und LAN-Interface
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 327: TAB_KON_633 Fehlercodes TUC_KON_341 „DHCP-Informationen beziehen“

Fehlercode	ErrorType	Severity	Fehlertext
4169	Technical	Error	Konnektor erhält keine DHCP-Informationen.
4170	Technical	Error	Konnektor besitzt identische IP-Adressen am WAN und LAN

[<=]

4.2.3.4 Interne TUCs, auch durch Fachmodule nutzbar

Keine.

4.2.3.5 Operationen an der Außenschnittstelle

Keine.

4.2.3.6 Betriebsaspekte

TIP1-A_4773 - Konfiguration des DHCP-Clients

Die DHCP-Client Funktionalität MUSS für LAN- und WAN-Interface vom Administrator getrennt aktivierbar und deaktivierbar sein (gemäß TAB_KON_634). Falls der DHCP-Client nicht verwendet wird MUSS sichergestellt werden, dass eine statische

Konfiguration, für den LAN-Adapter gemäß Tabelle TAB_KON_683 LAN-Adapter IP-Konfiguration bzw. für den WAN-Adapter gemäß Tabelle TAB_KON_685 WAN-Adapter IP-Konfiguration, existiert bevor die Netzwerkeinstellungen übernommen werden. Sobald Parameter geändert wurden, MUSS TUC_KON_256 „Systemereignis absetzen“ je nachdem auf welchem Interface der Client aktiviert oder deaktiviert wurde mit folgenden Parameter aufgerufen werden:

TUC_KON_256{"DHCP/LAN_CLIENT/STATECHANGED"; Op; Info;
"STATE=\$DHCP_CLIENT_LAN_STATE"; doDisp = false}
oder
TUC_KON_256{"DHCP/WAN_CLIENT/STATECHANGED "; Op; Info;
"STATE=\$DHCP_CLIENT_WAN_STATE "; doDisp = false}

Tabelle 328: TAB_KON_634 „Konfiguration des DHCP-Clients“

ReferenzID	Belegung	Bedeutung
DHCP_CLIENT_LAN_STATE	Enabled/Disabled	Der Administrator muss den DHCP-Client an der LAN-Schnittstelle aktivieren oder deaktivieren können.
DHCP_CLIENT_WAN_STATE	Enabled/Disabled	Der Administrator muss den DHCP-Client an der WAN-Schnittstelle aktivieren oder deaktivieren können.

[<=]

TIP1-A_4774 - Manuelles anstoßen eines DHCP-Lease-Renew
Der Administrator MUSS die Möglichkeit haben die DHCP-Lease des Konnektors für jedes Interface getrennt zu erneuern.

[<=]

TIP1-A_4776 - Setzen der IP-Adresse nach Timeout
Falls der DHCP-Client auf der LAN-Seite nach einem Timeout von 30s keine IP-Adresse bezogen hat, MUSS gemäß [RFC3927] eine Default-Adresse aus 169.254/16 vergeben werden.

[<=]

4.2.4 VPN-Client

Der VPN-Client beschreibt die Absicherung der Anbindung des Konnektors an die TI und die Bestandsnetze. Während der technische Kern dieser Funktion, der Aufbau der VPN-Kanäle zu den Konzentratoren, in [gemSpec_VPN_ZugD#TUC_VPN-ZD_0001] und [gemSpec_VPN_ZugD#TUC_VPN-ZD_0002] beschrieben wird, regelt dieses Kapitel die Interaktion, sowie die Konfiguration des VPN-Clients innerhalb des Konnektors.

Innerhalb des Kapitels VPN-Client werden folgende Präfixe für Bezeichner verwendet:

- Events (Topic Ebene 1): „NETWORK“
- Konfigurationsparameter: „VPN_“

4.2.4.1 Funktionsmerkmalweite Aspekte

TIP1-A_4778 - Anforderungen an den VPN-Client

6089 Der Konnektor MUSS sich im Rahmen des IPsec-Verbindungsaufbaus gegenüber den
 6090 VPN-Konzentratoren mit seiner Identität ID.NK.VPN ausweisen.
 6091 Der VPN-Client im Konnektor MUSS das folgende Event generieren, sobald der VPN-
 6092 Tunnel zur TI nicht mehr zur Verfügung steht:
 6093 Rufe TUC_KON_256 {"NETWORK/VPN_TI/DOWN"; Op; Warning;}
 6094 Der VPN-Client im Konnektor MUSS das folgende Event generieren, sobald der VPN-
 6095 Tunnel zum SIS nicht mehr zur Verfügung steht:
 6096 Rufe TUC_KON_256 {"NETWORKVPN_SIS/DOWN"; Op; Warning;}
 6097 Der Hersteller des Konnektor MUSS sicherstellen, dass eine Anbindung an einen
 6098 Konzentrador ausschließlich dann möglich ist, wenn (MGM_LU_ONLINE = Enabled)
 6099 gesetzt ist.
 6100 Der Administrator des Konnektor MUSS durch die Managementschnittstelle manuell einen
 6101 Verbindungsaufbau und einen Verbindungsabbau eines VPN-Tunnel zur TI (VPN_TI) oder
 6102 zu den SIS (VPN_SIS) initiieren können.
 6103 [\leq]

6104 TIP1-A_4779 - Wiederholte Fehler beim VPN-Verbindungsaufbau
 6105 Der Konnektor MUSS gewährleisten, dass nach einem Fehler beim VPN-
 6106 Verbindungsaufbau nicht unmittelbar ein weiterer Versuch des Verbindungsaufbaus
 6107 durchgeführt wird.
 6108 Hierzu MUSS der Hersteller ein inkrementelles (schrittweise anwachsend) Verfahren
 6109 wählen, welcher den zeitlichen Abstand zwischen einzelnen Versuchen des VPN-
 6110 Verbindungsaufbau definiert. Dieser Abstand MUSS maximal fünf Minuten betragen.
 6111 (Diese Pause soll es dem Konnektor ermöglichen, noch ausreichend Ressourcen für die
 6112 verbleibenden Services zur Verfügung zu stellen).
 6113 [\leq]

6114 4.2.4.2 Durch Ereignisse ausgelöste Reaktionen

6115 TIP1-A_4780 - TI VPN-Client Start Events
 6116 Beim Auftreten einer der nachfolgenden Events MUSS der Konnektor den TUC_KON_321
 6117 „Verbindung zu dem VPN-Konzentrator der TI aufbauen“ starten, sofern auch
 6118 MGM_LU_ONLINE = Enabled.

- 6119 • Event NETWORKVPN_TI/DOWN
- 6120 • Event MGM/LU_CHANGED/LU_ONLINE

6121 [\leq]

6122 TIP1-A_4781 - SIS VPN-Client Start Events
 6123 Beim Auftreten einer der nachfolgenden Events MUSS der Konnektor den TUC_KON_322
 6124 „Verbindung zu dem VPN-Konzentrator des SIS aufbauen“ starten, sofern
 6125 ANLW_INTERNET_MODUS = SIS, MGM_LU_ONLINE = Enabled und die Verbindung VPN-
 6126 Konzentrador TI aufgebaut ist:

- 6127 • Event NETWORKVPN_SIS/DOWN

6128 [\leq]

6129 TIP1-A_5417 - TI VPN-Client Stop Events
 6130 Beim Auftreten einer der nachfolgenden Events MUSS der Konnektor den VPN-Tunnel zur
 6131 TI beenden:

- 6132 • MGM/LU_CHANGED/LU_ONLINE mit (Active=Disabled)

6133 [\leq]

6134 TIP1-A_4782 - SIS VPN-Client Stop Events

6135 Beim Auftreten einer der nachfolgenden Events MUSS der Konnektor den VPN-Tunnel
6136 zum SIS beenden:

- 6137 • MGM/LU_CHANGED/LU_ONLINE mit (Active=Disabled)

6138 [\leq]

6139 Hinweis: Wenn der IPsec-Tunnel VPN_SIS aufgebaut ist, zeigt die Default Route im
6140 Konnektor auf die innere Tunnel-IP-Adresse des VPN-Konzentrators SIS. Dies ist bei
6141 einer Trennung und dem Wiederaufbau der Verbindung VPN_TI zu beachten.

6142 4.2.4.3 Interne TUCs, nicht durch Fachmodule nutzbar

6143 4.2.4.3.1 TUC_KON_321 „Verbindung zu dem VPN-Konzentrator der TI aufbauen“

6144 TIP1-A_4783 - TUC_KON_321 „Verbindung zu dem VPN-Konzentrator der TI aufbauen“
6145 Der Konnektor MUSS den technischen Use Case TUC_KON_321 „Verbindung zu dem
6146 VPN-Konzentrator der TI aufbauen“ umsetzen.
6147

6148 **Tabelle 329: TAB_KON_635 – TUC_KON_321 „Verbindung zu dem VPN-Konzentrator der**
6149 **TI aufbauen“**

Element	Beschreibung
Name	TUC_KON_321 Verbindung zu dem VPN-Konzentrator der TI aufbauen
Beschreibung	Es wird ein IPsec-Tunnel zum VPN-Konzentrator der TI aufgebaut werden. Über den erfolgreichen Aufbau wird per Event informiert.
Auslöser	Bootup-Phase TUC_KON_305 „LAN-Adapter initialisieren“ TUC_KON_306 „WAN-Adapter initialisieren“ Event MGM/LU_CHANGED/LU_ONLINE Event NETWORK/VPN/CONFIG_CHANGED Optional: Änderungen ANLW_AKTIVE_BESTANDSNETZE Manueller Aufruf über Managementschnittstelle
Vorbedingungen	Der TUC_KON_304 „Netzwerk-Routen einrichten“ MUSS fehlerfrei durchgelaufen sein.
Eingangsdaten	
Komponenten	Konnektor
Ausgangsdaten	Der virtuelle Adapter VPN_TI mit der IP-Adresse VPN_TUNNEL_TI_INNER_IP des Konnektors wurde zur Verfügung gestellt.

	<ul style="list-style-type: none"> • Innere Tunnel IP-Adresse des VPN-Konzentrators TI • DNS_SERVERS_TI • VPN_KONZENTRATOR_TI_IP_ADDRESS • DOMAIN_SRVZONE_TI
Standardablauf	<p>1) Wenn der Auslöser = Event NETWORK/VPN/CONFIG_CHANGED oder eine Änderung von ANLW_AKTIVE_BESTANDSNETZE ist, muss der VPN-Tunnel TI abgebaut werden.</p> <p>2) Wenn der VPN-Tunnel TI noch aktiv ist, ist der Ablauf abgeschlossen. Anderenfalls ist mit Ablaufschritt 3) fortzufahren.</p> <p>3) Prüfen, MGM_LU_ONLINE = Enabled, falls nicht ist der TUC ohne Ausgabe einer Fehlermeldung zu beenden.</p> <p>4) Prüfen, ob die im Konnektor hinterlegte CRL noch gültig ist. falls nicht, muss der TUC_KON_040 „CRL aktualisieren“ aufgerufen werden, Anschließend erneut prüfen, ob die im Konnektor hinterlegte CRL nun gültig ist. Falls die CRL nicht gültig ist, ist der TUC mit Fehler zu beenden.</p> <p>5) Aufrufen von TUC_VPN-ZD_0001 „IPsec Tunnel TI aufbauen“ Die folgenden Rückgabewerte des TUC_VPN-ZD_0001 „IPsec Tunnel TI aufbauen“ sind in die laufende Konfiguration des Konnektors zu übernehmen:</p> <ul style="list-style-type: none"> • VPN_TUNNEL_TI_INNER_IP • DNS_SERVERS_TI <p>6) Aufrufen von TUC_KON_304 „Netzwerk-Routen einrichten“ Sobald der Tunnel erfolgreich aufgebaut wurde, ist der folgende Event zu generieren: TUC_KON_256 {"NETWORK/VPN_TI/UP"; Op; Info;IP= \$VPN_TUNNEL_TI_INNER_IP}</p>
Varianten/Alternativen	Keine
Fehlerfälle	<p>(→4) CRL ist abgelaufen (outdated); Herstellerspezifisch kann entweder (4a) oder (4b) umgesetzt werden:</p> <p>(4a) Kritischer Fehlerzustand EC_CRL_Out_Of_Date wurde noch nicht festgestellt: 4173</p> <p>(4b) kritischer Fehlerzustand EC_CRL_Out_Of_Date wurde bereits festgestellt: 4002</p> <p>(->4) Wenn Fehler 4173 bzw. 4002 nicht zutreffen, ist ein herstellerspezifischer Fehler zu verwenden.</p>

	(→5) VPN-Tunnel konnte nicht aufgebaut werden; Fehlercode: 4174
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 330: TAB_KON_636 Fehlercodes TUC_KON_321 „Verbindung zu dem VPN-Konzentrator der TI aufbauen“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4002	Security	Fatal	Der Konnektor befindet sich in einem kritischen Betriebszustand
4172	Technical	Fatal	Es ist keine Online-Verbindung zulässig.
4173	Technical	Fatal	Die CRL ist nicht mehr gültig (outdated).
4174	Technical	Fatal	TI-VPN-Tunnel: Verbindung konnte nicht aufgebaut werden

[<=]

4.2.4.3.2 TUC_KON_322 „Verbindung zu dem VPN-Konzentrator des SIS aufbauen“

TIP1-A_4784 - TUC_KON_322 „Verbindung zu dem VPN-Konzentrator des SIS aufbauen“
Der Konnektor MUSS den technischen Use Case TUC_KON_322 „Verbindung zu dem VPN-Konzentrator der SIS aufbauen“ umsetzen.

Tabelle 331: TAB_KON_637 – TUC_KON_322 „Verbindung zu dem VPN-Konzentrator der SIS aufbauen“

Element	Beschreibung
Name	TUC_KON_322 Verbindung zu dem VPN-Konzentrator der SIS aufbauen
Beschreibung	Es muss ein IPsec-Tunnel zum VPN-Konzentrator der SIS aufgebaut werden

Auslöser	Bootup-Phase TUC_KON_305 „LAN-Adapter initialisieren TUC_KON_306 „WAN-Adapter initialisieren Event NETWORK/VPN/CONFIG_CHANGED Optional: Event MGM/LU_CHANGED/LU_ONLINE Manueller Aufruf über Managementschnittstelle
Vorbedingungen	ANLW_INTERNET_MODUS = SIS Die Verbindung VPN-Konzentrator TI ist aufgebaut. Der TUC_KON_304 „Netzwerk-Routen einrichten“ muss erfolgreich durchgeführt worden sein.
Eingangsdaten	Keine
Komponenten	Konnektor
Ausgangsdaten	Der virtuelle Adapter VPN_SIS mit der IP-Adresse VPN_TUNNEL_SIS_INNER_IP wurde zur Verfügung gestellt. <ul style="list-style-type: none"> • Innere Tunnel-IP-Adresse des VPN-Konzentrators SIS • VPN_KONZENTRATOR_SIS_IP_ADDRESS • DNS_SERVER_SIS
Standardablauf	1) Wenn der Auslöser Event NETWORK/VPN/CONFIG_CHANGED ist, muss der VPN-Tunnel SIS abgebaut werden. 2) Wenn der VPN-Tunnel SIS noch aktiv ist, ist der Ablauf abgeschlossen. Anderenfalls ist mit Ablaufschritt 3) fortzufahren. 3) Prüfen, ob (MGM_LU_ONLINE=Enabled). falls nicht ist der TUC ohne Ausgabe einer Fehlermeldung zu beenden. 4) entfällt 5) Prüfen, ob die im Konnektor hinterlegte CRL noch gültig ist. falls nicht, MUSS der TUC_KON_040 „CRL aktualisieren“ aufgerufen werden, Anschließend erneut prüfen, ob die im Konnektor hinterlegte CRL nun gültig ist. Falls die CRL nicht gültig ist, ist der TUC mit Fehler zu beenden. 6) Aufrufen von TUC_VPN-ZD_0002 „IPsec Tunnel SIS aufbauen“ 7) Aufrufen von TUC_KON_304 „Netzwerk-Routen einrichten“ Sobald der Tunnel erfolgreich aufgebaut wurde, ist der folgende Event zu generieren: TUC_KON_256 {"NETWORK/VPN_SIS/UP"; Op;

	Info;IP= \$VPN_TUNNEL_SIS_INNER_IP}
Varianten/Alternativen	Keine
Fehlerfälle	(→3) Keine Online-Verbindung zulässig; 4172 (→5) CRL ist abgelaufen (outdated); Herstellerspezifisch kann entweder (5a) oder (5b) umgesetzt werden: (5a) Kritischer Fehlerzustand EC_CRL_Out_Of_Date wurde noch nicht festgestellt: 4173 (5b) kritischer Fehlerzustand EC_CRL_Out_Of_Date wurde bereits festgestellt: 4002 (->5) Wenn Fehler 4173 bzw. 4002 nicht zutreffen, ist ein herstellerspezifischer Fehler zu verwenden. (→6) VPN Tunnel konnte nicht aufgebaut werden; Fehlercode: 4176
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 332: TAB_KON_638 Fehlercodes TUC_KON_322 „Verbindung zu dem VPN-Konzentrator der SIS aufbauen“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4002	Security	Fatal	Der Konnektor befindet sich in einem kritischen Betriebszustand
4172	Technical	Fatal	Es ist keine Online-Verbindung zulässig.
4173	Technical	Fatal	Die CRL ist nicht mehr gültig (outdated).
4176	Technical	Fatal	SIS-VPN-Tunnel: Verbindung konnte nicht aufgebaut werden

[<=]

6165 4.2.4.4 Interne TUCs, auch durch Fachmodule nutzbar

6166 Keine

6167 4.2.4.5 Operationen an der Außenschnittstelle

6168 Keine

6169 4.2.4.6 Betriebsaspekte

6170 TIP1-A_5415 - Initialisierung „VPN-Client“

6171 Der Konnektor MUSS in der Bootup-Phase zur Initialisierung des Funktionsmerkmals
6172 „VPN-Client“:

- 6173 • die Verbindung zum VPN-Konzentrator TI aufbauen (TUC_KON_321)
- 6174 • die Verbindung zum VPN-Konzentrator SIS aufbauen (TUC_KON_322)

6175 [\leq]

6176 TIP1-A_4785-03 - Konfigurationsparameter VPN-Client

6177 Die Managementschnittstelle MUSS es einem Administrator ermöglichen
6178 Konfigurationsänderungen am VPN-Client gemäß Tabelle TAB_KON_639 vorzunehmen.
6179 Der Konnektor MUSS bei einer Änderung der Konfigurationswerte den folgenden Event
6180 auslösen:

6181 Rufe TUC_KON_256 {"NETWORK/VPN/CONFIG_CHANGED"; Op; Info;; doDisp = false}

6182

6183 **Tabelle 333: TAB_KON_639 – Konfigurationsparameter VPN-Client**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
IKE_KEEPA_LIVE_MODUS	Enabled/Disabled	Der Administrator MUSS einstellen können, ob IKE Keep-Alive-Pakete gesendet werden. Ein Hinweis MUSS ausgegeben werden, dass dies bei Nutzung von Dial-Up-Verbindungen nicht zu empfehlen ist. Dies dient der Vermeidung von Kosten bei Nutzung eines Internetzugangs ohne Flatrate. Default-Wert: Enabled
IKE_KEEPA_LIVE_INTERVAL	X Sekunden	Der Administrator MUSS die Zeit in Sekunden angeben können, nach der ein neues IKE Keep-Alive-Paket gesendet wird. Default-Wert: 30
IKE_KEEPA_LIVE_RETRY	X	Der Administrator MUSS angeben können, nach wie vielen IKE Keep-Alive-Paketen ohne Acknowledge Message die Verbindung beendet wird. Default-Wert: 3
VPN_IDLE_TIMEOUT_MODUS	Enabled/Disabled	Der Administrator MUSS einstellen können, ob nach Inaktivität die VPN-Verbindung automatisch abgebaut werden soll. Ein Hinweis MUSS ausgegeben werden, dass dies insbesondere bei Nutzung von Dial-Up-Verbindungen Enabled werden sollte. Default-Wert: Disabled

VPN_IDLE_TIMEOUT	X Sekunden	Der Administrator MUSS die Zeit in Sekunden angeben können, nach der eine inaktive VPN-Verbindung zu einem Abbau der Verbindung führt. Default-Wert: 600
NAT_KEEPALIVE_MODUS	Enabled/Disabled	Der Administrator MUSS einstellen können, ob NAT Keep-Alive-Pakete gesendet werden. Ein Hinweis MUSS ausgegeben werden, dass dies insbesondere bei Nutzung von Dial-Up-Verbindungen nicht zu empfehlen ist. Default-Wert: Enabled
NAT_KEEPALIVE_INTERVAL	X Sekunden	Der Administrator MUSS die Zeit in Sekunden angeben können, nach der ein neues NAT Keep-Alive-Paket gesendet wird. Default-Wert: 20
VPN_KONZENTRATOR_TI_IP_ADDRESS	IP-Adresse	IP-Adresse des VPN-Konzentrators TI im Transportnetz zu dem der IPsec-Tunnel VPN_TI aufgebaut wird. Der Wert kann vom Administrator nur eingesehen werden.
VPN_KONZENTRATOR_SIS_IP_ADDRESSES	IP-Adresse	IP-Adresse des VPN-Konzentrators SIS im Transportnetz zu dem der IPsec-Tunnel VPN_SIS aufgebaut wird. Der Wert kann vom Administrator nur eingesehen werden.
VPN_TI_MTU	Paketgröße in Byte	Der Administrator MUSS die MTU für ESP-Pakete zur TI (excl. ESP-Header-Size) in den Grenzen von 576 bis 8076 konfigurieren können. Default-Wert: 1318
VPN_SIS_MTU	Paketgröße in Byte	Der Administrator MUSS die MTU für ESP Pakete zum SIS (excl. ESP-Header-Size) in den Grenzen von 576 bis 8076 konfigurieren können. Default-Wert: 1318
HASH_AND_URL	Enabled/Disabled	Der Administrator MUSS die Nutzung des hash&URL-Verfahrens zum Zertifikatsaustausch konfigurieren können. Wenn HASH_AND_URL = Enabled gesetzt ist, wird die URL für das hash&URL-Verfahren automatisch durch DNS SRV- und TXT-Anfragen mit Owner „_hashandurl._tcp.<DNS_DOMAIN_VPN_ZUGD_I NT>„ ermittelt. Default-Wert: Disabled

[<=]

4.2.5 Zeitdienst

Der Zeitdienst schafft die Grundlage einer gleichen Systemzeit für alle in der TI einzusetzenden Produkttypen. Grundsätzlich ist ein NTP-Server der Stratum-3-Ebene innerhalb des Konnektors erforderlich, welcher die Zeitangaben eines NTP-Servers

6190 Stratum-2-Ebene abfragt (GS-A_3942). Die in [gemSpec_Net#5.1] „NTP-Topologie“
6191 getroffenen Anforderungen werden durch dieses Kapitel erweitert.

6192 Innerhalb des Zeitdienstes werden folgende Präfixe für Bezeichner verwendet:

- 6193 • Events (Topic Ebene 1): „NTP“
- 6194 • Konfigurationsparameter: „NTP_“

6195 4.2.5.1 Funktionsmerkmalweite Aspekte

6196 TIP1-A_4786 - Maximale Zeitabweichung

6197 Falls der Leistungsumfang Online nicht aktiviert ist (MGM_LU_ONLINE=Disabled), MUSS
6198 sichergestellt werden, dass der maximale zulässige Fehler von +/- 20ppm (part per
6199 million) gegenüber einer Referenzuhr nicht überschritten wird. Dies entspricht einer
6200 maximalen Abweichung im Freilauf von +/- 34,56 Sekunden über 20 Tage.
6201 [\leq]

6202 TIP1-A_4787 - Konfigurationsabhängige Funktionsweise

6203 Der NTP-Server des Konnektors MUSS deaktiviert sein, falls der Konnektor
6204 Leistungsumfang Online nicht aktiviert ist (MGM_LU_ONLINE=Disabled).
6205 [\leq]

6206 Falls die Systemzeit des Konnektors zu stark von der Zeit der zentralen TI-Plattform
6207 abweicht, deutet dies auf ein schwerwiegendes Problem im Konnektor oder der
6208 Umgebung hin, da dies im ordnungsgemäßen Betrieb nicht auftreten sollte.

6209 TIP1-A_4788 - Verhalten bei Abweichung zwischen lokaler Zeit und erhaltenen Zeit

6210 Der Konnektor DARF die im Konnektor vorgehaltene Systemzeit im Rahmen einer
6211 automatisierten Synchronisation NICHT aktualisieren, wenn die lokale Zeit von der im
6212 Rahmen der Synchronisation erhaltenen Zeit um mehr als NTP_MAX_TIMEDIFFERENCE
6213 abweicht. Dies betrifft NICHT Änderungen in der Darstellung der Systemzeit, die
6214 zeitzonenbedingt sind (MEZ -> MESZ -> MEZ), da die Zeitsynchronisation grundsätzlich
6215 UTC berücksichtigt. Bei einer erstmaligen Synchronisierung nach dem Boot-Vorgang oder
6216 bei einer erstmaligen Synchronisierung bei der Inbetriebnahme des Konnektors darf eine
6217 Synchronisation trotz einer Zeitabweichung größer einer Stunde durchgeführt werden.
6218 Daher MUSS der Konnektor bei einer Abweichung von mehr als einer Stunde in den
6219 kritischen Betriebszustand EC_TIME_DIFFERENCE_INTOLERABLE übergehen, ein weiterer
6220 fachlicher Betrieb des Konnektors DARF NICHT mehr erfolgen.
6221 [\leq]

6222 Der kritische Betriebszustand kann anschließend über einen manuellen Eingriff (z. B.
6223 Reboot) behoben werden (siehe 3.3 Betriebszustand).

6224 TIP1-A_4789 - Zustandsvariablen des Konnektor Zeitdienstes

6225 TAB_KON_640 listet die zu verwendenden Zustandsvariablen des Konnektor NTP-
6226 Servers. Diese Werte DÜRFEN NICHT durch den Administrator geändert werden.
6227

6228 **Tabelle 334: TAB_KON_640 Zustandswerte für Konnektor NTP-Server**

ReferenzID	Belegung	Zustandswerte
NTP_WARN_PERIOD	30	Anzahl an Tagen nach der ersten erfolglosen Zeitsynchronisierung nach der eine Warnung an den Betreiber erfolgen soll
NTP_GRACE_PERIOD	50	Anzahl an Tagen nach der ersten erfolglosen Zeitsynchronisierung nach welcher der Konnektor in einen kritischen

		Betriebszustand übergehen muss. Dieser Parameter wirkt nur bei MGM_LU_ONLINE = Enabled.
NTP_MAX_ TIMEDIFFERENCE	3600	Maximale Zeitabweichung in Sekunden zwischen Systemzeit und Zeit des Stratum- 2-Zeitserver zum Zeitpunkt der Zeitsynchronisierung. Dieser Parameter wirkt nur bei MGM_LU_ONLINE = Enabled.

6229

6230 [\leq]6231 **4.2.5.2 Durch Ereignisse ausgelöste Reaktionen**

6232 Keine.

6233 **4.2.5.3 Interne TUCs, nicht durch Fachmodule nutzbar**

6234 Keine.

6235 **4.2.5.4 Interne TUCs, auch durch Fachmodule nutzbar**

6236 4.2.5.4.1 TUC_KON_351 "Liefere Systemzeit"

6237 TIP1-A_4790 - TUC_KON_351 „Liefere Systemzeit“

6238 Der Konnektor MUSS den technischen Use Case TUC_KON_351 „Liefere Systemzeit“
6239 umsetzen.

6240

6241 **Tabelle 335: TAB_KON_776 TUC_KON_351 „Liefere Systemzeit“**

Element	Beschreibung
Name	TUC_KON_351 „Liefere Systemzeit“
Beschreibung	Der Konnektor MUSS die Systemzeit auf Anforderung an Fachmodule liefern können.
Anwendungsumfeld	Den Fachanwendungen ist die Systemzeit zu liefern.
Eingangsanforderung	Die Echtzeituhr des Konnektors wurde gemäß den geforderten Synchronisationsintervallen aktualisiert (bei MGM_LU_ONLINE=Enabled) oder manuell gesetzt (bei MGM_LU_ONLINE=Disabled)
Auslöser und Vorbedingungen	Fachmodule benötigen die aktuelle Systemzeit des Konnektors.
Eingangsdaten	Echtzeituhr des Konnektors
Komponenten	Konnektor, Fachmodule
Ausgangsdaten	Systemzeit des Konnektors
Standardablauf	Siehe [gemSpec_Net]
Varianten/Alternativen	Keine

Fehlerfälle	4178: Konnektor retourniert keine Systemzeit
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

6242 **Tabelle 336: TAB_KON_641 Fehlercodes TUC_KON_351 „Liefere Systemzeit“**

Fehlercode	ErrorType	Severity	Fehlertext
4178	Technical	Error	Das Fachmodul konnte die aktuelle Systemzeit des Konnektors nicht abrufen

6243

6244 [\leq]

6245 4.2.5.5 Operationen an der Außenschnittstelle

6246 4.2.5.5.1 Sync_Time

6247 TIP1-A_4791 - Operation sync_Time

6248 Der NTP-Server des Konnektors MUSS an der Client-Schnittstelle eine Operation
6249 sync_Time anbieten.

6250

6251 **Tabelle 337: TAB_KON_642 Operation sync_Time**

Name	I_NTP_Time_Information:sync_Time
Beschreibung	Der Konnektor MUSS anfragenden Clients (z.B. Arztarbeitsplatz) per NTP-Version 4 die Systemzeit liefern
Aufrufparameter	Vgl. [NTPv4]
Rückgabe	Vgl. [NTPv4]
Vorbedingungen	MGM_LU_ONLINE=Enabled
Nachbedingungen	Der anfragende Client hat die korrekte Zeit geliefert bekommen.
Hinweise	Keine
Fehler	Der Aufruf schlägt fehl (bleibt unbeantwortet), wenn MGM_LU_ONLINE=Disabled

6252

6253 [\leq]

6254 4.2.5.6 Betriebsaspekte

6255 TIP1-A_4792 - Explizites Anstoßen der Zeitsynchronisierung

6256 Der Konnektor MUSS dem Administrator die Möglichkeit bieten, eine Synchronisation mit
6257 dem zentralen Zeitdienst explizit anzustoßen.

6258 [\leq]

6259 TIP1-A_4793 - Konfigurierbarkeit des Konnektor NTP-Servers

6260 Der Administrator MUSS die in TAB_KON_643 aufgelisteten Parameter über die

6261 Managementschnittstelle konfigurieren und die in TAB_KON_730 aufgelisteten Parameter

6262 ausschließlich einsehen können.

6263

6264 **Tabelle 338: TAB_KON_643 Konfiguration des Konnektor NTP-Servers**

ReferenzID	Belegung	Bedeutung
NTP_TIMEZONE	Zeitzone	Der Administrator MUSS die Zeitzone des Konnektors einstellen können. Default-Wert: Central European Time/Mitteuropäische Zeit (CET/MEZ)
NTP_TIME	Zeit	Der Administrator MUSS die Zeit des Konnektors (NTP_TIME) über die Managementschnittstelle manuell einstellen können.

6265 **Tabelle 339: TAB_KON_730 Einsehbare Konfigurationsparameter des Konnektor NTP-Servers**

6266

ReferenzID	Belegung	Bedeutung
NTP_SERVER_ADDR	IP-Adressen	Die Adressen des primären und sekundären Stratum-2-Zeitserver der zentralen TI-Plattform für die Synchronisation mit dem NTP-Server des Konnektors.

6267

6268 [**<=**]

6269 TIP1-A_4794 - Warnung und Übergang in kritischen Betriebszustand bei nichterfolgter Zeitsynchronisierung

6270 Befindet sich der Konnektor im Zustand EC_TIME_SYNC_PENDING_CRITICAL oder
6271 EC_Time_Difference_Intolerable, MUSS der Administrator eine Korrektur oder
6272 Bestätigung der Systemzeit vornehmen können. Anschließend MUSS der Konnektor wie
6273 nach einer erfolgreichen Zeitsynchronisation verfahren, d. h. der Tagezähler wird auf 0
6274 zurückgesetzt.

6275 [**<=**]

6276

6277 **4.2.5.6.1 TUC_KON_352 Initialisierung Zeitdienst**

6278 TIP1-A_4795 - TUC_KON_352 „Initialisierung Zeitdienst“

6279 Der Konnektor MUSS in der Bootup-Phase TUC_KON_352 "Initialisierung Zeitdienst"
6280 durchlaufen.

6281

6282 **Tabelle 340: TAB_KON_644 – TUC_KON_352 „Initialisierung Zeitdienst“**

Element	Beschreibung
Name	TUC_KON_352 „Initialisierung Zeitdienst“
Beschreibung	Der Konnektor muss zum Bootup den konnektoreigenen NTP-Server mit einem NTP-Server der zentralen TI-Plattform synchronisieren falls MGM_LU_ONLINE=Enabled.
Anwendungsumfeld	Synchronisierung der Systemzeit zur Startzeit

Eingangsanforderung	Keine
Auslöser	<ul style="list-style-type: none"> • Bootup • Event NETWORK/VPN_TI/UP
Vorbedingungen	Verbindung zum VPN-Konzentrator TI muss aufgebaut sein
Eingangsdaten	NTP-Server der zentralen TI-Plattform
Komponenten	Konnektor
Ausgangsdaten	Keine
Standardablauf	<p>Falls MGM_LU_ONLINE=Enabled:</p> <ul style="list-style-type: none"> • Durch eine DNS-Anfrage an den DNS-Forwarder zur Auflösung des SRV-RR mit dem Bezeichner "_ntp._udp.<DOMAIN_SRVZONE_TI>„ erhält der Konnektor Adressen der NTP-Server der zentralen TI-Plattform. • gemäß [NTPv4] • Falls keine Antwort erfolgt ist oder falls der Zeitserver nicht erreichbar ist, wird Fehler 4177 ausgelöst. Zur Feststellung werden die NTPv4 eigenen Timeoutwerte berücksichtigt.
Varianten/Alternativen	Keine
Fehlerfälle	4177: Der NTP-Server des Konnektors empfängt keine Systemzeit
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

6283 **Tabelle 341: TAB_KON_645 Fehlercodes TUC_KON_352 „Initialisierung Zeitdienst“**

Fehlercode	ErrorType	Severity	Fehlertext
4177	Technical	Warning	Der NTP-Server des Konnektors konnte nicht synchronisiert werden.

6284
6285 [**<=**]

4.2.6 Namensdienst und Dienstlokalisierung

Innerhalb des Namensdienstes werden folgende Präfixe für Bezeichner verwendet:

- Events (Topic Ebene 1): keine Events vorhanden
- Konfigurationsparameter: „DNS_“

4.2.6.1 Funktionsmerkmalweite Aspekte

TIP1-A_4796 - Grundlagen des Namensdienstes

Der Konnektor MUSS einen Recursive Caching Nameserver zur Auflösung von DNS-Anfragen sowie einen autoritativen Nameserver zur Verwaltung der Zone „konlan.“ bereitstellen.

Der Caching-Nameserver des Konnektors MUSS für Clientsysteme aus dem lokalen Netzwerk (ANLW_LAN_NETWORK_SEGMENT oder ANLW_LEKTR_INTRANET_ROUTES) erreichbar sein.

Der Caching-Nameserver des Konnektors MUSS einen Timeout für die Bearbeitung von DNS-Abfragen beachten. Konnte eine DNS-Abfrage nicht durchgeführt werden, MUSS die Bearbeitung abgebrochen werden.

[<=]

TIP1-A_6480 - Resource Records der Zone konlan.

Der Konnektor MUSS in der Zone „konlan.“ die folgenden Resource Records bereitstellen:

- label: „konnektor.konlan.“, ttl: <Time To Live>, class: IN, type: A, rdata: <LAN-seitige IP-Adresse des Konnektors>

Die in spitzen Klammern angegebenen Werte müssen implementierungs- und konfigurationsabhängig vergeben werden.

[<=]

TIP1-A_4797 - DNS-Forwards des DNS-Servers

Der DNS-Server des Konnektors MUSS die folgenden DNS-Forwards durchführen:

Tabelle 342: TAB_KON_687 DNS-Forwards des DNS-Servers

Domain	Forwarders	Bemerkungen
Namensraum TI, *.DNS_TOP_LEVEL_DOMAIN_TI	DNS_SERVERS_TI	DNS Forward Rule zur Auflösung aller DNS-Namen innerhalb des Namensraums der TI mit der Top Level Domain telematik (für die PU) und telematik-test (für die RU und TU).
Namensraum TI, Top Level Domain ti-wa (PU) und ti-wa-test (RU und TU).	DNS_SERVERS_TI	DNS Forward Rule zur Auflösung aller DNS-Namen innerhalb des Namensraums der TI mit der Top Level Domain ti-wa (für die PU) und ti-wa-test (für die RU und TU).
Namensraum angeschlossene Netze des Gesundheitswesens mit aAdG-NetG	DNS_SERVERS_BESTANDS_NETZE (Je Domainnamen eines	Je angeschlossenes Netz des Gesundheitswesens mit aAdG-NetG in ANLW_AKTIVE_BESTANDSNETZE wird eine DNS Forward Rule zur

(Domainnamen von angeschlossenen Netzen des Gesundheitswesens mit aAdG-NetG gemäß Bestandsnetze.xml)	angeschlossenen Netzes des Gesundheitswesens mit aAdG-NetG alle zugehörigen DNS-Server IP-Adressen gemäß Bestandsnetze.xml)	Auflösung von DNS-Namen innerhalb dieses Netzes verwendet.
Namensraum lokale Einsatzumgebung (DNS_DOMAIN_LEKTR)	DNS_SERVERS_LEKTR	DNS Forward Rule zur Auflösung aller DNS-Namen innerhalb der DNS-Domain DNS_DOMAIN_LEKTR
Namensraum Internet	DNS_SERVERS_SIS	Wenn der VPN-Tunnel SIS aktiv ist, muss eine Forward Rule für den Namensraum Internet über die DNS_SERVERS_SIS existieren.
Namensraum Internet	DNS_SERVERS_INT	Wenn der VPN-Tunnel SIS nicht aktiv ist, muss eine Forward Rule für den Namensraum Internet über die DNS_SERVERS_INT existieren
Lokale Zone „konlan.“	autoritativer Nameserver des Konnektors	DNS Forward Rule zur Auflösung aller DNS-Namen innerhalb der Zone „konlan.“

6312

6313 [**<=**]

6314 TIP1-A_4798 - DNS Stub-Resolver

6315 Der Stub-Resolver im Konnektor MUSS von allen internen Diensten zur Namensauflösung genutzt werden.

6316 Der Stub-Resolver im Konnektor MUSS immer den Caching-Nameserver im Konnektor anfragen.

6317 [**<=**]

6320 TIP1-A_4799 - Aktualität der DNS-Vertrauensanker sicherstellen

6321 Der Konnektor, der einen Caching Nameserver als Validating Resolver umsetzt, MUSS

6322 den DNSSEC-Vertrauensanker der TI aus dem Zertifikatspeicher in den Caching-

6323 Nameserver übernehmen, wenn ein Fehler bei der Validierung der Namensauflösung der

6324 TI aufgetreten ist. [**<=**]

6325

6326 **4.2.6.2 Durch Ereignisse ausgelöste Reaktionen**

6327 Keine.

6328 **4.2.6.3 Interne TUCs, nicht durch Fachmodule nutzbar**

6329 Keine.

6330 **4.2.6.4 Interne TUCs, auch durch Fachmodule nutzbar**

6331 4.2.6.4.1 TUC_KON_361 „DNS-Namen auflösen“

6332 TIP1-A_4801 - TUC_KON_361 „DNS-Namen auflösen“

6333 Der Konnektor MUSS den technischen Use Case TUC_KON_361 „DNS-Namen auflösen“
6334 umsetzen.

6335

6336 **Tabelle 343: TAB_KON_646 – TUC_KON_361 „DNS-Namen auflösen“**

Element	Beschreibung
Name	TUC_KON_361 „DNS-Namen auflösen“
Beschreibung	Ein FQDN wird in ein oder mehrere IPs aufgelöst
Auslöser	interne Anfrage (Basisdienst oder Fachmodul)
Vorbedingungen	Die vom Konnektor zu verwendenden DNS-Server (DNS_SERVERS_INT, DNS_SERVERS_TI, DNS_SERVERS_SIS, DNS_SERVERS_BESTANDSNETZE) müssen konfiguriert sein.
Eingangsdaten	FQDN (Name, für den die IP-Adressen ermittelt werden sollen)
Komponenten	Konnektor
Ausgangsdaten	LIST_OF_IP_ADDRESSES
Standardablauf	1) Mit dem FQDN wird eine Anfrage an den Stub-Resolver des Konnektors (Typ A und AAAA) durchgeführt. Für alle ermittelten IPv4-Adressen und IPv6-Adressen werden als LIST_OF_IP_ADDRESSES zurückgeliefert. Da IPv6 nicht produktiv eingesetzt wird muss die aufrufende Instanz die IPv6-Adressen ignorieren. Falls keine IP-Adressen ermittelt werden konnten, wird eine leere Liste zurückgeliefert.
Varianten/Alternativen	Keine
Fehlerfälle	(→ 1) Timeout der Anfrage; Fehlercode 4179 (→ 1) DNS-Fehler; Fehlercode 4180

Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

6337 **Tabelle 344: TAB_KON_647 Fehlercodes TUC_KON_361 „DNS Namen auflösen“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4179	Technical	Error	„DNS: Anfrage wurde wegen Timeout abgebrochen.“
4180	Technical	Fatal	„DNS: Es ist ein Fehler bei der Namensauflösung aufgetreten“ Die Fehlerdetails sind gemäß DNS-Protokoll zu ergänzen.

6338 [\leq]

6339 TIP1-A_4801-02 - ab PTV4: TUC_KON_361 „DNS-Namen auflösen“

6340 Der Konnektor MUSS den technischen Use Case TUC_KON_361 „DNS-Namen auflösen“
6341 umsetzen.

6342

6343 **Tabelle 345: TAB_KON_646 – TUC_KON_361 „DNS-Namen auflösen“**

Element	Beschreibung
Name	TUC_KON_361 „DNS-Namen auflösen“
Beschreibung	Ein FQDN wird in ein oder mehrere IPs aufgelöst
Auslöser	interne Anfrage (Basisdienst oder Fachmodul)
Vorbedingungen	Die vom Konnektor zu verwendenden DNS-Server (DNS_SERVERS_INT, DNS_SERVERS_TI, DNS_SERVERS_SIS, DNS_SERVERS_BESTANDSNETZE) müssen konfiguriert sein.
Eingangsdaten	FQDN (Name, für den die IP-Adressen ermittelt werden sollen)
Komponenten	Konnektor
Ausgangsdaten	LIST_OF_IP_ADDRESSES
Standardablauf	1) Mit dem FQDN wird eine Anfrage an den Stub-Resolver des Konnektors (Typ A und AAAA) durchgeführt. Für alle ermittelten IPv4-Adressen und IPv6-Adressen werden als LIST_OF_IP_ADDRESSES zurückgeliefert. Wird IPv6 nicht produktiv eingesetzt, muss die aufrufende Instanz die IPv6-Adressen ignorieren. Falls keine IP-Adressen ermittelt werden konnten, wird eine leere Liste zurückgeliefert.

Varianten/Alternativen	Keine
Fehlerfälle	(→ 1) Timeout der Anfrage; Fehlercode 4179 (→ 1) DNS-Fehler; Fehlercode 4180
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

6344 **Tabelle 346: TAB_KON_647 Fehlercodes TUC_KON_361 „DNS Namen auflösen“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4179	Technical	Error	„DNS: Anfrage wurde wegen Timeout abgebrochen.“
4180	Technical	Fatal	„DNS: Es ist ein Fehler bei der Namensauflösung aufgetreten“ Die Fehlerdetails sind gemäß DNS-Protokoll zu ergänzen.

6345
6346 [\leq]

6347 4.2.6.4.2 TUC_KON_362 „Liste der Dienste abrufen“

6348 TIP1-A_4802 - TUC_KON_362 „Liste der Dienste abrufen“

6349 Der Konnektor MUSS den technischen Use Case TUC_KON_362 „Liste der Dienste
6350 abrufen“ umsetzen.

6351 **Tabelle 347: TAB_KON_648 – TUC_KON_362 „Liste der Dienste abrufen“**

Element	Beschreibung
Name	TUC_KON_362 „Liste der Dienste abrufen“
Beschreibung	Ermittlung aller zu einer DNS-SD-Gruppe gehörenden DNS-Namen.
Auslöser	interne Anfrage (Basisdienst oder Fachmodul)
Vorbedingungen	Die vom Konnektor zu verwendenden DNS-Server müssen konfiguriert sein.
Eingangsdaten	FQDN des PTR Resource Records
Komponenten	Konnektor
Ausgangsdaten	LIST_OF_SRV_ENTITIES
Standardablauf	Mit dem FQDN wird eine Typ „PTR“ Anfrage an den Stub-Resolver des Konnektor gestellt.
Varianten/Alternativen	Keine

Fehlerfälle	(→ 1) Timeout der Anfrage; Fehlercode 4179 (→ 1) DNS-Fehler; Fehlercode 4180
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 348: TAB_KON_649 Fehlercodes TUC_KON_362 „Liste der Dienste abrufen“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4179	Technical	Error	„DNS: Anfrage wurde wegen Timeout abgebrochen.“
4180	Technical	Fatal	„DNS: Es ist ein Fehler bei der Namensauflösung aufgetreten“ Die Fehlerdetails sind gemäß [gemSpec_Net] zu ergänzen.

[<=]

4.2.6.4.3 TUC_KON_363 „Dienstdetails abrufen“

TIP1-A_4803 - TUC_KON_363 „Dienstdetails abrufen“

Der Konnektor MUSS den technischen Use Case TUC_KON_363 „Dienstdetails abrufen“ umsetzen.

Tabelle 349: TAB_KON_650 - TUC_KON_363 „Dienstdetails abrufen“

Element	Beschreibung
Name	TUC_KON_363 Dienstdetails abrufen
Beschreibung	Ermitteln aller DNS-SD-Details zu einem vollqualifizierten DNS-Namen.
Auslöser	interne Anfrage (Basisdienst oder Fachmodul)
Vorbedingungen	Die vom Konnektor zu verwendenden DNS-Server müssen konfiguriert sein.
Eingangsdaten	FQDN (der Name eines DNS-SD-Elements)
Komponenten	Konnektor
Ausgangsdaten	LIST_OF_SRV_ENTRIES LIST_OF_SRV_DETAILS
Standardablauf	1) Mit dem FQDN wird eine Typ-„SRV“-Anfrage an den Stub-Resolver des Konnektors gestellt. Die vom DNS-Server zurück gelieferten SRV-Einträge werden als LIST_OF_SRV_ENTRIES (bestehend aus TTL, Priority, Weight, Port, Target) zurückgeliefert. Wenn kein Eintrag gefunden werden konnte, wird eine

	<p>leere Liste LIST_OF_SRV_ENTRIES zurückgeliefert. 2) Mit dem FQDN wird zusätzlich eine Typ-„TXT“-Anfrage an den Stub-Resolver des Konnektors gestellt. Wenn ein oder mehrere entsprechende Einträge gefunden werden konnten, werden diese in einer gemeinsamen Liste LIST_OF_SRV_DETAILS (bestehend aus TTL und TXT) zusammengefasst. Wenn kein Eintrag gefunden werden konnte, wird eine leere Liste LIST_OF_SRV_DETAILS zurückgeliefert. Falls keine FQDN ermittelt werden konnten, wird je eine leere Liste LIST_OF_SRV_ENTRIES und LIST_OF_SRV_DETAILS zurückgeliefert.</p>
Varianten/Alternativen	Keine
Fehlerfälle	(→ 1-2) Timeout der Anfrage; Fehlercode 4179 (→ 1-2) DNS Fehler; Fehlercode 4180
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

6363 **Tabelle 350: TAB_KON_651 Fehlercodes TUC_KON_363 „Dienstdetails abrufen“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4179	Technical	Error	„DNS: Anfrage wurde wegen Timeout abgebrochen.“
4180	Technical	Fatal	„DNS: Es ist ein Fehler bei der Namensauflösung aufgetreten“ Die Fehlerdetails sind gemäß [gemSpec_Net] zu ergänzen.

6364
6365 [<=]

6366 4.2.6.5 Operationen an der Außenschnittstelle

6367 TIP1-A_4804 - Basisanwendung Namensdienst

6368 Der Konnektor MUSS für Clients eine Basisanwendung Namensdienst anbieten.

6369 **Tabelle 351: TAB_KON_652 Basisanwendung Namensdienst**

Name	Namendienst
Version	wird im Produktsteckbrief des Konnektors definiert
Namensraum	Keiner

Namensraum-Kürzel	Keiner	
Operationen	Name	Kurzbeschreibung
	GetIPAddress	Diese Operation ermöglicht die Auflösung von FQDNs in IP-Adressen
WSDL	Keines	
Schema	Keines	

6370

6371 [**<=**]6372 4.2.6.5.1 *GetIPAddress*

6373 TIP1-A_5035 - Operation GetIPAddress

6374 Der Namensdienst des Konnektors MUSS an der Client-Schnittstelle eine Operation
 6375 GetIPAddress anbieten.

6376

6377 **Tabelle 352: TAB_KON_653 Operation GetIPAddress**

Name	GetIPAddress
Beschreibung	Diese Operation ermöglicht die Auflösung von FQDN in IP-Adressen. (DNS-Forwarder Abfrage ohne Cache)
Aufrufparameter	Address (FQDN) DNSSECValidation (Boolean)
Rückgabe	IPAddr (IPAddress) DNSSECValidated (Boolean)
Vorbedingungen	Der DNS-Server im Konnektor muss aktiv sein. Die Forward Nameserver (DNS_SERVERS_TI, DNS_SERVERS_SIS, DNS_SERVERS_BESTANDSNETZE) müssen konfiguriert sein.
Nachbedingungen	Keine
Standardablauf	Für Details zu DNS Namensauflösung wird auf [gemSpec_Net] verwiesen.

6378

6379 [**<=**]6380 **4.2.6.6 Betriebsaspekte**

6381 TIP1-A_5416 - Initialisierung „Namensdienst und Dienstlokalisierung“

6382 Der Konnektor MUSS in der Bootup-Phase zur Initialisierung des Funktionsmerkmals
 6383 „Namensdienst und Dienstlokalisierung“:

6384 • den autoritativen Nameserver starten

6385 • den Caching-Nameserver starten.

6386 [**<=**]

6387 TIP1-A_4805 - Konfigurationsparameter Namensdienst und Dienstlokalisierung
6388 Der Administrator MUSS die in TAB_KON_654 aufgelisteten Parameter über die
6389 Managementschnittstelle konfigurieren und die in TAB_KON_731 aufgelisteten Parameter
6390 ausschließlich einsehen können.
6391 Nach jeder Änderung MUSS sichergestellt werden, dass die Änderungen sofort am
6392 autoritativen bzw. am Caching-Nameserver zur Verfügung stehen.
6393

6394 **Tabelle 353: TAB_KON_654 - Konfigurationsparameter Namensdienst**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
DNS_SERVERS_INT	Liste von IP-Adressen der DNS-Server	Liste von DNS-Servern für das Transportnetz. Die IP-Adressen KÖNNEN auf einen öffentlich zugänglichen Adressbereich eingeschränkt sein.
DNS_DOMAIN_VPN_ZUGD_INT	DNS Domainname	DNS-Domainname für die Service Discovery der VPN-Konzentratoren des VPN-Zugangsdienstes
DNS_SERVERS_LEKTR	Liste von IP-Adressen der DNS-Server	Liste von DNS-Servern, die zur Namensauflösung von Namensräumen in der Einsatzumgebung verwendet werden. Der Administrator MUSS die Liste von DNS-Servern, die die DNS_DOMAIN_LEKTR auflösen, bearbeiten können. Die IP-Adressen der DNS-Server KÖNNEN auf den Adressbereich der ANLW_LAN_IP_ADDRESS eingeschränkt sein.
DNS_DOMAIN_LEKTR	DNS Domainname	DNS Domainname, der von einem DNS-Server der Einsatzumgebung aufgelöst wird. Der Name DARF NICHT mit einem „.“ beginnen und nicht mit einem „.“ enden.
DNS_TA_CONFIG	Ist abhängig von der gewählten Umsetzung	Wenn der Konnektor als Validating Resolver für den Namensraum Internet implementiert ist gilt: Der Administrator MUSS die aktuellen DNSSEC Trustanchor für den Namensraum Internet auf geeignetem Weg in den Konnektor übernehmen können.

6395 **Tabelle 354: TAB_KON_731 Einsehbare Konfigurationsparameter Namensdienst**

ReferenzID	Belegung	Bedeutung
------------	----------	-----------

DNS_SERVERS_TI	Liste von IP-Adressen der DNS-Server	Liste von DNS-Servern, die zur Namensauflösung des Namensraums der TI verwendet werden
DNS_SERVERS_SIS	Liste von IP-Adressen der DNS-Server	Liste von DNS-Servern, die zur Namensauflösung des Namensraums Internet bei Nutzung des SIS verwendet werden
DNS_SERVERS_BESTANDSNETZE	Liste von IP-Adressen der DNS-Servern je Domäne je freigegebenem angeschlossenen Netz des Gesundheitswesens mit aAdG-NetG	Liste von DNS-Servern je Domain eines dieser freigegebenen Netze.
DNS_TOP_LEVEL_DOMAIN_TI	DNS Domainname	Top Level Domain des Namensraumes TI

6396
6397
6398 [**<=**]

6399 4.2.7 Optionale Verwendung von IPv6

6400 Der Konnektor kann zusätzlich eine IPv6-Adresse an den Netzwerkschnittstellen zum
6401 Transportnetz implementieren. Entscheidet sich der Hersteller für den parallelen Einsatz
6402 von IPv4 und IPv6 (Dual-Stack-Mode), sind die nachfolgenden Anforderungen dieses
6403 Kapitels umzusetzen. Einhergehend mit der Entscheidung, IPv6 an diesem Interface zu
6404 konfigurieren, ist der spätere VPN-Tunnelaufbau zur TI und SIS über das IPv6 Interface
6405 möglich. Die durch den jeweiligen IPv6-Tunnel zu transportierenden IP-Pakete sind IPv4
6406 adressierte Pakete.

6407 A_17199 - IPv6 - Adressierung der Schnittstelle zum Internet (Option IPv6)
6408 Der Konnektor MUSS bei Verwendung von IPv6 für den VPN-Tunnelaufbau zur TI und SIS
6409 auf geeignete Weise (z.B. DHCP vom IAG) mit einer IPv6-Adresse auf dem physikalischen
6410 Interface in Richtung Internet konfiguriert werden (Dual-Stack-Mode). [**<=**]

6411 A_17200 - IPv6 - Fragmentierung der IKEv2-Nachrichten (Option IPv6)
6412 Der Konnektor MUSS bei Verwendung von IPv6 für den VPN-Tunnelaufbau zur TI und SIS
6413 die Fragmentierung von IKEv2 Nachrichten gemäß [RFC7383] unterstützen. [**<=**]

6414
6415 A_17201 - IPv6 - Verhalten als IPv6 Router (Option IPv6)
6416 Der Konnektor MUSS bei Verwendung von IPv6 für den VPN-Tunnelaufbau zur TI und SIS
6417 die notwendige Route für das Erreichen des Internets bereitstellen. [**<=**]

6418 4.3 Konnektormanagement

6419 Das Konnektormanagement dient ausschließlich Betriebsaspekten des Konnektors. Daher
6420 wird in diesem Kapitel weitestgehend auf die übliche Strukturierung nach TUCs
6421 (intern/für Fachmodule), Außenoperationen und Betriebsaspekten verzichtet. Lediglich
6422 der KSR-Client verwendet diese Kapitelstruktur.

6423 Innerhalb des Konnektormanagements werden vorrangig folgende Präfixe für Bezeichner
6424 verwendet:

- 6425 • Events (Topic Ebene 1): „MGM“
- 6426 • Konfigurationsparameter: „MGM_“

6427 Eine Ausnahme hiervon bildet der Anteil der Software-Aktualisierung (KSR-Client). Dieser
6428 verwendet folgende Präfixe für Bezeichner:

- 6429 • Events (Topic Ebene 1): „KSR“
- 6430 • Konfigurationsparameter: „MGM_“

6431 TIP1-A_4806 - Verpflichtende Managementschnittstelle

6432 Der Konnektor MUSS LAN-seitig über eine Managementschnittstelle für Konfiguration und
6433 Diagnose verfügen.

6434 Die Ausführung der Schnittstelle ist herstellerspezifisch, MUSS aber entweder als
6435 Konfigurations-Frontend im Sinne einer eigenständigen Client-Applikation oder als Web-
6436 Oberfläche ausgeprägt sein.

6437 Wenn die Schnittstelle als Web-Oberfläche ausgeprägt ist, MUSS im Handbuch
6438 beschrieben sein, wo angegeben ist, welche Browser-Versionen für welche
6439 Betriebssysteme unterstützt werden (bspw. im Handbuch selbst oder über einen Link auf
6440 eine Web-Seite des Herstellers), und wo diese als installierbares Softwarepaket oder
6441 direkt ausführbare Datei bezogen werden können.

6442 Die Verbindung zur Managementschnittstelle MUSS zur Sicherung der Vertraulichkeit,
6443 Integrität und Authentizität durch Nutzung eines kryptographischen Verfahrens gemäß
6444 [gemSpec_Krypt] abgesichert werden, falls die Sicherheit der übertragenen Daten nicht
6445 auf andere Weise erreicht wird. Die Absicherung der Daten kann z. B. durch Nutzung von
6446 TLS unter Berücksichtigung der in [gemSpec_Krypt] angegebenen Algorithmen und
6447 Schlüssellängen geschehen.

6448 Die Managementschnittstelle MUSS in thematisch gegliederte Konfigurationsbereiche
6449 unterteilt sein. Die konkrete Gliederung selbst ist herstellerspezifisch.

6450 Die Managementschnittstelle KANN einen Managementbereich aufweisen, der nur für
6451 autorisierte Techniker des Herstellers zugänglich ist. Ein Zugriff auf diesen Bereich MUSS
6452 durch eine eigene Authentisierungsfunktion geschützt werden (z. B. durch
6453 Passwortschutz).

6454 [\leq]

6455 Die über die Managementschnittstelle zu erreichenden und zu verändernden Inhalte
6456 werden erhoben in:

- 6457 • diesem Kapitel
- 6458 • in allen Betriebsaspektkapiteln der Funktionsmerkmale, sowie der
6459 Übergreifenden Festlegungen
- 6460 • den Fachmodulspezifikationen der Fachanwendungen (siehe Kapitel 4.3.4).
- 6461 • Den übergreifenden Spezifikationen [gemSpec_Net] und [gemSpec_PKI]

6462 Eine Ergänzung um weitere, herstellerspezifische Konfigurationsinhalte ist möglich.

6463 TIP1-A_5661 - Automatisierung Managementschnittstelle

6464 Der Konnektor MUSS für die Automatisierung von Konnektor-Tests alle Funktionen, die
6465 über die Managementschnittstelle bereitgestellt werden, über eine LAN-seitige
6466 Schnittstelle ohne graphische Benutzerführung bereitstellen.

6467 Der Konnektorhersteller MUSS eine Dokumentation der Schnittstelle bereitstellen, welche
6468 die Nutzung so beschreibt, dass die Schnittstelle von der gematik in vollem Umfang
6469 genutzt werden kann. Die Dokumentation MUSS der gematik im Regelfall zwei Wochen
6470 vor Einreichung des Zulassungsobjekts bereitgestellt werden. Von diesem Regelfall KANN

6471 in Abstimmung mit der gematik abgewichen werden.
 6472 Die Schnittstelle SOLL mittels JSON [RFC7159] bereitgestellt werden. Wenn die
 6473 Bereitstellung nicht mittels JSON erfolgt, MUSS sie über eine vergleichbare Technologie
 6474 erfolgen.
 6475 Der Zugriff auf die Schnittstelle MUSS in RU/TU erlaubt sein. Falls der Zugriff in der PU
 6476 erlaubt ist, MUSS er dort ebenso wie die Managementschnittstelle abgesichert sein:

- 6477 • Die Verbindung zu dieser Schnittstelle MUSS zur Sicherung der Vertraulichkeit,
 6478 Integrität und Authentizität durch Nutzung eines kryptographischen
 6479 Verfahrens gemäß [gemSpec_Krypt] abgesichert werden, falls die Sicherheit
 6480 der übertragenen Daten nicht auf andere Weise erreicht wird. Die Absicherung
 6481 der Daten kann z. B. durch Nutzung von TLS unter Berücksichtigung der in
 6482 [gemSpec_Krypt] angegebenen Algorithmen und Schlüssellängen geschehen.
- 6483 • Der Konnektor MUSS die Schnittstelle mittels Benutzername und Passwort
 6484 oder einem mindestens gleich starken Mechanismus vor unberechtigtem
 6485 Zugang schützen.

6486 Ansonsten DARF der Zugriff in der PU NICHT möglich sein.
 6487 [**<=**]

6488 TIP1-A_4807 - Mandantenübergreifende Managementschnittstelle
 6489 Das Management des Konnektors MUSS über die Managementschnittstelle
 6490 mandantenübergreifend erfolgen. Dies bedeutet insbesondere, dass ein Administrator
 6491 (gemäß seiner Zugriffsberechtigungen) in einer Management-Session alle Einstellungen
 6492 einsehen und verändern können MUSS, egal welchem Mandanten diese Werte zugeordnet
 6493 sind.
 6494 [**<=**]

6495 TIP1-A_5658 - Konnektor, rollenspezifische Endpunkte der Managementschnittstelle
 6496 Der Konnektor MUSS die Managementschnittstelle mit zwei getrennten Endpunkten
 6497 implementieren. Der Konnektor MUSS sicherstellen, dass auf den einen Endpunkt nur
 6498 Nutzer mit der Rolle Lokaler-Administrator oder Super-Administrator zugreifen können,
 6499 und auf den anderen Endpunkt nur Nutzer mit der Rolle Remote-Administrator.
 6500 [**<=**]

6501 TIP1-A_5005 - Protokollierung in der Managementschnittstelle
 6502 Jede Änderung, die ein Administrator vornimmt, MUSS protokolliert werden durch
 6503 TUC_KON_271 „Schreibe Protokolleintrag“ {
 6504 topic=„MGM/ADMINCHANGES“;
 6505 eventType=Op;
 6506 severity=Info;
 6507 parameters =(„User=\$AdminUsername,
 6508 RefID=\$ReferenzID,
 6509 NewVal=\$NeuEingestellterWert“)}
 6510 Der hier geforderte Logging-Level gilt, wenn nicht an anderer Stelle eine abweichende
 6511 Regelung spezifiziert ist.
 6512 Wenn die Änderung über ein Remote-Management-System durchgeführt wird, ohne dass
 6513 ein Remote-Administrator im Konnektor konfiguriert ist, so MUSS als User eine Referenz
 6514 auf das Remote-Management-System verwendet werden.
 6515 Passwörter DÜRFEN NICHT in den Protokolleinträgen geschrieben werden.
 6516
 6517 [**<=**]

4.3.1 Zugang und Benutzerverwaltung des Konnektormanagements

Der Konnektor verfügt über keine Verwaltung der fachlichen Nutzer, wohl aber über eine Verwaltung der Nutzer, die in der Rolle eines Administrators den Konnektor konfigurieren und die Protokolle einsehen dürfen. Dabei werden drei Administrator-Rollen unterschieden:

1. Lokaler-Administrator: zur Konfiguration des Konnektors über die lokale Managementschnittstelle
2. Remote-Administrator: zur Konfiguration des Konnektors über die remote Managementschnittstelle.
3. Super-Administrator: zur Verwaltung von Benutzerkonten und zur Konfiguration des Konnektors über die lokale Managementschnittstelle

TIP1-A_4808 - Zugangsschutz der Managementschnittstelle

Der Konnektor MUSS sicherstellen, dass die Managementschnittstelle vor unberechtigtem Zugang geschützt ist. Die Managementschnittstelle MUSS durch eine Kombination aus Benutzername und Passwort oder einen mindestens gleich starken Mechanismus vor unberechtigtem Zugang geschützt sein.

Für die Erstellung und Verarbeitung von Passwörtern der Managementschnittstelle MÜSSEN die Empfehlungen der Grundsatz-Kataloge des BSI beachtet werden (siehe Maßnahme „M 2.11 Regelung des Passwortgebrauchs“ in [BSI_GK]).

Für die Passwörterstellung MUSS der Konnektor mindestens folgende Aspekte berücksichtigen:

- dem Benutzer muss es möglich sein, die Zeichen eines Passworts aus den Zeichenklassen Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Ziffern zu wählen. Ein Passwort muss Zeichen aus mindestens drei dieser Zeichenklassen enthalten.
- ein Passwort muss mindestens 8 Zeichen lang sein
- ein Passwort darf nicht die zugehörige Benutzerkennung enthalten (weder vorwärts noch rückwärts, bei Vergleich unter Ignorierung der Groß- und Kleinschreibung)
- die Wiederholung alter Passwörter beim Passwortwechsel durch den Benutzer selbst muss vom Konnektor verhindert werden (Passworthistorie). Dazu muss der Konnektor mindestens die letzten drei Passwörter eines Benutzers bei der Passwortneuvergabe erkennen und als neues Passwort ablehnen.

Für die Passwortverarbeitung MUSS der Konnektor mindestens folgende Aspekte berücksichtigen:

- für die Erstanmeldung neuer Benutzer müssen Einmalpasswörter vergeben werden, also Passwörter, die nach einmaligem Gebrauch gewechselt werden müssen. Gleiches gilt, wenn ein Passwort eines Benutzers vom Super-Admin zurückgesetzt wird.
- jeder Benutzer muss sein eigenes Passwort jederzeit ändern können
- bei der Eingabe darf das Passwort nicht im Klartext auf dem Bildschirm angezeigt werden
- die Passwörter müssen im Konnektor zugriffssicher gespeichert werden

- 6563 • der Konnektor muss nach einem durch den Super-Admin konfigurierbaren
6564 Zeitraum (Voreinstellung: 120 Tage) einen Passwortwechsel beim nächsten
6565 Login initiieren
- 6566 • erfolglose Anmeldeversuche müssen mit einer kurzen Fehlermeldung ohne
6567 Angabe von näheren Einzelheiten abgelehnt werden. Insbesondere darf bei
6568 erfolglosen Anmeldeversuchen nicht erkennbar sein, ob der eingegebene
6569 Benutzername oder das eingegebene Passwort (oder beides) falsch ist.
- 6570 • Nach einer Fehleingabe des Passworts muss eine Verzögerung bis zur
6571 nächsten Eingabemöglichkeit des Passworts für dieselbe Benutzerkennung
6572 erfolgen. Die Verzögerung soll 3 Sekunden betragen.
- 6573 **[<=]**
- 6574 Näheres hierzu regeln die Schutzprofile des Konnektors.
- 6575 TIP1-A_4810 - Benutzerverwaltung der Managementschnittstelle
- 6576 Der Konnektor MUSS eine Benutzerverwaltung für die Managementschnittstelle
6577 enthalten, in der anmeldeberechtigte Administratoren-Benutzer definiert werden können.
6578 Die Benutzerverwaltung MUSS die Administrator-Rollen Lokaler-Administrator, Remote-
6579 Administrator und Super-Administrator unterstützen.
- 6580 Den Administrator-Rollen MÜSSEN folgende Rechte zugewiesen sein:
- 6581 • Lokaler-Administrator:
- 6582 • ausschließlicher Zugriff über lokalen Endpunkt der Managementschnittstelle
- 6583 • Verwaltung aller Konfigurationsdaten und Durchführung aller
6584 Administratoraktionen mit Ausnahme von:
- 6585 • Benutzerverwaltung gemäß Tabelle TAB_KON_655
- 6586 • Remote-Administrator:
- 6587 • ausschließlicher Zugriff über remote-Endpunkt der Managementschnittstelle
- 6588 • Verwaltung aller Konfigurationsdaten und Durchführung aller
6589 Administratoraktionen mit Ausnahme von:
- 6590 • Benutzerverwaltung gemäß Tabelle TAB_KON_655
- 6591 • Konfigurationseinstellungen und Administratoraktionen gemäß Tabelle
6592 TAB_KON_851
- 6593 • Super-Administrator:
- 6594 • ausschließlicher Zugriff über lokalen Endpunkt der Managementschnittstelle
- 6595 • Benutzerverwaltung gemäß Tabelle TAB_KON_655
- 6596 • Verwaltung aller Konfigurationsdaten und Durchführung aller
6597 Administratoraktionen

Tabelle 355: TAB_KON_655 Konfigurationen der Benutzerverwaltung (Super-Administrator)

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
MGM_USER_LIST	Liste von Benutzernamen und deren	Liste von Benutzern und deren Kontaktdaten. Benutzerkonten MÜSSEN angelegt, geändert und gelöscht werden können.

	Kontaktdaten	Das Passwort eines Benutzerkontos MUSS neu gesetzt werden können.
MGM_ADMIN_RIGHTS	Liste von Zugriffsrechten eines Benutzers	<p>i. Eindeutige Zuordnung eines Benutzerkontos zu einer Rolle. Die Benutzerverwaltung MUSS sicherstellen, dass zu jeder Zeit mindestens ein Benutzerkonto mit der Rolle Super-Administrator vorhanden ist. Gewähren/Entziehen von Rechten für Benutzerkonten:</p> <p>ii. Zugriffsrechte bezüglich der Konfigurationsbereiche.</p> <p>iii. Recht zum Aufbau einer Remote-Management-Session und/oder zur Konfiguration des Remote-Management gemäß TAB_KON_663 (USER_INIT_REMOTESESSION).</p> <p>iv. Recht für einen Werksreset (USER_RESET_PERMISSION)</p>

6600 Die Benutzerverwaltung MUSS es jedem Benutzer ermöglichen Konfigurationsänderungen
 6601 gemäß Tabelle TAB_KON_656 vorzunehmen:
 6602

6603 **Tabelle 356: TAB_KON_656 Konfigurationen der Benutzerverwaltung**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
MGM_USER_INFO	Kontaktdaten	Der angemeldete Benutzer MUSS seine Kontaktdaten ändern können. Der Benutzername DARF NICHT änderbar sein.

6604
 6605 [\leq]

6606 4.3.2 Konnektornamen und Versionsinformationen

6607 TIP1-A_4811 - Festlegung des Konnektornamens
 6608 Der Konnektor MUSS die Konfiguration und Nutzung eines sprechenden
 6609 Konnektornamens unterstützen, der identisch zum Hostnamen des Konnektors ist. Der
 6610 Konnektornamen MUSS dauerhaft an der Managementschnittstelle angezeigt werden.
 6611 Die Managementschnittstelle MUSS es einem Administrator ermöglichen
 6612 Konfigurationsänderungen gemäß Tabelle TAB_KON_657 vorzunehmen:
 6613

6614 **Tabelle 357: TAB_KON_657 Konfigurationsparameter des Konnektornamens**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
------------	----------	---

MGM_KONN_ HOSTNAME	12 Zeichen	Der Konnektornamen MUSS folgende Anforderungen erfüllen (in Anlehnung an die Definition eines „Labels“ in [RFC1034]): <ul style="list-style-type: none"> • Verwendung der Buchstaben „A bis Z“ und „a bis z“, • Verwendung der Ziffern „0 bis 9“, • als Sonderzeichen „-“ (Minus), sowie • eine maximale Länge von 12 Zeichen, Die Verwendung weiterer Sonderzeichen sowie des Leerzeichens DARF NICHT möglich sein.
-----------------------	------------	---

6615 Optional KANN ein Hersteller zusätzlich zum Konnektor- bzw. Hostnamen die
6616 Konfiguration eines DNS-Suffixes vorsehen. Der DNS-Suffix DARF NICHT Bestandteil des
6617 Konnektornamens sein.

6618 [\leq]

6619 TIP1-A_4812 - Anzeige der Versionsinformationen (Selbstauskunft)

6620 Der Administrator MUSS die Versionsinformationen des Konnektors einsehen können.
6621 Dabei MÜSSEN alle über ProductInformation.xsd definierten Elemente verständlich
6622 angezeigt werden.

6623 Ferner MUSS der Administrator dabei die aktuelle Firmware-Gruppenversion des
6624 Konnektors einsehen können.

6625 [\leq]

6626 A_18929 - Sichtbarkeit der ECC-Vorbereitung an der Managementschnittstelle

6627 Der Hersteller MUSS die ECC-Vorbereitung der gSMC-K durch die Bezeichnung „ECC-
6628 Vorbereitet“ zusammen mit den Versionsinformationen des Konnektors an der
6629 Managementschnittstelle sichtbar machen.

6630 [\leq]

6631 TIP1-A_7255 - Anzeige von Fachmodulversionen

6632 Der Administrator MUSS die Versionen der in der Firmware des Konnektors enthaltenen
6633 Fachmodule einsehen können.

6634 [\leq]

6635 Fachmodulversionsinformationen sind nicht Bestandteil der Selbstauskunft gemäß
6636 ProductInformation.xsd.

6637 4.3.3 Konfigurationsdaten: Persistieren sowie Export-Import

6638 TIP1-A_4813 - Persistieren der Konfigurationsdaten

6639 Der Konnektor MUSS die Konfigurationsdaten nach Änderung persistieren. Dabei
6640 MÜSSEN Integrität, Authentizität und Vertraulichkeit der Konfigurationsdaten gewährt
6641 sein. Der Mechanismus hierfür ist herstellersistenspezifisch.

6642 Der Konnektor MUSS sicherstellen, dass immer ein integerer Konfigurationssatz
6643 persistiert ist.

6644 Bei der Konnektorinitialisierung MÜSSEN die persistierten Konfigurationsdaten eingelesen
6645 werden.

6646 Die Verpflichtung zur Persistierung gilt für alle innerhalb der Konnektor- und Fachmodul-
6647 Spezifikationen erhobenen Konfigurationsdaten.

6648 [\leq]

6649 TIP1-A_4814 - Export- Import von Konfigurationsdaten

6650 Der Administrator MUSS die gesamten Konfigurationsdaten des Konnektors ex- und
6651 importieren können. Dazu gehören die Konfigurationsparameter des Konnektors, die

6652 persistenten Daten wie im Informationsmodell des Konnektors (Tabelle TAB_KON_507
 6653 Informationsmodell Entitäten) definiert und die Pairing Informationen der
 6654 Kartenterminals.
 6655 Die Konfigurationsdaten des Anwendungs- und Netzkonnektors KÖNNEN gemeinsam oder
 6656 getrennt exportiert bzw. importiert werden. Das Format der Konfigurationsdaten ist
 6657 herstellerspezifisch.
 6658 Auf hardwareseitig baugleichen Geräten:

- 6659 • MUSS der Import von Konfigurationsdateien möglich sein, die unter der gleichen
 6660 oder einer früheren Firmwareversion exportiert wurden
- 6661 • SOLL der Import von Konfigurationsdateien möglich sein, die unter einer neueren
 6662 Firmwareversion exportiert wurden

6663 Der Import von Konfigurationsdateien, die von einem Konnektor mit anderer
 6664 Hardwareversion exportiert wurden, KANN ermöglicht werden.
 6665
 6666 (für Fachmodule siehe Kapitel 4.3.4)
 6667 Der Konnektor MUSS sicherstellen, dass der Exportvorgang nur von einem am Konnektor
 6668 angemeldeten User mit mindestens der Rolle Administrator ausgelöst werden kann.
 6669 Der Konnektor MUSS sicherstellen, dass der Importvorgang nur von einem am Konnektor
 6670 angemeldeten User mit der Rolle Super-Administrator ausgelöst werden kann.
 6671 Sowohl Ex- als auch Import MÜSSEN protokolliert werden durch TUC_KON_271 „Schreibe
 6672 Protokolleintrag“ {
 6673 topic = „MGM/CONFIG_EXIMPORT“;
 6674 eventType = Op;
 6675 severity = Info;
 6676 parameters = („User=\$AdminUsername,
 6677 Mode=[Export/Import]“).
 6678
 6679 **[<=]**

6680 A_19738 - Optionaler Import von Konfigurationsdaten durch lokalen Administrator
 6681 Der Konnektor KANN einem am Konnektor angemeldeten User mit der Rolle Lokaler-
 6682 Administrator erlauben, den Importvorgang von Konfigurationsdateien auszulösen, wenn
 6683 in den Konfigurationsdaten keine Benutzerdaten gemäß Tabelle TAB_KON_655 enthalten
 6684 sind. **[<=]**

6685 Nähere Vorgaben zum Ablauf des Imports der Kartenterminalinformationen finden sich
 6686 im Kapitel 4.1.4.6.3.

6687 TIP1-A_4815 - Export: Schutz der Integrität, Authentizität und Nichtabstreitbarkeit
 6688 Die **Integrität, Authentizität und Nichtabstreitbarkeit** der exportierten Daten MUSS
 6689 sichergestellt werden. Dies MUSS durch eine Signatur mit der OSIG-Identität der SM-B
 6690 oder mit einem herstellerspezifischen Schlüsselpaar realisiert werden. In die zu
 6691 signierenden Daten MUSS eine Zeitangabe zum Signaturzeitpunkt integriert werden.
 6692 Beim Import MUSS die Signatur vor der Übernahme der Daten erfolgreich verifiziert
 6693 worden sein. Im Laufe des Importvorgangs MUSS dem Administrator das zur Signatur
 6694 zugehörige Zertifikat (oder der herstellerspezifische öffentliche Schlüssel) sowie die
 6695 Zeitangabe zum Signaturzeitpunkt der exportierten Konfiguration angezeigt werden, und
 6696 der Administrator MUSS explizit bestätigen, dass er die zu dem angezeigten Zeitpunkt
 6697 gehörige Konfiguration importieren will.
 6698 Wird die SM-B zur Signatur eingesetzt, so MUSS die Prüfung des genutzten
 6699 Signaturzertifikats anhand von TUC_KON_037 erfolgen. Das Zertifikat der OSIG-
 6700 Identität, mit dem die Daten signiert wurden, MUSS zusammen mit den exportierten
 6701 Daten gespeichert werden, um eine Verifikation der Signatur auf neuen Konnektoren
 6702 auch ohne Zugriff auf die entsprechende SM-B zu ermöglichen.

6703 Da Konfigurationsdaten mit einem Schutzbedarf von mindestens „Hoch“ für Authentizität
 6704 und Nichtabstreitbarkeit exportiert werden (z. B. Pairing-Geheimnisse (ShS.KT.AUT) der
 6705 Kartenterminals), MUSS durch geeignete Maßnahmen sichergestellt werden, dass der
 6706 Zugriff auf die Daten auf eine natürliche Person rückführbar ist. Dies kann
 6707 organisatorisch (durch Einträge des Administrators in ein Betriebsführungs-Handbuch
 6708 beim Nutzer) technisch (durch eine personenbezogene Administratorenverwaltung) oder
 6709 äquivalent herstellerspezifisch erreicht werden.

6710 [**<=**]

6711 TIP1-A_4816 - Export: Schutz der Vertraulichkeit

6712 Zum Schutz der **Vertraulichkeit** der exportierten Daten MÜSSEN die Daten vor dem
 6713 Export verschlüsselt werden. Dies kann durch asymmetrische oder symmetrische
 6714 Verschlüsselungsverfahren nach [gemSpec_Krypt] realisiert werden.

6715 Wird ein rein symmetrisches Verfahren eingesetzt, so MUSS als Mindestanforderung eine
 6716 Passphrase einer Mindestlänge von 16 Zeichen (Groß- und Kleinbuchstaben, Ziffern und
 6717 Sonderzeichen) zur Verschlüsselung der Daten eingesetzt werden. Diese Passphrase
 6718 MUSS dabei vom Konnektor zufällig generiert werden und aus einer Kombination von
 6719 Buchstaben und Ziffern bestehen. Diese Passphrase MUSS dem Administrator
 6720 anschließend angezeigt werden.

6721 [**<=**]

6722 **4.3.4 Administration von Fachmodulen**

6723 Die Konfiguration von Fachmodulen ist innerhalb der Managementschnittstelle des
 6724 Konnektors von der Konfiguration der Plattformanteile des Konnektors logisch entkoppelt.
 6725 Die Festlegungen, welche Konfigurationsparameter und welche zusätzlichen
 6726 administrativen Funktionen für ein Fachmodul benötigt werden, werden in den jeweiligen
 6727 Fachmodulspezifikationen getroffen. Der Konnektor muss aber für jedes Fachmodul
 6728 hinsichtlich der Administrierbarkeit des Fachmoduls die folgende Basisfunktionalität zur
 6729 Verfügung stellen:

6730 TIP1-A_4818 - Konfigurieren von Fachmodulen

6731 Neben den Konfigurationsbereichen der Plattformanteile des Konnektors, MUSS die
 6732 Managementschnittstelle auch die Konfiguration der im Konnektor enthaltenen
 6733 Fachmodule unterstützen.

6734 Ein Administrator MUSS die in den Fachmodulspezifikationen enthaltenen
 6735 Konfigurationsparameter ändern und die dort definierten Informationen einsehen können.
 6736 Der Konnektor MUSS die Konfigurationsdaten von Fachmodulen nach deren Änderung
 6737 persistieren, sowie bei einem Neustart eines Fachmoduls die Fachmodul-
 6738 Konfigurationsdaten vor der Initialisierung des Fachmoduls einlesen.

6739 Die persistierten Fachmodulkonfigurationsdaten MÜSSEN ebenso wie die
 6740 plattformeigenen Konfigurationsdaten hinsichtlich ihrer Integrität und Authentizität sowie
 6741 ihrer Vertraulichkeit geschützt werden.

6742 Der Ex- und Import von Fachmodulkonfigurationen MUSS äquivalent zum Ex- und Import
 6743 der Plattformanteile für den Administrator möglich sein (siehe 4.3.3). Die
 6744 Konfigurationsdaten der Fachmodule KÖNNEN dabei in der Gesamt Export-Datei des
 6745 Konnektors enthalten sein oder separat exportiert und importiert werden.

6746 [**<=**]

6747 TIP1-A_5484 - Persistente Speicherung von Konfigurationsdaten der Fachmodule

6748 Der Konnektor MUSS den Fachmodulen die Möglichkeit bereitstellen, die in den
 6749 Fachmodulspezifikationen gekennzeichneten Konfigurationsdaten persistent zu speichern,
 6750 auszulesen und zu löschen. Je Fachmodul muss ein exklusiv durch das Fachmodul
 6751 nutzbarer Speicherbereich verwendet werden.

6752 Namenskonvention zur Kennzeichnung der Konfigurationsdaten der Fachmodule für

6753 persistent zu speichernde Daten:
 6754 FM_<fmName>_<fmDataName>
 6755

6756 **Tabelle 358: TAB_KON_833 Bezeichner für persistente Konfigurationsdaten für**
 6757 **Fachmodule**

Bezeichner	Bedeutung
FM	fester Namensbestandteil zur Kennzeichnung von persistenten fachmodulspezifischen Konfigurationsdaten
—	Trennzeichen
<fmName>	Name des Fachmoduls (innerhalb eines Fachmoduls konstanter Bezeichner)
—	Trennzeichen
<fmDataName>	Name der persistent zu speichernden fachmodulspezifischen Konfigurationsdaten

6758
 6759 [**<=**]

6760 4.3.5 Neustart und Werksreset

6761 TIP1-A_4819 - Auslösen eines Konnektorneustarts
 6762 Der Administrator MUSS einen Neustart des Konnektors auslösen können.
 6763 [**<=**]

6764 TIP1-A_4820 - Werksreset des Konnektors
 6765 Ein Administrator mit USER_RESET_PERMISSION MUSS einen Werksreset des
 6766 Konnektors auslösen können.
 6767 Zur Durchführung des Werksreset MUSS der Administrator nach Funktionsaufruf per
 6768 Sicherheitsabfrage zur Bestätigung des Werksresets aufgefordert werden. Nach
 6769 bestätigter Sicherheitsabfrage MUSS der Konnektor die gesamte Konfiguration des
 6770 Konnektors und alle internen Speicher, mit Ausnahme des aktuellen Vertrauensraums
 6771 sowie der Sicherheitsprotokolle und der installierten Firmware, auf den
 6772 Auslieferungszustand zurücksetzen. Die in CERT_IMPORTED_CA_LIST enthaltenen
 6773 Zertifikate MÜSSEN aus dem aktuellen Vertrauensraum gelöscht werden.
 6774 Die Durchführung des Werksresets MUSS protokolliert werden durch TUC_KON_271

6775 „Schreibe Protokolleintrag“ {
 6776 topic = „MGM/FACTORYSETTINGS“;
 6777 eventType = Op;
 6778 severity = Info;
 6779 parameters = „User=\$AdminUsername“}.

6780 Dieser Protokolleintrag DARF NICHT durch einen erfolgreichen Werksreset verloren
 6781 gehen.

6782 Der Hersteller MUSS ferner einen alternativen, herstellerspezifischen Weg zum Auslösen
 6783 des Werksresets vorsehen, welcher die Arbeitsabläufe beim Nutzer nur minimal
 6784 unterbricht. Auch für diesen zusätzlichen Weg MUSS zuvor eine Authentisierung durch
 6785 eine Kombination aus Benutzername und Passwort oder einem mindestens gleich starken
 6786 Mechanismus erfolgen. Der Mechanismus MUSS auch dann funktionieren, wenn sich
 6787 keiner der in der Benutzerverwaltung definierten Administratoren mehr erfolgreichen
 6788 anmelden kann.

6789
 6790 [**<=**]

4.3.6 Leistungsumfänge und Standalone-Szenarios

Obgleich der Konnektor in seinem Auslieferungszustand alle Leistungsmerkmale aufweisen muss, die gemäß Produktypsteckbrief gefordert werden, so soll es dem Administrator doch ermöglicht werden grundsätzliche Leistungsumfänge gezielt deaktivieren zu können, um den Konnektor so besser in die organisatorische/technische Struktur der Betriebsstätte eingliedern zu können.

TIP1-A_4821-02 - Aktivieren/Deaktivieren von Leistungsumfängen
Die Managementschnittstelle MUSS es einem Administrator ermöglichen Konfigurationsänderungen gemäß Tabelle TAB_KON_658 vorzunehmen:

Tabelle 359: TAB_KON_658 Aktivieren/Deaktivieren von Leistungsumfängen

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
MGM_LU_ONLINE	Enabled/ Disabled	Der Administrator MUSS den „Leistungsumfang Online“ aktivieren und deaktivieren können. Bei Veränderung MUSS TUC_KON_256 gerufen werden { topic = „MGM/LU_CHANGED/LU_ONLINE“; eventType = Op; severity = Info; parameters = „Active=\$MGM_LU_ONLINE“}
MGM_LU_SAK	Enabled/ Disabled	Der Administrator MUSS den „Leistungsumfang Signaturanwendungskomponente“ aktivieren und deaktivieren können. Default-Wert: Enabled Bei Veränderung MUSS TUC_KON_256 gerufen werden { topic = „MGM/LU_CHANGED/LU_SAK“; eventType = Op; severity = Info; parameters = „Active=\$MGM_LU_SAK“}

[<=]

Der Konfigurationsparameter MGM_LU_SAK wirkt hauptsächlich in dem Funktionsmerkmal „Signaturdienst“ (siehe Kapitel 4.1.8).

Ist MGM_LU_ONLINE Disabled, so baut der Konnektor grundsätzlich keine Online-Verbindungen auf (weder zur TI, noch zum SIS). Der Parameter wirkt hauptsächlich in den Funktionsmerkmalen:

- „Zertifikatsdienst“ (Kapitel 4.1.9)
- „TLS-Dienst“ (Kapitel 4.1.11)
- „Anbindung LAN/WAN“ (Kapitel 4.2.1)
- „VPN-Client“ (Kapitel 4.2.4)
- „Zeitdienst“ (Kapitel 4.2.5)
- „Software-Aktualisierungsdienst (KSR-Client)“ (Kapitel 4.3.9)

- „LDAP-Proxy“ (Kapitel 4.1.12)

Ob es sich bei einem Konnektor um den losgelöst (stand alone) vom Netz der Einsatzumgebung betriebenen handelt, also einen Konnektor, auf welchen kein Clientsystem zugreift, muss diesem mitgeteilt werden:

TIP1-A_4822 - Konnektor Standalone einsetzen

Die Managementschnittstelle MUSS es einem Administrator ermöglichen

Konfigurationsänderungen gemäß Tabelle TAB_KON_659 vorzunehmen:

Tabelle 360: TAB_KON_659 Konnektor Standalone einsetzen

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
MGM_STANDALONE_KON	Enabled/ Disabled	Der Administrator MUSS den Konnektor als alleinstehend konfigurieren können. Default-Wert: Disabled Bei Veränderung MUSS TUC_KON_256 gerufen werden { topic = „MGM/STANDALONE_CHANGED“; eventType = Op; severity = Info; parameters = „Active=\$MGM_STANDALONE_KON“}

[<=]

Das Setzen von MGM_STANDALONE_KON auf Enabled dient dem Konnektor als Anzeige, dass dieser ohne angeschlossenes Clientsystem (Primärsystem) betrieben wird. Diese Information kann seitens der Fachmodule verwendet werden, damit diese sich im Standalone-Fall anders als im Normalfall verhalten.

4.3.7 Online-Anbindung verwalten

Um Zugang zur TI erlangen zu können, muss der Betriebsstättenverantwortliche einen Vertrag mit einem Zugangsdienstprovider (ZGDP) abgeschlossen haben. Von diesem erhält er eine ContractID. Der Administrator muss den Konnektor (genauer das NK-Zertifikat C.NK.VPN) mit dieser Information unter Nutzung einer SM-B über den Registrierungsdienst des ZGDP bei diesem freischalten.

Die Berechtigung zur Einwahl in die TI ist von der Gültigkeit der **beiden** bei der Freischaltung übermittelten Zertifikate abhängig (C.NK.VPN und C.HCI.OSIG). Die Berechtigung zur Einwahl in die TI wird verweigert, bzw. eine bestehende Verbindung zur TI wird beendet, wenn ein Zertifikat abgelaufen oder gesperrt ist. Aus diesem Grund muss der Administrator vor Ablauf eines der beiden Zertifikate eine wiederholte Registrierung mit neuem Netzkonnektorzertifikat bzw. neuer SM-B beim ZGDP durchführen. (Hinweis: neue NK-Zertifikate werden erst mit Etablierung der Nachladefunktionalität für gSMC-K verfügbar sein.)

Soll ein Konnektor außer Betrieb genommen werden oder wird der Vertrag mit einem ZGDP gekündigt, muss der Administrator den Konnektor über den Registrierungsdienst des ZGDP abmelden.

TIP1-A_4824 - Freischaltdaten des Konnektors bearbeiten

Der Administrator MUSS die in TAB_KON_661 aufgelisteten Parameter über die Managementschnittstelle konfigurieren und die in TAB_KON_732 aufgelisteten Parameter ausschließlich einsehen können.

Tabelle 361: TAB_KON_661 Konfigurationsparameter der Konnektorfreischaltung

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
MGM_ZGDP_CONTRACTID	String	Der Administrator MUSS die vom Zugangsdienstprovider für die Freischaltung des Konnektors erhaltene ContractID eingeben können.
MGM_ZGDP_SMCB	ICCSN	Der Administrator MUSS die zur Freischaltung zu verwendende SM-B aus der Liste der verwalteten SM-Bs auswählen können.

Tabelle 362: TAB_KON_732 Einsehbare Konfigurationsparameter der Konnektorfreischaltung

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
MGM_ZGDP_REGSERVER	URI	URI des Registrierungsservers des Zugangsdienstproviders

Den Zustand der Freischaltung verwaltet der Konnektor gemäß Tabelle TAB_KON_662 Zustandswerte der Konnektorfreischaltung.
Im Auslieferungszustand MUSS MGM_TI_ACCESS_GRANTED=Disabled belegt sein.

Tabelle 363: TAB_KON_662 Zustandswerte der Konnektorfreischaltung

ReferenzID	Belegung	Zustandswerte
MGM_TI_ACCESS_GRANTED	Enabled/ Disabled	Status der Freischaltung des Konnektors: - Enabled: Konnektor wurde erfolgreich beim Zugangsdienstprovider freigeschaltet - Disabled: Freischaltung noch nicht erfolgt

[<=]

TIP1-A_4825 - Konnektor zur Nutzung (wiederholt) freischalten

Der Administrator MUSS den Konnektor über folgenden Mechanismus zur Nutzung freischalten bzw. eine vorhandene Freischaltung mit einer neuen SM-B aktualisieren können (Voraussetzung ist eine korrekte Konfiguration aller für einen Online-Zugang erforderlicher Parameter):

1. Der Konnektor MUSS eine registerKonnektorRequest-Struktur gemäß ProvisioningService.xsd [gemSpec_VPN_ZugD] erstellen und mit den entsprechenden Parametern befüllen (aktuelles Datum/Uhrzeit, C.NK.VPN, MGM_ZGDP_CONTRACTID). Der Konnektor MUSS die Request-Nachricht mittels der ausgewählten SM-B (ID.HCI.OSIG von MGM_ZGDP_SMCB) im Element registerKonnektorRequest/Signature signieren und das SM-B-Zertifikat im Element X509Data ablegen.

- 6876 Ist der nötige Sicherheitszustand für den privaten Schlüssel der SM-B nicht
6877 gesetzt, MUSS der Konnektor zur PIN-Verifikation an dem Kartenterminal
6878 auffordern, in dem die SM-B steckt.
- 6879 2. Der Konnektor ermittelt die URI des Registrierungsservers
6880 (MGM_ZGDP_REGSERVER) durch eine DNS-Anfrage nach dem SRV und TXT
6881 Resource Record „_regserver._tcp.<DNS_DOMAIN_VPN_ZUGD_INT>„
- 6882 3. Der Konnektor ruft unter Verwendung der erzeugten Request-Nachricht die in
6883 [gemSpec_VPN_ZugD#Tab_ZD_registerKonnektor] definierte Operation
6884 I_Registration_Service::registerKonnektor mit der Zieladresse
6885 MGM_ZGDP_REGSERVER auf.
- 6886 4. Der Konnektor zeigt dem Administrator den Inhalt von
6887 registerKonnektorResponse/AdditionalInformation und /Status an
- 6888 5. Der Response der Operation wird verarbeitet:
- 6889 a. Setze MGM_TI_ACCESS_GRANTED auf
6890 - Enabled, wenn /RegistrationStatus = „Registriert“
6891 - Disabled, wenn /RegistrationStatus = „Nicht registriert“
- 6892 b. Persistiere diese Zustandsinformation zusammen mit dem
6893 VPN:ContractStatus
- 6894 c. Verteile das folgende interne Ereignis über TUC_KON_256 {
6895 topic = "MGM/TI_ACCESS_GRANTED";
6896 eventType = Op;
6897 severity = Info;
6898 parameters = „Active=\$MGM_TI_ACCESS_GRANTED“;
6899 doDisp = false }
- 6900 Tritt während der Verarbeitungskette ein Fehler auf, so bricht die weitere Verarbeitung
6901 ab und der Administrator MUSS darüber geeignet informiert werden (u.a. Klartextanzeige
6902 des vom Registrierungsdienst gemeldeten Fehlers).
6903 Wenn eine Reregistrierung mit einer neuen SMC-B fehlschlägt (Request wird mit einem
6904 SOAP-Error beantwortet) dann ist der Konnektor nicht registriert
6905 (MGM_TI_ACCESS_GRANTED = Disabled).
6906 [**<=**]
- 6907 TIP1-A_4826 - Status Konnektorfreischaltung einsehen
6908 Der Administrator MUSS über die Managementschnittstelle den aktuellen Freischaltstatus
6909 einsehen können (MGM_TI_ACCESS_GRANTED). Ist der Konnektor aktuell freigeschaltet,
6910 so MUSS ihm dies zusammen mit dem VPN:ContractStatus angezeigt werden.
6911 [**<=**]
- 6912 Möchte ein Konnektoreigentümer das Gerät weiterveräußern oder vollständig außer
6913 Betrieb nehmen, so sollte er eine vorhandene Freischaltung zuvor rückgängig machen.
- 6914 TIP1-A_4827 - Konnektorfreischaltung zurücknehmen
6915 Ist MGM_TI_ACCESS_GRANTED=Enabled, dann MUSS der Administrator über die
6916 Managementschnittstelle des Konnektors die Freischaltung über den folgenden
6917 Mechanismus zurücknehmen können:
- 6918 1. Der Administrator MUSS eine Sicherheitsabfrage zur Zurücknahme der
6919 Freischaltung bestätigen
- 6920 2. Der Konnektor MUSS eine deRegisterKonnektorRequest-Struktur gemäß
6921 [gemSpec_VPN_ZugD] erstellen und mit den entsprechenden Parametern befüllen
6922 (aktuelles Datum/Uhrzeit, C.NK.VPN, MGM_ZGDP_CONTRACTID)

- 6923 3. Der Konnektor MUSS die Request-Nachricht mittels einer verfügbaren SM-B
 6924 (ID.HCI.OSIG) im Element deRegisterKonnektorRequest/Signature signieren.
 6925 (MGM_ZGDP_SMCB ist zu bevorzugen, es kann aber auch jede andere SM-B
 6926 verwendet werden)
 6927 Ist der nötige Sicherheitszustand für den privaten Schlüssel der SM-B nicht
 6928 gesetzt, MUSS der Konnektor zur PIN-Verifikation an dem Kartenterminal
 6929 auffordern, in dem die SM-B steckt.
- 6930 4. Der Konnektor ermittelt die URI des Registrierungsservers
 6931 (MGM_ZGDP_REGSERVER) durch eine DNS-Anfrage nach dem SRV und TXT
 6932 Resource Record „_regserver._tcp.<DNS_DOMAIN_VPN_ZUGD_INT>„
- 6933 5. Der Konnektor ruft unter Verwendung der erzeugten Request-Nachricht die in
 6934 [gemSpec_VPN_ZugD#Tab_ZD_deregisterKonnektor] definierte Operation
 6935 I_Registration_Service::deRegisterKonnektor mit der Zieladresse
 6936 MGM_ZGDP_REGSERVER auf.
- 6937 6. Der Konnektor zeigt dem Administrator den Inhalt von
 6938 deregisterKonnektorResponse/AdditionalInformation /ContractStatus und
 6939 /RegistrationStatus an
- 6940 7. Der Response der Operation wird verarbeitet:
- 6941 a. Setze MGM_TI_ACCESS_GRANTED auf
 6942 - Enabled, wenn /RegistrationStatus = „Registriert“
 6943 - Disabled, wenn /RegistrationStatus = „Nicht registriert“
- 6944 b. Persistiere diese Zustandsinformation zusammen mit dem Zeitpunkt
- 6945 c. Verteile das folgende interne Ereignis über TUC_KON_256: {
 6946 topic = "MGM/TI_ACCESS_GRANTED";
 6947 eventType = Op;
 6948 severity = Info;
 6949 parameters = „Active=\$MGM_TI_ACCESS_GRANTED“;
 6950 doDisp=false }
- 6951 Tritt während der Verarbeitungskette ein Fehler auf, so bricht die weitere Verarbeitung
 6952 ab und der Administrator MUSS darüber geeignet informiert werden (u.a. Klartextanzeige
 6953 des vom Registrierungsdienst gemeldeten Fehlers).
 6954 Wenn eine Deregistrierung mit einer neuen SMC-B fehlschlägt (Request wird mit einem
 6955 SOAP-Error beantwortet) dann ist der Konnektor weiterhin registriert
 6956 (MGM_TI_ACCESS_GRANTED = Enabled).
 6957 [**<=**]
- 6958 TIP1-A_5655 - Deregistrierung bei Außerbetriebnahme
 6959 Der Hersteller des Konnektors MUSS im Handbuch den Administrator darüber
 6960 informieren, dass der Konnektor bei dauerhafter Außerbetriebnahme (z. B. Verkauf,
 6961 Schenkung, Entsorgung) beim Zugangsdienstprovider deregistriert werden muss.
 6962 [**<=**]

6963 4.3.8 Remote Management (Optional)

6964 Im Betreibermodell der TI wird unter Remote Management ein delegierter Betrieb
 6965 dezentraler Produkte durch einen durch den Anwender beauftragten Servicepartner
 6966 verstanden. Der Servicepartner stellt als Vertragsbestandteil bevollmächtigte Personen
 6967 zur Verfügung, die sich ständig um die Betriebs- und Datensicherheit der dezentralen
 6968 Produkte im Rahmen eines Remote Managements kümmern.

- 6969 Voraussetzung für die Etablierung dieses Bestandteils des Betreibermodells der TI ist,
6970 dass ein dezentrales Produkt ein Remote Management technisch unterstützt. Die
6971 nachfolgend aufgeführten Anforderungen bilden die Grundlage für die Nutzung von
6972 Remote Management am Konnektor.
- 6973 Zum Remote Management gehören die Verwaltung von Konfigurationsdaten und die
6974 Durchführung weiterer Administratoraktionen wie z. B. die Aktualisierung der Software
6975 des Konnektors. Im Rahmen des Remote Managements kann der Konnektor Remote
6976 Monitoring unterstützen. Dazu übermittelt der Konnektor Betriebszustandsdaten an das
6977 Remote- Management-System.
- 6978 TIP1-A_7276-01 - Remote Management Konnektor
6979 Der Konnektor KANN Remote Management technisch unterstützen.
6980 Falls der Konnektor das Remote Management technisch unterstützt, MUSS der Konnektor
6981 alle Anforderungen, die das Remote Management (z.B. auch Remote-Administrator)
6982 betreffen, umsetzen.
6983 Andernfalls sind die Anforderungen, die das Remote Management (z.B. auch Remote-
6984 Administrator) betreffen, für den Konnektor nicht relevant.【<=】
- 6985
- 6986 TIP1-A_5647 - Remote Management Konnektor: Personenbezogene Daten
6987 Der Konnektor DARF über die Remote-Managementschnittstelle KEINE
6988 personenbezogenen Daten übertragen oder darstellen.
6989 【<=】
- 6990 TIP1-A_5648 - Remote Management Konnektor: Offene Schnittstelle
6991 Der Hersteller des Konnektors MUSS die zur Nutzung der Remote-
6992 Managementschnittstelle notwendigen Informationen offenlegen. Der Hersteller des
6993 Konnektors MUSS die Remote-Managementschnittstelle so spezifizieren und
6994 implementieren, dass diese auch für Dritte (z.B. einen durch den Anwender beauftragten
6995 Servicepartner) nutzbar ist.
6996 【<=】
- 6997 TIP1-A_5649 - Remote Management Konnektor: Standardbasierte Protokolle
6998 Der Hersteller des Konnektors SOLL für die Implementierung der Remote-
6999 Managementschnittstelle standardbasierte Verfahren und Protokolle einsetzen.
7000 【<=】
- 7001 TIP1-A_5650 - Remote Management Konnektor: Aufbau der Verbindung
7002 Der Konnektor MUSS sicherstellen, dass die Initiierung einer Remote-
7003 Managementverbindung im Sinne des Verbindungsaufbaus immer vom Konnektor
7004 ausgeht.
7005 【<=】
- 7006
- 7007 TIP1-A_5651 - Remote Management Konnektor: Absicherung der Verbindung
7008 Der Konnektor MUSS die Remote-Management-Verbindung durch Nutzung eines
7009 kryptographischen Verfahrens gemäß [gemSpec_Krypt] hinsichtlich Vertraulichkeit,
7010 Integrität und Authentizität absichern.
7011 【<=】
- 7012 Das Remote-Management-System authentisiert sich auf Transportebene zertifikatsbasiert
7013 gegenüber dem Konnektor.
- 7014 TIP1-A_7277 - Authentifizierung des Remote-Management-Systems
7015 Der Konnektor MUSS eine zertifikatsbasierte Authentifizierung des Remote-Management-
7016 Systems auf Transportebene durchführen.【<=】

- 7017 TIP1-A_7278 - Authentisierung des Konnektors gegenüber Remote-Management-System
 7018 Der Konnektor MUSS sich gegenüber dem Remote-Management-System zertifikatsbasiert
 7019 oder mittels Username/Password authentisieren. [<=]
- 7020 TIP1-A_7281 - Authentifizierung des Konnektors durch das Remote-Management-System
 7021 Das Remote-Management-System MUSS eine Authentifizierung des Konnektors
 7022 durchführen. [<=]
- 7023 Die Authentifizierung des Remote-Management-Systems durch den Konnektor auf
 7024 Transportebene ist verpflichtend gefordert.
- 7025 Darüber hinaus können optional Remote-Administratoren in der Benutzerverwaltung des
 7026 Konnektors konfiguriert werden. Wenn Remote-Administratoren in der
 7027 Benutzerverwaltung konfiguriert sind, muss der Konnektor diese verpflichtend auf
 7028 Anwendungsebene authentifizieren.
- 7029 Wenn kein Remote-Administrator konfiguriert ist, vertraut der Konnektor der
 7030 Benutzerverwaltung des Remote-Management-Systems. Auch wenn die Verwaltung von
 7031 Remote-Administratoren an das Remote-Management-System delegiert ist, werden alle
 7032 Zugriffe über das Remote-Management-System auf den Konnektor mit der Rolle Remote-
 7033 Administrator ausgeführt. Das Remote-Management-System muss die Authentisierung
 7034 der Remote-Administratoren und die Nachvollziehbarkeit der Zugriffe sicherstellen.
- 7035 TIP1-A_7279 - Authentifizierung des Remote-Administrators
 7036 Wenn in der Benutzerverwaltung des Konnektors Administratoren mit der Administrator-
 7037 Rolle Remote-Administrator konfiguriert sind, MUSS der Konnektor diese gemäß TIP1-
 7038 A_4808 authentifizieren. [<=]
- 7039 TIP1-A_7280 - Einschränkung der Rechte des Remote-Administrators
 7040 Der Konnektor DARF Remote-Administratoren Rechte gemäß TAB_KON_851 und
 7041 TAB_KON_655 NICHT gewähren. [<=]
- 7042
- 7043 **Tabelle 364: TAB_KON_851 Einschränkung der Rechte des Remote-Administrators**
 7044 **(Blacklist)**

Fachliche Anbindung der Clientsysteme		
TIP1-A_4517	Schlüssel und X.509-Zertifikate für die Authentisierung des Clientsystems erzeugen und exportieren sowie X.509-Zertifikate importieren	
TIP1-A_4518	Konfiguration der Anbindung Clientsysteme	
Kartendienst		
TIP1-A_5110	Übersicht über alle verfügbaren Karten	Karten vom Typ eGK und HBA DÜRFEN dem Remote-Administrator NICHT angezeigt werden
TIP1-A_5111	PIN-Management der SM-Bs für den Administrator	

Zertifikatsdienst		
TIP1-A_4704	Zertifikatsablauf anzeigen	Zertifikate von Karten vom Typ eGK und HBA DÜRFEN dem Remote-Administrator NICHT angezeigt werden
Protokollierungsdienst		
TIP1-A_4716	Einsichtnahme und Veränderung der Protokolle	Personenbezogene Daten DARF der Remote-Administrator NICHT einsehen und exportieren. Fachmodulprotokolle müssen daher entweder gesperrt, oder die personenbezogenen Daten aus diesen für den Remote-Administrator gefiltert werden.
TIP1-A_4814	Export- Import von Konfigurationsdaten	
Neustart und Werksreset		
TIP1-A_4820	Werksreset des Konnektors	

7045

7046 TIP1-A_5652 - Remote Management Konnektor: Konfiguration Remote Management
 7047 Der Konnektor MUSS sicherstellen, dass es ausschließlich einem Administrator mit einer
 7048 der Rollen {Lokaler Administrator; Super-Administrator} und dem Recht
 7049 USER_INIT_REMOTESESSION möglich ist, Konfigurationsänderungen gemäß
 7050 TAB_KON_663 vorzunehmen.

7051 **Tabelle 365: TAB_KON_663 Konfigurationen des Remote Managements**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
MGM_REMOTE_ALLOWED	Enabled/ Disabled	Der Administrator MUSS einstellen können, ob der Konnektor eine Remote-Management-Verbindung aufbauen kann, über die Konfigurationen vorgenommen werden können. Enabled: Der Konnektor kann eine Remote-Management-Verbindung aufbauen und erlaubt Konfiguration über das Remote-Management System. Disabled: Der Konnektor erlaubt keine Konfiguration über das

		Remote Management-System Default-Wert: Disabled
MGM_REMOTE_MONITORING_ALLOWED	Enabled / Disabled	<p>Der Konnektor KANN Remote-Monitoring unterstützen.</p> <p>In diesem Fall MUSS der Konnektor dem Administrator die Aktivierung und Deaktivierung des Remote-Monitoring ermöglichen.</p> <p>Enabled: Der Konnektor baut eine Remote-Managementverbindung auf.</p> <p>Der Konnektor übermittelt Betriebszustände gemäß TAB_KON_503 an das Remote-Management-System.</p> <p>Disabled: Remote-Monitoring ist deaktiviert. Der Konnektor übermittelt keine Betriebszustände an das Remote-Management-System.</p> <p>Default-Wert: Disabled</p>
Der Konnektor SOLL die Konfiguration der URL des Remote-Management-Systems, der Zertifikatsinformationen zur Authentisierung des Remote-Management-Systems und der Credentials für die Authentisierung des Konnektors beim Remote-Management-System ermöglichen.		

7052
7053
7054

[<=]

7055 TIP1-A_5653 - Remote Management Konnektor: Protokollierung Remote Management
7056 Der Konnektor MUSS im Rahmen des Remote-Managements folgende Aktionen
7057 protokollieren:

- 7058 • Beginn einer Remote-Session durch
7059 TUC_KON_271 „Schreibe Protokolleintrag“ {
7060 topic = „MGM/REMOTE_SESSION“;
7061 eventType = Op;
7062 severity = Info;
7063 parameters = („InitUser=\$AdminUsername,
7064 RemoteID=<Kennung der Gegenstelle>,
7065 Mode=[InitSuccess/InitFail]“)}
7066
- 7067 • Verbindungsabbau Remote-Session durch
7068 TUC_KON_271 „Schreibe Protokolleintrag“ {
7069 topic = „MGM/REMOTE_SESSION“;
7070 eventType = Op;
7071 severity = Info;
7072 parameters = („InitUser=\$AdminUsername,
7073 RemoteID=<Kennung der Gegenstelle>,
7074 Mode=Exit“}
7075 Die Protokollierungspflicht gilt nicht für das Remote Monitoring.
7076 Wenn ein remote-Zugriff erfolgt, ohne dass ein Remote-Administrator im
7077 Konnektor konfiguriert ist, so MUSS als InitUser eine Referenz auf das Remote-
Management-System verwendet werden.

7078 [**<=**]

7079 Ein Softwareupdate gemäß TIP1-A_5657 kann auch über das Remote Management
7080 initiiert, aktiviert und freigeschaltet werden.

7081 **4.3.9 Software- und Konfigurationsaktualisierung (KSR-Client)**

7082 Die Umsetzung des KSR-Clients bezüglich des Mechanismus zur Durchführung der
7083 Aktualisierungen, sowie die Art der Darstellung an der Managementschnittstelle sind
7084 herstellerspezifisch.

7085 Innerhalb der Software- und Konfigurationsaktualisierung (KSR-Client) werden folgende
7086 Präfixe für Bezeichner verwendet:

- 7087 • Events (Topic Ebene 1): „KSR“
- 7088 • Konfigurationsparameter: „MGM_“

7089 **4.3.9.1 Funktionsmerkmalweite Aspekte**

7090 Der Konnektor muss einen KSR-Client bereitstellen, über den der Administrator sowohl
7091 den Konnektor selbst als auch die vom Konnektor verwalteten Kartenterminals (CT-
7092 Objects in CTM_CT_LIST mit CT.CORRELATION>=„gepairt“ und
7093 CT.VALID_VERSION=True und CT.IS_PHYSICAL = Ja) softwareseitig aktualisieren kann.

7094 Weiterhin muss über den KSR-Client eine Aktualisierung von ausgewählten
7095 Konfigurationsdaten möglich sein.

7096 TIP1-A_4829 - Vollständige Aktualisierbarkeit des Konnektors

7097 Die Software-Aktualisierung des Konnektor SOLL sicherstellen, dass alle Software-
7098 Bestandteile des Konnektors aktualisiert werden können, damit eine ungehinderte
7099 Nachnutzung der Hardware-Basis im Feld mit neuen Funktionalitäten nicht durch
7100 nichtaktualisierbare Software-Bestandteile gefährdet wird. Weicht ein Hersteller für sein
7101 Konnektormodell von dieser Forderung in Teilen ab, so MUSS er im Rahmen der
7102 Zulassung nachweisen, dass dies auf Grund von Sicherheitsaspekten für sein
7103 eingereichtes Konnektormodell zwingend erforderlich ist.

7104 [**<=**]

7105 TIP1-A_5657-02 - Freischaltung von Softwareupdates

7106 Der Konnektor MUSS die Möglichkeit bieten, dass Softwareupdates durch den Nutzer
7107 bzw. einen von ihm beauftragten Administrator einzeln freigeschaltet werden.

7108 [**<=**]

7109 A_18387 - Automatische Softwareupdates

7110 Der Konnektor MUSS die Möglichkeit bieten, die automatische Installation von
7111 Softwareupdates pro Gerät (Konnektor und Kartenterminals) ein- und
7112 auszuschalten. [**<=**]

7113 A_18389 - Nur Nutzung von zugelassenen Versionen

7114 Der Hersteller des Konnektors MUSS in seinem Handbuch den Nutzer darauf hinweisen,
7115 dass er sich bei der Arbeit mit dem Konnektor vergewissern muss, dass er mit einer
7116 zugelassenen Version arbeitet und beschreiben, wie der Nutzer diese Information mittels
7117 seines Primärsystems erhalten kann.

7118 [**<=**]

7119 TIP1-A_6476 - Lieferung von Softwareupdates

7120 Der Hersteller des Konnektors MUSS jede zugelassene Firmware-Version umgehend als
7121 Update-Paket über die in [gemSpec_KSR] definierte Schnittstelle P_KSRS_Upload im
7122 Konfigurationsdienst (KSR) ablegen.

7123 Der Hersteller des Konnektors MUSS in den jeweiligen
7124 UpdateInformation/Firmware/FirmwareReleaseNotes eine Internet-URL zum Download
7125 des FW-Updates bereitstellen.

7126
7127 [\leq]

7128 TIP1-A_6026 - Anzeige URL zum Download des FW-Updates an der
7129 Managementschnittstelle
7130 Das Managementinterface des Konnektors MUSS einem authentisierten Administrator die
7131 Internet-URL zum Download des FW-Updates anzeigen.
7132 [\leq]

7133 4.3.9.2 Durch Ereignisse ausgelöste Reaktionen

7134 TIP1-A_4831 - KT-Update nach Wiedererreichbarkeit erneut anstoßen
7135 Wenn aus (TIP1-A_4840 Auslösen der durchzuführenden Updates) heraus für ein
7136 Kartenterminal noch ein ausstehendes Updates vorhanden ist, dessen
7137 Ausführungszeitpunkt nicht gesetzt oder überschritten ist, und für dieses Kartenterminal
7138 das Ereignis „CT/CONNECTED“ eintritt, so MUSS TUC_KON_281
7139 „Kartenterminalaktualisierung anstoßen“ für dieses KT gerufen werden.
7140 [\leq]

7141 4.3.9.3 Interne TUCs, nicht durch Fachmodule nutzbar

7142 4.3.9.3.1 TUC_KON_280 „Konnektoraktualisierung durchführen“

7143 TIP1-A_4832-02 - TUC_KON_280 „Konnektoraktualisierung durchführen“
7144 Der Konnektor MUSS den technischen Use Case TUC_KON_280 „Konnektoraktualisierung
7145 durchführen“ umsetzen.

7147 **Tabelle 366: TAB_KON_664 – TUC_KON_280 „Konnektoraktualisierung durchführen“**

Element	Beschreibung
Name	TUC_KON_280 „Konnektoraktualisierung durchführen“
Beschreibung	Dieser TUC aktualisiert den Konnektor mit einem Update, dessen Update-Dateien entweder direkt übergeben oder per UpdateInformation (vom KSRS bezogen) referenziert werden
Auslöser	<ul style="list-style-type: none"> Der Administrator hat UpdateInformation zur Anwendung ausgewählt und bestätigt bzw. ein lokales Updatepaket bezogen und zur Anwendung übergeben. automatisches Softwareupdate [A_18387]
Vorbedingungen	
Eingangsdaten	<ul style="list-style-type: none"> UpdateInformation (gemäß [gemSpec_KSR#5.2]) oder <ul style="list-style-type: none"> Updatepaket (herstellerspezifisch, von lokaler Datenquelle, mit enthaltenen FirmwareFiles)
Komponenten	Konnektor, Konfigurationsdienst

Ausgangsdaten	Keine
Nachbedingungen	Der Konnektor arbeitet basierend auf der übergebenen, im Updatepaket enthaltenen neuen Version.
Standardablauf	<p>Der Konnektor MUSS die zur Anwendung übergebene UpdateInformation wie folgt anwenden:</p> <ol style="list-style-type: none"> 1. Integrität und Authentizität der UpdateInformation prüfen (Mechanismus ist herstellerspezifisch) 2. Download aller in UpdateInformation.FirmwareFiles gelisteten Dateien. Dabei wird die Komprimierung des File Transfers vom Konfigurationsdienst über http „Content Coding“ [RFC2616] „gzip“ genutzt. 3. Integrität und Authentizität jeder der via UpdateInformation/FirmwareFiles heruntergeladenen Dateien prüfen (Mechanismus ist herstellerspezifisch) 4. Prüfen auf Zulässigkeit des Updates basierend auf der Firmware-Gruppe (siehe [gemSpec_OM#2.5]) 5. Anwenden der zur Verfügung stehenden FirmwareFiles <ol style="list-style-type: none"> a. TUC_KON_256{ <pre> topic = „KSR/UPDATE/START“; eventType = Sec; severity = Info; parameters = („Target=Konnektor, Name=\$MGM_KONN_HOSTNAME“)} (betroffene Fachmodule und Basisdienste reagieren und stoppen sich) </pre> b. Herstellerspezifischer Mechanismus zur Aktualisierung der internen Konnektorsoftware durch die FirmwareFiles inklusive anschließender Prüfung auf Erfolg. c. Bestehende Konfigurationsdaten des Konnektors MÜSSEN erhalten bleiben und sofern erforderlich und möglich automatisch auf die Definitionen der neuen Firmware angepasst werden. d. Ist ein händischer Anpassungs- oder Ergänzungsbedarf der Konfigurationsdaten erforderlich, so MUSS der Administrator hierüber geeignet informiert werden e. TUC_KON_256 { <pre> topic = „KSR/UPDATE/SUCCESS“; eventType = Sec; severity = Info; parameters = („Target=Konnektor, Name= \$MGM_KONN_HOSTNAME, NewFirmwareversion = UpdateInformation.FirmwareVersio n, </pre>

	<p>ConfigurationChanged=<Ja/Nein>, ManualInputNeeded=<Ja/Nein>„) }</p> <p>Der TUC endet in jedem Fall mit:</p> <pre>TUC_KON_256 { topic = „KSR/UPDATE/END“; eventType = Sec; severity = Info; parameters = („Target=Konnektor, Name=\$MGM_KONN_HOSTNAME“) }</pre> <p>(betroffene Fachmodule und Basisdienste reagieren und starten sich)</p>
Varianten/Alternativen	Sofern direkt ein Updatepaket (mit enthaltenen FirmwareFiles) übergeben wurde beginnt der Ablauf ab Nummer 4 mit der Integritätsprüfung des Updatepakets
Fehlerfälle	<p>Fehler in den folgenden Schritten des Ablaufs führen zu:</p> <p>a) Aufruf von TUC_KON_256 { topic = „KSR/ERROR“; eventType = \$ErrorType; severity = \$Severity; parameters = („Target=Konnektor, Name= \$MGM_KONN_HOSTNAME, Error=\$Fehlercode, Bedeutung=\$Fehlertext“) }</p> <p>b) Abbruch der Verarbeitung mit den ausgewiesenen Fehlercodes</p> <p>(→1) Integritätsprüfung UpdateInformation fehlgeschlagen, Fehlercode: 4181 (→2) Fehler bei der Downloaddurchführung, Fehlercode: 4182 (→3) Integritätsprüfung eines FirmwareFiles fehlgeschlagen, Fehlercode: 4183 (→4) Firmwaregruppenprüfung fehlgeschlagen, Fehlercode: 4185 (→5b) Interne Aktualisierung fehlgeschlagen, dann: 1. Rollback auf vorherige Version 2. Abbruch mit Fehlercode: 4184</p>
Nichtfunktionale Anforderungen	Der laufende Updatevorgang MUSS in der Managementschnittstelle ausgewiesen und der Fortschritt mindestens für die Schritte 1-5b dargestellt werden.
Zugehörige Diagramme	Abbildung PIC_KON_105 Aktivitätsdiagramm Konnektoraktualisierung durchführen

7148
7149

Tabelle 367: TAB_KON_665 Fehlercodes TUC_KON_280 „Konnektoraktualisierung durchführen“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			

4181	Security	Error	Integritätsprüfung UpdateInformation fehlgeschlagen.
4182	Security	Error	Download nicht aller UpdateFiles möglich.
4183	Security	Error	Integritätsprüfung UpdateFiles fehlgeschlagen.
4184	Security	Error	Anwendung der UpdateFiles fehlgeschlagen (<Details>).
4185	Security	Error	Firmware-Version liegt außerhalb der gültigen Firmware-Gruppe

7150
7151

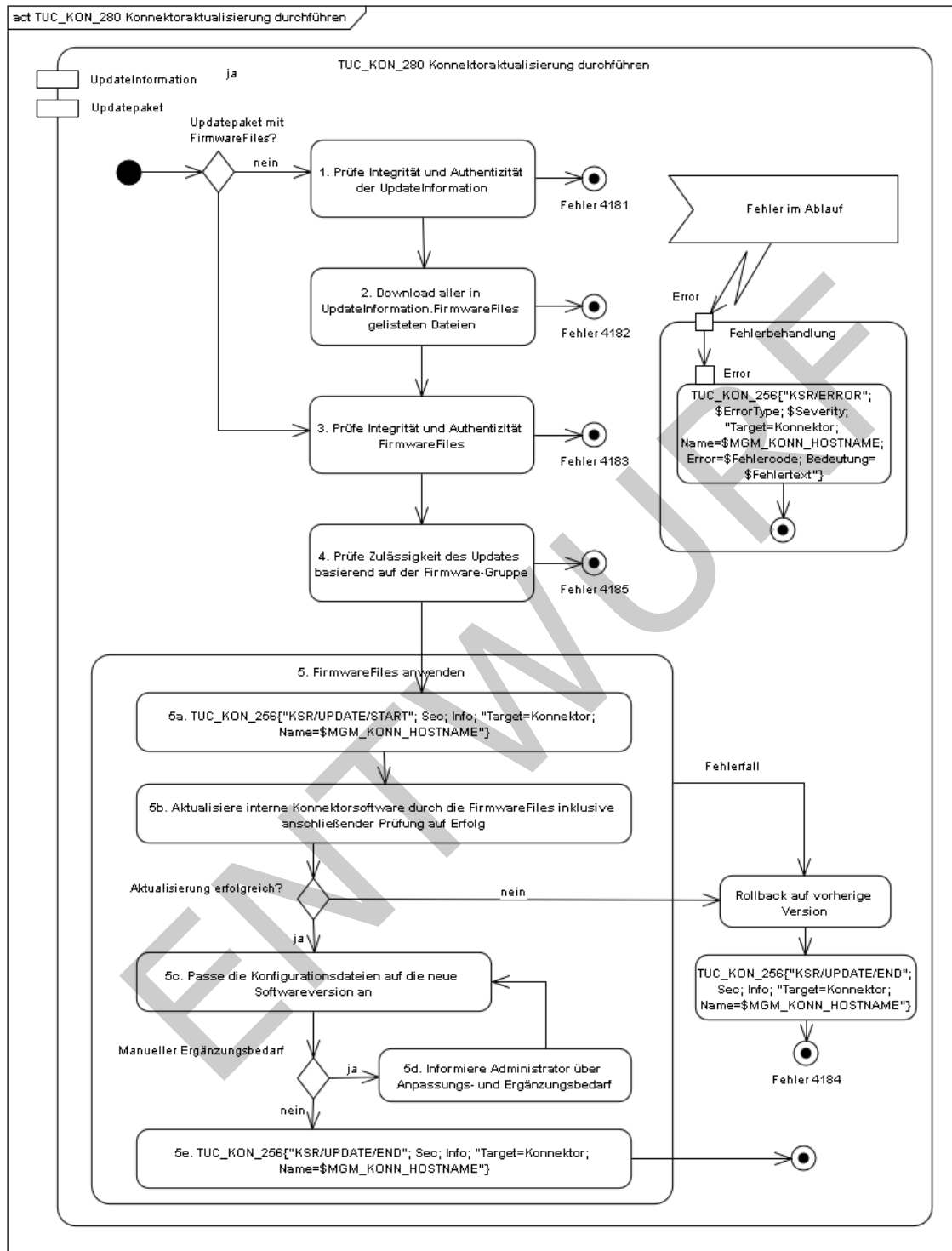


Abbildung 22: PIC_KON_105 Aktivitätsdiagramm Konnektoraktualisierung durchführen

[<=]

7152
7153
7154
7155

7156 4.3.9.3.2 TUC_KON_281 „Kartenterminalaktualisierung anstoßen“

7157 Im Vergleich zur Durchführung des Konnektor-Update (TUC_KON_280), werden die
7158 Updates der Kartenterminals nur durch den Konnektor initiiert. Der Konnektor liefert dem
7159 Kartenterminal das Updatefile, der eigentliche Updatevorgang (inklusive der Prüfung des
7160 Updatepakets auf Integrität und Authentizität) erfolgt ausschließlich und
7161 eigenverantwortlich auf Seiten des Kartenterminals.

7162 TIP1-A_4833-02 - TUC_KON_281 „Kartenterminalaktualisierung anstoßen“

7163 Der Konnektor MUSS den technischen Use Case TUC_KON_281

7164 „Kartenterminalaktualisierung anstoßen“ umsetzen.

7165

7166 **Tabelle 368: TAB_KON_666 – TUC_KON_281 „Kartenterminalaktualisierung anstoßen“**

Element	Beschreibung
Name	TUC_KON_281 „Kartenterminalaktualisierung anstoßen“
Beschreibung	Dieser TUC fordert ein Kartenterminal auf einen Update durchzuführen, dessen Update-Dateien entweder direkt übergeben oder per UpdateInformation (vom KSRS bezogen) referenziert werden
Auslöser	<ul style="list-style-type: none"> Der Administrator hat UpdateInformation für ein Kartenterminal zur Anwendung ausgewählt und bestätigt bzw. ein lokales Updatepaket für ein Kartenterminal bezogen und zur Anwendung übergeben. automatisches Softwareupdate [A_18387]
Vorbedingungen	<ul style="list-style-type: none"> CT(ctId).IS_PHYSICAL=Ja CT(ctId).CORRELATION>="gepaart"
Eingangsdaten	<ul style="list-style-type: none"> ctId (ID des Ziel-KTs) UpdateInformation (gemäß [gemSpec_KSR]) oder Updatepaket (herstellerspezifisch, von lokaler Datenquelle, mit enthaltenen FirmwareFiles)
Komponenten	Konnektor, Kartenterminal
Ausgangsdaten	Keine
Nachbedingungen	Das Kartenterminal arbeitet basierend auf der übergebenen, im Updatepaket enthaltenen neuen Version.
Standardablauf	<p>Der Konnektor MUSS die zur Anwendung übergebene UpdateInformation wie folgt anwenden:</p> <ol style="list-style-type: none"> Download der in UpdateInformation/FirmwareFiles gelisteten Datei (für KT-Updates darf nur genau ein FirmwareFile angegeben werden) TUC_KON_256{ <ul style="list-style-type: none"> topic = „KSR/UPDATE/START“; eventType = Sec; severity = Info; parameters = („Target=KT, CtID=\$ctId“) }

	<p>3. Durchführen des KT-Updates durch:</p> <p>a) Wechsel in eine Admin-Session durch TUC_KON_050 „Beginne Kartenterminalsitzung“{role=„Admin“; ctId}</p> <p>b) Senden der SICCT Kommandos: SICCT CT Download INIT, SICCT CT Download DATA (Übermittlung des UpdateFiles) und SICCT CT Download FINISH an ctId</p> <p>c) TUC_KON_256{ topic = „KSR/UPDATE/SUCCESS“; eventType = Sec; severity = Info; parameters = („Target=KT, Name= \$CT.HOSTNAME, CtID = \$ctId, NewFirmwareversion = <UpdateInformation.FirmwareVersion>„,}</p> <p>Der TUC endet in jedem Fall mit:</p> <ul style="list-style-type: none"> TUC_KON_256 { topic = „KSR/UPDATE/END“; eventType = Sec; severity = Info; parameters = („Target=KT, CtID = \$ctId“) }
Varianten/Alternativen	Sofern direkt ein Updatepaket (mit enthaltenem FirmwareFile) übergeben wurde beginnt der Ablauf ab Nummer 2 mit Signalisierung des Beginns des KT-Updates
Fehlerfälle	<p>Fehler in den folgenden Schritten des Ablaufs führen zu:</p> <p>a) Aufruf von TUC_KON_256 { topic = „KSR/ERROR“; eventType = \$ErrorType; severity = \$Severity; parameters = („Target=KT, Name=\$CT.HOSTNAME, CtID = \$ctId, Error=\$Fehlercode, Bedeutung=\$Fehlertext“) }</p> <p>b) Abbruch der Verarbeitung mit den ausgewiesenen Fehlercodes (→1) Download fehlgeschlagen, Fehlercode: 4186 (→3b) SICCT-Download fehlgeschlagen, Fehlercode: 4187</p>
Nichtfunktionale Anforderungen	<p>Die Durchführung eines KT-Updates DARF die weitere Operation des Konnektors NICHT behindern (weder auf Schnittstellenebene noch in der Managementschnittstelle). Der laufende Updatevorgang eines KT MUSS in der Managementschnittstelle ausgewiesen und der Fortschritt dargestellt werden.</p> <p>Der Konnektor MUSS mindestens 5 Kartenterminal-Updates parallel durchführen können.</p>
Zugehörige Diagramme	keine

7167 **Tabelle 369: TAB_KON_667 Fehlercodes TUC_KON_281 „Kartenterminalaktualisierung**
 7168 **anstoßen“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4186	Security	Error	Download nicht aller UpdateFiles möglich.
4187	Security	Error	KT-Update fehlgeschlagen (<Fehlerinfo gemäß SICCT>)

7169
 7170 [**<=**]

7171

7172 4.3.9.3.3 TUC_KON_282 „UpdateInformationen beziehen“

7173 TIP1-A_4834 - TUC_KON_282 „UpdateInformationen beziehen“

7174 Der Konnektor MUSS den technischen Use Case TUC_KON_282 „UpdateInformationen
 7175 beziehen“ umsetzen.

7176

7177 **Tabelle 370: TAB_KON_668 – TUC_KON_282 „UpdateInformationen beziehen“**

Element	Beschreibung
Name	TUC_KON_282 „UpdateInformationen beziehen“
Beschreibung	Dieser TUC ermittelt vom zentralen Konfigurationsdienst sowohl für den Konnektor als auch für alle durch ihn verwalteten Kartenterminals die verfügbaren UpdateInformationen
Auslöser	<ul style="list-style-type: none"> • Manuell durch den Administrator • Automatisch
Vorbedingungen	Keine
Eingangsdaten	Keine
Komponenten	Konnektor, Konfigurationsdienst
Ausgangsdaten	Keine
Nachbedingungen	Der Konnektor verfügt über alle aktuellen UpdateInformationen
Standardablauf	Der Konnektor MUSS folgende Schritte durchlaufen: <ol style="list-style-type: none"> 1. Der Konnektor MUSS die TLS-Verbindungen zum Konfigurationsdienst anhand des in MGM_KSR_FIRMWARE_URL angegebenen Wertes aufbauen. Dabei MUSS er das durch den Server präsentierte Zertifikat mittels TUC_KON_037 „Zertifikat prüfen“ { <pre>certificate = C.ZD.TSL-S; qualifiedCheck = not_required; offlineAllowNoCheck = true; policyList = oid_zd_tls_s;</pre>

	<p>intendedKeyUsage= intendedKeyUsage(C.ZD.TLS-S); intendedExtendedKeyUsage = id-kp-serverAuth; validationMode = OCSP} auf Gültigkeit prüfen. Das Server-Zertifikat C.ZD.TLS-S MUSS für den Konfigurationsdienst ausgestellt sein.</p> <p>2. Der Konnektor MUSS sowohl für sich wie auch für jedes Kartenterminal (CT) aus CTM_CT_LIST mit CT.IS_PHYSICAL=Ja und CT.CORRELATION>=„gepairt“ folgende Schritte durchlaufen:</p> <p>a. Belegen von listUpdatesRequest mit den korrekten Werten für ProductVendorID, ProductCode, HardwareVersion und FirmwareVersion</p> <p>b. Aufruf von I_KSRS_Download::list_Updates</p> <p>Liefert der Aufruf mindestens eine UpdateInformation mit einer UpdateInformation/Firmware/FWVersion > aktuelle Version der Konnektorsoftware, deren UpdateInformation/Firmware/FWPriority = „Kritisch“, dann geht der Konnektor über in den Betriebszustand EC_Connector_Software_Out_Of_Date.</p> <p>Liefert der Aufruf mindestens eine UpdateInformation mit einer UpdateInformation/Firmware/FWVersion > aktuelle Version der Kartenterminalsoftware, deren UpdateInformation/Firmware/FWPriority = „Kritisch“, dann geht der Konnektor über in den Betriebszustand EC_CardTerminal_Software_Out_Of_Date.</p> <p>3. Beenden der TLS-Verbindung</p>
Varianten/Alternativen	Keine
Fehlerfälle	<p>Fehler in den folgenden Schritten des Ablaufs führen zu:</p> <p>a) Aufruf von TUC_KON_256 { topic = „KSR/ERROR“; eventType = \$ErrorType; severity = \$Severity; parameters = („Error=\$Fehlercode; Bedeutung=\$Fehlertext“)}</p> <p>b) Abbruch der Verarbeitung mit den ausgewiesenen Fehlercodes (→1) Konfigurationsdienst nicht erreichbar, Fehlercode: 4188 (→1) Serverzertifikat ist nicht C.ZD.TLS_S, Fehlercode: 4189</p>

	(→2b) Fehler beim Beziehen der Updatelisten, Fehlercode: 4190
Nichtfunktionale Anforderungen	Der Konnektor muss die Vorgaben aus [gemSpec_Krypt#3.3.2] für TLS-Verbindungen und hinsichtlich ECC-Migration die Vorgaben aus [gemSpec_Krypt#5] befolgen.
Zugehörige Diagramme	keine

7178 **Tabelle 371: TAB_KON_669 Fehlercodes TUC_KON_282 „UpdateInformationen beziehen“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases, sowie der Fehlercodes von „I_KSRS_Download::listUpdates Response“ können folgende weitere Fehlercodes auftreten:			
4188	Technical	Error	Konfigurationsdienst nicht erreichbar, konfigurierte Adresse kontrollieren.
4189	Security	Fatal	Konfigurationsdienst liefert falsches Zertifikat
4190	Technical	Error	Fehler beim Beziehen der Updatelisten

7179

7180 [\leq]

7181 4.3.9.3.4 TUC_KON_283 „Infrastruktur Konfiguration aktualisieren“

7182 TIP1-A_5153 - TUC_Kon_283 „Infrastruktur Konfiguration aktualisieren“

7183 Der Konnektor MUSS den technischen Use Case TUC_Kon_283 „Infrastruktur Konfiguration aktualisieren“ umsetzen.

7185

7186 **Tabelle 372: TAB_KON_799 – TUC_KON_283 „Infrastruktur Konfiguration aktualisieren“**

Element	Beschreibung
Name	TUC_KON_283 Infrastruktur Konfiguration aktualisieren
Beschreibung	Dieser TUC liest die Infrastrukturdaten vom KSR ein.
Auslöser	Automatisch einmal täglich; BOOTUP, Administrator
Vorbedingungen	Der TUC_KON_304 „Netzwerk-Routen einrichten“ MUSS fehlerfrei durchgelaufen sein. Der TUC_KON_321 „Verbindung zu dem VPN-Konzentrator der TI aufbauen“ MUSS fehlerfrei durchgelaufen sein.
Eingangsdaten	Keine
Komponenten	Konnektor, Konfigurationsdienst

Ausgangsdaten	Keine
---------------	-------

ENTWURF

Standardablauf	<p>Der Konnektor MUSS folgende Schritte durchlaufen:</p> <ol style="list-style-type: none"> 1. „Einlesen des Konfigurations-XML“: <ol style="list-style-type: none"> a. Der Konnektor MUSS eine TLS-Verbindung zum Konfigurationsdienst anhand des in MGM_KSR_KONFIG_URL angegebenen Parameters aufbauen. Dabei MUSS er das durch den Server präsentierte Zertifikat mittels TUC_KON_037 „Zertifikat prüfen“ { <pre> certificate = C.ZD.TLS-S; qualifiedCheck = not_required; offlineAllowNoCheck = true; policyList = oid_zd_tls_s; intendedKeyUsage = intendedKeyUsage(C.ZD.TLS-S); intendedExtendedKeyUsage = id-kp-serverAuth; validationMode = OCSP} auf Gültigkeit prüfen. Das Server-Zertifikat C.ZD.TLS-S MUSS für den Konfigurationsdienst ausgestellt sein.</pre> b. Herunterladen der Konfigurationsdaten mittels I_KSRS_Download::get_Ext_Net_Config (MGM_KSR_KONFIG_URL, „Bestandsnetze.xml“) 2. Beenden der TLS-Verbindung „Prüfen der Versionskennung auf Änderungen“: Wenn das Element /Infrastructure/Version der heruntergeladenen Datei keine höhere Versionsnummer als die aktuell im Konnektor hinterlegte Version trägt, muss der TUC ohne Fehler beendet und ein Protokolleintrag geschrieben werden: TUC_KON_271 „Schreibe Protokolleintrag“ { <pre> topic = „KSR/UPDATE_KONFIG“; eventType = Op; severity = Info; parameters = („AlteVersion=\$aktuelleVersion, NeueVersion=/Infrastructure/Version “)} </pre> 3. Aktualisieren der Gesamtnetzliste Alle in der Datei enthaltenen Netzsegmente sind nach ANLW_BESTANDSNETZE zu übernehmen. In Abhängigkeit von ANLW_IA_BESTANDSNETZE sind neue angeschlossene Netze des Gesundheitswesens mit aAdG-NetG nach ANLW_AKTIVE_BESTANDSNETZE zu übernehmen. Identifiziert wird ein Bestandsnetz hierbei an dessen ID in der Bestandsnetze.xml (<ID>). War der Aktivierungsstatus eines dieser Netze bereits durch den Administrator manuell konfiguriert, so muss dieser Status erhalten bleiben. 4. „Aktualisieren von Konfigurationsinformationen“ Haben sich Konfigurationsdaten zu einem in
----------------	--

	<p>ANLW_AKTIVE_BESTANDSNETZE gelisteten Netz verändert, so</p> <ul style="list-style-type: none">a. sind die Änderungen entsprechend zu übernehmen und zu aktivieren (Anpassung ANLW_AKTIVE_BESTANDSNETZE, DHCP_AKTIVE_BESTANDSNETZE_ROUTES, DNS_SERVERS_BESTANDSNETZE).b. alle Statusänderungen an ANLW_AKTIVE_BESTANDSNETZE sind zu protokollieren. Der Protokolleintrag je Änderung enthält den Status, <ID>, <Name> und <NetworkAddress/NetworkPrefix> als topic=KSR/UPDATE_KONFIG,protocolType=OP und protocolSeverity=INFO.c. ist anschließend TUC_KON_304 „Netzwerk-Routen einrichten“ aufzurufen <p>5. „Entfernen von nicht mehr gültigen angeschlossenen Netzen des Gesundheitswesens mit aAdG-NetG“ Ist ein Netz in der neuen Datei gegenüber der alten Datei nicht mehr vorhanden, so:</p> <ul style="list-style-type: none">a. a) sind alle diesbezüglichen Daten zu entfernen und die Änderungen direkt aktiv zu schalten (Anpassung ANLW_AKTIVE_BESTANDSNETZE, DHCP_AKTIVE_BESTANDSNETZE_ROUTES, DNS_SERVERS_BESTANDSNETZE).b. b) ist anschließend TUC_KON_304 „Netzwerk-Routen einrichten“ aufzurufen. <p>6. Protokollierung der heruntergeladenen Version von Bestandsnetze.xml durch Aufruf von TUC_KON_271 „Schreibe Protokolleintrag“ { topic = „KSR/UPDATE_KONFIG“; eventType = Op; severity = Info; parameters = („AlteVersion=\$aktuelleVersion, NeueVersion=/Infrastructure/Version “)} “)}</p>
--	---

Varianten/Alternativen	Keine
Fehlerfälle	(→ 1-5) Es ist ein unerwarteter Fehler aufgetreten; Fehlercode: 4198
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 373: Tab_Kon_726 Fehlercodes TUC_KON_283 „Infrastruktur Konfiguration aktualisieren“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4198	Technical	Error	Beim Übernehmen der angeschlossenen Netze des Gesundheitswesens mit aAdG-NetG ist ein Fehler aufgetreten.

[<=]

4.3.9.4 Interne TUCs, auch durch Fachmodule nutzbar

4.3.9.4.1 TUC_KON_285 „UpdateInformationen für Fachmodul beziehen“

TIP1-A_6018 - TUC_KON_285 „UpdateInformationen für Fachmodul beziehen“

Der Konnektor MUSS den technischen Use Case TUC_KON_285 „UpdateInformationen für Fachmodul beziehen“ umsetzen.

Tabelle 374: TAB_KON_833 – TUC_KON_285 „UpdateInformationen für Fachmodul beziehen“

Element	Beschreibung
Name	TUC_KON_285 „UpdateInformationen für Fachmodul beziehen“
Beschreibung	Dieser TUC ermittelt vom zentralen Konfigurationsdienst für ein Fachmodul die verfügbaren UpdateInformationen eines angegebenen SW-Pakets.

Auslöser	<ul style="list-style-type: none"> Aufruf durch Fachmodul
Vorbedingungen	<ul style="list-style-type: none"> Verbindung zum VPN-Konzentrator der TI wurde erfolgreich aufgebaut
Eingangsdaten	<ul style="list-style-type: none"> productVendorID [String] - (Identifiziert den Hersteller des Produkts, für welches auf Updates geprüft werden soll.) productCode [String] - (Identifiziert das Produkt zusammen mit ProductVendorID, für welches auf Updates geprüft werden soll.) hwVersion [String] (Identifiziert die Hardware zusammen mit ProductCode und ProductVendorID, für welches auf Updates geprüft werden soll. [gemSpec_OM] beschreibt dieses Element ausführlich.) fwVersion [String] aktuell im Produkt verwendete Firmwareversion <p>Hinweis: Definition von productVendorID, productCode, hwVersion, fwVersion (entspricht FWVersion) siehe [gemSpec_KSR#TIP1-A_3331]</p>
Komponenten	Konnektor, Konfigurationsdienst
Ausgangsdaten	<ul style="list-style-type: none"> listOfUpdates [listUpdatesResponse] Liste von Update Informationen der verfügbaren Pakete für das angegebene Produkt; Datentyp listUpdatesResponse definiert in Konfigurationsdienst.xsd siehe [gemSpec_KSR]
Nachbedingungen	keine
Standardablauf	<p>Der Konnektor MUSS folgende Schritte durchlaufen:</p> <ol style="list-style-type: none"> Der Konnektor MUSS die TLS-Verbindung zum Konfigurationsdienst anhand des in MGM_KSR_FIRMWARE_URL angegebenen Wertes aufbauen. Dabei MUSS er das durch den Server präsentierte Zertifikat mittels TUC_KON_037 „Zertifikat prüfen“ { certificate = C.ZD.TSL-S; qualifiedCheck = not_required; offlineAllowNoCheck = true; policyList = oid_zd_tls_s; intendedKeyUsage = intendedKeyUsage(C.ZD.TSL-S); intendedExtendedKeyUsage = id-kp-serverAuth; validationMode = OCSP} auf Gültigkeit prüfen.

	<p>Das Server-Zertifikat C.ZD.TLS-S MUSS für den Konfigurationsdienst ausgestellt sein.</p> <ol style="list-style-type: none"> 2. Belegen von listUpdatesRequest mit den korrekten Werten für ProductVendorID, ProductCode, HardwareVersion und FirmwareVersion = fwVersion 3. Aufruf von I_KSRS_Download::list_Updates gemäß [gemSpec_KSR#TIP1-A_3331] 4. Beenden der TLS-Verbindung
Varianten/Alternativen	Keine
Fehlerfälle	<p>Fehler in den folgenden Schritten des Ablaufs führen zu:</p> <p>(→1) Konfigurationsdienst nicht erreichbar, Fehlercode: 4188</p> <p>(→1) Serverzertifikat ist nicht C.ZD.TLS_S, Fehlercode: 4189</p> <p>(→3) Fehler beim Beziehen der Updatelisten, Fehlercode: 4190</p>
Nichtfunktionale Anforderungen	Der Konnektor muss die Vorgaben aus [gemSpec_Krypt#3.3.2] für TLS-Verbindungen und hinsichtlich ECC-Migration die Vorgaben aus [gemSpec_Krypt#5] befolgen.
Zugehörige Diagramme	keine

7200 **Tabelle 375: TAB_KON_834 Fehlercodes TUC_KON_285 „UpdateInformationen für**
 7201 **Fachmodul beziehen“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases, sowie der Fehlercodes von „I_KSRS_Download::listUpdates Response“ können folgende weitere Fehlercodes auftreten:			
4188	Technical	Error	Konfigurationsdienst nicht erreichbar, konfigurierte Adresse kontrollieren.
4189	Security	Fatal	Konfigurationsdienst liefert falsches Zertifikat
4190	Technical	Error	Fehler beim Beziehen der Updatelisten

7202
 7203 **[<=]**

7204 **4.3.9.4.2 TUC_KON_286 „Paket für Fachmodul laden“**

7205 **TIP1-A_6019 - TUC_KON_286 „Paket für Fachmodul laden“**

7206 Der Konnektor MUSS den technischen Use Case TUC_KON_286 „Paket für Fachmodul
 7207 laden“ umsetzen.
 7208

7209

Tabelle 376: TAB_KON_835 – TUC_KON_286 „Paket für Fachmodul laden“

Element	Beschreibung
Name	TUC_KON_286 „Paket für Fachmodul laden“
Beschreibung	Dieser TUC lädt ein bestimmtes SW-Paket für ein Fachmodul vom zentralen Konfigurationsdienst.
Auslöser	Aufruf durch Fachmodul
Vorbedingungen	<ul style="list-style-type: none"> Verbindung zum VPN-Konzentrator der TI wurde erfolgreich aufgebaut
Eingangsdaten	<ul style="list-style-type: none"> filename (Filename des SW-Pakets, welches vom KSR geladen werden soll)
Komponenten	Konnektor, Konfigurationsdienst
Ausgangsdaten	<ul style="list-style-type: none"> swPackage (das durch filename am KSR identifizierte SW-Paket wurde heruntergeladen)
Nachbedingungen	keine
Standardablauf	<ol style="list-style-type: none"> Der Konnektor MUSS die TLS-Verbindung zum Konfigurationsdienst anhand des in MGM_KSR_FIRMWARE_URL angegebenen Wertes aufbauen. Dabei MUSS er das durch den Server präsentierte Zertifikat mittels TUC_KON_037 „Zertifikat prüfen“ { certificate = C.ZD.TLS-S; qualifiedCheck = not_required; offlineAllowNoCheck = true; policyList = oid_zd_tls_s; intendedKeyUsage = intendedKeyUsage(C.ZD.TLS-S); intendedExtendedKeyUsage = id-kp-serverAuth; validationMode = OCSP} auf Gültigkeit prüfen. Das Server-Zertifikat C.ZD.TLS-S MUSS für den Konfigurationsdienst ausgestellt sein. Herunterladen der Softwarepakets swPackage mittels I_KSRS_Download::get_File (MGM_KSR_FIRMWARE_URL /\$filename) Beenden der TLS-Verbindung swPackage an Aufrufer zurückgeben
Varianten/Alternativen	keine
Fehlerfälle	(→ 1) Verbindung zum KSR konnte nicht aufgebaut werden; Fehlercode: 4188 (→ 1) Serverzertifikat ist nicht C.ZD.TLS_S, Fehlercode: 4189 (→ 2) Wenn Größe des Pakets größer als 25MB, Fehlercode: 4242

	(→ 2) Sonstige Fehler beim Download: Das Paket konnte nicht geladen werden, Fehlercode: 4238
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

7210 **Tabelle 377: TAB_KON_836 Fehlercodes TUC_KON_286 „Paket für Fachmodul laden“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4188	Technical	Error	Konfigurationsdienst nicht erreichbar, konfigurierte Adresse kontrollieren.
4189	Security	Fatal	Konfigurationsdienst liefert falsches Zertifikat
4238	Technical	Error	Der Download des Pakets vom KSR ist fehlgeschlagen.
4242	Technical	Error	Der Download des Pakets vom KSR ist fehlgeschlagen. Das Paket ist größer als 25MB.

7211
7212 [\leq]

7213 4.3.9.5 Operationen an der Außenschnittstelle

7214 Keine.

7215 4.3.9.6 Betriebsaspekte

7216 4.3.9.6.1 TUC_KON_284 KSR-Client initialisieren

7217 TIP1-A_5938 - TUC_KON_284 „KSR-Client initialisieren“

7218 Der Konnektor MUSS in der Bootup-Phase TUC_KON_284 „KSR-Client initialisieren“
7219 durchlaufen.

7220

7221 **Tabelle 378: TAB_KON_864 – TUC_KON_284 „KSR-Client initialisieren“**

Element	Beschreibung
Name	TUC_KON_284 "KSR-Client initialisieren"
Beschreibung	Der Konnektor muss während des Bootups die Downloadpunkte für Konfigurationsdaten und Firmware ermitteln.
Eingangsanforderung	Keine
Auslöser und Vorbedingungen	Bootup Verbindung zum VPN-Konzentrator TI muss aufgebaut sein
Eingangsdaten	Keine

Komponenten	Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> MGM_KSR_KONFIG_URL MGM_KSR_FIRMWARE_URL
Standardablauf	<p>- Falls MGM_LU_ONLINE=Enabled:</p> <ul style="list-style-type: none"> - Durch DNS-Anfragen an den DNS-Forwarder zur Auflösung der SRV-RR und TXT-RR mit den Bezeichnern „_ksrkongfig._tcp.ksr.<TOP_LEVEL_DOMAIN_TI>“ und „_ksrfirmware._tcp.ksr.<TOP_LEVEL_DOMAIN_TI>“ erhält der Konnektor URLs der Downloadpunkte des KSR für Konfigurationsdaten (MGM_KSR_KONFIG_URL) und für Firmware (MGM_KSR_FIRMWARE_URL).
Varianten/Alternativen	Keine
Fehlerfälle	Keine
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

7222 **Tabelle 379: TAB_KON_822 Fehlercodes TUC_KON_284 „KSR-Client initialisieren“**

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können keine weiteren Fehlercodes auftreten.			

7223

7224 [**<=**]

7225 TIP1-A_4835-02 - Konfigurationswerte des KSR-Client

7226 Der Administrator MUSS die in TAB_KON_670 aufgelisteten Parameter über die
7227 Managementschnittstelle konfigurieren und die in TAB_KON_820 aufgelisteten Parameter
7228 ausschließlich einsehen können.

7229 **Tabelle 380: TAB_KON_670 Konfigurationsparameter der Software-Aktualisierung**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
MGM_KSR_AUTODOWNLOAD	Enabled/ Disabled	Der Administrator MUSS den automatischen Download verfügbarer Update-Pakete über den Konfigurationsparameter MGM_KSR_AUTODOWNLOAD an- und abschalten können. Default-Wert: Enabled

MGM_KSR_SHOW_TRIAL_UPDATES	Enabled / Disabled	Der Administrator MUSS einschalten können, dass zusätzlich zur Anzeige von Update-Paketen für den Online-Produktivbetrieb auch die Anzeige von Erprobungs-Update-Paketen erfolgt. Wenn MGM_KSR_SHOW_TRIAL_UPDATES von Disabled auf Enabled gesetzt wird, muss ein Warnhinweis angezeigt werden, dass die Installation von Erprobungs-Update-Paketen nur für Teilnehmer der Erprobungen vorgesehen ist. Default-Wert: Disabled
MGM_KSR_AUTO_UPDATE	Enabled / Disabled	Der Administrator MUSS pro Gerät (Konnektor und Kartenterminals) das automatische Softwareupdate ein- und ausschalten können. Default-Wert: Enabled Falls MGM_KSR_AUTO_UPDATE=Enabled wird MGM_KSR_AUTODOWNLOAD=Enabled gesetzt.
MGM_KSR_AUTO_UPDATE_TIME	Wochentag / Uhrzeit Oder täglich / Uhrzeit	Der Administrator MUSS den Wochentag und die Uhrzeit einstellen können, wann automatische Softwareupdates durchgeführt werden. Als Wochentag MUSS es neben den einzelnen Wochentagen auch einen Wert für eine tägliche Prüfung auf Aktualität und gegebenenfalls Durchführung von Softwareupdates geben. Default-Wert: Montag / 1:00 Uhr

Tabelle 381: TAB_KON_820 Einsehbare Konfigurationsparameter der Software-Aktualisierung

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
MGM_KSR_KONFIG_URL	URL	SOAP-Endpunkt des Konfigurationsdienstes zum Download von Konfigurationsdaten
MGM_KSR_FIRMWARE_URL	URL	SOAP-Endpunkt des Konfigurationsdienstes zum Download der Firmware

[<=]

Hinweis: Die Adressen des Konfigurationsdienstes werden im Rahmen des VPN-Verbindungsaufbaus ermittelt (siehe [gemSpec_VPN_ZugD#5.1.1.2 TUC_VPN-ZD_0001])

TIP1-A_6025 - Zugang zur TI sperren, wenn Deadline für kritische FW-Updates erreicht
Der Konnektor MUSS täglich überprüfen, ob unter den auf die aktuelle Konnektor-Firmware anwendbaren Updates ein Update mit FWPriority = „Kritisch“ ist, dessen Deadline (entspricht UpdateInformation/DeploymentInformation/Deadline) abgelaufen ist, d.h. Deadline <= Systemzeit. In diesem Fall MUSS der Konnektor den Verbindungsaufbau zur TI Plattform verhindern, bestehende Verbindungen in die TI abbauen und den kritischen Betriebszustand EC_FW_Not_Valid_Status_Blocked annehmen.

[<=]

7245 TIP1-A_4836 - Automatische Prüfung und Download von Update-Paketen
 7246 Der Konnektor MUSS täglich die folgenden Schritte durchführen:

- 7247 1. TUC_KON_282 „UpdateInformationen beziehen“ aufrufen.
- 7248 2. pro zurück geliefertem Listeneintrag prüfen, ob eine neuere Version enthalten ist,
 7249 als auf dem zugehörigen Gerät (Konnektor selbst oder Kartenterminal) vorhanden
- 7250 3. Ist für wenigstens ein Gerät eine neuere Version vorhanden, MUSS der Konnektor
 7251 darüber via
 7252 TUC_KON_256 „Systemereignis absetzen“ {
 7253 topic = „KSR/UPDATES_AVAILABLE“;
 7254 eventType = Op;
 7255 severity = Info;
 7256 parameters = (<Param>);
 7257 doLog=false }
 7258 informieren. Je gefundenem Update MUSS <Param> mit folgenden Werten belegt
 7259 sein:
 7260 <Param> = „ProductVendorID= \$UpdateInformation/ProductVendorID;
 7261 ProductCode= \$UpdateInformation/ProductCode;
 7262 ProductName=\$UpdateInformation/ProductName;
 7263 FirmwareVersion=\$UpdateInformation/FirmwareVersion;
 7264 Deadline=\$UpdateInformation/DeploymentInformation/Deadline;
 7265 FWPriority=\$UpdateInformation/Firmware/FWPriority;
 7266 FirmwareReleaseNotes=
 7267 \$UpdateInformation/Firmware/FirmwareReleaseNotes“
- 7268 4. Die listUpdateResponse mit neueren Firmwareversionen MÜSSEN für eine spätere
 7269 Einsichtnahme durch den Administrator bereitgehalten werden (via (TIP1-A_4837)
 7270 „Übersichtsseite des KSR-Client). Ein neuerlicher Abruf dieser Informationen DARF
 7271 NICHT erforderlich sein.
- 7272 5. Sofern ein Update-Paket für den Konnektor vorliegt, MUSS der Konnektor die mit
 7273 diesem Paket gelieferten Parameter Priority (entspricht
 7274 UpdateInformation/Firmware/FWPriority) und Deadline (entspricht
 7275 UpdateInformation/DeploymentInformation/Deadline) auswerten und bei
 7276 KSR:Priority=Kritisch persistent ablegen.
- 7277 6. Sofern MGM_KSR_AUTODOWNLOAD = Enabled, MUSS der Konnektor bei Update-
 7278 Paketen, die den Konnektor selbst betreffen, das Update-Paket mit der höchsten
 7279 FirmwareVersion über I_KSRS_Download::get_Updates herunterladen.
- 7280 7. Ist der Download von Update-Paketen für den Konnektor abgeschlossen, MUSS
 7281 der Konnektor darüber via
 7282 TUC_KON_256 „Systemereignis absetzen“ {
 7283 topic = „KSR/UPDATE/KONNEKTOR_DOWNLOAD_END“;
 7284 eventType = Op;
 7285 severity = Info;
 7286 parameters = (<Param>)}
 7287 informieren. Je heruntergeladenem FW-Paket MUSS <Param> mit folgenden
 7288 Werten belegt sein:
 7289 <Param> = „ProductVendorID= \$UpdateInformation/ProductVendorID;
 7290 ProductCode= \$UpdateInformation/ProductCode;
 7291 ProductName=\$UpdateInformation/ProductName;
 7292 FirmwareVersion=\$UpdateInformation/Firmware/FWVersion;
 7293 Deadline=\$UpdateInformation/DeploymentInformation/Deadline;

7294 FWPriority=\$UpdateInformation/Firmware/FWPriority;
 7295 FirmwareReleaseNotes
 7296 =\$UpdateInformation/Firmware/FirmwareReleaseNotes"

7297 8. Sofern MGM_KSR_AUTODOWNLOAD = Enabled, SOLL der Konnektor bei Update-
 7298 Paketen, die Kartenterminals betreffen, pro KT-Modell das Update-Paket mit der
 7299 höchsten FirmwareVersion über I_KSRS_Download::get_Updates herunterladen.

7300
 7301 Der Konnektor MUSS immer nur die neusten Update-Pakete für eine Nutzung vorhalten.
 7302 Eventuell vorhandene ältere, nicht genutzte Update-Pakete KÖNNEN überschrieben
 7303 werden.[<=]

7304 TIP1-A_4836-02 - ab PTV4: Automatische Prüfung und Download von Update-Paketen
 7305 Der Konnektor MUSS täglich die folgenden Schritte durchführen:

7306 1. TUC_KON_282 „UpdateInformationen beziehen“ aufrufen.
 7307 2. pro zurück geliefertem Listeneintrag prüfen, ob eine neuere Version enthalten ist,
 7308 als auf dem zugehörigen Gerät (Konnektor selbst oder Kartenterminal) vorhanden
 7309 3. Ist für wenigstens ein Gerät eine neuere Version vorhanden, MUSS der Konnektor
 7310 darüber via
 7311 TUC_KON_256 „Systemereignis absetzen“ {
 7312 topic = „KSR/UPDATES_AVAILABLE“;
 7313 eventType = Op;
 7314 severity = Info;
 7315 parameters = (<Param>);
 7316 doLog=false }
 7317 informieren. Je gefundenem Update MUSS <Param> mit folgenden Werten belegt
 7318 sein:
 7319 <Param> = „ProductVendorID= \$UpdateInformation/ProductVendorID;
 7320 ProductCode= \$UpdateInformation/ProductCode;
 7321 ProductName=\$UpdateInformation/ProductName;
 7322 FirmwareVersion=\$UpdateInformation/FirmwareVersion;
 7323 Deadline=\$UpdateInformation/DeploymentInformation/Deadline;
 7324 FWPriority=\$UpdateInformation/Firmware/FWPriority;
 7325 FirmwareReleaseNotes=
 7326 \$UpdateInformation/Firmware/FirmwareReleaseNotes"

7327 4. Ist für wenigstens ein Gerät eine neuere Version vorhanden, MUSS der Konnektor
 7328 in den Betriebszustand EC_FW_Update_Available übergehen.

7329 5. Die listUpdateResponse mit neueren Firmwareversionen MÜSSEN für eine spätere
 7330 Einsichtnahme durch den Administrator bereitgehalten werden (via (TIP1-A_4837)
 7331 „Übersichtsseite des KSR-Client). Ein neuerlicher Abruf dieser Informationen DARF
 7332 NICHT erforderlich sein.

7333 6. Sofern ein Update-Paket für den Konnektor selbst vorliegt, MUSS der Konnektor
 7334 die mit diesem Paket gelieferten Parameter Priority (entspricht
 7335 UpdateInformation/Firmware/FWPriority) und Deadline (entspricht
 7336 UpdateInformation/DeploymentInformation/Deadline) auswerten und bei
 7337 KSR:Priority=Kritisch persistent ablegen.

7338 7. Sofern MGM_KSR_AUTODOWNLOAD = Enabled, MUSS der Konnektor bei Update-
 7339 Paketen, die den Konnektor selbst betreffen, das Updatepaket mit der höchsten
 7340 FirmwareVersion über I_KSRS_Download::get_Updates herunterladen, falls das

- 7341 Update-Paket nicht bereits von einem vorherigen Download auf dem Konnektor
7342 vorhanden ist.
- 7343 8. Sofern I_KSRS_Download::get_Updates den http Status Code 503 Server
7344 Unavailable zurückgibt, MUSS der Konnektor die Informationen aus dem
7345 zurückgegebenen Retry-After Header nutzen, um den Zeitpunkt des Retry zu
7346 bestimmen.
- 7347 9. Ist der Download von Update-Paketen für den Konnektor abgeschlossen, MUSS
7348 der Konnektor darüber via
- 7349 TUC_KON_256 „Systemereignis absetzen“ {
7350 topic = „KSR/UPDATE/KONNEKTOR_DOWNLOAD_END“;
7351 eventType = Op;
7352 severity = Info;
7353 parameters = (<Param>)}
7354 informieren. Je heruntergeladenem FW-Paket MUSS <Param> mit folgenden
7355 Werten belegt sein:
7356 <Param> = „ProductVendorID= \$UpdateInformation/ProductVendorID;
7357 ProductCode= \$UpdateInformation/ProductCode;
7358 ProductName=\$UpdateInformation/ProductName;
7359 FirmwareVersion=\$UpdateInformation/Firmware/FWVersion;
7360 Deadline=\$UpdateInformation/DeploymentInformation/Deadline;
7361 FWPriority=\$UpdateInformation/Firmware/FWPriority;
7362 FirmwareReleaseNotes
7363 =\$UpdateInformation/Firmware/FirmwareReleaseNotes“
- 7364 10. Sofern MGM_KSR_AUTODOWNLOAD = Enabled, SOLL der Konnektor bei Update-
7365 Paketen, die Kartenterminals betreffen, pro KT-Modell das Updatepaket mit der
7366 höchsten FirmwareVersion über I_KSRS_Download::get_Updates herunterladen,
7367 falls das Update-Paket nicht bereits von einem vorherigen Download auf dem
7368 Konnektor vorhanden ist.
- 7369 11. Sofern I_KSRS_Download::get_Updates den http Status Code 503 Server
7370 Unavailable zurückgibt, MUSS der Konnektor die Informationen aus dem
7371 zurückgegebenen Retry-After Header nutzen, um den Zeitpunkt des Retry zu
7372 bestimmen.
- 7373
7374 Der Konnektor MUSS immer nur die neusten Update-Pakete für eine Nutzung vorhalten.
7375 Eventuell vorhandene ältere, nicht genutzte Update-Pakete KÖNNEN überschrieben
7376 werden.
7377 Nach einem erfolgreichen Download DÜRFEN die Namen der Dateien eines Update-
7378 Paketes beim Abspeichern NICHT verändert werden.【<=】
- 7379 TIP1-A_7220 - Konnektoraktualisierung File Transfer Ranges
7380 Der Konnektor KANN für den Download von Update-Paketen über
7381 I_KSRS_Download::get_Updates die Option Range Requests [RFC7233#3.1] zur
7382 Fortsetzung von unterbrochenen Transfers nutzen.【<=】
- 7383 TIP1-A_4837 - Übersichtsseite des KSR-Client
7384 Die Administrationsoberfläche des KSR-Clients MUSS dem Administrator eine
7385 Übersichtseite anbieten, die einen Geräteeintrag für den Konnektor selbst, sowie eine
7386 Liste von Geräteeinträgen für jedes Kartenterminal (CT) aus CTM_CT_LIST mit
7387 CT.IS_PHYSICAL=Ja und CT.CORRELATION>=„gepairt“ enthält.
7388 Der Administrator MUSS die Liste der Kartenterminals nach Kartenterminalmodellen
7389 gruppieren können (gleiche Werte für ProductVendorID, ProductCode, HardwareVersion

- 7390 und FirmwareVersion).
- 7391 Je Geräteeintrag MÜSSEN die über „Automatische Prüfung und Download von Update-
- 7392 Paketen“ ermittelten listUpdatesResponse bereitstehen.
- 7393 Je Geräteeintrag MUSS die Version der aktuell installierten Software dargestellt werden.
- 7394 Sind Bestandteile der installierten Software unabhängig aktualisierbar, so MUSS für jedes
- 7395 der Bestandteile die Version angezeigt werden.
- 7396 Der Administrator MUSS eine Aktualisierung aller listUpdatesResponse über
- 7397 TUC_KON_282 „UpdateInformationen beziehen“ auslösen können.
- 7398 Geräteeinträge, die über listUpdatesResponse mit neuerer Firmwareversion als das
- 7399 zugehörige Gerät verfügen, MÜSSEN hervorgehoben werden.
- 7400 Je Geräteeintrag MUSS die Zugehörigkeit der installierten Software und der Software-
- 7401 Updates zum Online-Produktivbetrieb oder zu einer Erprobung (inklusive Name der
- 7402 Erprobung) dargestellt werden.
- 7403 [**<=**]
- 7404 TIP1-A_4838 - Einsichtnahme in Update-Informationen
- 7405 Für alle Geräteeinträge MUSS der Administrator zu den listUpdatesResponse sowohl die
- 7406 FirmwareGroupReleaseNotes als auch jedes enthaltene UpdateInformation-Element
- 7407 einsehen können. Dazu MUSS der Konnektor
- 7408 • alle Felder der Struktur verständlich umsetzen und strukturiert anzeigen (inkl. der
 - 7409 Notes für jedes Firmwarefiles- und Documentationsfiles-Element)
 - 7410 • jedes über das Documentationfiles-Element erreichbare Dokument auf
 - 7411 Anforderung des Administrator herunterladen und anzeigen. Es MÜSSEN dabei
 - 7412 mindestens die folgenden Dokumentenformate zur Anzeige gebracht werden
 - 7413 können: Text, PDF, JPEG, TIFF
- 7414 [**<=**]
- 7415 TIP1-A_4839-01 - Festlegung der durchzuführenden Updates
- 7416 Der Administrator MUSS in der Übersichtsliste einzelne Geräteeinträge bzw. Gruppen mit
- 7417 der jeweils anzuwendenden UpdateInformation für die Durchführung eines Updates
- 7418 markieren können.
- 7419 Alternativ MUSS der Administrator neben der Markierung je Geräteeintrag bzw. Gruppe
- 7420 Update-Pakete lokal einspielen können (etwa durch ein Upload- bzw. Download-Interface
- 7421 in der Administrationsoberfläche).
- 7422 Je Geräteeintrag MUSS der Administrator einen individuellen Ausführungszeitpunkt für
- 7423 die Durchführung des Updates einstellen können.
- 7424 Der Administrator MUSS für den Geräteeintrag Konnektor festlegen können, ob dieses
- 7425 Update erst gestartet werden darf, wenn zuvor alle festgelegten KT-Updates erfolgreich
- 7426 durchlaufen wurden.
- 7427 Der Administrator MUSS zu jeder Zeit die gerätebezogene Festlegung für ein Update
- 7428 ändern bzw. löschen können, sofern dieses konkrete Update noch nicht begonnen wurde.
- 7429 Je Geräteeintrag MUSS der Administrator automatische Softwareupdates aktivieren und
- 7430 deaktivieren können.
- 7431 [**<=**]
- 7432 TIP1-A_4840-01 - Manuelles Auslösen der durchzuführenden Updates
- 7433 Der Administrator MUSS für die Liste der markierten Geräteeinträge ein gesammeltes
- 7434 Update auslösen können. Dieses MUSS nach folgendem Muster ablaufen:
- 7435 1. Alle Kartenterminaleinträge abarbeiten. Pro markiertem Kartenterminal:
- 7436 • Wenn Ausführungszeitpunkt nicht gesetzt:
 - 7437 Anwenden des definierten Updates mittels TUC_KON_281
 - 7438 „Kartenterminalaktualisierung anstoßen“

7439 • Wenn Ausführungszeitpunkt gesetzt:
 7440 Anwenden des definierten Updates mittels TUC_KON_281 sobald der
 7441 Ausführungszeitpunkt erreicht ist oder, sofern der Konnektor zum
 7442 Ausführungszeitpunkt nicht in Betrieb war, überschritten wurde. Konnte das
 7443 Kartenterminal nicht erreicht werden, so MUSS das gesetzte Update im KSR-Client
 7444 für eine spätere Anwendung erhalten bleiben (wird ereignisgesteuert neu
 7445 ausgelöst).

7446 2. Sofern die KonnektorUpdate-Abhängigkeit von KT-Updates nicht gesetzt wurde
 7447 oder wenn alle vorgesehenen Kartenterminal-Updates durchgeführt wurden,
 7448 MUSS das Konnektor-Updates mittels TUC_KON_280 „Konnektoraktualisierung
 7449 durchführen“ wie folgt begonnen werden:

7450 • wenn Ausführungszeitpunkt nicht gesetzt: TUC-Aufruf direkt

7451 • wenn Ausführungszeitpunkt gesetzt: TUC-Aufruf direkt sobald der
 7452 Ausführungszeitpunkt erreicht ist oder, sofern der Konnektor zum
 7453 Ausführungszeitpunkt nicht in Betrieb war, überschritten wurde

7454 Wenn der Administrator ein Erprobungs-Update zur Installation auswählt, MUSS er über
 7455 einen Warnhinweis darüber informiert werden,

7456 • dass es sich um ein Erprobungs-Update handelt,

7457 • für welche Erprobung es vorgesehen ist,

7458 • dass das Update-Paket nur installiert werden sollte, wenn die Institution oder
 7459 Organisation des Gesundheitswesens an der Erprobung teilnimmt,

7460 dass, falls die Institution oder Organisation des Gesundheitswesens nicht an der
 7461 Erprobung teilnimmt und dennoch das Update installiert wird, es zu funktionalen
 7462 Einschränkungen des Konnektors kommen kann. [\leq]

7463 Wurde die ECC-Migration durchgeführt, so muss sichergestellt werden, dass der
 7464 Konnektor auch wieder in den ursprünglichen Zustand, d.h. den Zustand vor der ECC-
 7465 Migration (TI-Vertrauensanker für RSA und Firmware vor der ECC-Migration),
 7466 zurückgesetzt werden kann.

7467 A_18390 - Automatisches Auslösen der durchzuführenden Updates

7468 Wenn für mindestens ein Gerät das automatische Softwareupdate aktiviert ist, MUSS der
 7469 Konnektor zur MGM_KSR_AUTO_UPDATE_TIME die Updates nach folgendem Muster
 7470 durchführen:

7471 • Alle Geräte (Kartenterminals und Konnektor), für die
 7472 MGM_KSR_AUTO_UPDATE=Enabled ist, werden markiert

7473 • Alle Kartenterminaleinträge abarbeiten

7474 • Pro markiertem Kartenterminal: Anwenden des automatischen Updates mittels
 7475 TUC_KON_281 „Kartenterminalaktualisierung anstoßen“

7476 • Sofern die Konnektorupdate-Abhängigkeit von KT-Updates nicht gesetzt wurde
 7477 oder wenn alle vorgesehenen Kartenterminal-Updates durchgeführt wurden,
 7478 MUSS für einen markierten Konnektor das Konnektor-Update mittels
 7479 TUC_KON_280 „Konnektoraktualisierung durchführen“ begonnen werden.

7480 [\leq]

7481 A_18391 - Automatisches Updates nicht nachholen

7482 Sofern der Konnektor zu MGM_KSR_AUTO_UPDATE_TIME nicht in Betrieb war, DÜRFEN
 7483 die automatischen Updates später NICHT nachgeholt werden. [\leq]

7484 A_18779 - Hinweise in KSR Update Paket zu Auto-Update

7485 Wenn mit einem Update erstmalig MGM_KSR_AUTO_UPDATE=Enabled aktiv wird, MUSS
7486 der Konnektorhersteller über das entsprechende KSR-Paket den Admin an der Konnektor
7487 Oberfläche darauf hinweisen, dass mit diesem Update der automatische Softwareupdate
7488 aktiv wird.

7489 [\leq]

7490 [A 20531 - Größe der Bestandsnetze.xml](#)

7491 [Der Konnektor MUSS eine Bestandsnetze.xml mit einer Größe von mindestens 3 MByte](#)
7492 [und 2000 Netzen \(XML Element <Network>\) verarbeiten können. \[\$\leq\$ \]](#)

7493 4.3.10 Konnektorstatus

7494 TIP1-A_5542 - Konnektor, Funktion zur Prüfung der Erreichbarkeit von Systemen
7495 Der Konnektor MUSS an der Managementschnittstelle eine Funktion anbieten, die es
7496 ermöglicht die Erreichbarkeit von Systemen durch Eingabe der IP-Adresse oder des FQDN
7497 zu prüfen. Das Ergebnis des Tests MUSS angezeigt werden.

7498 [\leq]

7499 4.4 Hardware-Merkmale des Konnektors

7500 TIP1-A_4841 - Hardware für Dauerbetrieb

7501 Der Konnektor MUSS sowohl in seiner Stromversorgung als auch in seinen restlichen
7502 Hardwarekomponenten auf einen 24x7-Dauerbetrieb ausgelegt sein.

7503 Der Hersteller DARF NICHT davon ausgehen oder gar in seiner Guidance darauf
7504 verweisen, dass der Konnektor mehrere Stunden am Tag nicht betrieben wird.

7505 [\leq]

7506 Diese Anforderung verlangt keinen Schutz gegen Stromausfall in den Betriebsräumen.

7507 TIP1-A_4842 - Gehäuseversiegelung

7508 Jeder Konnektor, der als Appliance (dezidierte, geschlossene Kombination aus
7509 spezifischer Hard- und Software) ausgeprägt ist, MUSS über eine fälschungssichere
7510 Gehäuseversiegelung verfügen. Die Versiegelung MUSS so angebracht werden, dass eine
7511 Öffnung des Gehäuses nicht ohne Beschädigung des Siegels erfolgen kann.

7512 Der Konnektor MUSS die Umsetzung entsprechend der Festlegungen für das
7513 Kartenterminal nach der TR-03120 [BSI TR-03120], Kapitel bzgl. Gehäuseversiegelung 9
7514 vornehmen.

7515 Die optische Gestaltung der Siegel ist herstellerspezifisch.

7516 [\leq]

7517 Die Prüfung auf Einhaltung der Versiegelungsvorgaben erfolgt nicht im Rahmen der CC-
7518 Evaluierung, sondern im Zuge der Prüfung auf funktionale Eignung.

7519 TIP1-A_4843 - Zustandsanzeige

7520 Im Betrieb MUSS der Zustand des Konnektors erkennbar sein. Zur Anzeige des
7521 Betriebszustandes des Konnektors SOLL es eine Signaleinrichtung (z. B. über Status-
7522 LEDs) am Konnektor geben. Falls keine Signalvorrichtung am Konnektorgehäuse
7523 verwendet wird MUSS es eine softwareseitige Lösung über das Managementinterface
7524 geben. Bei verbauter Hardware-Signalgebung KANN eine softwareseitige Lösung
7525 zusätzlich angeboten werden.

7526 Es MÜSSEN mindestens folgende angezeigt werden:

- 7527 • Power ON,
- 7528 • Link Status pro physischer Netzwerkschnittstelle

- 7529 • Fehler/Kritischer Betriebszustand gemäß Kapitel 3.3

7530 Es SOLLEN folgende Zustände angezeigt werden:

- 7531 • Status pro IPsec-Verbindung

7532 [\leq]

7533 TIP1-A_4844-02 - Ethernet-Schnittstellen

7534 Der Konnektor MUSS mindestens zwei Ethernetinterfaces nach [IEEE802.3] als
7535 physikalische Schnittstellen zur Verfügung stellen.

7536 [\leq]

7537

7538 TIP1-A_4845 - Verwendungsumgebung - Klima

7539 Als normaler Einsatzort wird für den Konnektor ein Büroraum angenommen. Der
7540 Konnektor MUSS die in Tabelle TAB_KON_671 aufgeführten Anforderungen erfüllen,
7541 welche unter der Annahme des normalen Einsatzortes erhoben werden.

7542

7543 **Tabelle 382: TAB_KON_671 Anforderungen Klima**

Prüfung Klima
Trockene Wärme (Dry Heat) nach DIN EN 60068-2-2 Methode Bb wird für die Bedingungen als obere Lagertemperatur von 55°C und einer Beanspruchungsdauer von 16 h geprüft und die Funktionsfähigkeit MUSS bestätigt werden.
Kälte (Cold) nach DIN EN 60068-2-1 Methode Ab wird für die Bedingungen als untere Lagertemperatur von -10°C und einer Beanspruchungsdauer von 16 h geprüft und die Funktionsfähigkeit MUSS bestätigt werden.
Nach den beiden oben genannten Belastungen durch extreme Lagertemperaturen und der Nachbehandlungsdauer von 1 h MUSS die Funktionsfähigkeit des Konnektors gewährleistet sein, was durch Funktionsprüfungen nachzuweisen ist.
Die Funktionsfähigkeit im Betrieb MUSS bei einer oberen Temperatur von 40°C über eine Dauer von 24 h gewährleistet sein. Dies wird für den Konnektor durch Prüfung nach DIN EN 60068-2-2 Methode Bb bei gleichzeitigen Funktionsprüfungen nachgewiesen.

7544

7545 [\leq]

7546 TIP1-A_4846 - Verwendungsumgebung – Vibration

7547 Die durch Vibrationen und mechanische Schockbelastungen auftretenden Belastungen
7548 MÜSSEN vom Konnektor schadensfrei gemäß IEC 68-2 Methode nach den Anforderungen
7549 aus TAB_KON_672 absolviert, geprüft und nachgewiesen werden.

7550

7551 **Tabelle 383: TAB_KON_672 Anforderungen Vibration**

Prüfung Vibration
Sinusförmige Schwingungstests (Vibration, sinusoidal) nach DIN EN 60068-2-6 Methode Fc in drei senkrecht stehenden Achsen in einem Frequenzbereich von 2 Hz bis 200 Hz üblicherweise 1 h je Achse MÜSSEN erfolgreich nachgewiesen werden. Bis zu einer Frequenz von 9 Hz wird dabei mit einer konstanten Amplitude von 1,5 mm belastet, darüber bis zur oberen Frequenz wird mit einer konstanten Beschleunigung von 5 m/s ² (0,5 g) belastet.

Es MÜSSEN mechanische Schockprüfungen (Shock) nach DIN EN 60068-2-27 Methode Ea in drei senkrecht stehenden Achsen (sechs Richtungen) erfolgreich nachgewiesen werden. Es wird dabei für jede Achse mit 3 positiven und 3 negativen Schocks mit 150 m/s^2 (15 g) Amplitude und einer Dauer von 11 ms belastet.

Dauerschocktests (Bump) nach DIN EN 60068-2-29 Methode Eb in drei senkrecht stehenden Achsen mit halbsinusförmigen Schocks MÜSSEN erfolgreich nachgewiesen werden. Es wird dabei für jede Achse mit 1000 positiven und 1000 negativen Schocks mit 100 m/s^2 (10 g) Amplitude und einer Dauer von 16 ms belastet.

7552
7553

[<=]

7554 TIP1-A_4846-02 - ab PTV4: Verwendungsumgebung – Vibration
7555 Die durch Vibrationen und mechanische Schockbelastungen auftretenden Belastungen
7556 MÜSSEN vom Konnektor schadensfrei gemäß IEC 68-2 Methode nach den Anforderungen
7557 aus TAB_KON_672 absolviert, geprüft und nachgewiesen werden.

7558

7559 **Tabelle 384: TAB_KON_672 Anforderungen Vibration**

Prüfung Vibration

Sinusförmige Schwingungstests (Vibration, sinusoidal) nach DIN EN 60068-2-6 Methode Fc in drei senkrecht stehenden Achsen in einem Frequenzbereich von 2 Hz bis 200 Hz üblicherweise 1 h je Achse MÜSSEN erfolgreich nachgewiesen werden. Bis zu einer Frequenz von 9 Hz wird dabei mit einer konstanten Amplitude von 1,5 mm belastet, darüber bis zur oberen Frequenz wird mit einer konstanten Beschleunigung von 5 m/s^2 (0,5 g) belastet.

Es MÜSSEN mechanische Schockprüfungen (Shock) nach DIN EN 60068-2-27 Methode Ea in drei senkrecht stehenden Achsen (sechs Richtungen) erfolgreich nachgewiesen werden. Es wird dabei für jede Achse mit 3 positiven und 3 negativen Schocks mit 150 m/s^2 (15 g) Amplitude und einer Dauer von 11 ms belastet.

Dauerschocktests (Bump) nach DIN EN 60068-2-27 Methode Eb in drei senkrecht stehenden Achsen mit halbsinusförmigen Schocks MÜSSEN erfolgreich nachgewiesen werden. Es wird dabei für jede Achse mit 1000 positiven und 1000 negativen Schocks mit 100 m/s^2 (10 g) Amplitude und einer Dauer von 16 ms belastet.

7560
7561

[<=]

7562

7563

5 Anhang A – Verzeichnisse

7564

5.1 Abkürzungen

Kürzel	Erläuterung
AMTS	Arzneimitteltherapiesicherheit
APPL DO	Application Label Data Object
CC	Common Criteria
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DO	Datenobjekt
DSL	Digital Subscriber Line
ECC	Elliptic Curve Cryptography
EVG	Evaluiierungsgegenstand
gSMC-K	Security Module Card Typ K (Konnektor)
gSMC-KT	Security Module Card Typ KT (Kartenterminal)
HBA	Heilberufsausweis
HSM-B	Hardware Security Module Typ B
IAG	Internet Access Gateway
ID	Identifizier
ISP	Internet Service Provider
KT	Kartenterminal
KVK	Krankenversichertenkarte
LAN	Local Area Network
MTOM	Message Transmission Optimization Mechanism

NFDM	Notfalldatenmanagement
NK	Netzkonnektor
NTP	Network Time Protokoll
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal
PKI	Public Key Infrastructure
PP	Protection Profile
PU	Produktivumgebung
PUK	Personal Unblocking Key
QES	Qualifizierte elektronische Signatur
RU	Referenzumgebung
SIS	Secure Internet Service
SMC-B	Security Module Card Typ B
SMTBD DO	SICCT Message-To-Be-Displayed Data Object
SOAP	Standard für die Kommunikation innerhalb der WEB-Services
TI	Telematikinfrastruktur
TLS	Transport Layer Security
TSF	TOE Security Functionality
TU	Testumgebung
TUC	Technischer Use Case
URL	Uniform Resource Locator
VPN	Virtual Private Network

VSDM	Versichertenstammdatenmanagement
VZD	Verzeichnisdienst
WAN	Wide Area Network
XML	Extensible Markup Language
ZD	Zertifizierungsdienst
ZOD 2.0	Zahnärzte Online Deutschland 2.0

5.2 Glossar

Begriff	Erläuterung
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.

Das Glossar wird als eigenständiges Dokument, vgl. [gemGlossar] zur Verfügung gestellt.

5.3 Abbildungsverzeichnis

Abbildung 1: PIC_KON_116 Schnittstellen des Konnektors von und zu anderen Produkttypen	30
Abbildung 2: PIC_KON_117 Logische Zerlegung des Konnektors in Anwendungs- und Netzkonnektor	32
Abbildung 3: PIC_KON_107 XML Struktur des Status Elements einer SOAP Antwort	65
Abbildung 4: PIC_Kon_100 Informationsmodell des Konnektors	72
Abbildung 5: PIC_KON_101 Aufrufkontext der Operation	82
Abbildung 6: PIC_KON_118 Aktivitätsdiagramm zu „TUC_KON_000 Prüfe Zugriffsberechtigung“	86
Abbildung 7: PIC_KON_071 Korrelationszustände eines eHealth-KT	108
Abbildung 8: PIC_KON_110 Aktivitätsdiagramm zu „Beginne Kartenterminalsitzung“ ..	117
Abbildung 9: PIC_KON_057 Aktivitätsdiagramm zu „Paare Kartenterminal“	124
Abbildung 10: PIC_KON_111 Aktivitätsdiagramm zu „PIN verifizieren“	163
Abbildung 11: PIC_KON_022 Grundsätzlicher Aufbau der Ereignisnachricht	235
Abbildung 12: PIC_KON_112 Aktivitätsdiagramm zu „Systemereignis absetzen“	242
Abbildung 13: PIC_KON_058 Aktivitätsdiagramm „Daten hybrid verschlüsseln“	279
Abbildung 14: PIC_KON_059 Aktivitätsdiagramm „Daten hybrid entschlüsseln“	285
Abbildung 15: PIC_KON_103 Use Case Diagramm Signaturdienst (nonQES)	318

7586	Abbildung 16: PIC_KON_104 Use Case Diagramm Signaturdienst (QES)	319
7587	Abbildung 17: PIC_KON_102 Use Case Diagramm Signaturdienst (Komfortsignatur)...	319
7588	Abbildung 18: PIC_KON_113 Aktivitätsdiagramm zu „QES-Signaturen erstellen“	330
7589	Abbildung 19: PIC_KON_114 Aktivitätsdiagramm zu „Dokument QES signieren“	354
7590	Abbildung 20: PIC_KON_118 Aufbau und Struktur der Protokolldateien für Plattform und	
7591	Fachmodule	448
7592	Abbildung 21: PIC_KON_115 Kommunikationsregeln Konnektor	470
7593	Abbildung 22: PIC_KON_105 Aktivitätsdiagramm Konnektoraktualisierung durchführen	
7594	547
7595	Abbildung 23: PIC_KON_120 Abbildung von CardSessions auf logische Kanäle	657
7596	Abbildung 24: PIC_KON_007 Übersicht Zeichensatz ISO646DE/DIN66003	659
7597	Abbildung 25: Szenario einer einfachen Installation	661
7598	Abbildung 26: Szenario einer Installation mit mehreren Behandlungsräumen	663
7599	Abbildung 27: Szenario einer Integration der TI Produkte in eine bestehende	
7600	Infrastruktur	664
7601	Abbildung 28: Szenario einer Integration der TI Produkte in eine bestehende	
7602	Infrastruktur mit existierendem Router	666
7603	Abbildung 29: Szenario mit zentral gesteckten HBA und SMC-B	667
7604	Abbildung 30: Szenario mit zentralem Primärsystem als Clientsystem	669
7605	Abbildung 31: Szenario für den Zugriff	671
7606	Abbildung 32: Standalone-Szenario mit physischer Trennung im Konnektor	673
7607	Abbildung 1: PIC_KON_116 Schnittstellen des Konnektors von und zu anderen	
7608	Produkttypen	30
7609	Abbildung 2: PIC_KON_117 Logische Zerlegung des Konnektors in Anwendungs- und	
7610	Netzkonnektor	32
7611	Abbildung 3: PIC_KON_107 XML-Struktur des Status-Elements einer SOAP-Antwort	65
7612	Abbildung 4: PIC_KON_100 Informationsmodell des Konnektors	72
7613	Abbildung 5: PIC_KON_101 Aufrufkontext der Operation	82
7614	Abbildung 6: PIC_KON_118 Aktivitätsdiagramm zu „TUC_KON_000 Prüfe	
7615	Zugriffsberechtigung“	86
7616	Abbildung 7: PIC_KON_071 Korrelationszustände eines eHealth-KT	108
7617	Abbildung 8: PIC_KON_110 Aktivitätsdiagramm zu „Beginne Kartenterminalsitzung“ ..	117
7618	Abbildung 9: PIC_KON_057 Aktivitätsdiagramm zu „Paire Kartenterminal“	124
7619	Abbildung 10: PIC_KON_111 Aktivitätsdiagramm zu „PIN verifizieren“	163
7620	Abbildung 11: PIC_KON_022 Grundsätzlicher Aufbau der Ereignisnachricht	235
7621	Abbildung 12: PIC_KON_112 Aktivitätsdiagramm zu „Systemereignis absetzen“	242
7622	Abbildung 13: PIC_KON_058 Aktivitätsdiagramm „Daten hybrid verschlüsseln“	279
7623	Abbildung 14: PIC_KON_059 Aktivitätsdiagramm „Daten hybrid entschlüsseln“	285
7624	Abbildung 15: PIC_KON_103 Use Case Diagramm Signaturdienst (nonQES)	318

7625	Abbildung 16: PIC KON 104 Use Case Diagramm Signaturdienst (QES)	319
7626	Abbildung 17: PIC KON 102 Use Case Diagramm Signaturdienst (Komfortsignatur) ...	319
7627	Abbildung 18: PIC KON 113 Aktivitätsdiagramm zu „QES Signaturen erstellen“	330
7628	Abbildung 19: PIC KON 114 Aktivitätsdiagramm zu „Dokument QES signieren“	354
7629	Abbildung 20: PIC KON 118 Aufbau und Struktur der Protokolldateien für Plattform und	
7630	Fachmodule	448
7631	Abbildung 21: PIC KON 115 Kommunikationsregeln Konnektor	470
7632	Abbildung 22: PIC KON 105 Aktivitätsdiagramm Konnektoraktualisierung durchführen	
7633	547
7634	Abbildung 23: PIC KON 120 Abbildung von CardSessions auf logische Kanäle	657
7635	Abbildung 24: PIC KON 007 Übersicht Zeichensatz ISO646DE/DIN66003	659
7636	Abbildung 25: Szenario einer einfachen Installation	661
7637	Abbildung 26: Szenario einer Installation mit mehreren Behandlungsräumen	663
7638	Abbildung 27: Szenario einer Integration der TI Produkte in eine bestehende	
7639	Infrastruktur	664
7640	Abbildung 28: Szenario einer Integration der TI Produkte in eine bestehende	
7641	Infrastruktur mit existierendem Router	666
7642	Abbildung 29: Szenario mit zentral gesteckten HBA und SMC-B	667
7643	Abbildung 30: Szenario mit zentralem Primärsystem als Clientsystem	669
7644	Abbildung 31: Szenario für den Zugriff	671
7645	Abbildung 32: Standalone-Szenario mit physischer Trennung im Konnektor	673
7646		

7647 5.4 Tabellenverzeichnis

7648	Tabelle 1: TAB_KON_500 Wertetabelle Kartentypen	38
7649	Tabelle 2: TAB_KON_856: Identitäten des Konnektors auf der gSMC-K	40
7650	Tabelle 3: TAB_KON_503 Betriebszustand_Fehlerzustandsliste	45
7651	Tabelle 4: TAB_KON_504 Ausführungserlaubnis für Dienste in kritischen Fehlerzuständen	
7652	51
7653	Tabelle 5: TAB_KON_502 Fehlercodes „Betriebszustand“	57
7654	Tabelle 6: TAB_KON_505 Konfigurationswerte Missbrauchserkennung	57
7655	Tabelle 7: TAB_KON_852 Konfigurationsvarianten der Verbindungen zwischen Konnektor	
7656	und Clientsystemen	60
7657	Tabelle 8: TAB_KON_506 Konfigurationsparameter der Clientsystem Authentisierung ...	62
7658	Tabelle 9: TAB_KON_812 Umgebungsabhängige Konfigurationsparameter	68
7659	Tabelle 10: TAB_KON_507 Informationsmodell Entitäten	72
7660	Tabelle 11: TAB_KON_508 Informationsmodell Attribute	76
7661	Tabelle 12: TAB_KON_509 Informationsmodell Entitätenbeziehungen	77

7662	Tabelle 13: TAB_KON_510 Informationsmodell Constraints.....	79
7663	Tabelle 14: TAB_KON_511 — TUC_KON_000 „Prüfe Zugriffsberechtigung“	82
7664	Tabelle 15: TAB_KON_512 Zugriffsregeln-Beschreibung	85
7665	Tabelle 16: TAB_KON_513 Zugriffsregeln-Regelzuordnung.....	87
7666	Tabelle 17: TAB_KON_514-01 Zugriffsregeln-Definition	88
7667	Tabelle 18: TAB_KON_515 Fehlercodes TUC_KON_000 „Prüfe Zugriffsberechtigung“	92
7668	Tabelle 19: TAB_KON_143 — TUC_KON_080 „Dokument validieren“	94
7669	Tabelle 20: TAB_KON_144 Fehlercodes TUC_KON_080 „Dokument validieren“	96
7670	Tabelle 21: TAB_KON_516 Basisanwendung Dienstverzeichnisdienst	98
7671	Tabelle 22: TAB_KON_517 Schemabeschreibung Produktinformation	
7672	(ProductInformation.xsd)	99
7673	Tabelle 23: TAB_KON_518 Schemabeschreibung Serviceinformation	
7674	(Serviceinformation.xsd)	100
7675	Tabelle 24: TAB_KON_519 — TUC_KON_041 „Einbringen der Endpunktinformationen	
7676	während der Bootup-Phase“	101
7677	Tabelle 25: TAB_KON_520 Fehlercodes TUC_KON_041 „Einbringen der	
7678	Endpunktinformationen während der Bootup-Phase“	102
7679	Tabelle 26: TAB_KON_521 Schnittstelle der Basisanwendung Dienstverzeichnisdienst	102
7680	Tabelle 27: TAB_KON_522 Parameterübersicht des Kartenterminaldienstes	104
7681	Tabelle 28: TAB_KON_785 Erlaubte SICCT-Kommandos bei CT.CONNECTED=Nein	109
7682	Tabelle 29: TAB_KON_727 Terminalanzeigen beim Anfordern und Auswerfen von Karten	
7683	110
7684	Tabelle 30: TAB_KON_039 — TUC_KON_050 „Beginne Kartenterminalsitzung“	112
7685	Tabelle 31: TAB_KON_523 Fehlercodes TUC_KON_050 „Beginne Kartenterminalsitzung“	
7686	118
7687	Tabelle 32: TAB_KON_524 — TUC_KON_054 „Kartenterminal hinzufügen“	118
7688	Tabelle 33: TAB_KON_525 Fehlercodes TUC_KON_054 „Kartenterminal hinzufügen“	120
7689	Tabelle 34: TAB_KON_041 — TUC_KON_053 „Paare Kartenterminal“	120
7690	Tabelle 35: TAB_KON_113 Fehlercodes TUC_KON_053 „Paare Kartenterminal“	123
7691	Tabelle 36: TAB_KON_526 — TUC_KON_055 „Befülle CT-Object“	125
7692	Tabelle 37: TAB_KON_112 — TUC_KON_051 „Mit Anwender über Kartenterminal	
7693	interagieren“	126
7694	Tabelle 38: TAB_KON_114 Fehlercodes TUC_KON_051 „Mit Anwender über	
7695	Kartenterminal interagieren“	128
7696	Tabelle 39: TAB_KON_723 — TUC_KON_056 „Karte anfordern“	129
7697	Tabelle 40: TAB_KON_724 Fehlercodes TUC_KON_056 „Karte anfordern“	131
7698	Tabelle 41: TAB_KON_725 — TUC_KON_057 „Karte auswerfen“	131
7699	Tabelle 42: TAB_KON_796 Fehlercodes TUC_KON_057 „Karte auswerfen“	133
7700	Tabelle 43: TAB_KON_854 — TUC_KON_058 „Displaygröße ermitteln“	134

7701	Tabelle 44: TAB_KON_855 Fehlercodes TUC_KON_058 „Displaygröße ermitteln“	135
7702	Tabelle 45: TAB_KON_722 Basisdienst Kartenterminaldienst	135
7703	Tabelle 46: TAB_KON_716 Operation RequestCard	135
7704	Tabelle 47: TAB_KON_717 Ablauf RequestCard	137
7705	Tabelle 48: TAB_KON_718 Fehlercodes „RequestCard“	137
7706	Tabelle 49: TAB_KON_719 Operation EjectCard	138
7707	Tabelle 50: TAB_KON_720 Ablauf EjectCard	139
7708	Tabelle 51: TAB_KON_721 Fehlercodes Operation „EjectCard“	140
7709	Tabelle 52: TAB_KON_527 Konfigurationswerte eines Kartenterminalobjekts	140
7710	Tabelle 53: TAB_KON_528 Informationsparamter des Kartenterminaldienstes	141
7711	Tabelle 54: TAB_KON_529 Anzeigewerte zu einem Kartenterminalobjekt	142
7712	Tabelle 55: TAB_KON_530 Konfigurationswerte eines Kartenterminalobjekts	144
7713	Tabelle 56: TAB_KON_531 Parameterübersicht des Kartendienstes	147
7714	Tabelle 57: TAB_KON_090 Terminalanzeigen beim Eingeben der PIN am Kartenterminal	
7715	150
7716	Tabelle 58: TAB_KON_734 — TUC_KON_001 „Karte öffnen“	155
7717	Tabelle 59: TAB_KON_735 — TUC_KON_026	158
7718	Tabelle 60: TAB_KON_824 Fehlercodes TUC_KON_026 „Liefere CardSession“	159
7719	Tabelle 61: TAB_KON_087 — TUC_KON_012 „PIN verifizieren“	159
7720	Tabelle 62: TAB_KON_089 Fehlercodes TUC_KON_012 „PIN verifizieren“	163
7721	Tabelle 63: TAB_KON_736 — TUC_KON_019 „PIN ändern“	164
7722	Tabelle 64: TAB_KON_093 Fehlercodes TUC_KON_019 „PIN ändern“	167
7723	Tabelle 65: TAB_KON_236 — TUC_KON_021 „PIN entsperren“	168
7724	Tabelle 66: TAB_KON_193 Fehlercodes TUC_KON_021 „PIN entsperren“	171
7725	Tabelle 67 TAB_KON_532 — TUC_KON_022 „Liefere PIN-Status“	172
7726	Tabelle 68: TAB_KON_091 Fehlercodes TUC_KON_022 „Liefere PIN-Status“	174
7727	Tabelle 69: TAB_KON_240 — TUC_KON_027 „PIN-Schutz ein-/ausschalten“	174
7728	Tabelle 70: TAB_KON_838 Mapping von pinRef auf ANW	177
7729	Tabelle 71: TAB_KON_241 Fehlercodes TUC_KON_027 „PIN-Schutz ein-/ausschalten“ ..	177
7730	Tabelle 72: TAB_KON_533 — TUC_KON_023 „Karte reservieren“	178
7731	Tabelle 73: TAB_KON_534 Fehlercodes TUC_KON_023 „Karte reservieren“	179
7732	Tabelle 74: TAB_KON_096 — TUC_KON_005 „Card-to-Card authentisieren“	180
7733	Tabelle 75: TAB_KON_673 AuthMode für C2C	182
7734	Tabelle 76: TAB_KON_674 Erlaubte Parameterkombinationen und resultierende CV-	
7735	Zertifikate für C2C	183
7736	Tabelle 77: TAB_KON_535 Fehlercodes TUC_KON_005 „Card-to-Card authentisieren“	183
7737	Tabelle 78: TAB_KON_218 — TUC_KON_202 „LeseDatei“	184

7738	Tabelle 79: TAB_KON_536 Fehlercodes TUC_KON_202 „LeseDatei“	185
7739	Tabelle 80: TAB_KON_219 — TUC_KON_203 „SchreibeDatei“	186
7740	Tabelle 81: TAB_KON_537 Fehlercodes TUC_KON_203 „SchreibeDatei“	187
7741	Tabelle 82: TAB_KON_204 — TUC_KON_204 „LöscheDateiInhalt“	188
7742	Tabelle 83: TAB_KON_785 Fehlercodes TUC_KON_204 „LöscheDateiInhalt“	189
7743	Tabelle 84: TAB_KON_538 — TUC_KON_209 „LeseRecord“	190
7744	Tabelle 85: TAB_KON_539 Fehlercodes TUC_KON_209 „LeseRecord“	191
7745	Tabelle 86: TAB_KON_224 — TUC_KON_210 „SchreibeRecord“	192
7746	Tabelle 87: TAB_KON_540 Fehlercodes TUC_KON_210 „SchreibeRecord“	193
7747	Tabelle 88: TAB_KON_211 — TUC_KON_211 „LöscheRecordInhalt“	194
7748	Tabelle 89: TAB_KON_786 Fehlercodes TUC_KON_211 „LöscheRecordInhalt“	195
7749	Tabelle 90: TAB_KON_228 — TUC_KON_214 „FügeHinzuRecord“	196
7750	Tabelle 91: TAB_KON_541 Fehlercodes TUC_KON_214 „FügeHinzuRecord“	197
7751	Tabelle 92: TAB_KON_229 — TUC_KON_215 „SucheRecord“	198
7752	Tabelle 93: TAB_KON_542 Fehlercodes TUC_KON_215 „SucheRecord“	199
7753	Tabelle 94: TAB_KON_110 — TUC_KON_018 „eGK Sperrung prüfen“	200
7754	Tabelle 95: TAB_KON_239 Fehlercodes TUC_KON_018 „eGK Sperrung prüfen“	201
7755	Tabelle 96: TAB_KON_108 — TUC_KON_006 „Datenzugriffsaudit eGK schreiben“	202
7756	Tabelle 97: TAB_KON_238 Fehlercodes TUC_KON_006 „Datenzugriffsaudit eGK	
7757	schreiben“	203
7758	Tabelle 98: TAB_KON_231 — TUC_KON_218 „Signiere“	203
7759	Tabelle 99: TAB_KON_543 Fehlercodes TUC_KON_218 „Signiere“	205
7760	Tabelle 100: TAB_KON_232 — TUC_KON_219 „Entschlüssele“	205
7761	Tabelle 101: TAB_KON_210 Fehlercodes TUC_KON_219 „Entschlüssele“	206
7762	Tabelle 102: TAB_KON_215 TUC_KON_200 „SendeAPDU“	207
7763	Tabelle 103: TAB_KON_216 Fehlercodes TUC_KON_200 „SendeAPDU“	208
7764	Tabelle 104: TAB_KON_737 — TUC_KON_024 „Karte zurücksetzen“	208
7765	Tabelle 105: TAB_KON_544 Fehlercodes TUC_KON_024 „Karte zurücksetzen“	209
7766	Tabelle 106: TAB_KON_230 — TUC_KON_216 „LeseZertifikat“	210
7767	Tabelle 107: TAB_KON_209 Fehlercodes TUC_KON_216 „LeseZertifikat“	211
7768	Tabelle 108: TAB_KON_827 TUC_KON_036 „LiefereFachlicheRolle“	212
7769	Tabelle 109: TAB_KON_829 Fehlercodes TUC_KON_036 „LiefereFachlicheRolle“	213
7770	Tabelle 110: TAB_KON_038 Basisanwendung Karten- und Kartenterminaldienst	213
7771	Tabelle 111: TAB_KON_047 Operation VerifyPin	214
7772	Tabelle 112: TAB_KON_738 Ablauf VerifyPin	216
7773	Tabelle 113: TAB_KON_545 Fehlercodes „VerifyPin“	217
7774	Tabelle 114: TAB_KON_049 Operation ChangePin	217

7775	Tabelle 115: TAB_KON_546 Ablauf ChangePin	219
7776	Tabelle 116: TAB_KON_547 Fehlercodes „ChangePin“	220
7777	Tabelle 117: TAB_KON_051 Operation GetPinStatus	220
7778	Tabelle 118: TAB_KON_548 Ablauf GetPinStatus	222
7779	Tabelle 119: TAB_KON_549 Fehlercodes „GetPinStatus“	222
7780	Tabelle 120: TAB_KON_053 Operation UnblockPin	223
7781	Tabelle 121: TAB_KON_550 Ablauf UnblockPIN	225
7782	Tabelle 122: TAB_KON_551 Fehlercodes „UnblockPin“	226
7783	Tabelle 123: TAB_KON_242 Operation EnablePin	226
7784	Tabelle 124: TAB_KON_243 Ablauf EnablePin	227
7785	Tabelle 125: TAB_KON_244 Fehlercodes „EnablePin“	228
7786	Tabelle 126: TAB_KON_245 Operation DisablePin	229
7787	Tabelle 127: TAB_KON_246 Ablauf DisablePin	230
7788	Tabelle 128: TAB_KON_247 Fehlercodes „DisablePin“	231
7789	Tabelle 129: TAB_KON_554 Konfiguration des Kartendienstes	232
7790	Tabelle 130: TAB_KON_555 TUC_KON_025 „Initialisierung Kartendienst“	232
7791	Tabelle 131: TAB_KON_030 Ereignisnachricht	236
7792	Tabelle 132: TAB_KON_556 TUC_KON_256 „Systemereignis absetzen“	237
7793	Tabelle 133: TAB_KON_557 Fehlercodes TUC_KON_256 „Systemereignis absetzen“ ...	242
7794	Tabelle 134: TAB_KON_558 TUC_KON_252 „Liefere KT_Liste“	242
7795	Tabelle 135: TAB_KON_559 TUC_KON_253 „Liefere Karten_Liste“	243
7796	Tabelle 136: TAB_KON_560 Fehlercodes TUC_KON_253 „Liefere Karten_Liste“	245
7797	Tabelle 137: TAB_KON_561 TUC_KON_254 „Liefere Ressourcendetails“	245
7798	Tabelle 138: TAB_KON_562 Fehlercodes TUC_KON_254 „Liefere Ressourcendetails“ ...	247
7799	Tabelle 139: TAB_KON_029 Basisanwendung Systeminformationsdienst	247
7800	Tabelle 140: TAB_KON_563 Operation GetCardTerminals	248
7801	Tabelle 141: TAB_KON_564 Ablauf GetCardTerminals	250
7802	Tabelle 142: TAB_KON_823 Fehlercodes „GetCardTerminals“	251
7803	Tabelle 143: TAB_KON_565 Operation GetCards	251
7804	Tabelle 144: TAB_KON_566 Ablauf GetCards	255
7805	Tabelle 145: TAB_KON_567 Fehlercodes „GetCards“	256
7806	Tabelle 146: TAB_KON_568 Operation GetResourceInformation	256
7807	Tabelle 147: TAB_KON_569 Ablauf GetResourceInformation	259
7808	Tabelle 148: TAB_KON_570 Fehlercodes „GetResourceInformation“	260
7809	Tabelle 149: TAB_KON_571 Operation Subscribe	260
7810	Tabelle 150: TAB_KON_572 Ablauf Subscribe	262

7811	Tabelle 151: TAB_KON_573 Fehlercodes „Subscribe“	263
7812	Tabelle 152: TAB_KON_574 Operation Unsubscribe	263
7813	Tabelle 153: TAB_KON_575 Ablauf Unsubscribe	264
7814	Tabelle 154: TAB_KON_576 Fehlercodes „Unsubscribe“	264
7815	Tabelle 155: TAB_KON_792 Operation RenewSubscriptions	265
7816	Tabelle 156: TAB_KON_793 Ablauf RenewSubscriptions	265
7817	Tabelle 157: TAB_KON_794 Fehlercodes „RenewSubscriptions“	266
7818	Tabelle 158: TAB_KON_577 Operation GetSubscription	267
7819	Tabelle 159: TAB_KON_578 Ablauf GetSubscription	268
7820	Tabelle 160: TAB_KON_579 Fehlercodes „GetSubscription“	269
7821	Tabelle 161: TAB_KON_580 Konfigurationswerte des Systeminformationsdienstes	
7822	(Administrator)	269
7823	Tabelle 162: TAB_KON_581 Verschlüsselungsdienst Operationen für	
7824	EVT_MONITOR_OPERATIONS	270
7825	Tabelle 163: TAB_KON_747 KeyReference für Encrypt /DecryptDocument	271
7826	Tabelle 164: TAB_KON_859 Werteliste und Defaultwert des Parameters crypt bei	
7827	hybrider Verschlüsselung	272
7828	Tabelle 165: TAB_KON_739 – TUC_KON_070 „Daten hybrid verschlüsseln“	272
7829	Tabelle 166: TAB_KON_073 Vorgaben zum Format verschlüsselter XML Dokumente ...	280
7830	Tabelle 167: TAB_KON_740 Fehlercodes TUC_KON_070 „Daten hybrid verschlüsseln“	280
7831	Tabelle 168: TAB_KON_140 – TUC_KON_071 „Daten hybrid entschlüsseln“	281
7832	Tabelle 169: TAB_KON_142 Fehlercodes TUC_KON_071 „Daten hybrid entschlüsseln“	285
7833	Tabelle 170: TAB_KON_741 – TUC_KON_072 „Daten symmetrisch verschlüsseln“	285
7834	Tabelle 171: TAB_KON_742 Fehlercodes TUC_KON_072 „Daten symmetrisch	
7835	verschlüsseln“	286
7836	Tabelle 172: TAB_KON_743 – TUC_KON_073 „Daten symmetrisch entschlüsseln“	286
7837	Tabelle 173: TAB_KON_744 Fehlercodes TUC_KON_073 „Daten symmetrisch	
7838	entschlüsseln“	287
7839	Tabelle 174: TAB_KON_860 – TUC_KON_075 „Symmetrisch verschlüsseln“	287
7840	Tabelle 175: TAB_KON_861 – TUC_KON_076 „Symmetrisch entschlüsseln“	289
7841	Tabelle 176: TAB_KON_745 Basisdienst Verschlüsselungsdienst	290
7842	Tabelle 177: TAB_KON_071 Operation EncryptDocument	291
7843	Tabelle 178: TAB_KON_746 Ablauf EncryptDocument	302
7844	Tabelle 179: TAB_KON_141 Fehlercodes „EncryptDocument“	302
7845	Tabelle 180: TAB_KON_075 Operation DecryptDocument	303
7846	Tabelle 181: TAB_KON_076 Ablauf DecryptDocument	305
7847	Tabelle 182: TAB_KON_145 Fehlercodes „DecryptDocument“	305
7848	Tabelle 183: TAB_KON_582 – Signaturverfahren Dokumentensignatur	306

7849	Tabelle 184: TAB_KON_585 — Zusätzliche Signaturverfahren für	
7850	Dokumentensignaturprüfung.....	308
7851	Tabelle 185: TAB_KON_778 — Einsatzbereich der Signaturvarianten für XAdES, CAdES	
7852	und PAdES.....	308
7853	Tabelle 186: TAB_KON_583 — Default Signaturverfahren	311
7854	Tabelle 187: TAB_KON_584 nonQES Operationen für EVT_MONITOR_OPERATIONS....	311
7855	Tabelle 188: TAB_KON_900 Zertifikate und private Schlüssel für Signaturerstellung und	
7856	Signaturprüfung (QES und nonQES)	312
7857	Tabelle 189: TAB_KON_862 Werteliste und Defaultwert des Parameters crypt bei QES-	
7858	Erzeugung.....	313
7859	Tabelle 190: TAB_KON_863 Werteliste und Defaultwert des Parameters crypt bei	
7860	nonQES Erzeugung.....	313
7861	Tabelle 191: TAB_KON_748 — TUC_KON_155 „Dokumente zur Signatur vorbereiten“ ..	319
7862	Tabelle 192: TAB_KON_586 Fehlercodes TUC_KON_155 „Dokumente zur Signatur	
7863	vorbereiten“	323
7864	Tabelle 193: TAB_KON_749 — TUC_KON_165 „Signaturvoraussetzungen für nonQES	
7865	prüfen“	323
7866	Tabelle 194: TAB_KON_587 Fehlercodes TUC_KON_165 „Signaturvoraussetzungen für	
7867	nonQES prüfen“	324
7868	Tabelle 195: TAB_KON_750 — TUC_KON_166 „nonQES Signaturen erstellen“.....	324
7869	Tabelle 196: TAB_KON_120 Fehlercodes TUC_KON_166 „nonQES Signaturen erstellen“	
7870	325
7871	Tabelle 197: TAB_KON_751 — TUC_KON_152 „Signaturvoraussetzungen für QES prüfen“	
7872	326
7873	Tabelle 198: TAB_KON_588 Fehlercodes TUC_KON_152 „Signaturvoraussetzungen für	
7874	QES prüfen“	327
7875	Tabelle 199: TAB_KON_752 — TUC_KON_154 „QES Signaturen erstellen“	327
7876	Tabelle 200: TAB_KON_126 Fehlercodes TUC_KON_154 „QES Signaturen erstellen“ ...	330
7877	Tabelle 201: TAB_KON_293 — TUC_KON_168 „Einzelsignatur QES erstellen“	331
7878	Tabelle 202: TAB_KON_590 Fehlercodes TUC_KON_168 „Einzelsignatur QES erstellen“	
7879	332
7880	Tabelle 203: TAB_KON_870 — TUC_KON_158 „Komfortsignaturen erstellen“	332
7881	Tabelle 204: TAB_KON_873 Fehlercodes TUC_KON_158 „Komfortsignaturen erstellen“	
7882	334
7883	Tabelle 205: TAB_KON_753 — TUC_KON_160 „Dokumente nonQES signieren“	335
7884	Tabelle 206: TAB_KON_127 Fehlercodes TUC_KON_160 „Dokumente nonQES signieren“	
7885	337
7886	Tabelle 207: TAB_KON_753 — TUC_KON_160 „Dokumente nonQES signieren“	338
7887	Tabelle 208: TAB_KON_127 Fehlercodes TUC_KON_160 „Dokumente nonQES signieren“	
7888	340
7889	Tabelle 209: TAB_KON_121 — TUC_KON_161 „nonQES Dokumentsignatur prüfen“	341

7890	Tabelle 210: TAB_KON_124 Fehlercodes TUC_KON_161 „nonQES-Dokumentensignatur	
7891	prüfen“	345
7892	Tabelle 211: TAB_KON_754 Übersicht Status für Prüfung einer Dokumentensignatur..	346
7893	Tabelle 212: TAB_KON_430 — TUC_KON_162 „Kryptographische Prüfung der XML-	
7894	Dokumentensignatur“	348
7895	Tabelle 213: TAB_KON_431 Fehlercodes TUC_KON_162 „Kryptographische Prüfung der	
7896	XML-Dokumentensignatur“	349
7897	Tabelle 214: TAB_KON_755 — TUC_KON_150 „Dokumente QES signieren“	349
7898	Tabelle 215: TAB_KON_128 Fehlercodes TUC_KON_150 „Dokument QES signieren“ ...	355
7899	Tabelle 216: TAB_KON_192 Verhalten des Konnektors beim Abbruch einer Stapelsignatur	
7900	356
7901	Tabelle 217: TAB_KON_591 — TUC_KON_151 „QES-Dokumentensignatur prüfen“	357
7902	Tabelle 218: TAB_KON_592 Fehlercodes TUC_KON_151 „QES-Dokumentensignatur	
7903	prüfen“	361
7904	Tabelle 219: TAB_KON_593 Übersicht Status für Prüfung einer Dokumentensignatur..	362
7905	Tabelle 220: TAB_KON_871 — TUC_KON_170 „Dokumente mit Komfort signieren“	363
7906	Tabelle 221: TAB_KON_872 Fehlercodes TUC_KON_170 „Dokumente mit Komfort	
7907	signieren“	366
7908	Tabelle 222: TAB_KON_883 — TUC_KON_171 „Komfortsignatur einschalten“	366
7909	Tabelle 223: TAB_KON_886 Fehlercodes TUC_KON_171 „Komfortsignatur einschalten“	
7910	368
7911	Tabelle 224: TAB_KON_884 — TUC_KON_172 „Komfortsignatur ausschalten“	368
7912	Tabelle 225: TAB_KON_887 Fehlercodes TUC_KON_172 „Komfortsignatur ausschalten“	
7913	369
7914	Tabelle 226: TAB_KON_885 — TUC_KON_173 „Liefere Signaturmodus“	370
7915	Tabelle 227: TAB_KON_888 Fehlercodes TUC_KON_173 „Liefere Signaturmodus“	371
7916	Tabelle 228: TAB_KON_197 Basisdienst Signaturdienst (nonQES und QES)	372
7917	Tabelle 229: TAB_KON_065 Operation SignDocument (nonQES und QES)	373
7918	Tabelle 230: TAB_KON_756 Ablauf Operation SignDocument (nonQES und QES)	385
7919	Tabelle 231: TAB_KON_757 Fehlercodes „SignDocument (nonQES und QES)“	386
7920	Tabelle 232: TAB_KON_066 Operation VerifyDocument (nonQES und QES)	386
7921	Tabelle 233: TAB_KON_760 Ablauf Operation VerifyDocument (nonQES und QES)	391
7922	Tabelle 234: TAB_KON_761 Fehlercodes „VerifyDocument (nonQES und QES)“	392
7923	Tabelle 235: TAB_KON_840 Operation StopSignature	392
7924	Tabelle 236: TAB_KON_841 Ablauf Operation StopSignature	393
7925	Tabelle 237: TAB_KON_842 Fehlercodes „StopSignature“	393
7926	Tabelle 238: TAB_KON_843 Operation GetJobNumber	393
7927	Tabelle 239: TAB_KON_844 Ablauf Operation GetJobNumber	394
7928	Tabelle 240: TAB_KON_845 Fehlercodes „GetJobNumber“	394

7929	Tabelle 241: TAB_KON_874 ActivateComfortSignature	394
7930	Tabelle 242: TAB_KON_877 Ablauf ActivateComfortSignature	395
7931	Tabelle 243: TAB_KON_879 Fehlercodes ActivateComfortSignature	396
7932	Tabelle 244: TAB_KON_875 DeactivateComfortSignature	396
7933	Tabelle 245: TAB_KON_878 Ablauf DeactivateComfortSignature	397
7934	Tabelle 246: TAB_KON_880 Fehlercodes DeactivateComfortSignature	397
7935	Tabelle 247: TAB_KON_876 GetSignatureMode	397
7936	Tabelle 248: TAB_KON_882 Ablauf GetSignatureMode	399
7937	Tabelle 249: TAB_KON_881 Fehlercodes GetSignatureMode	399
7938	Tabelle 250: TAB_KON_596 Konfigurationswerte des Signaturdienstes (Administrator)	
7939	399
7940	Tabelle 251: TAB_KON_596 Konfigurationswerte des Signaturdienstes (Administrator)	
7941	400
7942	Tabelle 252: TAB_KON_853 intendedKeyUsage bei Zertifikatsprüfung	402
7943	Tabelle 253: TAB_KON_858 Kartenobjekt in Abhängigkeit vom kryptographischen	
7944	Verfahren	403
7945	Tabelle 254: TAB_KON_825 Fehlercodes „TLS Verbindungsaufbau zum TSL Dienst“ ...	405
7946	Tabelle 255: TAB_KON_826 Fehlercodes „TLS Verbindungsaufbau zum TSL Dienst bei	
7947	Prüfung der technischen Rolle“	406
7948	Tabelle 256: TAB_KON_597 Operationen in EVT_MONITOR_OPERATIONS	407
7949	Tabelle 257: TAB_KON_766 TUC_KON_032 „TSL aktualisieren“	407
7950	Tabelle 258: TAB_KON_598 Fehlercodes TUC_KON_032 „TSL aktualisieren“	410
7951	Tabelle 259: TAB_KON_618 TUC_KON_031 „BNetzA VL aktualisieren“	410
7952	Tabelle 260: TAB_KON_619 Fehlercodes TUC_KON_031 „BNetzA VL aktualisieren“	411
7953	Tabelle 261: TAB_KON_767 TUC_KON_040 „CRL aktualisieren“	411
7954	Tabelle 262: TAB_KON_599 Fehlercodes TUC_KON_040 „CRL aktualisieren“	413
7955	Tabelle 263: TAB_KON_768 TUC_KON_033 „Zertifikatsablauf prüfen“	413
7956	Tabelle 264: TAB_KON_600 Fehlercodes TUC_KON_033 „Zertifikatsablauf prüfen“	416
7957	Tabelle 265: TAB_KON_769 TUC_KON_037 „Zertifikat prüfen“	416
7958	Tabelle 266: TAB_KON_601 Fehlercodes TUC_KON_037 „Zertifikat prüfen“	421
7959	Tabelle 267: TAB_KON_818 TUC_KON_042 „CV Zertifikat prüfen“	421
7960	Tabelle 268: TAB_KON_819 Fehlercodes TUC_KON_042 „CV Zertifikat prüfen“	423
7961	Tabelle 269: TAB_KON_770 TUC_KON_034 „Zertifikatsinformationen extrahieren“	423
7962	Tabelle 270: TAB_KON_602 Fehlercodes TUC_KON_034 „Zertifikatsinformationen	
7963	extrahieren“	426
7964	Tabelle 271: TAB_KON_771 Basisanwendung Zertifikatsdienst	426
7965	Tabelle 272: TAB_KON_676 Operation CheckCertificateExpiration	427
7966	Tabelle 273: TAB_KON_677 Ablauf CheckCertificateExpiration	428

7967	Tabelle 274: TAB_KON_603 Fehlercodes „CheckCertificateExpiration“	429
7968	Tabelle 275: TAB_KON_678 Operation ReadCardCertificate	430
7969	Tabelle 276: TAB_KON_679 Ablauf ReadCardCertificate	432
7970	Tabelle 277: TAB_KON_604 Fehlercodes „ReadCardCertificate“	433
7971	Tabelle 278: TAB_KON_795 Operation VerifyCertificate	434
7972	Tabelle 279: TAB_KON_797 Ablauf VerifyCertificate	435
7973	Tabelle 280: TAB_KON_800 Fehlercodes „VerifyCertificate“	436
7974	Tabelle 281: TAB_KON_772 TUC_KON_035 „Zertifikatsdienst initialisieren“	436
7975	Tabelle 282: TAB_KON_605 Fehlercodes TUC_KON_035 „Zertifikatsdienst initialisieren“	437
7976		
7977	Tabelle 283: TAB_KON_606 Konfiguration des Zertifikatsdienstes	438
7978	Tabelle 284: TAB_KON_733 Einsetzbare Konfigurationsparameter des Zertifikatsdienstes	439
7979		
7980	Tabelle 285: TAB_KON_857 Fehlercodes beim Import des Cross-Zertifikats für TI-Vertrauensanker ECC	441
7981		
7982	Tabelle 286: TAB_KON_607 TUC_KON_271 „Schreibe Protokolleintrag“	444
7983	Tabelle 287: TAB_KON_608 Fehlercodes TUC_KON_271 „Schreibe Protokolleintrag“	447
7984	Tabelle 288: TAB_KON_609 Konfigurationswerte des Protokollierungsdienstes (Administrator)	449
7985		
7986	Tabelle 289: TAB_KON_610 TUC_KON_272 „Initialisierung Protokollierungsdienst“ ..	450
7987	Tabelle 290: TAB_KON_611 Fehlercodes TUC_KON_272 „Initialisiere Protokollierungsdienst“	451
7988		
7989	Tabelle 291: TAB_KON_773 TUC_KON_110 „Kartenbasierte TLS-Verbindung aufbauen“	452
7990		
7991	Tabelle 292: TAB_KON_612 Fehlercodes TUC_KON_110 „Kartenbasierte TLS-Verbindung aufbauen“	453
7992		
7993	Tabelle 293: TAB_KON_774 TUC_KON_111 „Kartenbasierte TLS-Verbindung abbauen“	454
7994		
7995	Tabelle 294: TAB_KON_613 Fehlercodes TUC_KON_111 „Kartenbasierte TLS-Verbindung abbauen“	455
7996		
7997	Tabelle 295: TAB_KON_805 TUC_KON_290 „LDAP-Verbindung aufbauen“	456
7998	Tabelle 296: TAB_KON_815 TUC_KON_291 „Verzeichnis abfragen“	457
7999	Tabelle 297: TAB_KON_816 TUC_KON_292 „LDAP-Verbindung trennen“	458
8000	Tabelle 298: TAB_KON_817 TUC_KON_293 „Verzeichnisabfrage abbrechen“	459
8001	Tabelle 299: TAB_KON_780 Signaturverfahren Externe Authentisierung	460
8002	Tabelle 300: TAB_KON_839 Basisdienst Authentifizierungsdienst	461
8003	Tabelle 301: TAB_KON_781 Operation ExternalAuthenticate	462
8004	Tabelle 302: TAB_KON_782 Ablauf Operation ExternalAuthenticate	465
8005	Tabelle 303: TAB_KON_783 Übersicht Fehler Operation ExternalAuthenticate	465

8006	Tabelle 304: TAB_KON_784 Privater Schlüssel je Karte für ExternalAuthenticate	465
8007	Tabelle 305: TAB_KON_680 Mapping der Netzwerksegmente	468
8008	Tabelle 306: TAB_KON_681 Definition der vom Konnektor verwendeten VPN Tunnel ..	469
8009	Tabelle 307: TAB_KON_682 Definition der Konnektor IP Adressen	469
8010	Tabelle 308: TAB_KON_614 TUC_KON_305 „LAN Adapter initialisieren“	479
8011	Tabelle 309: TAB_KON_615 Fehlercodes TUC_KON_305 „LAN Adapter initialisieren“...	480
8012	Tabelle 310: TAB_KON_616 TUC_KON_306 „WAN Adapter initialisieren“	480
8013	Tabelle 311: TAB_KON_617 Fehlercodes TUC_KON_306 „WAN Adapter initialisieren“ ..	481
8014	Tabelle 312: TAB_KON_622 TUC_KON_304 „Netzwerk Routen einrichten“	482
8015	Tabelle 313: TAB_KON_623 Fehlercodes TUC_KON_304 „Netzwerk Routen einrichten“	
8016	484
8017	Tabelle 314: TAB_KON_683 LAN Adapter IP Konfiguration	485
8018	Tabelle 315: TAB_KON_684 LAN Adapter Erweiterte Parameter	485
8019	Tabelle 316: TAB_KON_685 WAN Adapter IP Konfiguration	486
8020	Tabelle 317: TAB_KON_686 WAN Adapter Erweiterte Parameter	487
8021	Tabelle 318: TAB_KON_624 „Konfigurationsparameter der Anbindung LAN/WAN“	488
8022	Tabelle 319: TAB_KON_625 Konfigurationsparameter Firewall Schnittstelle	491
8023	Tabelle 320: TAB_KON_626 „Liefere Netzwerkinformationen über DHCP“	492
8024	Tabelle 321: TAB_KON_627 „Aktivierung des DHCP Servers“	493
8025	Tabelle 322: TAB_KON_628 „Basiskonfiguration des DHCP Servers“	494
8026	Tabelle 323: TAB_KON_629 „Client Gruppenspezifische Konfigurationsoptionen des	
8027	Konnektor DHCP Servers“	494
8028	Tabelle 324: TAB_KON_630 TUC_KON_343 „Initialisierung DHCP Server“	496
8029	Tabelle 325: TAB_KON_631 Fehlercodes TUC_KON_343 „Initialisierung DHCP Server“	497
8030	Tabelle 326: TAB_KON_632 TUC_KON_341 „DHCP Informationen beziehen“	498
8031	Tabelle 327: TAB_KON_633 Fehlercodes TUC_KON_341 „DHCP Informationen beziehen“	
8032	499
8033	Tabelle 328: TAB_KON_634 „Konfiguration des DHCP Clients“	500
8034	Tabelle 329: TAB_KON_635 TUC_KON_321 „Verbindung zu dem VPN Konzentration der	
8035	TI aufbauen“	502
8036	Tabelle 330: TAB_KON_636 Fehlercodes TUC_KON_321 „Verbindung zu dem VPN-	
8037	Konzentrator der TI aufbauen“	504
8038	Tabelle 331: TAB_KON_637 TUC_KON_322 „Verbindung zu dem VPN Konzentration der	
8039	SIS aufbauen“	504
8040	Tabelle 332: TAB_KON_638 Fehlercodes TUC_KON_322 „Verbindung zu dem VPN-	
8041	Konzentrator der SIS aufbauen“	506
8042	Tabelle 333: TAB_KON_639 Konfigurationsparameter VPN Client	507
8043	Tabelle 334: TAB_KON_640 Zustandswerte für Konnektor NTP Server	509
8044	Tabelle 335: TAB_KON_776 TUC_KON_351 „Liefere Systemzeit“	510

8045	Tabelle 336: TAB_KON_641 Fehlercodes TUC_KON_351 „Liefere Systemzeit“	511
8046	Tabelle 337: TAB_KON_642 Operation sync_Time	511
8047	Tabelle 338: TAB_KON_643 Konfiguration des Konnektor NTP-Servers.....	512
8048	Tabelle 339: TAB_KON_730 Einsehbare Konfigurationsparameter des Konnektor NTP-	
8049	Servers	512
8050	Tabelle 340: TAB_KON_644 — TUC_KON_352 „Initialisierung Zeitdienst“	512
8051	Tabelle 341: TAB_KON_645 Fehlercodes TUC_KON_352 „Initialisierung Zeitdienst“	513
8052	Tabelle 342: TAB_KON_687 DNS-Forwards des DNS-Servers	514
8053	Tabelle 343: TAB_KON_646 — TUC_KON_361 „DNS-Namen auflösen“	516
8054	Tabelle 344: TAB_KON_647 Fehlercodes TUC_KON_361 „DNS-Namen auflösen“	517
8055	Tabelle 345: TAB_KON_646 — TUC_KON_361 „DNS-Namen auflösen“	517
8056	Tabelle 346: TAB_KON_647 Fehlercodes TUC_KON_361 „DNS-Namen auflösen“	518
8057	Tabelle 347: TAB_KON_648 — TUC_KON_362 „Liste der Dienste abrufen“	518
8058	Tabelle 348: TAB_KON_649 Fehlercodes TUC_KON_362 „Liste der Dienste abrufen“ ...	519
8059	Tabelle 349: TAB_KON_650 — TUC_KON_363 „Dienstdetails abrufen“	519
8060	Tabelle 350: TAB_KON_651 Fehlercodes TUC_KON_363 „Dienstdetails abrufen“	520
8061	Tabelle 351: TAB_KON_652 Basisanwendung Namensdienst	520
8062	Tabelle 352: TAB_KON_653 Operation GetIPAddress	521
8063	Tabelle 353: TAB_KON_654 — Konfigurationsparameter Namensdienst	522
8064	Tabelle 354: TAB_KON_731 Einsehbare Konfigurationsparameter Namensdienst	522
8065	Tabelle 355: TAB_KON_655 Konfigurationen der Benutzerverwaltung (Super-	
8066	Administrator)	527
8067	Tabelle 356: TAB_KON_656 Konfigurationen der Benutzerverwaltung	528
8068	Tabelle 357: TAB_KON_657 Konfigurationsparameter des Konnektornamens	528
8069	Tabelle 358: TAB_KON_833 Bezeichner für persistente Konfigurationsdaten für	
8070	Fachmodule	532
8071	Tabelle 359: TAB_KON_658 Aktivieren/Deaktivieren von Leistungsumfängen	533
8072	Tabelle 360: TAB_KON_659 Konnektor Standalone einsetzen	534
8073	Tabelle 361: TAB_KON_661 Konfigurationsparameter der Konnektorfreischaltung	535
8074	Tabelle 362: TAB_KON_732 Einsehbare Konfigurationsparameter der	
8075	Konnektorfreischaltung	535
8076	Tabelle 363: TAB_KON_662 Zustandswerte der Konnektorfreischaltung	535
8077	Tabelle 364: TAB_KON_851 Einschränkung der Rechte des Remote-Administrators	
8078	(Blacklist)	539
8079	Tabelle 365: TAB_KON_663 Konfigurationen des Remote-Managements	540
8080	Tabelle 366: TAB_KON_664 — TUC_KON_280 „Konnektoraktualisierung durchführen“ ..	543
8081	Tabelle 367: TAB_KON_665 Fehlercodes TUC_KON_280 „Konnektoraktualisierung	
8082	durchführen“	545

8083	Tabelle 368: TAB_KON_666 – TUC_KON_281 „Kartenterminalaktualisierung anstoßen“	
8084	548
8085	Tabelle 369: TAB_KON_667 Fehlercodes TUC_KON_281 „Kartenterminalaktualisierung	
8086	anstoßen“.....	550
8087	Tabelle 370: TAB_KON_668 – TUC_KON_282 „UpdateInformationen beziehen“.....	550
8088	Tabelle 371: TAB_KON_669 Fehlercodes TUC_KON_282 „UpdateInformationen beziehen“	
8089	552
8090	Tabelle 372: TAB_KON_799 – TUC_KON_283 „Infrastruktur Konfiguration aktualisieren“	
8091	552
8092	Tabelle 373: Tab_Kon_726 Fehlercodes TUC_KON_283 „Infrastruktur Konfiguration	
8093	aktualisieren“.....	556
8094	Tabelle 374: TAB_KON_833 – TUC_KON_285 „UpdateInformationen für Fachmodul	
8095	beziehen“.....	556
8096	Tabelle 375: TAB_KON_834 Fehlercodes TUC_KON_285 „UpdateInformationen für	
8097	Fachmodul beziehen“.....	558
8098	Tabelle 376: TAB_KON_835 – TUC_KON_286 „Paket für Fachmodul laden“.....	559
8099	Tabelle 377: TAB_KON_836 Fehlercodes TUC_KON_286 „Paket für Fachmodul laden“.....	560
8100	Tabelle 378: TAB_KON_864 – TUC_KON_284 „KSR-Client initialisieren“.....	560
8101	Tabelle 379: TAB_KON_822 Fehlercodes TUC_KON_284 „KSR-Client initialisieren“.....	561
8102	Tabelle 380: TAB_KON_670 Konfigurationsparameter der Software-Aktualisierung.....	561
8103	Tabelle 381: TAB_KON_820 Einschbare Konfigurationsparameter der Software-	
8104	Aktualisierung.....	562
8105	Tabelle 382: TAB_KON_671 Anforderungen Klima.....	569
8106	Tabelle 383: TAB_KON_672 Anforderungen Vibration.....	569
8107	Tabelle 384: TAB_KON_672 Anforderungen Vibration.....	570
8108	Tabelle 385: TAB_KON_779 „Profilierung der Signaturformate“.....	609
8109	Tabelle 386 TAB_KON_775 „Profilierung der Dokumentformate und Nachrichten“.....	616
8110	Tabelle 387: TAB_KON_688 Version der Schemas aus dem Namensraum des Konnektors	
8111	618
8112	Tabelle 388: TAB_KON_798 Schnittstellenversionen.....	621
8113	Tabelle 389 – TAB_KON_777 Events Interne Mechanismen.....	627
8114	Tabelle 390 – TAB_KON_711 Architektur der TI-Plattform, Berechtigt Fachmodule.....	645
8115	Tabelle 391 – TAB_KON_712 Architektur der TI-Plattform, Berechtigt Clientsysteme...	650
8116	Tabelle 392 – TAB_KON_713 Architektur der TI-Plattform, Berechtigt eHealth-KT.....	652
8117	Tabelle 393 – TAB_KON_714 Architektur der TI-Plattform, Berechtigt Administrator...	652
8118	Tabelle 394: Aufzähltypen.....	675
8119	Tabelle 1: TAB_KON_500 Wertetabelle Kartentypen.....	38
8120	Tabelle 2: TAB_KON_856: Identitäten des Konnektors auf der gSMC-K.....	40
8121	Tabelle 3: TAB_KON_503 Betriebszustand Fehlerzustandsliste.....	45

8122	Tabelle 4: TAB KON 504 Ausführungserlaubnis für Dienste in kritischen Fehlerzuständen	51
8123	
8124	Tabelle 5: TAB KON 502 Fehlercodes „Betriebszustand“	57
8125	Tabelle 6: TAB KON 505 Konfigurationswerte Missbrauchserkennung	57
8126	Tabelle 7: TAB KON 852 Konfigurationsvarianten der Verbindungen zwischen Konnektor	
8127	und Clientsystemen	60
8128	Tabelle 8: TAB KON 506 Konfigurationsparameter der Clientsystem-Authentisierung	62
8129	Tabelle 9: TAB KON 812 Umgebungsabhängige Konfigurationsparameter	68
8130	Tabelle 10: TAB KON 507 Informationsmodell Entitäten	72
8131	Tabelle 11: TAB KON 508 Informationsmodell Attribute	76
8132	Tabelle 12: TAB KON 509 Informationsmodell Entitätenbeziehungen	77
8133	Tabelle 13: TAB KON 510 Informationsmodell Constraints	79
8134	Tabelle 14: TAB KON 511 – TUC KON 000 „Prüfe Zugriffsberechtigung“	82
8135	Tabelle 15: TAB KON 512 Zugriffsregeln Beschreibung	85
8136	Tabelle 16: TAB KON 513 Zugriffsregeln Regelzuordnung	87
8137	Tabelle 17: TAB KON 514-01 Zugriffsregeln Definition	88
8138	Tabelle 18: TAB KON 515 Fehlercodes TUC KON 000 „Prüfe Zugriffsberechtigung“	92
8139	Tabelle 19: TAB KON 143 – TUC KON 080 „Dokument validieren“	94
8140	Tabelle 20: TAB KON 144 Fehlercodes TUC KON 080 „Dokument validieren“	96
8141	Tabelle 21: TAB KON 516 Basisanwendung Dienstverzeichnisdienst	98
8142	Tabelle 22: TAB KON 517 Schemabeschreibung Produktinformation	
8143	(ProductInformation.xsd)	99
8144	Tabelle 23: TAB KON 518 Schemabeschreibung Serviceinformation	
8145	(Serviceinformation.xsd)	100
8146	Tabelle 24: TAB KON 519 - TUC KON 041 „Einbringen der Endpunktinformationen	
8147	während der Bootup-Phase“	101
8148	Tabelle 25: TAB KON 520 Fehlercodes TUC KON 041 „Einbringen der	
8149	Endpunktinformationen während der Bootup-Phase“	102
8150	Tabelle 26: TAB KON 521 Schnittstelle der Basisanwendung Dienstverzeichnisdienst	102
8151	Tabelle 27: TAB KON 522 Parameterübersicht des Kartenterminaldienstes	104
8152	Tabelle 28: TAB KON 785 Erlaubte SICCT-Kommandos bei CT.CONNECTED=Nein	109
8153	Tabelle 29: TAB KON 727 Terminalanzeigen beim Anfordern und Auswerfen von Karten	
8154	110
8155	Tabelle 30: TAB KON 039 – TUC KON 050 „Beginne Kartenterminalsitzung“	112
8156	Tabelle 31: TAB KON 523 Fehlercodes TUC KON 050 „Beginne Kartenterminalsitzung“	
8157	118
8158	Tabelle 32: TAB KON 524 – TUC KON 054 „Kartenterminal hinzufügen“	118
8159	Tabelle 33: TAB KON 525 Fehlercodes TUC KON 054 „Kartenterminal hinzufügen“	120
8160	Tabelle 34: TAB KON 041 – TUC KON 053 „Paire Kartenterminal“	120

8161	Tabelle 35: TAB KON 113 Fehlercodes TUC KON 053 „Paire Kartenterminal“	123
8162	Tabelle 36: TAB KON 526 – TUC KON 055 „Befülle CT-Object“	125
8163	Tabelle 37: TAB KON 112 – TUC KON 051 „Mit Anwender über Kartenterminal	
8164	interagieren“	126
8165	Tabelle 38: TAB KON 114 Fehlercodes TUC KON 051 „Mit Anwender über	
8166	Kartenterminal interagieren“	128
8167	Tabelle 39: TAB KON 723 - TUC KON 056 „Karte anfordern“	129
8168	Tabelle 40: TAB KON 724 Fehlercodes TUC KON 056 „Karte anfordern“	131
8169	Tabelle 41: TAB KON 725 – TUC KON 057 „Karte auswerfen“	131
8170	Tabelle 42: TAB KON 796 Fehlercodes TUC KON 057 „Karte auswerfen“	133
8171	Tabelle 43: TAB KON 854 – TUC KON 058 „Displaygröße ermitteln“	134
8172	Tabelle 44: TAB KON 855 Fehlercodes TUC KON 058 „Displaygröße ermitteln“	135
8173	Tabelle 45: TAB KON 722 Basisdienst Kartenterminaldienst.....	135
8174	Tabelle 46: TAB KON 716 Operation RequestCard	135
8175	Tabelle 47: TAB KON 717 Ablauf RequestCard	137
8176	Tabelle 48: TAB KON 718 Fehlercodes „RequestCard“	137
8177	Tabelle 49: TAB KON 719 Operation EjectCard	138
8178	Tabelle 50: TAB KON 720 Ablauf EjectCard	139
8179	Tabelle 51: TAB KON 721 Fehlercodes Operation „EjectCard“	140
8180	Tabelle 52: TAB KON 527 Konfigurationswerte eines Kartenterminalobjekts	140
8181	Tabelle 53: TAB KON 528 Informationsparamter des Kartenterminaldienstes.....	141
8182	Tabelle 54: TAB KON 529 Anzeigewerte zu einem Kartenterminalobjekt.....	142
8183	Tabelle 55: TAB KON 530 Konfigurationswerte eines Kartenterminalobjekts	144
8184	Tabelle 56: TAB KON 531 Parameterübersicht des Kartendienstes.....	147
8185	Tabelle 57: TAB KON 090 Terminalanzeigen beim Eingeben der PIN am Kartenterminal	
8186	150
8187	Tabelle 58: TAB KON 734 – TUC KON 001 „Karte öffnen“	155
8188	Tabelle 59: TAB KON 735 - TUC KON 026.....	158
8189	Tabelle 60: TAB KON 824 Fehlercodes TUC KON 026 „Liefere CardSession“	159
8190	Tabelle 61: TAB KON 087 – TUC KON 012 „PIN verifizieren“	159
8191	Tabelle 62: TAB KON 089 Fehlercodes TUC KON 012 „PIN verifizieren“	163
8192	Tabelle 63: TAB KON 736 – TUC KON 019 „PIN ändern“	164
8193	Tabelle 64: TAB KON 093 Fehlercodes TUC KON 019 „PIN ändern“	167
8194	Tabelle 65: TAB KON 236 – TUC KON 021 „PIN entsperren“.....	168
8195	Tabelle 66: TAB KON 193 Fehlercodes TUC KON 021 „PIN entsperren“.....	171
8196	Tabelle 67 TAB KON 532 – TUC KON 022 „Liefere PIN-Status“	172
8197	Tabelle 68: TAB KON 091 Fehlercodes TUC KON 022 „Liefere PIN-Status“	174

8198	Tabelle 69: TAB KON 240 - TUC KON 027 „PIN-Schutz ein-/ausschalten“	174
8199	Tabelle 70: TAB KON 838 Mapping von pinRef auf ANW	177
8200	Tabelle 71: TAB KON 241 Fehlercodes TUC KON 027 „PIN-Schutz ein/ausschalten“ ..	177
8201	Tabelle 72: TAB KON 533 - TUC KON 023 „Karte reservieren“	178
8202	Tabelle 73: TAB KON 534 Fehlercodes TUC KON 023 „Karte reservieren“.....	179
8203	Tabelle 74: TAB KON 096 – TUC KON 005 „Card-to-Card authentisieren“	180
8204	Tabelle 75: TAB KON 673 AuthMode für C2C	182
8205	Tabelle 76: TAB KON 674 Erlaubte Parameterkombinationen und resultierende CV-	
8206	Zertifikate für C2C.....	183
8207	Tabelle 77: TAB KON 535 Fehlercodes TUC KON 005 „Card-to-Card authentisieren“	183
8208	Tabelle 78: TAB KON 218 – TUC KON 202 „LeseDatei“	184
8209	Tabelle 79: TAB KON 536 Fehlercodes TUC KON 202 „LeseDatei“	185
8210	Tabelle 80: TAB KON 219 – TUC KON 203 „SchreibeDatei“	186
8211	Tabelle 81: TAB KON 537 Fehlercodes TUC KON 203 „Schreibe Datei“	187
8212	Tabelle 82: TAB KON 204 – TUC KON 204 „LöscheDateiInhalt“.....	188
8213	Tabelle 83: TAB KON 785 Fehlercodes TUC KON 204 „LöscheDateiInhalt“	189
8214	Tabelle 84: TAB KON 538 – TUC KON 209 „LeseRecord“.....	190
8215	Tabelle 85: TAB KON 539 Fehlercodes TUC KON 209 „LeseRecord“	191
8216	Tabelle 86: TAB KON 224 – TUC KON 210 „SchreibeRecord“	192
8217	Tabelle 87: TAB KON 540 Fehlercodes TUC KON 210 „SchreibeRecord“	193
8218	Tabelle 88: TAB KON 211 – TUC KON 211 „LöscheRecordInhalt“	194
8219	Tabelle 89: TAB KON 786 Fehlercodes TUC KON 211 „LöscheRecordInhalt“	195
8220	Tabelle 90: TAB KON 228 – TUC KON 214 „FügeHinzuRecord“	196
8221	Tabelle 91: TAB KON 541 Fehlercodes TUC KON 214 „FügeHinzuRecord“.....	197
8222	Tabelle 92: TAB KON 229 – TUC KON 215 „SucheRecord“	198
8223	Tabelle 93: TAB KON 542 Fehlercodes TUC KON 215 „SucheRecord“	199
8224	Tabelle 94: TAB KON 110 - TUC KON 018 „eGK-Sperrung prüfen“	200
8225	Tabelle 95: TAB KON 239 Fehlercodes TUC KON 018 „eGK-Sperrung prüfen“	201
8226	Tabelle 96: TAB KON 108 - TUC KON 006 „Datenzugriffsaudit eGK schreiben“	202
8227	Tabelle 97: TAB KON 238 Fehlercodes TUC KON 006 „Datenzugriffsaudit eGK	
8228	schreiben“	203
8229	Tabelle 98: TAB KON 231 – TUC KON 218 „Signiere“	203
8230	Tabelle 99: TAB KON 543 Fehlercodes TUC KON 218 „Signiere“	205
8231	Tabelle 100: TAB KON 232 – TUC KON 219 „Entschlüssele“	205
8232	Tabelle 101: TAB KON 210 Fehlercodes TUC KON 219 „Entschlüssele“	206
8233	Tabelle 102: TAB KON 215 TUC KON 200 „SendeAPDU“	207
8234	Tabelle 103: TAB KON 216 Fehlercodes TUC KON 200 „SendeAPDU“	208

8235	Tabelle 104: TAB KON 737 – TUC KON 024 „Karte zurücksetzen“	208
8236	Tabelle 105: TAB KON 544 Fehlercodes TUC KON 024 „Karte zurücksetzen“	209
8237	Tabelle 106: TAB KON 230 – TUC KON 216 „LeseZertifikat“	210
8238	Tabelle 107: TAB KON 209 Fehlercodes TUC KON 216 „LeseZertifikat“	211
8239	Tabelle 108: TAB KON 827 TUC KON 036 „LiefereFachlicheRolle“	212
8240	Tabelle 109: TAB KON 829 Fehlercodes TUC KON 036 „LiefereFachlicheRolle“	213
8241	Tabelle 110: TAB KON 038 Basisanwendung Karten- und Kartenterminaldienst	213
8242	Tabelle 111: TAB KON 047 Operation VerifyPin	214
8243	Tabelle 112: TAB KON 738 Ablauf VerifyPin	216
8244	Tabelle 113: TAB KON 545 Fehlercodes „VerifyPin“	217
8245	Tabelle 114: TAB KON 049 Operation ChangePin	217
8246	Tabelle 115: TAB KON 546 Ablauf ChangePin	219
8247	Tabelle 116: TAB KON 547 Fehlercodes „ChangePin“	220
8248	Tabelle 117: TAB KON 051 Operation GetPinStatus	220
8249	Tabelle 118: TAB KON 548 Ablauf GetPinStatus	222
8250	Tabelle 119: TAB KON 549 Fehlercodes „GetPinStatus“	222
8251	Tabelle 120: TAB KON 053 Operation UnblockPin	223
8252	Tabelle 121: TAB KON 550 Ablauf UnblockPIN	225
8253	Tabelle 122: TAB KON 551 Fehlercodes „UnblockPin“	226
8254	Tabelle 123: TAB KON 242 Operation EnablePin	226
8255	Tabelle 124: TAB KON 243 Ablauf EnablePin	227
8256	Tabelle 125: TAB KON 244 Fehlercodes „EnablePin“	228
8257	Tabelle 126: TAB KON 245 Operation DisablePin	229
8258	Tabelle 127: TAB KON 246 Ablauf DisablePin	230
8259	Tabelle 128: TAB KON 247 Fehlercodes „DisablePin“	231
8260	Tabelle 129: TAB KON 554 Konfiguration des Kartendienstes	232
8261	Tabelle 130: TAB KON 555 - TUC KON 025 „Initialisierung Kartendienst“	232
8262	Tabelle 131: TAB KON 030 Ereignisnachricht	236
8263	Tabelle 132: TAB KON 556 - TUC KON 256 „Systemereignis absetzen“	237
8264	Tabelle 133: TAB KON 557 Fehlercodes TUC KON 256 „Systemereignis absetzen“ ...	242
8265	Tabelle 134: TAB KON 558 – TUC KON 252 „Liefere KT Liste“	242
8266	Tabelle 135: TAB KON 559 – TUC KON 253 „Liefere Karten Liste“	243
8267	Tabelle 136: TAB KON 560 Fehlercodes TUC KON 253 „Liefere Karten Liste“	245
8268	Tabelle 137: TAB KON 561 - TUC KON 254 „Liefere Ressourcendetails“	245
8269	Tabelle 138: TAB KON 562 Fehlercodes TUC KON 254 „Liefere Ressourcendetails“ ...	247
8270	Tabelle 139 TAB KON 029 Basisanwendung Systeminformationsdienst	247

8271	Tabelle 140: TAB KON 563 Operation GetCardTerminals	248
8272	Tabelle 141: TAB KON 564 Ablauf GetCardTerminals	250
8273	Tabelle 142: TAB KON 823 Fehlercodes „GetCardTerminals“	251
8274	Tabelle 143: TAB KON 565 Operation GetCards	251
8275	Tabelle 144: TAB KON 566 Ablauf GetCards	255
8276	Tabelle 145: TAB KON 567 Fehlercodes „GetCards“	256
8277	Tabelle 146: TAB KON 568 Operation GetResourceInformation	256
8278	Tabelle 147: TAB KON 569 Ablauf GetResourceInformation	259
8279	Tabelle 148: TAB KON 570 Fehlercodes „GetResourceInformation“	260
8280	Tabelle 149: TAB KON 571 Operation Subscribe.....	260
8281	Tabelle 150: TAB KON 572 Ablauf Subscribe	262
8282	Tabelle 151 TAB KON 573 Fehlercodes „Subscribe“	263
8283	Tabelle 152: TAB KON 574 Operation Unsubscribe	263
8284	Tabelle 153: TAB KON 575 Ablauf Unsubscribe	264
8285	Tabelle 154: TAB KON 576 Fehlercodes „Unsubscribe“	264
8286	Tabelle 155: TAB KON 792 Operation RenewSubscriptions	265
8287	Tabelle 156: TAB KON 793 Ablauf RenewSubscriptions	265
8288	Tabelle 157: TAB KON 794 Fehlercodes „RenewSubscriptions“	266
8289	Tabelle 158: TAB KON 577 Operation GetSubscription	267
8290	Tabelle 159: TAB KON 578 Ablauf GetSubscription	268
8291	Tabelle 160: TAB KON 579 Fehlercodes „GetSubscription“	269
8292	Tabelle 161: TAB KON 580 Konfigurationswerte des Systeminformationsdienstes	
8293	(Administrator)	269
8294	Tabelle 162: TAB KON 581 Verschlüsselungsdienst-Operationen für	
8295	EVT MONITOR OPERATIONS.....	270
8296	Tabelle 163: TAB KON 747 KeyReference für Encrypt-/DecryptDocument.....	271
8297	Tabelle 164: TAB KON 859 Werteliste und Defaultwert des Parameters crypt bei	
8298	hybrider Verschlüsselung.....	272
8299	Tabelle 165: TAB KON 739 - TUC KON 070 „Daten hybrid verschlüsseln“.....	272
8300	Tabelle 166: TAB KON 073 Vorgaben zum Format verschlüsselter XML-Dokumente...	280
8301	Tabelle 167: TAB KON 740 Fehlercodes TUC KON 070 „Daten hybrid verschlüsseln“	280
8302	Tabelle 168: TAB KON 140 – TUC KON 071 „Daten hybrid entschlüsseln“	281
8303	Tabelle 169: TAB KON 142 Fehlercodes TUC KON 071 „Daten hybrid entschlüsseln“	285
8304	Tabelle 170: TAB KON 741 – TUC KON 072 „Daten symmetrisch verschlüsseln“	285
8305	Tabelle 171: TAB KON 742 Fehlercodes TUC KON 072 „Daten symmetrisch	
8306	verschlüsseln“	286
8307	Tabelle 172: TAB KON 743 - TUC KON 073 „Daten symmetrisch entschlüsseln“	286

8308	Tabelle 173: TAB KON 744 Fehlercodes TUC KON 073 „Daten symmetrisch	
8309	entschlüsseln“	287
8310	Tabelle 174: TAB KON 860 – TUC KON 075 „Symmetrisch verschlüsseln“	287
8311	Tabelle 175: TAB KON 861 - TUC KON 076 „Symmetrisch entschlüsseln“	289
8312	Tabelle 176: TAB KON 745 Basisdienst Verschlüsselungsdienst	290
8313	Tabelle 177: TAB KON 071 Operation EncryptDocument	291
8314	Tabelle 178: TAB KON 746 Ablauf EncryptDocument	302
8315	Tabelle 179: TAB KON 141 Fehlercodes „EncryptDocument“	302
8316	Tabelle 180: TAB KON 075 Operation DecryptDocument	303
8317	Tabelle 181: TAB KON 076 Ablauf DecryptDocument	305
8318	Tabelle 182: TAB KON 145 Fehlercodes „DecryptDocument“	305
8319	Tabelle 183: TAB KON 582 – Signaturverfahren Dokumentensignatur.....	306
8320	Tabelle 184: TAB KON 585 – Zusätzliche Signaturverfahren für	
8321	Dokumentensignaturprüfung.....	308
8322	Tabelle 185: TAB KON 778 – Einsatzbereich der Signaturvarianten für XAdES, CAdES	
8323	und PAdES.....	308
8324	Tabelle 186: TAB KON 583 – Default-Signaturverfahren	311
8325	Tabelle 187: TAB KON 584 nonQES-Operationen für EVT MONITOR OPERATIONS....	311
8326	Tabelle 188: TAB KON 900 Zertifikate und private Schlüssel für Signaturerstellung und	
8327	Signaturprüfung (QES und nonQES)	312
8328	Tabelle 189: TAB KON 862 Werteliste und Defaultwert des Parameters crypt bei QES-	
8329	Erzeugung	313
8330	Tabelle 190: TAB KON 863 Werteliste und Defaultwert des Parameters crypt bei	
8331	nonQES-Erzeugung.....	313
8332	Tabelle 191: TAB KON 748 - TUC KON 155 „Dokumente zur Signatur vorbereiten“ ..	319
8333	Tabelle 192: TAB KON 586 Fehlercodes TUC KON 155 „Dokumente zur Signatur	
8334	vorbereiten“	323
8335	Tabelle 193: TAB KON 749 – TUC KON 165 „Signaturvoraussetzungen für nonQES	
8336	prüfen“	323
8337	Tabelle 194: TAB KON 587 Fehlercodes TUC KON 165 „Signaturvoraussetzungen für	
8338	nonQES prüfen“	324
8339	Tabelle 195: TAB KON 750 – TUC KON 166 „nonQES Signaturen erstellen“	324
8340	Tabelle 196: TAB KON 120 Fehlercodes TUC KON 166 „nonQES Signaturen erstellen“	
8341	325
8342	Tabelle 197: TAB KON 751 – TUC KON 152 „Signaturvoraussetzungen für QES prüfen“	
8343	326
8344	Tabelle 198: TAB KON 588 Fehlercodes TUC KON 152 „Signaturvoraussetzungen für	
8345	QES prüfen“.....	327
8346	Tabelle 199: TAB KON 752 – TUC KON 154 „QES Signaturen erstellen“	327
8347	Tabelle 200: TAB KON 126 Fehlercodes TUC KON 154 „QES Signaturen erstellen“ ...	330

8348	Tabelle 201: TAB KON 293 - TUC KON 168 „Einzelsignatur QES erstellen“	331
8349	Tabelle 202: TAB KON 590 Fehlercodes TUC KON 168 „Einzelsignatur QES erstellen“	332
8350	Tabelle 203: TAB KON 870 – TUC KON 158 „Komfortsignaturen erstellen“	332
8351	Tabelle 204: TAB KON 873 Fehlercodes TUC KON 158 „Komfortsignaturen erstellen“	334
8352	Tabelle 205: TAB KON 753 – TUC KON 160 „Dokumente nonQES signieren“	335
8353	Tabelle 206: TAB KON 127 Fehlercodes TUC KON 160 „Dokumente nonQES signieren“	337
8354	Tabelle 207: TAB KON 753 – TUC KON 160 „Dokumente nonQES signieren“	338
8355	Tabelle 208: TAB KON 127 Fehlercodes TUC KON 160 „Dokumente nonQES signieren“	340
8356	Tabelle 209: TAB KON 121 - TUC KON 161 „nonQES Dokumentensignatur prüfen“	341
8357	Tabelle 210: TAB KON 124 Fehlercodes TUC KON 161 „nonQES Dokumentensignatur prüfen“	345
8358	Tabelle 211: TAB KON 754 Übersicht Status für Prüfung einer Dokumentensignatur ..	346
8359	Tabelle 212: TAB KON 430 – TUC KON 162 „Kryptographische Prüfung der XML-Dokumentensignatur“	348
8360	Tabelle 213: TAB KON 431 Fehlercodes TUC KON 162 „Kryptographische Prüfung der XML-Dokumentensignatur“	349
8361	Tabelle 214: TAB KON 755 – TUC KON 150 „Dokumente QES signieren“	349
8362	Tabelle 215: TAB KON 128 Fehlercodes TUC KON 150 „Dokument QES signieren“ ...	355
8363	Tabelle 216: TAB KON 192 Verhalten des Konnektors beim Abbruch einer Stapelsignatur	356
8364	Tabelle 217: TAB KON 591 - TUC KON 151 „QES-Dokumentensignatur prüfen“	357
8365	Tabelle 218: TAB KON 592 Fehlercodes TUC KON 151 „QES Dokumentensignatur prüfen“	361
8366	Tabelle 219: TAB KON 593 Übersicht Status für Prüfung einer Dokumentensignatur ..	362
8367	Tabelle 220: TAB KON 871 – TUC KON 170 „Dokumente mit Komfort signieren“	363
8368	Tabelle 221: TAB KON 872 Fehlercodes TUC KON 170 „Dokumente mit Komfort signieren“	366
8369	Tabelle 222: TAB KON 883 – TUC KON 171 „Komfortsignatur einschalten“	366
8370	Tabelle 223: TAB KON 886 Fehlercodes TUC KON 171 „Komfortsignatur einschalten“	368
8371	Tabelle 224: TAB KON 884 – TUC KON 172 „Komfortsignatur ausschalten“	368
8372	Tabelle 225: TAB KON 887 Fehlercodes TUC KON 172 „Komfortsignatur ausschalten“	369
8373	Tabelle 226: TAB KON 885 – TUC KON 173 „Liefere Signaturmodus“	370
8374	Tabelle 227: TAB KON 888 Fehlercodes TUC KON 173 „Liefere Signaturmodus“	371
8375	Tabelle 228: TAB KON 197 Basisdienst Signaturdienst (nonQES und QES)	372

8388	Tabelle 229: TAB KON 065 Operation SignDocument (nonQES und QES)	373
8389	Tabelle 230: TAB KON 756 Ablauf Operation SignDocument (nonQES und QES)	385
8390	Tabelle 231: TAB KON 757 Fehlercodes „SignDocument (nonQES und QES)“	386
8391	Tabelle 232: TAB KON 066 Operation VerifyDocument (nonQES und QES)	386
8392	Tabelle 233: TAB KON 760 Ablauf Operation VerifyDocument (nonQES und QES)	391
8393	Tabelle 234: TAB KON 761 Fehlercodes „VerifyDocument (nonQES und QES)“	392
8394	Tabelle 235: TAB KON 840 Operation StopSignature	392
8395	Tabelle 236: TAB KON 841 Ablauf Operation StopSignature	393
8396	Tabelle 237: TAB KON 842 Fehlercodes „StopSignature“	393
8397	Tabelle 238: TAB KON 843 Operation GetJobNumber	393
8398	Tabelle 239: TAB KON 844 Ablauf Operation GetJobNumber	394
8399	Tabelle 240: TAB KON 845 Fehlercodes „GetJobNumber“	394
8400	Tabelle 241: TAB KON 874 ActivateComfortSignature	394
8401	Tabelle 242: TAB KON 877 Ablauf ActivateComfortSignature	395
8402	Tabelle 243: TAB KON 879 Fehlercodes ActivateComfortSignature	396
8403	Tabelle 244: TAB KON 875 DeactivateComfortSignature	396
8404	Tabelle 245: TAB KON 878 Ablauf DeactivateComfortSignature	397
8405	Tabelle 246: TAB KON 880 Fehlercodes DeactivateComfortSignature	397
8406	Tabelle 247: TAB KON 876 GetSignatureMode	397
8407	Tabelle 248: TAB KON 882 Ablauf GetSignatureMode	399
8408	Tabelle 249: TAB KON 881 Fehlercodes GetSignatureMode	399
8409	Tabelle 250: TAB KON 596 Konfigurationswerte des Signaturdienstes (Administrator)	
8410	399
8411	Tabelle 251: TAB KON 596 Konfigurationswerte des Signaturdienstes (Administrator)	
8412	400
8413	Tabelle 252: TAB KON 853- intendedKeyUsage bei Zertifikatsprüfung	402
8414	Tabelle 253: TAB KON 858 Kartenobjekt in Abhängigkeit vom kryptographischen	
8415	Verfahren	403
8416	Tabelle 254: TAB KON 825 Fehlercodes „TLS-Verbindungsaufbau zum TSL-Dienst“ ...	405
8417	Tabelle 255: TAB KON 826 Fehlercodes „TLS-Verbindungsaufbau zum TSL-Dienst bei	
8418	Prüfung der technischen Rolle“	406
8419	Tabelle 256: TAB KON 597 Operationen in EVT MONITOR OPERATIONS	407
8420	Tabelle 257: TAB KON 766 TUC KON 032 „TSL aktualisieren“	407
8421	Tabelle 258: TAB KON 598 Fehlercodes TUC KON 032 „TSL aktualisieren“	410
8422	Tabelle 259: TAB KON 618 TUC KON 031 „BNetzA-VL aktualisieren“	410
8423	Tabelle 260: TAB KON 619 Fehlercodes TUC KON 031 „BNetzA-VL aktualisieren“	411
8424	Tabelle 261: TAB KON 767 TUC KON 040 „CRL aktualisieren“	411
8425	Tabelle 262: TAB KON 599 Fehlercodes TUC KON 040 „CRL aktualisieren“	413

8426	Tabelle 263: TAB KON 768 TUC KON 033 „Zertifikatsablauf prüfen“	413
8427	Tabelle 264: TAB KON 600 Fehlercodes TUC KON 033 „Zertifikatsablauf prüfen“	416
8428	Tabelle 265: TAB KON 769 TUC KON 037 „Zertifikat prüfen“	416
8429	Tabelle 266: TAB KON 601 Fehlercodes TUC KON 037 „Zertifikat prüfen“	421
8430	Tabelle 267: TAB KON 818 TUC KON 042 „CV-Zertifikat prüfen“	421
8431	Tabelle 268: TAB KON 819 Fehlercodes TUC KON 042 „CV-Zertifikat prüfen“	423
8432	Tabelle 269: TAB KON 770 TUC KON 034 „Zertifikatsinformationen extrahieren“	423
8433	Tabelle 270: TAB KON 602 Fehlercodes TUC KON 034 „Zertifikatsinformationen	
8434	extrahieren“	426
8435	Tabelle 271: TAB KON 771 Basisanwendung Zertifikatsdienst	426
8436	Tabelle 272: TAB KON 676 Operation CheckCertificateExpiration	427
8437	Tabelle 273: TAB KON 677 Ablauf CheckCertificateExpiration	428
8438	Tabelle 274: TAB KON 603 Fehlercodes „CheckCertificateExpiration“	429
8439	Tabelle 275: TAB KON 678 Operation ReadCardCertificate	430
8440	Tabelle 276: TAB KON 679 Ablauf ReadCardCertificate	432
8441	Tabelle 277: TAB KON 604 Fehlercodes „ReadCardCertificate“	433
8442	Tabelle 278: TAB KON 795 Operation VerifyCertificate	434
8443	Tabelle 279: TAB KON 797 Ablauf VerifyCertificate	435
8444	Tabelle 280: TAB KON 800 Fehlercodes „VerifyCertificate“	436
8445	Tabelle 281: TAB KON 772 TUC KON 035 „Zertifikatsdienst initialisieren“	436
8446	Tabelle 282: TAB KON 605 Fehlercodes TUC KON 035 „Zertifikatsdienst initialisieren“	
8447	437
8448	Tabelle 283: TAB KON 606 Konfiguration des Zertifikatsdienstes	438
8449	Tabelle 284: TAB KON 733 Einsehbare Konfigurationsparameter des Zertifikatsdienstes	
8450	439
8451	Tabelle 285: TAB KON 857 - Fehlercodes beim Import des Cross-Zertifikats für TI-	
8452	Vertrauensanker ECC	441
8453	Tabelle 286: TAB KON 607 – TUC KON 271 „Schreibe Protokolleintrag“	444
8454	Tabelle 287: TAB KON 608 Fehlercodes TUC KON 271 „Schreibe Protokolleintrag“ ...	447
8455	Tabelle 288: TAB KON 609 Konfigurationswerte des Protokollierungsdienstes	
8456	(Administrator)	449
8457	Tabelle 289: TAB KON 610 – TUC KON 272 „Initialisierung Protokollierungsdienst“ ..	450
8458	Tabelle 290: TAB KON 611 Fehlercodes TUC KON 272 „Initialisiere	
8459	Protokollierungsdienst“	451
8460	Tabelle 291: TAB KON 773 – TUC KON 110 „Kartenbasierte TLS-Verbindung aufbauen“	
8461	452
8462	Tabelle 292: TAB KON 612 Fehlercodes TUC KON 110 „Kartenbasierte TLS-Verbindung	
8463	aufbauen“	453

8464	Tabelle 293: TAB KON 774 - TUC KON 111 „Kartenbasierte TLS-Verbindung abbauen“	
8465	454
8466	Tabelle 294: TAB KON 613 Fehlercodes TUC KON 111 „Kartenbasierte TLS-Verbindung	
8467	abbauen“ 	455
8468	Tabelle 295: TAB KON 805 - TUC KON 290 „LDAP-Verbindung aufbauen“ 	456
8469	Tabelle 296: TAB KON 815 – TUC KON 291 „Verzeichnis abfragen“ 	457
8470	Tabelle 297: TAB KON 816 – TUC KON 292 „LDAP-Verbindung trennen“..... 	458
8471	Tabelle 298: TAB KON 817 – TUC KON 293 „Verzeichnisabfrage abbrechen“ 	459
8472	Tabelle 299: TAB KON 780 – Signaturverfahren Externe Authentisierung 	460
8473	Tabelle 300: TAB KON 839 Basisdienst Authentifizierungsdienst 	461
8474	Tabelle 301: TAB KON 781 Operation ExternalAuthenticate 	462
8475	Tabelle 302: TAB KON 782 Ablauf Operation ExternalAuthenticate 	465
8476	Tabelle 303: TAB KON 783 Übersicht Fehler Operation ExternalAuthenticate 	465
8477	Tabelle 304: TAB KON 784 Privater Schlüssel je Karte für ExternalAuthenticate 	465
8478	Tabelle 305: TAB KON 680 Mapping der Netzwerksegmente 	468
8479	Tabelle 306: TAB KON 681 Definition der vom Konnektor verwendeten VPN-Tunnel .. 	469
8480	Tabelle 307: TAB KON 682 Definition der Konnektor IP-Adressen 	469
8481	Tabelle 308: TAB KON 614 - TUC KON 305 „LAN-Adapter initialisieren“ 	479
8482	Tabelle 309: TAB KON 615 Fehlercodes TUC KON 305 „LAN-Adapter initialisieren“... 	480
8483	Tabelle 310: TAB KON 616 - TUC KON 306 „WAN-Adapter initialisieren“ 	480
8484	Tabelle 311: TAB KON 617 Fehlercodes TUC KON 306 „WAN-Adapter initialisieren“ . 	481
8485	Tabelle 312: TAB KON 622 - TUC KON 304 „Netzwerk-Routen einrichten“ 	482
8486	Tabelle 313: TAB KON 623 Fehlercodes TUC KON 304 „Netzwerk-Routen einrichten“	
8487 	484
8488	Tabelle 314: TAB KON 683 LAN-Adapter IP-Konfiguration 	485
8489	Tabelle 315: TAB KON 684 LAN-Adapter Erweiterte Parameter 	485
8490	Tabelle 316: TAB KON 685 WAN-Adapter IP-Konfiguration 	486
8491	Tabelle 317: TAB KON 686 WAN-Adapter Erweiterte Parameter 	487
8492	Tabelle 318: TAB KON 624 – „Konfigurationsparameter der Anbindung LAN/WAN“ 	488
8493	Tabelle 319: TAB KON 625 - Konfigurationsparameter Firewall-Schnittstelle 	491
8494	Tabelle 320: TAB KON 626 „Liefere Netzwerkinformationen über DHCP“ 	492
8495	Tabelle 321: TAB KON 627 „Aktivierung des DHCP-Servers“ 	493
8496	Tabelle 322: TAB KON 628 „Basiskonfiguration des DHCP-Servers“ 	494
8497	Tabelle 323: TAB KON 629 „Client-Gruppenspezifische Konfigurationsoptionen des	
8498	Konnektor-DHCP-Servers“ 	494
8499	Tabelle 324: TAB KON 630 - TUC KON 343 „Initialisierung DHCP-Server“ 	496
8500	Tabelle 325: TAB KON 631 Fehlercodes TUC KON 343 „Initialisierung DHCP-Server“ 	497
8501	Tabelle 326: TAB KON 632 – TUC KON 341 „DHCP Informationen beziehen“ 	498

8502	Tabelle 327: TAB KON 633 Fehlercodes TUC KON 341 „DHCP-Informationen beziehen“	499
8503	
8504	Tabelle 328: TAB KON 634 „Konfiguration des DHCP-Clients“	500
8505	Tabelle 329: TAB KON 635 – TUC KON 321 „Verbindung zu dem VPN-Konzentrator der	
8506	TI aufbauen“	502
8507	Tabelle 330: TAB KON 636 Fehlercodes TUC KON 321 „Verbindung zu dem VPN-	
8508	Konzentrator der TI aufbauen“	504
8509	Tabelle 331: TAB KON 637 – TUC KON 322 „Verbindung zu dem VPN-Konzentrator der	
8510	SIS aufbauen“	504
8511	Tabelle 332: TAB KON 638 Fehlercodes TUC KON 322 „Verbindung zu dem VPN-	
8512	Konzentrator der SIS aufbauen“	506
8513	Tabelle 333: TAB KON 639 – Konfigurationsparameter VPN-Client	507
8514	Tabelle 334: TAB KON 640 Zustandswerte für Konnektor NTP-Server	509
8515	Tabelle 335: TAB KON 776 TUC KON 351 „Liefere Systemzeit“	510
8516	Tabelle 336: TAB KON 641 Fehlercodes TUC KON 351 „Liefere Systemzeit“	511
8517	Tabelle 337: TAB KON 642 Operation sync Time	511
8518	Tabelle 338: TAB KON 643 Konfiguration des Konnektor NTP-Servers	512
8519	Tabelle 339: TAB KON 730 Einsehbare Konfigurationsparameter des Konnektor NTP-	
8520	Servers	512
8521	Tabelle 340: TAB KON 644 – TUC KON 352 „Initialisierung Zeitdienst“	512
8522	Tabelle 341: TAB KON 645 Fehlercodes TUC KON 352 „Initialisierung Zeitdienst“	513
8523	Tabelle 342: TAB KON 687 DNS-Forwards des DNS-Servers	514
8524	Tabelle 343: TAB KON 646 – TUC KON 361 „DNS-Namen auflösen“	516
8525	Tabelle 344: TAB KON 647 Fehlercodes TUC KON 361 „DNS Namen auflösen“	517
8526	Tabelle 345: TAB KON 646 – TUC KON 361 „DNS-Namen auflösen“	517
8527	Tabelle 346: TAB KON 647 Fehlercodes TUC KON 361 „DNS Namen auflösen“	518
8528	Tabelle 347: TAB KON 648 – TUC KON 362 „Liste der Dienste abrufen“	518
8529	Tabelle 348: TAB KON 649 Fehlercodes TUC KON 362 „Liste der Dienste abrufen“	519
8530	Tabelle 349: TAB KON 650 - TUC KON 363 „Dienstdetails abrufen“	519
8531	Tabelle 350: TAB KON 651 Fehlercodes TUC KON 363 „Dienstdetails abrufen“	520
8532	Tabelle 351: TAB KON 652 Basisanwendung Namensdienst	520
8533	Tabelle 352: TAB KON 653 Operation GetIPAddress	521
8534	Tabelle 353: TAB KON 654 - Konfigurationsparameter Namensdienst	522
8535	Tabelle 354: TAB KON 731 Einsehbare Konfigurationsparameter Namensdienst	522
8536	Tabelle 355: TAB KON 655 Konfigurationen der Benutzerverwaltung (Super-	
8537	Administrator)	527
8538	Tabelle 356: TAB KON 656 Konfigurationen der Benutzerverwaltung	528
8539	Tabelle 357: TAB KON 657 Konfigurationsparameter des Konnektornamens	528

8540	Tabelle 358: TAB KON 833 Bezeichner für persistente Konfigurationsdaten für	
8541	Fachmodule.....	532
8542	Tabelle 359: TAB KON 658 Aktivieren/Deaktivieren von Leistungsumfängen.....	533
8543	Tabelle 360: TAB KON 659 Konnektor Standalone einsetzen.....	534
8544	Tabelle 361: TAB KON 661 Konfigurationsparameter der Konnektorfreisaltung	535
8545	Tabelle 362: TAB KON 732 Einsehbare Konfigurationsparameter der	
8546	Konnektorfreisaltung	535
8547	Tabelle 363: TAB KON 662 Zustandswerte der Konnektorfreisaltung	535
8548	Tabelle 364: TAB KON 851 Einschränkung der Rechte des Remote-Administrators	
8549	(Blacklist).....	539
8550	Tabelle 365: TAB KON 663 Konfigurationen des Remote Managements.....	540
8551	Tabelle 366: TAB KON 664 – TUC KON 280 „Konnektoraktualisierung durchführen“ ..	543
8552	Tabelle 367: TAB KON 665 Fehlercodes TUC KON 280 „Konnektoraktualisierung	
8553	durchführen“	545
8554	Tabelle 368: TAB KON 666 – TUC KON 281 „Kartenterminalaktualisierung anstoßen“	
8555	548
8556	Tabelle 369: TAB KON 667 Fehlercodes TUC KON 281 „Kartenterminalaktualisierung	
8557	anstoßen“	550
8558	Tabelle 370: TAB KON 668 – TUC KON 282 „UpdateInformationen beziehen“.....	550
8559	Tabelle 371: TAB KON 669 Fehlercodes TUC KON 282 „UpdateInformationen beziehen“	
8560	552
8561	Tabelle 372: TAB KON 799 – TUC KON 283 „Infrastruktur Konfiguration aktualisieren“	
8562	552
8563	Tabelle 373: Tab Kon 726 Fehlercodes TUC KON 283 „Infrastruktur Konfiguration	
8564	aktualisieren“	556
8565	Tabelle 374: TAB KON 833 – TUC KON 285 „UpdateInformationen für Fachmodul	
8566	beziehen“	556
8567	Tabelle 375: TAB KON 834 Fehlercodes TUC KON 285 „UpdateInformationen für	
8568	Fachmodul beziehen“	558
8569	Tabelle 376: TAB KON 835 – TUC KON 286 „Paket für Fachmodul laden“.....	559
8570	Tabelle 377: TAB KON 836 Fehlercodes TUC KON 286 „Paket für Fachmodul laden“ ..	560
8571	Tabelle 378: TAB KON 864 – TUC KON 284 „KSR-Client initialisieren“	560
8572	Tabelle 379: TAB KON 822 Fehlercodes TUC KON 284 „KSR-Client initialisieren“	561
8573	Tabelle 380: TAB KON 670 Konfigurationsparameter der Software-Aktualisierung	561
8574	Tabelle 381: TAB KON 820 Einsehbare Konfigurationsparameter der Software-	
8575	Aktualisierung.....	562
8576	Tabelle 382: TAB KON 671 Anforderungen Klima	569
8577	Tabelle 383: TAB KON 672 Anforderungen Vibration.....	569
8578	Tabelle 384: TAB KON 672 Anforderungen Vibration.....	570
8579	Tabelle 385: TAB KON 779 „Profilierung der Signaturformate“	609

Tabelle 386 TAB KON 775 „Profilierung der Dokumentformate und Nachrichten“	616
Tabelle 387: TAB KON 688 Version der Schemas aus dem Namensraum des Konnektors	618
Tabelle 388: TAB KON 798 Schnittstellenversionen	621
Tabelle 389 – TAB KON 777 Events Interne Mechanismen	627
Tabelle 390 – TAB KON 711 Architektur der TI-Plattform, Berechtigt Fachmodule	645
Tabelle 391 – TAB KON 712 Architektur der TI-Plattform, Berechtigt Clientsysteme...	650
Tabelle 392 – TAB KON 713 Architektur der TI-Plattform, Berechtigt eHealth-KT.....	652
Tabelle 393 – TAB KON 714 Architektur der TI-Plattform, Berechtigt Administrator ...	652
Tabelle 394: Aufzähltypen	675

5.5 Referenzierte Dokumente

5.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer sind in der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemKPT_Sich_Kon]	gematik: Sicherheitskonzept Konnektor
[gemKPT_Test]	gematik: Testkonzept
[gemSpec_COS]	gematik: Spezifikation des Card Operating System (COS) – Elektrische Schnittstelle
[gemSpec_Karten_Fach_TIP]	gematik: Befüllvorschriften für die Plattformanteile der Karten der TI
[gemSpec_Kon_SigProxy]	gematik: Spezifikation Konnektor Signaturproxy
[gemSpec_Kon_TBAuth]	gematik: Spezifikation Konnektor Basisdienst tokenbasierte Authentisierung
[gemSpec_eGK_ObjSys]	gematik: Spezifikation der elektronischen Gesundheitskarte eGK-Objektsystem - für Karten der Generation 2

[gemSpec_eGK_ObjSys_G2.1]	gematik: Spezifikation der elektronischen Gesundheitskarte eGK-Objektsystem - für Karten der Generation 2.1
[gemSpec_eGK_P1]	gematik: Die Spezifikation der elektronische Gesundheitskarte; Teil 1 – Spezifikation der elektrischen Schnittstelle - für Karten der Generation 1+
[gemSpec_eGK_P2]	gematik: Die Spezifikation der elektronische Gesundheitskarte; Teil 2 – Grundlegende Applikationen - für Karten der Generation 1+
[gemSpec_gSMC-K_ObjSys]	gematik: Spezifikation der gSMC-K Objektsystem
[gemSpec_gSMC-KT_ObjSys]	gematik: Spezifikation gSMC-KT Objektsystem
[gemSpec_HBA_ObjSys]	gematik: Spezifikation HBA Objektsystem
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_KSR]	gematik: Spezifikation Konfigurationsdienst
[gemSpec_KT]	gematik: Spezifikation eHealth-Kartenterminal
[gemSpec_Net]	gematik: Spezifikation Netzwerk
[gemSpec_OID]	gematik: Spezifikation OID
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_Perf]	gematik: Performance und Mengengerüst TI-Plattform
[gemSpec_PKI]	gematik: Spezifikation PKI
[gemSpec_SMC-B_ObjSys]	gematik: Spezifikation SMC-B Objektsystem
[gemSpec_VPN_ZugD]	gematik: Spezifikation VPN-Zugangsdienst
[gemSpec_VZD]	gematik: Spezifikation Verzeichnisdienst

8601 5.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[7816-4]	ISO/IEC 7816-4: 2005 (2nd edition) Identification cards — Integrated circuit cards - Part 4: Organization, security and commands for interchange
[ALGCAT]	Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, vom 11.12.2015 (auch online verfügbar: https://www.bundesanzeiger.de mit dem Suchbegriff „BAnz AT 01.02.2016 B5“).

[Basic Profile1.2]	Basic Profile Version 1.2 http://www.ws-i.org/Profiles/BasicProfile-1.2-2010-11-09.html
[Basic Profile2.0]	Basic Profile Version 2.0 http://www.ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html
[BSI_GK]	BSI: IT-Grundschutz-Kataloge (15. Ergänzungslieferung 2016) https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf
[BSI-TR-03111]	Technical Guideline BSI TR-03111 Elliptic Curve Cryptography, Version 2.10, Date: 2018-06-01 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechnicalGuidelines/TR03111/BSI-TR-03111_V-2-1_pdf.pdf?__blob=publicationFile&v=2
[BSI-TR03114]	BSI (22.10.2007): Technische Richtlinie – Stapelsignatur mit dem Heilberufsausweis; Version 2.0 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03114/BSI-TR-03114.pdf?__blob=publicationFile&v=1
[BSI TR-03120]	BSI (23.10.2007): BSI - Technische Richtlinie – Sichere Kartenterminalidentität (Betriebskonzept); Version 1.0 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03120/BSI-TR-03120.pdf?__blob=publicationFile&v=1
[CAeS]	ETSI: Electronic Signature Formats, Electronic Signatures and Infrastructures (ESI) – Technical Specification, ETSI TS 101 733 V2.2.1, via http://www.etsi.org
[Canon XML1.1]	Canonical XML Version 1.1 http://www.w3.org/TR/2008/REC-xml-c14n11-20080502/
[CDA]	ISO/HL7 27932:2009 Data Exchange Standards -- HL7 Clinical Document Architecture, Release 2
[CDA-Sig]	Erstellung von XML-Signaturen für Dokumente nach Clinical Documents Architecture – R2, Elektronische Signatur von Arztbriefen, Ärztekammern in NRW im Auftrag der Bundesärztekammer, Version 1.6 vom 19.04.2010
[COMMON_PKI]	Common PKI Specifications for Interoperable Applications Version 2.0, 20 January 2009 http://www.t7ev.org/themen/entwickler/common-pki-v20-spezifikation.html ISIS-MTT Core Specification, 2004, Version 1.1 https://www.teletrust.de/fileadmin/files/ISIS-MTT_Profile_SigGOptions_v1.1.pdf

[CMS]	Cryptographic Message Syntax (CMS), September 2009 http://tools.ietf.org/html/rfc5652
[DIN 66003]	DIN 66003:1999 Informationsverarbeitung; 7-Bit-Code
[HPC-P1]	Spezifikation des elektronischen Heilberufsausweises Version 2.3.2, 05.08.2009, Teil I: Kommandos, Algorithmen und Funktionen der COS Plattform
[HPC-P2]	Spezifikation des elektronischen Heilberufsausweises Version 2.3.2, 05.08.2009, Teil II: HPC - Anwendungen und Funktionen
[HPC-P3]	Spezifikation des elektronischen Heilberufsausweises Version 2.3.2, 05.08.2009, Teil III: SMC - Anwendungen und Funktionen
[HüKo06]	BSI (2006): Hühnlein, Detlef/Korte, Ulrike: Grundlagen der elektronischen Signatur
[IEEE 802.3]	Technical Committee Computer Communications of the IEEE Computer Society, USA (1985): IEEE standards for local area networks: carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications ISBN: 0-7381-4253-0
[ISO 8601]	International Organization for Standardization (2006-09): Data elements and interchange formats -- Information interchange -- Representation of dates and times
[KVK]	Spitzenverbände der Krankenkassen, Kassenärztliche Bundesvereinigung und Kassenzahnärztlichen Bundesvereinigung (gültig ab 25. November 2009): Technische Spezifikation der Versichertenkarte Version: 2.08
[MIME]	RFC 2045 , RFC 2046 , RFC 2047 , RFC 2048 , RFC 2049
[NTPv4]	Internet Engineering Task Force (IETF) (06/2010): Network Time Protocol Version 4: Protocol and Algorithms Specification http://www.ietf.org/rfc/rfc5905.txt
[OASIS-AdES]	OASIS: Advanced Electronic Signature Profiles of the OASIS Digital Signature Service Version 1.0, OASIS Standard, http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-AdES-spec-v1.0-os.pdf
[OASIS-DSS]	OASIS: Digital Signature Service Core Protocols, Elements, and Bindings, Version 1.0, OASIS Standard, via http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf

[OASIS-SP]	OASIS: Signature Policy Profile of the OASIS Digital Signature Services Version 1.0, Committee Draft 01, 18 May 2009, http://docs.oasis-open.org/dss-x/profiles/sigpolicy/oasis-dssx-1.0-profiles-sigpolicy-cd01.pdf
[OASIS-VR]	OASIS: Profile for comprehensive multi-signature verification reports for OASIS Digital Signature Services Version 1.0, Committee Specification 01, 12 November 2010, http://docs.oasis-open.org/dss-x/profiles/verificationreport/oasis-dssx-1.0-profiles-vr-cs01.pdf
[PAdES-1]	European Telecommunications Standards Institute (ETSI): Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview – a framework document for PAdES, ETSI TS 102 778-1 V1.1.1, Technical Specification, 2009
[PAdES-3]	European Telecommunications Standards Institute (ETSI): Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced – PAdES-BES and PAdES-EPES Profiles, ETSI TS 102 778-3 V1.1.2, Technical Specification, 2009
[PAdES-4]	European Telecommunications Standards Institute (ETSI): Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term – PAdES-LTV Profile, ETSI TS 102 778-4 V1.1.2, Technical Specification, 2009
[ISO 19005]	ISO 19005 – Document management – Electronic document file format for long-term preservation
[PDF/A-2]	ISO 19005-2:2011 – Document management – Electronic document file format for long-term preservation – Part 2: Use of ISO 32000-1 (PDF/A-2)
[PP_NK]	Common Criteria Schutzprofil (Protection Profile) Schutzprofil 1: Anforderungen an den Netzkonnektor BSI-CC-PP-0097
[PP_KON]	Common Criteria Schutzprofil (Protection Profile) Schutzprofil 2: Anforderungen an den Konnektor: BSI-CC-PP-0098
[RFC792]	IETF (September 1981) INTERNET CONTROL MESSAGE PROTOCOL http://tools.ietf.org/html/rfc792
[RFC1034]	RFC 1034 (November 1987): Domain Names – Concepts and Facilities http://tools.ietf.org/html/rfc1034
[RFC1122]	RFC 1122 (Oktober 1989): Requirements for Internet Hosts -- Communication Layers http://tools.ietf.org/html/rfc1122

[RFC1812]	F. Baker (ed.): Requirements for IP Version 4 Routers, IETF RFC 1812, http://www.ietf.org/rfc/rfc1812.txt
[RFC1918]	RFC1918 (Februar 1996): Address Allocation for Private Internets http://tools.ietf.org/html/rfc1918
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://tools.ietf.org/html/rfc2119
[RFC2131]	Network Working Group (03/1997): Dynamic Host Configuration Protocol http://www.ietf.org/rfc/rfc2131.txt
[RFC2132]	Network Working Group (03/1997): DHCP Options and BOOTP Vendor Extensions http://www.ietf.org/rfc/rfc2132.txt
[RFC2617]	Network Working Group (06/1999): HTTP Authentication: Basic and Digest Access Authentication http://www.ietf.org/rfc/rfc2617.txt
[RFC2818]	Network Working Group (05/2000): HTTP Over TLS http://www.ietf.org/rfc/rfc2818.txt
[RFC3447]	B. Kaliski: PKCS #1: RSA Encryption, Version 2.1, RFC3447,
[RFC2616]	Network Working Group (06/1999): Hypertext Transfer Protocol -- HTTP/1.1 http://www.ietf.org/rfc/rfc2616.txt
[RFC2644]	D. Senie: <i>Changing the Default for Directed Broadcasts in Routers</i> , IETF RFC 2644, http://www.ietf.org/rfc/rfc2644.txt
[RFC2663]	P. Srisuresh, M. Holdrege: <i>IP Network Address Translator (NAT) Terminology and Considerations</i> , IETF RFC 2663, http://www.ietf.org/rfc/rfc2663.txt
[RFC3022]	RFC 3022 (Januar 2001): Traditional IP Network Address Translator (Traditional NAT) http://tools.ietf.org/html/rfc3022
[RFC3275]	D. Eastlake, J. Reagle, D. Solo: <i>(Extensible Markup Language) XML Signature Syntax and Processing</i> , IETF RFC 3275, via http://www.ietf.org/rfc/rfc3275.txt
[RFC3279]	W. Polk, R. Hously, L. Bassham: <i>Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile</i> , IETF RFC 3279, http://www.ietf.org/rfc/rfc3279.txt

[RFC3629]	Network Working Group (11/2003): UTF-8, a transformation format of ISO 10646 http://www.ietf.org/rfc/rfc3629.txt
[RFC3927]	Network Working Group (05/2005): Dynamic Configuration of IPv4 Link-Local Addresses http://www.ietf.org/rfc/rfc3927.txt
[RFC3986]	Network Working Group (01/2005): Uniform Resource Identifier (URI): Generic Syntax
[RFC4122]	RFC 4122 (July 2005): A Universelly Unique Identifier UUID URN Namespace http://tools.ietf.org/html/rfc4122
[RFC4632]	Network Working Group (08/2006): Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan http://tools.ietf.org/html/rfc4632
[RFC5246]	RFC 5246 (August 2008): The Transport Layer Security (TLS) Protocol Version 1.2; http://tools.ietf.org/html/rfc5246
[RFC5652]	R. Housley: Cryptographic Message Syntax (CMS), RFC 5652 (September 2009) http://tools.ietf.org/html/rfc5652
[RFC 6598]	RFC 6598 (April 2012): IANA-Reserved IPv4 Prefix for Shared Address Space http://tools.ietf.org/html/rfc6598
[RFC6931]	RFC 6931 (April 2013): Additional XML Security Uniform Resource Identifiers (URIs) http://tools.ietf.org/html/rfc6931
[RFC7159]	RFC 7159 (March 2014): The JavaScript Object Notation (JSON) Data Interchange Format http://tools.ietf.org/html/rfc7159
[S/MIME]	RFC 5751 (Januar 2010): Secure/Multipurpose Internet Mail Extensions (S/MIME), Version 3.2, Message Specification http://www.ietf.org/rfc/rfc5751.txt
[SOAP1.1]	Simple Object Access Protocol (SOAP) 1.1 W3C Note (08 May 2000) https://www.w3.org/TR/2000/NOTE-SOAP-20000508/
[SOAP1.2]	SOAP Version 1.2 Part 1: Messaging Framework (Second Edition) W3C Recommendation (27 April 2007) http://www.w3.org/TR/2007/REC-soap12-part1-20070427/

[SICCT]	TeleTrust (17.12.2010): SICCT Secure Interoperable ChipCard Terminal, Version 1.21 https://www.teletrust.de/fileadmin/docs/projekte/sicct/SICCT-Spezifikation-1.21.pdf
[TIFF6]	TIFF Revision 6.0 (Final, June 3, 1992) https://www.adobe.io/open/standards/TIFF/_jcr_content/contentbody/download/file.res/TIFF6.pdf.html
[WSDL1.1]	W3C Note (15.03.2001): Web Services Description Language (WSDL) 1.1 http://www.w3.org/TR/wsdl
[XAdES]	European Telecommunications Standards Institute (ETSI): Technical Specification XML Advanced Electronic Signatures (XAdES). ETSI Technical Specification TS 101 903, Version 1.4.2, 2010
[XMLDSig]	W3C Recommendation (06.2008): XML-Signature Syntax and Processing http://www.w3.org/TR/2008/REC-xmlsig-core-20080610/
[XMLEnc]	XML Encryption Syntax and Processing W3C Recommendation 11 April 2013 http://www.w3.org/TR/xmlenc-core1/
[XPath]	W3C Recommendation (14 December 2010) XML Path Language (XPath) 2.0 (Second Edition) http://www.w3.org/TR/2010/REC-xpath20-20101214/
[XSLT]	W3C Recommendation (23 January 2007) XSL Transformations (XSLT) Version 2.0 http://www.w3.org/TR/2007/REC-xslt20-20070123/
[XAdES Baseline Profile]	European Telecommunications Standards Institute (ETSI): Electronic Signatures and Infrastructure (ESI); XAdES Baseline Profile; ETSI Technical Specification TS 103 171, Version 2.1.1, 2012-03
[CADES Baseline Profile]	European Telecommunications Standards Institute (ETSI): Electronic Signatures and Infrastructure (ESI); CADES Baseline Profile; ETSI Technical Specification TS 103 173, Version 2.1.1, 2013-04
[PADES Baseline Profile]	European Telecommunications Standards Institute (ETSI): Electronic Signatures and Infrastructure (ESI); PAdES Baseline Profile; ETSI Technical Specification TS 103 172, Version 2.2.2, (2013-04)
[XSL]	W3C Recommendation (05.12.2006): Extensible Stylesheet language (XSL) Version 1.1 http://www.w3.org/TR/2006/REC-xsl11-20061205/

[MTOM]	SOAP Message Transmission Optimization Mechanism W3C Recommendation 25 January 2005 http://www.w3.org/TR/2005/REC-soap12-mtom-20050125/
[MTOM-SOAP1.1]	W3C Member Submission 05 April 2006 SOAP 1.1 Binding for MTOM 1.0 https://www.w3.org/Submission/soap11mtom10/
[WS-MTOM Policy]	W3C Member Submission 18 November 2007 MTOM Serialization Policy Assertion 1.1
[COS-G2]	Common Criteria Protection Profile, Card Operating System Generation 2, (PP COS G2), BSI-CC-PP-0082-V2

8602
8603

6 Anhang B – Profilierung der Signatur- und Verschlüsselungsformate (normativ)

6.1 Profilierung der Verschlüsselungsformate

6.2 Profilierung der Signaturformate

Tabelle 385: TAB_KON_779 „Profilierung der Signaturformate“

Aspekt (QES/nonQES)	Festlegung (XML-Signatur/CMS-Signatur/PDF-Signatur)
Zertifikatsreferenz (QES und nonQES)	<p><u>XML-Signatur</u> Bei der Signaturerstellung ist das XML-Element <code>SigningCertificate</code> gemäß den Vorgaben aus XAdES Kapitel 7.2.2 „The SigningCertificate element“ anzulegen. Bei der Signaturprüfung ist es gemäß XAdES Kapitel G.2.2.5 „Verification technical rules“ [XAdES] zu prüfen. Grundsätzlich sind auch Signaturen zu prüfen, die keine Zertifikatsreferenz enthalten. Das Prüfergebnis muss dann widerspiegeln, dass diese Sicherheitsfunktion nicht enthalten war.</p> <p><u>CMS-Signatur</u> Bei der Signaturerstellung ist das Attribut <code>signing certificate reference</code> gemäß CAAdES Kapitel 5.7.3 „Signing Certificate Reference Attributes“ [CAAdES] anzulegen. Bei der Signaturprüfung ist es gemäß CAAdES Kapitel 5.6.3 „Message signature verification process“ [CAAdES] zu prüfen. Grundsätzlich sind auch Signaturen zu prüfen, die keine Zertifikatsreferenz enthalten. Das Prüfergebnis muss dann widerspiegeln, dass diese Sicherheitsfunktion nicht enthalten war.</p> <p><u>PDF-Signatur</u> Bei der Signaturerstellung ist das Attribut <code>signing certificate reference</code> gemäß den Vorgaben aus [PAdES-3] Kapitel 4.4.3 „Signing Certificate Reference Attribute“ anzulegen. Bei der Signaturprüfung ist es gemäß [PAdES-3] Kapitel 4.6.1 „Signing Certificate Reference Validation“ zu prüfen. Grundsätzlich sind auch Signaturen zu prüfen, die keine Zertifikatsreferenz enthalten. Das Prüfergebnis muss dann widerspiegeln, dass diese Sicherheitsfunktion nicht enthalten war.</p>

Signaturablage	<u>PDF-Signatur</u> Sie Signatur wird als Incremental Update gemäß [PDF/A-2] Kapitel 7.5.6 an das Dokument angefügt.
Parallelsignatur (QES und nonQES)	<u>XML-Signatur</u> Parallele Signaturen werden durch je ein <code>ds:signature</code> -Element pro Signatur abgebildet. Für die Signaturvariante „enveloping“ werden parallele Signaturen nicht angeboten. <u>CMS-Signatur:</u> Parallele Signaturen werden durch je einen <code>SignerInfo</code> -Container pro Signatur realisiert. <u>PDF-Signatur:</u> Parallele Signaturen werden nicht angeboten.
Dokumentexkludierende Gegensignatur (QES und nonQES)	<u>XML-Signatur</u> Die Implementierung erfolgt mittels Countersignature gemäß [XAdES], Kapitel 7.2.4. Jede vorhandene Parallel-Signatur wird gegensigniert. <u>CMS-Signatur:</u> Die Implementierung erfolgt mittels der Countersignature gemäß CMS-Spezifikation [RFC5652]. Jede vorhandene Parallel-Signatur wird gegensigniert. <u>PDF-Signatur:</u> Dokumentexkludierende Gegensignaturen werden nicht angeboten.
Referenzierung (QES und nonQES)	<u>XML-Signatur</u> Bei der Signaturerzeugung verwendet der Konnektor in der Signatur nur ID-basierte Referenzen. Bei der Signaturprüfung reagiert der Konnektor bei Abweichungen hiervon mit Fehler 4208.
	<u>XML-Signatur / CMS-Signatur</u> Bei XML-Dokumenten und XML-Signaturen kann die Referenzierung von Objekten auf zwei Arten erfolgen: <ul style="list-style-type: none"> – Ist kein XML-Schema vorhanden, so werden die Werte des ID-Attributs des referenzierten Elements verwendet. – Wird ein XML-Schema übergeben, so muss dieses die ID-Attribute zur Referenzierung festlegen. Bei Abweichungen reagiert der Konnektor mit Fehlercode 4115.
Anzahl unterstützter Signaturen (QES und nonQES)	<u>XML-Signatur / CMS-Signatur / PDF-Signatur</u> Es müssen mindestens 20 Signaturen pro Dokument unterstützt werden. Sind mehr als die unterstützte Anzahl von Signaturen in einem Dokument enthalten, wird die Operation mit Fehler 4001 abgebrochen.

6.3 Profilierung VerificationReport

Anforderung eines ausführlichen Prüfberichts

Folgende Aufrufparameter müssen unterstützt werden:

```
<ReturnVerificationReport
  xmlns="urn:oasis:names:tc:dss-x:1.0:profiles:verificationreport:schema#"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:dss-x:1.0:profiles:verificationreport:schema#
    oasis-dssx-1.0-profiles-vr-cd1.xsd">
  <IncludeVerifier>false</IncludeVerifier>
  <IncludeCertificateValues>true</IncludeCertificateValues>
  <IncludeRevocationValues>true</IncludeRevocationValues>
  <ExpandBinaryValues>false</ExpandBinaryValues>
  <ReportDetailLevel>
    urn:oasis:names:tc:dss-
    x:1.0:profiles:verificationreport:reportdetail:allDetails
  </ReportDetailLevel>
</ReturnVerificationReport>
```

Verwendung des erzeugten VerificationReport

Für die folgenden Inhalte müssen die angegebenen Strukturen benutzt werden. Im Standard angegebene Pflichtfelder von erzeugten Strukturen müssen ggf. zusätzlich gefüllt werden:

1. Prüfzeitpunkt (Systemzeit des Konnektors zum Zeitpunkt der Prüfung)

```
/VerificationReport/
  dss:VerificationTimeInfo/
    dss:VerificationTime
```

2. Signaturzeitpunkt(Ermittelter_Signaturzeitpunkt_Eingebettet)

```
/VerificationReport/
  IndividualReport/
    SignedObjectIdentifier/
      SignedProperties/
        SignedSignatureProperties/
          XAdES:SigningTime
```

Die Signierzeit SigningTime ist nicht nur für XAdES-Signaturen, sondern allgemein für Signaturen gemäß AdES-Baseline-Profilierung, also auch für CAAdES und PAdES zu füllen.

- 8646 3. Angenommener Signaturzeitpunkt gemäß TIP1-A_5540 (QES) und TIP1-A_5545
8647 (nonQES)
- 8648 /VerificationReport/
8649 IndividualReport/
8650 Details/
8651 dss:VerificationTimeInfo/
8652 dss:VerificationTime
8653
- 8654 4. der binäre Wert der Signatur
- 8655 /VerificationReport/
8656 IndividualReport/
8657 SignedObjectIdentifier/
8658 SignatureValue
- 8659 5. Kurztext
- 8660 Der signierte Kurztext wird in folgendem XML-Element zurückgegeben:
- 8661 /VerificationReport/
8662 IndividualReport/
8663 SignedObjectIdentifier/
8664 SignedProperties/
8665 Other/
8666 SIG:ShortText
8667
- 8668 6. Das folgende Element mit den Werten true/false gibt an, ob eine
8669 Zertifikatsreferenz gemäß Anhang B2 vorhanden ist (true) oder nicht (false):
- 8670 /VerificationReport/
8671 IndividualReport/
8672 SignedObjectIdentifier/
8673 SignedProperties/
8674 Other/
8675 SIG:ReferenceToSignerCertificate
- 8676 7. Sämtliche signierte Attribute, deren Rückgabe nicht explizit über andere Elemente
8677 geregelt ist, werden als direkt anzeigbare Key/Value-Paare zurückgeben. Dabei
8678 sind sowohl Key und Value bereits für die Anzeige formatiert. Der Key wird in
8679 einer Zeile dargestellt. Der Value wird in mehreren Zeilen dargestellt, wobei ein
8680 Zeilenumbruch durch 'CARRIAGE RETURN (CR)' 'LINE FEED (LF)' erzeugt wird und
8681 keine weiteren Steuerzeichen erlaubt sind.
- 8682 /VerificationReport/
8683 IndividualReport/
8684 SignedObjectIdentifier/
8685 SignedProperties/

8686 Other/
 8687 SIG:DisplayableAttributes

8688 8. das Ergebnis der Signaturprüfung
 8689 /VerificationReport/
 8690 IndividualReport/
 8691 Result

8692 9. handelt es sich bei der Signatur um eine Gegensignatur wird diese als solche
 8693 markiert
 8694
 8695 /DetailedSignatureReport/
 8696 Properties/
 8697 UnsignedProperties/
 8698 Other/
 8699 SIG:CounterSignatureMarker

8700 und mit
 8701
 8702 /DetailedSignatureReport/
 8703 Properties/
 8704 UnsignedProperties/
 8705 Other/
 8706 SIG:CounterSignatureMarker/
 8707 SignatureValueReference/
 8708 @IdRef
 8709
 8710

8711 auf jede (eine oder mehrere) gegensignierte Signaturen verwiesen. Dabei
 8712 zeigt IdRef auf den jeweiligen gegensignierten Signaturwert
 8713
 8714 /VerificationReport/
 8715 IndividualReport/
 8716 SignedObjectIdentifier/
 8717 ds:SignatureValue/
 8718 @Id

8719 10. das Ergebnis der Zertifikatsprüfung,
 8720 /VerificationReport/
 8721 IndividualReport/
 8722 Details/
 8723 DetailedSignatureReport/
 8724 CertificatePathValidity/
 8725 PathValiditySummary/

8726 ResultMajor

8727 11. Inhalt des Zertifikates, auf dem beruhend signiert wurde

8728 /VerificationReport/

8729 IndividualReport/

8730 Details/

8731 DetailedSignatureReport/

8732 CertificatePathValidity/

8733 PathValidityDetail/

8734 CertificateValidity/

8735 CertificateValue

8736 12. den Signaturalgorithmus der Dokumentensignatur (URI, angelehnt an den

8737 Wertebereich des Feldes ds:SignatureMethod),

8738 /VerificationReport/

8739 IndividualReport/

8740 Details/

8741 DetailedSignatureReport/

8742 SignatureOK/

8743 SignatureAlgorithm

8744

8745 13. aussagekräftiger Hinweis zum verminderten Beweiswert hinsichtlich Authentizität

8746 und Integrität der Signatur, wenn einer der bei der Signaturprüfung identifizierten

8747 und unterstützten Algorithmen zum Zeitpunkt der Signaturprüfung nicht mehr laut

8748 Algorithmenkatalog [ALGCAT] als geeignet eingestuft wird. Auszuwerten sind die

8749 Festlegungen des ALGCAT sowohl bezogen auf die Vergangenheit als auch auf die

8750 Zukunft.

8751 Für alle geprüften Zertifikate:

8752 ../

8753 vr:CertificateValidity/

8754 vr:SignatureOK/

8755 vr:SignatureAlgorithm/

8756 vr:Suitability/

8757 ./ResultMajor= urn:oasis:names:tc:dss:1.0:detail:invalid

8758 ./ResultMessage="Algorithmen seit <Jahr> als unsicher eingestuft"

8759 14. PathValidity bis zur TrustAnchor-TSL

8760 //CertificateValidity/ChainingOK/ResultMajor (ab dem zweiten Zertifikat in der

8761 Kette)

8762 //CertificateValidity/CertificateStatus/CertStatusOK/ResultMajor

8763 //CertificateValidity/CertificateValue

8764 Für das Feld TrustAnchor ist

8765 "urn:oasis:names:tc:dss-
8766 x:1.0:profiles:verificationreport:trustanchor:certDataBase"
8767 zu verwenden.

8768 15. Prüfergebnis des Gültigkeitszeitraums
8769 /VerificationReport/
8770 IndividualReport/
8771 Details/
8772 DetailedSignatureReport/
8773 CertificatePathValidity/
8774 PathValidityDetail/
8775 CertificateValidity/
8776 ValidityPeriodOK/
8777 ResultMajor

8778 16. Prüfung der Extensions
8779 /VerificationReport/
8780 IndividualReport/
8781 Details/
8782 DetailedSignatureReport/
8783 CertificatePathValidity/
8784 PathValidityDetail/
8785 CertificateValidity/
8786 ExtensionsOK/
8787 ResultMajor

8788 17. Zeitstempel und Herkunft der OCSP-Antwort für das Signaturzertifikat
8789 /VerificationReport/
8790 IndividualReport/
8791 Details/
8792 DetailedSignatureReport/
8793 CertificatePathValidity/
8794 PathValidityDetail/
8795 CertificateValidity/
8796 CertificateStatus/
8797 RevocationEvidence/
8798 OCSPValidity/
8799 OCSPIdentifier/
8800 ./XAdES:ResponderID/XAdES:ByName
8801 ./XAdES:ProducedAt

18. OCSP Antwort für das Signaturzertifikats

/VerificationReport/

IndividualReport/

Details/

/vr:DetailedSignatureReport/

vr:CertificatePathValidity/

vr:PathValidityDetail/

vr:CertificateValidity/

vr:CertificateStatus/

vr:RevocationEvidence/

vr:OCSPValidity/

vr:OCSPValue

Sonderfälle:

Dokument mit parallelen Signaturen

Für jede Signatur wird ein IndividualReport erzeugt.

Dokument mit Signatur und Gegensignatur

Für jede Signatur wird ein IndividualReport erzeugt.

6.4 Profilierung der Dokumentenformate und Nachrichten

Tabelle 386 TAB_KON_775 „Profilierung der Dokumentformate und Nachrichten“

XML-Dokument	<p>Es gelten folgende Mindestanforderungen, die der Konnektor bezüglich Dokumentenstruktur und Dokumenteninhalt unterstützen muss:</p> <ul style="list-style-type: none"> - Hierarchietiefe des Dokumentenbaums: 30 Ebenen - Anzahl von XML-Elementen im Dokument: 30.000 - Anzahl von XML-Attributen je XML-Element: 20 - Anzahl von direkten Kindern eines XML-Elements: 50 - Länge von XML-Bezeichnern (z. B. Elementnamen, Attributnamen, Namespace-Prefixes, usw.): 200 - Anzahl von Transformationen: 64 - Element-Größe pro Einzelknoten im Base64-codierten Dokument: 30 MB
	<p>Es dürfen keine ENTITY-Deklarationen im XML-Dokument vorkommen.</p>

	Zu verifizierende XML-Dokumente dürfen im <Transforms>-Teil ihrer Referenzen weder XPath-Ausdrücke noch XSL-Transformationen enthalten.
	Bei Referenzen (ReferenceType) darf das Optionale URI-Attribut nicht vorhanden sein, oder es muss leer sein.
	XInclude darf nicht unterstützt werden.
	Die Attribute schemaLocation und noNamespaceSchemaLocation dürfen nicht unterstützt werden.

8822

8823

ENTWURF

8824 7 Anhang D – Übersicht über die verwendeten Versionen

8825 Für den Fall, dass Schnittstellenversionen unterstützt werden müssen, die den gleichen
 8826 TargetNamespace nutzen, kann der Konnektor zu diesen Schnittstellenversionen
 8827 einheitlich einen SOAP-Endpunkt anbieten, der die höchste der Schnittstellenversionen
 8828 implementiert.

8829 **Tabelle 387: TAB_KON_688 Version der Schemas aus dem Namensraum des Konnektors**

Schemas aus dem Namensraum des Konnektors „http://ws.gematik.de/conn“		
XSD Name	CardEvents.xsd	
XSD Schemaversion	6.0.0	
TargetNamespace	http://ws.gematik.de/conn/CardEvents/v6.0	
XSD Name	CardService.xsd	
XSD Schemaversion	8.1.3	
TargetNamespace	http://ws.gematik.de/conn/CardService/v8.1	
XSD Name	CardServiceCommon.xsd	
XSD Schemaversion	2.0.0	
TargetNamespace	http://ws.gematik.de/conn/CardServiceCommon/v2.0	
XSD Name	CardTerminalInfo.xsd	
XSD Schemaversion	8.1.0	
TargetNamespace	http://ws.gematik.de/conn/CardTerminalInfo/v8.1	

	XSD Name	CardTerminalService.xsd
	XSD Schemaversion	1.1.2
	TargetNamespace	http://ws.gematik.de/conn/CardTerminalService/v1.1
	XSD Name	CertificateService_v6_0_2.xsd
	XSD Schemaversion	6.0.2
	<u>TargetNamespace</u>	<u>http://ws.gematik.de/conn/CertificateService/v6.0</u>
	<u>XSD Name</u>	<u>CertificateService.xsd</u>
	<u>XSD Schemaversion</u>	<u>6.0.1</u>
	TargetNamespace	http://ws.gematik.de/conn/CertificateService/v6.0
	XSD Name	CertificateServiceCommon.xsd
	XSD Schemaversion	2.0.1
	TargetNamespace	http://ws.gematik.de/conn/CertificateServiceCommon/2.0
	XSD Name	ConnectorCommon.xsd
	XSD Schemaversion	5.0.0
	TargetNamespace	http://ws.gematik.de/conn/ConnectorCommon/v5.0
	XSD Name	ConnectorContext.xsd

	XSD Schemaversion	2.0.0
	TargetNamespace	http://ws.gematik.de/conn/ConnectorContext/v2.0
	XSD Name	EncryptionService_v6_1_2.xsd
	XSD Schemaversion	6.1.2
	TargetNamespace	http://ws.gematik.de/conn/EncryptionService/v6.1
	XSD Name	EncryptionService.xsd
	XSD Schemaversion	6.1.21
	TargetNamespace	http://ws.gematik.de/conn/EncryptionService/v6.1
	XSD Name	EventService.xsd
	XSD Schemaversion	7.2.1
	TargetNamespace	http://ws.gematik.de/conn/EventService/v7.2
	XSD Name	ServiceDirectory.xsd
	XSD Schemaversion	3.1.0
	TargetNamespace	http://ws.gematik.de/conn/ServiceDirectory/v3.1
	XSD Name	SignatureService_V7_5_0.xsd
	XSD Schemaversion	7.5.0
	TargetNamespace	http://ws.gematik.de/conn/SignatureService/v7.5

	XSD Name	SignatureService_V7_4_3.xsd
	XSD Schemaversion	7.4.3
	TargetNamespace	http://ws.gematik.de/conn/SignatureService/v7.4
	XSD Name	SignatureService.xsd
	XSD Schemaversion	7.4.2
	TargetNamespace	http://ws.gematik.de/conn/SignatureService/v7.4
	Der Signaturdienst des Konnektors MUSS sich an der Außenschnittstelle konform zu den gehärteten Schemas XSD_HARDENED verhalten. Die konkreten Schemas zu dem Bezeichner XSD_HARDENED legt die Dokumentenlandkarte fest.	

8830
8831

8832 **Tabelle 388: TAB_KON_798 Schnittstellenversionen**

**Pro Dienst mit Operationen an der Außenschnittstelle:
WSDLs des Konnektors und verwendete XSDs aus dem Namensraum der
gematik <http://ws.gematik.de>**

Kartendienst (CardService)

	WSDL Name	CardService.wsdl
	WSDL-Version	8.1.2
	TargetNamespace	http://ws.gematik.de/conn/CardService/WSDL/v8.1
	verwendete XSDs	CardService.xsd, CardServiceCommon.xsd, ConnectorCommon.xsd, ConnectorContext.xsd, ProductInformation.xsd, TelematikError.xsd

Kartendienst (CardService)

WSDL Name	CardService.wsdl
WSDL-Version	8.1.1
TargetNamespace	http://ws.gematik.de/conn/CardService/WSDL/v8.1
verwendete XSDs	CardService.xsd, CardServiceCommon.xsd, ConnectorCommon.xsd, ConnectorContext.xsd, ProductInformation.xsd, TelematikError.xsd

Kartendienst (CardService)

WSDL Name	CardService.wsdl
WSDL-Version	8.1.0
TargetNamespace	http://ws.gematik.de/conn/CardService/WSDL/v8.1
verwendete XSDs	CardService.xsd, CardServiceCommon.xsd, ConnectorCommon.xsd, ConnectorContext.xsd, ProductInformation.xsd, TelematikError.xsd

Kartenterminaldienst (CardTerminalService)

WSDL Name	CardTerminalService.wsdl
WSDL-Version	1.1.0
TargetNamespace	http://ws.gematik.de/conn/CardTerminalService/ WSDL/v1.1

	verwendete XSDs	CardTerminalService.xsd, CardService.xsd, CardTerminalService.xsd, CardServiceCommon.xsd, ConnectorCommon.xsd, ConnectorContext.xsd, TelematikError.xsd
Systeminformationsdienst (EventService)		
	WSDL Name	EventService.wsdl
	WSDL-Version	7.2.0
	TargetNamespace	http://ws.gematik.de/conn/EventService/ WSDL/v7.2
	verwendete XSDs	CardService.xsd, CardServiceCommon.xsd, CardTerminalInfo.xsd, ConnectorCommon.xsd, ConnectorContext.xsd, EventService.xsd, ProductInformation.xsd, TelematikError.xsd
Zertifikatsdienst (CertificateService)		
	WSDL Name	CertificateService.wsdl
	WSDL-Version	6.0.1
	TargetNamespace	http://ws.gematik.de/conn/CertificateService/ WSDL/v6.0
	verwendete XSDs	CertificateService.xsd, CertificateServiceCommon.xsd, ConnectorCommon.xsd, ConnectorContext.xsd

Zertifikatsdienst (CertificateService)

WSDL Name	CertificateService.wsdl
WSDL-Version	6.0.0
TargetNamespace	http://ws.gematik.de/conn/CertificateService/ WSDL/v6.0
verwendete XSDs	CertificateService.xsd, CertificateServiceCommon.xsd, ConnectorCommon.xsd, ConnectorContext.xsd

Verschlüsselungsdienst (EncryptionService)

WSDL Name	EncryptionService.wsdl
WSDL-Version	6.1.1
TargetNamespace	http://ws.gematik.de/conn/EncryptionService/ WSDL/v6.1
verwendete XSDs	ConnectorCommon.xsd, ConnectorContext.xsd, EncryptionService.xsd

Verschlüsselungsdienst (EncryptionService)

WSDL Name	EncryptionService.wsdl
WSDL-Version	6.1.0
TargetNamespace	http://ws.gematik.de/conn/EncryptionService/ WSDL/v6.1
verwendete XSDs	ConnectorCommon.xsd, ConnectorContext.xsd, EncryptionService.xsd

Signaturdienst (SignatureService)		
	WSDL Name	SignatureService_V7_5_0.wsdl
	WSDL-Version	7.5.0
	TargetNamespace	http://ws.gematik.de/conn/SignatureService/WSDL/v7.5
	verwendete XSDs	../tel/error/TelematikError.xsd, ConnectorContext.xsd, SignatureService_V7_5_0.xsd
Signaturdienst (SignatureService)		
	WSDL Name	SignatureService_V7_4_1.wsdl
	WSDL-Version	7.4.1
	TargetNamespace	http://ws.gematik.de/conn/SignatureService/WSDL/v7.4
	verwendete XSDs	../tel/error/TelematikError.xsd, ConnectorContext.xsd, SignatureService_V7_4_3.xsd
Signaturdienst (SignatureService)		
	WSDL Name	SignatureService.wsdl
	WSDL-Version	7.4.0
	TargetNamespace	http://ws.gematik.de/conn/SignatureService/WSDL/v7.4
	verwendete XSDs	../tel/error/TelematikError.xsd, ConnectorContext.xsd, SignatureService.xsd
Authentifizierungsdienst (AuthSignatureService)		

	WSDL Name	AuthSignatureService.wsdl
	WSDL-Version	7.4.1
	TargetNamespace	http://ws.gematik.de/conn/AuthSignatureService/WSDL/v7.4
	verwendete XSDs	../tel/error/TelematikError.xsd, ConnectorContext.xsd, SignatureService.xsd
Authentifizierungsdienst (AuthSignatureService)		
	WSDL Name	AuthSignatureService.wsdl
	WSDL-Version	7.4.0
	TargetNamespace	http://ws.gematik.de/conn/AuthSignatureService/WSDL/v7.4
	verwendete XSDs	../tel/error/TelematikError.xsd, ConnectorContext.xsd, SignatureService.xsd

8833
8834

8835

8 Anhang F – Übersicht Events

8836

Tabelle 389 – TAB_KON_777 Events Interne Mechanismen

Topic Ebene1 /Topic Ebene2 /Topic Ebene3	Typ	Schwere	P r o t	A n C l i e n t s	Parameter	Bedeutung	Auslöser (TUC/Op)
Interne Mechanismen							
BOOTUP /BOOTUP_COMPLETE	Op	Info	x	x		Änderung des Betriebszustand des	
OPERATIONAL_STATE /EC_CardTerminal_Software_Out_Of_Date (\$ctId)	Op	Info	x	x	Value=true/false; CtID=\$ctId; Bedeutung=\$EC.description	Änderung des Betriebszustand des durch Änderung im Fehlerzustand (Änderung im Value).	
OPERATIONAL_STATE EC_CardTerminal_SMC-KT_Certificate_Expires_Soon (\$ctId)	Op	Info	x	x	Value=true/false; CtID=\$ctId; Bedeutung=\$EC.description	Änderung des Betriebszustand des durch Änderung im Fehlerzustand (Änderung im Value).	TUC_KON_050
OPERATIONAL_STATE /EC_Connector_Software_Out_Of_Date	Op	Info	x	x	Value=true/false; Bedeutung=\$EC.description	"	
OPERATIONAL_STATE /EC_FW_Not_Valid_Status_Blocked	Sec	Fatal	x	x	Value=true/false; Bedeutung=\$EC.description	"	

OPERATIONAL_STATE /EC_Time_Sync_Not_Successful	Op	Info	x	x	Value=true/ false; LastSyncAttempt = \$lastSyncAttempt Timestamp; LastSyncSuccess = \$lastSyncSuccess Timestamp; Bedeutung= \$EC.description	"	
OPERATIONAL_STATE /EC_TSL_Update_Not_Successful	Op	Info	x	x	Value=true/ false; Bedeutung= \$EC.description ; LastUpdateTSL= \$lastUpdate TSLTimestamp	"	
OPERATIONAL_STATE /EC_TSL_Expiring	Sec	Info	x	x	Value=true/ false; NextUpdateTSL= \$NextUpdate- Element der TSL; Bedeutung= \$EC.description	"	
OPERATIONAL_STATE /EC_TSL_Trust_Anchor_Expiring	Sec	Info	x	x	Value=true/ false; ExpiringDate TrustAnchor= Ablaufdatum der Vertrauens ankergültigkeit ; Bedeutung= \$EC.description	"	
OPERATIONAL_STATE /EC_LOG_OVERFLOW	Op	Warni ng	x	x	Value=true/ false; Protokoll=\$Prot okoll; Bedeutung= \$EC.description	"	TUC_KON_2 71

OPERATIONAL_STATE /EC_CRL_Expiring	Sec	Warni ng	x	x	Value=true/ false; NextUpdateTSL= \$NextUpdate- Element der TSL; Bedeutung= \$EC.description	"	
OPERATIONAL_STATE /EC_Time_Sync_Pending_Warnin g	Sec	Warni ng	x	x	Value=true/ false; LastSyncSuccess = \$lastSyncSucces s Timestamp; Bedeutung= \$EC.description	"	
OPERATIONAL_STATE /EC_TSL_Out_Of_Date_Within_G race_Period	Sec	Warni ng	x	x	Value=true/ false; NextUpdateTSL= \$NextUpdate- Element der TSL; GracePeriodTSL= CERT_TSL_ DEFAULT_GRACE_ PERIOD_DAYS; Bedeutung= \$EC.description	"	
OPERATIONAL_STATE /EC_CardTerminal_Not_Availab le(\$ctId)	Op	Error	x	x	Value=true/ false; CtID=\$ctId; Bedeutung =\$EC.descriptio n	"	
OPERATIONAL_STATE /EC_No_VPN_TI_Connection	Op	Error	x	x	Value=true/ false; Bedeutung= \$EC.description	"	
OPERATIONAL_STATE /EC_No_VPN_SIS_Connection	Op	Error	x	x	Value=true/ false; Bedeutung= \$EC.description	"	

OPERATIONAL_STATE /EC_No_Online_Connection	Op	Error	x	x	Value=true/ false; Bedeutung= \$EC.description	"	
OPERATIONAL_STATE /EC_IP_Addresses_Not_Availabl e	Sec	Error	x	x	Value=true/ false; Bedeutung= \$EC.description	"	
OPERATIONAL_STATE /EC_CRL_Out_Of_Date	Sec	Fatal	x	x	Value=true/ false; NextUpdateCRL= \$NextUpdate der CRL; Bedeutung= \$EC.description	"	
OPERATIONAL_STATE /EC_Firewall_Not_Reliable	Sec	Fatal	x	x	Value=true/ false; Bedeutung= \$EC.description	"	
OPERATIONAL_STATE /EC_Random_Generator_Not_Rel iable	Sec	Fatal	x	x	Value=true/ false; Bedeutung= \$EC.description	"	
OPERATIONAL_STATE /EC_SecureKeyStore_Not_Avail able	Sec	Fatal	x	x	Value=true/ false; Bedeutung= \$EC.description	"	
OPERATIONAL_STATE /EC_Security_Log_Not_Writabl e	Op	Fatal	x	x	Value=true/ false; Bedeutung= \$EC.description	"	
OPERATIONAL_STATE /EC_Software_Integrity_Check _Failed	Sec	Fatal	x	x	Value=true/ false; Bedeutung= \$EC.description	"	

OPERATIONAL_STATE /EC_Time_Difference_Intolerable	Sec	Fatal	x	x	Value=true/ false; Bedeutung= \$EC.description ; NtpTimedifference= Zeitabweichung; NtpMaxAllowedTime difference= NTP_MAX_TIMEDIFFERENCE; Bedeutung= \$EC.description	"	
OPERATIONAL_STATE /EC_Time_Sync_Pending_Critical	Sec	Fatal	x	x	Value=true/ false; LastSyncSuccess= \$lastSyncSuccess Timestamp; NtpGracePeriod= NTP_GRACE_PERIOD; Bedeutung= \$EC.description	"	
OPERATIONAL_STATE /EC_TSL_Trust_Anchor_Out_Of_Date	Sec	Fatal	x	x	Value=true/ false; ExpiringDate TrustAnchor= Ablaufdatum der Vertrauensanker gültigkeit; Bedeutung= \$EC.description	"	
OPERATIONAL_STATE /EC_TSL_Out_Of_Date_Beyond_Grace_Period	Sec	Fatal	x	x	Value=true/ false; Next UpdateTSL= \$NextUpdate- Element der TSL; GracePeriodTSL= CERT_TSL_ DEFAULT_ GRACE_PERIOD_DAYS; Bedeutung= \$EC.description	"	

OPERATIONAL_STATE /EC_CRYPTOPERATION_ALARM	Sec	Warni ng	x	x	Value=true/ false; Operation= \$Operationsname ; Count=\$Summenwe rt; Arbeitsplatz =\$<Liste operations- aufrufenden workplace IDs>; Meldung=' Auffällige Häufung von Operationsaufru fen in den letzten 10 Minuten'	"	
OPERATIONAL_STATE /EC_OTHER_ERROR_STATE (\$no)	\$Type	\$Seve rity	x	x	Value=true/ false; Bedeutung= \$EC.description	"	
OPERATIONAL_STATE /EC_BNetzA_VL_Update_Not_Suc cessful	Op	Info	x	x	Value=true/ false; LastUpdate BNetzAVL= \$lastUpdateBNet zAVL Timestamp; Bedeutung= \$EC.description ;	"	
OPERATIONAL_STATE /EC_BNetzA_VL_not_valid	Sec	Warni ng	x	x	Value=true/ false; NextUpdate BNetzAVL= \$NextUpdate- Element der BNetzA-VL; Bedeutung= \$EC.description ;	"	
Zugriffsberechtigungsdienst							
Dokumentvalidierungsdienst							

Dienstverzeichnisdienst							
Kartenterminaldienst							
CT /ERROR	\$Error Type	\$Severity	x	x	CtID=\$CT.ID; Name=\$CT.HOSTNAME; Error=\$Fehlercode; Bedeutung=\$Fehlertext	Bei der Kommunikation mit dem KT ist ein Fehler aufgetreten	TUC_KON_051 TUC_KON_053
CT /CONNECTED	Op	Info	x	x	CtID=\$CT.CTID; Hostname=\$CT.HOSTNAME	Die Verbindung zu einem Kartenterminal wurde hergestellt	
CT /DISCONNECTED	Op	Info	x	x	CtID=\$CT.CTID; Hostname=\$CT.HOSTNAME	Die Verbindung zu einem Kartenterminal wurde unterbrochen	
CT /TLS_ESTABLISHMENT_FAILURE	\$Error Type	\$Severity	x	x	CtID = \$CT.ID; Name=\$CT.HOSTNAME; Error=\$Fehlercode; Bedeutung=\$Fehlertext	Im Rahmen des Verbindungsaufbaus sind Fehler aufgetreten	TUC_KON_050
CT /CT_ADDING_ERROR	\$Error Type	\$Severity	x	x	IP=\$IP-Adresse; Name=\$Hostname; Error=\$Fehlercode; Bedeutung=\$Fehlertext	Bei dem Versuch ein KT der Verwaltung zuzufügen ist ein Fehler aufgetreten	TUC_KON_054
CT /SLOT_FREE	Op	Info	-	-	CtID=\$CT.CTID; SlotNo=\$CT.SLOTS_USED[X]	Internes Event von Kartenterminaldienst --> Kartendienst. Informiert, dass ein Slot frei wurde. Wird im Kartendienst ausgewertet und verursacht dort CARD/REMOVED	

CT /SLOT_IN_USE	Op	Info	-	-	CtID=\$CT.CTID; SlotNo=<FU- Nummer aus Ereignisnachric ht>	Internes Event von Kartenterminal dienst --> Kartendienst. Informiert, dass ein Slot belegt wurde. Wird im Kartendienst ausgewertet und verursacht dort CARD/INSERTED	
Kartendienst							
CARD /INSERTED	Op	Info	x	x	CardHandle= \$CARD.CARDHANDL E; CardType=\$CARD. TYP; CardVersion= \$CARD.VER; ICCSN=\$CARD.ICC SN; CtID=\$CARD.CTID ; SlotID= \$CARD.SLOTID; InsertTime= \$CARD.INSERTTIM E; CardHolderName= \$CARD.CARD HOLDERNAME; KVNR=\$CARD.KVNR	Eine Karte wurde gesteckt	TUC_KON_0 01 (als Reaktion auf CTM /SLOT_IN_ USE)
CARD /REMOVED	Op	Info	x	x	CardHandle= \$CARD.CARDHANDL E; CardType=\$CARD. TYP; CardVersion= \$CARD.VER; ICCSN=\$CARD.ICC SN; CtID=\$CARD.CTID ; SlotID= \$CARD.SLOTID; InsertTime= \$CARD.INSERTTIM E; CardHolderName= \$CARD.CARDHOLDE R NAME; KVNR=\$CARD.KVNR	Eine Karte wurde gezogen	Reaktion auf CTM/SLOT_ FREE

CARD /PIN /VERIFY_STARTED	Op	Info	-	x			
CARD /PIN /VERIFY_FINISHED	Op	Info	-	x			
CARD /PIN /CHANGE_STARTED	Op	Info	-	x			
CARD /PIN /CHANGE_FINISHED	Op	Info	-	x			
CARD /PIN /ENABLE_STARTED	Op	Info	-	x	CardHandle=\$; CardType=\$; ICCSN=\$; CtID=\$; SlotID=\$; PinRef=\$PinRef; PinInputCtID =\$PinInputKT	PIN-Schutz anschalten beginnt	TUC_KON_0 27
CARD /PIN /ENABLE_FINISHED	Op	Info	-	x	CardHandle=\$; CardType=\$; ICCSN=\$; CtID=\$; SlotID=\$; PinRef=\$PinRef; PinInputCtID =\$PinInputKT	PIN-Schutz anschalten wurde beendet	TUC_KON_0 27
CARD /PIN /DISABLE_STARTED	Op	Info	-	x	CardHandle=\$; CardType=\$; ICCSN=\$; CtID=\$; SlotID=\$; PinRef=\$PinRef; PinInputCtID =\$PinInputKT	PIN-Schutz ausschalten beginnt	TUC_KON_0 27

CARD /PIN /DISABLE_FINISHED	Op	Info	-	x	CardHandle=\$; CardType=\$; ICCSN=\$; CtID=\$; SlotID=\$; PinRef=\$PinRef; PinInputCtID =\$PinInputKT	PIN-Schutz ausschalten wurde beendet	TUC_KON_0 27
Systeminformationsdienst							
Verschlüsselungsdienst							
Signaturdienst							
SIG /SIGNDOC /NEXT_SUCCESSFUL	Op	Info	-	X	\$Jobnummer	Die nächste Signatur aus einem Signaturstapel wurde erfolgreich erstellt.	TUC_KON_1 66 „nonQES Signaturen erstellen“ TUC_KON_1 54 „QES Signaturen erstellen“
Zertifikatsdienst							
CERT /TSL /IMPORT	Op	Error	x	-	\$Fehlerbeschrei bung	Manueller Import der TSL fehlgeschlagen	TUC_KON_0 32 "TSL aktualisiere n"
CERT /TSL /UPDATED	Op	Info	x	-		Eine neue TSL wurde erfolgreich in den TrustStore eingespielt	TUC_KON_0 32 "TSL aktualisiere n"
CERT /CRL /INVALID	Op	Error	x	-		Prüfung der Signatur der CRL fehlgeschlagen	TUC_KON_0 40 "CRL aktualisiere n"

CERT /CRL /IMPORT	Op	Error	x	-	\$Fehlerbeschreibung	Manueller Import der CRL fehlgeschlagen	TUC_KON_040 "CRL aktualisieren"
CERT /CRL /UPDATED	Op	Info	x	-		Die CRL wurde erfolgreich aktualisiert	TUC_KON_040 "CRL aktualisieren"
CERT /CARD /EXPIRATION	Op	Warning	x	x	CARD_TYPE=gSMC-K; ICCSN=\$ICCSN; Konnektor=\$MGM_KONN_HOSTNAME; ZertName=<Name des Zertifikatsobjekts>; ExpirationDate=\$validity	gSMC-K abgelaufen	TUC_KON_033 "Zertifikatsablauf prüfen"
CERT /CARD /EXPIRATION	Op	Warning	-	x	CARD_TYPE=\$Type; ICCSN=\$ICCSN; CARD_HANDLE=\$CardHandle; CardHolderName=\$CardHolderName; ZertName=<Name des Zertifikatsobjekts>; ExpirationDate=\$validity	Sonstige Karte abgelaufen	TUC_KON_033 "Zertifikatsablauf prüfen"
CERT /CARD /EXPIRATION	Op	Info	-	x	CARD_TYPE=gSMC-K; ICCSN=\$ICCSN; Konnektor=\$MGM_KONN_HOSTNAME; ZertName=<Name des Zertifikatsobjekts>; ExpirationDate=\$validity; DAYS_LEFT=\$validity-\$Today	gSMC-K läuft innerhalb von DAYS_LEFT Tagen ab	TUC_KON_033 "Zertifikatsablauf prüfen"

CERT /CARD /EXPIRATION	Op	Info	-	x	CARD_TYPE=\$Type; ICCSN=\$ICCSN; CARD_HANDLE=\$CardHandle; CardHolderName=\$CardHolderName; ZertName=<Name des Zertifikatsobje kts>; ExpirationDate=\$validity; DAYS_LEFT=\$validity-\$Today	Sonstige Karte läuft innerhalb von DAYS_LEFT Tagen ab	TUC_KON_0 33 "Zertifikatsa blauf prüfen"
CERT /BNETZA_VL /UPDATED	Op	Info	x	-		Eine neue BNetzA-VL wurde erfolgreich in den TrustStore eingespielt	TUC_KON_0 31 " BNetzA-VL aktualisiere n"
CERT /BNETZA_VL /IMPORT	Op	Error	x	-	\$Fehlerbeschrei bung	Manueller Import der BNetzA-VL fehlgeschlagen	TUC_KON_0 31 " BNetzA-VL aktualisiere n"
Protokollierungsdienst							
LOG /ERROR	\$Err or Type	\$Seve rity	-	-	Error=\$Fehlerco de	Im Protokollierung sdienst auftretende Fehler werden verteilt	TUC_KON_2 71
LOG /CRYPTO_OP	Sec	Info	x	-	Operation=\$Operationsname ; <für alle betroffenen Schlüssel:> Karte=\$ICCSN; Keyref=<Referen z auf den Schlüssel>; CARD_HANDLE=\$CardHandle; CardHolderName=\$CardHolderName		
TLS-Dienst							

Anbindung LAN/WAN							
ANLW /LAN /IP_CHANGED	Op	Warni ng	x	-	IP=\$dieNeueIP	Wenn der LAN-Adapter eine neue IP oder Netzwerk bekommen hat	DHCP, Management schnittstelle
ANLW /WAN /IP_CHANGED	Op	Info	x	-	IP=\$dieNeueIP	Wenn der WAN-Adapter eine neue IP oder Netzwerk bekommen hat	DHCP, Management schnittstelle
DHCP-Server							
DHCP /SERVER /STATECHANGED	Op	Info	x	x	STATE=\$DHCP_SERVER_STATE		Administrator
DHCP Client							
DHCP /LAN_CLIENT /RENEW	Op	Info	x	x	IP_ADDRESS=<Belegung>		TUC_KON_341
DHCP /WAN_CLIENT /RENEW	Op	Info	x	x	IP_ADDRESS=<Belegung>		TUC_KON_341
DHCP /LAN_CLIENT /STATECHANGED	Op	Info	x	x	STATE=\$DHCP_CLIENT_LAN_STATE		
DHCP /WAN_CLIENT /STATECHANGED	Op	Info	x	x	STATE=\$DHCP_CLIENT_WAN_STATE		
VPN-Client							
NETWORK /VPN_TI /UP	Op	Info	x	x		Wenn der VPN-Tunnel zur TI erfolgreich aufgebaut worden ist.	

NETWORK /VPN_TI /DOWN	Op	Info	x	x		Wenn der VPN-Tunnel zur TI nicht mehr zur Verfügung steht.	AFO
NETWORK /VPN /CONFIG_CHANGED	Op	Info	x	-		Wenn die Konfiguration des VPN-Clients angepasst wurde.	Management schnittstelle
NETWORK /VPN_SIS /UP	Op	Info	x	x		Wenn der VPN-Tunnel zum SIS erfolgreich aufgebaut worden ist.	
NETWORK /VPN_SIS /DOWN	Op	Info	x	x		Wenn der VPN-Tunnel zum SIS nicht mehr zur Verfügung steht.	AFO
Zeitdienst							
NTP /ENTERCRITICALSTATE	Op	FATAL	x	-	MESSAGE= „CRITICALTIME DEVIATION“	Zeitabweichung von mehr als einer Stunde entdeckt	
Namensdienst und Dienstlokalisierung							
Leistungsumfänge und Standalone-Szenarios							
MGM /ADMINCHANGES	Op	Info	x	-	User= \$AdminUsername; RefID=\$Referenz ID; NewVal= \$NeuEingestellt er Wert“	Änderungen die der Admin vornimmt werden protokolliert	
MGM /CONFIG_EXIMPORT	Op	Info	x	-	User= \$AdminUsername; Mode= [Export/Import]	Dokumentiert (via Mode), dass die Konnektor konfiguration exportiert oder importiert wurde.	

MGM /FACTORYSETTINGS	Op	Info	x	-	User= \$AdminUsername	Ein ausgelöster Werksreset wird protokolliert	
MGM /REMOTE_SESSION	Op	Info	x	-	InitUser= \$AdminUsername; RemoteID=<Kennu ng der Gegenstelle>; Mode= [InitSuccess/ InitFail/Exit]	Protokollierung des Versuchs, des Beginns und des Endes einer Remote- Management Session	
MGM /LU_CHANGED /LU_ONLINE	Op	Info	x	x	Active= \$MGM_LU_ONLINE	Leistungsumfan g Online wurde aktiviert/ deaktiviert	Administrat or
MGM /LU_CHANGED /LU_SAK	Op	Info	x	x	Active= \$MGM_LU_SAK	Leistungsumfan g Signatur anwendungs komponente wurde aktiviert/deakti viert	Administrat or
MGM /STANDALONE_CHANGED	Op	Info	x	x	Active= \$MGM_STANDALONE _KON	Festlegung des Konnektors als "Alleinstehend" wurde geändert	Administrat or
In- und Außerbetriebnahme							
MGM /TI_ACCESS_GRANTED	Op	Info	x	-	Active= \$MGM_TI_ACCESS_ GRANTED	Der Konnektor wurde erfolgreich freigeschaltet	Administrat or
Software- Aktualisierungsdienst (KSR-Client)							
KSR /ERROR	\$Err or Type	\$Seve rity	x	x	Target=Konnekto r; Name= <MGM_KONN_HOSTN AME>; Error=\$Fehlerco de; Bedeutung= \$Fehlertext	Während der Konnektor aktualisierung ist ein Fehler aufgetreten	TUC_KON_2 80

KSR /ERROR	\$Error Type	\$Severity	x	x	Target=KT; Name= <KT-Friendly Name>; CtID=\$CtID; Error=\$Fehlercode; Bedeutung= \$Fehlertext	Während einer Kartenterminal aktualisierung ist ein Fehler aufgetreten	TUC_KON_2 81
KSR /ERROR	\$Error Type	\$Severity	x	x	Error=\$Fehlercode; Bedeutung= \$Fehlertext	Im KSR-Client ist ein Fehler aufgetreten	TUC_KON_2 82
KSR /UPDATE /START	Sec	Info	x	x	<u>für TUC_KON_280</u> Target=Konnektor; Name= <MGM_KONN_HOSTNAME> <u>für TUC_KON_281</u> Target=KT; CtID=\$CtID	Ein Updateprozess im Konnektor wird gestartet, Ziel Konnektor oder Kartenterminal	TUC_KON_2 80 TUC_KON_2 81
KSR /UPDATE /SUCCESS	Sec	Info	x	x	<u>für TUC_KON_280</u> Target=Konnektor; Name= <MGM_KONN_HOSTNAME>; NewFirmwareversion= <UpdateInformation. FirmwareVersion >; ConfigurationChanged =<Ja/Nein>; ManualInputNeeded= <Ja/Nein> <u>für TUC_KON_281</u> Target=KT; Name= <KT-FriendlyName>; CtID=\$CtID; NewFirmwareversion= <UpdateInformation. FirmwareVersion >	Die Firmware des Konnektors/ eines Kartenterminals wurde erfolgreich aktualisiert	TUC_KON_2 80 TUC_KON_2 81

KSR /UPDATE /END	Sec	Info	x	x	für TUC KON 280 Target=Konnekto r; Name= <MGM_KONN_HOSTN AME> für TUC KON 281 Target=KT; CtID=\$CtID	Ein Updateprozess im Konnektor wurde beendet	TUC_KON_2 80 TUC_KON_2 81
KSR /UPDATE /KONNEKTOR_DOWNLOAD_END	Op	Info	x	x	Je heruntergeladene m FW-Paket: ProductVendorID = \$UpdateInformat ion/ ProductVendorID ; ProductCode= \$UpdateInformat ion/ ProductCode; ProductName= \$UpdateInformat ion/ ProductName; FirmwareVersion = \$UpdateInformat ion/ Firmware/FWVers ion; Deadline= \$UpdateInformat ion/ DeploymentInfor mation/ Deadline; FWPriority= \$UpdateInformat ion/ Firmware/FWPrio rity; FirmwareRelease Notes= \$UpdateInformat ion/ Firmware/ FirmwareRelease Notes	Download der Konnektor Firmware abgeschlossen	TIP1- A_6025

KSR /UPDATES_AVAILABLE	Op	Info	-	x	<p>Je gefundenem FW-Paket:</p> <p>ProductVendorID = \$UpdateInformation/ProductVendorID ;</p> <p>ProductCode= \$UpdateInformation/ProductCode;</p> <p>ProductName= \$UpdateInformation/ProductName;</p> <p>FirmwareVersion = \$UpdateInformation/FirmwareVersion ;</p> <p>Deadline= \$UpdateInformation/DeploymentInformation/Deadline;</p> <p>FWPriority= \$UpdateInformation/Firmware/FWPriority;</p> <p>FirmwareRelease Notes= \$UpdateInformation/Firmware/FirmwareRelease Notes</p>	Ein oder mehrere Updates auf neuere Versionen sind verfügbar	TIP1-A_4836
KSR /UPDATE_KONFIG	Op	Info	x	-	AlteVersion, NeueVersion	Aktualisierung Bestandsnetze	TUC_KON_283

8837

8838 Die Abbildungsvorschrift von Fehler- auf Event-Type lautet:

8839

- Security → Security,

8840

- Technical → Operation,

8841

- Infrastructure → Infrastructure,

8842

- Business → Business,

8843

- Other → Other

9 Anhang H – Mapping von „Architektur der TI-Plattform“ auf Konnektorspezifikation

Tabelle 390 – TAB_KON_711 Architektur der TI-Plattform, Berechtigtes Fachmodule

Interface	Operation	→ Funktionsmerkmal	Interface
I_Cert_Verification	verify_Certificate	→ Zertifikatsdienst	TUC_KON_037 "Zertifikat prüfen"
I_Crypt_Operations	decrypt_Document	→ Verschlüsselungsdienst	TUC_KON_071 "Daten hybrid entschlüsseln"
	encrypt_Document	→	TUC_KON_070 "Daten hybrid verschlüsseln"
I_DNS_Name_Information	get_FQDN	→ Namensdienst und Dienstlokalisierung	TUC_KON_364 „DNS Reverse Lookup durchführen“
	get_IP_Address	→	TUC_KON_361 „DNS Namen auflösen“
	get_Service_Information	→ Namensdienst und Dienstlokalisierung	TUC_KON_362 „Liste der Dienste abrufen“ TUC_KON_363 „Dienstdetails abrufen“
I_IP_Transport	send_Data_TI	→	
I_KT_Operations	interact_with_User	→ Kartenterminaldienst	TUC_KON_051 "Mit Anwender über Kartenterminal interagieren"
I_KV_Card_Handling	discard_Card_Usage_Reference	→ ---	--- keine Umsetzung notwendig. Erfolgt implizit

	get_Card_Usage_Reference	→	---	--- keine Umsetzung notwendig. Erfolgt implizit
I_KV_Card_Operations	decrypt_Data	→	Kartendienst	TUC_KON_219 "Entschlüssele"
	do_Reset	→		TUC_KON_024 "Karte zurücksetzen"
	erase_Card_Data	→		TUC_KON_211 „LöscheRecordInhalt“ TUC_KON_204 „LöscheDateiInhalt“
	extract_card_data	→	Zertifikatsdienst	TUC_KON_034 "Zertifikatsinformationen extrahieren"
	read_Card_Data	→	Kartendienst	TUC_KON_202 "LeseDatei"
		→		TUC_KON_209 "LeseRecord"
		→		TUC_KON_215 "SucheRecord"
	read_KVK	→		TUC_KON_202 "Lese Datei"
	send_APDU	→		TUC_KON_200 "SendeAPDU"
	sign_Data	→		TUC_KON_218 "Signiere"
	verify_eGK	→		TUC_KON_018 "eGK-Sperrung prüfen"
	write_Card_Data	→		TUC_KON_203 "SchreibeDatei"

		→		TUC_KON_210 "SchreibeRecord"
		→		TUC_KON_214 "FügeHinzurecord"
	write_eGK_Protocol	→		TUC_KON_006 "Datenzugriffsaudit eGK schreiben"
I_KV_Card_Reservati on	handle_Session	→	Kartendienst	TUC_KON_023 "Karte reservieren"
I_KV_Card_Unlockin g	authorize_Card	→	Kartendienst	TUC_KON_005 "Card-to-Card authentisieren"
	change_PIN	→		TUC_KON_019 "PIN ändern"
	enable_PIN disable_PIN	→		TUC_KON_027 „PIN-Schutz ein-/ ausschalten“
	do_C2C	→		TUC_KON_005 "Card-to-Card authentisieren"
	get_PIN_Status	→		TUC_KON_022 "Liefere PIN- Status"
	initialize_PIN	→		TUC_KON_019 "PIN ändern"
	unblock_PIN	→		TUC_KON_021 "PIN entsperren"
	verify_PIN	→		TUC_KON_012 "PIN verifizieren"
I_Notification_From_ FM	notify	→	Systeminformatio nsdienst	TUC_KON_256 "Systemereignis absetzen"

I_Local_Storage	write_Data read_Data erase_Data	→	Konnektormanagement	TIP1-A_5484
I_Poll_System_Information	get_Ressource_Information	→	Systeminformationsdienst	TUC_KON_254 "Liefere Ressourcendetails"
	get_Ressource_List	→		TUC_KON_252 "Liefere KT_Liste"
	get_Ressource_List	→		TUC_KON_253 "Liefere Karten_Liste"
I_Reg_Notification	register_for_Notifications	→	---	--- keine Umsetzung notwendig. Erfolgt implizit
I_Role_Information	get_Role	→	Kartendienst	TUC_KON_036 „LiefereFachliche Rolle“
I_SAK_Operations	sign_Document_QES	→	Signaturdienst	TUC_KON_150 „Dokumente QES signieren“
	verify_Document_QES	→		TUC_KON_151 "QES Dokumentensignatur prüfen"
I_Sign_Operations	sign_Document	→	Signaturdienst	TUC_KON_160 „Dokumente nonQES signieren“
	external_Authenticate	→		TUC_KON_160 „Dokumente nonQES signieren“
	verify_Document	→		TUC_KON_161 „nonQES Dokumentsignatur prüfen“

	get_Certificate	→	Kartendienst	TUC_KON_216 „LeseZertifikat“
I_Symm_Crypt_Operations	decrypt_Document_Symmetric	→	Verschlüsselungsdienst	TUC_KON_073 "Daten symmetrisch entschlüsseln"
	encrypt_Document_Symmetric	→		TUC_KON_072 "Daten symmetrisch verschlüsseln"
I_Synchronised_System_Time	get_Time	→	Zeitdienst	TUC_KON_351 "Liefere Systemzeit"
I_TLS_Client	send_Secure	→	TLS-Dienst	TUC_KON_110 "Kartenbasierte TLS-Verbindung aufbauen"
		→		TUC_KON_111 "Kartenbasierte TLS-Verbindung abbauen"
		→	Anbindung LAN/WAN	AFOs: Routing der IP-Pakete von Fachmodul (=Konnektor intern) --> VPN_TI
I_Directory_Query	search_Directory	→	LDAP-Proxy	TUC_KON_290 „LDAP-Verbindung aufbauen“
		→		TUC_KON_291 „Verzeichnis abfragen“
		→		TUC_KON_292 „LDAP-Verbindung trennen“

		→		TUC_KON_293 „Verzeichnisabfrage abbrechen“
I_KSRC_FM_Support	list_available_Packages	→	Software- Aktualisierung (KSR-Client)	TUC_KON_285 „UpdateInformationen für Fachmodul beziehen“
	load_Package	→		TUC_KON_286 „Paket für Fachmodul laden“

8847

8848

8849

Tabelle 391 – TAB_KON_712 Architektur der TI-Plattform, Berechtig Clientssysteme

Interface	Operation	→ Funktionsmerkmal	Interface:Operation
I_Crypt_Operations	decrypt_Document	→ Verschlüsselungsdienst	EncryptionService:DecryptDocument
	encrypt_Document	→	EncryptionService:EncryptDocument
I_DNS_Name_Resolution	get_FQDN	→ Namensdienst und Dienstlokalisierung	GetFQDN
	get_IP_Address	→	GetIPAddress
I_IP_Transport	send_Data_External	→ Anbindung LAN/WAN	AFOs: Routing der IP-Pakete von Client --> VPN_SIS
I_KV_Card_Handling	discard_Card_Usage_Reference	→ ---	--- keine Umsetzung notwendig. Erfolgt implizit
	get_Card_Usage_Reference	→ ---	--- keine Umsetzung notwendig. Erfolgt implizit

I_KV_Card_Unlocking	change_PIN	→	Kartendienst	CardService :ChangePin
	disable_PIN	→		CardService :EnablePin
	enable_PIN	→		CardService :DisablePin
	get_PIN_Status	→		CardService :GetPinStatus
	initialize_PIN	→		CardService :ChangePin
	unlock_PIN	→		CardService :UnlockPin
	verify_PIN	→		CardService :VerifyPin
I_Poll_System_Information	get_Ressource_Information	→	Systeminformationssdienst	EventService :GetResourceInformation
	get_Ressource_List	→		EventService :GetCardTerminals
	get_Ressource_List	→		EventService :GetCards
I_Reg_Notification	register_for_Notifications	→	Systeminformationssdienst	EventService :Subscribe
		→		EventService :Unsubscribe
		→		EventService :GetSubscription
I_SAK_Operations	sign_Document_QES	→	Signaturdienst	SignatureService :SignDocument
	verify_Document_QES	→		SignatureService :VerifyDocument
I_Sign_Operations	sign_Document	→	Signaturdienst	SignatureService :SignDocument

	verify_Document	→		SignatureService :VerifyDocument
	external_Authenticate	→	Authentifizierungs dienst	AuthSignatureSer vice :ExternalAuthenti cate
	get_Certificate	→	Zertifikatsdienst	CertificateService :ReadCardCertific ate
I_NTP_Time_Infor mation	sync_Time	→	Zeitdienst	I_NTP_Time_Infor mation :sync_Time
I_Directory_Query	search_Directory	→	LDAP-Proxy	LDAP-Operation (TIP1-A_5521)

8850

8851

8852

Tabelle 392 – TAB_KON_713 Architektur der TI-Plattform, Berechtig eHealth-KT

Interface	Operation	→	Funktionsmerkmal	Interface:Operation
I_Notification	notify	→	SICCT	Ereignisdienst :SICCT- Ereignisnachrichten
		→	SICCT	Ereignisdienst :ServiceAnnouncement

8853

8854

8855

Tabelle 393 – TAB_KON_714 Architektur der TI-Plattform, Berechtig Administrator

Interface	Operation	- >	Funktionsmerkmal	Interface:Operation
I_Change_System_Ti me	set_System_Ti me	- >	Zeitdienst	TIP1-A_4793 Konfigurierbarkeit des Konnektor NTP- Servers
I_Facade_Access_Conf iguration	add_Clientsyste m	- >	Fachliche Anbindung der Clientsysteme	TIP1-A_4518 Konfiguration der Anbindung Clientsysteme
	remove_Clients ystem			

	set_CS_Access_Mode			
I_KSRC_Local_Management	do_local_Update	- Software- > Aktualisierung (KSR-Client)		TUC_KON_280 "Konnektoraktualisierung durchführen"
I_KSRC_Management	do_Update	- Software- > Aktualisierung (KSR-Client)		TUC_KON_280 "Konnektoraktualisierung durchführen"
				TUC_KON_281 "Kartenterminalaktualisierung anstoßen"
	list_available_Updates			TUC_KON_282 "Update Informationen beziehen"
I_KTV_Management	configure_KTs	- Kartenterminalverwaltung >		Managementschnittstelle :TIP1-A_4555 Manuelles Hinzufügen eines Kartenterminals
				Managementschnittstelle :TIP1-A_4540 Reaktion auf KT Service Announcement
				Managementschnittstelle :TIP1-A_4556 Pairing mit Kartenterminal durchführen
				Managementschnittstelle :TIP1-A_4557 Ändern der Korrelationswerte eines Kartenterminals

10 Anhang I – Umsetzungshinweise (informativ)

In diesem Anhang finden sich Darstellungen und Informationen, die ein Konnektorhersteller zur Umsetzung der normativen Anforderungen in ein konkretes Produkt berücksichtigen kann. Sie wurden im Rahmen der Erhebung der normativen Anforderungen erarbeitet, um die Umsetzbarkeit der Anforderungen zu bestätigen. Dieser Anhang soll als Unterstützung für eine Umsetzung verstanden werden und erhebt keinen Anspruch auf Korrektheit und Vollständigkeit.

10.1 Systemüberblick

10.1.1 – Hinweise zur Sicherheitsevaluierung nach Common Criteria

Gemäß dem Sicherheitskonzept des Konnektors [gemKPT_Sich_Kon] muss die Software des Konnektors nach Common Criteria (CC) evaluiert und geprüft werden.

Diese Software erbringt Sicherheitsleistungen in zwei wesentlichen Funktionsblöcken. Durch diese Aufteilung ist es möglich, dass die einzelnen Funktionsblöcke zeitlich voneinander unabhängig bzw. sogar von unterschiedlichen Herstellern implementiert, evaluiert und geprüft werden können. Es werden zwei Schutzprofile (Protection Profile) für die Funktionsblöcke des Konnektors erstellt. Es handelt sich dabei um die Schutzprofile des Netzkonnektors (KONN.NK) sowie des Anwendungskonnektors (KONN.AK) inklusive der Signaturanwendungskomponente. Das Schutzprofil des Sicherheitsmoduls für den Konnektor (SM-K) wird in diesem Kapitel nicht betrachtet.

Diese Schutzprofile definieren eine implementierungsunabhängige Menge von Sicherheitsanforderungen für die einzelnen Konnektorfunktionsblöcke bzw. Konnektorbestandteile. Anhand dieser Schutzprofile werden von den Herstellern der Konnektoren die Sicherheitsvorgaben (Security Targets) für die konkreten Umgebungen erstellt, welche als Eingangsdokumente für den Zertifizierungsprozess der jeweiligen konkreten Komponenten eingesetzt werden. Diese zu evaluierenden Komponenten werden als Evaluierungsgegenstand (EVG) bezeichnet.

10.1.1.1 Separationsmechanismen des Konnektors

Damit es nach einer erfolgreichen Evaluierung eines Konnektors auch weiterhin möglich bleibt, Software oder Daten, die keinen direkten Einfluss auf Sicherheitsfunktionen der EVGs aufweisen, ohne eine Re-Evaluierung definiert auszutauschen, hinzuzufügen oder zu erweitern, ist eine Separation der Komponenten des EVG dringend anzuraten.

Implementiert der Hersteller keine bzw. nicht ausreichende Separationsmechanismen, so ist bei bestimmten Update-Arten von einer aufwändigen Re-Evaluierung des entsprechenden EVGs auszugehen. Die Separation dient also der Trennung zwischen ausführbarem Code des EVG, welcher Sicherheitsfunktionen umsetzt, und zusätzlichem ausführbarem Code auf dem Konnektor, welcher keine Sicherheitsfunktionen umsetzt.

Die Wahl der Separationsmechanismen steht dem Hersteller frei und muss in den Sicherheitsvorgaben für den EVG beschrieben und als solcher evaluiert werden. Aus diesen Sicherheitsvorgaben ergibt sich auch, welche Update-Arten bei welchen Separationsmechanismen eine Re-Evaluierung des EVG erfordern und wie aufwendig diese Re-Evaluierung ausfällt.

8898 Unter diese Update-Arten können beispielsweise – je nach Konnektorarchitektur, CC-
8899 Dokumentation oder Konnektorimplementierung – Bestandteile des unter dem Konnektor
8900 arbeitenden Betriebssystems, die Installation dezentraler Komponenten von Fachlogik
8901 oder Konfigurationsdaten des Konnektors fallen.

8902 Als Beispiel für Separationsmechanismen sei auf die folgende informative Aufzählung
8903 verwiesen, welche jedoch keinen Anspruch auf Vollständigkeit besitzen kann und nur
8904 mögliche Alternativen aufzeigt:

- 8905 • Java-Sandbox-Konzept,
- 8906 • Interpreter mit restriktiver Laufzeitprüfung,
- 8907 • vom Betriebssystem bereitgestellte Prozess- und Speichertrennung,
- 8908 • virtuelle Maschinen,
- 8909 • physische Trennung durch separierte Hardware.

8910 Je nach gewähltem Architekturansatz des Herstellers sind nicht alle hier genannten
8911 Alternativen für die Separation des EVG auf dem Konnektor anwendbar.

8912 Insbesondere sollte der Hersteller den eigentlichen Update-Prozess und die dafür
8913 verantwortliche Komponente mit besonderer Sorgfalt beschreiben, spezifizieren und
8914 implementieren. Bei einer fehlerhaften Implementierung dieser Komponente besteht die
8915 Gefahr einer Schwächung oder des Ausschaltens von Sicherheitsfunktionen des EVG. Die
8916 Update-Komponente muss eine sichere Zuweisung der Updates zu den separierten
8917 Bestandteilen des EVGs gewährleisten. Auch ist zu betonen, dass der EVG immer die
8918 Integrität der Daten des Updates und die Authentizität des Absenders prüfen muss, bevor
8919 ein Update akzeptiert wird. Der Update-Komponente muss somit besondere Beachtung
8920 geschenkt werden.

8921 **10.1.1.2 Granularität der TSF**

8922 Die TSF (TOE Security Functionality) eines EVG besteht aus Subsystemen und Modulen,
8923 wobei ein Modul die genaueste Beschreibung einer Funktionalität darstellt und unterhalb
8924 der Subsysteme angesiedelt ist. Subsysteme beschreiben das Design des EVG und
8925 können wiederum – je nach Komplexität eines EVGs – aus weiteren Subsystemen
8926 bestehen. Ein Entwickler sollte außer der Modulbeschreibung keine weiteren
8927 Informationen zur Implementierung der dort beschriebenen Funktionalität benötigen.

8928 Die Subsysteme und Module der TSF gliedern sich in drei Klassen:

- 8929 (a) SFR-Enforcing Subsysteme und Module. Hierunter fallen die Subsysteme und
8930 Module, welche eine funktionale Sicherheitsanforderung direkt durchsetzen.
- 8931 (b) SFR-Supporting Subsysteme und Module. Hierunter fallen die Subsysteme und
8932 Module, welche bei der Durchsetzung einer funktionalen Sicherheitsanforderung
8933 unterstützend wirken.
- 8934 (c) SFR-Non-Interfering Subsysteme und Module. Hierunter fallen die Subsysteme
8935 und Module, welche keine Leistung bei der Erfüllung einer funktionalen
8936 Sicherheitsanforderung erbringen.

8937 Sollte nach einer erfolgreichen CC-Evaluierung eines Konnektors die Notwendigkeit zur
8938 Änderung der Software des Konnektors gegeben sein, so ist unter Umständen eine Re-
8939 Evaluierung des EVG erforderlich. Diese Notwendigkeit kann sich aus der Behebung von
8940 nachträglich erkannten Fehlern, aufgetretenen Sicherheitslücken, Schwächen eines
8941 Standardverfahrens oder einer erforderlichen Erweiterung der Funktionalität ergeben.

8942 Im Rahmen der Aufzählung der Anforderungen an die Beschreibung des EVG-Design
8943 (ADV_TDS) wird bereits die Aufteilung der TSF auf Subsysteme und Module beschrieben.
8944 Trotzdem soll hiermit ausdrücklich geraten werden, die Aufteilung der TSF auf die
8945 Subsysteme und Module selbst und die Aufteilung der Subsysteme und Module auf die
8946 drei o. g. Klassen möglichst feingranular durchzuführen.

8947 Denn so

- 8948 1. können einfacher umfassende Tests durchgeführt und die Testabdeckung
8949 sichergestellt werden,
- 8950 2. kann bei der Veränderung von Programmcode der Evaluator die Auswirkungen auf
8951 SFR-Enforcing, Supporting oder Non-Interfering SFRs einfacher herausfinden und
8952 damit die Kosten und den zeitlichen Aufwand einer Re-Evaluierung senken.
- 8953 3. kann bei der Veränderung von Programmcode, welcher als SFR-Non-Interfering
8954 eingestuft wird, das Maintenance-Verfahren anstelle einer Re-Evaluierung
8955 angewandt werden, welches einen erheblichen zeitlichen und damit auch
8956 monetären Vorteil gegenüber dem Re-Evaluierungsverfahren darstellt.

8957 **10.2 Übergreifende Festlegungen**

8958 **10.2.1 Interne Mechanismen**

8959 **10.2.1.1 Zufallszahlen und Schlüssel**

8960 Der Konnektor kann zur Erzeugung von Zufallszahlen und Einmalschlüsseln einen
8961 Hardware- oder Software-Generator verwenden. Als Quelle für Zufallszahlen kann der
8962 Konnektor die gSMC-K verwenden.

8963 **10.3 Funktionsmerkmale**

8964 **10.3.1 Anwendungskonnektor**

8965 **10.3.1.1 Administration des Informationsmodells**

8966 Wie die Administration der persistenten Entitäten und Beziehungen des
8967 Informationsmodells im Detail über die bereitzustellende Administrationsoberfläche
8968 erfolgt, entscheidet der Hersteller.

8969 Es wird folgende Reihenfolge für die Pflege des Informationsmodells empfohlen.

- 8970 1. Mandantenübergreifende Administration:
 - 8971 • Es werden die Entitäten Arbeitsplätze, Clientsysteme mit
8972 Authentifizierungsmerkmalen CS-AuthMerkmal und SMC-B_Verwaltet
8973 erfasst.
8974 Die Eingabe der Kartenterminals erfolgt über die Kartenterminalverwaltung.
 - 8975 • Es wird die Beziehungen zwischen Arbeitsplatz und Kartenterminals „lokal“ und
8976 „entfernt (zentral)“ eingepflegt.
- 8977 2. Mandantenbezogene Administration:
 - 8978 • Die Definition bzw. Auswahl eines Mandanten bildet den Einstiegspunkt.

- Pro Mandanten werden aus den bereits eingepflegten Entitäten „Kartenterminal“, „Arbeitsplatz“, „Clientsystem“, „SMC-B_Verwaltet“ die für den Mandanten im Zugriff erlaubten zugeordnet.
- Pro Mandant erfolgt eine Zuordnung der Arbeitsplätze zu Clientsystemen.
- Pro Mandant erfolgt eine Zuordnung der lokalen Kartenterminals, über die jeweils pro Arbeitsplatz die Eingabe der Remote-PIN erfolgen darf.

10.3.1.2 Vorgehensvariante für das Handling von CardSessions

Das in der [TIP1-A_4560] „Rahmenbedingungen für Kartensitzungen“ geforderte Verhalten, ließe sich über folgenden Mechanismus umsetzen:

Verschiedene Clientsystem (oder verschiedene Nutzer an einem Clientsystem) möchten auf Daten der über CardHandle adressierten Smartcard zugreifen.

Für die Zugriffe müssen, je nach Definition der Zugriffsbedingung in der Zielkarte, bestimmte Sicherheitszustände erreicht werden (durch Verifikation einer PIN oder durch C2C). Diese erreichten Sicherheitszustände werden innerhalb einer Karte jeweils an einen logischen Kanäle (bzw. den Basiskanal) gebunden, d. h., das Erhöhen oder Absenken eines Sicherheitszustands wirkt nicht außerhalb des logischen Kanals, in dem die Veränderung verursacht wurde.

Finden nun Clientsystemzugriffe in unterschiedlichen Kontexten (Mandant, Clientsystem, Arbeitsplatz und Nutzer verschieden) auf die gleiche Karte statt, so muss sichergestellt sein, dass PIN-Eingaben und durchgeführte C2C nur für den Kontext wirksam sind, in welchem sie durchgeführt wurden. Dies ließe sich erreichen, wenn jeder Kontext auf einen eigenen logischen Kanal der Karte abgebildet würde. Leider unterstützen der HBA und die SMC-B nur vier, die eGK nur einen logischen Kanal. Mehrere gleichzeitige unterschiedliche Kontexte wären somit nicht möglich.

Eine mögliche Lösung für beliebig viele gleichzeitige Kontexte:

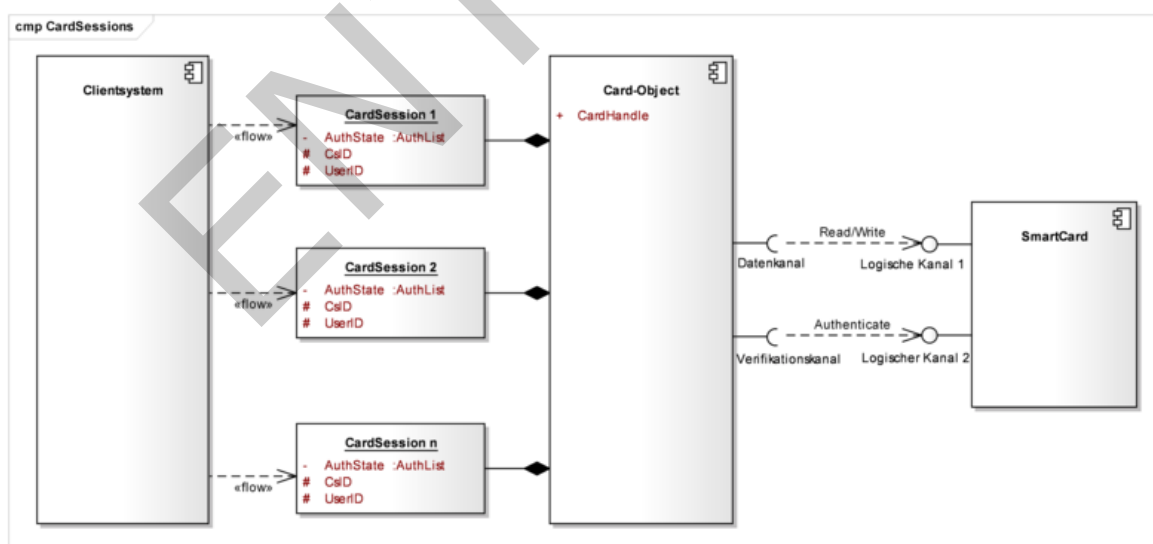


Abbildung 23: PIC_KON_120 Abbildung von CardSessions auf logische Kanäle

Der Kartendienst fungiert als Multiplexer. Er spiegelt die Zugriffsrechte der Karte und wendet deren Regeln selbständig gegen die unterschiedlichen Zugriffe durch Clientsysteme an.

- 9010 Für jedes Card-Objekt wird „in Richtung Clientsystem“ pro Kontext genau eine
 9011 CardSession erzeugt und verwaltet. Zugriffe des Clientsystems erfolgen somit „im
 9012 Kontext“ einer CardSession.
- 9013 In Richtung Karte verwendet das Card-Object genau zwei Kanäle (zwei logische oder
 9014 einen logischen und einen Basiskanal):
- 9015 • Einen Datenkanal, über den die Datenbewegungen und kryptographischen
 9016 Operationen laufen und
 - 9017 • Einen Verifikationskanal, der ausschließlich für Authentisierungszwecke verwendet
 9018 wird
- 9019 In jeder CardSession werden die in ihrem Kontext erreichten Sicherheitszustände
 9020 vermerkt. Das Vorgehen für die Durchführung der Verifikationen und des Vermerkens der
 9021 erreichten Sicherheitszustände, sowie der Datenzugriffe folgt folgenden Regeln (hier für
 9022 PIN-Verifikation, sinngleich auch für C2C):
- 9023 • Soll über eine CardSession eine PIN-Verifikation für PinRef_A gegen eine Karte
 9024 durchgeführt werden und der erhöhte Sicherheitszustand für PinRef_A ist noch
 9025 nicht erreicht (bsp. direkt nach einem Karten-Reset), dann leite die Verifikation
 9026 über den Datenkanal (initiale Freischaltung des Datenkanals für folgende
 9027 Datenzugriffe).
 - 9028 • Soll über eine CardSession eine PIN-Verifikation für PinRef_A gegen eine Karte
 9029 durchgeführt werden und der erhöhte Sicherheitszustand für PinRef_A ist auf dem
 9030 Datenkanal bereits erreicht, dann leite die Verifikation über den
 9031 Verifikationskanal.
 - 9032 • Wurde durch eine CardSession eine Verifikation für PinRef_A erfolgreich
 9033 durchgeführt, wird dieser erreichte Sicherheitszustand für PinRef_A in der
 9034 zugreifenden CardSession vermerkt
 - 9035 • Datenzugriffe auf oder Kryptooperationen mit Karten werden durch den
 9036 Kartendienst nur zugelassen, wenn die zugreifende CardSession über einen für
 9037 diese Zugriffe benötigten erhöhten Sicherheitszustand verfügt. Ist der benötigte
 9038 Vermerk für die zugreifende CardSession nicht vorhanden, beantwortet der
 9039 Kartendienst die Anfrage mit der passenden Kartenfehlermeldung. Es erfolgt keine
 9040 Interaktion mit der Karte.
- 9041 Diese Regeln führen dazu, dass eine durch CardSession Y fehlgeschlagene Verifikation für
 9042 PinRef_A die zuvor erfolgreich durch CardSession X durchgeführte Verifikation nicht
 9043 beeinflusst. Kartenzugriffe auf dem Datenkanal sind für CardSession X weiterhin möglich,
 9044 da der Verlust des erhöhten Sicherheitszustands durch fehlerhafte Verifikation immer nur
 9045 im Verifikationskanal erfolgt.
- 9046 Dieser Mechanismus funktioniert mit zwei Kanälen zu einer Karte für beliebig viele
 9047 CardSessions.

9048 **10.3.1.3 Darstellung von Terminal-Anzeigen auf einem Kartenterminal**

- 9049 Die folgenden Ausführungen dienen der Klarstellung für die korrekte Verwendung der zur
 9050 Verfügung stehenden Datenobjekte (DO) zur Darstellung von Terminal-Anzeigen an
 9051 einem Kartenterminal nach SICCT- und eHealth-Kartenterminal-Spezifikation.
- 9052 Die SICCT-Spezifikation enthält eine Liste von Datenobjekten (DO), die von den
 9053 Kartenterminals unterstützt werden müssen oder können. Dabei gibt es zwei
 9054 Datenobjekte zur Anzeige von Terminal-Anzeigen: APPL DO und SMTBD DO.

- 9055 Kartenterminals müssen APPL DO (steht für Application Label Data Object) unterstützen.
 9056 APPL DOs müssen immer eine 7 Bit ISO646DE/DIN66003-Codierung enthalten
 9057 [DIN66003].
- 9058 Kartenterminals können SMTBD DO (steht für SICCT Message-To-Be-Displayed Data
 9059 Object) unterstützen, müssen dieses aber nicht. Über SMTBD DOs können weitere
 9060 Zeichensätze am Display angezeigt werden.
- 9061 Der Konnektor soll APPL DOs verwenden. Er kann SMTBD DOs verwenden, wenn er
 9062 sicherstellt, dass das angesteuerte Kartenterminal diese unterstützt und die dargestellte
 9063 Meldung der Klartextmeldung entspricht, die mittels APPL DO erreicht worden wäre.
- 9064 Um dem Kartenterminal den Umbruch längerer Texte über das Zeilenende hinaus zu
 9065 erleichtern, enthalten die Terminal-Anzeigen das Zeichen 0x0B als „Soll-
 9066 Zeilenumbrüche“. Die „Soll-Zeilenumbrüche“ werden nicht als Textzeichen gezählt. Sie
 9067 zeigen einen potentiellen Zeilenumbruch an. Diese müssen vom Kartenterminal
 9068 herausgefiltert werden und werden nicht durch andere Zeichen ersetzt.
- 9069 Die Maximallänge für Terminal-Anzeigen beträgt ohne PIN-Eingabe (OUTPUT [O]) 48
 9070 Zeichen.
- 9071 Besonderheit bei Terminal-Anzeigen, die zu einer PIN-Eingabe (INPUT [I]) auffordern:
- 9072 Für die PIN-Eingabe wird eine strukturierte Terminal-Anzeige übergeben, aufgeteilt auf
 9073 maximal 40 Zeichen für die Terminal-Anzeige plus maximal 10 Zeichen für den sog. PIN-
 9074 Prompt (bei Platz für zusätzliche 6 Zeichen für die PIN-Eingabe). Ein gültiger String hat
 9075 die Form: <Terminal-Anzeige>0x0F<PIN-Prompt>. Auch die Terminal-Anzeige für
 9076 Eingaben soll mit „Soll-Zeilenumbrüchen“ versehen werden.
- 9077 Bei der Übertragung der Terminal-Anzeige ist auf die korrekte Codierung der
 9078 Zeichenkette zu achten. Der einzige Zeichensatz, der von allen Kartenterminals
 9079 unterstützt werden MUSS, ist (7 Bit) ISO646DE/DIN66003 [DIN66003]. Dadurch darf
 9080 eine Terminal-Anzeige auch deutsche Sonderzeichen enthalten.
- 9081
- 9082

Hex Cod e	...0	... 1	... 2	... 3	... 4	... 5	... 6	... 7	... 8	... 9	... A	... B	... C	... D	... E	... F
0...	<i>diverse Steuerzeichen - nicht verwendet -</i>															
1...	<i>diverse Steuerzeichen - nicht verwendet -</i>															
2...	<i>space</i>	!	"	#	\$	%	&	'	()	*	+	,	-	.	/
3...	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4...	§	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5...	P	Q	R	S	T	U	V	W	X	Y	Z	Ä	Ö	Ü	^	_
6...	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7...	p	q	r	s	t	u	v	w	x	y	z	ä	ö	ü	ß	<i>de /</i>

Abbildung 24: PIC_KON_007 Übersicht Zeichensatz ISO646DE/DIN66003

9085

ENTWURF

11 Anhang K – Szenarien im dezentralen Umfeld

Die folgenden Szenarien für den Einsatz der Produkte der Telematikinfrastruktur beschreiben informativ Varianten und Optionen, die durch die Spezifikationen abgedeckt werden.

Die vorliegenden Abbildungen in diesem Anhang fokussieren auf das dezentrale Umfeld und verzichten daher auf die Darstellung der zentralen Anteile, wie das zentrale Netzwerk der Telematikinfrastruktur, welches über den „VPN-Konzentrator TI“ erreichbar ist.

Der Konnektor, sowie die Netzwerkkomponenten Switch und IAG (Internet Access Gateway) sind in den folgenden Szenarien zum Schutz vor unerlaubtem Zugriff gemäß den Annahmen des Sicherheitskonzeptes vor unbefugten physischen Zugriffen geschützt installiert.

Die folgenden Abschnitte stellen jeweils ein Szenario in der Übersicht als Diagramm, eine Beschreibung sowie eine kurze Auflistung der Voraussetzungen und Auswirkungen dar.

11.1 Szenario 1: Einfache Installation ohne spezielle Anforderungen und ohne bestehende Infrastruktur

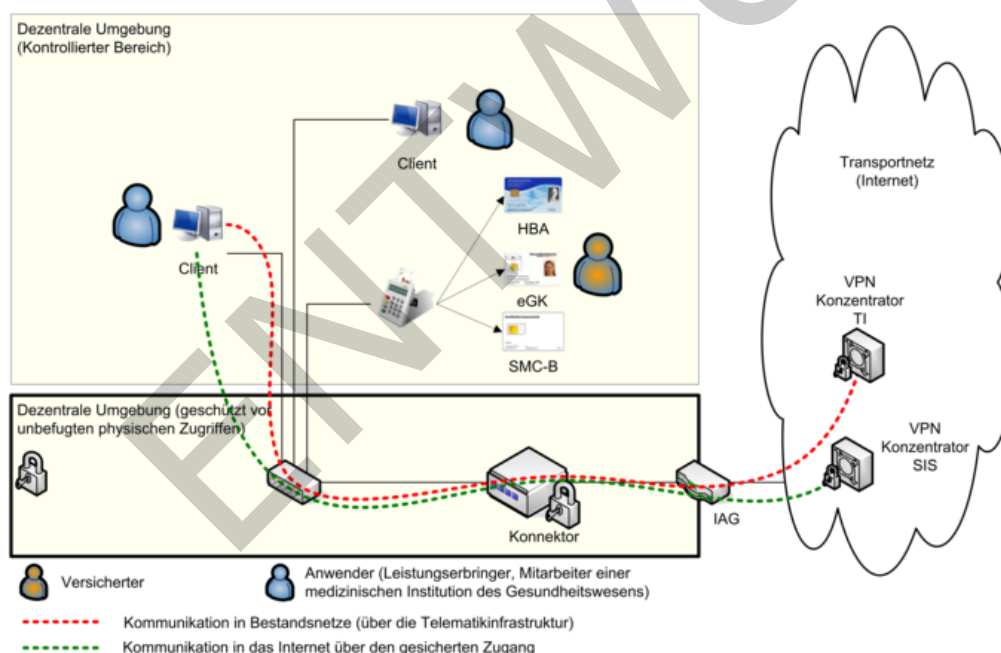


Abbildung 25: Szenario einer einfachen Installation

11.1.1 Beschreibung des Szenarios

Abbildung 25 zeigt ein einfaches Szenario für das dezentrale Umfeld. Es wird der Konnektor als Default-Gateway für jegliche IP-Kommunikation aus dem LAN in das WAN eingesetzt. Dabei übernimmt der Konnektor das Routing der Kommunikation in das Internet über den SIS (Secure Internet Service) und in die an die TI angeschlossenen

9110 Bestandsnetze. Die Bezeichnung IAG (Internet Access Gateway) steht für die Geräte, die
9111 den Internetzugang ermöglichen und typischerweise vom Internet Service Provider (ISP)
9112 zur Verfügung gestellt werden (z.B. DSL Router und DSL Modem).

9113 Ein oder mehrere Clientsysteme können über den Konnektor Anwendungsfälle der
9114 Telematikinfrastruktur initiieren und über den Konnektor und die zentrale TI-Plattform in
9115 Bestandsnetze kommunizieren (rote gestrichelte Linie). Dabei ist die Nutzung der
9116 Anwendungsfälle der Telematikinfrastruktur je nach Konfiguration des Konnektors
9117 entweder nur authentifizierten Clients möglich oder beliebigen Clients.

9118 In diesem einfachen Szenario werden über ein einziges Kartenterminal die SMC-B, der
9119 HBA und auch die eGK des Versicherten gelesen, es können dazu alternativ auch
9120 mehrere Kartenterminals genutzt werden.

9121 Darüber hinaus können die Clientsysteme über den SIS (Secure Internet Service) auf
9122 Dienste des Internets zugreifen.

9123 **11.1.2 Voraussetzungen**

- 9124 • Anbindung der bestehenden Clientsysteme an ein zum Konnektor kompatibles
9125 LAN muss möglich sein.
- 9126 • Konfiguration des Konnektors als Default-Gateway in den Clientsystemen und
9127 Konfiguration der notwendigen VPN-Tunnel im Konnektor, um in die
9128 verschiedenen Netze zu routen.
- 9129 • Verfügbarkeit einer SMC-B

9130 **11.1.3 Auswirkungen**

- 9131 • Die Clientsysteme können über den Konnektor Anwendungsfälle der TI initiieren
- 9132 • Die Clientsysteme können über den Konnektor auf das Internet und
9133 Bestandsnetze zugreifen

11.2 Szenario 2: Installation mit mehreren Behandlungsräumen

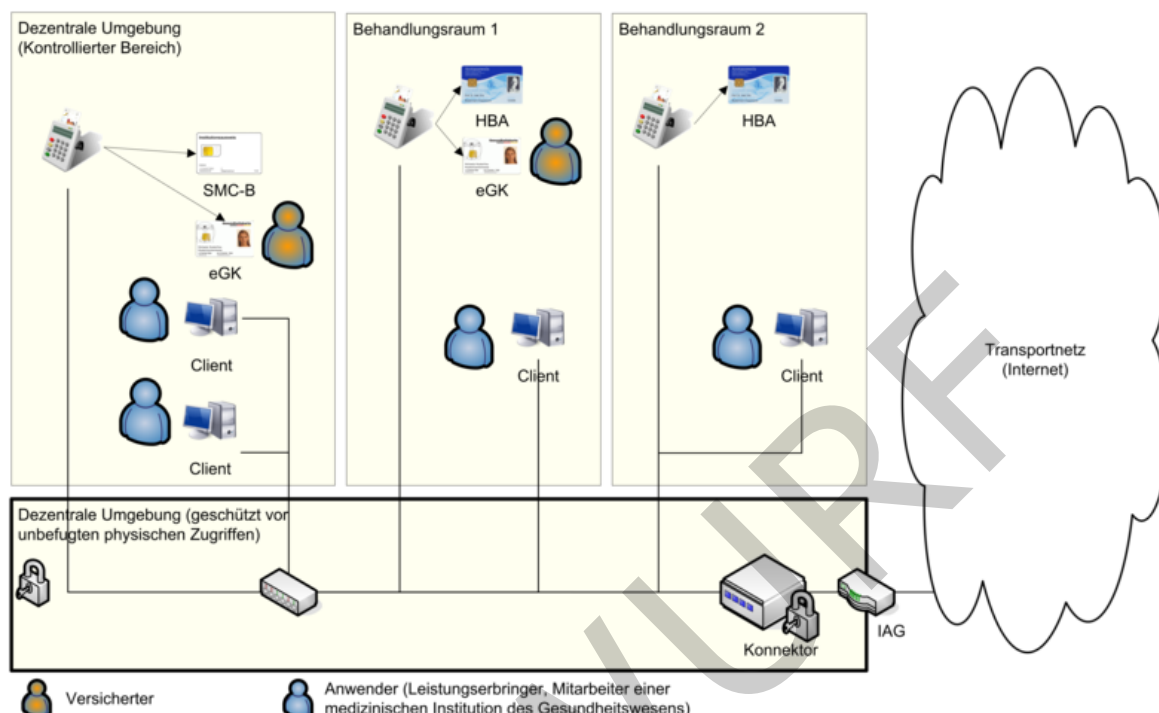


Abbildung 26: Szenario einer Installation mit mehreren Behandlungsräumen

11.2.1 Beschreibung des Szenarios

Mit der in Szenario 1 skizzierten Topologie kann auch ein Szenario bedient werden, bei dem mehrere Behandlungsräume unterstützt werden (siehe Abbildung 26). Dabei ist in jedem Behandlungsraum mindestens ein Kartenterminal vorzusehen, so dass die eGK gelesen werden kann.

Auf die Darstellung der Kommunikationswege in zentrale Netze wurde in Abbildung 26 verzichtet, da sich hier keine Änderung gegenüber Szenario 1 ergibt.

Durch die Ressourcenverwaltung des Konnektors wird sichergestellt, dass bei Anwendungsfällen diejenigen Kartenterminals angesprochen werden, welche dem Arbeitsplatz zugeordnet sind, von dem aus der Anwendungsfall initiiert wurde.

11.2.2 Voraussetzungen

- Anbindung der bestehenden Clientsysteme an ein zum Konnektor kompatibles LAN muss möglich sein.
- Konfiguration des Konnektors als Default-Gateway in den Clientsystemen und Einrichtung der notwendigen VPN-Tunnel im Konnektor, um in die verschiedenen Netze zu routen.
- Verfügbarkeit einer SMC-B und mehrerer Kartenterminals und Clientsysteme

- 9156 • Die Clientsysteme und Kartenterminals und deren Relationen sind dem Konnektor
9157 über Konfiguration bekannt gemacht worden.

9158 11.2.3 Auswirkungen

- 9159 • Die Clientsysteme können über den Konnektor Anwendungsfälle der TI initiieren
9160 • Die Clientsysteme können über den Konnektor auf das Internet (über den SIS)
9161 und Bestandsnetze zugreifen
9162 • Der HBA-Inhaber muss seinen HBA mit sich führen und kann diesen in den
9163 einzelnen Kartenterminals der Behandlungsräume nutzen.

9164 11.3 Szenario 3: Integration in bestehende Infrastruktur ohne 9165 Netzsegmentierung

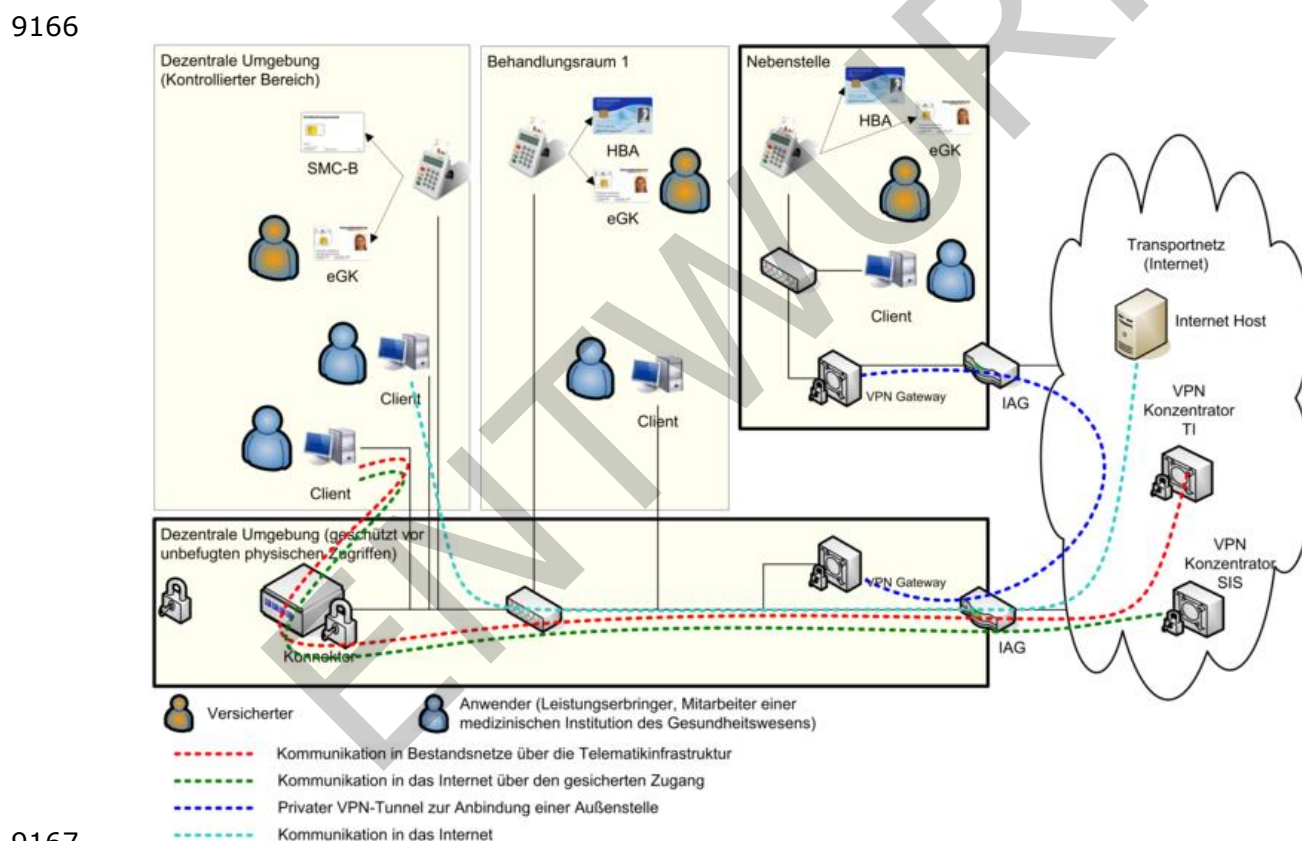


Abbildung 27: Szenario einer Integration der TI Produkte in eine bestehende Infrastruktur

9171 11.3.1 Beschreibung des Szenarios

9172 Im Falle einer bereits vorhandenen Infrastruktur im dezentralen Bereich können die
9173 Produkte der TI, insbesondere der Konnektor, so in die Infrastruktur integriert werden,
9174 dass Bestandsanwendungen bereits erprobte Kommunikationswege weiter nutzen
9175 können.

9176 Wie in Abbildung 27 beispielhaft dargestellt, existiert bereits eine Infrastruktur, die
 9177 sowohl einen Internetzugang für die Arbeitsplätze ermöglicht (gestrichelte Linie in
 9178 türkis), als auch eine Nebenstelle über VPN anbindet (gestrichelte Linie in blau). In
 9179 diesem Fall wird der Konnektor als zusätzliches Gerät an das bestehende Netzwerk
 9180 angeschlossen und nutzt den bereits vorhandenen Internetanschluss zur Kommunikation
 9181 in die TI.

9182 Für die Clientsysteme muss in diesem Szenario je nach individuellem Anforderungsprofil
 9183 entschieden werden, ob das jeweilige Clientsystem über die Telematikinfrastuktur
 9184 kommunizieren können soll und den gesicherten Internetzugang (SIS) nutzen soll oder
 9185 nicht.

9186 Soll ein Clientsysteme nicht über die Telematikinfrastuktur kommunizieren, bleibt der
 9187 IAG als Default-Gateway dieses Clientsystems konfiguriert. In diesem Fall routet der IAG
 9188 die eingehenden IP-Pakete mit öffentlichen Zieladressen weiter in das Internet. Die
 9189 gestrichelte Linie in türkis zeigt beispielhaft einen Zugriff in das Internet.

9190 Soll ein Clientsystem über die Telematikinfrastuktur kommunizieren oder den
 9191 gesicherten Internetzugang (SIS) nutzen, muss der Konnektor als Default-Gateway
 9192 konfiguriert werden. In diesem Fall routet der Konnektor die eingehenden IP-Pakete, die
 9193 nicht für ihn bestimmt sind, entweder durch den VPN-Tunnel der TI über die
 9194 Telematikinfrastuktur in ein angeschlossenes Bestandsnetz, (gestrichelte Linie in rot)
 9195 oder durch den VPN-Tunnel zum SIS (Secure Internet Service) in das Internet
 9196 (gestrichelte Linie in grün). Sollte kein sicherer Internetzugang konfiguriert sein, so
 9197 würde der Konnektor den Traffic verwerfen und ggf. per ICMP dem Client eine anderes
 9198 Gateway (IAG) vorschlagen. Alternativ können die von den Clients benötigten Routing-
 9199 Informationen manuell oder per DHCP konfiguriert werden.

9200 11.3.2 Voraussetzungen

- 9201 • Konnektor ist kompatibel zur bestehenden Infrastruktur (Vernetzung)
- 9202 • Die bestehende Infrastruktur verfügt über einen Internetzugang
- 9203 • Verfügbarkeit einer SMC-B und mehrerer Kartenterminals
- 9204 • Die Clientsysteme und Kartenterminals und deren Relationen sind dem Konnektor
 9205 über Konfiguration bekannt gemacht worden.

9206 11.3.3 Auswirkungen

- 9207 • Produkte der Telematik können „minimal-invasiv“ in die bestehende Infrastruktur
 9208 integriert werden. Bestehende Kommunikationswege können weiter genutzt
 9209 werden.
- 9210 • Für Clients kann je nach individuellen Anforderungsprofil der sichere
 9211 Internetzugang über den Konnektor genutzt werden oder der direkte
 9212 Internetzugang über den bestehenden IAG

Das Diagramm zeigt die Telematikinfrastruktur (TI) in einem Gesundheitswesen. Es ist in vier Hauptbereiche unterteilt:

- Dezentrale Umgebung (Kontrollierter Bereich):** Enthält eine SMC-B, eine eGK, einen Client und einen weiteren Client. Ein roter gestrichelter Pfeil führt von der eGK zum Router, ein grüner gestrichelter Pfeil von einem Client zum Router.
- Behandlungsraum 1:** Enthält eine HBA, eine eGK und einen Client. Ein roter gestrichelter Pfeil führt von der HBA zum Router, ein grüner gestrichelter Pfeil von einem Client zum Router.
- Nebenstelle:** Enthält eine HBA, eine eGK, einen Client, einen VPN Gateway und einen IAG. Ein roter gestrichelter Pfeil führt von der HBA zum Router, ein grüner gestrichelter Pfeil von einem Client zum Router. Ein blauer gestrichelter Pfeil führt vom VPN Gateway zum IAG.
- Transportnetz (Internet):** Enthält einen VPN Konzentratoren TI, einen VPN Konzentratoren SIS und einen weiteren VPN Konzentratoren SIS. Ein roter gestrichelter Pfeil führt von der TI zum IAG, ein grüner gestrichelter Pfeil von der SIS zum IAG.

Die Kommunikation erfolgt über die Telematikinfrastruktur (TI) und ein gesichertes Internet-Zugang. Die Nebenstelle ist über einen privaten VPN-Tunnel mit der TI verbunden. Die TI ist über einen VPN-Konzentrator mit dem Internet-Transportnetz verbunden.

Legende:

- Versicherter
- Anwender (Leistungserbringer, Mitarbeiter einer medizinischen Institution des Gesundheitswesens)
- Kommunikation in Bestandsnetze über die Telematikinfrastruktur
- Kommunikation in das Internet über den gesicherten Zugang
- Privater VPN-Tunnel zur Anbindung einer Außenstelle

11.4.1 Beschreibung des Szenarios

11.4.2 Voraussetzungen

- Konnektor ist kompatibel zur bestehenden Infrastruktur (Vernetzung)
- Verfügbarkeit einer SMC-B und mehrerer Kartenterminals
- Der Konnektor ist dem bestehenden Router als Gateway bekannt gemacht.

11.4.3 Auswirkungen

- Produkte der Telematik können „minimal-invasiv“ in die bestehende Infrastruktur integriert werden. Bestehende Kommunikationswege können weiter genutzt werden.
- Die Default-Gateway-Konfiguration der Clients muss nicht geändert werden.

11.5 Szenario 5: Zentral gesteckter HBA

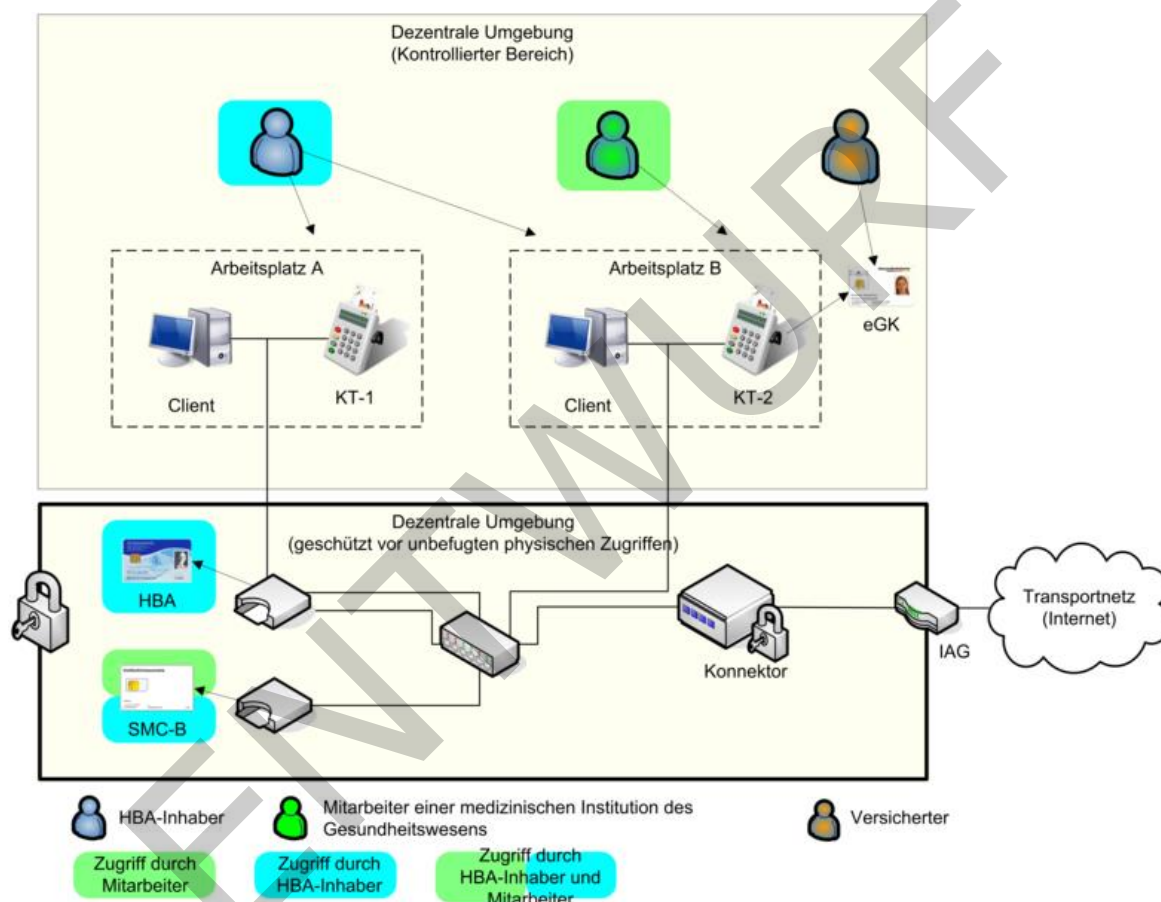


Abbildung 29: Szenario mit zentral gesteckten HBA und SMC-B

11.5.1 Beschreibung des Szenarios

Dieses Szenario zeichnet sich dadurch aus dass ein HBA nicht durch seinen Inhaber mitgeführt und am Arbeitsplatz gesteckt wird, sondern zentral und geschützt vor unbefugten physischen Zugriffen gesteckt bleibt.

Der HBA-Inhaber greift über jeden konfigurierten Arbeitsplatz auf seinen HBA zu. Die Remote-PIN-Eingabe erfolgt unter Verwendung des lokal am Arbeitsplatz vorhandenen eHealth-Kartenterminals.

9248 Die Mechanismen zum Zugriff auf eine zentral gesteckte SMC-B funktionieren analog zum
9249 HBA.

9250 **11.5.2 Voraussetzungen**

9251 Folgende zusätzliche Punkte müssen erfüllt sein, um dieses Szenario umzusetzen:

- 9252 • Stecken der zentral gesteckten Karten HBA und SMC-B (ohne direkte Aufsicht)
9253 und Sicherstellung des Schutzes vor unbefugtem physischen Zugriff
- 9254 • Konfiguration im Konnektor: Lokales eHealth-Kartenterminals als lokales eHealth-
9255 Kartenterminal für eine Remote-PIN-Eingabe eines bestimmten Arbeitsplatzes.
9256 *Im abgebildeten Beispiel KT-1 für Arbeitsplatz A und KT-2 für Arbeitsplatz B.*
- 9257 • Konfiguration im Konnektor: Assoziation der gewünschten Arbeitsplätze zum
9258 jeweiligen Kartenterminal mit zentral gesteckter Karte.
9259 *Im abgebildeten Beispiel Arbeitsplatz A assoziiert mit dem eHealth-Kartenterminal
9260 des HBAs und Arbeitsplatz B mit eHealth-Kartenterminal des HBAs und dem
9261 eHealth-Kartenterminal der SMC-B.*

9262 **11.5.3 Auswirkung**

- 9263 • HBA muss nicht mehr durch seinen Inhaber mitgeführt werden
- 9264 • SMC-B muss nicht mehr unter ständiger Aufsicht eines Mitarbeiters einer
9265 Organisation des Gesundheitswesens sein.

11.6 Szenario 6: Installation mit zentralem PS

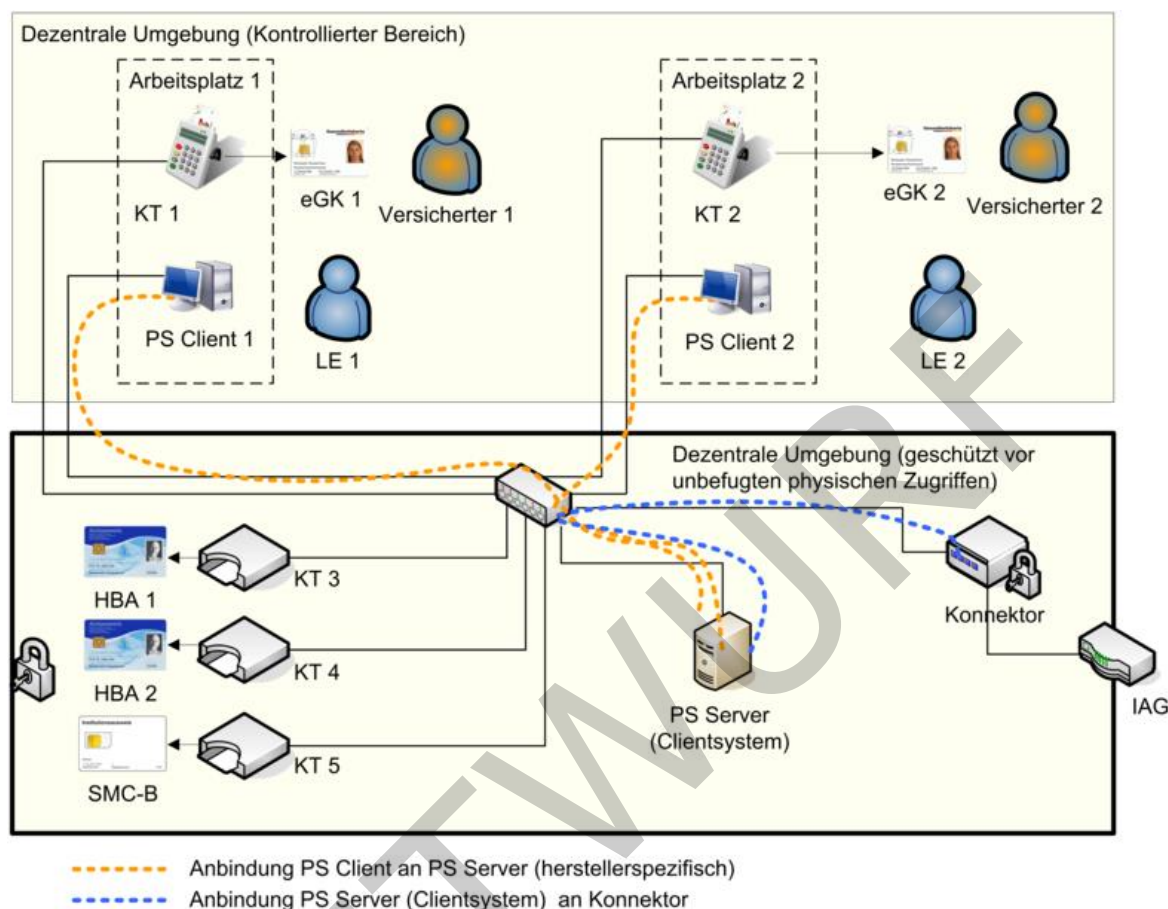


Abbildung 30: Szenario mit zentralem Primärsystem als Clientsystem

11.6.1 Beschreibung des Szenarios

Das Szenario skizziert eine dezentrale Konfiguration, bei der das Primärsystem aus einem Serveranteil „PS Server“ und mehreren Clientanteilen „PS Client“ besteht. Die Anbindung zwischen dem „PS Server“ und den „PS Clients“ ist herstellerspezifisch. Der „PS Server“ fungiert als ein einziges Clientsystem gegenüber der TI bzw. dem Konnektor (z.B. als Terminalserver). Die Clientsystemschnittstelle des Konnektors wird ausschließlich vom „PS Server“ genutzt. Der „PS Server“ muss bei der Kommunikation mit dem Konnektor eine Übersetzung der zugreifenden „PS Clients“ auf die entsprechende Entität „Arbeitsplatz“ des Konnektors durchführen.

Beispielhaft zeigt das Szenario zwei Arbeitsplätze mit jeweils einem Kartenterminal für die eGK sowie zentral gesteckte SMC-B und HBAs. Alternativ sind auch lokal am Arbeitsplatz gesteckte HBAs möglich.

9283 11.6.2 Voraussetzungen

- 9284 • Netzanbindung aller Komponenten (u. a. KT, PS Client, PS Server, Konnektor) in
9285 der dezentralen Umgebung bis einschließlich zur Netzwerkschicht (IP-Ebene)
- 9286 • Konfiguration des Primärsystems mit seinen Anteilen „PS Server“ und ggf.
9287 mehreren „PS Clients“ passend zum Informationsmodell des Konnektors
9288 (herstellerspezifisch).
- 9289 • Konfiguration des Konnektors. U. a.:
 - 9290 • Informationsmodell:
9291 Beim Beispielszenario u.a Entitäten „Clientsystem“ für „PS Server“,
9292 „Arbeitsplatz“ für „Arbeitsplatz 1“ und Arbeitsplatz 2“, „Kartenterminal“ und
9293 „KT-Slot“ für „KT 1“ – „KT 5“, „Mandat“ für die vorgesehene Anzahl von
9294 Mandaten, „SM-B_Verwaltet“ sowie entsprechende Entitätenbeziehungen.
 - 9295 • Anbindung PS Server (ggf. über TLS)
 - 9296 • Pairing der Kartenterminals
 - 9297 • Gesteckte Karten (SMC-B, HBA, eGK)
 - 9298 • Anmeldung Nutzer am „PS Client“

9299 11.6.3 Auswirkungen

- 9300 • An den verschiedenen Arbeitsplätzen können für die definierten Mandaten und
9301 Nutzer Anwendungsfälle der TI initiiert werden.
- 9302 • HBA-Inhaber müssen entsprechen der gewählten HBA-Deployment-Varianten
 - 9303 • ihren HBA zentral stecken und über das Remote-PIN-Verfahren zugreifen
 - 9304 • ihren HBA mit sich führen und lokal in Kartenterminal der Arbeitsplätze stecken

11.7 Szenario 7: Mehrere Mandanten

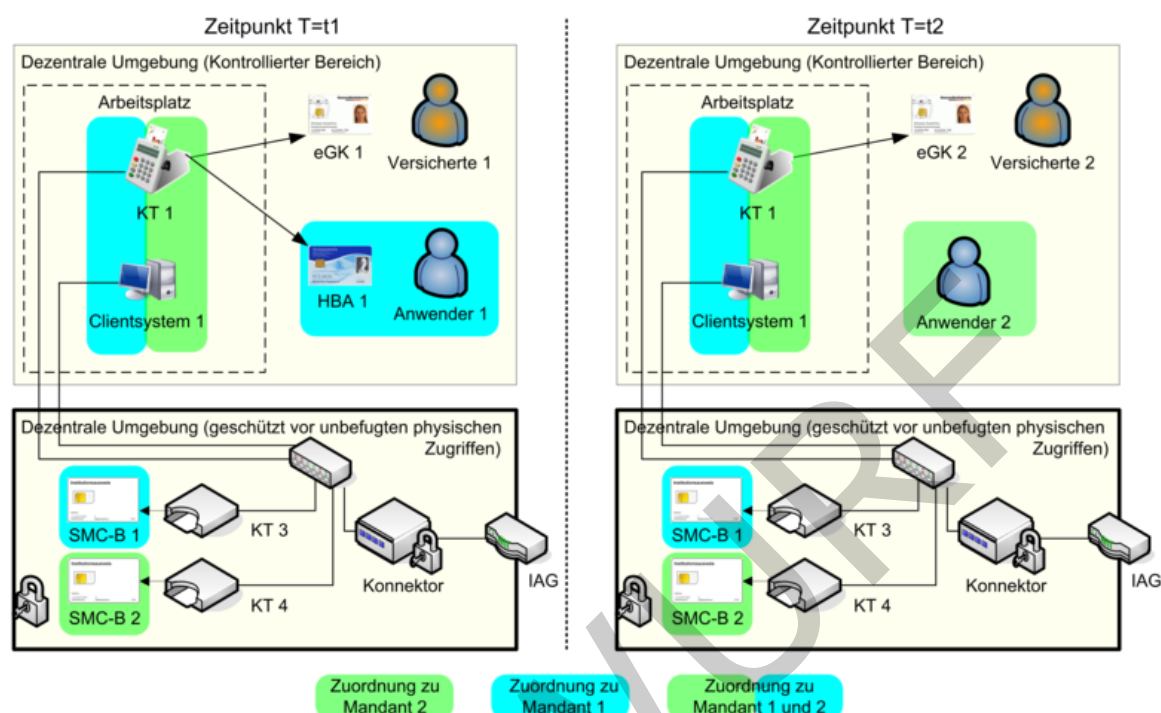


Abbildung 31: Szenario für den Zugriff

11.7.1 Beschreibung des Szenarios

Das Szenario skizziert eine dezentrale Konfiguration, bei der mehrere Mandanten vorhanden sind, wobei jedem Mandant eine eigene SMC-B zugeordnet ist. Die SMC-Bs sind zentral zusammen mit dem Konnektor geschützt vor unbefugten physischen Zugriffen installiert. Die Komponenten Arbeitsplätze, Clientsysteme und Kartenterminals müssen eine Zuordnung zum Mandanten haben, wobei Zuordnungen zu mehreren Mandanten möglich sind. Das Beispiel zeigt einen Arbeitsplatz mit „Clientsystem 1“ und „KT 1“, der zu unterschiedlichen Zeiten durch verschiedene Mandanten verwendet wird. Zum Zeitpunkt T=t1 greift ein Anwender 1 mit HBA 1 über einen Anwendungsfall im Kontext Mandat 1 auf die TI zu, wobei der Versicherte 1 mit eGK 1 am Anwendungsfall beteiligt ist. Zum Zeitpunkt T=t2 wird ein anderer Anwendungsfall im Kontext von Mandat 2 durch einen Anwender 2 ohne HBA initiiert, wobei der Versicherte 2 mit eGK 2 am Anwendungsfall beteiligt ist. Das Clientsystem stellt hierbei den Mandantenbezug sowie die Nutzer Authentisierung sicher. Als Variante können auch mehrere Mandanten eine Zuordnung zu einer einzelnen SMC-B haben. Weiterhin können auch in diesem Szenario HBAs zentral gesteckt werden.

11.7.2 Voraussetzungen

- Netzerkennung aller Komponenten (u. a. KT, Clientsystem, Konnektor) in der dezentralen Umgebung bis einschließlich zur Netzwerkschicht (IP-Ebene)

- 9329 • Konfiguration der Clientsysteme („Clientsystem 1“), passend zum
- 9330 Informationsmodell des Konnektors (herstellerspezifisch).
- 9331 • Konfiguration des Konnektors. U. a.:
- 9332 • Konfiguration Konnektor:
- 9333 Beim Beispielszenario u.a Entitäten „Clientsystem“ für „Clientsystem 1“,
- 9334 „Arbeitsplatz“ für „Arbeitsplatz 1“, „Kartenterminal“ und „KT-Slot“ für „KT 1“ –
- 9335 „KT 4“, „Mandat“ für „Mandant 1“ und „Mandant 2“, „SM-B_Verwaltet“ für
- 9336 „SMC-B 1“ und SMC-B 2“ sowie entsprechende Entitätenbeziehungen
- 9337 • Anbindung „Clientsystem 1“ (ggf. über TLS)
- 9338 • Pairing der Kartenterminals
- 9339 • Gesteckte Karten (SMC-B 1, SMC-B 2, HBA 1, eGK 1, eGK 2)
- 9340 • Anmeldung eines Anwenders mit Mandantenbezug am Clientsystem

9341 **11.7.3 Auswirkungen**

- 9342 • An den verschiedenen Arbeitsplätzen können für die definierten Mandaten und
- 9343 Anwender Anwendungsfälle der TI initiiert werden.
- 9344 • HBA-Inhaber müssen entsprechen der gewählten HBA-Deployment-Varianten
- 9345 • ihren HBA zentral stecken und über das Remote-PIN-Verfahren zugreifen
- 9346 • ihren HBA mit sich führen und lokal in Kartenterminal der Arbeitsplätze stecken

11.8 Szenario 9: Standalone Konnektor - Physische Trennung

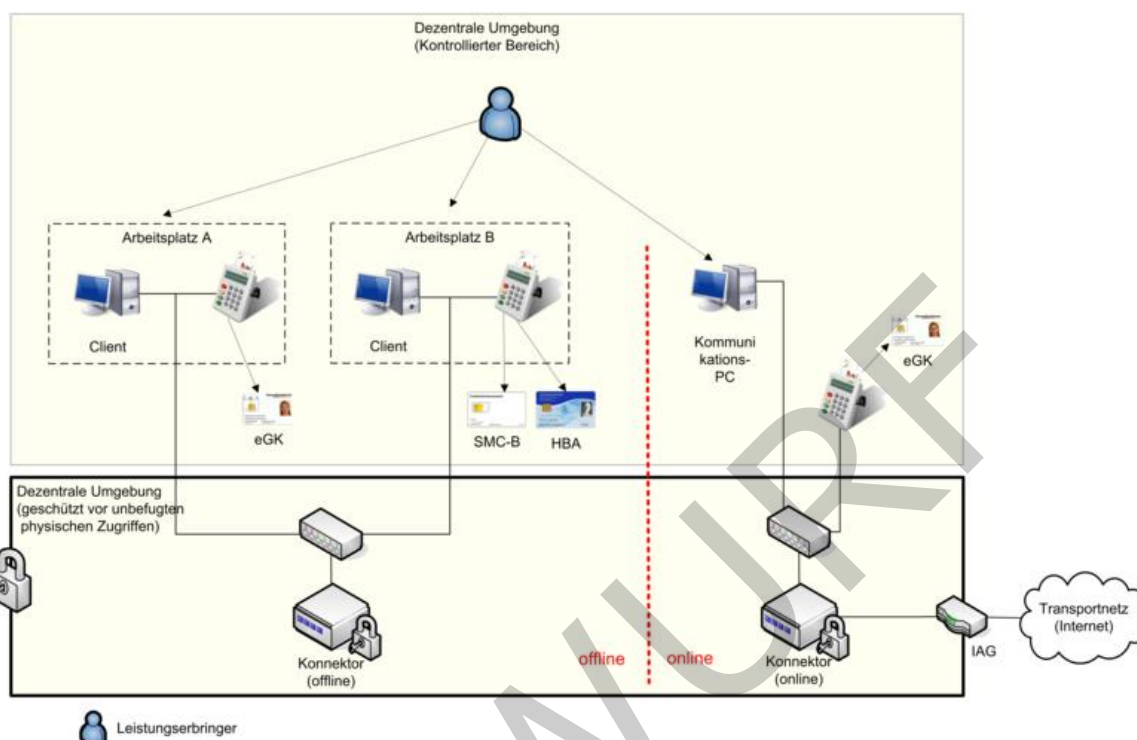


Abbildung 32: Standalone-Szenario mit physischer Trennung im Konnektor

11.8.1 Beschreibung des Szenarios

Dieses Szenario stellt eine Variante des Standalone-Szenarios dar, bei dem eine physische Trennung der Konnektoren eingesetzt wurde.

Im Standalone-Szenario besteht eine Trennung zwischen den Praxissystemen der dezentralen Umgebung, welche offline (also, ohne Anbindung an die zentrale TI-Plattform) betrieben werden und den für das Update der eGK durch die Fachanwendung VSDM notwendigen Komponenten, welche online (also, mit Verbindung in die zentrale TI-Plattform) betrieben werden.

Die physische Trennung im Standalone-Szenario zeichnet sich dadurch aus, dass getrennte Komponenten zum Einsatz kommen. Der Online-Konnektor ist mit der zentralen TI-Plattform verbunden und ermöglicht das VSDM Update der eGKs. Ein am Online-Konnektor angebundener Kommunikations-PC kann darüber hinaus über den sicheren Internetzugang der TI auf das Internet und über den VPN-Konzentrator TI auf Bestandsnetze zugreifen.

Sollten die Online-/Offline-Systeme nicht netztechnisch voneinander getrennt sein, so obliegt es dem Administrator der Praxissysteme sicherzustellen, dass die netztechnische Verbindung keine Gefährdung für die Praxissysteme zur Folge hat.

Im Offline-Konnektor sind einzelne Funktionen nicht verfügbar, andere haben einen eingeschränkten Funktionsumfang. So kann z.B. eine QES erzeugt oder geprüft aber dabei keine aktuelle Statusauskunft (OCSP-Response) für die eingesetzten Zertifikate eingeholt werden. Dies hat zur Folge, dass bei Erzeugung einer QES keine Statusauskunft

- 9373 für das Signaturzertifikat in die Signatur eingebettet werden kann und bei einer Prüfung
9374 der QES nur eine eventuell in die Signatur eingebettet Statusauskunft des Zertifikats
9375 berücksichtigt werden kann.
- 9376 Der Nutzer muss in diesem Fall selber entscheiden ob der gebotene Funktionsumfang für
9377 seinen Anwendungsfall ausreichend ist.

9378 **11.8.2 Voraussetzungen**

- 9379 Folgende zusätzliche Punkte müssen erfüllt sein, um dieses Szenario umzusetzen:
- 9380 • Konfiguration im Konnektor: Es muss konfiguriert werden, welche Komponenten
9381 von welchem Konnektor (online/offline) verwendet werden dürfen.
 - 9382 • Ein eHealth-Kartenterminal oder ein Arbeitsplatz darf immer nur mit einem der
9383 Konnektoren verbunden sein.
 - 9384 • Konfiguration im Konnektor: Im Offline-Konnektor wird kein VPN-Kanal
9385 konfiguriert.
 - 9386 • Clients bzw. Kommunikations-PC müssen sicherstellen, dass sie nur den jeweils
9387 richtigen Konnektor ansprechen.
 - 9388 • Es sollte eine netztechnische Trennung des Online- und Offline-Segmentes
9389 erfolgen. Wird dies nicht umgesetzt, dann obliegt es dem Administrator der
9390 Praxissysteme sicherzustellen, dass die netztechnische Verbindung keine
9391 Gefährdung für die Praxissysteme zur Folge hat.
9392 Sollte keine netztechnische Trennung erfolgen, so kann nur einer der Konnektoren
9393 als DHCP-Server agieren. Es wird empfohlen hier den Offline-Konnektor zu
9394 verwenden, da dort tendenziell mehr Systeme angeschlossen sind. Die am Online-
9395 Konnektor angeschlossenen Systeme müssen dann direkt konfiguriert werden.

9396 **11.8.3 Auswirkung**

- 9397 • Erhöhter Aufwand durch separate Konnektoren und separate eHealth-
9398 Kartenterminals.
- 9399 • Trennung der Praxissysteme von der zentralen TI-Plattform ist für den
9400 Leistungserbringer nachweislich sichergestellt.
- 9401 • Eingeschränkte Funktionalität der TI für Praxissysteme (nur Offline-Funktionalität)
- 9402 • Notwendige Prüfung des Leistungserbringers, ob eingeschränkte Funktionalität
9403 (insbesondere bei Sicherheitsfunktionen) akzeptabel ist.
- 9404 • Sicherer Internetzugang der TI nur über den Kommunikations-PC nutzbar.
- 9405 • Zugang zu Bestandsnetzen über den VPN-Konzentrator TI nur über den
9406 Kommunikations-PC nutzbar

12 Anhang L – Datentypen von Eingangs- und Ausgangsdaten

Tabelle 394: Aufzähltypen

Typname	Werteliste
[Boolean]	{true false}
[EncryptionType]	{CMS XMLEnc S/MIME}
[EventType]	{Op Sec Perf}
[EventSeverity]	{Debug Info Warn Err Fatal}
[KtOutputMode]	{Input OutputWait OutputConfirm OutputKeep OutputErase}
[PinStatus]	{VERIFIED VERIFYABLE BLOCKED TRANSPORT_PIN EMPTY_PIN DISABLED}
[PinResult]	{OK REJECTED BLOCKED ERROR}
[PukResult]	{OK REJECTED BLOCKED ERROR}
[VerificationResult]	{VALID INVALID INCONCLUSIVE}