

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

Übergreifende Spezifikation Spezifikation PKI

Version: 2.89.0 CC
Revision: 198563230758
Stand: 02.0330.04.2020
Status: zur Abstimmung freigegeben
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemSpec_PKI

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Datum	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
2.0.0	05.10.17		freigegeben	gematik
			Einarbeitung der abgestimmten Änderungen, Einarbeitung der Errata 1.6.4-1, 1.6.4-2 und 1.6.4-3	gematik
2.1.0	18.12.17		Einarbeitung der Änderungen zu OPB1 R1.6.4-0, der abgestimmten Änderungen, Einarbeitung der Errata und die Entfernung von LE-AdV	gematik
2.2.0	14.05.18		Einarbeitung der Änderungen gemäß der Änderungsliste P15.2. und P15.4	gematik
2.3.0	26.10.18		Einarbeitung der Änderungen gemäß der Änderungsliste P15.9	
2.3.1			Einarbeitung P15.11	
2.4.0	18.12.18		Einarbeitung P17.1/ePA	
	21.12.18		redaktionelle Anpassung "Tab_PKI_109 Werte für das Präfix <TSP-ID>"	gematik
	09.01.19		Redaktionelle Korrektur der Anpassung P17.1/ePA in Kap. 5.9.3.3 und 5.9.3.4	gematik
2.5.0	15.05.19		Einarbeitung P18.1	gematik
2.6.0	28.06.19		Einarbeitung P19.1	gematik

2.7.0	02.10.19		Einarbeitung P20.1 und P16.1/2	gematik
2.7.0	02.10.19		freigegeben	gematik
2.8.0	02.03.20		Einarbeitung P21.1	gematik
2.89.0 CC	02.0330.04.20		freigegebenAnpassungen gemäß Änderungsliste P22.1 und Scope- Themen aus Systemdesign R4.0.0	gematik

Inhaltsverzeichnis

1	Einordnung des Dokumentes	17
1.1	Zielsetzung	17
1.2	Zielgruppe	17
1.3	Geltungsbereich	17
1.4	Abgrenzungen	17
1.5	Methodik	18
2	Notation kryptographischer Objekte	19
2.1	Basis-Bezeichner	19
2.2	Optionale Bezeichnung der technischen Ausprägung	19
2.3	Optionales Unterscheidungsmerkmal bei gleicher technischer Ausprägung	19
2.4	Allgemeine Notationsvorschrift	20
2.5	Type (Objekttyp)	20
2.6	Holder (Objektbesitzer)	21
2.7	Usage (Objektverwendung)	23
2.8	n (lfd. Nummer)	24
2.9	Instance (Ausprägung)	25
2.10	Beispiele zur Umsetzung	26
2.10.1	Beispiele für asymmetrische Objekte	26
2.10.2	Beispiele für symmetrische Objekte	27
3	CA-Strukturen	28
3.1	Übergreifende Festlegung für CA der TI	28
3.1.1	Übersicht der Identitäten/Zertifikate	28
3.1.2	Laufzeiten der CA	28
3.1.3	Unterstützung verschiedener Schlüsselgenerationen	28
3.2	TI-Betriebsumgebungen	29
3.2.1	PKI-Sicht auf die Produktivumgebung	30
3.2.2	PKI-Sicht auf Test- u. Referenzumgebung (PKI TeRe)	30
3.2.3	Pseudo-QES PKI in Test- u. Referenzumgebung	31
3.3	Zentrale Aussteller-CAs in der TI für nonQES-Zertifikate	31
3.4	Spezifische Aussteller-CA in der TI	32
4	Kodierung von X.509-Identitäten	34
4.1	Namensregeln und -formate	34
4.1.1	Verarbeitung von Sonderzeichen	34
4.1.2	Definition der Subject-DNs für Personen und Komponenten	34
4.1.3	SubjectDN von CA-Zertifikaten und von OCSP-Responder-Zertifikaten	34

68	4.2 Schlüssel der Versichertenidentität (eGK)	35
69	4.3 Pseudonym der Versichertenidentität (eGK)	35
70	4.3.1 Versicherten-Pseudonym in X.509-Zertifikaten der eGK	35
71	4.3.2 Eindeutigkeit des Pseudonym	36
72	4.3.3 Pseudonym-Erstellungsregel	36
73	4.3.4 Hs-ZW – Herausgeberspezifischer Zufallswert (hs-ZW)	37
74	4.3.5 Kodierung des Pseudonyms	38
75	4.4 Berufsgruppen-ID der Leistungserbringer	39
76	4.4.1 Berufsgruppe des Heilberufers	39
77	4.5 ID der Organisation/Einrichtung des Gesundheitswesens	40
78	4.5.1 Typ und Exemplar der Organisation/Einrichtung des Gesundheitswesens	40
79	4.6 Technische Rolle von Komponenten und Diensten	40
80	4.6.1 Technische Rolle im Komponentenzertifikat	40
81	4.7 Telematik-ID	41
82	4.7.1 Abbildung der Telematik-ID im X.509-Zertifikat	41
83	4.7.2 Aufbau der Telematik-ID	42
84	4.7.2.1 Sektoraler Präfix	42
85	4.7.2.2 Separator	43
86	4.7.2.3 Fortsatz der Telematik-ID	43
87	4.8 Kodierung der Zertifikate	44
88	4.8.1 Kodierung der Attribute	44
89	4.8.2 Stringlänge der Attribute	45
90	4.8.3 Struktur	45
91	4.8.3.1 serialNumber	46
92	4.8.3.2 Admission	46
93	4.8.3.3 CertificatePolicies	48
94	4.8.3.4 CRLDistributionPoints	50
95	4.8.3.5 SubjectAltNames	51
96	4.9 Erläuterungen zu Zertifikatsprofilen	52
97	4.9.1 Allgemeine Erläuterungen	52
98	4.9.2 Berufs-/Rollenattribute und Sperrbarkeit	52
99	4.9.3 Benennung der Zertifikatsprofile	53
100	4.9.4 Distinguished Name	53
101	4.10 Kodierung der Betriebsumgebungen in Zertifikaten	55
102	4.11 Kartenverlust und Deaktivierung von Chipkarten	56
103	5 X.509-Zertifikate	58
104	5.1 eGK – Versichertenkarte	58
105	5.1.1 Definition der Versichertenidentität	58
106	5.1.2 Belegung der Felder im SubjectDN	59
107	5.1.3 X.509-Zertifikatsprofile der eGK	60
108	5.1.3.1 C.CH.AUT und C.CH.AUT_ALT – Authentisierung eGK	60
109	5.1.3.2 C.CH.ENC – Verschlüsselung eGK	62
110	5.1.3.3 C.CH.QES – Qualifizierte Signatur eGK (optional)	64
111	5.1.3.4 C.CH.AUTN – Technische Authentisierung eGK	66
112	5.1.3.5 C.CH.ENCV – Technische Verschlüsselung eGK	67
113	5.2 HBA – Heilberufsausweis	69
114	5.2.1 X.509-Zertifikatsprofile des HBA	69

115	5.2.1.1 C.HP.AUT – Authentisierung HBA	69
116	5.2.1.2 C.HP.ENC – Verschlüsselung HBA	71
117	5.2.1.3 C.HP.QES – Qualifizierte Signatur HBA	73
118	5.3 SMC-B – Ausweis einer Organisation/Einrichtung des Gesundheitswesens	77
119	5.3.1 Definition der Organisationsidentität	77
120	5.3.2 Aufbau Anschriftzone nach [DIN5008]	78
121	5.3.3 Umgang mit überlangen Attributen im SubjectDN	79
122	5.3.4 X.509 Zertifikatsprofile der SMC-B	79
123	5.3.4.1 C.HCI.AUT – Authentisierung SMC-B	79
124	5.3.4.2 C.HCI.ENC – Verschlüsselung SMC-B	81
125	5.3.4.3 C.HCI.OSIG – Signatur SMC-B	83
126	5.4 HSM-B – Ausweis einer Organisation/Einrichtung des Gesundheitswesens	85
127	5.5 gSMC-KT – eHealth Kartenterminal	85
128	5.5.1 Definition der Kartenterminalidentität	85
129	5.5.2 X.509 Zertifikatsprofile der gSMC-KT	86
130	5.5.2.1 C.SMKT.AUT – Identität der gSMC-KT	86
131	5.6 gSMC-K – Konnektor	87
132	5.6.1 Definition und Zuweisung der Konnektoridentität	87
133	5.6.2 Aufbau des SubjectDN	88
134	5.6.3 Statusprüfung von Konnektorzertifikaten	88
135	5.6.4 X.509 Zertifikatsprofile des Konnektors	89
136	5.6.4.1 C.NK.VPN – VPN Authentisierung Netzkonnektor	89
137	5.6.4.2 C.AK.AUT – Authentisierung Anwendungskonnektor	90
138	5.6.4.3 C.SAK.AUT – Authentisierung Signaturdienst	92
139	5.7 VPN-Zugangsdienst	94
140	5.7.1 Definition und Zuweisung der Zugangsdienstidentitäten	94
141	5.7.2 Aufbau des SubjectDN	95
142	5.7.3 X.509 Zertifikatsprofile des Zugangsdienstes	95
143	5.7.3.1 C.VPNK.VPN – VPN Authentisierung Zugangsdienst TI	95
144	5.7.3.2 C.VPNK.VPN-SIS – VPN Authentisierung Zugangsdienst Sicherer Internetzugang	96
145	5.8 ZD – Zentrale Dienste	98
146	5.8.1 Definition der Identität der Zentralen Dienste	98
147	5.8.2 Aufbau des SubjectDN	98
148	5.8.3 X.509 Zertifikatsprofile der Zentralen Dienste	99
149	5.8.3.1 C.ZD.TLS-S Server Authentisierung (chemals C.SF.SSL-S)	99
150	5.9 FD – Fachanwendungsspezifische Dienste	100
151	5.9.1 Definition der Identität der Fachanwendungsspezifischen Dienste	100
152	5.9.2 Aufbau des SubjectDN	101
153	5.9.3 X.509 Zertifikatsprofile der Fachanwendungsspezifischen Dienste	101
154	5.9.3.1 C.FD.TLS-C Client Authentisierung (chemals C.SF.SSL-C)	101
155	5.9.3.2 C.FD.TLS-S Server Authentisierung (chemals C.SF.SSL-S)	103
156	5.9.3.3 C.FD.SIG Signatur Fachdienst	104
157	5.9.3.4 C.FD.AUT Authentisierung Fachdienst	106
158	5.9.3.5 C.FD.ENC Verschlüsselung Fachdienst	108
159	5.10 CM – Clientmodul	109
160	5.10.1 Definition der Identität eines Clientmoduls	109
161	5.10.2 Aufbau des SubjectDN	110

165	5.10.3 X.509 Zertifikatsprofil des Clientmoduls	110
166	5.10.3.1 C.CM.TLS-CS Clientmodul Authentisierung	110
167	5.11 SGD-HSM – Schlüsselerzeugungsdienst-HSM	112
168	5.11.1 Beschreibung der Identität	112
169	5.11.2 X.509 Zertifikatsprofil der SGD-HSM	112
170	5.12 CA – Zertifikatsprofile	114
171	5.12.1 GEM.RCA<n> – Zentrale Root CA_nonQES	114
172	5.12.2 <tsp>. <usage> CA<n> – Aussteller CA_nonQES	116
173	5.12.3 <tsp>.HBA-qCA<n> – Aussteller CA_QES	118
174	5.13 OCSP – Statusauskunftsdienst	120
175	5.13.1 Definition der OCSP-Signer-Identität	120
176	5.13.2 Aufbau des SubjectDN	120
177	5.13.3 X.509-Profil des OCSP-Signer-Zertifikates	120
178	5.13.3.1 C.GEM.OCSP-OCSP-Signer-Zertifikat	120
179	5.14 CRL – Statusauskunftsdienst	122
180	5.14.1 Definition der CRL-Signer-Identität	122
181	5.14.2 Aufbau des SubjectDN	123
182	5.14.3 X.509-Profil des CRL-Signer-Zertifikates	123
183	5.14.3.1 C.GEM.CRL-CRL-Signaturzertifikat	123
184	5.15 TSL – Zertifikatsprofile	124
185	5.15.1 Definition der TSL-Signer-Identität	124
186	5.15.2 Aufbau des SubjectDN	125
187	5.15.3 X.509-Zertifikatsprofil der TSL-Signer-CA	125
188	5.15.4 TSL-Signer-Zertifikat	126
189	5.15.5 TSL-OCSP-Responder-Zertifikat	127
190	6 CV-Zertifikate	128
191	6.1 Festlegungen zur Abgrenzung	128
192	6.2 Namensregeln und -formate	128
193	6.3 Rollen und Profile	129
194	6.3.1 Rollenauthentisierung	129
195	6.3.2 Authentisierung einer Funktionseinheit	137
196	6.4 CV-Zertifikatsprofile der Generation 2	138
197	6.4.1 Berechtigung einer CVC-CA zur Zertifikatserstellung	138
198	6.4.2 Aufbau und Bestandteile der CV-Zertifikate der Generation 2	139
199	6.4.3 Zertifikatsprofil eines CV-Zertifikates für ELC-Schlüssel	140
200	6.4.3.1 Certificate Profile Identifier (CPI)	140
201	6.4.3.2 Certification Authority Reference (CAR)	140
202	6.4.3.3 Öffentlicher Schlüssel	141
203	6.4.3.4 Certificate Holder Reference (CHR)	142
204	6.4.3.5 Certificate Holder Authorization Template (CHAT)	144
205	6.4.3.6 Certificate Effective Date (CED)	145
206	6.4.3.7 Certificate Expiration Date (CXD)	145
207	6.4.3.8 Zu signierende Nachricht M eines CV-Zertifikates der Generation 2	146
208	6.4.4 Struktur und Inhalt eines CV-Zertifikates für ELC-Schlüssel der Generation 2	146
209	146
210	6.4.5 Struktur und Inhalt eines CV-Zertifikates für ELC-Schlüssel der Generation 2	147
211	147
212	6.4.5.1 Struktur und Inhalt von CA-CV-Zertifikaten für ELC-Schlüssel	148

213	6.4.5.2 Struktur und Inhalt von Cross-CV-Zertifikaten für ELC-Schlüssel.....	150
214	6.4.5.3 Struktur und Inhalt von Endnutzer-CV-Zertifikaten für ELC-Schlüssel...	151
215	6.4.6 Flagliste mit Berechtigungen in CV-Zertifikaten für ELC-Schlüssel.....	153
216	7 Festlegung von OIDs.....	159
217	8 Prüfung von Zertifikaten.....	160
218	8.1 Vertrauensraum der TI.....	162
219	8.1.1 TSL im Kontext der ECC Migration.....	164
220	8.1.2 Initialisierung TI-Vertrauensraum.....	164
221	8.1.2.1 TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“.....	168
222	8.1.3 Geplanter Wechsel TI-Vertrauensanker.....	174
223	8.1.3.1 TUC_PKI_013 „Import TI-Vertrauensanker aus TSL“.....	174
224	8.1.3.2 TSL-Einträge für die Bereitstellung neuer TI-Vertrauensanker.....	177
225	8.1.3.3 Prüfung der TSL nach Wechsel des TI-Vertrauensanker.....	179
226	8.1.4 Ungeplanter Wechsel des TI-Vertrauensanker.....	180
227	8.2 TSL-Prüfung.....	180
228	8.2.1 Erreichbarkeit und Download der TSL.....	180
229	8.2.1.1 TUC_PKI_017 „Lokalisierung TSL-Download-Adressen“.....	180
230	8.2.1.2 TUC_PKI_016 „Download der TSL-Datei“.....	182
231	8.2.2 Vertrauensstatus und Authentifizieren der TSL.....	185
232	8.2.2.1 TUC_PKI_019 „Prüfung der Aktualität der TSL“.....	185
233	8.2.2.2 TUC_PKI_020 „XML-Dokument validieren“.....	193
234	8.2.2.3 TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“.....	194
235	8.2.2.4 TUC_PKI_012 „XML-Signatur-Prüfung“.....	197
236	8.2.3 TSL-Sicherheitsaspekte.....	198
237	8.2.4 TSL-Zeitparameter.....	199
238	8.2.5 ServiceTypeIdentifier "unspecified".....	199
239	8.3 Zertifikatsprüfung X.509-nonQES.....	200
240	8.3.1 Zertifikatsprüfung in der TI.....	201
241	8.3.1.1 TUC_PKI_018 „Zertifikatsprüfung in der TI“.....	201
242	8.3.1.2 TUC_PKI_002 „Gültigkeitsprüfung des Zertifikats“.....	208
243	8.3.1.3 TUC_PKI_003 „CA-Zertifikat in TSL-Informationen finden“.....	210
244	8.3.1.4 TUC_PKI_004 „Mathematische Prüfung der Zertifikatssignatur“.....	213
245	8.3.2 Statusprüfung.....	216
246	8.3.2.1 TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln“.....	216
247	8.3.2.2 TUC_PKI_006 „OCSP-Abfrage“.....	218
248	8.3.2.3 TUC_PKI_021 „CRL-Prüfung“.....	226
249	8.3.2.4 Szenarien für Offline- und Timeout von OCSP.....	232
250	8.3.2.5 Statusprüfung von eGK-Zertifikaten.....	232
251	8.3.3 Ermittlung von Autorisierungsinformationen.....	232
252	8.3.3.1 Bestätigte Zertifikatsinformationen.....	232
253	8.3.3.2 TUC_PKI_009 „Rollenermittlung“.....	232
254	8.3.3.3 TUC_PKI_007 „Prüfung Zertifikatstyp“.....	236
255	8.3.4 Weitere Prüfungen.....	241
256	8.3.4.1 Umgang mit kritischen Extensions.....	241
257	8.4 Überprüfung der Zertifikate auf Netzwerk- und Transportebene.....	241
258	8.4.1 TLS-Verbindungsaufbau.....	241
259	8.4.2 IPsec-Verbindungsaufbau.....	242
260	8.5 Zertifikatsprüfung X.509-QES.....	242
261	8.5.1 TUC_PKI_030 „QES-Zertifikatsprüfung“.....	243

262	8.5.2 TUC_PKI_036 „BNetzA-VL Aktualisierung“	252
263	8.6 Fehlercodes bei TLS- und Zertifikatsprüfung X.509	256
264	8.7 Zertifikatsprüfung CV-Zertifikate der 2. Generation	264
265	9 OCSP-Statusinformation	267
266	9.1 Statusprüfung	267
267	9.1.1 Schnittstelle I-OCSP-Status-Information	267
268	9.1.1.1 Schnittstellendefinition	268
269	9.1.1.1.1 OCSP-Request	269
270	9.1.1.1.2 OCSP-Response	270
271	9.1.1.2 Umsetzung	271
272	9.1.1.3 Nutzung	271
273	9.1.2 Artefakte	272
274	9.1.2.1 OCSP-Response-Response-Status	272
275	9.1.2.2 OCSP-Response-Zeiten	272
276	9.1.2.3 OCSP-Response-CertStatus	273
277	9.1.2.4 OCSP-Response-CertID	274
278	9.1.2.5 OCSP-Response-Sperrzeitpunkt und Sperrgrund	274
279	9.1.2.6 OCSP-Response-CertHash	274
280	9.1.3 Testunterstützung	275
281	9.1.4 Hardwaremerkmale	275
282	10 Anhang A – Sektorspezifische Ausprägungen der SMC-B-	
283	Zertifikate	276
284	10.1 KZBV	276
285	10.2 KBV	278
286	10.3 DKG	280
287	10.4 GKV-Spitzenverband	282
288	10.5 Apothekerschaft	285
289	10.6 AdV-Umgebung im Auftrag der Kostenträger	287
290	10.7 SMC-B-ORG	289
291	11 Anhang B – Verzeichnisse	297
292	11.1 Abkürzungen	297
293	11.2 Glossar	302
294	11.3 Abbildungsverzeichnis	302
295	11.4 Tabellenverzeichnis	304
296	11.5 Referenzierte Dokumente	312
297	11.5.1 Dokumente der gematik	312
298	11.5.2 Weitere Dokumente	313
299	12 Anhang C – Sektorspezifische Ausprägungen der HBA	
300	Zertifikate	317
301	12.1 BÄK	317

302	12.2 BZÄK.....	319
303	12.3 BPtK.....	321
304	12.4 Apothekerschaft.....	323
305	1 Einordnung des Dokumentes	17
306	1.1 Zielsetzung	17
307	1.2 Zielgruppe	17
308	1.3 Geltungsbereich	17
309	1.4 Abgrenzungen	17
310	1.5 Methodik	18
311	1.5.1 Hinweis auf offene Punkte	18
312	2 Notation kryptographischer Objekte.....	19
313	2.1 Basis-Bezeichner	19
314	2.2 Optionale Bezeichnung der technischen Ausprägung	19
315	2.3 Optionales Unterscheidungsmerkmal bei gleicher technischer Ausprägung	19
316	2.4 Allgemeine Notationsvorschrift	20
317	2.5 Type (Objekttyp)	20
318	2.6 Holder (Objektbesitzer).....	21
319	2.7 Usage (Objektverwendung).....	23
320	2.8 n (lfd. Nummer)	24
321	2.9 Instance (Ausprägung)	25
322	2.10 Beispiele zur Umsetzung	26
323	2.10.1 Beispiele für asymmetrische Objekte	26
324	2.10.2 Beispiele für symmetrische Objekte	27
325		
326	3 CA-Strukturen	28
327	3.1 Übergreifende Festlegung für CA der TI	28
328	3.1.1 Übersicht der Identitäten/Zertifikate	28
329	3.1.2 Laufzeiten der CA.....	28
330	3.1.3 Unterstützung verschiedener Schlüsselgenerationen.....	28
331	3.2 TI-Betriebsumgebungen.....	29
332	3.2.1 PKI-Sicht auf die Produktivumgebung	30
333	3.2.2 PKI-Sicht auf Test- u. Referenzumgebung (PKI-TeRe)	30
334	3.2.3 Pseudo-QES PKI in Test- u. Referenzumgebung	31
335	3.3 Zentrale Aussteller-CAs in der TI für nonQES-Zertifikate.....	31
336	3.4 Spezifische Aussteller-CA in der TI.....	32
337	4 Kodierung von X.509-Identitäten	34
338	4.1 Namensregeln und -formate.....	34
339	4.1.1 Verarbeitung von Sonderzeichen	34

340	4.1.2 Definition der Subject-DNs für Personen und Komponenten.....	34
341	4.1.3 SubjectDN von CA-Zertifikaten und von OCSP-Responder-Zertifikaten	34
342	4.2 Schlüssel der Versichertenidentität (eGK)	35
343	4.3 Pseudonym der Versichertenidentität (eGK)	35
344	4.3.1 Versicherten-Pseudonym in X.509-Zertifikaten der eGK	35
345	4.3.2 Eindeutigkeit des Pseudonym.....	36
346	4.3.3 Pseudonym-Erstellungsregel	36
347	4.3.4 Hs-ZW – Herausgeberspezifischer Zufallswert (hs-ZW)	37
348	4.3.5 Kodierung des Pseudonyms	38
349	4.4 Berufsgruppen-ID der Leistungserbringer	39
350	4.4.1 Berufsgruppe des Heilberufers.....	39
351	4.5 ID der Organisation/Einrichtung des Gesundheitswesens.....	40
352	4.5.1 Typ und Exemplar der Organisation/Einrichtung des Gesundheitswesens.....	40
353	4.6 Technische Rolle von Komponenten und Diensten.....	40
354	4.6.1 Technische Rolle im Komponentenzertifikat.....	40
355	4.7 Telematik-ID	41
356	4.7.1 Abbildung der Telematik-ID im X.509-Zertifikat.....	41
357	4.7.2 Aufbau der Telematik-ID	42
358	4.7.2.1 Sektoraler Präfix	42
359	4.7.2.2 Separator.....	43
360	4.7.2.3 Fortsatz der Telematik-ID.....	43
361	4.8 Kodierung der Zertifikate	44
362	4.8.1 Kodierung der Attribute	44
363	4.8.2 Stringlänge der Attribute.....	45
364	4.8.3 Struktur.....	45
365	4.8.3.1 serialNumber.....	46
366	4.8.3.2 Admission	46
367	4.8.3.3 CertificatePolicies	48
368	4.8.3.4 CRLDistributionPoints.....	50
369	4.8.3.5 SubjectAltNames.....	51
370	4.9 Erläuterungen zu Zertifikatsprofilen	52
371	4.9.1 Allgemeine Erläuterungen	52
372	4.9.2 Berufs-/Rollenattribute und Sperrbarkeit	52
373	4.9.3 Benennung der Zertifikatsprofile	53
374	4.9.4 Distinguished Name.....	53
375	4.10 Kodierung der Betriebsumgebungen in Zertifikaten	55
376	4.11 Kartenverlust und Deaktivierung von Chipkarten	56
377	5 X.509-Zertifikate	58
378	5.1 eGK – Versichertenkarte.....	58
379	5.1.1 Definition der Versichertenidentität.....	58
380	5.1.2 Belegung der Felder im SubjectDN	59
381	5.1.3 X.509-Zertifikatsprofile der eGK	60
382	5.1.3.1 C.CH.AUT und C.CH.AUT_ALT – Authentisierung eGK.....	60
383	5.1.3.2 C.CH.ENC – Verschlüsselung eGK	62
384	5.1.3.3 C.CH.QES – Qualifizierte Signatur eGK (optional).....	64
385	5.1.3.4 C.CH.AUTN – Technische Authentisierung eGK	66
386	5.1.3.5 C.CH.ENCV – Technische Verschlüsselung eGK.....	67

5.2 HBA – Heilberufsausweis	69
5.2.1 X.509 Zertifikatsprofile des HBA	69
5.2.1.1 C.HP.AUT – Authentisierung HBA	69
5.2.1.2 C.HP.ENC – Verschlüsselung HBA	71
5.2.1.3 C.HP.QES – Qualifizierte Signatur HBA	73
5.3 SMC-B – Ausweis einer Organisation/Einrichtung des Gesundheitswesens	77
5.3.1 Definition der Organisationsidentität	77
5.3.2 Aufbau Anschriftzone nach [DIN5008]	78
5.3.3 Umgang mit überlangen Attributen im SubjectDN	79
5.3.4 X.509 Zertifikatsprofile der SMC-B	79
5.3.4.1 C.HCI.AUT – Authentisierung SMC- B	79
5.3.4.2 C.HCI.ENC – Verschlüsselung SMC-B	81
5.3.4.3 C.HCI.SIG – Signatur SMC-B	83
5.4 HSM-B – Ausweis einer Organisation/Einrichtung des Gesundheitswesens	85
5.5 gSMC-KT – eHealth-Kartenterminal	85
5.5.1 Definition der Kartenterminalidentität	85
5.5.2 X.509 Zertifikatsprofile der gSMC-KT	86
5.5.2.1 C.SMKT.AUT – Identität der gSMC-KT	86
5.6 gSMC-K – Konnektor	87
5.6.1 Definition und Zuweisung der Konnektoridentität	87
5.6.2 Aufbau des SubjectDN	88
5.6.3 Statusprüfung von Konnektorzertifikaten	88
5.6.4 X.509 Zertifikatsprofile des Konnektors	89
5.6.4.1 C.NK.VPN – VPN-Authentisierung Netzkonnektor	89
5.6.4.2 C.AK.AUT – Authentisierung Anwendungskonnektor	90
5.6.4.3 C.SAK.AUT – Authentisierung Signaturdienst	92
5.7 VPN-Zugangsdienst	94
5.7.1 Definition und Zuweisung der Zugangsdienstidentitäten	94
5.7.2 Aufbau des SubjectDN	95
5.7.3 X.509-Zertifikatsprofile des Zugangsdienstes	95
5.7.3.1 C.VPNK.VPN – VPN-Authentisierung Zugangsdienst TI	95
5.7.3.2 C.VPNK.VPN-SIS – VPN-Authentisierung Zugangsdienst Sicherer Internetzugang	96
5.8 ZD – Zentrale Dienste	98
5.8.1 Definition der Identität der Zentralen Dienste	98
5.8.2 Aufbau des SubjectDN	98
5.8.3 X.509 Zertifikatsprofile der Zentralen Dienste	99
5.8.3.1 C.ZD.TLS-S Server-Authentisierung (ehemals C.SF.SSL-S)	99
5.9 FD – Fachanwendungsspezifische Dienste	100
5.9.1 Definition der Identität der Fachanwendungsspezifischen Dienste	100
5.9.2 Aufbau des SubjectDN	101
5.9.3 X.509 Zertifikatsprofile der Fachanwendungsspezifischen Dienste	101
5.9.3.1 C.FD.TLS-C Client-Authentisierung (ehemals C.SF.SSL-C)	101
5.9.3.2 C.FD.TLS-S Server-Authentisierung (ehemals C.SF.SSL-S)	103
5.9.3.3 C.FD.SIG Signatur Fachdienst	104
5.9.3.4 C.FD.AUT Authentisierung Fachdienst	106
5.9.3.5 C.FD.ENC Verschlüsselung Fachdienst	108
5.10 CM – Clientmodul	109

437	5.10.1 Definition der Identität eines Clientmoduls	109
438	5.10.2 Aufbau des SubjectDN	110
439	5.10.3 X.509 Zertifikatsprofil des Clientmoduls	110
440	5.10.3.1 C.CM.TLS-CS Clientmodul-Authentisierung	110
441	5.11 SGD-HSM – Schlüsselgenerierungsdienst-HSM	112
442	5.11.1 Beschreibung der Identität	112
443	5.11.2 X.509 Zertifikatsprofil der SGD-HSM	112
444	5.12 CA - Zertifikatsprofile	114
445	5.12.1 GEM.RCA<n> - Zentrale Root-CA_nonQES	114
446	5.12.2 <tsp>.<usage>-CA<n> - Aussteller-CA_nonQES	116
447	5.12.3 <tsp>.HBA-qCA<n> - Aussteller-CA_QES	118
448	5.13 OCSP – Statusauskunftsdienst	120
449	5.13.1 Definition der OCSP-Signer-Identität	120
450	5.13.2 Aufbau des SubjectDN	120
451	5.13.3 X.509-Profil des OCSP-Signer-Zertifikates	120
452	5.13.3.1 C.GEM.OCSP OCSP-Signer-Zertifikat	120
453	5.14 CRL – Statusauskunftsdienst	122
454	5.14.1 Definition der CRL-Signer-Identität	122
455	5.14.2 Aufbau des SubjectDN	123
456	5.14.3 X.509 Profil des CRL-Signer-Zertifikates	123
457	5.14.3.1 C.GEM.CRL CRL-Signaturzertifikat	123
458	5.15 TSL - Zertifikatsprofile	124
459	5.15.1 Definition der TSL-Signer-Identität	124
460	5.15.2 Aufbau des SubjectDN	125
461	5.15.3 X.509 Zertifikatsprofil der TSL-Signer-CA	125
462	5.15.4 TSL-Signer- Zertifikat	126
463	5.15.5 TSL-OCSP-Responder-Zertifikat	127
464	6 CV-Zertifikate	128
465	6.1 Festlegungen zur Abgrenzung	128
466	6.2 Namensregeln und -formate	128
467	6.3 Rollen und Profile	129
468	6.3.1 Rollenauthentisierung	129
469	6.3.2 Authentisierung einer Funktionseinheit	137
470	6.4 CV-Zertifikatsprofile der Generation 2	138
471	6.4.1 Berechtigung einer CVC-CA zur Zertifikatserstellung	138
472	6.4.2 Aufbau und Bestandteile der CV-Zertifikate der Generation 2	139
473	6.4.3 Zertifikatsprofil eines CV-Zertifikates für ELC-Schlüssel	140
474	6.4.3.1 Certificate Profile Identifier (CPI)	140
475	6.4.3.2 Certification Authority Reference (CAR)	140
476	6.4.3.3 Öffentlicher Schlüssel	141
477	6.4.3.4 Certificate Holder Reference (CHR)	142
478	6.4.3.5 Certificate Holder Authorization Template (CHAT)	144
479	6.4.3.6 Certificate Effective Date (CED)	145
480	6.4.3.7 Certificate Expiration Date (CXD)	145
481	6.4.3.8 Zu signierende Nachricht M eines CV-Zertifikates der Generation 2	146
482	6.4.4 Struktur und Inhalt eines CV-Zertifikates für ELC-Schlüssel der Generation 2	146
483	146

484	6.4.5 Struktur und Inhalt eines CV-Zertifikates für ELC-Schlüssel der Generation 2	
485	147
486	6.4.5.1 Struktur und Inhalt von CA CV-Zertifikaten für ELC-Schlüssel	148
487	6.4.5.2 Struktur und Inhalt von Cross-CV-Zertifikaten für ELC-Schlüssel	150
488	6.4.5.3 Struktur und Inhalt von Endnutzer-CV-Zertifikaten für ELC-Schlüssel...	151
489	6.4.6 Flagliste mit Berechtigungen in CV-Zertifikaten für ELC-Schlüssel.....	153
490	7 Festlegung von OIDs.....	159
491	8 Prüfung von Zertifikaten.....	160
492	8.1 Vertrauensraum der TI.....	162
493	8.1.1 TSL im Kontext der ECC-Migration	164
494	8.1.2 Initialisierung TI-Vertrauensraum	164
495	8.1.2.1 TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“.....	168
496	8.1.3 Geplanter Wechsel TI-Vertrauensanker	174
497	8.1.3.1 TUC_PKI_013 „Import TI-Vertrauensanker aus TSL“.....	174
498	8.1.3.2 TSL-Einträge für die Bereitstellung neuer TI-Vertrauensanker	177
499	8.1.3.3 Prüfung der TSL nach Wechsel des TI-Vertrauensanker.....	179
500	8.1.4 Ungeplanter Wechsel des TI-Vertrauensanker	180
501	8.2 TSL-Prüfung	180
502	8.2.1 Erreichbarkeit und Download der TSL.....	180
503	8.2.1.1 TUC_PKI_017 „Lokalisierung TSL Download-Adressen“	180
504	8.2.1.2 TUC_PKI_016 „Download der TSL-Datei“	182
505	8.2.2 Vertrauensstatus und Authentifizieren der TSL	185
506	8.2.2.1 TUC_PKI_019 „Prüfung der Aktualität der TSL“	185
507	8.2.2.2 TUC_PKI_020 „XML-Dokument validieren“	193
508	8.2.2.3 TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“	194
509	8.2.2.4 TUC_PKI_012 „XML-Signatur-Prüfung“	197
510	8.2.3 TSL-Sicherheitsaspekte.....	198
511	8.2.4 TSL-Zeitparameter	199
512	8.2.5 ServiceTypeIdentifier "unspecified"	199
513	8.3 Zertifikatsprüfung X.509 nonQES	200
514	8.3.1 Zertifikatsprüfung in der TI.....	201
515	8.3.1.1 TUC_PKI_018 „Zertifikatsprüfung in der TI“	201
516	8.3.1.2 TUC_PKI_002 „Gültigkeitsprüfung des Zertifikats“.....	208
517	8.3.1.3 TUC_PKI_003 „CA-Zertifikat in TSL-Informationen finden“.....	210
518	8.3.1.4 TUC_PKI_004 „Mathematische Prüfung der Zertifikatssignatur“	213
519	8.3.2 Statusprüfung	216
520	8.3.2.1 TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln“	216
521	8.3.2.2 TUC_PKI_006 „OCSP-Abfrage“	218
522	8.3.2.3 TUC_PKI_021 „CRL-Prüfung“.....	226
523	8.3.2.4 Szenarien für Offline und Timeout von OCSP	232
524	8.3.2.5 Statusprüfung von eGK-Zertifikaten	232
525	8.3.3 Ermittlung von Autorisierungsinformationen	232
526	8.3.3.1 Bestätigte Zertifikatsinformationen	232
527	8.3.3.2 TUC_PKI_009 „Rollenermittlung“	232
528	8.3.3.3 TUC_PKI_007 „Prüfung Zertifikatstyp“.....	236
529	8.3.4 Weitere Prüfungen	241
530	8.3.4.1 Umgang mit kritischen Extensions	241
531	8.4 Überprüfung der Zertifikate auf Netzwerk- und Transportebene	241
532	8.4.1 TLS-Verbindungsaufbau	241

533	8.4.2 IPsec-Verbindungsaufbau	242
534	8.5 Zertifikatsprüfung X.509 QES	242
535	8.5.1 TUC_PKI_030 „QES-Zertifikatsprüfung“	243
536	8.5.2 TUC_PKI_036 „BNetzA-VL Aktualisierung“	252
537	8.6 Fehlercodes bei TSL- und Zertifikatsprüfung X.509	256
538	8.7 Zertifikatsprüfung CV-Zertifikate der 2. Generation	264
539	9 OCSP-Statusinformation	267
540	9.1 Statusprüfung	267
541	9.1.1 Schnittstelle I_OCSP_Status_Information	267
542	9.1.1.1 Schnittstellendefinition	268
543	9.1.1.1.1 OCSP-Request	269
544	9.1.1.1.2 OCSP-Response	270
545	9.1.1.2 Umsetzung	271
546	9.1.1.3 Nutzung	271
547	9.1.2 Artefakte	272
548	9.1.2.1 OCSP-Response – Response Status	272
549	9.1.2.2 OCSP-Response – Zeiten	272
550	9.1.2.3 OCSP-Response – CertStatus	273
551	9.1.2.4 OCSP-Response – CertID	274
552	9.1.2.5 OCSP-Response – Sperrzeitpunkt und Sperrgrund	274
553	9.1.2.6 OCSP-Response – CertHash	274
554	9.1.2.7 OCSP-Response – Responder-Zertifikate	275
555	9.1.3 Testunterstützung	275
556	9.1.4 Hardwaremerkmale	275
557	10 Anhang A – Sektorspezifische Ausprägungen der SMC-B-	
558	Zertifikate	276
559	10.1 KZBV	276
560	10.2 KBV	278
561	10.3 DKG	280
562	10.4 GKV-Spitzenverband	282
563	10.5 Apothekerschaft	285
564	10.6 AdV-Umgebung im Auftrag der Kostenträger	287
565	10.7 SMC-B-ORG	289
566	10.8 Weitere Leistungserbringerinstitutionen	291
567	10.9 Weitere Ärztliche Institutionen	293
568	11 Anhang B – Verzeichnisse	297
569	11.1 Abkürzungen	297
570	11.2 Glossar	302
571	11.3 Abbildungsverzeichnis	302
572	11.4 Tabellenverzeichnis	304

573	11.5 Referenzierte Dokumente.....	312
574	11.5.1 Dokumente der gematik.....	312
575	11.5.2 Weitere Dokumente.....	313
576	12 Anhang C – Sektorspezifische Ausprägungen der HBA	
577	Zertifikate.....	317
578	12.1 BÄK	317
579	12.2 BZÄK.....	319
580	12.3 BPtK	321
581	12.4 Apothekerschaft	323
582	12.5 Weitere Leistungserbringer	326
583		

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende übergreifende Spezifikation definiert Anforderungen für den Themenbereich PKI, die bei der Realisierung (bzw. dem Betrieb) von Produkttypen der TI zu beachten sind. Diese Anforderungen sind als übergreifende Regelungen relevant für Interoperabilität und Verfahrenssicherheit.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter von Produkten der TI, die Zertifikate verwalten oder nutzen.

1.3 Geltungsbereich

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

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 Erlaubnisse/Lizenzen von den betroffenen Schutzrechtinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzungen

Im vorliegenden Dokument werden Verfahren und Profile für digitale Zertifikate (X.509, CVC für die Generation G2), beschrieben. Nicht beschrieben werden die Prozesse und Verfahren zur Personalisierung der Karten selbst.

Die normativen Vorgaben bzgl. verwendbarer kryptographischer Algorithmen trifft das Dokument [gemSpec_Krypt].

1.5 Methodik

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

Sie werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>

Text / Beschreibung

[<=]

Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und Textmarke [<=] angeführten Inhalte.

Folgende Namenskonvention gilt für TSP als Adressaten für spezifische Anforderungen, die im vorliegenden Konzept definiert werden:

- TSP-X.509
Übergreifende Bezeichnung für alle Herausgeber von X.509-Zertifikaten, dies sind die Produkttypen TSP-X.509 QES, TSP-X.509 nonQES und gematik Root-CA

1.5.1 Hinweis auf offene Punkte

Themen, die noch intern geklärt werden müssen oder eine Entscheidung benötigen, sind wie folgt im Dokument gekennzeichnet:

Beispiel für einen offenen Punkt.

2 Notation kryptographischer Objekte

2.1 Basis-Bezeichner

Folgende Notation wird verwendet, um Schlüssel und Zertifikate einheitlich zu benennen und zu identifizieren. Die Notation besteht aus drei durch einen Punkt „.“ getrennten Teilen mit folgender Bedeutung:

<Objekttyp>.<Objektbesitzer>.<Objektverwendung>

Im weiteren Dokument werden dafür die kürzeren englischen Begriffe verwendet:

<type>.<holder>.<usage>

Für den Objekttyp wird eine zusammenfassende Ebene mit dem Kürzel „ID“ eingeführt. Alle Notationen zu einem Objekt (Schlüssel, Zertifikate) werden unter diesem Kürzel „ID“ zusammengefasst, wobei die Bezeichner in allen Teilen übereinstimmen.

Mittels dieser Notation wird jeweils ein *Typ* eines Objektes, wie z. B. der Verschlüsselungsschlüssel einer eGK, benannt, nicht ein einzelnes spezifisches Objekt. Deshalb beschreibt diese Notation keine Laufzeiten konkreter Objekte oder deren Zuordnung zu spezifischen Anwendungsschichten oder Kartengenerationen.

2.2 Optionale Bezeichnung der technischen Ausprägung

Kann ein bestimmtes Objekt in verschiedenen technischen Ausprägungen auftreten, wird das o. g. dreistufige Bezeichnungsschema um ein 4. Element mit der Bezeichnung der technischen Ausprägung (Algorithmen, Schlüssellänge) ergänzt (siehe Kapitel 2.9).

Im weiteren Dokument ist das 4. Element, soweit aufgeführt, jeweils *kursiv* dargestellt.

**<Objekttyp>.<Objektbesitzer>.<Objektverwendung><Ild.
Nummer>.<Ausprägung>**

<type>.<holder>.<usage><n>.<instance>

Auf diese Weise werden z. B. bei mehreren in einer Karte angelegten Schlüsseln die Schlüssel- und korrespondierenden Zertifikatsreferenzen eindeutig hergestellt.

2.3 Optionales Unterscheidungsmerkmal bei gleicher technischer Ausprägung

Zur Differenzierung von Krypto-Objekten – bei sonst identischer technischer Ausprägung – kann im Element „Objektverwendung“ (Usage) zum eigentlichen Verwendungskürzel eine laufende Nummer ergänzt werden.

Beispiel:

PrK.CH.ENCN.R2048, wobei n mit 1 beginnt und fortlaufend nummeriert wird

Ein Anwendungsfall ist bspw., dass Objekte auf Karten in Vorbereitung bzw. zur Unterstützung kommender Kartengenerationen bereits vorgesehen werden und diese in der gleichen technischen Ausprägung implementiert werden.

2.4 Allgemeine Notationsvorschrift

Die Benennung kryptographischer Objekte erfolgt gemäß der Notationsvorschrift in Tab_PKI_201.

Tabelle 1: Tab_PKI_201 Allgemeine Notationsvorschrift für kryptographische Objekte

<Objektbezeichner>	::= <type>.<holder>.<usage><n>.<instance>
Die Verwendung von instance (Ausprägung) bzw. von n (laufende Nummer) ist jeweils optional und wird anhand der Notwendigkeit der Unterscheidung verschiedener technischer Ausprägungen bzw. bei gleicher technischer Ausprägung entschieden.	

2.5 Type (Objekttyp)

Der Objekttyp (type) wird bei der Benennung kryptographischer Objekte entsprechend Tab_PKI_202 gekennzeichnet.

Tabelle 2: Tab_PKI_202: Notationsvorgaben für Objekttyp

<type>	::= <key> <certificate> <ID>
<key>	::= <private key> <public key> <secret key> <individual key> <shared secret>
<certificate>	::= <X.509v3 certificate> <card verifiable certificate>
<ID>	::= <X.509v3 ID> <card verifiable ID>

Wertebereich von <key>

<private key>	::= PrK (asym.)
<public key>	::= PuK (asym.)
<secret key>	::= SK (sym.)
<individual key>	::= IK (sym.)
<shared secret>	::= ShS (sym.) (Pairing Geheimnis)

Wertebereich von <certificate>

Die Differenzierung von X.509- und CV-Zertifikaten wird im jeweiligen Verwendungszweck („Usage“) vorgenommen. Somit entfällt die Notwendigkeit nach getrennten Bezeichnern für das Feld „certificate“.

<X.509v3 certificate>	::= C
<card verifiable certificate>	::= C

Wertebereich von <ID>

Die Differenzierung von X.509- und CV-Identitäten wird analog der Vorgehensweise bei Zertifikaten im jeweiligen Verwendungszweck („Usage“) vorgenommen. Es entfällt die Notwendigkeit nach getrennten Bezeichnungen für „ID“.

```
<X.509v3 ID> ::= ID
<card verifiable ID> ::= ID
```

2.6 Holder (Objektbesitzer)

Die Definition der Holder unterscheidet zwischen X.509- und CVC-Objekten. Die möglichen Holder für symmetrische Objekte entsprechen i. A. den X.509-Objekten. Dabei versteht sich die Liste als Aufzählung aller möglichen, nicht aller erlaubten Holder. Welche im Falle der einzelnen Objekte sinnvoll sind und verwendet werden, wird durch die Definition der Objekte in den jeweiligen Architekturen und Spezifikationen bestimmt.

Objektbesitzer (im technischen Sinne) können Personen, Organisationen, Chipkarten oder auch Sicherheitsmodule sowie unterschiedliche Dienste im Rahmen der TI sein.

Während des Lebenszyklus eines Objektes können sich die Holder ändern. Im vorliegenden Dokument ist mit dem Holder immer der Holder während der Betriebsphase gemeint.

Bei der Benennung von kryptographischen Objekten wird der Objektbesitzer (holder) gemäß Tab_PKI_203 gekennzeichnet. Holder MUSS für alle drei Bereiche Schlüssel, Zertifikat und ID einheitlich verwendet werden.

Tabelle 3: Tab_PKI_203 Notationsvorgaben für Objektbesitzer

<holder> ::= <holder X.509 SK> <holder CVC>
<holder X.509 SK> ::= <root certification authority> <health professional> <card holder> <Clientmodul> <health care institution> <security module Kartenterminal> <Anwendungskonnektor> <Netzkonnektor> <VPN Zugangsdienst> <gematik Trust-service Status List> <Trust Service Provider> <Signatur Anwendungs Komponente> <Fachanwendungsspezifischer Dienst> <Zentraler Dienst> <Generischer Holder>
<holder CVC> ::= <root certification authority> <certification authority> <certification authority eGK> <certification authority HPC> <certification authority SMC> <certification authority SAK> <health professional card> <health professional card role> <health professional card device> <electronic health card> <security module card> <security module card role> <security module card device> <certification authority CAMS_HPC> <certification authority CAMS_SMC> <CAMS of HPC> <CAMS of SMC> <Kostenträger Adv>

Zu beachten bei kartenrelevanten Objekten, wie eGK und HBA sind unterschiedliche Bezeichnung der Holder in der X.509-Welt gegenüber CVC: bspw. wird bei der eGK der Holder für X.509 als „card holder“ bezeichnet (da es sich um eine Person handelt),

711 während der Holder für CVC bei der gleichen Karte als „eGK“ bezeichnet wird (da der
712 Holder nicht die Person, sondern die Karte selbst ist).

713

714 Wertebereich von <holder X.509 | SK>

715 <root certification authority> ::= RCA

716 <health professional> ::= HP

717 <card holder> ::= CH (Versicherte)

718 <Clientmodul> ::= CM

719 <health care institution> ::= HCI

720 <security module Kartenterminal> ::= SMKT

721 <Anwendungskonnektor> ::= AK

722 <Netzkonnektor> ::= NK

723 <VPN Zugangsdienst> ::= VPNK

724 <gematik Trust-service Status List> ::= TSL

725 <Signatur Anwendungs Komponente> ::= SAK

726 <TLS> ::= TLS

727 <Fachdienst VSD> ::= VSD

728 <Zentraler Dienst> ::= ZD

729 <Trust Service Provider> ::= <Generischer Holder> | <tsp>

730 <Generischer Holder> ::= GEM (anbieter- u. diensteunabhängig)

731 <tsp> (<tsp> wird hier nicht weiter formal beschrieben. Dieser Platzhalter steht für
732 einen mit der gematik vereinbarten Bezeichner für einen spezifischen TSP-X.509. Der
733 Bezeichner kann bis zu 40 Zeichen enthalten, bzw. die Konkatenation <tsp>.<usage>-
734 CA<n> darf nicht mehr als 64 Zeichen [im UTF-8-Format] enthalten, da sie in den
735 Common Name von CA-Zertifikaten eingetragen wird. S. a. Tab_PKI_229.)

736

737 Wertebereich von <holder CVC>

738 <root certification authority> ::= RCA

739 <certification authority> ::= CA

740 <certification authority eGK> ::= CA_eGK

741 <certification authority HPC> ::= CA_HPC

742 <certification authority SMC> ::= CA_SMC

743 <certification authority SAK> ::= CA_SAK

744 <certification authority for CAMS of HPC> ::= CA_CAMS_HPC (opt.)

745 <certification authority for CAMS of SMC> ::= CA_CAMS_SMC (opt.)

746 <CAMS of HPC> ::= CAMS_HPC (opt.)

747 <CAMS of SMC> ::= CAMS_SMC (opt.)

748 <health professional card> ::= HPC

749 <health professional card role> ::= HPC_Role
750 <health professional card device> ::= HPC_Device
751 <electronic health card> ::= eGK (elektronische Gesundheitskarte)
752 <security module card> ::= SMC
753 <security module card role> ::= SMC_role
754 <security module card device> ::= SMC_device
755 <Signatur Anwendungs Komponente> ::= SAK
756 <Komfort-Merkmal> ::= KM (RFID-Token)
757 <Kostenträger AdV> ::= KTRADV

758 2.7 Usage (Objektverwendung)

759 Bei der Benennung von kryptographischen Objekten wird die Objektverwendung (usage)
760 gemäß des vorgesehenen Einsatzzweckes anhand Tab_PKI_204 bezeichnet. Usage wird
761 dabei für alle drei Bereiche Schlüssel, Zertifikat und ID einheitlich verwendet.

762

763 **Tabelle 4: Tab_PKI_204 Notationsvorgaben für Objektverwendung**

<usage> ::= <usage X.509 SK> <usage CVC>
<usage X.509 SK> ::= <qualified electronic signature> <electronic signature> <electronic signature of an organization> <encipherment> <authentication X509> <authentication X509 alternative-id> <certsign X509> <VPN Tunnel> <VPN-Tunnel secure internet service> <TLS> <TLS-Client> <TLS-Server> <TLS-Clientmodul> <authentication message X509> <authentication X509 organisation> <encipherment prescription> <OCSP> <CRL> <calculation message auth. code> <key generation> <certification authority component> <certification authority VPNservice> <certification authority SMC-B> <certification authority HBA>
usage CVC> ::= <authentication CVC> <authentication role CVC> <authentication device CVC> <certsign CVC> <authentication device CVC RPE> <authentication device CVC RPS> <authentication device CVC SUK>

764 Schlüssel, Zertifikate und IDs zu CVC werden grundsätzlich mit einem Suffix „_CVC“ im
765 Feld „Objektverwendung“ (usage) versehen. Implikation daraus: ist kein „_CVC“ in usage
766 angehängt, handelt es sich um ein Objekt im X.509-Kontext. Beispiel:
767 PrK.SAK.AUTD_CVC

768

769 Wertebereich von <usage X.509 | SK>

770 <qualified electronic signature> ::= QES
771 <electronic signature> ::= SIG
772 <electronic signature of an organization> ::= OSIG
773 <encipherment> ::= ENC

774 <encipherment prescription> ::= ENCV
775 <authentication X509> ::= AUT
776 <authentication X509 organisation> ::= AUTO (opt.)
777 <authentication message X509> ::= AUTN
778 <authentication X509 alternative-id> ::= AUT_ALT
779 <certsign X509> ::= CA
780 <VPN-Tunnel> ::= VPN
781 <VPN-Tunnel secure internet service> ::= VPN-SIS
782 <TLS> ::= TLS
783 <TLS-Client> ::= TLS-C
784 <TLS-Server> ::= TLS-S
785 <TLS-Clientmodul> ::= TLS-CS
786 <OCSP> ::= OCSP
787 <calculation message auth. code> ::= MAC
788 <key generation> ::= KG
789 <CRL> ::= CRL
790 <certification authority component> ::= KOMP
791 <certification authority VPNservice> ::= VPNK
792 <certification authority SMC-B> ::= SMCB
793 <certification authority HBA> ::= HBA
794
795 **Wertebereich von <usage CVC>**
796 <certsign CVC> ::= CS
797 <authentication CVC> ::= AUT_CVC
798 <authentication role CVC> ::= AUTR_CVC
799 <authentication device CVC> ::= AUTD_CVC
800 <authentication device CVC AKS> ::= AUTD_AKS_CVC (Auslösung Komfortsignatur)
801 <authentication device CVC RPE> ::= AUTD_RPE_CVC (Remote-PIN-Empfänger)
802 <authentication device CVC RPS> ::= AUTD_RPS_CVC (Remote-PIN-Sender)
803 <authentication device CVC SUK> ::= AUTD_SUK_CVC (Stapel- und komfortfähige
804 SSEE)

805 2.8 n (lfd. Nummer)

806 Bei der Benennung von kryptographischen Objekten erfolgt bei Gleichartigkeit eine
807 Unterscheidung durch Durchnummerieren der Elemente mittels laufender Nummer. Die
808 laufende Nummer wird für alle drei Bereiche Schlüssel, Zertifikat und ID einheitlich
809 verwendet.

Wertebereich von <Ifd. Nummer>

n ist eine positive natürliche Zahl grösser 0 und ohne vorangestellte 0. n ist auf 4 Stellen begrenzt.

2.9 Instance (Ausprägung)

Besteht die Notwendigkeit der Unterscheidung kryptographischer Objekte anhand deren technischer Ausprägung, wird in der Notation dieser Objekte das jeweilige Kryptosystem mit der Schlüssellänge gemäß Tab_PKI_205 angegeben.

Tabelle 5: Tab_PKI_205-01 Notationsvorgaben für Ausprägung

<instance> ::= <instance X.509> <instance CVC> <instance SYM>	
Asymmetrische Objekte	<instance X.509> ::= <X.509 RSA 2048 > <X.509 RSA 3072 > <X.509 ECC 256 > <X.509 ECC 384 > <X.509 ECC 512 >
	<instance CVC> ::= <CVC RSA 2048 > <CVC ECC 256 > <CVC ECC 384 > <CVC ECC 512 >
Symmetrische Objekte	Bei symmetrischen Objekten wird das verwendete Verfahren genannt, wenn die Bedingungen aus Abschnitt 2.2 vorliegen.
	<instance SYM> ::= <2KeyTripleDES> <3KeyTripleDES> <AES mit 128 Bit> <AES mit 256 Bit>

Hinweis: Die normativen Vorgaben bzgl. verwendbarer kryptographischer Algorithmen trifft das Dokument [gemSpec_Krypt]. Die nachfolgenden Listen für Wertebereiche geben deren Verwendung im Kontext der Notation kryptographischer Objekte an.

Wertebereich von <instance X.509>

<X.509 RSA 2048 > ::= R2048
 <X.509 RSA 3072 > ::= R3072
 <X.509 ECC 256 > ::= E256
 <X.509 ECC 384 > ::= E384
 <X.509 ECC 512 > ::= E512

Wertebereich von <instance CVC>

~~<CVC RSA 2048 > ::= R2048~~
 <CVC ECC 256 > ::= E256
 <CVC ECC 384 > ::= E384
 <CVC ECC 512 > ::= E512

836

837 **Wertebereich von <instance SYM>**

838 <2KeyTripleDES> ::= 2DES

839 <3KeyTripleDES> ::= 3DES

840 <AES mit 128 Bit> ::= AES128

841 <AES mit 256 Bit> ::= AES256

842 2.10 Beispiele zur Umsetzung

843 2.10.1 Beispiele für asymmetrische Objekte

§44 Tabelle 6: Tab_PKI_206-01 Beispiele für asymmetrische Objekte

Komponente	Fachliche Beschreibung	Name des Zertifikats	Name des privaten Schlüssels	Name des öffentlichen Schlüssels mit einer konkreten technischen Ausprägung
eGK	X.509-Zertifikat/Schlüssel des Versicherten für die Verschlüsselung	C.CH.ENC	PrK.CH.ENC	PuK.CH.ENC2.R2048
	CV-Zertifikat der eGK zur C2C-Authentisierung	C.eGK.AUT_CVC	PrK.eGK.AUT_CVC	PuK.eGK.AUT_CVC.E256
HBA	X.509-Zertifikat/Schlüssel des Heilberufers für eine QES	C.HP.QES	PrK.HP.QES	PuK.HP.QES.R2048
	CV-Zertifikat des HBA zur C2C-Geräteauthentisierung	C.HPC.AUTD_SUK_CVC	PrK.HPC.AUTD_SUK_CVC	PuK.HPC.AUTD_SUK_CVC.R2048E256
SMC	X.509-Zertifikat/Schlüssel der Institution für eine elektronische Signatur	C.HCI.OSIG	PrK.HCI.OSIG	PuK.HCI.OSIG.E256
	CV-Zertifikat der SMC zur C2C-Rollenauthentisierung	C.SMC.AUTR_CVC	PrK.SMC.AUTR_CVC	PuK.SMC.AUTR_CVC.E256

VPN-Zugangsdienst	X.509-Zertifikat/Schlüssel des VPN-Zugangsdienstes	C.VPNK.VPN	PrK.VPNK.VPN	PuK.VPNK.VPN.R2048
Fachanw. spez. Dienst allgem.	X.509-Zertifikat/Schlüssel eines Fachanwendungsspez. Dienstes als Server für TLS-Verbindung	C.FD.TLS-S	PrK.FD.TLS-S	PuK.FD.TLS-S.R2048
Fachdienst VSD	X.509-Zertifikat/Schlüssel des VSD-Fachdienstes zum Signieren einer Nachricht	C.VSD.AUT	PrK.VSD.AUT	PuK.VSD.AUT R2048

845 **2.10.2 Beispiele für symmetrische Objekte**

846 **Tabelle 7: Tab_PKI_207 Beispiele für symmetrische Objekte**

Komponente	Fachliche Beschreibung	Name des geheimen Schlüssels	Name des geheimen Schlüssels mit einer konkreten technischen Ausprägung
eGK	Kartenindividueller Schlüssel für die Authentifizierung zwischen eGK und CMS	SK.CMS.AUT	SK.CMS.AUT.3DES
	Kartenindividueller Schlüssel für Verschlüsselung zwischen eGK und VSD	SK.VSD.ENC	SK.VSD.ENC.AES256
Fachdienst VSD	Masterschlüssel zur Ableitung der kartenindividuellen Schlüssel SK.VSD.AUT	SK.VSD.KG	SK.VSD.KG.AES128

3 CA-Strukturen

Für die Anforderungen aus dem operativen Produktivbetrieb der TI sowie den davon verschiedenen Anforderungen für Entwicklung, Test und Zulassung andererseits werden in der TI jeweils getrennte, in sich abgeschlossene PKIen implementiert.

Nachfolgend werden folgende Aspekte der CA-Strukturen der TI spezifiziert:

- Betriebsumgebungen
- CA-Gültigkeitszeiträume
- Definition der CA-Namen
 - für Produktivumgebung
 - Test- und Referenzumgebungen

3.1 Übergreifende Festlegung für CA der TI

In diesem Kapitel werden Aspekte der CA-Strukturen in der TI beschrieben.

GS-A_4257 - Hauptsitz und Betriebsstätte

Die gematik Root-CA, ein TSP-X.509 nonQES, ein TSP-X.509 QES, ein TSP-CVC die CVC-Root und der TSL-Dienst MÜSSEN ihren Hauptsitz und die Betriebsstätten für den tatsächlichen Betrieb in einem Land der Europäischen Union haben.
[<=]

3.1.1 Übersicht der Identitäten/Zertifikate

Für eine Übersicht der kryptographischen Identitäten, für die entsprechende CA-Strukturen zu bilden sind, siehe [gemKPT_PKI_TIP#3.1.1].

3.1.2 Laufzeiten der CA

Die zulässigen Gültigkeitszeiträume für CA-Zertifikate sind in der Policy [gem-RL_TSL_SP_CP#7.3.2] spezifiziert.

3.1.3 Unterstützung verschiedener Schlüsselgenerationen

Beim Betrieb der CAs in der TI werden Zertifikate verschiedener Schlüsselgenerationen parallel unterstützt (vgl. [gemKPT_PKI_TIP#TIP1-A_6878]). Die Schlüsselgeneration eines Zertifikats wird durch dessen Schlüsselalgorithmus und Signaturalgorithmus festgelegt.

GS-A_5511 - Unterstützung der Schlüsselgeneration RSA durch TSP-X.509 nonQES

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN die Schlüsselgeneration RSA (gemäß [gemSpec_Krypt#GS-A_4357]) unterstützen.
[<=]

Hinweis: Derzeit existieren für die Schlüsselgeneration „RSA“ der gematik Root-CA die Zertifikate C.GEM.RCA1 und C.GEM.RCA2. Da letzteres bis Januar 2027 gültig ist, ist kein weiterer Schlüsselversionswechsel innerhalb dieser Schlüsselgeneration vorgesehen.

GS-A_5528 - Unterstützung der Schlüsselgeneration ECDSA durch TSP-X.509 nonQES

Die gematik Root-CA und ein TSP-X.509 nonQES, der Zertifikate für die Kartengeneration G2.1 erstellt oder verwendet, MÜSSEN die Schlüsselgeneration ECDSA (gemäß [gemSpec_Krypt#GS-A_4357]) unterstützen.
[<=]

GS-A_5512 - Unterstützung der Schlüsselgeneration RSA durch TSP-X.509 QES

Ein TSP-X.509 QES MUSS die Schlüsselgeneration RSA gemäß [gemSpec_Krypt#GS-A_4358] unterstützen.
[<=]

GS-A_5529 - Unterstützung der Schlüsselgeneration ECDSA durch TSP-X.509 QES

Ein TSP-X.509 QES, der Zertifikate für die Kartengeneration G2.1 erstellt oder verwendet, MUSS die Schlüsselgeneration ECDSA gemäß [gemSpec_Krypt#GS-A_4358] unterstützen.
[<=]

GS-A_5513 - Wahl des Signaturalgorithmus für Zertifikate

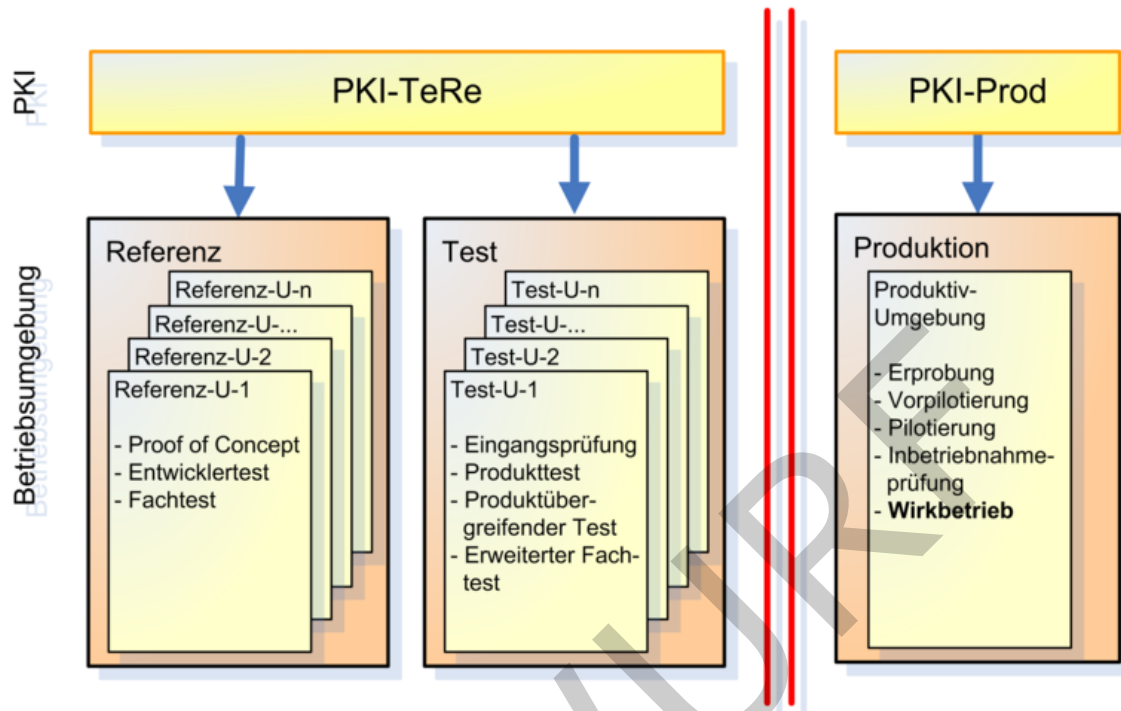
Die gematik Root-CA, die TSP-X.509 QES und die TSP-X.509 nonQES MÜSSEN Zertifikate mit dem Signaturalgorithmus der Schlüsselgeneration des Zertifikats signieren. Ausgenommen davon sind die Crosszertifikate der gematik Root-CA.
[<=]

3.2 TI-Betriebsumgebungen

Für die Anforderungen von Entwicklung, Test, Zulassung und Wirkbetrieb sind folgende Betriebsumgebungen durch eine PKI zu unterstützen.

- 1..n Testumgebungen
für z. B. Produkt- und produktübergreifende Tests im Rahmen der Zulassung von Komponenten und Diensten.
- 1..n Referenzumgebungen
für eigenverantwortliche Tests seitens der Hersteller und Diensteanbieter.
- Produktivumgebung
Es wird genau eine Produktivumgebung für den Wirkbetrieb implementiert.

914



915

916

Abbildung 1: Betriebsumgebungen aus Sicht der PKI

917

3.2.1 PKI-Sicht auf die Produktivumgebung

918

Grundlagen und Anforderungen der CA-Struktur für die Produktivumgebung sind in [gemKPT_PKI_TIP#3] ausgeführt.

919

920

3.2.2 PKI-Sicht auf Test- u. Referenzumgebung (PKI-TeRe)

921

Die gemeinsame PKI-TeRe unterstützt und vereinfacht die abgestuften Test-, Freigabe- und Zulassungsprozesse über diese beiden Umgebungen hinweg, d. h. die verwendeten Identitäten und die damit ausgestatteten Karten, Geräte und Dienste können in beiden Umgebungen gleichermaßen betrieben werden.

922

923

924

925

Neben den in der PKI-TeRe gemeinsam genutzten Produkttypen (gematik Root-CA, TSP-X.509 nonQES) werden einige andere Elemente aus Gründen der besseren Abbildbarkeit von Test-Szenarien für Test- und Referenzumgebung separat zur Verfügung gestellt. Dazu gehört der TSL-Dienst.

926

927

928

929

Die PKI-TeRe verfügt über keinerlei Übergänge zur Produktivumgebung - weder netzwerktechnisch noch hinsichtlich des TI-Vertrauensraumes.

930

931

GS-A_4695 - Zentrale Root-CA für Test- und Referenzumgebung

932

Der Anbieter der gematik Root-CA MUSS in der Test- und Referenzumgebung eine zentrale TeRe-Root-CA bereitstellen und hieraus TeRe-CAs der zweiten Ebene zertifizieren.

933

934

935

[<=]

GS-A_4696 - OCSP-Responder für gematik TeRe-Root-CA im Internet

Der Anbieter der gematik Root-CA MUSS einen OCSP-Responder für die CA-Zertifikate der TeRe-Root-CA im Internet bereitstellen.

[<=]

GS-A_4697 - PKI für Test- und Referenzumgebung

Der TSP-X.509 nonQES MUSS für jede von ihm betriebene CA der Produktivumgebung eine korrespondierende CA für die Test- und Referenzumgebung implementieren.

[<=]

Die CA-Struktur entspricht insgesamt derjenigen der Produktivumgebung.

3.2.3 Pseudo-QES PKI in Test- u. Referenzumgebung

In der Test- und in der Referenzumgebung werden auch QES-Komponenten getestet, es wird darum eine zur Produktivumgebung analoge Infrastruktur für QES-Zertifikate aufgebaut, die „Pseudo-QES PKI“. Dies beinhaltet:

- Ein Zertifikatsherausgeber für HBA-Zertifikate muss eine separate Pseudo-QES PKI zur Ausgabe von Pseudo-QES-Zertifikaten für HBA-Testkarten und HBA-Entwicklerkarten aufbauen.
- Zur Abbildung der BNetzA-VL in der Test- und Referenzumgebung wird eine Pseudo-BNetzA-VL verwendet. Diese ist analog zur BNetzA-VL strukturiert und enthält die zusätzlichen CAs, die als funktionales QES-Äquivalent in der Test- und Referenzumgebung dienen.

GS-A_4698 - Pseudo-QES PKI für PKI-TeRe

Der TSP-X.509 QES SOLL für jede von ihm betriebene QES-CA der Produktivumgebung eine funktional äquivalente CA in der PKI-TeRe implementieren.

[<=]

GS-A_5483 - Aufnahme der Pseudo-QES CA in die Pseudo-BNetzA-VL

Der TSP-X.509 QES MUSS jede von ihm in der PKI-TeRe betriebene CA in die Pseudo-BNetzA-VL aufnehmen lassen.

[<=]

3.3 Zentrale Aussteller-CAs in der TI für nonQES-Zertifikate

Die TI-Plattform stellt zentrale Aussteller-CAs für nonQES-Zertifikate der verschiedenen Anwendungsbereiche zur Verfügung.

GS-A_4702 - Zentrale Aussteller-CA für nonQES-Zertifikate

Der TSP-X.509 nonQES, der eine zentrale Aussteller-CA in der TI für die Ausgabe von nonQES-X.509-Zertifikaten für Komponenten oder Dienste bereitstellt, MUSS (1) die Zertifikatsstruktur gemäß Tab_PKI_212 und (2) im `commonName` die `<usage>` = KOMP, sowie (3) im `organizationalUnitName` den `<usageName>` = 'Komponenten' umsetzen.

[<=]

Davon ausgenommen ist die Aussteller-CA für die Ausgabe von X.509-Zertifikaten für VPN-Zugangsdienste.

GS-A_5212 - Zentrale Aussteller-CA für VPN-Zugangsdienst-Zertifikate

Der TSP-X.509 nonQES, der eine zentrale Aussteller-CA in der TI für die Ausgabe von nonQES-X.509-Zertifikaten für VPN-Zugangsdienste bereitstellt, MUSS (1) die Zertifikatsstruktur gemäß Tab_PKI_212 und (2) im `commonName` die `<usage>` = VPNK,

979 sowie (3) im `organizationalUnitName` den `<usageName>` = 'VPN-Zugangsdienst'
980 umsetzen.
981 [`<=>`]

982 3.4 Spezifische Aussteller-CA in der TI

983 Alternativ können TSP-X.509 nonQES auch dienstespezifische Aussteller-CAs, für
984 definierte Einsatzbereiche (bspw. Konnektor) betreiben.

985 **GS-A_4703 - CA-Zertifikatsprofil für nonQES-Zertifikate**

986 Ein TSP-X.509 nonQES und der Anbieter des TSL-Dienstes MÜSSEN für die Beantragung
987 einer Aussteller-CA unterhalb der zentralen gematik-Root-CA die Zertifikatsstruktur
988 gemäß Tab_PKI_212 und einem CA-Namen entsprechend der Tabelle Tab_PKI_213
989 umsetzen.
990 [`<=>`]

991 **GS-A_4704 - Nutzung von CA mit spezifischem Verwendungszweck**

992 Ein TSP-X.509 nonQES, TSP-X.509 QES und der Anbieter des TSL-Dienstes DÜRFEN aus
993 einer Aussteller-CA mit einem spezifischen Verwendungszweck NICHT weitere EE-
994 Zertifikate für andere Zwecke ausgeben.
995 [`<=>`]

996 **GS-A_4828 - Vorgaben zur Bildung von nonQES-CA-Namen**

997 Ein TSP-X.509 nonQES MUSS für eine Aussteller-CA unterhalb der zentralen gematik-
998 Root-CA (1) die Zertifikatsstruktur gemäß Tab_PKI_212 umsetzen und (2) für die Bildung
999 des `subjectDN` im Feld `subject.commonName` die Einträge aus der Spalte `<usage>` sowie
1000 (3) im Feld `organizationalUnitName` die korrespondierenden Einträge aus der Spalte
1001 `<usageName>` aus der Tabelle Tab_PKI_213 umsetzen.
1002 [`<=>`]

1003 **Tabelle 8: Tab_PKI_213 Erlaubte Werte für `<usage>` und `<usageName>`**

Spezifischer CA-Einsatzbereich	<code><usage></code> im Feld <code>commonName</code>	<code><usageName></code> im Feld <code>organizationalUnitName</code>
Heilberufsausweis	HBA	Heilberufsausweis
Berufsausweis	BA	Berufsausweis
Institutionskarten	SMCB	Institution des Gesundheitswesens
eHealth-Kartenterminals	SMKT	Kartenterminal
Konnektor	KON NK AK SAK	Konnektor Netzkonnektor Anwendungskonnektor SigAnwendKomponente
Zentrale Dienste	ZD	ZentraleDienste
Fachanwendungsspezif. Dienst	FD	Fachanwendungsspezifischer Dienst
OCSP-Dienst	OCSP	OCSP-Signer
CRL-Dienst	CRL	CRL-Signer

TSL-Dienst	TSL	TSL-Signer
VPN-Zugangsdienst	VPNK	VPN-Zugangsdienst
Elektronische Gesundheitskarte	EGK	Elektronische Gesundheitskarte
Elektronische Gesundheitskarte (alternative Versichertenidentitäten)	EGK-ALVI	eGK alternative Vers-Ident
Komponenten (Geräte und Dienste)	KOMP	Komponenten

1004

1005

4 Kodierung von X.509-Identitäten

1006

4.1 Namensregeln und -formate

1007

Die Abbildung einer realen Identität (Person, Dienst, Komponente) in ein X.509-Zertifikat erfolgt durch den Inhalt der Felder *SubjectDN* (*subject distinguishedName*).

1008

1009

4.1.1 Verarbeitung von Sonderzeichen

1010

GS-A_4705-01GS-A_4705 - Verarbeitung von Sonderzeichen in PKI-Komponenten

1011

1012

gematik-Root-CA, TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN sicherstellen, dass von ihnen eingesetzte Komponenten in der Lage sind, Sonderzeichen wie ä, ü, ö, ß etc. anhand eines Zeichensatzes gemäß Tab_PKI_229-01 in den einzelnen Namens-elementen zu verarbeiten und darzustellen.

1013

1014

1015

1016

~~Es MUSS dazu ein Zeichensatz gemäß [Common-PKI#Part1] unterstützt werden.~~

1017

[<=]

1018

Aufgrund der weit verbreiteten 8-Bit-Kodierung (z.B. MS Windows, Apache Server) kann alternativ der Zeichensatz [ISO8859-1] zur Darstellung der Sonderzeichen verwendet werden.

1019

1020

1021

Distinguished Names können daher generell mit diesen Sonderzeichen gebildet werden.

1022

1023

Bei Kommunikationspartnern außerhalb Deutschlands kann die Verwendung von Umlauten zu Problemen führen, z. B. bei der Darstellung von Distinguished Names. Die zuständigen Instanzen für die Namensgebung müssen diese Problematik berücksichtigen.

1024

1025

Für TI-interne TLS-Server und TLS-Client-Zertifikate können Umlaute und UTF-8-Codierungen verwendet werden, da auch für diese Komponenten eine Unterstützung eines Zeichensatzes gemäß [Common-PKI#Part 1] (s. e.)GS-A-4705-01) gefordert ist.

1026

1027

1028

4.1.2 Definition der Subject-DNs für Personen und Komponenten

1029

- Definition der Versichertenidentität in Kap 5.1.15.11

1030

- Definition der Organisationsidentität in Kap 5.3.1

1031

- Definition der Identitäten von Konnektor und SMKT in Kap. 5.5.1 bzw. 5.6.1

1032

- Definition der Identitäten der Zentralen Dienste und Fachanwendungsspezifischen Dienste in Kap. 5.8.1 und 5.9.1

1033

1034

4.1.3 SubjectDN von CA-Zertifikaten und von OCSP-Responder-Zertifikaten

1035

1036

GS-A_4706 - Vorgaben zu SubjectDN von CA- und OCSP-Zertifikaten

1037

gematik-Root-CA, TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN bzgl. Aufbau des SubjectDN in CA-Zertifikaten und OCSP-Responder-Zertifikaten folgende Vorgaben

1038

umsetzen: (a) Der subjectDN einer CA bzw. eines OCSP-Responders muss diese

1039

eindeutig innerhalb der TI identifizieren. (b) Das Attribut commonName muss enthalten

1040

sein und den relevanten Namen der CA bzw. des OCSP-Responders enthalten. (c) Das

1041

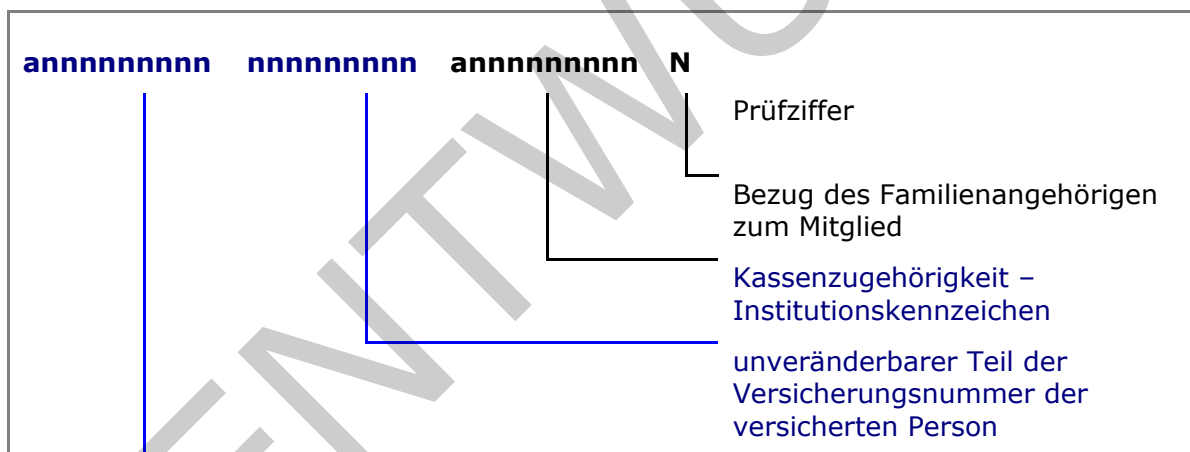
1042 Attribut organizationName muss enthalten sein und den Namen des TSP enthalten. (d)
1043 Das Attribut countryName muss enthalten sein und das Herkunftsland des TSP (Land der
1044 Anschrift des TSP) enthalten. (e) Die Attribute serialNumber und organizationalUnitName
1045 können enthalten sein, sollen jedoch nur dann verwendet werden, falls sie für die
1046 Eindeutigkeit des subjectDN notwendig sind. (f) Das Attribut organizationIdentifier kann
1047 enthalten sein. (g) Darüber hinaus sollen keine weiteren Attribute enthalten sein.
1048 [\leq]

1049 4.2 Schlüssel der Versichertenidentität (eGK)

1050 Gemäß SGB § 290 definieren die Spitzenverbände der Krankenkassen die Struktur der
1051 Krankenversichertennummer, die aus einem unveränderbaren Teil zur Identifikation des
1052 Versicherten und einem veränderbaren Teil, der bundeseinheitliche Angaben zur
1053 Kassenzugehörigkeit enthält.

1054 In den Zertifikaten C.CH.AUT, C.CH.ENC und C.CH.QES der eGK sowie C.CH.AUT_ALT der
1055 alternativen Versichertenidentitäten, wird in zwei OU-Feldern jeweils ein eindeutiger
1056 Schlüssel für den Versicherten sowie die Versicherungs-Institution aufgenommen:

- 1057 • OU = unveränderbarer Teil der KV-Nummer
- 1058 • OU = Institutionskennzeichen



1059 **Abbildung 2: Aufbau der Krankenversicherthennummer**

1060 4.3 Pseudonym der Versichertenidentität (eGK)

1061 In den Zertifikaten C.CH.AUTN bzw. C.CH.ENCV der eGK (Schlüssel ohne PIN-Eingabe
1062 nutzbar) wird im Feld `commonName` des `subjectDN` anstelle der personenbezogenen
1063 Klartextdaten ein Pseudonym verwendet.

1064 4.3.1 Versicherten-Pseudonym in X.509-Zertifikaten der eGK

1065 **GS-A_4572 - Abbildung Pseudonym in X.509-Zertifikaten der eGK**

1066 Der TSP-X.509 nonQES (eGK) MUSS im Feld `commonName` der Zertifikatstypen C.CH.AUTN
1067 bzw. C.CH.ENCV das Pseudonym des Versicherten aufnehmen.
1068 [\leq]

4.3.2 Eindeutigkeit des Pseudonym

Das Pseudonym dient als Ordnungskriterium (Primärschlüssel) für die Ablage von medizinischen Objekten und muss daher innerhalb der Herausgeber-Domäne über die Versicherten hinweg eindeutig sein. In Verbindung mit dem Herausgeber ist das Pseudonym so innerhalb der gesamten TI eindeutig.

GS-A_4573 - Eindeutigkeit des Pseudonyms innerhalb Herausgeber-Domäne

Der TSP-X.509 nonQES (eGK) MUSS das im AUTN- und ENCV-Zertifikat des Versicherten gespeicherte Pseudonym innerhalb der Herausgeber-Domäne (IssuerDomain) eindeutig gestalten.

[<=]

4.3.3 Pseudonym-Erstellungsregel

Die Bildung des Pseudonyms erfolgt nach einer Ableitungsregel aus bereits vorliegenden personenbezogenen Daten (KVNR) sowie durch ein herausgeberspezifisches Geheimnis. So kann auf den Einsatz eines technisch-organisatorischen Hintergrundsystems zur Verwaltung der Zuordnung von Pseudonymen zu Klaridentitäten verzichtet werden.

GS-A_4574 - Pseudonym-Erstellungsregel

Der TSP-X.509 nonQES (eGK) MUSS das Pseudonym des Versicherten nach folgender Regel bilden: SHA-256 Hashwert über die Konkatenierung der Datenfelder (1) Nachname des Versicherten, (2) unveränderbarer Teil der KVNR des Versicherten und (3) einer vom Herausgeber (Kostenträger) verwendeten Zusatzinformation (herausgeberspezifischer Zufallswert).

[<=]

Substring(SHA-256 Hash über Datenfelder, 1, 20):
• Inhaber (Nachname des Versicherten)
• unveränderbarer Teil der KVNR des Versicherten
• herausgeberspezifischer Zufallswert (hs-ZW)

Durch Verwendung dieses Verfahrens kann der Nachweis erbracht werden, dass eine bestimmte KVNR zu einem bestimmten Inhaber und dem entsprechenden Zertifikatsherausgeber gehört, ohne dass die KVNR in einem (öffentlichen) Zertifikats-Verzeichnis gespeichert werden muss.

Bei Kenntnis des Nachnamens sowie der KVNR eines Versicherten und sofern der vom Herausgeber verwendete Zufallswert zur Verfügung gestellt wird, kann das Pseudonym nachgerechnet werden. Dabei ist ein auch im Negativ-Fall zuverlässiges Prüfungsergebnis nur möglich, wenn die Anzahl der zu verwendenden Iterationsschritte beschränkt wird.

Beispiel:

Nachname =
„Mustername1“

KVNR (unveränderlicher Teil, 10-stellig, AN) =
„M331784849“

1107 herausgeberspezifischer Zufallswert (16-stellig, h) =
1108 „A32C93C6946314A9“

1109 Konkatenation =
1110 „Mustername1M331784849A32C93C6946314A9“

1111 SHA-256- Hashwert =
1112 "E3F3555165491A7FBE3F355516549E3F3555165902BFAF254518C469E584A793"

1113 Für den `commonName` werden die ersten 20 Hex-Zeichen (Variationsbreite 80 Bit)
1114 verwendet:

1115 `commonName` =
1116 "E3F3555165491A7FBE3F"

1117 **GS-A_4575 - Prüfung auf Eindeutigkeit des Pseudonyms**

1118 Der TSP-X.509 nonQES (eGK) MUSS nach Erzeugung des Pseudonyms prüfen, ob dieses
1119 Pseudonym vom Kartenherausgeber bereits vergeben wurde. Ist dies der Fall, MUSS das
1120 Pseudonym mit inkrementiertem hs-ZW neu generiert und erneut auf Eindeutigkeit
1121 geprüft werden.
1122 [\leq]

1123 **GS-A_4576 - Pseudonym auf eGK-Ersatzkarten**

1124 Der TSP-X.509 nonQES (eGK) MUSS bei Ausstellung eines eGK-Ersatzausweises
1125 innerhalb der definierten Verwendungsperiode des herstellerspezifischen Zufallswertes
1126 (hs-ZW) dasselbe Pseudonym verwenden wie auf der vorgängigen Karte.
1127 [\leq]

1128 **GS-A_4577 - Pseudonym auf eGK-Folgekarten**

1129 Der TSP-X.509 nonQES (eGK) MUSS bei Ausstellung eines eGK-Ersatzausweises nach
1130 Ablauf der definierten Verwendungsperiode des hs-ZW oder bei Ausstellung einer
1131 Folgekarte nach Ablauf des Gültigkeitszeitraums der vorgängigen Karte ein neues
1132 Pseudonym auf Grundlage des geänderten hs-ZW vergeben.
1133 [\leq]

1134 **4.3.4 Hs-ZW – Herausgeberspezifischer Zufallswert (hs-ZW)**

1135 Da der herausgeberspezifische Zufallswert für alle Versicherten eines Herausgebers
1136 identisch ist, muss dieser periodisch, z. B. jährlich gewechselt werden.

1137 **GS-A_4578 - eGK hs-ZW Bildungsregel**

1138 Der eGK-Herausgeber MUSS einen individuellen herausgeberspezifischen Zufallswert (hs-
1139 ZW) aus mindestens 16 Hexadezimal-Ziffern (64 Bit) festlegen, der jeweils kollisionsfrei
1140 zu allen vorherigen hs-ZW dieses eGK-Herausgebers ist.
1141 [\leq]

1142 **GS-A_4579 - eGK hs-ZW Verwendung/Wechsel**

1143 Der eGK-Herausgeber MUSS den aktuellen hs-ZW für alle Versichertenzertifikate für eine
1144 bestimmte Verwendungsperiode verwenden und mindestens einmal jährlich wechseln.
1145 [\leq]

1146 **GS-A_4580 - eGK hs-ZW Archivierung**

1147 Der eGK-Herausgeber MUSS alle nicht mehr verwendeten hs-ZW für Zwecke der
1148 Rekonstruktion von Pseudonymen für mindestens 10 Jahre sicher speichern und
1149 berechtigten Teilnehmern der TI verfügbar machen.
1150 [\leq]

4.3.5 Kodierung des Pseudonyms

Für das eGK-Pseudonym gilt folgende Systematik für Erstellung und Verwendung.

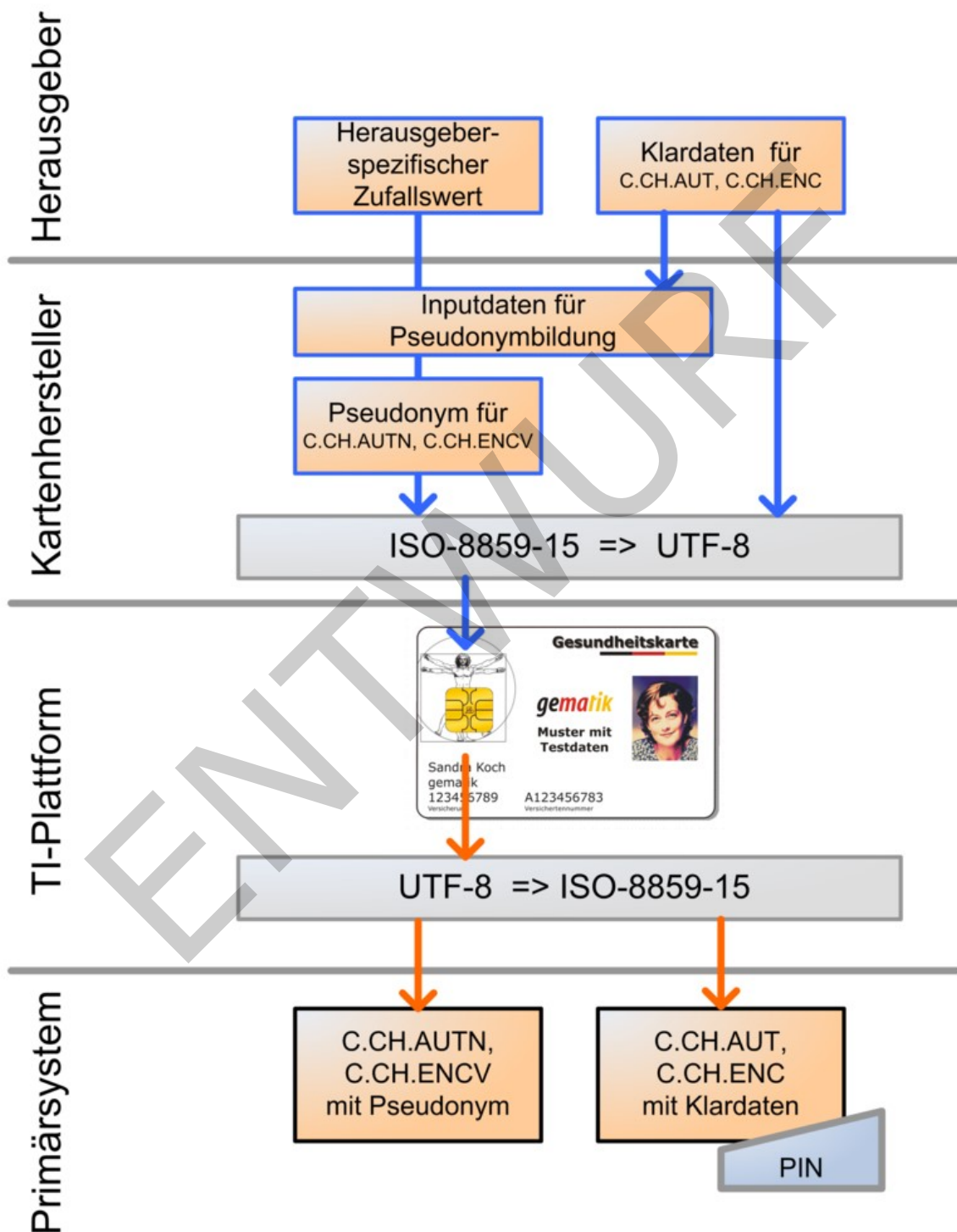


Abbildung 3: Pseudonym Kodierung in X.509-Versichertenzertifikaten

1156
1157

1158 **GS-A_4582 - Pseudonym-Personalisierung im X.509-SubjectDN**

1159 Der eGK-Herausgeber MUSS das Pseudonym im UTF-8-Zeichensatz codiert in das
1160 Zertifikat der eGK einbringen.
1161 [\leq]

1162 **4.4 Berufsgruppen-ID der Leistungserbringer**

1163 **4.4.1 Berufsgruppe des Heilberufers**

1164 Die Admission Extension der HBA beinhaltet die Berufsgruppe des Heilberufers als Text
1165 und in Form einer maschinenlesbaren OID sowie zusätzlich einen Schlüsselwert für die
1166 einzelne Person in Form der Telematik-ID (s. Abschnitt 4.7.1). Optional können weitere
1167 Berufsgruppenmerkmale des Heilberufers in diese Struktur aufgenommen werden.

1168 Die konkreten OID-Werte sind in [gemSpec_OID#3.5.1.1] definiert.

1169 **GS-A_4583 - Berufsgruppenkennzeichen für HBA**

1170 Der HBA-Herausgeber MUSS die Berufsgruppe(n) des Heilberufers in Form einer
1171 textuellen Bezeichnung und einer OID gemäß Tab_PKI_221 in jedes Zertifikat eines HBA
1172 gleichlautend einbringen und dabei die Werte aus [gemSpec_OID#GS-A_4442]
1173 verwenden.

1174 [\leq]

1175 **GS-A_4584 - Verwendung von Berufsgruppenkennzeichen**

1176 TSP-X.509 nonQES und TSP-X.509 QES DÜRFEN NICHT Berufsgruppenkennzeichen, für
1177 deren Verwendung sie nicht zugelassen und beauftragt sind, in HBA-Zertifikate
1178 einbringen.

1179 [\leq]

1180

1181 **Tabelle 9: Tab_PKI_221 Berufsgruppenkennzeichnung**

Art der ID	Ort	X.509 Feldname	Format	Inhalt	Beispiel
Berufsgruppe / Rolle	Admission	ProfessionItem	Text	<Berufsgruppe>	Ärztin/Arzt
		ProfessionOID	OID	oid_<berufsgruppe>	1.2.276.0.76.4.30
Einzelne Person	Admission	RegistrationNumber	AN	<Telematik-ID>	1-1a25sd-d529

4.5 ID der Organisation/Einrichtung des Gesundheitswesens

4.5.1 Typ und Exemplar der Organisation/Einrichtung des Gesundheitswesens

Die Admission Extension der SMC-B beinhaltet die Art der Organisation/Einrichtung des Gesundheitswesens als Text und in Form einer maschinenlesbaren OID sowie zusätzlich die einzelne Institution in Form der Telematik-ID (s. Abschnitt 4.7.1).

Die konkreten OID-Werte sind in [gemSpec_OID#3.5.1.3] definiert.

GS-A_4585 - Typ der Organisation/Einrichtung des Gesundheitswesens für SMC-B

Der SMC-B-Herausgeber MUSS den Typ der Organisation/Einrichtung des Gesundheitswesens in Form einer textuellen Bezeichnung und einer OID gemäß Tab_PKI_222 in jedes Zertifikat einer SMC-B gleichlautend einbringen und dabei die Werte aus [gemSpec_OID#GS-A_4443] verwenden.

[<=]

GS-A_4586 - Verwendung von Institutionskennzeichen

TSP-X.509 nonQES DÜRFEN Institutskennzeichen, für deren Verwendung sie nicht zugelassen und beauftragt sind, NICHT in SMC-B-Zertifikate einbringen.

[<=]

Tabelle 10: Tab_PKI_222 Institutionstypkennzeichnung

Art der ID	Ort	X.509 Feldname	Form at	Inhalt	Beispiel
Institutions typ	Admissi on	ProfessionItem	Text	<Institutionstyp>	Zahnarztpraxis
		ProfessionOID	OID	oid_<institutionstyp>	1.2.276.0.76.4.51
Einzelne Institution	Admissi on	RegistrationNumber	AN	<Telematik-ID>	2- 2a25sd-d529

4.6 Technische Rolle von Komponenten und Diensten

4.6.1 Technische Rolle im Komponentenzertifikat

Die Admission Extension der Komponentenzertifikate beinhaltet die technische Rolle der Komponente bzw. des Dienstes als Text und in Form einer maschinenlesbaren OID, aber keine zusätzliche Kennung einer einzelnen Instanz vergleichbar der Telematik-ID.

Die konkreten OID-Werte sind in [gemSpec_OID#3.5.4] definiert.

GS-A_4707 - Kennzeichen für Technische Rolle für Komponenten und Dienste

Der Kartenherausgeber MUSS die technische Rolle einer Komponente bzw. eines Dienstes in Form einer textuellen Bezeichnung und einer OID gemäß Tab_PKI_230 in jedes Zertifikat der Komponente bzw. des Dienstes gleichlautend einbringen und dabei die Werte aus [gemSpec_OID#GS-A_4446] verwenden.

[<=]

GS-A_4708 - Verwendung von Kennzeichen für Technische Rolle

TSP-X.509 nonQES für gSMC MÜSSEN ausschließlich solche Kennzeichen für technische Rollen in Komponentenzertifikate einbringen, für die der Antragsteller nachweislich berechtigt ist.

[<=]

Tabelle 11: Tab_PKI_230 Kennzeichnung Technische Rolle

Art der ID	Ort	X.509 Feldname	Format	Inhalt	Beispiel
Technische Rolle	Admission	ProfessionItem	Text	<Technische Rolle>	Netzkonnektor
		ProfessionOID	OID	oid_<Technische Rolle>	1.2.276.0.76.4.104

4.7 Telematik-ID

Die Telematik-ID repräsentiert als eineindeutiges Merkmal die Identität eines Teilnehmers, also eines Leistungserbringers im HBA respektive einer Organisation/Einrichtung des Gesundheitswesens in einer SMC-B. Die Telematik-ID muss daher über alle Sektoren hinweg eineindeutig bezogen auf die elektronische Identität der betroffenen Teilnehmer in der Telematikinfrastruktur sein. Die Zuordnung der Telematik-ID zum Teilnehmer wird in [gemKPT_PKI_TIP] beschrieben.

Für Ersatzkarten und Austauschkarten wird die Telematik-ID der Originalkarte verwendet.

Für Folgekarten muss die Telematik-ID nicht identisch zur Vorgängerkarte sein. Der Arzt und die medizinische Institution können eine neue Telematik-ID beantragen oder auch die bisherige in der Folgekarte wieder verwenden.

GS-A_4958 - Neue Telematik-ID bei Folgekarten

Der Kartenherausgeber MUSS bei der Ausgabe von Folgekarten dem Antragsteller die Möglichkeit bieten, eine neue Telematik-ID zu beziehen.

[<=]

GS-A_4960 - System für Sektorkennzeichen

Der Gesamtbetriebsverantwortliche der TI MUSS zur Sicherstellung der Eindeutigkeit der Telematik-ID über die verschiedenen Sektoren des Gesundheitswesens hinweg ein System für Sektorkennzeichen als Bestandteil (Präfix) der Telematik-ID etablieren und verwalten.

[<=]

4.7.1 Abbildung der Telematik-ID im X.509-Zertifikat

Die Telematik-ID wird im Feld **registrationNumber** der Extension Admission hinterlegt, vgl. Beispiel in Tabelle 12.

GS-A_4709 - Abbildung der Telematik-ID in Admission-Struktur

TSP-X.509 nonQES MÜSSEN zur Abbildung der Telematik-ID in HBA- sowie SMC-B-Zertifikaten eine Admission Extension aufnehmen, die eine oder mehrere Struktur(en) „ProfessionInfo“ und darin im Feld „registrationNumber“ die Telematik-ID enthalten

1250 muss.
1251 [\leq]

1252 **GS-A_4901 - Einheitliche Admission in Zertifikaten einer Karte**
1253 TSP-X.509 QES und TSP-X.509 nonQES SOLLEN die Admission Extension in allen X.509-
1254 Zertifikaten einer Karte identisch einbringen. In den Herausgabe-Policies können
1255 Ausnahmen hiervon definiert sein.
1256 [\leq]

1257

1258 **Tabelle 12: Tab_PKI_224 Telematik-ID-Kennzeichnung**

Art der ID	Ort	X.509 Feldname	Format	Inhalt	Beispiel
Berufsgruppe / Rolle	Admission	ProfessionItem	Text	<Berufsgruppe>	Ärztin/Arzt
		ProfessionOID	OID	oid <berufsgruppe>	1.2.276.0.76.4.30
Einzelne Person / Institution	Admission	registrationNumber	AN	<Telematik-ID>	1-1a25sd-d529

1259 **4.7.2 Aufbau der Telematik-ID**

1260 **GS-A_4587 - Gesamtlänge der Telematik-ID**
1261 Herausgeber von HBA und SMC-B MÜSSEN sicherstellen, dass die Gesamtlänge der
1262 Telematik-ID (Präfix, Separator und Fortsatz) 128 Zeichen nicht überschreitet.
1263 [\leq]

1264

1265 **Tabelle 13: Tab_PKI_223 Aufbau der Telematik-ID**

Bestandteil	Inhalt	Länge	Format
Präfix	Nummernkreis der jeweiligen Organisation (Unterscheidung der Sektoren)	nicht festgelegt	N
Separator	Trennzeichen zwischen Präfix und Fortsatz	„-“	
Fortsatz	eindeutige Nummer, sektorspezifisch (z. B. Betriebsstätten-Nr. o. ä.)	nicht festgelegt	AN

1266 *Anmerkung zur Darstellung des Formats: N=numerisch, AN=alphanumerisch*

1267 **4.7.2.1 Sektoraler Präfix**

1268 **GS-A_4710 - Präfix der Telematik-ID**
1269 Herausgeber von HBA und SMC-B MÜSSEN die in Tab_PKI_101 festgelegten Präfixe der
1270 Telematik-ID verwenden.
1271 [\leq]

1272

Tabelle 14: Tab_PKI_101-01 Normative Festlegung für das Präfix der Telematik-ID.

Präfix	Sektor	Zuständige Organisationen
1	Ärzeschaft	BAEK, KBV
2	Zahnärzeschaft	BZÄK, KZBV
3	Apothekerschaft	BAK
4	Psychotherapeuteschaft	BPTK
5	Krankenhaus	DKG
6	(Reserved for future use)	
7	KTR-AdV	
8	Kostenträger	GKV-SV
9	Weitere Organisationen des Gesundheitswesens	gematik
10	Weitere Leistungserbringer des Gesundheitswesens und deren Institutionen	eGBR
11	Gesundheitshandwerke	ZDH

Hinweis: Kassenärztliche Vereinigungen (KVen) geben SMC-Bs für die Betriebsstätten ihrer Mitglieder aus. Dies betrifft neben den Praxen der Kassenärzte auch solche von Vertragspsychotherapeuten. Als Mitglied der KBV teilt eine KV dabei eine Telematik-ID mit Präfix „1“ zu, auch wenn es sich um die Betriebsstätte eines Psychotherapeuten handelt.

Der Nummernraum des Präfixes wird durch die [Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH \(gematik\)](#) gematik GmbH verwaltet.

4.7.2.2 Separator

GS-A_4711 - Separator der Telematik-ID

Herausgeber von HBA und SMC-B MÜSSEN sicherstellen, dass bei der Abbildung der Telematik-ID das Präfix vom Rest der Telematik-ID durch einen Separator getrennt wird und als Separator das Minuszeichen „-“ mit ASCII-Wert 45 dezimal beziehungsweise 0x2D hexadezimal verwendet wird.

[<=]

4.7.2.3 Fortsatz der Telematik-ID

GS-A_4712 - Definition und Eindeutigkeit der Telematik-ID

Kartenherausgeber von HBA und SMC-B in den jeweiligen Sektoren MÜSSEN Syntax, Semantik und Vergabe des Fortsatzes der Telematik-ID so definieren, dass die Eindeutigkeit des sektorspezifischen Anteils der Telematik-ID gewährleistet ist.

[<=]

Beispiele für die weiterführende Unterteilung für den Bereich der Ärzteschaft:

- Die Telematik-ID beginnt mit 1-1 bei einem eArztausweis (HPC),

- Die Telematik-ID beginnt mit 1-2 bei einem ePraxisausweis (SMC).

GS-A_4713 - Zeichensatz für den Fortsatz der Telematik-ID

TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN den vom jeweiligen Sektor vorgegebenen Zeichensatz für den Fortsatz der Telematik-ID verwenden.

[<=]

4.8 Kodierung der Zertifikate

4.8.1 Kodierung der Attribute

In diesem Kapitel werden die für alle X.509-Zertifikate einheitlich geltenden Felder und ihre Kodierung aufgeführt. Ergänzende profilspezifische Kodierungsvorgaben sind bei den jeweiligen Profilen ausgeführt.

GS-A_4714-01GS-A_4714 - Kodierung der Attribute in X.509-Zertifikaten

TSP-X.509 und der Anbieter des TSL-Dienstes MÜSSEN bei der Kodierung der Attribute in X.509-Zertifikaten die Vorgaben aus Tab_PKI_229-01 umsetzen. Die Vorgaben sind unabhängig davon, ob das jeweilige Attribut innerhalb eines issuer (Typ Name)-, subject (Typ Name)- oder eines extension (Typ Extension)-Elementes im Zertifikat verwendet wird.

[<=]

Tabelle 15: Tab_PKI_229-01 Kodierung der Attribute in X.509-Zertifikaten

Attribut / Attribut-OID (Common-PKI , RFC 5280)	Kodierung	Max. Stringlänge (Zeichen)
commonName {id-at 3}	UTF8String[RFC3629] *)	64
surName {id-at 4}	UTF8String[RFC3629] *)	64
localityName {id-at 7}	UTF8String[RFC3629] *)	128
stateOrProvinceName {id-at 8}	UTF8String[RFC3629] *)	128
streetAddress {id-at 9}	UTF8String[RFC3629] *)	128
organizationName {id-at 10}	UTF8String[RFC3629] *)	64
organizationalUnitName {id-at 11}	UTF8String[RFC3629] *)	64
title {id-at 12}	UTF8String[RFC3629] *)	64
postalCode {id-at 17}	UTF8String[RFC3629] *)	40
givenName {id-at 42}	UTF8String[RFC3629] *)	64
serialNumber {id-at 5}	PrintableString [RFC5280]	64

countryName {id-at 6}	PrintableString [RFC5280] gültiger "ISO 3166-1 alpha-2 country code" [ISO 3166-1] (s.a. [X.520] Kap. 6.3.1)	2
organizationIdentifier {id-at 97}	UTF8String [X.520] Annex A und [ETSI EN 319 412-1] Kap. 5.1.3 (natürliche Person)/5.1.4 (juristische Person)	-
*) Einschränkung des erlaubten Zeichensatzes auf dedizierte ISO-Subsets gemäß Vorgaben der jeweiligen Kartenherausgeber		

[<=]

4.8.2 Stringlänge der Attribute

GS-A_4715-01GS-A_4715 - Maximale Stringlänge der Attribute im SubjectDN

TSP-X.509 und der Anbieter des TSL-Dienstes MÜSSEN bzgl. der maximalen Stringlänge der Attribute in X.509-Zertifikaten die Vorgaben aus Tab_PKI_229-01 umsetzen. Die Vorgaben sind unabhängig davon, ob das jeweilige Attribut innerhalb eines issuer (Typ Name)-, subject (Typ Name)- oder eines extension (Typ Extension)-Elementes im Zertifikat verwendet wird.

[<=]

GS-A_4716 - Umgang mit überlangen Organisationsnamen im SubjectDN

Der TSP-X.509 nonQES für Komponenten, die gematik Root-CA und der Anbieter des TSL-Dienstes MÜSSEN für den Fall, dass der Wert des Attributs organizationName {id-at 10} in X.509-Zertifikaten eine String-Länge größer als 64 Zeichen hat, sicherstellen, dass die Angabe im subject auf 64 Zeichen abgekürzt wird und die Extension SubjectAltNames {2 5 29 17} mit der ungekürzten Angabe in das Zertifikat eingefügt wird.

[<=]

Hinweis:

Die TSP-X.509 nonQES für SMC-B nehmen eine etwaige Befüllung der Extension SubjectAltNames gemäß den Vorgaben des jeweiligen Sektors vor. Diese sind den jeweiligen sektorspezifischen SMC-B Zertifikatsprofilen zu entnehmen.

4.8.3 Struktur

Für einige Extensions (Zertifikatserweiterungen) definiert [~~Common-PKI~~RFC5280] Kap. 4.2 mehrere unterschiedliche Ausprägungen der Strukturen. Um die Verwendung von Zertifikaten in der TI zu vereinfachen werden spezifisch einschränkende Festlegungen für Extensions gemäß Tab_PKI_226-01 festgelegt. ~~Dies erfolgt jeweils in Form einer angepassten Common-PKI-Tabelle.~~ Die Spalte „ASN.1 Definition“ beschreibt die ASN.1 Struktur. Die Spalte „TI-spezifische Vorgaben“ trifft Festlegungen für einzelne Elemente. Für nicht aufgeführte Extensions stellt die TI keine über die Standarddefinition hinausgehenden Anforderungen.

4.8.3.1 serialNumber

Wird zur Eindeutigkeit von Zertifikaten innerhalb der TI und zur Identifizierung von Zertifikaten verschiedener TSPs das Präfix TSP-ID innerhalb der *subjectSerialNumber* genutzt, so werden die Werte folgender Tabelle Tab_PKI_109 verwendet.

Tabelle 16: Tab_PKI_109 Werte für das Präfix <TSP-ID>

Präfix <TSP-ID>	Zertifizierungsdiensteanbieter
10	D-TRUST
11	Signtrust
12	T-Systems Telesec
13	S-Trust
14	TC TrustCenter
15	DGN
16	medisign
19	atos

Der Nummernraum des Präfixes wird durch die [Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH \(gematik\)](#) gematik GmbH verwaltet.

Im Falle der Clusterung von Diensten besteht evtl. die Notwendigkeit jeder Instanz ein eigenes Zertifikat auszustellen. Damit die Eindeutigkeit des SubjectDN im jeweiligen Zertifikat gewährleistet ist, kann die Ausprägung der Instanz in das Feld serialNumber übernommen werden.

GS-A_4725 - Eindeutiger SubjectDN durch serialNumber

Ein TSP-X.509 nonQES KANN die Eindeutigkeit des SubjectDN in einem X.509-Zertifikat für Zentrale Dienste und Fachanwendungsspezifischen Dienste durch die Verwendung des Attributes serialNumber {id-at-serialNumber} gewährleisten.

[<=]

GS-A_4726 - Verwendung von serialNumber zur Schaffung eindeutiger SubjectDNs

TSP-X.509 nonQES MÜSSEN bei Verwendung des Attributs serialNumber in X.509-Zertifikaten für Zentrale Dienste und Fachanwendungsspezifische Dienste den Inhalt entsprechend dem folgenden Format aufbauen: Instanz (fünfstellige Dezimalzahl) + "-" + Unterscheidung Zertifikat (alphanumerischer Wert).

[<=]

4.8.3.2 Admission

Die Extension Admission enthält Angaben zur Registrierung und zu der beruflichen Zulassung (und somit auch zu daraus ableitbaren Autorisierungsinformationen) sowohl als Text als auch in Form einer maschinenlesbaren OID.

Für die verschiedenen Zertifikatstypen sind dies jeweils:

- die Berufsgruppen (HBA/BA),
- der Status als Versicherte/-r (eGK und alternative Versichertenidentitäten),
- der Typ der Organisation/Institution (SMC-B) oder

- die technische Rolle (Komponentenzertifikate).

Außerdem können die Telematik-ID und die registrierende bzw. zulassende Stelle (admissionAuthority) in Admission eingetragen werden (in HBA-, BA- und SMC-B-Zertifikaten).

GS-A_4717-01GS-A_4717 - TI-spezifische Vorgabe zur Nutzung der Extension Admission

TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN bei Verwendung der Extension Admission {id-commonpki-at1 3 36 8 3 3} die Struktur in X.509-Zertifikaten entsprechend Tab_PKI_226-01 erstellen-

[<=>]

Tabelle 17: Tab_PKI_226-01 Struktur Admission

#	ASN.1 definition	TI-spezifische Vorgaben
1	id-isismtt-at-admission OBJECT IDENTIFIER ::= {id-isismtt-at1 3 36 8 3 3}	Identifizierung des Objekts über die OID
2	id-isismtt-at-namingAuthorities OBJECT IDENTIFIER ::= {id-isismtt-at1 3 36 8 3 11}	Identifizierung des Objekts über die OID
3	AdmissionSyntax ::= SEQUENCE {	
4	admissionAuthority GeneralName OPTIONAL,	Angabe (optional) der admissionAuthority auf der obersten Ebene der Extension in Form eines Distinguished Name (directoryName). In den jeweiligen Zertifikatsprofilen und -ausprägungen wird dieser Distinguished Name in Textform gemäß [RFC4514] dargestellt.
5	contentsOfAdmissions SEQUENCE OF Admissions }	Diese Sequenz MUSS genau ein Element vom Typ Admissions enthalten.
6	Admissions ::= SEQUENCE {	
7	admissionAuthority [0] EXPLICIT GeneralName OPTIONAL,	
8	namingAuthority [1] EXPLICIT NamingAuthority OPTIONAL,	
9	professionInfos SEQUENCE OF ProfessionInfo }	Diese Sequenz MUSS ein Element vom Typ ProfessionInfo enthalten.

-		
14	ProfessionInfo ::= SEQUENCE {	
15	namingAuthority [0] EXPLICIT NamingAuthority OPTIONAL,	
16	professionItems SEQUENCE OF DirectoryString (SIZE(1..128)),	professionItems enthält ein Element von Typ DirectoryString Für DirectoryString MUSS die Kodierung UTF8String verwendet werden.
17	professionOIDs SEQUENCE OF OBJECT IDENTIFIER OPTIONAL,	Dieses Element MUSS eine OID enthalten.
18	registrationNumber PrintableString(SIZE(1..128)) OPTIONAL,	Wenn dieses optionale Feld enthalten ist, enthält es die Telematik-ID. In QES-HBA-Zertifikaten für Ärzte wird das Feld registrationNumber nicht gesetzt.
19	addProfessionInfo OCTET STRING OPTIONAL }	

[<=]

4.8.3.3 CertificatePolicies

Die Extension CertificatePolicies enthält in X.509-Zertifikaten der TI zwei unterschiedliche Informationstypen:

- es werden ein oder mehrere Bezeichner für die Policies aufgenommen, die Festlegungen für Herausgabe und Einsatz dieser Zertifikate enthalten
- es wird ein Element eingefügt, das den Bezeichner für den Zertifikatstyp enthält (nur bei EE-Zertifikaten).

GS-A_4718 - TI-spezifische Vorgabe zur Nutzung der Extension

CertificatePolicies

TSP-X.509 MÜSSEN bei Verwendung der Extension CertificatePolicies {2 5 29 32} die Struktur in X.509-Zertifikaten entsprechend Tab_PKI_227 erstellen.

[<=]

Tabelle 18: Tab_PKI_227 Struktur CertificatePolicies

#	Asn.1 Definition	TI-spezifische Vorgaben
1	CertificatePolicies ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation	In allen End-Entity-Zertifikaten MUSS genau ein Element dieser Sequenz enthalten.

2	PolicyInformation ::= SEQUENCE {	
3	policyIdentifier CertPolicyId,	Dieses Element MUSS mindestens zweimal enthalten sein: 1 - Policy-OID (einmal oder mehrfach) 2 - Zertifikatstyp-OID (genau einmal bei EE-Zertifikaten, nicht bei Signer- EE-Zertifikaten)
4	policyQualifiers SEQUENCE SIZE(1..MAX) OF PolicyQualifierInfo OPTIONAL }	Enthält das Element PolicyIdentifier die Zertifikatstyp-OID, DARF das Element policyQualifiers NICHT verwendet werden
5	CertPolicyId ::= OBJECT IDENTIFIER	
6	PolicyQualifierInfo ::= SEQUENCE {	
7	policyQualifierId PolicyQualifierId,	
8	qualifier ANY DEFINED BY policyQualifierId }	
9	id-qt OBJECT IDENTIFIER ::= {id-pkix 2}	
10	id-qt-cps OBJECT IDENTIFIER ::= {id-qt 1}	
11	id-qt-unotice OBJECT IDENTIFIER ::= {id-qt 2}	
12	PolicyQualifierId ::= OBJECT IDENTIFIER {id-qt-cps id-qt-unotice }	
13	CPSUri ::= IA5String	
14	UserNotice ::= SEQUENCE {	
15	noticeRef NoticeReference OPTIONAL,	

16	explicitText DisplayText OPTIONAL }	
17	NoticeReference ::= SEQUENCE {	
18	organization DisplayText,	
19	noticeNumber SEQUENCE OF INTEGER }	
20	DisplayText ::= CHOICE {	
20a	ia5String IA5String (SIZE (1..200)),	
21	visibleString VisibleString (SIZE (1..200)),	
22	bmpString BMPString (SIZE (1..200)),	
23	utf8String UTF8String (SIZE (1..200)) }	

4.8.3.4 CRLDistributionPoints

Zertifikate des Zugangsdienstes C.VPNK.VPN und C.VPNK.VPN-SIS können im Internet mittels einer CRL auf ihren Sperrstatus geprüft werden. Daneben gibt es die übliche Prüfbarkeit des Sperrstatus über einen OCSP-Responder.

GS-A_5074 - Bereitstellung CRL und OCSP für Zertifikate des VPN-Zugangsdienstes

Der TSP-X.509 nonQES, der eine Aussteller-CA für die Ausgabe von C.VPNK.VPN und C.VPNK.VPN-SIS Zertifikaten betreibt, MUSS für diese Zertifikate eine CRL im Internet bereitstellen. Er MUSS ebenfalls für die Verteilung der Sperrinformationen der eben genannten Zertifikate über OCSP im Internet Statusinformationen zur Verfügung stellen. [≤]

Innerhalb der TI sind CRLs für die Statusprüfung von Zertifikaten nicht vorgesehen.

GS-A_5516 - Schlüsselgenerationen der CRL für Zertifikate des VPN-Zugangsdienstes

Der TSP-X.509 nonQES, der eine Aussteller-CA für die Ausgabe von C.VPNK.VPN und C.VPNK.VPN-SIS-Zertifikaten betreibt, MUSS für jede Schlüsselgeneration eine CRL bereitstellen und mit einem CRL-Signer-Zertifikat derselben Schlüsselgeneration (gemäß [gemSpec_Krypt] #GS-A_4357) bestätigen. [≤]

4.8.3.5 SubjectAltNames

GS-A_4719 - TI-spezifische Vorgabe zur Nutzung der Extension SubjectAltNames

TSP-X.509 MÜSSEN bei Verwendung der (optionalen) Extension SubjectAltNames {2 5 29 17} die Struktur in X.509-Zertifikaten entsprechend Tab_PKI_228 erstellen.
[<=]

Tabelle 19: Tab_PKI_228 Struktur SubjectAltName

#	Asn.1 Definition	TI-spezifische Vorgaben
1	SubjectAltNames ::= GeneralNames	Ein GeneralNames-Feld enthält eine Sequenz von GeneralName-Elementen. Die Typ-Ausprägungen in den folgenden Zeilen sind für GeneralName zulässig.
2	rfc822Name [1] IMPLICIT IA5String,	E-Mail-Adresse in der Form rfc822Name
3	dNSName [2] IMPLICIT IA5String,	"Domain Name Label" wie in [RFC5280], Kap. 4.2.1.6. beschrieben
4	otherName [0] IMPLICIT OtherName, OtherName ::= SEQUENCE { type-id OBJECT IDENTIFIER value [0] EXPLICIT ANY DEFINED BY type-id }	,type-id' ist gleich dem OID eines Attributes im SubjectDN. Als ,value' ist ein UTF8-String enthalten. Dieser String enthält <ul style="list-style-type: none"> den im Attribut enthaltenen Namen in voller Länge, wenn er aufgrund der Längenbeschränkung im SubjectDN gekürzt werden musste oder bei Bedarf einen Alternativnamen oder eine Ergänzung zu diesem Attribut.

Erläuterung:

Überlange Attribute des Subject Distinguished Name (SubjectDN) werden gekürzt, um die für sie geltenden Längenvorgaben einzuhalten (s. Tab_PKI_229 „Kodierung der Attribute in X.509-Zertifikaten“). Sie werden aber in der Extension „SubjectAltNames“ in voller Länge abgebildet.

Felder des „SubjectAltNames“ werden als „GeneralName“ gespeichert. Für die Verwendung von überlangen Namen wird der GeneralName-Typ OtherName benutzt. Dessen Struktur ist wie folgt aufgebaut:

```
OtherName ::= SEQUENCE {
    type-id OBJECT IDENTIFIER,
    value [0] EXPLICIT ANY DEFINED BY type-id }
}
```

1453 Die `type-id` entspricht der OID des zu verlängernden Feldes:

- 1454 • `commonName` {id-at 3}
- 1455 • `organizationalUnitName` {id-at 11}
- 1456 • `organizationName` {id-at 10}

1457 Bei Bedarf kann die beschriebene Struktur auch verwendet werden, um Alternativnamen
1458 oder Ergänzungen zum Namen aufzunehmen, welcher im durch `type-id` bezeichneten
1459 Attribut des SubjectDN enthalten ist, auch wenn dieser nicht gekürzt werden musste.

1460 Für weitere Informationen, siehe auch ITU-T Rec. X.501 | [ISO/IEC9594-2]. Das Format
1461 des `value` wird entsprechend demjenigen des Attributes festgelegt, bei den Attributen
1462 `commonName`, `organizationalUnitName` und `organizationName` handelt es sich dabei
1463 immer um UTF8String.

1464 4.9 Erläuterungen zu Zertifikatsprofilen

1465 Dieses Kapitel enthält eine Reihe von Erläuterungen und Hilfestellungen zum Verständnis
1466 der in Kapitel 5 dargestellten Zertifikatsprofile sämtlicher X.509-Zertifikate.

1467 4.9.1 Allgemeine Erläuterungen

1468 Die Angabe Kardinalität gibt an, wie oft ein Element in einem Zertifikat enthalten sein
1469 muss. Ein optionales Feld hat so z. B. eine Kardinalität von 0-1. Eine Kardinalität von 1
1470 bezeichnet ein Pflichtfeld, das nur ein Mal auftreten darf.

1471 Die Bezeichner „ZD, FD“ werden in den Festlegungen zu X.509-Zertifikaten als
1472 Kurzbezeichnungen für die Rollen von Zentralen Diensten und
1473 Fachanwendungsspezifischen Diensten verwendet.

1474 Die Attribute einer Berufsgruppe, einer medizinischen Institution oder technischen Rolle
1475 werden in den X.509-Zertifikaten anhand einer maschinenlesbaren OID und einem
1476 textuellen Bezeichner beschrieben. Siehe hierzu auch Kap 4.4 bis 4.6.

1477 Die normative Festlegung der Werte der Felder `professionItems` und `professionOIDs`
1478 erfolgt in den Tabellen Tab_PKI_402, Tab_PKI_403 und Tab_PKI_406 in
1479 [gemSpec_OID#3.5].

1480 Für die Festlegung des Zertifikatstyps in der Extension CertificatePolicies wird eine OID-
1481 Referenz verwendet. Die normative Festlegung der durch diese Referenz dargestellten
1482 OIDs trifft das Dokument [gemSpec_OID# Tab_PKI_405].

1483 4.9.2 Berufs-/Rollenattribute und Sperrbarkeit

1484 **GS-A_4721 - Beantragung Rollenattribute im X.509-Zertifikatsrequest**

1485 Der TSP-X.509 nonQES der Komponenten-PKI MUSS bei der Erstellung von X.509-
1486 Zertifikate für Dienste sicherstellen, dass ein Diensteanbieter nur Zertifikate für die
1487 Rollen beantragen kann, für die dieser Diensteanbieter in der TI von der gematik
1488 zugelassen ist.

1489 [`<=`]

GS-A_4961 - Verwendung zugewiesener Berufs- und Rollenattribute

Die Kartenherausgeber MÜSSEN genau die Berufs- und Rollenattribute verwenden, die den zertifizierten Identitäten entweder auf gesetzlicher Grundlage oder durch Zuweisung einer gesetzlich autorisierten Standesvertretung zugewiesen wurden. Für die codierte Form dieser Attribute MÜSSEN die von der TI-Plattform verwalteten Berufs- und Rollencodes verwendet werden.

[<=]

GS-A_4722 - Belegung der Felder professionInfos

Der TSP-X.509 nonQES MUSS bei der Erstellung von X.509-Zertifikaten sicherstellen, dass die Werte `professionItems` und `professionOIDs` den Festlegungen für den Typ des beantragten Zertifikats entsprechen.

[<=]

GS-A_4724 - Komplettsperrung aller Zertifikate einer Karte

TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN sicherstellen, dass alle Zertifikate auf einem Kartenexemplar durch einen Sperrauftrag gesperrt werden können (sofern für die jeweiligen Zertifikatstypen die Statusinformationsbereitstellungen gefordert sind).

[<=]

4.9.3 Benennung der Zertifikatsprofile

Mit den Zertifikatsprofilen sind in den folgenden Unterabschnitten auch einheitliche Namen für die Zertifikate genannt. Das Benennungsschema ist in Kap. 2 beschrieben.

4.9.4 Distinguished Name

Die Bezeichnung von Entitäten in X.509-Zertifikaten (in den Feldern „Subject“, „Issuer“ oder „admissionAuthority“) erfolgt über eine Datenstruktur, welche „Distinguished Name“ genannt wird. Beispiel:

"CN=John Smith,OU=Sales,O=ACME Limited,L=Moab,ST=Utah,C=US"

Ein Distinguished Name diente ursprünglich zur eindeutigen Bezeichnung eines Eintrages in einem X.500- (bzw. LDAP-) Verzeichnis. Der entsprechende Datentyp wird deshalb auch als „directoryName“ bezeichnet, und da der Aufbau eines solchen Verzeichnisses einer hierarchischen Baumstruktur folgt, ist auch ein Distinguished Name hierarchisch aufgebaut, auch wenn ein Distinguished Name in einem Zertifikat unabhängig von einem Verzeichnis und dessen Struktur erstellt werden kann.

Distinguished Names werden in X.509-Zertifikaten binär als „Sequence“, also als geordnete Folge codiert. Das hierarchisch höchste Element ist das erste in der Sequenz. Dabei handelt es sich in Distinguished Names gemäß den Zertifikatsprofilen, wie sie in Kapitel 5 dargestellt werden, üblicherweise um das Element „countryName=DE“ bzw. „C=DE“.

Die Textdarstellung eines Distinguished Name wird in [RFC4514] („Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names“) standardisiert: Objekte bzw. Knoten in der Hierarchie werden durch Kommas getrennt, und das hierarchisch höchste Element steht ganz hinten. Das Beispiel im einleitenden Absatz ist gemäß der RFC4514-Notation dargestellt.

Distinguished Names können auch tabellarisch dargestellt werden. Dabei wird das hierarchisch höchste Element zuunterst aufgeführt. Die Reihenfolge in den Subject-Feldern in den Zertifikatsprofilen in Kapitel 5 folgt auch der tabellarischen Darstellung.

1534 Das hierarchisch tiefste Element (commonName bzw. CN) wird jeweils zuoberst notiert,
1535 „C=DE“ ganz unten in der Tabelle.

1536 Für den Aufbau der Hierarchie von Distinguished Names existieren keine starren Regeln.
1537 Es gibt aber eingespielte Best-Practices dazu, und im Annex B von [X.521] werden
1538 Empfehlungen zum Aufbau formuliert. Z. B. soll ein countryName-Element, sofern
1539 vorhanden, als oberstes Element unter der Wurzel des Baumes eingefügt werden,
1540 organizationalUnitName (OU) soll hierarchisch immer unterhalb des organizationName
1541 (O) liegen etc.

1542 Die in diesem Dokument (insbesondere in Kapitel 5) spezifizierten Distinguished Names
1543 sind ausnahmslos gemäß diesen Empfehlungen aufgebaut.

1544 **A_15676 - Reihenfolge der Elemente im SubjectDN von X.509-Zertifikaten**

1545 Der TSP-X.509 und der TSL-Dienst SOLLEN die Reihenfolge der Elemente im SubjectDN
1546 von erstellten X.509-Zertifikaten gemäß der Zertifikatsprofilltabellen in [gemSpec_PKI]
1547 umsetzen. Dabei sind die Elemente in den Zertifikatsprofilltabellen in aufsteigender
1548 Hierarchie angeordnet. In den X.509-Zertifikaten sind die Elemente in der Reihenfolge
1549 der entsprechenden absteigenden Hierarchie zu realisieren.

1550 [**<=**]

1551 Beispiel für einen SubjectDN mit absteigender Hierarchie in einem C.HCI.AUT-Zertifikat
1552 gemäß Tab_PKI_238 (dort in aufsteigender Hierarchie aufgelistet):

1553 SubjectDN (String)

1554 C=DE, O=2-299999999999 NOT-VALID, serialNumber=12.80276002791200027011,
1555 CN=Zahnarztpraxis Prof. Dr. Dr. Dr. med. rer. nat. Dip:PN TEST-ONLY

1556

1557 SubjectDN (ASN.1-Codierung)

```
1558 SEQUENCE {  
1559   SET {  
1560     SEQUENCE {  
1561       OBJECT IDENTIFIER countryName (2 5 4 6)  
1562       PrintableString 'DE'  
1563     }  
1564   }  
1565   SET {  
1566     SEQUENCE {  
1567       OBJECT IDENTIFIER organizationName (2 5 4 10)  
1568       UTF8String '2-299999999999 NOT-VALID'  
1569     }  
1570   }  
1571   SET {  
1572     SEQUENCE {  
1573       OBJECT IDENTIFIER serialNumber (2 5 4 5)  
1574       PrintableString '12.80276002791200027011'  
1575     }  
1576   }  
1577   SET {  
1578     SEQUENCE {  
1579       OBJECT IDENTIFIER commonName (2 5 4 3)  
1580       UTF8String  
1581         'Zahnarztpraxis Prof. Dr. Dr. Dr. med. rer. nat. '  
1582         'Dip:PN TEST-ONLY'  
1583     }  
1584   }  
}
```

1585 }
1586

1587 4.10 Kodierung der Betriebsumgebungen in Zertifikaten

1588 Zertifikate für Test- und Referenzumgebungen werden je TSP aus genau einer vollständig
1589 separaten Test-PKI ausgestellt. Siehe hierzu auch Kap 3.

1590 **GS-A_4727 - PKI-Separierung von Test- und Produktivumgebung in der TI**

1591 Der TSP-X.509 und der Anbieter des TSL-Dienstes DÜRFEN für die Generierung von EE-
1592 Zertifikaten der Produktivumgebung NICHT eine CA der Testumgebung verwenden.
1593 Umgekehrt DÜRFEN der TSP-X.509 und der Anbieter des TSL-Dienstes für die
1594 Generierung von EE-Zertifikaten der Testumgebung NICHT eine CA der
1595 Produktivumgebung verwenden.

1596 [\leq]

1597 **GS-A_4588 - CA-Namen für Test-PKI der TI**

1598 Der TSP-X.509 und der Anbieter des TSL-Dienstes MÜSSEN die Namen (CN: und O:)
1599 sämtlicher CAs in der Test-PKI entsprechend den korrespondierenden CAs der
1600 Produktivumgebung vergeben und diese um den String „TEST-ONLY“ im CN-Feld sowie
1601 „NOT-VALID“ im O-Feld ergänzen.

1602 [\leq]

1603 **GS-A_4589 - EE-Namen für Test-PKI der TI**

1604 TSP-X.509 nonQES (außer eGK) und TSP-X.509 QES MÜSSEN die Namen (CN: und O:)
1605 der EE-Zertifikate in der Test-PKI entsprechend den korrespondierenden
1606 Zertifikatsprofilen der Produktivumgebung verwenden und ergänzen:

1607 (a) für HBA-, Institutions- und Signer-Zertifikate um den String „TEST-ONLY“ im CN-Feld
1608 sowie um den String „NOT-VALID“ im O-Feld,

1609 (b) für Komponentenzertifikate um den String "TEST-ONLY - NOT-VALID" im O-Feld.

1610

1611

1612 [\leq]

1613 Die Fallunterscheidung in GS-A_4589 rührt daher, dass die Markierung als Testzertifikat
1614 prominent im Common Name (CN) erfolgen soll, wenn immer dies möglich ist. Falls dem
1615 Inhalt des Common Name eine funktionale Bedeutung zukommen kann (z. B. bei einem
1616 TLS-Server-Zertifikat mit FQDN im Common Name), muss aber darauf verzichtet werden.
1617 Dies ist bei Zertifikaten für Komponenten (Dienste und Geräte/gSMC) der Fall.

1618 Die folgende Tabelle dient der Detaillierung dieses Sachverhaltes:

1619

1620 **Tabelle 20: Common Name (CN) der End-Entity-Zertifikate Test-PKI**

Zertifikatstyp	Halter / Art	CN Test-PKI gleich CN Produktiv-PKI?
C.HCI.AUT	Organisation/Institution	Nein
C.HCI.ENC	Organisation/Institution	Nein
C.HCI.OSIG	Organisation/Institution	Nein
C.HP.AUT	Person	Nein
C.HP.ENC	Person	Nein

C.HP.QES	Person	Nein
C.GEM.OCSP	Signer	Nein
C.GEM.CRL	Signer	Nein
C.TSL.SIG	Signer	Nein
C.SMKT.AUT	Gerät	Ja
C.NK.VPN	Gerät	Ja
C.AK.AUT	Gerät	Ja
C.SAK.AUT	Gerät	Ja
C.VPNK.VPN	Dienst	Ja
C.VPNK.VPN-SIS	Dienst	Ja
C.ZD.TLS-C	Dienst	Ja
C.ZD.TLS-S	Dienst	Ja
C.FD.TLS-C	Dienst	Ja
C.FD.TLS-S	Dienst	Ja
C.FD.SIG	Dienst	Ja
C.FD.AUT	Dienst	Ja
C.FD.ENC	Dienst	Ja
C.CM.TLS-CS	Dienst	Ja
C.SGD-HSM.AUT	Dienst	Ja

1621
1622

1623 **GS-A_4590 - Zertifikatsprofile für Test-PKI**

1624 Der TSP-X.509 und der Anbieter des TSL-Dienstes SOLLEN die Feldattribute (außer CN:
1625 und O:) für sämtliche Zertifikate in der Test-PKI gemäß den korrespondierenden Profilen
1626 der Produktivumgebung setzen.
1627 [\leq]

1628 **4.11 Kartenverlust und Deaktivierung von Chipkarten**

1629 **GS-A_4962 - Verhalten bei Kartenverlust und Änderung persönlicher Daten**

1630 Der Kartenherausgeber MUSS den Zertifikatsnehmer verpflichten, Sperrungen seiner
1631 Karte bzw. seines Sicherheitsmoduls bei dem Kartenherausgeber oder bei einer von ihm
1632 benannten Stelle durchführen zu lassen. Sperrgründe können beispielsweise der Verlust
1633 der Karte bzw. des Sicherheitsmoduls sowie Änderungen zu registrierungsrelevanten
1634 persönlichen Daten sein (z. B. Änderung der Zugehörigkeit zu einer Berufsgruppe).
1635 [\leq]

1636 **GS-A_4963 - Deaktivierung von Chipkarten nach Gültigkeitsende**

1637 Der Kartenherausgeber MUSS Vorgaben definieren, wie eine Chipkarte sowie die
1638 enthaltenen kryptographischen Schlüssel nach Ablauf ihrer definierten Gültigkeitsdauer

1639 dauerhaft unbrauchbar gemacht werden.
1640 [\leq]

ENTWURF

5 X.509-Zertifikate

In diesem Kapitel werden die Anforderungen an X.509-Zertifikate formuliert, wobei die generischen Festlegungen aus Kap. 3 für alle Zertifikatsprofile gelten, soweit anwendbar.

~~Die Schreibweise der Termini entspricht [Common-PKI].~~

Bei Verwendung der keyUsage „nonRepudiation“ und „contentCommitment“ wird technisch dasselbe KeyUsage-Bit gesetzt. In dieser Spezifikation wird einheitlich die Bezeichnung „nonRepudiation“ verwendet.

Eine Gesamtübersicht aller kryptographischen Identitäten (X.509- und CV-) mit deren Einsatzfeldern findet sich in [gemKPT_Arch_TIP#AnhB].

GS-A_4965 - Keine Suspendierung von X.509-Zertifikaten (außer für eGK)

Ein TSP-X.509 DARF für X.509-Zertifikate – außer denen der eGK – eine Suspendierung NICHT implementieren.

[<=]

Die Bedingungen für Sperrung und Suspendierung (nur bei eGK) von Zertifikaten werden in [gemRL_TSL_SP_CP#5.9] beschrieben.

Für Zertifikate, die auf Karten gespeichert werden, sind Größenbeschränkungen zu beachten.

GS-A_5337 - Größenbeschränkung von X.509 Zertifikaten auf Karten

Ein TSP X.509 (außer ein TSP X.509 für eGK) MUSS sicherstellen, dass die von ihm erzeugten Zertifikate, die für die Speicherung auf Karten vorgesehen sind, die Maximalgröße der dafür vorgesehenen Kartenobjekte - gemäß der relevanten Objektsystemspezifikationen - nicht überschreiten. Wenn zu lange Eingangsdaten vorliegen sind diese in Abstimmung mit dem Antragsteller/Kartenherausgeber zu ändern.

[<=]

5.1 eGK – Versichertenkarte

Die Festlegungen in diesem Kapitel gelten sowohl für die Zertifikate bzw. Identitäten auf der eGK selbst als auch für die alternativen Versichertenidentitäten, die nicht auf der eGK-Smartcard gespeichert sind.

5.1.1 Definition der Versichertenidentität

Folgende Datenfelder bilden die Namensidentität des Versicherten

1. Vorname des Versicherten
2. Familienname des Versicherten
3. Titel des Versicherten
4. Namenszusatz
5. Vorsatzwort

Diese Daten werden in den folgenden Feldern des **subjectDN** des Versicherten im Zertifikat abgebildet:

- 1678 • `commonName`
- 1679 • `title`
- 1680 • `givenName`
- 1681 • `surname`

1682 **GS-A_4966 - Nutzung bestehender Versichertendatensätze für eGK-Zertifikate**
1683 Für die Erstellung von Versichertenkarten SOLL der Kartenherausgeber bestehende
1684 Versichertendatensätze für die Registrierung von Zertifikatsnehmern verwenden.
1685 [`<=`]

1686 5.1.2 Belegung der Felder im SubjectDN

1687 Die zwei Namenszeilen, die auf die eGK optisch personalisiert werden, bestehen aus
1688 jeweils 28 Zeichen, die beide zusammen mit einem zusätzlichen Leerzeichen als
1689 Trennzeichen den `commonName` des Versicherten bilden. Die Begrenzung auf 64 Zeichen
1690 wird erfüllt.

1691 Für die Bildung der anderen Felder wird der Name des Versicherten in der natürlichen
1692 Schreibweise und Reihenfolge herangezogen.

1693 Titel Vorname Namenszusatz Vorsatzwort Familienname

1694 **GS-A_4967 - Vergabe und Übermittlung eindeutiger Versicherten-ID**
1695 Die Kostenträger MÜSSEN für den Versicherten eine eindeutige ID vergeben und zur
1696 Zertifikaterstellung an den Zertifikatsherausgeber zur Einbringung in die Zertifikate
1697 übermitteln.
1698 [`<=`]

1699 **GS-A_4968 - Erzeugung und Einbringung der KVNR**
1700 Der eGK-Kartenherausgeber MUSS als eindeutigen Identifier des Versicherten die KVNR
1701 gemäß gesetzlicher Vorgaben erzeugen und Festlegungen treffen, welche Anteile der
1702 KVNR in die Versichertenkarten einzubringen sind.
1703 [`<=`]

1704 **GS-A_4592 - Bildung des surname im SubjectDN eGK-Zertifikat**
1705 Der Kartenherausgeber MUSS für das Feld `surname` im SubjectDN der eGK-Zertifikate das
1706 Attribut *Familienname* verwenden und MUSS bei erforderlichen Kürzungen bis zur
1707 maximal zulässigen Länge des Feldes folgende Regel anwenden: (a) ein ggf. vorhandener
1708 dritter Familienname ist ggf. bis auf den Anfangsbuchstaben zu kürzen und die Kürzung
1709 durch einen Punkt kenntlich zu machen. Ist die Kürzung nicht ausreichend, MUSS
1710 zusätzlich gelten: (b) ein zweiter Familienname ist ggf. bis auf den Anfangsbuchstaben zu
1711 kürzen und die Kürzung durch einen Punkt kenntlich zu machen.
1712 [`<=`]

1713 **GS-A_4593 - Bildung des givenName im SubjectDN eGK-Zertifikat**
1714 Der Kartenherausgeber MUSS für das Feld `givenName` im SubjectDN der eGK-Zertifikate
1715 die Attribute *Vorname Namenszusatz Vorsatzwort* verwenden und MUSS bei
1716 erforderlichen Kürzungen bis zur maximal zulässigen Länge des Feldes folgende Regel
1717 anwenden: (a) ein ggf. vorhandener dritter Rufname ist auf den Anfangsbuchstaben zu
1718 verkürzen und die Kürzung durch Punkt kenntlich zu machen. Ist die Kürzung nicht
1719 ausreichend, MUSS zusätzlich gelten: (b) ein zweiter Rufname ist ggf. bis auf den
1720 Anfangsbuchstaben zu kürzen und die Kürzung durch Punkt kenntlich zu machen.
1721 [`<=`]

GS-A_4594 - Bildung des title im SubjectDN eGK-Zertifikat

Der Kartenherausgeber MUSS für das Feld `title` im SubjectDN der eGK-Zertifikate das Attribut *Titel* verwenden. Kürzungen können bei Überschreitung der maximal zulässigen Länge vorgenommen werden; Kürzungsregeln sind nicht definiert.

[<=]

Beispielsatz der Feldinhalte

Name: Dr.-Ing. Peter-Wilhelm Markgraf von Meckelburg-Vorpommeln

Im Zertifikat wären folgende Attribute zu verwenden:

Tabelle 21: Tab_PKI_231 Personennamen im subjectDN

Feld	Inhalt
commonName	Dr. Peter-W. Markgraf von Meckelburg-Vorpommeln
title	Dr.-Ing.
givenName	Peter-Wilhelm Markgraf von
surname	Meckelburg-Vorpommeln

5.1.3 X.509-Zertifikatsprofile der eGK

Nach den Vorgaben des Lastenheftes kann die Suspendierung von nonQES-Zertifikaten der eGK als unter Bestandsschutz stehend interpretiert werden. Mangels eines praktischen Nutzens soll die Suspendierung von Zertifikaten in der TI generell nicht als obligatorische Anforderung gelten. Bestandssysteme der eGK können ggf. vorhandene Schnittstellen und Prozesse zur Suspendierung und Desuspendierung für die nonQES-Zertifikate der eGK jedoch beibehalten. Dies gilt nicht für die Zertifikate der alternativen Versichertenidentitäten.

GS-A_4969 - Suspendierung von eGK-Zertifikaten (nonQES)

Ein Kartenherausgeber SOLL für die X.509-Zertifikate der eGK eine Suspendierung und Desuspendierung von nonQES-Zertifikaten NICHT implementieren. Für das optional auf der eGK befindliche QES-Zertifikat und die AUT_ALT-Zertifikate ist eine Suspendierung/Desuspendierung nicht möglich.

[<=]

In den folgenden Unterkapiteln sind die Zertifikatsprofile der Zertifikate auf der eGK und der alternativen Versichertenidentitäten aufgelistet. Einziger Unterschied der alternativen Versichertenidentitäten zu den Zertifikaten auf der eGK ist ein abweichender Zertifikatstyp im Feld `CertificatePolicies`.

5.1.3.1 C.CH.AUT und C.CH.AUT_ALT – Authentisierung eGK

GS-A_4595 - Umsetzung Zertifikatsprofil C.CH.AUT

Der TSP-X.509 nonQES (eGK) MUSS C.CH.AUT gemäß Tab_PKI_232 umsetzen.

[<=]

A_17989 - Umsetzung Zertifikatsprofil C.CH.AUT_ALT

Der TSP-X.509 nonQES (eGK) MUSS C.CH.AUT_ALT gemäß Tab_PKI_232 umsetzen.

[<=]

1757 Tabelle 22: Tab_PKI_232 C.CH.AUT und C.CH.AUT_ALT Authentisierung eGK

Element		Inhalt	Kar.	
certificate		C.CH.AUT, C.CH.AUT_ALT		
	tbsCertificate			
	version	2 (v3)		
	serialNumber	gemäß [RFC5280#4.1.2.2.]		
	signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	issuer	DN der ausstellenden CA		
	validity	Gültigkeit des Zertifikats (von - bis)		
	subject			
	CommonName	CN = Aufgedruckte Namenszeilen der Karte	1	
	title	Titel des Versicherten	0-1	
	givenName	Vorname des Versicherten	1	
	surname	Nachname des Versicherten	1	
	organizationalUnitName	OU = unveränderbarer Teil der KV-Nummer	1	
	organizationalUnitName	OU = Institutionskennzeichen	1	
	organizationName	O = Herausgeber	1	
	countryName	C = DE	1	
	subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers	1	
	extensions			critical
	SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Versicherten	1	FALSE
	KeyUsage {2 5 29 15}	<i>Für Schlüsselgeneration RSA:</i> digitalSignature keyEncipherment <i>Für Schlüsselgeneration ECDSA:</i> digitalSignature	1 0-1 1	TRUE
	SubjectAltNames {2 5 29 17}	rfc822Name	0-1	FALSE
	BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE

	CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) <i>Für Zertifikate der eGK:</i> policyIdentifier = <oid_egk_aut> <i>Für Zertifikate der alternativen Versichertenidentitäten:</i> policyIdentifier = <oid_egk_aut_alt>	1 0-1 1 1	FALSE
	CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
	AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
	Admission {1 3 36 8 3 3}	professionItem = Beschreibung zu <oid_versicherter> gemäß [gemSpec_OID#GS-A_4442] professionOID = OID <oid_versicherter> gemäß gemSpec_OID#GS-A_4442	1 1	FALSE
	ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth	0-1	FALSE
	<i>andere Erweiterungen</i>		0	
signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS- A_4359]		
signature		Wert der Signatur		

5.1.3.2 C.CH.ENC – Verschlüsselung eGK

GS-A_4596 - Umsetzung Zertifikatsprofil C.CH.ENC

Der TSP-X.509 nonQES (eGK) MUSS C.CH.ENC gemäß Tab_PKI_233 umsetzen.

[<=]

Tabelle 23: Tab_PKI_233 C.CH.ENC Verschlüsselung eGK

Element		Inhalt	Kar.	
certificate		C.CH.ENC		
	tbsCertificate			
	version	2 (v3)		
	serialNumber	gemäß [RFC5280#4.1.2.2.]		
	signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt# GS- A_4362]		
	issuer	DN der ausstellenden CA		

		validity	Gültigkeit des Zertifikats (von - bis)		
		subject			
		CommonName	CN = Aufgedruckte Namenszeilen der Karte	1	
		title	Titel des Versicherten	0-1	
		givenName	Vorname des Versicherten	1	
		surname	Nachname des Versicherten	1	
		organizationalUnitName	OU = unveränderbarer Teil der KV-Nummer	1	
		organizationalUnitName	OU = Institutionskennzeichen	1	
		organizationName	O = Herausgeber	1	
		countryName	C = DE	1	
		subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4362] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers	1	
		extensions	Erweiterungen		critical
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Versicherten	1	FALSE
		KeyUsage {2 5 29 15}	<i>Für Schlüsselgeneration RSA:</i> keyEncipherment dataEncipherment <i>Für Schlüsselgeneration ECDSA:</i> keyAgreement	1 1 1	TRUE
		SubjectAltNames {2 5 29 17}	rfc822Name	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_egk_enc>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = Beschreibung zu <oid_versicherter> gemäß [gemSpec_OID#GS-A_4442]	1 1	FALSE

		professionOID = OID <oid_versicherter> gemäß gemSpec_OID#GS-A_4442		
	ExtendedKeyUsage {2 5 29 37}		0	
	andere Erweiterungen		0	
	signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt# GS- A_4362]		
	signature	Wert der Signatur		

1763 **5.1.3.3 C.CH.QES – Qualifizierte Signatur eGK (optional)**

1764 **Tabelle 24: Tab_PKI_234 C.CH.QES Qualifizierte Signatur eGK**

Element		Inhalt	Kar.	
certificate		C.CH.QES		
	tbsCertificate			
	version	2 (v3)		
	serialNumber	gemäß [RFC5280#4.1.2.2.]		
	signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt# GS-A_4358]		
	issuer	DN der ausstellenden CA		
	validity	Gültigkeit des Zertifikats (von - bis)		
	subject			
	CommonName	CN = Aufgedruckte Namenszeilen der Karte	1	
	title	Titel des Versicherten	0-1	
	givenName	Vorname des Versicherten	1	
	surname	Nachname des Versicherten	1	
	organizationalUnitName	OU = unveränderbarer Teil der KV- Nummer	1	
	organizationalUnitName	OU = Institutionskennzeichen	1	
	organizationName	O = Herausgeber	1	
	countryName	C = DE	1	
	subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS- A_4358] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers	1	

extensions	Erweiterungen		critical
SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Versicherten	1	FALSE
KeyUsage {2 5 29 15}	nonRepudiation	1	TRUE
BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_egk_qes>	1 0-1 1	FALSE
CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
SubjectDirectoryAttributes (2.5.29.9)	Angaben, die den Zertifikatsinhaber zusätzlich zu den Angaben unter 'subject' eindeutig identifizieren: Titel (optional), Geburtstag (optional), Geburtsort (optional), Geburtsname (optional)	0-1	FALSE
AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
Admission {1 3 36 8 3 3}	professionItem = Beschreibung zu <oid_versicherter> gemäß [gemSpec_OID#GS-A_4442] professionOID = OID <oid_versicherter> gemäß gemSpec_OID#GS-A_4442	1 1	FALSE
QCStatements (1.3.6.1.5.5.7.1.3)	id-qcs-pkixQCSyntax- v1(1.3.6.1.5.5.7.11.1) Konformität zu Syntax und Semantik nach [RFC3739] (optional) id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) Ausgabe des Zertifikats erfolgte konform zur Europäischen Richtlinie 1999/93/EG und nach dem Recht des Landes, nach dem die CA arbeitet. (obligatorisch)	1 1	FALSE
ExtendedKeyUsage {2 5 29 37}		0	
<i>andere Erweiterungen</i>		0	
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt# GS-A_4358]		
signature	Wert der Signatur		

5.1.3.4 C.CH.AUTN - Technische Authentisierung eGK

GS-A_4598 - Umsetzung Zertifikatsprofil C.CH.AUTN

Der TSP-X.509 nonQES (eGK) MUSS C.CH.AUTN gemäß Tab_PKI_235 umsetzen.

[<=]

Tabelle 25: Tab_PKI_235 C.CH.AUTN Technische Authentisierung eGK

Element		Inhalt	Kar.	
certificate		C.CH.AUTN		
	tbsCertificate			
	version	2 (v3)		
	serialNumber	gemäß [RFC5280#4.1.2.2.]		
	signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	issuer	DN der ausstellenden CA		
	validity	Gültigkeit des Zertifikats (von - bis)		
	subject			
	CommonName	CN = Pseudonym der Versichertenidentität	1	
	organizationalUnitName	OU = Institutionskennzeichen	1	
	organizationName	O = Herausgeber	1	
	countryName	C = DE	1	
	subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers	1	
	extensions			critical
	SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Versicherten	1	FALSE
	KeyUsage {2 5 29 15}	Für Schlüsselgeneration RSA: digitalSignature keyEncipherment Für Schlüsselgeneration ECDSA: digitalSignature	1 0-1 1	TRUE
	SubjectAltNames {2 5 29 17}	rfc822Name	0-1	FALSE
	BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE

	CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_egk_autn>	1 0-1 1	FALSE
	CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
	AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
	Admission {1 3 36 8 3 3}	professionItem = Beschreibung zu <oid_versicherter> gemäß [gemSpec_OID#GS-A_4442] professionOID = OID <oid_versicherter> gemäß gemSpec_OID#GS-A_4442	1 1	FALSE
	ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth	1	FALSE
	andere Erweiterungen		0	
signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS- A_4359]		
signature		Wert der Signatur		

1771 **5.1.3.5 C.CH.ENCV - Technische Verschlüsselung eGK**
 1772 **GS-A_4599 - Umsetzung Zertifikatsprofil C.CH.ENCV**
 1773 Der TSP-X.509 nonQES (eGK) MUSS C.CH.ENCV gemäß Tab_PKI_236 umsetzen.
 1774 [**<=**]

1775
 1776 **Tabelle 26: Tab_PKI_236 C.CH.ENCV Technische Verschlüsselung eGK**

Element		Inhalt	Kar.	
certificate		C.CH.ENCV		
	tbsCertificate			
	version	2 (v3)		
	serialNumber	gemäß [RFC5280#4.1.2.2.]		
	signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS- A_4362]		
	issuer	DN der ausstellenden CA)		
	validity	Gültigkeit des Zertifikats (von – bis)		

	subject			
	CommonName	CN = Pseudonym der Versichertenidentität	1	
	organizationalUnitName	OU = Institutionskennzeichen	1	
	organizationName	O = Herausgeber	1	
	countryName	C = DE	1	
	subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt# GS-A_4362] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers	1	
	extensions	Erweiterungen		critical
	SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Versicherten	1	FALSE
	KeyUsage {2 5 29 15}	<i>Für Schlüsselgeneration RSA:</i> keyEncipherment dataEncipherment <i>Für Schlüsselgeneration ECDSA:</i> keyAgreement	1 1 1	TRUE
	SubjectAltNames {2 5 29 17}	rfc822Name	0-1	FALSE
	BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
	CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_egk_encv>	1 0-1 1	FALSE
	CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
	AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
	Admission {1 3 36 8 3 3}	professionItem = Beschreibung zu <oid_versicherter> gemäß [gemSpec_OID#GS-A_4442] professionOID = OID <oid_versicherter> gemäß gemSpec_OID#GS-A_4442	1 1	FALSE
	ExtendedKeyUsage {2 5 29 37}		0	
	andere Erweiterungen		0	

signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4362]		
signature	Wert der Signatur		

1777 5.2 HBA – Heilberufsausweis

1778 GS-A_5042 - Kodierung der X.509-Zertifikate für HBA und SMC-B

1779 TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN bei der Herausgabe von Zertifikaten für
1780 HBA und SMC-B die übergreifenden Kodierungsvorschriften aus [gemSpec_PKI#4]
1781 umsetzen.

1782
1783 [\leq]

1784 5.2.1 X.509 Zertifikatsprofile des HBA

1785 5.2.1.1 C.HP.AUT – Authentisierung HBA

1786 GS-A_5531-01 - Umsetzung Zertifikatsprofil C.HP.AUT

1787 Der TSP-X.509 nonQES MUSS C.HP.AUT gemäß Tab_PKI_268_1 umsetzen. [\leq]

1788 Tabelle 27: Tab_PKI_268_1 C.HP.AUT Authentisierung HBA

Element	Inhalt *)	Kar.	
certificate	C.HP.AUT		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
issuer	Distinguished Name (DN) der Aussteller-CA gemäß [gemSpec_PKI# GS-A_4737]		
validity	Gültigkeit des Zertifikats (von – bis)		
subject			
commonName **)	Vor- und Nachname des Inhabers (bei Kürzung ev. Suffix :PN)	1	
title **)	nicht gesetzt	0	
givenName **)	Vornamen des Inhabers	1	
surName **)	Nachname des Inhabers	1	
serialNumber **)	Eindeutige Identifikationsnummer (dieselbe wie in ENC und QES)	1	

		organizationalUnitName	nicht gesetzt	0	
		organizationName	nicht gesetzt	0	
		countryName	DE	1	
		andere Attribute		0	
	subjectPublicKeyInfo		Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		critical
	extensions				
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Inhabers	1	FALSE
		KeyUsage {2 5 29 15}	Für Schlüsselgeneration RSA: digitalSignature keyEncipherment Für Schlüsselgeneration ECDSA: digitalSignature keyAgreement	1 1 1 1	TRUE
		SubjectAltNames {2 5 29 17}	rfc822Name = E-Mail-Adresse	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = <URL zur Publikation der Zertifikatsrichtlinie(n)> policyIdentifier = <oid_hba_aut> gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP-spezifischen Zertifikatsrichtlinie ggf. weitere sektorspezifische policyIdentifier und policyQualifierInfo	1 0-1 1 0-1 0-1 0-1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	admissionAuthority = {O=< zuständige Registrierungsstelle gemäß sektorspezifischer Ausprägung*>,C=DE} professionItem = gemäß [gemSpec_OID#GS-A_4442] professionOID = gemäß [gemSpec_OID#GS-A_4442]	1 1 1 1	FALSE

			registrationNumber = Telematik-ID des Inhabers		
		ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth keyPurposeId = id-kp- emailProtection	1 1	FALSE
		ValidityModel {1 3 6 1 4 1 8301 3 5}	nicht gesetzt	0	FALSE
		QCStatements {1 3 6 1 5 5 7 1 3}	nicht gesetzt	0	FALSE
		additionalInformation {1 3 36 8 3 15}	nicht gesetzt	0	FALSE
		Restriction {1 3 36 8 3 8}	nicht gesetzt	0	FALSE
		andere Erweiterungen		0	
		signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
		signature	Wert der Signatur		

1789 *) Sektorspezifische Ausprägungen der HBA-Zertifikate sind dem Anhang C zu
1790 entnehmen.

1791 **) Kodierung in einem SET als einziges Multivalued Relative Distinguished Name
1792 Element (multivaluedRDN) (siehe Hinweis unten unter Zusatzinformationen)

1793 5.2.1.2 C.HP.ENC – Verschlüsselung HBA

1794 GS-A_5532-01 - Umsetzung Zertifikatsprofil C.HP.ENC

1795 Der TSP-X.509 nonQES MUSS C.HP.ENC gemäß Tab_PKI_269_1 umsetzen.[<=]

1796 **Tabelle 281: Tab_PKI_269_1 C.HP.ENC Verschlüsselung HBA**

Element	Inhalt *)	Kar.	
certificate	C.HP.ENC		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
issuer	Distinguished Name (DN) der Aussteller-CA gemäß [gemSpec_PKI# GS-A_4737]		
validity	Gültigkeit des Zertifikats (von - bis)		
subject			

	commonName **)	Vor- und Nachname des Inhabers (bei Kürzung ev. Suffix :PN)	1	
	title **)	nicht gesetzt	0	
	givenName **)	Vornamen des Inhabers	1	
	surName **)	Nachname des Inhabers	1	
	serialNumber **)	Eindeutige Identifikationsnummer (dieselbe wie in AUT und QES)	1	
	organizationalUnitName	nicht gesetzt	0	
	organizationName	nicht gesetzt	0	
	countryName	DE	1	
	andere Attribute		0	
subjectPublicKeyInfo		Algorithmus gemäß [gemSpec_Krypt#GS-A_4362] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
extensions				critical
	SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Inhabers	1	FALSE
	KeyUsage {2 5 29 15}	Für Schlüsselgeneration RSA: keyEncipherment dataEncipherment Für Schlüsselgeneration ECDSA: keyAgreement	1 1 1	TRUE
	SubjectAltNames {2 5 29 17}	rfc822Name = E-Mail-Adresse	0-1	FALSE
	BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
	CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = <URL zur Publikation der Zertifikatsrichtlinie(n)> policyIdentifier = <oid_hba_enc> gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP-spezifischen Zertifikatsrichtlinie ggf. weitere sektorspezifische policyIdentifier und policyQualifierInfo	1 0-1 1 0-1 0-1 0-1	FALSE
	CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE

	AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
	Admission {1 3 36 8 3 3}	admissionAuthority = {O=< zuständige Registrierungsstelle gemäß sektorspezifischer Ausprägung*>,C=DE} professionItem = gemäß [gemSpec_OID#GS-A_4442] professionOID = gemäß [gemSpec_OID#GS-A_4442] registrationNumber = Telematik-ID des Inhabers	1 1 1	FALSE
	ExtendedKeyUsage {2 5 29 37}	nicht gesetzt	0	FALSE
	ValidityModel {1 3 6 1 4 1 8301 3 5}	nicht gesetzt	0	FALSE
	QCStatements {1 3 6 1 5 5 7 1 3}	nicht gesetzt	0	FALSE
	additionalInformation {1 3 36 8 3 15}	nicht gesetzt	0	FALSE
	Restriction {1 3 36 8 3 8}	nicht gesetzt	0	FALSE
	andere Erweiterungen		0	
signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
signature		Wert der Signatur		

1797 *) Sektorspezifische Ausprägungen der HBA-Zertifikate sind dem Anhang C zu
1798 entnehmen.

1799 **) Kodierung in einem SET als einziges Multivalued Relative Distinguished Name
1800 Element (multivaluedRDN) (siehe Hinweis unten unter Zusatzinformationen)

1801 5.2.1.3 C.HP.QES – Qualifizierte Signatur HBA

1802 GS-A_5533 - Umsetzung Zertifikatsprofil C.HP.QES

1803 Der TSP-X.509 QES MUSS C.HP.QES gemäß Tab_PKI_270 umsetzen.

1804 [\leq]

1805 GS-A_5533-01 - Umsetzung Zertifikatsprofil C.HP.QES

1806 Der TSP-X.509 QES MUSS C.HP.QES gemäß Tab_PKI_270_1 umsetzen.[\leq]

1807 Tabelle 29: Tab_PKI_270_1 C.HP.QES Qualifizierte Signatur HBA

Element		Inhalt *)	Kar.	
certificate		C.HP.QES		
	tbsCertificate			
	version	2 (v3)		

		serialNumber	gemäß [RFC5280#4.1.2.2.]		
		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4358]		
		issuer	Distinguished Name (DN) der Aussteller-CA gemäß [gemSpec_PKI# GS-A_4948]		
		validity	Gültigkeit des Zertifikats (von – bis)		
		subject			
		commonName **)	Vor- und Nachname des Inhabers (bei Kürzung ev. Suffix :PN)	1	
		title **)	nicht gesetzt	0	
		givenName **)	Vorname des Inhabers	1	
		surName **)	Nachname des Inhabers	1	
		serialNumber **)	Eindeutige Identifikationsnummer (dieselbe wie in AUT und ENC)	1	
		organizationalUnitName	nicht gesetzt	0	
		organizationName	nicht gesetzt	0	
		countryName	DE	1	
		andere Attribute		0	
		subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4358] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
		extensions			critical
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Inhabers	1	FALSE
		KeyUsage {2 5 29 15}	nonRepudiation (laut RFC5280 alternative Bezeichnung „contentCommitment“)	1	TRUE
		SubjectAltNames {2 5 29 17}	nicht gesetzt	0	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = <URL zur Publikation der Zertifikatsrichtlinie(n)> policyIdentifier = <oid_hba_qes> gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <id-etsi-qcp-natural-qscd> {0.4.0.194112.1.2} policyIdentifier = <OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP-	1 0-1 1 1 0-1 0-1 0-1	FALSE

			spezifischen Zertifikatsrichtlinie ggf. weitere sektorspezifische policyIdentifier und policyQualifierInfo		
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst URL des CA-Zertifikats (vgl. EN 319 412-2 Kap. 4.4.1)	1 0-1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	admissionAuthority = {O=< zuständige Registrierungsstelle gemäß sektorspezifischer Ausprägung*>,C=DE} professionItem = gemäß [gemSpec_OID#GS-A_4442] professionOID = gemäß [gemSpec_OID#GS-A_4442] registrationNumber : Details dazu jeweils in den sektorspezifischen Profilen in Anhang C	1 1 1 0-1	FALSE
		ExtendedKeyUsage {2 5 29 37}	nicht gesetzt	0	FALSE
		ValidityModel {1 3 6 1 4 1 8301 3 5}	id-validity-Model-chain {1 3 6 1 4 1 8301 3 5 1}	1	FALSE
		QCStatements {1 3 6 1 5 5 7 1 3}	esi4-qcStatement-1 mit id-etsi-qcs- QcCompliance {0 4 0 1862 1 1}, statementInfo nicht gesetzt esi4-qcStatement-2 mit id-etsi-qcs- QcLimitValue {0 4 0 1862 1 2}, statementInfo (currency = "EUR", amount (INT), exponent (INT)) esi4-qcStatement-3 mit id-etsi-qcs- QcRetentionPeriod {0 4 0 1862 1 3} esi4-qcStatement-4 mit id-etsi-qcs-QcSSCD {0 4 0 1862 1 4}, statementInfo nicht gesetzt esi4-qcStatement-5 mit id-etsi-qcs-QcPDS {0 4 0 1862 1 5} esi4-qcStatement-6 mit id-etsi-qct-esign {0 4 0 1862 1 6 1}	1 0-1 0-1 1 0-1 0-1	FALSE
		additionalInformation {1 3 36 8 3 15}	nicht gesetzt	0	FALSE
		Restriction {1 3 36 8 3 8}	Falls das optionale esi4-qcStatement-2 gesetzt und/ oder hier ein Freitext enthalten ist, muss diese Erweiterung mindestens die folgende Ergänzung enthalten: <i>Jegliche Beschränkungen gelten nicht für Anwendungen gemäß § 291a SGB V.</i>	0-1	FALSE

		andere Erweiterungen		0	
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4358]		
	signature		Wert der Signatur		

*) Sektorspezifische Ausprägungen der HBA-Zertifikate sind dem Anhang C zu entnehmen.

**) Kodierung in einem SET als einziges Multivalued Relative Distinguished Name Element (multivaluedRDN) (siehe Hinweis unten unter Zusatzinformationen)

Zusatzinformationen zu einzelnen Feldern:

- **SubjectDN**

Bildungsregel-Vorschlag gemäß Informationen aus bisherigen Sektor-Spezifikationen:

$CN=[Vollst.Name (:PN)] + GN=[Vornamen]+SN=[Nachname]+SerNr=[int],C=DE$

Hinweis: Die Plus- und Komma-Zeichen sind in der Kodierung des SubjectDN nicht enthalten – dienen hier lediglich als Trenn-Markierung zwischen den Feldinhalten (siehe auch [RFC4514]).

Kürzungsregel-Hinweis für den CN (entnommen aus bisheriger Sektor-Spezifikation):

„Der commonName enthält den vollständigen Namen des Inhabers, ohne akademische Titel (auch wenn sie im Personalausweis des Antragstellers eingetragen sind). Die Länge des Attributes ist auf 64 Zeichen beschränkt. Falls der vollständige Name nicht aufgenommen werden kann (z. B. weil er zu lang ist), dann muss, nur dann, wenn dies aus gesetzlichen Bestimmungen hervorgeht, der commonName als Pseudonym gekennzeichnet werden. In diesem Fall muss der Zusatz „:PN“ (ohne Anführungsstriche) aufgenommen werden; die effektive Länge reduziert sich damit auf 61 Zeichen. Falls eine Kürzung vorgenommen werden soll, entsprechen die Kürzungsregeln den Regelungen in der eGK-Spezifikation:

- Rufname und Nachname bleiben vollständig, Vornamen werden auf den ersten Buchstaben plus Punktzeichen gekürzt
- falls immer noch >61 bzw. 64 Zeichen: der Nachname wird gekürzt und mit Punktzeichen gekennzeichnet, so dass die Gesamtlänge (ggf. inkl. :PN) 64 Zeichen beträgt“

- **SubjectSerialNumber**

Zusätzliche Hinweise gemäß Informationen aus bisherigen Sektor-Spezifikationen:

Das Attribut serialNumber im ENC und AUT-Zertifikat soll den gleichen Wert wie im QES-Zertifikat haben. Hiermit soll ermöglicht werden, dass mit einem präsentierten AUT-Zertifikat leichter das entsprechende ENC-Zertifikat desselben HBAs, mittels Konstruktion des DN, aufgefunden werden kann.

Bildungs-Vorschlag für subjectSerialNumber:

$subjectSerialNumber = <TSP-ID>.<ICCSN>$

(<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)

1847 *Hinweis: Statt der ICCSN in der Bildungsregel können auch andere TSP-*
1848 *spezifische IDs verwendet werden, die der Länge der ICCSN entsprechen.*

- 1849 • **serialNumber, givenName, surname, title und commonName als SET-**
1850 **OF**

1851 Die Attribute serialNumber, givenName, surname, ggf. title und commonName werden in
1852 einem SET-OF als ein einziges multivaluedRDN kodiert. Die entsprechenden
1853 Kodierungsregeln von X.690 Abs. 11.6 "Set-of components" und RFC_5280 Anhang B
1854 (Reihenfolge im SET) müssen berücksichtigt werden. Attribute im RDN müssen anhand
1855 der String-Länge der Attribut-Werte, in aufsteigender Reihenfolge sortiert, in die
1856 Kodierung einfließen.

1857 **5.3 SMC-B – Ausweis einer Organisation/Einrichtung des** 1858 **Gesundheitswesens**

1859 Die SMC Typ B definiert die Identität einer Organisation oder Einrichtung des
1860 Gesundheitswesens (z. B. Arztpraxis, Krankenhaus, Apotheke, Betriebsstätte nicht-
1861 ärztlicher Psychotherapeut oder auch Geschäftsstellen von Kostenträgern) und wird
1862 deshalb auch „Institutionenkarte“ genannt.

1863 Bzgl. Nutzung bestehender LE-Datensätze für SMC-B-Zertifikate ist die Anforderung GS-
1864 A_4970 (s. Kap. 5.2) zu berücksichtigen.

1865 **5.3.1 Definition der Organisationsidentität**

1866 Der eindeutige Identitätsname der Organisation wird durch folgende Felder gebildet:

- 1867 • **commonName**
1868 • **organizationName**
1869 • **countryName**

1870 Die serialNumber kann weiterhin als technisches Unterscheidungsmerkmal (falls mittels
1871 commonName und organizationName bei einem Issuer keine Eindeutigkeit des Subjects
1872 erreicht werden kann) im SubjectDN dienen.

1873 Der eindeutige Identitätsschlüssel der Organisation oder Einrichtung des
1874 Gesundheitswesens wird durch die Telematik-ID in der Zertifikatserweiterung
1875 „Admission“ abgebildet; s. Abschnitt 4.6.

1876 **GS-A_4971 - Zuordnung von SMC-B zur Institution**

1877 Die Kartenherausgeber MÜSSEN die eindeutige Zuordnung von SMC-B zur berechtigten
1878 Institution sicherstellen.
1879 [**<=**]

1880 Der Zugriff eines Leistungserbringers auf medizinische Daten von Anwendungen der
1881 elektronischen Gesundheitskarte gemäß §291a SGB V mit einer SMC-B darf nur in
1882 Verbindung mit einem HBA erfolgen.

1883 **A_15190 - HBA als Grundlage zur Nutzung von medizinischen Anwendungen**

1884 Die Kartenherausgeber von SMC-B, welche Leistungserbringern den Zugriff auf Daten
1885 von Anwendungen der elektronischen Gesundheitskarte gemäß §291a SGB V ermöglicht,
1886 MÜSSEN mittels organisatorischer oder technischer Maßnahmen sicherstellen, dass der

1887 Nutzer der SMC-B entweder selbst über einen HBA verfügt oder zu einer Institution
1888 gehört, der ein HBA zur Verfügung steht.[<=]

1889 Hinweis 1: Von dieser Regelung sind SM-B für Gesellschafterorganisationen (ohne CVC)
1890 oder Kostenträger (Zugriffsprofil CHA.8 [gemSpec_PKI#Tab_PKI_254]) nicht betroffen,
1891 da sie keinen Zugriff auf die entsprechenden Daten erlauben. Ebenso sind SM-B mit
1892 Zugriffsprofil CHA.1 [gemSpec_PKI#Tab_PKI_254] nicht betroffen, da sie dem Zugriff
1893 des Versicherten selbst in der KTR-AdV-Umgebung dienen.

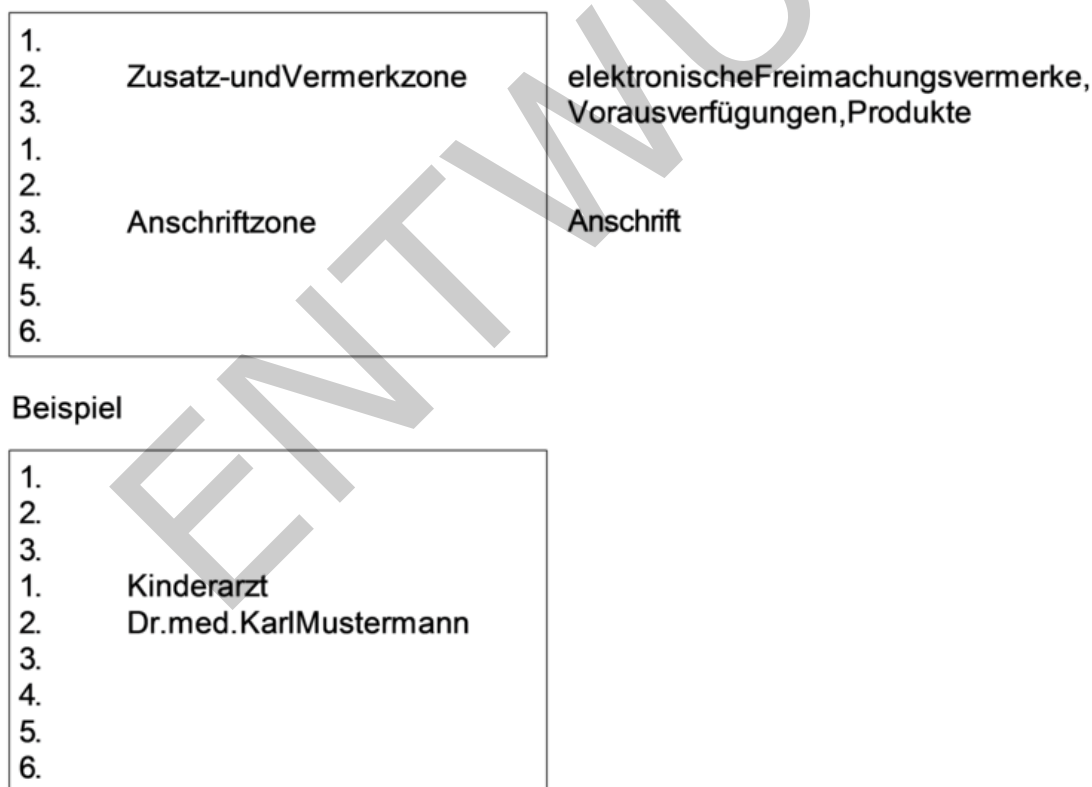
1894 Hinweis 2: Ein HBA im Sinne dieser Anforderung ist ein HBA oder eine HBA-
1895 Vorläuferkarte (HBA-qSig und ZOD_2.0).

1896 5.3.2 Aufbau Anschriftzone nach [DIN5008]

1897 Die ersten zwei Zeilen der Anschriftzone werden für den Inhalt des `commonName`
1898 verwendet.

1899 Der `commonName` beinhaltet somit den „Kurzname“ der Institution, so wie sie sich selbst
1900 auf dem Anschriftenfeld findet. Da dieses Feld von der Institution frei gestaltet werden
1901 kann, ist nachfolgend nur eine exemplarische Variante abgebildet. Die Art der Institution
1902 ist eindeutig in der Admission Extension hinterlegt.

1903



Beispiel

1904

1905

1906

Abbildung 4: Das Anschriftenfeld nach DIN5008

1907 *Hinweis: Für den Sonderfall der „Berufsausübungsgemeinschaften“ (ehemals*
1908 *„Gemeinschaftspraxen“) gilt die Ausnahme, dass die Zeile 2 der Anschriftzone [DIN5008]*
1909 *optional ist. Somit ist Zeile 1 Pflichtfeld, die Zeilen 3 und/oder 4 sind wie Zeile 2 optional,*
1910 *um darüber die Praxisbezeichnung (Bsp. „Praxis Bülowbogen“) mit aufzunehmen.*

1911 **5.3.3 Umgang mit überlangen Attributen im SubjectDN**

1912 Siehe Kapitel 4.8.3.5 „SubjectAltNames“.
1913

1914 **5.3.4 X.509 Zertifikatsprofile der SMC-B**

1915 **5.3.4.1 C.HCI.AUT – Authentisierung SMC- B**

1916 **GS-A_4600 - Umsetzung Zertifikatsprofil C.HCI.AUT**

1917 Der TSP-X.509 nonQES MUSS C.HCI.AUT gemäßTab_PKI_238 umsetzen.
1918 [\leq]

1919

1920 **Tabelle 30: Tab_PKI_238 C.HCI.AUT Authentisierung SMC-B**

Element		Inhalt *)	Kar.	
certificate		C.HCI.AUT		
	tbsCertificate			
		version	2 (v3)	
		serialNumber	gemäß [RFC5280#4.1.2.2.]	
		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]	
		issuer	Distinguished Name (DN) der Aussteller-CA	
		validity	Gültigkeit des Zertifikats (von – bis)	
		subject		
		commonName	Erste zwei Zeilen des Adressenfeldes	1
		title	Titel des Verantwortlichen/Inhabers	0-1
		givenName	Vorname des Verantwortlichen/Inhabers	0-1
		surName	Nachname des Verantwortlichen/Inhabers	0-1
		serialNumber	Ti-weit eindeutige Identifikationsnummer	0-1
		organizationalUnitName	Organisationseinheit der Organisation/Einrichtung des Gesundheitswesens	0-1
		organizationName	Name der Organisation/Einrichtung des Gesundheitswesens	0-1
		streetAddress	Strasse, Hausnummer	0-1
		postalCode	Postleitzahl	0-1
		localityName	Stadt	0-1
		stateOrProvinceName	Bundesland	0-1

		countryName	DE	1	
		andere Attribute		0	
		subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		critical
		extensions			
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels der Organisation/Einrichtung des Gesundheitswesens	1	FALSE
		KeyUsage {2 5 29 15}	Für Schlüsselgeneration RSA: digitalSignature keyEncipherment Für Schlüsselgeneration ECDSA: digitalSignature	1 1 1	TRUE
		SubjectAltNames {2 5 29 17}	rfc822Name ggf. überlange Institutionsnamen, Alternativnamen oder Ergänzungen	0-1 0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_smc_b_aut> policyIdentifier = <OID d. TSP-spezifischen Policy>	1 0-1 1 0-1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	admissionAuthority = {O=<zuständige Registrierungsstelle gemäß sektorspezifischer Ausprägung*>,C=DE} professionItem = Beschreibung der Institution gemäß [gemSpec_OID#GS- A_4443] professionOID = OID der Institution gemäß [gemSpec_OID#GS-A_4443] registrationNumber = Telematik-ID der Institution	0-1 1 1 1	FALSE
		ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth	1	FALSE

		andere Erweiterungen		0	
	signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]			
	signature	Wert der Signatur			

1921 *) Sektorspezifische Ausprägungen der SMC-B Zertifikate sind dem Anhang A zu
1922 entnehmen

1923 5.3.4.2 C.HCI.ENC – Verschlüsselung SMC-B

1924 GS-A_4601 - Umsetzung Zertifikatsprofil C.HCI.ENC

1925 Der TSP-X.509 nonQES MUSS C.HCI.ENC gemäß Tab Tab_PKI_239 umsetzen.

1926 [\leq]

1927

1928 Tabelle 31: Tab_PKI_239 C.HCI.ENC Verschlüsselung SMC-B

Element		Inhalt *)	Kar.	
certificate		C.HCI.ENC		
	tbsCertificate			
	version	2 (v3)		
	serialNumber	gemäß [RFC5280#4.1.2.2.]		
	signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4362]		
	issuer	Distinguished Name (DN) der Aussteller-CA		
	validity	Gültigkeit des Zertifikats (von – bis)		
	subject			
	commonName	Erste zwei Zeilen des Adressenfeldes	1	
	title	Titel des Verantwortlichen/Inhabers	0-1	
	givenName	Vorname des Verantwortlichen/Inhabers	0-1	
	surName	Nachname des Verantwortlichen/Inhabers	0-1	
	serialNumber	TI-weit eindeutige Identifikationsnummer	0-1	
	organizationalUnitName	Organisationseinheit der Organisation/Einrichtung des Gesundheitswesens	0-1	
	organizationName	Name der Organisation/Einrichtung des Gesundheitswesens	0-1	
	streetAddress	Strasse, Hausnummer	0-1	
	postalCode	Postleitzahl	0-1	

			localityName	Stadt	0-1	
			stateOrProvinceName	Bundesland	0-1	
			countryName	DE	1	
			andere Attribute		0	
			subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt# GS-A_4362] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		critical
			extensions			
			SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels der Organisation/Einrichtung des Gesundheitswesens	1	
			KeyUsage {2 5 29 15}	Für Schlüsselgeneration RSA: keyEncipherment dataEncipherment Für Schlüsselgeneration ECDSA: keyAgreement	1 1 1	
			SubjectAltNames {2 5 29 17}	rfc822Name ggf. überlange Institutionsnamen, Alternativnamen oder Ergänzungen	0-1 0-1	
			BasicConstraints {2 5 29 19}	ca = FALSE	1	
			CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_smc_b_enc> policyIdentifier = <OID d. TSP-spezifischen Policy>	1 0-1 1 0-1	
			CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	
			AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
			Admission {1 3 36 8 3 3}	admissionAuthority = {O=<zuständige Registrierungsstelle gemäß sektorspezifischer Ausprägung*>,C=DE} professionItem = Beschreibung der Institution gemäß [gemSpec_OID#GS-A_4443] professionOID = OID der Institution gemäß [gemSpec_OID#GS-A_4443] registrationNumber = Telematik-ID der Institution	0-1 1 1 1	FALSE

		ExtendedKeyUsage {2 5 29 37}		0	
		<i>andere Erweiterungen</i>		0	
signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4362]			
signature		Wert der Signatur			

1929 *) Sektorspezifische Ausprägungen der SMC-B Zertifikate sind dem Anhang A zu
1930 entnehmen

1931 5.3.4.3 C.HCI.OSIG – Signatur SMC-B

1932 GS-A_4602 - Umsetzung Zertifikatsprofil C.HCI.OSIG

1933 Der TSP-X.509 nonQES MUSS C.HCI.OSIG gemäß Tab_PKI_240 umsetzen.
1934 [\leq]

1935

1936 **Tabelle 32: Tab_PKI_240 C.HCI.OSIG Signatur SMC-B**

Element		Inhalt *)	Kar.	
certificate		C.HCI.OSIG		
	tbsCertificate			
	version	2 (v3)		
	serialNumber	gemäß [RFC5280#4.1.2.2.]		
	signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
	issuer	Distinguished Name (DN) der Aussteller-CA		
	validity	Gültigkeit des Zertifikats (von – bis)		
	subject			
	commonName	Erste zwei Zeilen des Anschriftenfeldes	1	
	title	Titel des Verantwortlichen/Inhabers	0-1	
	givenName	Vorname des Verantwortlichen/Inhabers	0-1	
	surName	Nachname des Verantwortlichen/Inhabers	0-1	
	serialNumber	Ti-weit eindeutige Identifikationsnummer	0-1	
	organizationalUnitName	Organisationseinheit der Organisation/Einrichtung des Gesundheitswesens	0-1	
	organizationName	Name der Organisation/Einrichtung des Gesundheitswesens	0-1	

			streetAddress	Strasse, Hausnummer	0-1	
			postalCode	Postleitzahl	0-1	
			localityName	Stadt	0-1	
			stateOrProvinceName	Bundesland	0-1	
			countryName	DE	1	
			andere Attribute		0	
			subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4357] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		critical
			extensions			
			SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels der Organisation/Einrichtung des Gesundheitswesens	1	FALSE
			KeyUsage {2 5 29 15}	nonRepudiation	1	TRUE
			SubjectAltNames {2 5 29 17}	rfc822Name ggf. überlange Institutionsnamen, Alternativnamen oder Ergänzungen	0-1 0-1	FALSE
			BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
			CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_smc_b_osig> policyIdentifier = <OID d. TSP-spezifischen Policy>	1 0-1 1 0-1	FALSE
			CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
			AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
			Admission {1 3 36 8 3 3}	admissionAuthority = {O=<zuständige Registrierungsstelle gemäß sektorspezifischer Ausprägung*>,C=DE} professionItem = Beschreibung der Institution gemäß [gemSpec_OID#GS-A_4443] professionOID = OID der Institution gemäß [gemSpec_OID#GS-A_4443] registrationNumber = Telematik-ID der Institution	0-1 1 1 1	FALSE

		ExtendedKeyUsage {2 5 29 37}		0	
		andere Erweiterungen		0	
	signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS- A_4357]			
	signature	Wert der Signatur			

1937 *) Sektorspezifische Ausprägungen der SMC-B Zertifikate sind dem Anhang A zu
1938 entnehmen

1939 5.4 HSM-B – Ausweis einer Organisation/Einrichtung des 1940 Gesundheitswesens

1941 Bestehen höhere Performance-Anforderungen an eine SMC-B (z. B. in Krankenhäusern),
1942 kann als funktionales Äquivalent eine HSM-basierte Lösung eingesetzt werden. Gemäß
1943 Anforderung [gemKPT_PKI_TIP#TIP1-A_2084] sind die X.509-Zertifikate eines HSM-B
1944 entsprechend den Festlegungen der X.509-Zertifikate für SMC-B auszuführen.

1945 5.5 gSMC-KT – eHealth-Kartenterminal

1946 Für gSMC-KT ausgestellte Zertifikate werden nicht statusgeprüft. Für diese Zertifikate
1947 muss ein TSP somit keinen Sperrdienst und keine Statusauskünfte bereitstellen.

1948 Siehe dazu auch Anhang A der [gemRL_TSL_SP_CP#AnhA].

1949 Das Zertifikat eines gSMC-KT enthält nur Informationen über die Identität des SMKT, des
1950 Geräteherstellers sowie des Zertifikateherausgebers. Die Bedeutung des Zertifikats
1951 beschränkt sich auf folgende Aspekte:

- 1952 • die gSMC-KT basiert auf einer hierfür durch die gematik zugelassenen
1953 Chipkartenplattform
- 1954 • das Zertifikat wurde durch einen hierfür durch die gematik zugelassenen TSP-
1955 X.509 nonQES an einen KT-Hersteller ausgestellt

1956 Das Zertifikat eines gSMC-KT repräsentiert nach dem Pairing die Identität eines eHealth-
1957 Kartenterminals.

1958 5.5.1 Definition der Kartenterminalidentität

1959 Die Identität einer gSMC-KT ist durch den *SubjectDN* (*subject distinguishedName*) des
1960 Zertifikats gegeben mit folgendem Aufbau:

- 1961 • **commonName** = [ICCSN des gSMC-KT]
- 1962 • **organizationName** = [Name des Kartenterminal-Herstellers],
- 1963 • **countryName** = [Herkunftsland des Kartenterminal-Herstellers]

1964 **5.5.2 X.509 Zertifikatsprofile der gSMC-KT**

1965 **5.5.2.1 C.SMKT.AUT – Identität der gSMC-KT**

1966 **GS-A_4604 - Umsetzung Zertifikatsprofil C.SMKT.AUT**

1967 Der TSP-X.509 nonQES MUSS C.SMKT.AUT gemäß Tab_PKI_241 umsetzen.

1968 [\leq]

1969

1970 **Tabelle 33: Tab_PKI_241 C.SMKT.AUT gSMC-KT**

Element		Inhalt	Kar.	
certificate		C.SMKT.AUT		
	tbsCertificate			
	version	2 (v3)		
	serialNumber	gemäß [RFC5280#4.1.2.2.]		
	signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	issuer	DN der ausstellenden CA		
	validity	Gültigkeit des Zertifikats (von – bis)		
	subject			
	commonName	ICCSN der gSMC-KT	1	
	organizationalUnitName	Relevante Einheit des Kartenterminal-Herstellers	0-1	
	organizationName	Name des Kartenterminal-Herstellers	1	
	countryName	Herkunftsland des Kartenterminal-Herstellers	1	
	andere Attribute		0	
	subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
	extensions			critical

	SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Kartenterminals	1	FALSE
	KeyUsage {2 5 29 15}	<i>Für Schlüsselgeneration RSA:</i> digitalSignature keyEncipherment <i>Für Schlüsselgeneration ECDSA:</i> digitalSignature	1 1 1	TRUE
	SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Kartenterminal-Herstellers	0-1	FALSE
	BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
	CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_smkt_aut>	1 0-1 1	FALSE
	CRLDistributionPoints {2 5 29 31}		0	FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}		0	FALSE
	AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
	Admission {1 3 36 8 3 3}	professionItem = Beschreibung zu <oid_kt> gemäß [gemSpec_OID#GS-A_4446] professionOID = OID <oid_kt> gemäß [gemSpec_OID#GS-A_4446]	1 1	FALSE
	ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-serverAuth	1	FALSE
	andere Erweiterungen		0	
signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
signature		Wert der Signatur		

1971 5.6 gSMC-K – Konnektor

1972 5.6.1 Definition und Zuweisung der Konnektoridentität

1973 Die Identität einer gSMC-K wird durch die ICCSN in Verbindung mit dem Datum der
1974 erstmaligen Zertifizierung der gSMC-K gebildet.

GS-A_4605 - Verwendung registrierter Daten für gSMC-K-Zertifikatsbeantragung

Der Konnektor-Hersteller MUSS sicherstellen, dass bei der Beantragung von X.509-Zertifikaten für Konnektoren für die Felder `SubjectDN` nur die Werte verwendet werden, die im Rahmen seiner Zulassung registriert sind.

[<=]

GS-A_4606 - Identischer ICCSN in allen Zertifikaten einer gSMC-K

Der Konnektor-Hersteller MUSS sicherstellen, dass bei der Beantragung der X.509-Zertifikate für die zu einer gSMC-K gehörenden Zertifikate der Wert ICCSN für das Feld `commonName` in allen drei zu einer gSMC-K gehörenden Zertifikaten identisch angegeben wird.

[<=]

GS-A_4607 - Zuordnung Konnektorinstanz zu verbauter gSMC-K

Der Konnektorhersteller MUSS den Zusammenhang zwischen Konnektorinstanz sowie der darin verbauten gSMC-K dokumentieren und hierüber gegenüber der gematik jederzeit Auskunft geben können.

[<=]

5.6.2 Aufbau des SubjectDN

Der *SubjectDN* (*subject distinguishedName*) des Zertifikats verbindet die ICCSN mit der Identität des Herstellers und sichert damit die Rückverfolgbarkeit jeder Zertifikatsverwendung eines der Konnektorzertifikate:

- `commonName` = [ICCSN der gSMC-K] + "-" + [Kartenausgabedatum in der Form JJJJMMTT]
- `organizationName` = [Name des Konnektor-Herstellers],
- `countryName` = [Herkunftsland des Konnektor-Herstellers]

5.6.3 Statusprüfung von Konnektorzertifikaten

GS-A_4608 - Statusprüfung von Konnektorzertifikaten

Der TSP-X.509 nonQES MUSS für die von ihm ausgestellten X.509-Zertifikate des Konnektors eine Statusprüfung per OCSP gemäß Tabelle Tab_PKI_237 sowohl in der TI als auch im Internet vorsehen.[<=]

Tabelle 34: Tab_PKI_237 Statusprüfung von Konnektorzertifikaten

Konnektorzertifikat	Statusprüfung per OCSP	Bereitstellung Statusinformation
C.NK.VPN	Ja	MUSS
C.AK.AUT	Ja	MUSS
C.SAK.AUT	Ja	MUSS

2008 **5.6.4 X.509 Zertifikatsprofile des Konnektors**

2009 **5.6.4.1 C.NK.VPN – VPN-Authentisierung Netzkonnektor**

2010 Die Identität des Netzkonnektors dient der Authentisierung gegenüber den zentralen
2011 Netzwerkdiensten und wird für die Anmeldung an den VPN-Konzentratoren genutzt.

2012 **GS-A_4609 - Umsetzung Zertifikatsprofil C.NK.VPN**

2013 Der TSP-X.509 nonQES MUSS C.NK.VPN gemäß Tab_PKI_242 umsetzen.

2014 [\leq]

2015

2016 **Tabelle 35: Tab_PKI_242 Zertifikatsprofil C.NK.VPN VPN-Authentisierung Netzkonnektor**

Element		Inhalt	Kar.	
certificate		C.NK.VPN		
	tbsCertificate			
	version	2 (v3)		
	serialNumber	gemäß [RFC5280#4.1.2.2.]		
	signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4360]		
	issuer	DN der ausstellenden CA		
	validity	Gültigkeit des Zertifikats (von – bis)		
	subject			
	commonName	<ICCSN der gSMC-K>- <Kartenausgabedatum in der Form JJJJMMTT >	1	
	organizationalUnitName	Relevante Einheit des Konnektor- Herstellers	0-1	
	organizationName	Name des Konnektor-Herstellers	1	
	streetAddress	Anschrift des Konnektor-Herstellers	0-1	
	postalCode	Postleitzahl der Anschrift des Konnektor- Herstellers	0-1	
	localityName	Stadt der Anschrift des Konnektor- Herstellers	0-1	
	stateOrProvinceName	Bundesland der Anschrift des Konnektor- Herstellers	0-1	
	countryName	Herkunftsland des Konnektor-Herstellers	1	
	andere Attribute		0	
	subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt# GS-A_4360] und individueller Wert des		

		öffentlichen Schlüssels des Zertifikatsinhabers		
	extensions			critical
	SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Konnektors	1	FALSE
	KeyUsage {2 5 29 15}	<i>Für Schlüsselgeneration RSA:</i> digitalSignature keyEncipherment <i>Für Schlüsselgeneration ECDSA:</i> digitalSignature	1 1 1	TRUE
	SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Konnektor-Herstellers	0-1	FALSE
	BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
	CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_nk_vpn>	1 0-1 1	FALSE
	CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
	AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
	Admission {1 3 36 8 3 3}	professionItem = Beschreibung zu <oid_nk> gemäß [gemSpec_OID#GS- A_4446] professionOID = OID <oid_nk> gemäß [gemSpec_OID#GS-A_4446]	1 1	FALSE
	ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth keyPurposeId = id-kp-serverAuth	1 1	FALSE
	andere Erweiterungen		0	
	signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS- A_4360]		
	signature	Wert der Signatur		

2017 5.6.4.2 C.AK.AUT - Authentisierung Anwendungskonnektor

2018 Die Identität des Anwendungskonnektors dient der Authentisierung für TLS-Verbindungen
2019 gegenüber dem Primärsystem.

2020 **GS-A_4610 - Umsetzung Zertifikatsprofil C.AK.AUT**
 2021 Der TSP-X.509 nonQES MUSS C.AK.AUT gemäß Tab_PKI_243 umsetzen.
 2022 [\leq]

2023

2024 **Tabelle 36: Tab_PKI_243 Zertifikatsprofil C.AK.AUT Authentisierung**
 2025 **Anwendungskonnektor**

Element	Inhalt	Kar.	
certificate	C.AK.AUT		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
issuer	DN der ausstellenden CA		
validity	Gültigkeit des Zertifikats (von – bis)		
subject			
commonName	<ICCSN der gSMC-K>-< Kartenausgabedatum in der Form JJJJMMTT >	1	
organizationalUnitName	Relevante Einheit des Konnektor-Herstellers	0-1	
organizationName	Name des Konnektor-Herstellers	1	
streetAddress	Anschrift des Konnektor-Herstellers	0-1	
postalCode	Postleitzahl der Anschrift des Konnektor-Herstellers	0-1	
localityName	Stadt der Anschrift desKonnektor-Herstellers	0-1	
stateOrProvinceName	Bundesland der Anschrift des Konnektor-Herstellers	0-1	
countryName	Herkunftsland des Konnektor-Herstellers	1	
andere Attribute		0	
subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
extensions			critical

	SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Konnektors	1	FALSE
	KeyUsage {2 5 29 15}	<i>Für Schlüsselgeneration RSA:</i> digitalSignature keyEncipherment <i>Für Schlüsselgeneration ECDSA:</i> digitalSignature	1 1 1	TRUE
	SubjectAltNames {2 5 29 17}	dNSName = „konnektor.konlan“ bei überlangem organizationName: Langname des Konnektor-Herstellers	1 0-1	FALSE
	BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
	CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_ak_aut>	1 0-1 1	FALSE
	CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
	AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
	Admission {1 3 36 8 3 3}	professionItem = Beschreibung zu <oid_ak> gemäß [gemSpec_OID#GS-A_4446] professionOID = OID <oid_ak> gemäß [gemSpec_OID#GS-A_4446]	1 1	FALSE
	ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth keyPurposeId = id-kp-serverAuth	1 1	FALSE
	andere Erweiterungen		0	
signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
signature		Wert der Signatur		

5.6.4.3 C.SAK.AUT - Authentisierung Signaturdienst

Die Identität des Signaturdienstes dient zur Authentisierung gegenüber den Kartenterminals. Darüber hinaus muss sich der Signaturdienst des Konnektors gegenüber dem Heilberufsausweis mittels eines CV-Zertifikats (C.SAK.AUTD_CVC) mit einer spezifischen Rolle (Profil) ausweisen, um Stapelsignaturen durchführen zu können.

GS-A_4611 - Umsetzung Zertifikatsprofil C.SAK.AUT

Der TSP-X.509 nonQES MUSS C.SAK.AUT gemäß Tab_PKI_244 umsetzen.

[<=]

2034

2035

Tabelle 37: Tab_PKI_244 Zertifikatsprofil C.SAK.AUT Authentisierung SAK

Element		Inhalt	Kar.	
certificate		C.SAK.AUT		
	tbsCertificate			
	version	2 (v3)		
	serialNumber	gemäß [RFC5280#4.1.2.2.]		
	signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	issuer	DN der ausstellenden CA		
	validity	Gültigkeit des Zertifikats (von – bis)		
	subject			
	commonName	<ICCSN der gSMC-K>-<Kartenausgabedatum in der Form JJJJMMTT>	1	
	organizationalUnitName	Relevante Einheit des Konnektor-Herstellers	0-1	
	organizationName	Name des Konnektor-Herstellers	1	
	streetAddress	Anschrift des Konnektor-Herstellers	0-1	
	postalCode	Postleitzahl der Anschrift des Konnektor-Herstellers	0-1	
	localityName	Stadt der Anschrift des Konnektor-Herstellers	0-1	
	stateOrProvinceName	Bundesland der Anschrift des Konnektor-Herstellers	0-1	
	countryName	Herkunftsland des Konnektor-Herstellers	1	
	andere Attribute		0	
	subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
	extensions			critical
	SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Konnektors	1	FALSE
	KeyUsage {2 5 29 15}	Für Schlüsselgeneration RSA: digitalSignature keyEncipherment	1 1	TRUE

			Für Schlüsselgeneration ECDSA: digitalSignature	1	
	SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Konnektor-Herstellers		0-1	FALSE
	BasicConstraints {2 5 29 19}	ca = FALSE		1	TRUE
	CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_sak_aut>		1 0-1 1	FALSE
	CRLDistributionPoints {2 5 29 31}	keine Festlegung		0-1	FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst		1	FALSE
	AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA		1	FALSE
	Admission {1 3 36 8 3 3}	professionItem = Beschreibung zu <oid_sak> gemäß [gemSpec_OID#GS- A_4446] professionOID = OID <oid_sak> gemäß [gemSpec_OID#GS-A_4446]		1 1	FALSE
	ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth keyPurposeId = id-kp-serverAuth		1 1	FALSE
	andere Erweiterungen			0	
	signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS- A_4359]			
	signature	Wert der Signatur			

2036 5.7 VPN-Zugangsdienst

2037 Der VPN-Zugangsdienst ermöglicht den Konnektoren einerseits einen IPsec-Tunnel über
2038 ein Transportnetz zum VPN-Zugangsdienst und verbindet darüber die Organisationen des
2039 Gesundheitswesens mit dem zentralen Netz der TI, zusätzlich ermöglicht er den
2040 Konnektoren den Aufbau eines separaten IPsec-Tunnels über das Transportnetz, durch
2041 den der sichere Internetzugang erreichbar ist. Für diesen Zweck ist eine separate
2042 kryptographische Identität vorgesehen.

2043 5.7.1 Definition und Zuweisung der Zugangsdienstidentitäten

2044 Die beiden Identitäten des Zugangsdienstes werden durch den jeweiligen FQDN des
2045 Dienstes in Verbindung mit einem zusätzlichen Instanzenkennzeichen gebildet.

2046 Bzgl. Verwendung des FQDN ist die Anforderung GS-A_4720 (s. Kap. 5.9.1) zu
2047 berücksichtigen.

2048 **5.7.2 Aufbau des SubjectDN**

2049 Siehe Tab_PKI_245.

2050 **5.7.3 X.509-Zertifikatsprofile des Zugangsdienstes**

2051 **5.7.3.1 C.VPNK.VPN - VPN-Authentisierung Zugangsdienst TI**

2052 **GS-A_4613 - Umsetzung Zertifikatsprofil C.VPNK.VPN**

2053 Der TSP-X.509 nonQES MUSS C.VPNK.VPN gemäß Tab_PKI_245 umsetzen.

2054 [\leq]

2055

2056 **Tabelle 38: Tab_PKI_245 Zertifikatsprofil C.VPNK.VPN VPN-Authentisierung**
2057 **Zugangsdienst TI**

Element	Inhalt	Kar.	
certificate	C.VPNK.VPN		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4360]		
issuer	DN der ausstellenden CA		
validity	Gültigkeit des Zertifikats (von – bis)		
subject			
commonName	FQDN des Zugangsdienstes gemäß Festlegung aus Dienstezulassung	1	
serialNumber	Zur Unterscheidung gleichartiger Instanzen	0-1	
organizationName	Name des Zugangsdiensteanbieters	1	
countryName	Land der Anschrift des Zugangsdiensteanbieters	1	
andere Attribute		0	
subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4360] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
extensions			critical
SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Konzentrators	1	FALSE

		KeyUsage {2 5 29 15}	<i>Für Schlüsselgeneration RSA:</i> digitalSignature keyEncipherment <i>Für Schlüsselgeneration ECDSA:</i> digitalSignature	1 1 1	TRUE
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Zugangsdiensteanbieters dNSName = FQDN des Dienstes gemäß Zuweisung (Hinweis: siehe CommonName oben)	0-1 1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_vpnk_vpn>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}	URL für CRL-Statusdienst DN d. CRL-Ausstellers (f. indirekte CRL, s. RFC5280#4.2.1.13) reasons	1 1 0	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = Beschreibung zu <oid_vpnz_ti> gemäß [gemSpec_OID#GS- A_4446] professionOID = OID <oid_vpnz_ti> gemäß [gemSpec_OID#GS-A_4446]	1 1	FALSE
		ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth keyPurposeId = id-kp-serverAuth	1 1	FALSE
		andere Erweiterungen		0	
signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS- A_4360]			
signature		Wert der Signatur			

5.7.3.2 C.VPNK.VPN-SIS - VPN-Authentisierung Zugangsdienst Sicherer Internetzugang

GS-A_4830 - Umsetzung Zertifikatsprofil C.VPNK.VPN-SIS

Der TSP-X.509 nonQES MUSS C.VPNK.VPN-SIS gemäß Tab_PKI_265 umsetzen.

[<=]

2064
2065

**Tabelle 39: Tab_PKI_265 Zertifikatsprofil C.VPNK.VPN-SIS VPN-Authentisierung
Zugangsdienst Sicherer Internetzugang**

Element		Inhalt	Kar.	
certificate		C.VPNK.VPN-SIS		
	tbsCertificate			
		version	2 (v3)	
		serialNumber	gemäß [RFC5280#4.1.2.2.]	
		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4360]	
		issuer	DN der ausstellenden CA	
		validity	Gültigkeit des Zertifikats (von – bis)	
		subject		
		commonName	FQDN des Zugangsdienstes gemäß Festlegung aus Dienstezulassung	1
		serialNumber	Zur Unterscheidung gleichartiger Instanzen	0-1
		organizationName	Name des Zugangsdiensteanbieters	1
		countryName	Land der Anschrift des Zugangsdiensteanbieters	1
		andere Attribute		0
	subjectPublicKeyInfo		Algorithmus gemäß [gemSpec_Krypt#GS-A_4360] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers	
	extensions			critical
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Konzentrators	1 FALSE
		KeyUsage {2 5 29 15}	Für Schlüsselgeneration RSA: digitalSignature keyEncipherment Für Schlüsselgeneration ECDSA: digitalSignature	1 1 1 TRUE
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Zugangsdiensteanbieters dNSName = FQDN des Dienstes gemäß Zuweisung (Hinweis: siehe CommonName oben)	0-1 1 FALSE

	BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
	CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_vpnk_vpn_sis>	1 0-1 1	FALSE
	CRLDistributionPoints {2 5 29 31}	URL für CRL-Statusdienst DN d. CRL-Ausstellers (f. indirekte CRL, s. RFC5280#4.2.1.13) reasons	1 1 0	FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
	AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
	Admission {1 3 36 8 3 3}	professionItem = Beschreibung zu <oid_vpnz_sis> gemäß [gemSpec_OID#GS- A_4446] professionOID = OID <oid_vpnz_sis> gemäß [gemSpec_OID#GS-A_4446]	1 1	FALSE
	ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth keyPurposeId = id-kp-serverAuth	1 1	FALSE
	andere Erweiterungen		0	
signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS- A_4360]		
signature		Wert der Signatur		

2066 5.8 ZD – Zentrale Dienste

2067 5.8.1 Definition der Identität der Zentralen Dienste

2068 Die Identität des Zentralen Dienstes wird durch den Fully Qualified Domain Name (FQDN)
2069 des Dienstes in Verbindung mit einem zusätzlichen Instanzenkennzeichen gebildet.

2070 5.8.2 Aufbau des SubjectDN

2071 Siehe Tab_PKI_247.

2072 Die Eindeutigkeit der Identität des Dienstes innerhalb der Telematikinfrastruktur MUSS
2073 bereits durch den Inhalt der folgenden Attribute innerhalb des *SubjectDN* gegeben sein:

- 2074 • `subject.commonName`
- 2075 • `subject.serialNumber`

2076 **5.8.3 X.509 Zertifikatsprofile der Zentralen Dienste**

2077 **5.8.3.1 C.ZD.TLS-S Server-Authentisierung (ehemals C.SF.SSL-S)**

2078 **GS-A_4615 - Umsetzung Zertifikatsprofil C.ZD.TLS-S**

2079 Der TSP-X.509 nonQES MUSS C.ZD.TLS-S gemäß Tab_PKI_247 umsetzen.

2080 [\leq]

2081

2082 **Tabelle 40: Tab_PKI_247 C.ZD.TLS-S Server-Authentisierung Zentrale Dienste**

Element		Inhalt	Kar.	
certificate		C.ZD.TLS-S		
	tbsCertificate			
	version	2 (v3)		
	serialNumber	gemäß [RFC5280#4.1.2.2.]		
	signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	issuer	DN der ausstellenden CA		
	validity	Gültigkeit des Zertifikats (von – bis)		
	subject			
	commonName	FQDN des Dienstes gemäß Zuweisung	1	
	serialNumber	bei Bedarf zur Unterscheidung gleichartiger Instanzen	0-1	
	organizationName	Name des verantwortlichen Anbieters	1	
	countryName	Land der Anschrift des verantwortlichen Anbieters	1	
	andere Attribute		0	
	subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
	extensions			critical
	SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Zentralen Dienstes	1	FALSE
	KeyUsage {2 5 29 15}	Für Schlüsselgeneration RSA: digitalSignature keyEncipherment	1 1	TRUE

			Für Schlüsselgeneration ECDSA: digitalSignature	1	
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	FALSE
			dNSName = FQDN des Dienstes gemäß Zuweisung (Hinweis: siehe CommonName oben)	1	
		BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_zd_tls_s>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = Beschreibung der technischen Rolle gemäß [gemSpec_OID#GS-A_4446] professionOID = OID der technischen Rolle gemäß [gemSpec_OID#GS-A_4446]	1 1	FALSE
		ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-serverAuth	1	FALSE
		andere Erweiterungen		0	
		signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS- A_4359]		
		signature	Wert der Signatur		

2083 5.9 FD – Fachanwendungsspezifische Dienste

2084 5.9.1 Definition der Identität der Fachanwendungsspezifischen 2085 Dienste

2086 Gemäß übergreifender Definition beinhaltet der Begriff „Fachanwendungsspezifischer
2087 Dienst“ die Fachdienste und Intermediäre.

2088 Als Erweiterung eines fachanwendungsspezifischen Dienstes gelten weiterhin
2089 Clientmodule, die in der Consumerzone (LE-Umgebung) auf den lokalen Systemen
2090 Teilfunktionalitäten des Dienstes bereitstellen oder unterstützen (s. a. Kap. 5.10).

2091 Die Identität des Fachanwendungsspezifischen Dienstes wird durch den Fully Qualified
2092 Domain Name (FQDN) des Dienstes in Verbindung mit einem zusätzlichen
2093 Instanzenkennzeichen gebildet.

2094 **GS-A_4720 - Verwendung registrierter Werte für subjectDN**

2095 Anbieter von zentralen und fachanwendungsspezifischen Diensten in der TI MÜSSEN bei
2096 der Beantragung von X.509-Zertifikaten für den FQDN im **subjectDN** ausschließlich einen
2097 FQDN aus dem zugehörigen Namensraum der TI unter Beachtung des zugewiesenen
2098 Domainnamen verwenden. Dabei MUSS der verwendete FQDN mit dem FQDN der
2099 zugewiesenen Komponente übereinstimmen.
2100 [**<=**]

2101 **5.9.2 Aufbau des SubjectDN**

2102 Siehe Tab_PKI_249 oder Tab_PKI_250.

2103 Die Eindeutigkeit der Identität des Dienstes innerhalb der Telematikinfrastruktur MUSS
2104 bereits durch den Inhalt der folgenden Attribute innerhalb des *SubjectDN* gegeben sein:

- 2105 • `subject.commonName`
- 2106 • `subject.serialNumber`

2107 **5.9.3 X.509 Zertifikatsprofile der Fachanwendungsspezifischen**
2108 **Dienste**

2109 **5.9.3.1 C.FD.TLS-C Client-Authentisierung (ehemals C.SF.SSL-C)**

2110 **GS-A_4617 - Umsetzung Zertifikatsprofil C.FD.TLS-C**

2111 Der TSP-X.509 nonQES MUSS C.FD.TLS-C gemäß Tab_PKI_249 umsetzen.
2112 [**<=**]

2113

2114 **Tabelle 41: Tab_PKI_249 C.FD.TLS-C Client-Authentisierung Fachanwendungsspezifische**
2115 **Dienste**

Element	Inhalt	Kar.	
certificate	C.FD.TLS-C		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
issuer	DN der ausstellenden CA		
validity	Gültigkeit des Zertifikats (von – bis)		
subject			

			commonName	FQDN des Dienstes gemäß Zuweisung	1	
			serialNumber	bei Bedarf zur Unterscheidung gleichartiger Instanzen	0-1	
			organizationName	Name des verantwortlichen Anbieters	1	
			countryName	Land der Anschrift des verantwortlichen Anbieters	1	
			andere Attribute		0	
			subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
			extensions			critical
			SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Fachanwendungsspezifischen Dienstes	1	FALSE
			KeyUsage {2 5 29 15}	<i>Für Schlüsselgeneration RSA:</i> digitalSignature keyEncipherment <i>Für Schlüsselgeneration ECDSA:</i> digitalSignature	1 1 1	TRUE
			SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters dNSName = FQDN des Dienstes gemäß Zuweisung (Hinweis: siehe CommonName oben)	0-1 1	FALSE
			BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
			CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_fd_tls_c>	1 0-1 1	FALSE
			CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
			AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
			Admission {1 3 36 8 3 3}	professionItem = Beschreibung der technischen Rolle gemäß [gemSpec_OID#GS-A_4446] professionOID = OID der technischen Rolle gemäß [gemSpec_OID#GS-A_4446]	1 1	FALSE

		ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth	1	FALSE
		<i>andere Erweiterungen</i>		0	
signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS- A_4359]		
signature			Wert der Signatur		

2116 **5.9.3.2 C.FD.TLS-S Server-Authentisierung (ehemals C.SF.SSL-S)**

2117 **GS-A_4618 - Umsetzung Zertifikatsprofil C.FD.TLS-S**

2118 Der TSP-X.509 nonQES MUSS C.FD.TLS-S gemäß Tab_PKI_250 umsetzen.

2119 [\leq]

2120

2121 **Tabelle 42: Tab_PKI_250 C.FD.TLS-S Server-Authentisierung**
2122 **Fachanwendungsspezifische Dienste**

Element		Inhalt	Kar.	
certificate		C.FD.TLS-S		
	tbsCertificate			
		version	2 (v3)	
		serialNumber	gemäß [RFC5280#4.1.2.2.]	
		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]	
		issuer	DN der ausstellenden CA	
		validity	Gültigkeit des Zertifikats (von – bis)	
		subject		
		commonName	FQDN des Dienstes gemäß Zuweisung	1
		serialNumber	bei Bedarf zur Unterscheidung gleichartiger Instanzen	0-1
		organizationName	Name des verantwortlichen Anbieters	1
		countryName	Land der Anschrift des verantwortlichen Anbieters	1
		andere Attribute		0
	subjectPublicKeyInfo		Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers	

extensions			critical
SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Fachanwendungsspezifischen Dienstes	1	FALSE
KeyUsage {2 5 29 15}	<i>Für Schlüsselgeneration RSA:</i> digitalSignature keyEncipherment <i>Für Schlüsselgeneration ECDSA:</i> digitalSignature	1 1 1	TRUE
SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters dNSName = FQDN des Dienstes gemäß Zuweisung (Hinweis: siehe CommonName oben)	0-1 1	FALSE
BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_fd_tls_s>	1 0-1 1	FALSE
CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
Admission {1 3 36 8 3 3}	professionItem = Beschreibung der technischen Rolle gemäß [gemSpec_OID#GS-A_4446] professionOID = OID der technischen Rolle gemäß [gemSpec_OID#GS-A_4446]	1 1	FALSE
ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-serverAuth	1	FALSE
andere Erweiterungen		0	
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
signature	Wert der Signatur		

2123

2124 5.9.3.3 C.FD.SIG Signatur Fachdienst

2125 A_15172 - Umsetzung Zertifikatsprofil C.FD.SIG

2126 Der TSP-X.509 nonQES MUSS C.FD.SIG gemäß Tab_PKI_251 umsetzen. [<=]

2127

2128 **Tabelle 43: Tab_PKI_251 C.FD.SIG Signatur fachanwendungsspezifische Dienste**

Element		Inhalt	Kar.	
certificate		C.FD.SIG		
	tbsCertificate			
	version	2 (v3)		
	serialNumber	gemäß [RFC5280#4.1.2.2.]		
	signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	issuer	DN der ausstellenden CA		
	validity	Gültigkeit des Zertifikats (von – bis)		
	subject			
	commonName	Name des Dienstes gemäß Festlegung aus Dienstezulassung	1	
	serialNumber	bei Bedarf zur Unterscheidung gleichartiger Instanzen	0-1	
	organizationName	Name des verantwortlichen Anbieters	1	
	countryName	Land der Anschrift des verantwortlichen Anbieters	1	
	andere Attribute		0	
	subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
	extensions			critical
	SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Fachanwendungsspezifischen Dienstes	1	FALSE
	KeyUsage {2 5 29 15}	<i>digitalSignature</i>	1	TRUE
	SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	FALSE
	BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
	CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur	1 0-1 1	FALSE

			Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_fd_sig>		
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = Beschreibung der technischen Rolle gemäß [gemSpec_OID#GS-A_4446] professionOID = OID der technischen Rolle gemäß [gemSpec_OID#GS-A_4446]	1 1	FALSE
		ExtendedKeyUsage {2 5 29 37}		0	FALSE
		andere Erweiterungen		0	
		signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS- A_4359]		
		signature	Wert der Signatur		

2129

2130 5.9.3.4 C.FD.AUT Authentisierung Fachdienst

2131 A_15591 - Umsetzung Zertifikatsprofil C.FD.AUT

2132 Der TSP-X.509 nonQES MUSS C.FD.AUT gemäß Tab_PKI_275 umsetzen.[<=]

2133

2134 **Tabelle 44: Tab_PKI_275 C.FD.AUT Authentisierung fachanwendungsspezifische**
2135 **Dienste**

Element	Inhalt	Kar.	
certificate	C.FD.AUT		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS- A_4359]		
issuer	DN der ausstellenden CA		
validity	Gültigkeit des Zertifikats (von – bis)		
subject			

			commonName	Name des Dienstes gemäß Festlegung aus Dienstezulassung	1	
			serialNumber	bei Bedarf zur Unterscheidung gleichartiger Instanzen	0-1	
			organizationName	Name des verantwortlichen Anbieters	1	
			countryName	Land der Anschrift des verantwortlichen Anbieters	1	
			andere Attribute		0	
			subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		critical
			extensions			
			SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Fachanwendungsspezifischen Dienstes	1	
			KeyUsage {2 5 29 15}	<i>Für Schlüsselgeneration RSA:</i> digitalSignature keyEncipherment <i>Für Schlüsselgeneration ECDSA:</i> digitalSignature	1 1 1	
			SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	
			BasicConstraints {2 5 29 19}	ca = FALSE	1	
			CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_fd_aut>	1 0-1 1	
			CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	
			AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	
			Admission {1 3 36 8 3 3}	professionItem = Beschreibung der technischen Rolle gemäß [gemSpec_OID#GS-A_4446] professionOID = OID der technischen Rolle gemäß [gemSpec_OID#GS-A_4446]	1 1	
			ExtendedKeyUsage {2 5 29 37}		0	

		<i>andere Erweiterungen</i>		0	
	signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]			
	signature	Wert der Signatur			

2136

2137 **5.9.3.5 C.FD.ENC Verschlüsselung Fachdienst**

2138 **A_16213 - Umsetzung Zertifikatsprofil C.FD.ENC**

2139 Der TSP-X.509 nonQES MUSS C.FD.ENC gemäß Tab_PKI_276 umsetzen.[<=]

2140

2141 **Tabelle 45: Tab_PKI_276 C.FD.ENC Verschlüsselung fachanwendungsspezifische Dienste**

Element		Inhalt	Kar.	
certificate		C.FD.ENC		
	tbsCertificate			
	version	2 (v3)		
	serialNumber	gemäß [RFC5280#4.1.2.2.]		
	signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	issuer	DN der ausstellenden CA		
	validity	Gültigkeit des Zertifikats (von – bis)		
	subject			
	commonName	Name des Dienstes gemäß Festlegung aus Dienstezulassung	1	
	serialNumber	bei Bedarf zur Unterscheidung gleichartiger Instanzen	0-1	
	organizationName	Name des verantwortlichen Anbieters	1	
	countryName	Land der Anschrift des verantwortlichen Anbieters	1	
	<i>andere Attribute</i>		0	
	subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
	extensions			critical

	SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Fachanwendungsspezifischen Dienstes	1	FALSE
	KeyUsage {2 5 29 15}	<i>Für Schlüsselgeneration RSA:</i> keyEncipherment dataEncipherment <i>Für Schlüsselgeneration ECDSA:</i> keyAgreement	1 1 1	TRUE
	SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	FALSE
	BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
	CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_fd_enc>	1 0-1 1	FALSE
	CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
	AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
	Admission {1 3 36 8 3 3}	professionItem = Beschreibung der technischen Rolle gemäß [gemSpec_OID#GS-A_4446] professionOID = OID der technischen Rolle gemäß [gemSpec_OID#GS-A_4446]	1 1	FALSE
	ExtendedKeyUsage {2 5 29 37}		0	FALSE
andere Erweiterungen		0		
signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS- A_4359]		
signature		Wert der Signatur		

2142

2143 5.10 CM – Clientmodul

2144 5.10.1 Definition der Identität eines Clientmoduls

2145 Der Identitätsbereich „Fachanwendungsspezifischer Dienst“ umfasst Dienste und
2146 Intermediäre innerhalb der TI sowie zusätzlich damit in funktionalem Zusammenhang
2147 stehende Clientmodule in der Consumerzone (LE-Umgebung).

- 2148 Die Identität eines Clientmoduls wird durch den Anbieter des zugehörigen
2149 Fachanwendungsspezifischen Dienstes nach dessen eigener Systematik festgelegt.
2150 Seitens der TI-Plattform werden hierzu keine Vorgaben definiert, da diese Zertifikate
2151 keine Plattformleistung der TI darstellen, sondern die gegenseitige Authentisierung
2152 zwischen einem spezifischen Dienst und seinem zugehörigen lokalem Clientmodul
2153 unterstützen.
- 2154 Ein berechtigter Antragsteller für ein C.FD.TLS-* Zertifikat kann auf der Grundlage
2155 derselben Berechtigung zusätzlich auch C.CM.TLS-CS-Zertifikate beziehen.
- 2156 Ein Clientmodul-Zertifikat wird von der CA für Fachdienstzertifikate ausgestellt.
- 2157 Ein Clientmodul-Zertifikat kann als Exemplar- oder Gattungszertifikat ausgestellt werden.

2158 5.10.2 Aufbau des SubjectDN

- 2159 Siehe Tab_PKI_267.
- 2160 Die Eindeutigkeit der Identität des Clientmoduls ist durch den Anbieter des Dienstes nach
2161 eigener Systematik sicher zu stellen:
- 2162 • `subject.commonName`
 - 2163 • `subject.serialNumber`

2164 5.10.3 X.509 Zertifikatsprofil des Clientmoduls

2165 5.10.3.1 C.CM.TLS-CS Clientmodul-Authentisierung

2166 GS-A_5280 - Umsetzung Zertifikatsprofil C.CM.TLS-CS

- 2167 Der TSP-X.509 nonQES MUSS C.CM.TLS-CS gemäß Tab_PKI_267 umsetzen.
2168 [\leq]

2169

2170 **Tabelle 46: Tab_PKI_267 C.CM.TLS-CS Clientmodul-Authentisierung**

Element		Inhalt	Kar.	
certificate		C.CM.TLS-CS		
	tbsCertificate			
		version	2 (v3)	
		serialNumber	gemäß [RFC5280#4.1.2.2.]	
		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]	
		issuer	DN der ausstellenden CA	
		validity	Gültigkeit des Zertifikats (von – bis)	
		subject		
		commonName	keine Festlegung	1

		serialNumber	bei Bedarf zur Unterscheidung gleichartiger Instanzen (z.B. Release-Nr.)	0-1	
		organizationName	Name des verantwortlichen Anbieters	1	
		countryName	Land der Anschrift des verantwortlichen Anbieters	1	
		andere Attribute		0	
		subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
		extensions			critical
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Clientmoduls	1	FALSE
		KeyUsage {2 5 29 15}	<i>Für Schlüsselgeneration RSA:</i> digitalSignature keyEncipherment <i>Für Schlüsselgeneration ECDSA:</i> digitalSignature	1 1 1	TRUE
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_cm_tls_c>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	keine Festlegung	0-1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = Beschreibung der technischen Rolle gemäß [gemSpec_OID#GS-A_4446] professionOID = OID der technischen Rolle gemäß [gemSpec_OID#GS-A_4446]	1 1	FALSE
		ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth keyPurposeId = id-kp-serverAuth	1 1	FALSE
		andere Erweiterungen		0	

signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
signature	Wert der Signatur		

2171

2172

2173 5.11 SGD-HSM – Schlüsselgenerierungsdienst-HSM

2174 5.11.1 Beschreibung der Identität

2175 Ein HSM mit einem speziellen Firmware-Modul ist zentraler Bestandteil eines
2176 Schlüsselgenerierungsdienstes [gemSpec_SGD]. Ein solches als SGD-HSM bezeichnetes
2177 HSM muss eine für einen Client (bspw. ein ePA-Frontend des Versicherten (FdV) oder ein
2178 FM ePA) prüfbare Identität besitzen. Diese Identität wird verwendet um damit öffentliche
2179 ECDH-Schlüssel zu authentisieren, die für die Schlüsselgenerierungsfunktionalität
2180 benötigt werden. Dabei ist es wichtig, dass es verschiedene SGD-HSM gibt, jeweils solche
2181 mit einer Identität entweder vom Typ 1 (oid_sgd1_hsm) und solche vom Typ 2
2182 (oid_sgd2_hsm) (vgl. professionItem in C.SGD-HSM.AUT und [\[gemSpec OID#GS-A_4446\]](#),
2183 und vgl. auch [\[gemSpec SGD#A_17848\]](#)).

2184 Die Identität wird von der Komponenten-PKI ausgegeben. Ein solches Zertifikat wird
2185 jedoch explizit in der TSL aufgeführt (vgl. [\[gemSpec SGD#A_17846\]](#)) und wird daher
2186 von den Clients über einen speziellen Weg geprüft
2187 (vgl. [\[gemSpec SGD#A_17847\]](#)). Durch die direkte Aufführung in der TSL ist die
2188 Identität unabhängig von der Sicherheitsleistung der Komponenten-PKI.

2189 5.11.2 X.509 Zertifikatsprofil der SGD-HSM

2190 A_17844 - Umsetzung Zertifikatsprofil C.SGD-HSM.AUT

2191 Der TSP-X.509 nonQES MUSS das Zertifikatsprofil C.SGD-HSM.AUT nach Tab_PKI_296
2192 umsetzen.

2193
2194 [\leq]

2195 **Tabelle 47: Tab_PKI_296 C.SGD-HSM.AUT Authentisierung SGD-HSM**

Element	Inhalt	Kar.	
certificate	C.SGD-HSM.AUT		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
issuer	DN der ausstellenden CA		

		validity		Gültigkeit des Zertifikats (von – bis)		
		subject				
			commonName	<SGD>-<Namensteil des Dienstes (frei wählbar)>	1	
			serialNumber	bei Bedarf zur Unterscheidung gleichartiger Instanzen	0-1	
			organizationName	Name des verantwortlichen Anbieters	1	
			countryName	Land der Anschrift des verantwortlichen Anbieters	1	
			andere Attribute		0	
		subjectPublicKeyInfo		Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		critical
		extensions				
			SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Dienstes	1	
			KeyUsage {2 5 29 15}	digitalSignature	1	
			SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	
			BasicConstraints {2 5 29 19}	ca = FALSE	1	
			CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_sgd_hsm_aut>	1 0-1 1	
			CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	
			AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	
			Admission {1 3 36 8 3 3}	professionItem = Beschreibung der technischen Rolle gemäß [gemSpec_OID#GS-A_4446] professionOID = OID der technischen Rolle gemäß [gemSpec_OID#GS-A_4446]	1 1	
			ExtendedKeyUsage {2 5 29 37}		0	
			andere Erweiterungen		0	

signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
signature	Wert der Signatur		

2196

2197 5.12 CA - Zertifikatsprofile

2198 **GS-A_4730 - Eindeutige Identifizierung der CA-Zertifikate**

2199 Der TSP-X.509 nonQES und TSP-X.509 QES MUSS bei der Beantragung von X.509-CA-
2200 Zertifikaten sicherstellen, dass der subjectDN die CA eindeutig innerhalb der TI
2201 identifiziert.

2202 [\leq]

2203 **GS-A_4731 - Attribute der CA-Zertifikate**

2204 Der TSP-X.509 nonQES und TSP-X.509 QES SOLL bei der Beantragung von X.509-CA-
2205 Zertifikaten nur die Attribute mit der Kardinalität 1 verwenden.

2206 [\leq]

2207 **GS-A_4732 - Extension der CA-Zertifikate**

2208 Der TSP-X.509 nonQES (eGK) und die gematik Root-CA SOLLEN bei der Erstellung eines
2209 Root- bzw. self-signed CA-Zertifikats die Extension AuthorityKeyIdentifier entfallen
2210 lassen.

2211 [\leq]

2212 Die eindeutige Benennung der CA-Zertifikate im Feld `commonName` erfolgt gemäß Kap. 2.2
2213 nach dem Schema:

2214 `<holder>.<usage>-CA<n>`

2215 (Analog zum Schema `<type>.<holder>.<usage><n>`, welches in Kap. 2.2 beschrieben
2216 wird.)

2217 Der Suffix `<n>` kennzeichnet hierbei die fortlaufende Nummerierung innerhalb eines Typs
2218 von CA-Zertifikaten – beginnend ab dem Wert 1. Dabei wird `<n>` auch bei
2219 Schlüsselgenerations-Wechseln fortgesetzt.

2220

2221 **GS-A_4735 - Namenskonvention für CA-Zertifikate**

2222 Der TSP-X.509 nonQES und TSP-X.509 QES MUSS für jede von ihm betriebene CA die
2223 Namenskonventionen gemäß [GS-A_4588], [GS-A_4590] umsetzen sowie die
2224 Namensbildung im Feld `commonName` nach dem Schema `<holder>.<usage>-CA<n>`
2225 vornehmen.

2226 [\leq]

2227 5.12.1 GEM.RCA<n> - Zentrale Root-CA_nonQES

2228 **GS-A_4736 - Umsetzung Zentrale nonQES-Root-CA-Zertifikat**

2229 Die gematik-Root-CA MUSS die Namenskonvention und Attributsbelegung der Felder für
2230 folgende CA-Zertifikate umsetzen gemäß:

2231 a) Tab_PKI_211 für gematik-Root-CA,

2232 b) Tab_PKI_212 für i) Zentrale Aussteller-CA_nonQES, ii) Aussteller-CA_nonQES, iii)

2233 TSL-Signer-CA. [\leq]

2234

2235 **Tabelle 48: Tab_PKI_211 GEM.R-CA<n> – Zentrale gematik Root-CA_nonQES der TI**

Element		Inhalt	Kar.	
certificate		C.GEM.RCA<n>		
	tbsCertificate			
	version	2 (v3)		
	CertificateSerialNumber	gemäß [RFC5280#4.1.2.2]		
	signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
	issuer	derselbe DN wie unter "subject" aufgeführt		
	validity	Gültigkeit des Zertifikats (von - bis)		
	subject			
	commonName	GEM.RCA<n>	1	
	serialNumber	Zur Unterscheidung gleichartiger Instanzen	0-1	
	organizationalUnitName	Zentrale Root-CA der Telematikinfrastruktur	1	
	organizationName	gematik GmbH	1	
	countryName	DE	1	
	andere Attribute		0	
	subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4357] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
	extensions			critical
	SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels der Zentralen gematik Root-CA, für die dieses Zertifikat ausgestellt wird.	1	FALSE
	KeyUsage {2 5 29 15}	keyCertSign crlSign	1 0-1	TRUE
	SubjectAltNames {2 5 29 17}		0	FALSE
	BasicConstraints {2 5 29 19}	ca = TRUE pathLength	1 0	TRUE
	CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie)	1 1	FALSE

	CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
	AuthorityKeyIdentifier {2 5 29 35}		0	FALSE
	Admission {1 3 36 8 3 3}		0	FALSE
	ExtendedKeyUsage {2 5 29 37}		0	FALSE
	andere Erweiterungen		0	
	signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
	signature	Wert der Signatur		

2236 5.12.2 <tps>.<usage>-CA<n> - Aussteller-CA_nonQES

2237 GS-A_4737 - Umsetzung nonQES-CA-Zertifikate

2238 Der TSP-X.509 nonQES MUSS für die von ihm betriebenen CAs die Attributsbelegung der
2239 Felder gemäß Tab_PKI_212 und die Namenskonvention gemäß Tab_PKI_213 umsetzen.
2240 [**<=>**]

2241

2242 Tabelle 49: Tab_PKI_212 <tps>.<usage>-CA<n> -Aussteller- CA_nonQES der TI

Element	Inhalt	Kar.	
certificate	C.<tps>.<usage>-CA<n>		
tbsCertificate			
version	2 (v3)		
CertificateSerialNumber	gemäß [RFC5280#4.1.2.2]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
issuer	DN der ausstellenden CA		
validity	Gültigkeit des Zertifikats (von - bis)		
subject			
commonName	<tps>.<usage>-CA<n> *) **)	1	
serialNumber	Zur Unterscheidung gleichartiger Instanzen	0-1	

		organizationalUnitName	<usageName>-CA der Telematikinfrastruktur **)	0-1	
		organizationName	<tspName> *)	1	
		countryName	DE	1	
		andere Attribute		0	
	subjectPublicKeyInfo		Algorithmus gemäß [gemSpec_Krypt#GS-A_4357] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
	extensions				critical
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels der CA, für die dieses Zertifikat ausgestellt wird	1	FALSE
		KeyUsage {2 5 29 15}	keyCertSign crlSign	1 0-1	TRUE
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = TRUE pathLength = 0	1 1	TRUE
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) ODER davon abweichend: CAs für HBA-AUT/ENC-Zertifikate: policyIdentifier = <oid_policy_hba_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie	1 1 1 0-1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}		0	FALSE
		ExtendedKeyUsage {2 5 29 37}		0	FALSE
		andere Erweiterungen		0	
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		

signature	Wert der Signatur		
-----------	-------------------	--	--

2243 *) Für CA-Zertifikate der zentralen PKI wird für <tsp> die Bezeichnung "GEM" und für
2244 <tspName> "gematik GmbH" eingesetzt; für von TSPs betriebene Sub-CAs wird das
2245 jeweilige TSP-Kürzel sowie der vollständige TSP-Name eingefügt.

2246 **) Die erlaubten Werte für <usage> und <usageName> werden in Tab_PKI_213
2247 aufgeführt.

2248 5.12.3 <tsp>.HBA-qCA<n> - Aussteller-CA_QES

2249 GS-A_4948 - Umsetzung QES-CA-Zertifikate

2250 Der TSP-X.509 QES MUSS für die Zertifikate der von ihm betriebenen CAs die
2251 Attributsbelegung der Felder gemäß Tab_PKI_215 umsetzen.

2252 [**<=**]

2253

2254 **Tabelle 1: Tab_PKI_215 <tsp>.HBA-qCA<n> - Aussteller- CA_QES der TI**

Element	Inhalt	Kar.	
certificate	C.<tsp>.HBA-qCA<n>		
tbsCertificate			
version	2 (v3)		
CertificateSerialNumber	gemäß [RFC5280#4.1.2.2]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4358]		
issuer	DN der ausstellenden CA		
validity	Gültigkeit des Zertifikats (von - bis)		
subject			
commonName	<tsp>.HBA-qCA <n> *)	1	
organizationalUnitName	Qualifizierter VDA der Telematikinfrastruktur	0-1	
organizationIdentifier	Vom VDA verwendeter organizationIdentifier gemäß [ETSI EN 319 412-2] und [X.520]	0-1	
organizationName	Name des VDA für QES	1	
countryName	DE	1	
andere Attribute		0	
subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4358] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		

extensions			critical
SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels der CA, für die dieses Zertifikat ausgestellt wird	1	FALSE
KeyUsage {2 5 29 15}	keyCertSign crlSign	1 0-1	TRUE
SubjectAltNames {2 5 29 17}		0	FALSE
BasicConstraints {2 5 29 19}	ca = TRUE pathLength = 0	1 1	TRUE
CertificatePolicies {2 5 29 32}	policyIdentifier = <id-etsi-qcp-natural-qscd> {0.4.0.194112.1.2} policyQualifierInfo = URL der Zertifikatsrichtlinie policyIdentifier = <oid_policy_hba_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie Ggf. weitere policyIdentifier Ggf. weitere policyQualifierInfo	0-1 0-1 1 0-1 0-n 0-n	FALSE
CRLDistributionPoints {2 5 29 31}	CDP	0-1	FALSE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	0-1	FALSE
AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
Admission {1 3 36 8 3 3}		0	FALSE
ValidityModel {1 3 6 1 4 1 8301 3 5}	id-validity-Model-chain {1 3 6 1 4 1 8301 3 5 1}	1	FALSE
ExtendedKeyUsage {2 5 29 37}		0	FALSE
QCStatements {1.3.6.1.5.5.7.1.3}	<id-etsi-qcs-QcCompliance> {0.4.0.1862.1.1} Ggf. weitere Einträge	0-1 0-n	FALSE
andere Erweiterungen	Ggf. weitere Erweiterungen durch die BNetzA gesetzt, die hier jedoch nicht spezifiziert sind.		
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4358]		
signature	Wert der Signatur		

2255 *) Der Name kann mit oder ohne Leerzeichen vor der laufenden Nr. <n> geschrieben
2256 werden.

2257 **5.13 OCSP – Statusauskunftsdienst**

2258 **5.13.1 Definition der OCSP-Signer-Identität**

2259 Die Identität eines OCSP-Responders wird durch den `commonName` gebildet, zur
2260 Sicherstellung der Eindeutigkeit bedarfsweise ergänzt um ein Merkmal im Feld
2261 `subject.serialNumber`.

2262 **GS-A_4738 - Eindeutige Identifizierung der OCSP-Signer-Zertifikate**

2263 Der TSP-X.509 nonQES und der Anbieter des TSL-Dienstes MÜSSEN bei der Beantragung
2264 von X.509-OCSP-Signer-Zertifikaten sicherstellen, dass der subjectDN das OCSP-Signer-
2265 Zertifikat eindeutig innerhalb der TI identifiziert.
2266 [`<=`]

2267 **GS-A_4739 - Attribute der OCSP-Signer-Zertifikate**

2268 Der TSP-X.509 nonQES und der Anbieter des TSL-Dienstes SOLLEN bei der Beantragung
2269 von X.509-OCSP-Signer-Zertifikaten nur die Attribute mit der Kardinalität 1 verwenden.
2270 [`<=`]

2271 **GS-A_5514 - Verwendung separater OCSP-Signer-Zertifikate**

2272 Ein TSP-X.509 nonQES, die gematik Root-CA und der Anbieter des TSL-Dienstes MÜSSEN
2273 für jede unterstützte Schlüsselgeneration (gemäß [`gemSpec_Krypt#GS-A_4357`]) jeweils
2274 ein separates OCSP-Signer-Zertifikat verwenden.
2275 [`<=`]

2276 *Hinweis: Neue OCSP-Signer-Zertifikate sollten gemäß [RFC6960] signiert werden. Zu*
2277 *beachten ist, dass OCSP-Signer-Zertifikate zur Verwendung in der TI in die TSL*
2278 *eingebracht werden müssen. (vgl. [`gemSpec_TSL#TIP1-A_4084`] sowie TUC_PKI_006*
2279 *„OCSP-Abfrage“, Schritt 5.)*

2280 **5.13.2 Aufbau des SubjectDN**

2281 Siehe Tab_PKI_253.

2282

2283 **5.13.3 X.509-Profil des OCSP-Signer-Zertifikates**

2284 **5.13.3.1 C.GEM.OCSP OCSP-Signer-Zertifikat**

2285 **GS-A_4741 - Umsetzung Zertifikatsprofil C.GEM.OCSP**

2286 Der TSP-X.509 nonQES, die gematik-Root-CA und der TSL-Dienst MÜSSEN C.GEM.OCSP
2287 gemäß Tab_PKI_253 umsetzen.
2288 [`<=`]

2289

2290 **Tabelle 50: Tab_PKI_253 C.GEM.OCSP Zertifikatsprofil OCSP-Signer**

Element	Inhalt	Kar.	
certificate	C.GEM.OCSP		
tbsCertificate			

		version	2 (v3)		
		serialNumber	gemäß [RFC5280#4.1.2.2.]		
		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
		issuer	DN der ausstellenden CA		
		validity	Gültigkeit des Zertifikats (von – bis)		
		subject			
		commonName	Name des OCSP-Responders	1	
		serialNumber	Zur Unterscheidung gleichartiger Instanzen	0-1	
		organizationalUnitName	Name der Abteilung für den Betrieb des OCSP	0-1	
		organizationName	Name des OCSP-Dienstanbieters	1	
		countryName	Land der Anschrift des OCSP-Dienstanbieters	1	
		andere Attribute		0	
		subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4357] und individueller Wert des öffentlichen Schlüssels des Zertifikatsbesitzers		
		extensions			critical
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des OCSP-Signers	1	FALSE
		KeyUsage {2 5 29 15}	nonRepudiation	1	TRUE
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie)	1 0-1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	0-1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		ExtendedKeyUsage {2 5 29 37}	KeyPurposeId = id-kp-OCSPSigning	1	FALSE

		id-pkix-ocsp-nocheck {1.3.6.1.5.5.7.48.1.5}	OCSP-Nocheck = NULL	0-1	FALSE
		andere Erweiterungen		0	
		signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS- A_4357]		
		signature	Wert der Signatur		

2291 5.14 CRL – Statusauskunftsdienst

2292 **GS-A_5066-01 - Indirekte CRL gemäß Standards**

2293 ~~GS-A_5066 - Indirekte CRL gemäß [Common-PKI]~~ Der TSP-X.509 nonQES für
2294 Komponenten MUSS CRLs für X.509-Zertifikate als indirekte CRLs gemäß [~~Common-~~
2295 ~~PKIRFC5280~~] und [~~RFC5280#4.2.1.13X.509~~] unter Verwendung eines dedizierten CRL-
2296 Signers erzeugen.

2297 [~~<=~~]

2298 Weitere relevante Referenzen sind im Rahmen der CRL-Prüfung gemäß GS-A_4900
2299 detailliert angegeben.

2300

2301 5.14.1 Definition der CRL-Signer-Identität

2302 Die Identität eines CRL-Signers wird durch den `commonName` gebildet, zur Sicherstellung
2303 der Eindeutigkeit bedarfsweise ergänzt um ein Merkmal im Feld `subject.serialNumber`.

2304 **GS-A_4935 - Eindeutige Identifizierung der CRL-Signer-Zertifikate**

2305 Der TSP-X.509 nonQES MUSS bei der Beantragung von X.509-CRL-Signer-Zertifikaten
2306 sicherstellen, dass der `subjectDN` das CRL-Signer-Zertifikat eindeutig innerhalb der TI
2307 identifiziert.

2308 [~~<=~~]

2309 **GS-A_4936 - Attribute der CRL-Signer-Zertifikate**

2310 Der TSP-X.509 nonQES SOLL bei der Beantragung von X.509-CRL-Signer-Zertifikaten nur
2311 die Attribute mit der Kardinalität 1 verwenden.

2312 [~~<=~~]

2313 **GS-A_4937 - Ableitung des CRL-Signer-Zertifikates**

2314 Ein TSP-X.509 nonQES MUSS das CRL-Signer-Zertifikat der jeweiligen
2315 Schlüsselgeneration für die von ihm be-triebenen CRL-Dienste aus der VPNK-CA
2316 derselben Schlüsselgeneration beziehen.

2317 [~~<=~~]

2318 **GS-A_5515 - Bezug separater CRL-Signer-Zertifikate**

2319 Ein TSP-X.509 nonQES, der CRL-Dienste betreibt, MUSS für jede unterstützte
2320 Schlüsselgeneration (gemäß [gemSpec_Krypt#GS-A_4357]) jeweils ein separates CRL-
2321 Signer-Zertifikat beziehen.

2322 [~~<=~~]

2323 **5.14.2 Aufbau des SubjectDN**

2324 Siehe Tab_PKI_214.

2325

2326 **5.14.3 X.509 Profil des CRL-Signer-Zertifikates**

2327 **5.14.3.1 C.GEM.CRL CRL-Signaturzertifikat**

2328 **GS-A_4939 - Umsetzung Zertifikatsprofil C.GEM.CRL**

2329 Der TSP-X.509 nonQES MUSS C.GEM.CRL gemäß Tab_PKI_214 umsetzen.

2330 [\leq]

2331

2332 **Tabelle 51: Tab_PKI_214 C.GEM.CRL Zertifikatsprofil CRL-Signer**

Element		Inhalt	Kar.	
certificate		C.GEM.CRL		
	tbsCertificate			
	version	2 (v3)		
	serialNumber	gemäß [RFC5280#4.1.2.2.]		
	signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
	issuer	DN der ausstellenden CA		
	validity	Gültigkeit des Zertifikats (von – bis)		
	subject			
	commonName	Name des CRL-Signers	1	
	serialNumber	Zur Unterscheidung gleichartiger Instanzen	0-1	
	organizationalUnitName	Name der Abteilung für den Betrieb des CRL-Signer	0-1	
	organizationName	Name des CRL-Diensteanbieters	1	
	countryName	Land der Anschrift des CRL-Diensteanbieters	1	
	andere Attribute		0	
	subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4357] und individueller Wert des öffentlichen Schlüssels des Zertifikatsbesitzers		
	extensions			critical

	SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des CRL-Signers	1	FALSE
	KeyUsage {2 5 29 15}	crlSign	1	TRUE
	SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	FALSE
	BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
	CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie)	1 0-1	FALSE
	CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	keine Festlegung	0-1	FALSE
	AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
	ExtendedKeyUsage {2 5 29 37}		0	FALSE
	andere Erweiterungen		0	
signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS- A_4357]		
signature		Wert der Signatur		

2333 5.15 TSL - Zertifikatsprofile

2334 5.15.1 Definition der TSL-Signer-Identität

2335 Die Identität des TSL-Signers wird durch einen eindeutigen **commonName** bedarfsweise
2336 ergänzt um ein Merkmal im Feld **subject.serialNumber** gebildet.

2337 **GS-A_4742 - Eindeutige Identifizierung der TSL-Signer-Zertifikate**

2338 Der Anbieter des TSL-Dienstes MUSS bei der Beantragung von X.509-TSL-Signer-
2339 Zertifikaten sicherstellen, dass der subjectDN das TSL-Signer-Zertifikat eindeutig
2340 innerhalb der TI identifiziert.

2341 [**<=**]

2342 **GS-A_4743 - Attribute der TSL-Signer-Zertifikate**

2343 Der Anbieter des TSL-Dienstes SOLL bei der Beantragung von X.509-TSL-Signer-
2344 Zertifikaten nur die Attribute mit der Kardinalität 1 verwenden.

2345 [**<=**]

2346 **5.15.2 Aufbau des SubjectDN**

2347 Siehe Tab_PKI_252_01.

2348 **5.15.3 X.509 Zertifikatsprofil der TSL-Signer-CA**

2349 **GS-A_4744 - Zentrale TSL-Signer-CA-Zertifikate**

2350 Der Anbieter des TSL-Dienstes MUSS für die von ihm betriebenen TSL-Signer-CAs die
2351 Attributsbelegung der Felder gemäß Tab_PKI_212 und die Namenskonvention für den
2352 TSL-Dienst gemäß Tab_PKI_213 umsetzen.

2353 [**<=>**]

2354

2355 **A_17686 - TSL-Signer-CA Cross-Zertifikate (ECC-Migration)**

2356 Der TSL-Dienst MUSS für die TSL-Signer-CA der Schlüsselgeneration ECDSA beidseitige
2357 Cross-Zertifikate zu der aktiven TSL-Signer-CA der Schlüsselgeneration RSA bereitstellen
2358 und dabei die folgenden Punkte berücksichtigen:

- 2359
- 2360 • das bereits existierende Schlüsselmateriale (PublicKey) der TSL-Signer-CA (ECDSA)
2361 wird durch die TSL-Signer-CA (RSA) mit deren PrivateKey signiert und damit das
2362 Cross-Zertifikat mit dem Namen C.GEM.TSL-CA<Index der ECDSA-CA>-
CROSS<Index der RSA-CA> erzeugt
 - 2363 • das bereits existierende Schlüsselmateriale (PublicKey) der TSL-Signer-CA (RSA)
2364 wird durch die TSL-Signer-CA (ECDSA) mit deren PrivateKey signiert und damit
2365 das Cross-Zertifikat mit dem Namen C.GEM.TSL-CA<Index der RSA-CA>-
2366 CROSS<Index der ECDSA-CA> erzeugt

2367

2368 [**<=>**]

2369

2370 **A_17687 - TSL-Signer-CA Cross-Zertifikate – Attributsbelegung (ECC-Migration)**

2371 Der TSL-Dienst MUSS für die zu erstellenden Cross-Zertifikate die Attributsbelegung der
2372 Felder gemäß Tab_PKI_212 umsetzen, wobei Abweichungen bei folgenden Elementen
2373 vorzunehmen sind:

- 2374
- 2375 • <certificate> = C.GEM.TSL-CA<X>-CROSS<Y>
 - 2376 • <commonName> = GEM.TSL-CA<X>-CROSS<Y>

2377 Dabei ist jeweils <X> der Index des zu signierenden TSL-Signer-CA-Schlüssels
2378 (PublicKey) und <Y> der Index des signierenden TSL-Signer-CA-Schlüssels (PrivateKey).

2378

2379 [**<=>**]

2380 *Beispiele für TSL-Signer-CA Cross-Zertifikate:*

- 2381
- 2382 • C.GEM.TSL-CA1-CROSS3

2383 Erklärung: Das Cross-Zertifikat ist für TSL-Signer-CA1 (RSA Public Key)
2384 ausgestellt und von TSL-Signer-CA3 (ECDSA) signiert.

- 2384
- 2385 • C.GEM.TSL-CA3-CROSS1

2386 Erklärung: Das Cross-Zertifikat ist für TSL-Signer-CA3 (ECDSA Public Key)
2387 ausgestellt und von TSL-Signer-CA1 (RSA) signiert.

2388 **5.15.4 TSL-Signer- Zertifikat**

2389 **GS-A_4745-01 - Umsetzung Zertifikatsprofil C.TSL.SIG für TSL-Dienst**

2390 Der TSL-Dienst MUSS das TSL-Signer-Zertifikat C.TSL.SIG gemäß Tab_PKI_252_01

2391 umsetzen.

2392 [\leq]

2393

2394 **Tabelle 52: Tab_PKI_252_01 C.TSL.SIG Zertifikatsprofil TSL-Signer**

Element		Inhalt	Kar.	
certificate		C.TSL.SIG		
	tbsCertificate			
	version	2 (v3)		
	serialNumber	gemäß [RFC5280#4.1.2.2.]		
	signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
	issuer	DN der ausstellenden CA		
	validity	Gültigkeit des Zertifikats (von – bis)		
	subject			
	commonName	TSL Signing Unit <n>	1	
	serialNumber	Zur Unterscheidung gleichartiger Instanzen	0-1	
	organizationalUnitName	Name der Abteilung für den Betrieb des TSL-Dienstes	0-1	
	organizationName	gematik GmbH	1	
	countryName	DE	1	
	andere Attribute		0	
	subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4357] und individueller Wert des öffentlichen Schlüssels des Zertifikatsbesitzers		
	extensions			critical
	SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des TSL-Signers	1	FALSE
	KeyUsage {2 5 29 15}	nonRepudiation	1	TRUE
	SubjectAltNames {2 5 29 17}		0	FALSE

	BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
	CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_tsl_signer>	1	FALSE
	CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
	AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
	ExtendedKeyUsage {2 5 29 37}	KeyPurposeId = id-tsl-kpTslSigning gemäß [ETSI_TS_102_231_v3.1.2#6.2]	1	FALSE
	andere Erweiterungen		0	
	signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS- A_4357]		
	signature	Wert der Signatur		

Hinweis: [ETSI_TS_102_231_V3.1.2], Kap. 6.2 empfiehlt, den Inhalt von „SchemeOperatorName“ (vgl. [gemSpec_TSL]) als „organizationName“ im Subject Distinguished Name einzutragen. „SchemeOperatorName“ wiederum MUSS gemäß [ETSI_TS_102_231_V3.1.2], Kap. 5.3.4 den eingetragenen Namen enthalten. „gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH“ ist aber zu lang für das Feld „organizationName“, vgl. Kap. 5.3.3 Umgang mit überlangen Attributen im SubjectDN und Kap. 4.8.3.5 SubjectAltNames.

5.15.5 TSL-OCSP-Responder-Zertifikat

GS-A_4747 - Umsetzung Zertifikatsprofil C.GEM.OCSP für TSL-Dienst

Der TSL-Dienst MUSS für die OCSP-Prüfung des TSL-Signer-Zertifikats ein OCSP-Signer-Zertifikat C.GEM.OCSP gemäß Tab_PKI_253 umsetzen.

[<=]

GS-A_4918 - Ableitung des OCSP-Signer-Zertifikates für TSL-Dienst

Der TSL-Dienst MUSS das OCSP-Signer-Zertifikat der jeweiligen Schlüsselgeneration gemäß [RFC6960] von der TSL-Signer-CA derselben Schlüsselgeneration beziehen.[<=]

2412

6 CV-Zertifikate

2413 Dieses Kapitel enthält Anforderungen an die Profilattribute für CV-Zertifikate sowie deren
2414 Verwendung. Hierzu gehört auch die Festlegung von Vorgaben zur Identifizierung der
2415 ausgebenden CA bzw. des Zertifikatsinhabers sowie die Definition von Rollen- und
2416 Geräteprofilen mit denen Zugriffsrechte des Karteninhabers bzw. die Verfügbarkeit von
2417 Funktionseinheiten eines Gerätes verbunden sind.

2418 **GS-A_4972 - Bezug des CV-Zertifikat**

2419 Ein Kartenherausgeber KANN das nicht-personenbezogene CV-Zertifikat nach
2420 entsprechender Registrierung vom TSP-CVC-CA beziehen.
2421 [\leq]

2422 **GS-A_4973 - Ausstellung aller CV-Zertifikate einer Karte durch gleiche CVC-Sub-CA**

2423 Der Kartenherausgeber MUSS sicherstellen, dass alle zu einer Chipkarte gehörenden CV-
2424 Zertifikate durch dieselbe CA der zweiten Ebene erzeugt werden.
2425 [\leq]
2426

2427 **6.1 Festlegungen zur Abgrenzung**

2428 Grundsätzlich sind CV-Zertifikatsprofile zu unterscheiden für

- 2429 • CVC-CAs, die als Herausgeber von CV-Zertifikaten für Endteilnehmer fungieren,
2430 und
- 2431 • Endteilnehmer, d. h. Kartentypen wie eGK, HBA, SM-B und gSMC.

2432 Der öffentliche Root-Schlüssel der PKI für CV-Zertifikate wird direkt als Datenfeld in den
2433 Karten hinterlegt. Die Bereitstellung des öffentlichen Root-Schlüssels in Form eines CV-
2434 Zertifikates ist nicht erforderlich.

2435 **GS-A_4974 - CV-Ausstattung von Smartcards der TI**

2436 Ein Kartenherausgeber, der Smartcards für Einsatzbereiche der TI herausgeben will,
2437 MUSS sicherstellen, dass die Karten über folgende CV-Ausstattung verfügen: (a)
2438 mindestens ein CV-Schlüsselpaar mit zugeordnetem CV-Zertifikat. Es können mehrere
2439 Schlüsselpaare mit jeweils eigenem CV-Zertifikat und unterschiedlichen Profilattributen
2440 enthalten sein, die die Karte für unterschiedliche Funktionen in der TI-
2441 Anwendungslandschaft autorisieren können (b) das CV-CA-Zertifikat der zweiten Ebene
2442 sowie (c) der öffentliche Schlüssel der CV-Root.
2443 [\leq]
2444

2444 **6.2 Namensregeln und -formate**

2445 Anforderungen an Namensregeln und -formate ergeben sich aus der Identifikation von
2446 Herausgebern von CV-Zertifikaten sowie von Zertifikatsinhabern.

2447 Der Herausgeber eines CV-Zertifikats wird über das Datenelement Certificate Authority
2448 Reference (CAR) identifiziert. Anforderungen an die Formatierung und den Inhalt der CAR
2449 sind im Abschnitt 6.4.3.2 beschrieben.

Der Inhaber eines CV-Zertifikats wird im Datenelement Certificate Holder Reference (CHR) angegeben. Anforderungen an die Formatierung und den Inhalt der CHR sind im Abschnitt 6.4.3.4 beschrieben.

6.3 Rollen- und gerätebasierte Zugriffsprofile

6.3 Rollen und Profile

In einem CV-Zertifikat einer Chipkarte ist das Zugriffsprofil dieser Chipkarte enthalten. Dabei wird gemäß [gemKPT_PKI_TIP#5.1] unterschieden zwischen einem Zugriffsprofil für eine

- Authentisierung einer Rolle (CV-Rollen-Zertifikate) bzw. für eine
- Authentisierung einer Funktionseinheit eines Gerätes (CV-Gerätezertifikate).

Die technische Umsetzung der Zuordnung zu Zugriffsprofilen in CV-Zertifikaten erfolgt für Karten der Generation 2 über eine Flagliste, die die Berechtigungen steuert und im Feld CHAT gespeichert ist (siehe Kapitel 6.4.6).

6.3.1 Rollenauthentisierung

GS-A_4620 - Zugriffsprofil einer eGK

Der Kartenherausgeber MUSS sicherstellen, dass das CV-Rollen-Zertifikat einer eGK als Zugriffsprofil CHAT.0 den Wert '00 0000 0000 0000' hat.

[<=]

GS-A_4621 - Zugriffsprofil von HBA und SM-B (SMC-B, HSM-B)

Der Kartenherausgeber MUSS sicherstellen, dass bei einem HBA bzw. einer SM-B das Zugriffsprofil in einem CV-Zertifikat der Rolle des Karteninhabers bzw. der Organisation gemäß Tabelle Tab_PKI_254 entspricht.

Eine Ausnahme hiervon ist die SM-B für Gesellschafterorganisationen, da sie keine CV-Rollenzertifikate erhält.

[<=]

A_16179 - Zugriffsprofil einer KTR-AdV

Der Kartenherausgeber für SM-B KTR-AdV MUSS sicherstellen, dass die CV-Rollen-Zertifikate für eine KTR-AdV jeweils das Zugriffsprofil CHAT.1 bzw. CHAT.0 gemäß [gemSpec_PKI#Tab_PKI_254] besitzen.

[<=]

In der folgenden Tabelle werden die Zugriffsprofile im Kontext der sie nutzenden fachlichen Akteure dargestellt. Der Kern der Tabelle wurde mit den LEOs, Kostenträgern und dem BMG abgestimmt. Sie bilden die Basis für die Rechtezuweisung auf den Smartcards der Generation 2.

Die Tabelle enthält auch, welche Organisation als sog. „Qualifizierende Stelle“ (vgl. Tab_PKI_254) die Berechtigung für die Zugriffsprofile in CV-Zertifikaten vergibt und damit die Betreiber von CVC-CAs der zweiten Ebene autorisiert, diese Profile in die CV-Zertifikate einzubringen. Für derzeit nicht verwendete Profile ist diese Zuordnung offen.

Es werden die Zugriffsprofile 0 – 9 für eine Rollenauthentisierung unterschieden:

2492

2493

Tabelle 53: Tab_PKI_254 Zugriffsprofile für eine Rollenauthentisierung

Profile / Akteure / Rollen und OID aus gemSpec_PKI					X.509 Admission Extension	
Zugriffsprofil	Kartenart	Beschreibung fachlicher Akteur	Fachliche Rolle	Qualifizierende Stelle	professionItem	OID-Referenz
0						
CHAT.0	eGK	Versicherter	Versicherter	keine Qualifizierung	Versicherte/-r	oid_versicherter
CHAT.0	KTR-Adv	KTR-Adv	Versicherter	gesetzliche Krankenkasse	Adv-Umgebung bei Kostenträger	oid_adv_ktr
1						
CHAT.1	KTR-Adv	KTR-Adv	Versicherter	gesetzliche Krankenkasse	Adv-Umgebung bei Kostenträger	oid_adv_ktr
2						
CHAT.2A	HBA – Arzt	Arzt in einer Institution (z. B. eigene Praxis, Gemeinschaftspraxis, Krankenhaus). Auch der ärztliche Psychotherapeut fällt unter diese Kategorie.	Arzt	BAEK	Ärztin/Arzt	oid_arzt
CHAT.2ZA	HBA – Zahnarzt	Zahnarzt in einer Institution	Zahnarzt	BZÄK	Zahnärztin/Zahnarzt	oid_zahnarzt
CHAT.2A	(H)BA für Mitarbeiter(innen) in Arztpraxis, oder Krankenhaus	Mitarbeiter medizinische Institution (z. B. in Arztpraxis, Krankenhaus). Der „Mitarbeiter medizinische Institution“ verkörpert gegenüber der TI die	Nicht definiert	Nicht definiert	Nicht definiert	Nicht definiert

		Institution des Arztes				
CHAT .2ZA	(H)BA für Mitarb eiter- (innen) in Zahna rzt- praxis	Mitarbeiter medizinische Institution (z. B. in Zahnarztpraxis) . Der „Mitarbeiter medizinische Institution“ verkörpert gegenüber der TI die Institution des Zahnarztes	Nicht definie rt	Nicht definier t	Nicht definiert	Nicht definiert
CHAT .2A	SMC-B	Mitarbeiter medizinische Institution Arztpraxis (inkl. Praxis ärztlicher Psychotherapeu t) mit Autorisierung und Protokollierung gemäß § 291a Abs. 5 Satz 4 SGB V. Der „Mitarbeiter medizinische Institution“ verkörpert gegenüber der TI die Institution des Arztes.	Mitarbe iter Arzt	KV	Betriebsstätte Arzt	oid_praxis_arzt
CHAT .2A	SMC-B	Behörden des Öffentlichen Gesundheitsdi enstes sowie Institutionen der Fachärzte für Arbeitsmedizi n, Betriebsärzte und Institutio nen der Vorsorge- oder Rehabilitation nach SGB V § 107 Absatz 2	Mitarbe iter weitere Ärztlich e Institut ion	Nicht definier t	Betriebsstätt e Arbeitsmedizi n Betriebsstätt e Öffentlicher Gesundheitsd ienst Betriebsstätt e Vorsorge- und Rehabilitatio n	oid_arbeitsmedizin oid_gesundheitsdien st oid_vorsorge_reha

		oder der medizinischen Rehabilitation nach SGB VI oder der Heilbehandlung einschließlich medizinischer Rehabilitation nach SGB VII				
CHAT .2Z A	SMC-B	Mitarbeiter medizinische Institution Zahnarztpraxis mit Autorisierung und Protokollierung gemäß § 291a Abs. 5 Satz 4 SGB V. Der „Mitarbeiter medizinische Institution“ verkörpert gegenüber der TI die Institution des Zahnarztes.	Mitarbeiter Zahnarzt	KZBV	Zahnarztpraxis	oid_zahnarztpraxis
CHAT .2A	SMC-B	Mitarbeiter medizinische Institution Krankenhaus mit Autorisierung und Protokollierung gemäß § 291a Abs. 5 Satz 4 SGB V. Der „Mitarbeiter medizinische Institution“ verkörpert gegenüber der TI die Institution des Arztes.	Mitarbeiter Krankenhaus	DKTIG	Krankenhaus	oid_krankenhaus
3						
CHAT .3	HBA – Apotheker	Apotheker in einer öffentlichen Apotheke	Apotheker	BAK	Apotheker/in	oid_apotheker

		oder einer Krankenhausapotheke, jeweils mit Sitz in Deutschland.				
CHAT .3	(H)BA für Mitarbeiter (-innen) der Apotheke	Mitarbeiter Apotheke als berufsmäßiger Gehilfe oder Person, die zur Vorbereitung auf den Beruf tätig ist, gemäß § 291a Abs. 4 [SGB V]. Der „Mitarbeiter Apotheke“ verkörpert gegenüber der TI die Institution des Apothekers.	Apotheker	BAK	Apotheker-assistent/in Pharmazieingenieur/in Apotheken-assistent/-in	oid_apotheker assistent oid_pharmazie ingenieur oid_apotheken assistent
CHAT .3	SMC-B	Mitarbeiter Apotheke mit Autorisierung und Protokollierung gemäß § 291a Abs.5 Satz 4 SGB V. Der „Mitarbeiter Apotheke“ verkörpert gegenüber der TI die Institution des Apothekers.	Mitarbeiter Apotheke	Für den jeweiligen Betrieb s-erlaubnis-inhaber zuständige Apothekerkammer	Öffentliche Apotheke	oid_öffentliche _apotheke
4						
CHAT .4	HBA – Psychotherapeut	Psychotherapeut, Psychologischer Psychotherapeut, Kinder- und Jugendlichen-psychotherapeut	Psychotherapeut	BPTK	Psychotherapeut/ in Psychologische/r Psychotherapeut/ in Kinder- und Jugendlichen-psychotherapeut/-in	oid_psychotherapeut oid_ps_psychotherapeut oid_kuj_psychotherapeut

CHAT .4	SMC- B	Institutionskarte eines Psychotherapeuten. Der mit der Karte mögliche Zugriff auf die medizinischen Anwendungen der eGK ist ausschließlich dem psychologischen Psychotherapeuten und dem Kinder- und Jugendlichen-psychotherapeuten selbst gestattet und nicht seinen berufsmäßigen Gehilfen.	Mitarbeiter Psychotherapeut	KV	Betriebsstätte Psychotherapeut	oid_praxis_psychotherapeut
5						

CHAT .5	(H)BA sonstige Leistungs- erbringer	Heilmittelerbringer mit (H)BA Hilfsmittelerbringer mit BA	Sonstige Leistungs- erbringer	Nicht definiert	Nicht definiert Altenp- fleger/-in Pflegefachfrau- en und Pflegefachmän- ner Hebamme Physiotherape- ut/-in Augenoptiker/- in und Optometrist/- in Hörakustiker/- in Orthopädiesch- uhmacher/-in Betriebsstätte Orthopädiotec- hniker Betriebsstätte Zahntechniker Zahntechniker /-in	oid_altenpfleger oid_pflegefachkraft oid_hebamme oid_physiotherapeut oid_augenoptiker oid_hoerakustiker oid_institution_orthopa- edieschuhmacher oid_orthopaedieschuh- macher oid_institution_zahntec- hniker oid_zahntechniker Nicht definiert
CHAT .5	SMC-B sonstige Leistungs- erbringer	Institutionskar- te eines Hilfsmitt- elerbringer mit BA.	Institut ion Sonstige Leistungs- erbringer	Nicht definiert	Betriebsstätte Gesundheits-, Kranken- und Altenpflege Betriebsstätte Geburtshilfe Betriebsstätte Physiotherapie Betriebsstätte Augenoptiker Betriebsstätte Hörakustiker Betriebsstätte Orthopädiesch- uhmacher Betriebsstätte Orthopädiotec	oid_institution_pflege oid_geburtshilfe oid_praxis_physiothera- peut oid_institution_augen- optiker oid_institution_hoerak- ustiker oid_institution_orthopa- edieschuhmacher

					hniker Betriebsstätte Zahntechniker Rettungsleitste lle Betriebsstätte Sanitätsdienst Bundeswehr	oid_institution_orthopa edietechniker oid_institution_zahntec hniker oid_rettungsleitstellen oid_sanitaetsdienst_bu ndeswehr
6						
CHA. 6	SMC	Kein fachlicher Akteur - wird nicht verwendet	Nicht definie rt	Nicht definier t	Nicht definiert	Nicht definiert
7						
CHAT .7	(H)BA	Rettungsassiste nt Bei den Akteuren handelt es sich um „Angehörige eines anderen Heilberufs, die für die Berufsausübung oder die Führung der Berufsbezeichn ung eine staatlich geregelter Ausbildung“ (§ 291a Abs. 4 Satz 1 Nr. 2e) absolviert haben.	Andere r Heilber uf	Nicht definier t	Rettungs- assistent/-in Notfall- sanitäter/-in	oid_rettungsassistent oid_notfallsanitaeter
CHAT .7	SMC-B	Mobile Einrichtung Rettungsdienst	Nicht definier rt	Nicht definier t	Betriebsstätte Mobile Einrichtung Rettungsdienst	oid_mobile_einrichtung _rettungsdienst
8						
CHAT .8	SMC-B (ohne Zugriff auf med. Daten)	Mitarbeiter von Gesundheits- einrichtungen ohne eigenen HBA oder BA	Mitarbe iter Medizin ische Institut ion	Nicht definier t	Nicht definiert	Nicht definiert

CHAT .8		Mitarbeiter von Krankenkassen	Mitarbeiter Kosten träger	GKV-SV	Betriebsstätte Kostenträger	oid_kostentraeger
CHAT .8		Verifikationskarten Kostenträger	Mitarbeiter Kosten träger	GKV-SV	n.a. (Karte enthält keine X.509)	n.a. (Karte enthält keine X.509)
9						
CHAT .9	SMC-B (mit Zugriff auf med. Daten)	a) Mitarbeiter von Gesundheitseinrichtungen ohne eigenen HBA oder BA	a) Mitarbeiter Medizinische Institution	Nicht definiert	Nicht definiert	Nicht definiert
CHAT .9		b) ohne zugeordneten Akteur, sichere Einsatzumgebung für Versicherten	b) Versicherter	Nicht definiert	Nicht definiert	Nicht definiert

2494

2495 6.3.2 Authentisierung einer Funktionseinheit

2496 Es werden die Zugriffsprofile CHAT.51, CHAT.53 – CHAT.55 für eine Authentisierung
2497 einer Funktionseinheit unterschieden (CV-Gerätezertifikate). Es handelt sich dabei um
2498 CV-Zertifikate der Generation 2:

2499

2500 **Tabelle 54: Tab_PKI_255 Zugriffsprofile G2 für eine Authentisierung einer**
2501 **Funktionseinheit**

Zugriffsprofil		CV-Zertifikate für	Funktionseinheit
CHAT.51		gSMC-K	Signaturanwendungskomponente (SAK)
CHAT.53		HBA	Stapelfähige SSEE und Remote-PIN-Empfänger
CHAT.54		gSMC-KT	Remote-PIN-Sender
CHAT.55		SM-B	Remote-PIN-Empfänger

2502 *Hinweis 1: Das Zugriffsprofil CHAT.52 war für die SMC-RFID vorgesehen, diese wird*
2503 *derzeit nicht verwendet.*

2504 *Hinweis 2: Ursprünglich wurden auch Zugriffsprofile bzw. CV-Gerätezertifikate für die*
2505 *Generation 1 festgelegt. In der Praxis kommen aber nur CV-Gerätezertifikate der*
2506 *Generation 2 zum Einsatz.*

2507

2508 **GS-A_4622 - Zugriffsprofil einer gSMC-K**

2509 Der Kartenherausgeber MUSS sicherstellen, dass das CV-Gerätezertifikat einer gSMC-K
2510 als Flagliste den Wert '0000 0000 0001' hat (Zugriffsprofil 51 für G2 gemäß
2511 Tab_PKI_918).

2512 [\leq]

2513 **GS-A_5126 - Zugriffsprofil einer gSMC-KT**

2514 Der Kartenherausgeber MUSS sicherstellen, dass das CV-Gerätezertifikat einer gSMC-KT
2515 als Flagliste den Wert '00 0000 0000 0002' hat (Zugriffsprofil 54 für G2 gemäß
2516 Tab_PKI_918).

2517 [\leq]

2518 **GS-A_4623 - Zugriffsprofil eines HBA**

2519 Der Kartenherausgeber MUSS sicherstellen, dass das CV-Gerätezertifikat eines HBA als
2520 Flagliste den Wert '00 0000 0000 000C' hat (Zugriffsprofil 53 für G2 gemäß
2521 Tab_PKI_918).

2522 [\leq]

2523 **GS-A_4624 - Zugriffsprofil einer SM-B**

2524 Der Kartenherausgeber MUSS sicherstellen, dass das CV-Gerätezertifikat einer SM-B als
2525 Flagliste den Wert '00 0000 0000 0004' hat (Zugriffsprofil 55 für G2 gemäß
2526 Tab_PKI_918).

2527 [\leq]

2528 **GS-A_5335 - Zugriffsprofil einer gSMC-K für Administrationszwecke**

2529 Der Kartenherausgeber MUSS sicherstellen, dass die Flagliste des CV-Zertifikats für die
2530 Authentisierung einer gSMC-K gegenüber einem Aktualisierungssystem den Wert '00
2531 0000 0000 0000' hat (Zugriffsprofil 0 für G2 gemäß Tab_PKI_918).

2532 [\leq]

2533 **6.4 CV-Zertifikatsprofile der Generation 2**

2534 Für G2-Karten ist der Einsatz von elliptischen Kurven (ELC) in CV-Zertifikaten
2535 vorgesehen, basierend auf den Festlegungen in [EN 14890-1]. Die CV-Zertifikate
2536 erhalten eine komplett neue Struktur, es erfolgt ein Umstieg von nicht
2537 selbstbeschreibenden, RSA-basierten Zertifikaten auf selbstbeschreibende, ELC-basierte
2538 Zertifikate mit Anhang (Appendix).

2539 Im Gegensatz zu den nicht selbstbeschreibenden Zertifikaten werden die
2540 selbstbeschreibenden Zertifikate durch Konkatenation der Datenobjekte gebildet. Dabei
2541 wird jedem Datenfeld ein Tag und ein Längenfeld vorangestellt, damit jedes Datenfeld
2542 eindeutig interpretiert werden kann (Tag, Length, Value-Prinzip (TLV)). Der zu
2543 signierende Teil ist die Konkatenation der Datenobjekte.

2544 **6.4.1 Berechtigung einer CVC-CA zur Zertifikatserstellung**

2545 TSP-CVC, die zur Ausstellung von CV-Zertifikaten für

2546

- genau einen Kartentyp mit einem oder mehreren zugehörigen CV-
2547 Gerätezertifikaten

2548

- und genau ein Rollen-Zugriffsprofil (nur bei HBA u. SMC-B)

2549 berechtigt sind, erhalten ein CV-CA-Zertifikat, in dem nur genau diese Zugriffsprofile
2550 über die hinterlegte Flaglist abgebildet sind.

2551 TSP-CVC, die zur Ausstellung von CV-Zertifikaten für mehrere Kartentypen berechtigt
2552 sind, können ein CV-CA-Zertifikat mit kombinierten Zugriffsprofilen nach folgendem
2553 Schema beantragen:

- 2554 • CVC-CA für eGK
2555 Diese CV-Zertifikate sind immer aus einer dedizierten CVC-CA zu erstellen. Eine
2556 Kombination mit anderen Zugriffsprofilen ist nicht zulässig.
- 2557 • CVC-CA für HBA und SMC-B
2558 Die Ausstellung von CV-Zertifikaten dieser Kartentypen in allen
2559 Ausprägungsformen kann durch eine einzige CVC-CA mit kombinierten
2560 Zugriffsprofilen (veroderte Flaglist) erfolgen.
- 2561 • CVC-CA für gSMC-x
2562 Die Ausstellung von CV-Zertifikaten dieser Kartentypen in allen
2563 Ausprägungsformen kann durch eine einzige CVC-CA mit kombinierten
2564 Zugriffsprofilen (veroderte Flaglist) erfolgen.

2565 **GS-A_5213 - CA-Flaglist für CVC-CA eines Profiltyps**

2566 Die CVC-Root-CA MUSS bei der Generierung eines CA-Zertifikates
2567 (a) für eine CVC-CA, welche ausschließlich zur Ausstellung von EE-Zertifikaten eines
2568 bestimmten Zugriffsprofils (oder eines spezifischen Tupels aus Geräte- und Rollen-
2569 Zugriffsprofilen) aus Tab_PKI_919, genau die zugeordnete Flaglist aus der Spalte Sub-CA
2570 in das CA-Zertifikat einbringen.
2571 (b) Für eine CVC-CA mit kombinierten Zugriffsprofilen ist die Veroderung der zugehörigen
2572 Flaglisten aus Tab_PKI_919 zulässig für die Zugriffsprofile
2573 (b.1) aller HBA- und SMC-B sowie
2574 (b.2) aller gSMC-K und gSMC-KT.
2575 [\leq]

2576 **6.4.2 Aufbau und Bestandteile der CV-Zertifikate der Generation 2**

2577 Obwohl die Struktur selbstbeschreibend ist, enthalten die CV-Zertifikate einen Certificate
2578 Profile Identifier, der angibt, welche Datenelemente in welcher Reihenfolge in das CV-
2579 Zertifikat einzustellen sind. Im Einzelnen sind das:

- 2580 1. Certificate Profile Identifier (CPI) gemäß 6.4.3.1
- 2581 2. Certification Authority Reference (CAR) gemäß 6.4.3.2
- 2582 3. Öffentlicher Schlüssel: Das Datenobjekt zum öffentlichen Schlüssel enthält neben
2583 einer OID, welche den Verwendungszweck des öffentlichen Schlüssels
2584 kennzeichnet, den öffentlichen Punkt Q (siehe [EN 14890-1#Table 234]).
- 2585 4. Certificate Holder Reference (CHR) gemäß 6.4.3.4
- 2586 5. Certificate Holder Authorization Template (CHAT): Eine Flagliste
2587 beschreibt gemäß [EN 14890-1#14.9.3.6] die Rechte, die einem
2588 Zertifikatsinhaber nach einer erfolgreichen Authentisierung eingeräumt werden.
- 2589 6. Certificate Effective Date (CED): Dieses Datenobjekt enthält das Datum des
2590 Inkrafttretens des Zertifikates.
- 2591 7. Certificate Expiration Date (CXD): Dieses Datenobjekt enthält das Datum mit dem
2592 Gültigkeitsende des Zertifikates.

2593 **Berechtigungssteuerung über die Flagliste im Feld CHAT**

2594 Die Zugriffsberechtigung einer Karte auf die Inhalte einer anderen Karte (Bsp. HBA auf
2595 eGK) kann sehr differenziert über einzelne Bits der sog. Flagliste im Feld CHAT gesteuert
2596 werden.

2597 • Im CVC-CA-Zertifikat (ausgestellt durch die CVC-Root-CA) steuert die Flagliste,
2598 welche CV-Berechtigungen durch diese CA ausgestellt werden können.

2599 • Im CV-Zertifikat (ausgestellt durch eine CVC-CA) einer Karte steuert die Flagliste,
2600 über welche Berechtigung diese Karte (d. h. der Karten- und Zertifikatsinhaber)
2601 gegenüber anderen Karten der TI verfügt.

2602 **6.4.3 Zertifikatsprofil eines CV-Zertifikates für ELC-Schlüssel**

2603 Für ELC-Schlüssel ist genau ein Zertifikatsprofil zu berücksichtigen. Dieses
2604 Zertifikatsprofil gilt sowohl für CV-Zertifikate, welche den öffentlichen Schlüssel einer CA
2605 transportieren, als auch für CV-Zertifikate, welche öffentliche Schlüssel zu
2606 Authentisierungszwecken transportieren.

2607 **6.4.3.1 Certificate Profile Identifier (CPI)**

2608 Die hier folgenden Anforderungen sind konform zu Table 205 aus [EN 14890-1#14.9.2].

2609 **GS-A_4986 - Datenobjekt für das Feld Card Profile Identifier in G2**

2610 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2611 MUSS den Wert für den CPI in das Datenobjekt '5F29' einstellen.

2612 [\leq]

2613 **GS-A_4987 - Wert des Card Profile Identifier in G2**

2614 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2615 MUSS als Wert für den CPI '70' eintragen.

2616 [\leq]

2617 **6.4.3.2 Certification Authority Reference (CAR)**

2618 Die hier folgenden Anforderungen sind konform zu [EN 14890-1#14.7.2].

2619 **Tabelle 55: Tab_PKI_266 Aufbau CAR für Karten der Generation 2**

	CA Name	Service-Indikator	CA-spezifische Information	Algorithmenreferenz	Datum
Länge	5 Byte	1 BCD	1 BCD	2 BCD	2 BCD
zugelassene Werte	Anbieterkennung gemäß Registrierung bei Fraunhofer SIT	Verwendungszweck des PrK: '8' für die Ausstellung von CA-Zertifikaten '1' für die Ausstellung von EE-Zertifikate	zur freien Verwendung durch den Anbieter; dient der Unterscheidung verschiedener CA-	'02' für ELC/ECC	letzte 2 Ziffern des Jahres der CA-Schlüsselerzeugung

			Schlüsselpaar re		
--	--	--	---------------------	--	--

2620 *Hinweis: Die Anbieterkennung - bestehend aus 5 Buchstaben - wird hier gemäß [EN*
2621 *14890-1] auch "CA Name" genannt. Es handelt sich dabei aber nicht um den Namen der*
2622 *CA als technische Instanz, sondern um den Namen des TSP (TSP-CVC oder CVC-Root).*
2623 *Nur die vollständige CAR benennt und referenziert den öffentlichen Schlüssel einer CVC-*
2624 *CA eindeutig.*

2625 **GS-A_4988 - Datenobjekt für das Feld Certificate Authority Reference in G2**

2626 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2627 MUSS den Wert für die CAR in das Datenobjekt '42' einstellen

2628 [\leq]

2629 **GS-A_4989 - Länge der Certificate Authority Reference in G2**

2630 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2631 MUSS für die CAR ein acht Oktett langes Wertfeld verwenden.

2632 [\leq]

2633 **GS-A_4990 - Verwendung des Feldes Certificate Authority Reference in G2**

2634 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2635 MUSS das Feld CAR weiter unterteilen in die Konkatenation der Datenelemente CA Name,
2636 Service-Indikator, CA-spezifische Information, Algorithmenreferenz und Datum sowie
2637 dabei die Festlegungen bzgl. Länge und zugelassener Werte gemäß Tab_PKI_266
2638 berücksichtigen.

2639 [\leq]

2640 **GS-A_4991 - Zuordnung von CAR zu Schlüsselpaar des Herausgebers für G2**

2641 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2642 MUSS sicherstellen, dass die Zuordnung zwischen Certificate Authority Reference (CAR)
2643 und Schlüsselpaar eindeutig ist.

2644 [\leq]

2645 **6.4.3.3 Öffentlicher Schlüssel**

2646 Für den Aufbau des öffentlichen Schlüssels gelten die folgenden Anforderungen, konform
2647 zu [BSI-TR-03110#D.3]:

2648 **GS-A_4992 - Datenobjekt für den öffentlichen Schlüssel**

2649 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2650 MUSS den öffentlichen Schlüssel in das Datenobjekt '7F49' einstellen.

2651 [\leq]

2652 **GS-A_4993 - Aufbau eines öffentlichen Schlüssel**

2653 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2654 MUSS in das Wertfeld des Datenobjekt '7F49' des öffentlichen Schlüssels genau zwei
2655 Datenobjekte eintragen. Dabei MÜSSEN das erste Datenobjekt ein Objektidentifizier
2656 OIDPuK gemäß Tabelle Tab_PKI_901 und das zweite Datenobjekt ein Datenobjekt
2657 DO '86' mit dem öffentlichen Punkt Q, dessen Wertfeld sich aus Tabelle Tab_PKI_902
2658 ergibt, sein.

2659 [\leq]

2660

2661 **Tabelle 56: Tab_PKI_901 Objektidentifizier des öffentlichen Schlüssels eines CV-**
2662 **Zertifikats der Generation 2**

Verwendungszweck des CV-Zertifikats	Domainparameter	Objektidentifizier
Transport des öffentlichen Signaturprüfchlüssels einer CA	brainpoolP256r1	OID _{PuK} = '06-L06-ecdsa-with-SHA256' OID _{Hex} = '06 08 2A8648CE3D040302' OID _{Dez} = '1.2.840.10045.4.3.2'
	brainpoolP384r1	OID _{PuK} = '06-L06-ecdsa-with-SHA384' OID _{Hex} = '06 08 2A8648CE3D040303' OID _{Dez} = '1.2.840.10045.4.3.3'
	brainpoolP512r1	OID _{PuK} = '06-L06-ecdsa-with-SHA512' OID _{Hex} = '06 08 2A8648CE3D040304' OID _{Dez} = '1.2.840.10045.4.3.4'
Transport eines öffentlichen Authentisierungsschlüssels	brainpoolP256r1	OID _{PuK} = '06-L06-authS_gemSpec-COS-G2_ecc-with-sha256' OID _{Hex} = '06 06 2B2403050301' OID _{Dez} = '1.3.36.3.5.3.1'
	brainpoolP384r1	OID _{PuK} = '06-L06-authS_gemSpec-COS-G2_ecc-with-sha384' OID _{Hex} = '06 06 2B2403050302' OID _{Dez} = '1.3.36.3.5.3.2'
	brainpoolP512r1	OID _{PuK} = '06-L06-authS_gemSpec-COS-G2_ecc-with-sha512' OID _{Hex} = '06 06 2B2403050303' OID _{Dez} = '1.3.36.3.5.3.3'

2663 **Tabelle 57: Tab_PKI_902 Punkt Q des öffentlichen Schlüssels eines CV-Zertifikats der**
2664 **Generation 2**
2665

Domainparameter	Codierung eines öffentlichen Punktes Q in DO'86'
brainpoolP256r1	DO'86' = '86 - 41 - P2OS(Q)'
brainpoolP384r1	DO'86' = '86 - 61 - P2OS(Q)'
brainpoolP512r1	DO'86' = '86 - 8181 - P2OS(Q)'

2666 *Hinweis: In Tab_PKI_902 beschreibt P2OS(Q) die Konvertierung eines Punktes Q in einen*
2667 *Oktettstring gemäß „Uncompressed Encoding“ aus [BSI-TR-03111#3.2.1].*

2668 **6.4.3.4 Certificate Holder Reference (CHR)**

2669 Die hier folgenden Anforderungen weichen bezüglich der Längenvorgaben von [EN-
2670 14890#14.7.3] ab.

2671 **GS-A_4994 - Datenobjekt für die Certificate Holder Reference**

2672 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2673 MUSS die Certificate Holder Reference in das Datenobjekt '5F20' einstellen.

2674 [**<=**]

GS-A_4995 - Wertfeld der Certificate Holder Reference

Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS in das Wertfeld der Certificate Holder Reference eine Schlüsselreferenz zum öffentlichen Schlüssel gemäß [GS-A_4629], bei Ausgabe des CV-Zertifikats durch die CVC-Root-CA, bzw. gemäß [GS-A_4630], bei Ausgabe des CV-Zertifikats durch die CVC-CA, in das CV-Zertifikat der Generation 2 einstellen.

[<=]

GS-A_4629 - CHR des CV-Zertifikats einer CVC-CA

Die CVC-Root-CA MUSS als Wert für die CHR gemäß Tab_PKI_258 die CAR der CVC-CA zu dem Schlüsselpaar eintragen, für den das CV-Zertifikat erzeugt wird.

[<=]

GS-A_4630 - CHR des CV-Zertifikats einer Chipkarte

Der TSP-CVC MUSS als Wert für die CHR gemäß Tab_PKI_258 ein Datum eintragen, das aus der Konkatenation einer zwei Byte langen, innerhalb der Chipkarte eindeutigen Schlüsselidentifikation und der 10 Byte langen ICCSN als weltweit eindeutigen Identifier der Chipkarte besteht.

[<=]

Bei dem Aufbau und der Belegung des Feldes CHR wird unterschieden zwischen einem CV-Zertifikat für eine CVC-CA und einem CV-Zertifikat für eine Chipkarte:

Tabelle 58: Tab_PKI_258 Aufbau CHR

CV-Zertifikat für	Länge CHR	Inhalt	
		CHR	Anforderung für CHR
CVC-CA	8 Bytes siehe Kap. 6.4.3.2	CAR zu dem Schlüsselpaar siehe Kap. 6.4.3.2	
Chipkarte	12 Bytes	'xx xx' ICCSN der Chipkarte	
	Zertifikat		
eGK	C.eGK.AUT_CVC.E256	'00 09' ICCSN	Card-G2-A_2363
HBA	C.HPC.AUTR_CVC.R2048E256	'00 1006' ICCSN	Card-G2-A_33853386
	C.HPC.AUTRAUTD_SUK_CVC.E256	'00 0609' ICCSN	Card-G2-A_33863387

	C.HPC.AUTD_SUKSMC.AUTR_CVC.E256	'00 0906' ICCSN	Card-G2- A_33873389
SMC-B	C.SMC.AUTRAUTD__RPE_CVC.R2048E256	'00 1009' ICCSN	Card-G2- A_33883390
	C.SMC.AUTRAUT_CVC.E256	'00 0605' ICCSN	Card-G2- A_33893328
	C.SMC.AUTD__RPEAUT_CVC.E256E384	'00 0906' ICCSN	Card-G2- A_33903331
gSMC-K	C.SMC.AUTSAK.AUTD_CVC.E256	'00 050A' ICCSN	Card-G2- A_33282638
	C.SMC.AUTSAK.AUTD_CVC.E384	'00 060F' ICCSN	Card-G2- A_33312640
	C.SAKSMC.AUTD_RPS_CVC.E256	'00 0A' ICCSN	Card-G2- A_26382500
	C.SAK:SMS.AUTD_RPS_CVC.E384	'00 0F' ICCSN	Card-G2- A_26402502
gSMC-KT	C.SMC.AUTD_RPSKTRADV.AUTR_CVC.E256	'00 0A05' ICCSN	Card-G2- A_2500 -
	C:SMS.AUTD_RPS_CVC.E384	'00 0F' ICCSN	Card-G2- A_2502
KTR-AdV	C.KTRADV.AUTR_CVC.E256	'00 05' ICCSN	-

2697 Anmerkung: Die ICCSN der KTR-AdV entspricht der ICCSN der verwendeten SM-B KTR-
2698 AdV.

2699 Eine Chipkarte kann auch mehrere Schlüsselpaare für eine C2C-Authentisierung (und
2700 damit auch mehrere CV-Zertifikate) enthalten. Über die konkrete Belegung von 'xx xx'
2701 wird sichergestellt, dass die Zuordnung von CV-Zertifikat zu einem Schlüsselpaar der
2702 Chipkarte eindeutig ist. Das genaue Vorgehen hierbei wird durch die einzelnen
2703 Spezifikationen der konkreten Chipkarten der TI festgelegt.

2704 6.4.3.5 Certificate Holder Authorization Template (CHAT)

2705 Die hier folgenden Anforderungen sind konform zu [EN 14890-1#14.9.3.6].

GS-A_4996 - Wertfeld des Certificate Holder Authorization Templates

Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS das Certificate Holder Authorization Template in das Datenobjekt '7F4C' einstellen.

[<=]

GS-A_4997 - Aufbau der Certificate Holder Authorization Templates

Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS in das Wertfeld des Datenobjekt '7F4C' genau zwei Datenobjekte eintragen. Dabei MUSS das zweite Datenobjekt ein Datenobjekt DO'53' gemäß Tabelle Tab_PKI_910 (bei Anwendung von oid_cvc_fl_ti) oder Tab_PKI_911 (bei Anwendung von oid_cvc_fl_cms) sein und das erste Datenobjekt einen Objektidentifizier OIDflags gemäß Tabelle Tab_PKI_904 enthalten, der angibt, wie die Flags im zweiten Datenobjekt zu interpretieren sind. Die Umsetzung eines bestimmten Berechtigungsprofils MUSS durch die Kombination der Einzelflags gemäß TAB_PKI_918 erfolgen.

[<=]

Tabelle 59: Tab_PKI_904 Mögliche Objektidentifizier OIDflags in Certificate Holder Authorization Templates

OIDflags
OIDflags = '06-L06-oid_cvc_fl_ti
OIDflags = '06-L06- oid_cvc_fl_cms

Hinweis: Die Festlegung der OID erfolgt in der Spezifikation Festlegung von OIDs [gemSpec_OID#Tab_PKI_408].

6.4.3.6 Certificate Effective Date (CED)

Die hier folgenden Angaben sind konform zu [BSI-TR-03110-3#D.2.1.3].

GS-A_4998 - Datenobjekt des Certificate Effective Date

Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS das Certificate Effective Date in das Datenobjekt '5F25' einstellen.

[<=]

GS-A_4999 - Länge des Certificate Effective Date

Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS für das Certificate Effective Date ein Wertfeld der Länge sechs Oktett einstellen.

[<=]

GS-A_5000 - Format des Certificate Effective Date

Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS ein Datum in der Form YYMMDD in unkomprimierter BCD Form in das Wertfeld des Certificate Effective Date eintragen.

[<=]

6.4.3.7 Certificate Expiration Date (CXD)

Die hier folgenden Angaben sind konform zu [BSI-TR-03110-3#D.2.1.3].

GS-A_5001 - Datenobjekt des Certificate Expiration Date

Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS das Certificate Expiration Date in das Datenobjekt '5F24' einstellen.

[<=]

2747 **GS-A_5002 - Länge des Certificate Expiration Date**
 2748 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
 2749 MUSS für das Certificate Expiration Date ein Wertfeld der Länge sechs Oktett einstellen.
 2750 [\leq]

2751 **GS-A_5003 - Format des Certificate Expiration Date**
 2752 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
 2753 MUSS ein Datum in der Form YYMMDD in unkomprimierter BCD Form in das Wertfeld des
 2754 Certificate Expiration Date eintragen.
 2755 [\leq]

2756 **6.4.3.8 Zu signierende Nachricht M eines CV-Zertifikates der Generation** 2757 **2**

2758 **GS-A_5004 - Tag der zu signierenden Nachricht M eines CV-Zertifikates**
 2759 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
 2760 MUSS die zu signierende Nachricht des CV-Zertifikats in das Datenobjekt '7F4E'
 2761 einstellen.
 2762 [\leq]

2763 **GS-A_5005 - Datenstruktur der zu signierenden Nachricht M eines CV-**
 2764 **Zertifikates**
 2765 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
 2766 MUSS die zu signierende Nachricht M des CV-Zertifikats gemäß Tabelle Tab_PKI_905
 2767 bilden.
 2768 [\leq]

2769

2770 **Tabelle 60: Tab_PKI_905 Zu signierende Nachricht M eines CV-Zertifikates**

<i>M</i>	=	DO '7F4E'
DO '7F4E'	=	'7F4E'-L7F4E-(DO '5F29' DO '42' DO '7F49' DO '5F20' DO '7F4C' DO '5F25' DO '5F24')

2771 **6.4.4 Struktur und Inhalt eines CV-Zertifikates für ELC-Schlüssel** 2772 **der Generation 2**

2773 **GS-A_5006 - Signatur des Zertifikatsdatenobjekts**
 2774 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
 2775 MUSS die Signatur der Nachricht *M* des CV-Zertifikates in Abhängigkeit vom
 2776 Domainparameter des privaten Signaturschlüssels *PrK* des Herausgebers gemäß Tabelle
 2777 Tab_PKI_906 erzeugen.
 2778 [\leq]

2779

2780 **Tabelle 61: Tab_PKI_906 Signatur der Nachricht M eines CV-Zertifikats**

Domainparameter des privaten Schlüssels <i>PrK</i>	Signaturformat
---	----------------

brainpoolP256r1	(R, S) = ECDSA(PrK , SHA_256(M)) im Format ecdsa-plain-SHA256 gemäß BSI-TR-03111#5.2.1.1
brainpoolP384r1	(R, S) = ECDSA(PrK , SHA_384(M)) im Format ecdsa-plain-SHA384 gemäß BSI-TR-03111#5.2.1.1
brainpoolP512r1	(R, S) = ECDSA(PrK , SHA_512(M)) im Format ecdsa-plain-SHA512 gemäß BSI-TR-03111#5.2.1.1

2781

2782 **GS-A_5007 - Tag eines Zertifikatsdatenobjekts**

2783 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2784 MUSS die Inhalte des Zertifikatsdatenobjekts in das Datenobjekt '7F21' einstellen.

2785 [\leq]

2786 **GS-A_5008 - Aufbau eines Zertifikatsdatenobjekts**

2787 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2788 MUSS das CV-Zertifikat als zusammengesetztes Datenobjekt gemäß Tabelle
2789 Tab_PKI_907 erzeugen. Er MUSS dabei sicherstellen, dass das zusammengesetzte
2790 Datenelement genau die beiden primitiven Datenobjekte in der dargestellten Reihenfolge
2791 enthält.

2792 [\leq]

2793

2794 **Tabelle 62: Tab_PKI_907 Struktur und Inhalt eines CV-Zertifikat**

Tag	L	Wert		
'7F21'	L7F21	CV-Zertifikat		
		Tag	L	Wert
		'7F4E'	L7F4E	Nachricht M (gemäß Tabelle 60: Tab_PKI_905 Zu signierende Nachricht M eines CV- Zertifikates) ohne Tag und Längenangabe
		'5F37'	L5F37	Signatur = $R S$ (gemäß Tabelle 61: Tab_PKI_906 Signatur der Nachricht M eines CV-Zertifikats)

2795 **6.4.5 Struktur und Inhalt eines CV-Zertifikates für ELC-Schlüssel**
2796 **der Generation 2**

2797 Die nachfolgenden Strukturdiagramme fassen die zuvor beschriebenen Definitionen und
2798 Festlegungen zu den einzelnen Feldern der CV-Zertifikate übersichtlich zusammen,
2799 normativ sind jedoch nur die in den Anforderungen ausgewiesenen Definitionen.

2800 **6.4.5.1 Struktur und Inhalt von CA CV-Zertifikaten für ELC-Schlüssel**

2801 **Tabelle 63: Tab_PKI_912 CA CV-Zertifikate für 256 bit ELC-Schlüssel, insgesamt**
2802 **220 Oktett**

Tag	L	Wert					
´7F21´	´81D8´	CV-Zertifikat					
		Tag	L	Wert			
		´7F4E´	´8191´	Nachricht <i>M</i>			
			Tag	L	Wert		
			´5F29´	´01´	CPI = ´70´		
			´42´	´08´	CAR		
			´7F49´	´4D´	öffentlicher Schlüssel		
				Tag	L	Wert	
				´06´	´08´	´2A8648CE3D040302´	
				´86´	´41´	P2OS(Q, 32)	
			´5F20´	´08´	CHR		
			´7F4C´	´13´	CHAT		
				Tag	L	Wert	
				´06´	´08´	OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}	
				´53´	´07´	´xx...xx´, Flagliste	
			´5F25´	´06´	CED		
			´5F24´	´06´	CXD		
			´5F37´	´40´	Signatur = <i>R</i> <i>S</i>		

2803

2804 **Tabelle 64: Tab_PKI_913 CA CV-Zertifikate für 384 bit ELC-Schlüssel, insgesamt**
2805 **285 Oktett**

Tag	L	Wert				
‘7F21’	‘820118’	CV-Zertifikat				
		Tag	L	Wert		
		‘7F4E’	‘81B1’	Nachricht <i>M</i>		
			Tag	L	Wert	
			‘5F29’	‘01’	CPI = ‘70’	
			‘42’	‘08’	CAR	
			‘7F49’	‘6D’	öffentlicher Schlüssel	
				Tag	L	Wert
		‘06’		‘08’	‘2A8648CE3D040303’	

			´86´	´61´	P2OS(Q, 48)
		´5F20´	´08´	CHR	
		´7F4C´	´13´	CHAT	
			Tag	L	Wert
			´06´	´08´	OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}
			´53´	´07´	´XX...XX´, Flagliste
		´5F25´	´06´	CED	
		´5F24´	´06´	CXD	
´5F37´	´60´	Signatur = R S			

2806

2807

2808

Tabelle 65: Tab_PKI_914 CA CV-Zertifikate für 512 bit ELC-Schlüssel, insgesamt 352 Oktett

Tag	L	Wert			
'7F21'	'82015B'	CV-Zertifikat			
		Tag	L	Wert	
		'7F4E'	'81D3'	Nachricht <i>M</i>	
				Tag	L
				'5F29'	'01'
				'42'	'08'
				'7F49'	'818E'
				Wert	
				'06'	'08'
				'2A8648CE3D040304'	
				'86'	'8181'
				P2OS(Q, 64)	
				'5F20'	'08'
				CHR	
				'7F4C'	'13'
				CHAT	
				Wert	
				'06'	'08'
				OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}	
				'53'	'07'
				'xx...xx', Flagliste	

			5F25	06	CED
			5F24	06	CXD
	5F37	8180	Signatur = R S		

2809

2810 6.4.5.2 Struktur und Inhalt von Cross-CV-Zertifikaten für ELC-Schlüssel

2811 Ein Cross-CV-Zertifikat ist ein CV-Zertifikat, welches verschiedene Vertrauensräume
2812 verbindet. Eine CVC-Root-CA bestätigt den öffentlichen Schlüssel einer anderen CVC-
2813 Root-CA.

2814 **Tabelle 66: Tab_PKI_937 Cross-CV-Zertifikat für ELC-Schlüssel**

Tag	L	Wert			
7F21	*	CV-Zertifikat			
		Tag	L	Wert	
		7F4E	*	Nachricht M	
				Tag	L Wert
				5F29	01 CPI = 70
				42	08 CAR
				7F49	* öffentlicher Schlüssel
					Tag L Wert
					06 08 *
				86	* *
				5F20	08 CHR
				7F4C	13 CHAT
					Tag L Wert
					06 08 OID = oid_cvc_fl_ti
				53	07 FF FFFF FFFF FFFF
				5F25	06 CED
				5F24	06 CXD
		5F37	*	Signatur = R S	

2815 *Anmerkung: Die mit * gefüllten Feldinhalte müssen anhand der in 6.4.5.1 spezifizierten*
2816 *Zertifikatsprofile für 256/384/512 bit ELC-Schlüssel ermittelt bzw. berechnet werden.*

6.4.5.3 Struktur und Inhalt von Endnutzer-CV-Zertifikaten für ELC-Schlüssel

Tabelle 67: Tab_PKI_915 Endnutzer-CV-Zertifikate für 256 bit ELC-Schlüssel, insgesamt 222 Oktett

Tag	L	Wert				
‘7F21’	‘81DA’	CV-Zertifikat				
	Tag	L	Wert			
	‘7F4E’	‘8193’	Nachricht <i>M</i>			
		Tag	L	Wert		
		‘5F29’	‘01’	CPI = ‘70’		
		‘42’	‘08’	CAR		
		‘7F49’	‘4B’	öffentlicher Schlüssel		
				Tag	L	Wert
				‘06’	‘06’	‘2B2403050301’
				‘86’	‘41’	P2OS(Q, 32)
		‘5F20’	‘0C’	CHR		
		‘7F4C’	‘13’	CHAT		
				Tag	L	Wert
				‘06’	‘08’	OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}
				‘53’	‘07’	‘xx...xx’, Flagliste
		‘5F25’	‘06’	CED		
	‘5F24’	‘06’	CXD			
	‘5F37’	‘40’	Signatur = <i>R</i> <i>S</i>			

Tabelle 68: Tab_PKI_916 Endnutzer-CV-Zertifikate für 384 bit ELC-Schlüssel, insgesamt 287 Oktett

Tag	L	Wert				
‘7F21’	‘82011A’	CV-Zertifikat				
		Tag	L	Wert		
		‘7F4E’	‘81B3’	Nachricht <i>M</i>		
			Tag	L	Wert	
			‘5F29’	‘01’	CPI = ‘70’	
			‘42’	‘08’	CAR	
			‘7F49’	‘6B’	öffentlicher Schlüssel	
					Tag	L

			'06	'06	'2B2403050302'
			'86	'61	P2OS(Q, 48)
		'5F20'	'0C'	CHR	
		'7F4C'	'13'	CHAT	
			Tag	L	Wert
			'06	'08	OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}
			'53	'07	'xx...xx', Flagliste
		'5F25'	'06'	CED	
		'5F24'	'06'	CXD	
		'5F37'	'60'	Signatur = R S	

2825
2826

2827
2828

Tabelle 69: Tab_PKI_917 Endnutzer-CV-Zertifikate für 512 bit ELC-Schlüssel, insgesamt 354 Oktett

Tag	L	Wert				
7F21	82015D	CV-Zertifikat				
		Tag	L	Wert		
		7F4E	81D5	Nachricht M		
		Tag	L	Wert		
		5F29	01	CPI = 70		
		42	08	CAR		
		7F49	818C	öffentlicher Schlüssel		
				Tag	L	Wert
				06	06	2B2403050303
				86	8181	P2OS(Q, 64)
		5F20	0C	CHR		
		7F4C	13	CHAT		
				Tag	L	Wert
				06	08	OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}
				53	07	xx...xx, Flagliste
		5F25	06	CED		
		5F24	06	CXD		
		5F37	8180	Signatur = R S		

2829 Der Wert für OID_{PKI} ergibt sich dabei entsprechend Tabelle 57: Tab_PKI_901
2830 Objektidentifizier des öffentlichen Schlüssels eines CV-Zertifikats der Generation 2.

2831 **6.4.6 Flagliste mit Berechtigungen in CV-Zertifikaten für ELC-** 2832 **Schlüssel**

2833 Die Flagliste *flagList* im DO '53' innerhalb von CHAT eines CV-Zertifikates erfüllt zwei
2834 Aufgaben: Zum einen zeigt sie in den oberen beiden Bits an, welche Rolle das CV-
2835 Zertifikat in der PKI-Struktur spielt. Die übrigen Bits zeigen an, welche Aktionen nach
2836 einer erfolgreichen Authentisierung freigeschaltet werden. Die Festlegungen zur Rolle
2837 sind konform zu [BSI-TR-03110-3#C.4]. Anders als in [BSI-TR-03110-3#C.4] wird im
2838 Folgenden dem höchstwertigen Bit der Flagliste die Nummer null zugeordnet. In den Bits
2839 b2 bis b55 zeigt ein gesetztes Bit an, dass durch eine erfolgreiche Authentisierung das
2840 Recht erworben wird die zugehörige Aktion durchzuführen. In den Bits b2 bis b55 zeigt
2841 ein gelöscht Bit an, dass auch nach einer erfolgreichen Authentisierung die zugehörige
2842 Aktion nicht freigeschaltet ist.

2843

2844 **Tabelle 70: Tab_PKI_910 TI-PKI, Bedeutung der Bits innerhalb der Flagliste eines CHAT**

Bitnummer	Bedeutung
Rollenkennzeichnung in den Bits b0 und b1	
b0 b1 = 11 ₂	Rolle = Root-CA-Schlüssel (in [BSI-TR-03110-3] als CVCA bezeichnet)
b0 b1 = 10 ₂	Rolle = CA unterhalb der Root-CA
b0 b1 = 00 ₂	Rolle = CVC enthält öffentlichen Authentisierungsschlüssel
Flaglist mit Funktionen, die nach einer erfolgreichen Authentisierung freigeschaltet werden	
b02	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b03	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b04	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b05	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b06	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b07	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b08	eGK: Verwendung der ESIGN-AUTN-Funktionalität mit PIN.CH
b09	eGK: Verwendung der ESIGN-AUTN Funktionalität ohne PIN
b10	eGK: Verwendung der ESIGN-ENCV Funktionalität mit PIN.CH
b11	eGK: Verwendung der ESIGN-ENCV Funktionalität ohne PIN
b12	eGK: Verwendung der ESIGN-AUT Funktionalität
b13	eGK: Verwendung der ESIGN-ENC Funktionalität
b14	eGK: Notfalldatensatz verbergen und sichtbar machen

b15	eGK: Notfalldatensatz schreiben, löschen (hier „erase“, nicht „delete“) mit PIN.NFD
b16	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b17	eGK: Notfalldatensatz lesen mit MRPIN.NFD
b18	eGK: Notfalldatensatz lesen ohne PIN
b19	eGK: Persönliche Erklärungen (DPE) verbergen und sichtbar machen
b20	eGK: DPE schreiben, löschen (hier „erase“, nicht „delete“) mit MRPIN.DPE
b21	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b22	eGK: DPE lesen mit MRPIN.DPE_READ
b23	eGK: DPE lesen ohne PIN
b24	eGK: Einwilligungen und Verweise im DF.HCA verbergen und sichtbar machen
b25	eGK: Einwilligungen im DF.HCA lesen und löschen (hier „erase“, nicht „delete“)
b26	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b27	eGK: Einwilligungen im DF.HCA schreiben
b28	eGK: Verweise im DF.HCA lesen und schreiben
b29	eGK: Geschützte Versichertendaten lesen mit PIN.CH
b30	eGK: Geschützte Versichertendaten lesen ohne PIN
b31	eGK: Loggingdaten schreiben mit PIN.CH
b32	eGK: Loggingdaten schreiben ohne PIN
b33	eGK: Zugriff in den AdV-Umgebungen (vormals: Loggingdaten lesen)
b34	eGK: Prüfungsnachweis lesen und schreiben
b35	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b36	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b37	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b38	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b39	eGK: Gesundheitsdatendienste verbergen und sichtbar machen
b40	eGK: Gesundheitsdatendienste lesen, schreiben und löschen (hier „erase“)
b41	eGK: Organspendedatensatz lesen mit MRPIN.OSE
b42	eGK: Organspendedatensatz lesen ohne PIN
b43	eGK: Organspendedatensatz schreiben, löschen (hier „erase“, nicht „delete“) mit MRPIN.OSE
b44	eGK: Organspendedatensatz aktivieren/deaktivieren mit MRPIN.OSE

b45	eGK: AMTS-Datensatz verbergen und sichtbar machen
b46	eGK: AMTS-Datensatz lesen
b47	eGK: AMTS-Datensatz schreiben, löschen (hier „erase“, nicht „delete“)
b48	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b49	Fingerprint des COS erstellen
b50	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b51	Auslöser Komfortsignatur
b52	Sichere Signaturerstellungseinheit (SSEE)
b53	Remote-PIN Empfänger
b54	Remote-PIN Sender
b55	SAK für Stapel- oder Komfortsignatur

2845

2846 *Hinweis: Die Rechtedifferenzierung zwischen den Rollen Ärztin/Arzt und*
 2847 *Zahnärztin/Zahnarzt ist in die Tabelle Tab_PKI_918 aufgenommen worden: für die*
 2848 *beiden Berufsgruppen gibt es unterschiedliche CHAT-Werte gemäß den Zuordnungen der*
 2849 *Rechte, die gleichlautend gelten für die entsprechenden Institutionskarten SMC-B der*
 2850 *Arztpraxen/Krankenhäuser (CHAT-Wert wie für Ärztin/Arzt) bzw. der Zahnarztpraxen*
 2851 *(CHAT-Wert wie für Zahnärztin/Zahnarzt)*

2852

2853 **Tabelle 71: Tab_PKI_918 Abbildung von Rollenberechtigungen Zugriffsprofilen auf**
 2854 **äquivalente Flaglisten**

Zugriffsprofil		CHAT-Wert / Flagliste (G2)
Rolle (AUTR_CVC)	CHAT.0	‘00 0000 0000 0000’
	CHAT.1	‘00 AE1A CDC1 DC00’
	CHAT.2A Ärztin/Arzt Fachliche Institution des Arztes Krankenhaus	‘00 5D29 DAA0 BB00’
	CHAT.2ZA Zahnärztin/Zahnarzt Fachliche Institution des Zahnarztes	‘00 5D20 DAA0 8300’
	CHAT.3	‘00 5C40 DAA0 8300’
	CHAT.4	‘00 4C40 DAA0 8200’
	CHAT.5	‘00 5C00 02A0 0000’

	CHAT.6	wird nicht verwendet
	CHAT.7	‘00 0020 0480 0000’
	CHAT.8	‘00 4000 02A0 0000’
	CHAT.9	‘00 6800 0AA0 0000’
Gerät (AUTD _CVC)	CHAT.51	‘00 0000 0000 0001’
	CHAT.53	‘00 0000 0000 000C’
	CHAT.54	‘00 0000 0000 0002’
	CHAT.55	‘00 0000 0000 0004’
Adminis- tration (AUT _CVC)	CHAT.0	‘00 0000 0000 0000’

2855 *Anmerkung: Zur Berechnung der Sub-CA-Flagliste einer bestimmten Karte muss das*
2856 *Zugriffsprofil der zugehörigen Rolle mit denen des Geräts kombiniert werden (siehe*
2857 *Tab_PKI_919).*

2858
2859 *Beispiel: Ein TSP-CVC ist nur für die Ausgabe von CV-Zertifikaten für Zahnärzte-HBAs*
2860 *zugelassen.*

2861 *Die Flagliste für das Profil CHAT.2ZA des Rollen-Zertifikates lautet* ‘00 5D20 DAA0
2862 *8300’.*

2863 *Die Flagliste für das Profil CHAT.53 des Geräte-Zertifikates lautet* ‘00 0000 0000
2864 *000C’.*

2865 *Die Kombination, bzw. Veroderung der beiden Flaglisten ergibt* ‘00 5D20 DAA0 830C’.

2866 *Die Flagliste einer Sub-CA beginnt mit der Bit-Folge ‘10’ (vgl. Tab_PKI_910). Der Wert*
2867 *für die Flagliste des CA-Zertifikates des TSP-CVC in Tab_PKI_919 lautet* ‘80 5D20
2868 *DAA0 830C’.*

2869

2870 **Tabelle 72: Tab_PKI_919 Sub-CA-Flaglisten nach Kartentyp (G2) und Zugriffsprofilen**

Kartentyp / Geräte- Zugriffsprofil	Rollen- Zugriffsprofil	Sub-CA
CHAT-Wert / Flagliste für ein bestimmtes Zugriffsprofil		
eGK	CHAT.0	‘8000000000000000’
KTR-AdV	CHAT.1 & CHAT.0	‘80AE1ACDC1DC04’
gSMC-K / CHAT.51	-	‘8000000000000001’
gSMC-KT / CHAT.54	-	‘8000000000000002’

HBA / CHAT.53	CHAT.2A	‘805D29DAA0BB0C’
HBA / CHAT.53	CHAT.2ZA	‘805D20DAA0830C’
HBA / CHAT.53	CHAT.3	‘805C40DAA0830C’
HBA / CHAT.53	CHAT.4	‘804C40DAA0820C’
HBA / CHAT.53	CHAT.5	‘805C0002A0000C’
HBA / CHAT.53	CHAT.7	‘8000200480000C’
SMC-B / CHAT.55	CHAT.1	‘80AE1ACDC1DC04’
SMC-B / CHAT.55	CHAT.2A	‘805D29DAA0BB04’
SMC-B / CHAT.55	CHAT.2ZA	‘805D20DAA08304’
SMC-B / CHAT.55	CHAT.3	‘805C40DAA08304’
SMC-B / CHAT.55	CHAT.4	‘804C40DAA08204’
SMC-B / CHAT.55	CHAT.8	‘80400002A00004’
SMC-B / CHAT.55	CHAT.9	‘8068000AA00004’
CHAT-Wert / Flagliste für kombinierte Zugriffsprofile		
eGK	CHAT.0	–
gSMC-K und gSMC-KT / CHAT.51 & 54	–	‘800000000000003’
HBA und SMC-B / CHAT.53 & 55	CHAT.1 - 5 & 7- 9	‘80FF7BDFE1FF0C’

Tabelle 73: Tab_PKI_911 CMS-PKI, Bedeutung der Bits innerhalb der Flagliste eines CHAT

Bitnummer	Bedeutung
Rollenkennzeichnung in den Bits b0 und b1	
b0 b1 = 11 ₂	Rolle = Root-CA-Schlüssel (in [BSI-TR-03110-3] als CVCA bezeichnet)
b0 b1 = 10 ₂	Rolle = CA unterhalb der Root-CA
b0 b1 = 00 ₂	Rolle = CVC enthält öffentlichen Authentisierungsschlüssel
Flagliste mit Funktionen, die nach einer erfolgreichen Authentisierung freigeschaltet werden	
b02 ... b07	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen

b08	Administrative Tätigkeiten CMS
b09	Administrative Tätigkeiten VSD
b10	Administrative Tätigkeiten zum Schreiben von CV-Zertifikaten
b11	Administrative Tätigkeiten eines TSP zur Laufzeitverlängerung der QES-Anwendung
b12 ... b55	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen

2874

ENTWURF

2875

7 Festlegung von OIDs

2876 In der vorliegenden Spezifikation wird die Verwendung von OIDs in den
2877 Zertifikatsprofilen der TI-PKI über die Verwendung der OID-Referenznamen geregelt. Die
2878 Zuordnung dieser OID-Referenzen zu den konkreten OID-Werten sowie deren Verwaltung
2879 der OIDs werden im Dokument [gemSpec_OID] normativ beschrieben.

ENTWURF

2880

8 Prüfung von Zertifikaten

2881 Für die Nutzung und Statusprüfung von Zertifikaten in der TI gilt:

- 2882 • Das TSL-Signer-CA-Zertifikat (RSA oder ECDSA) bildet den Vertrauensanker für
2883 die TI.
- 2884 • Das TSL-Signer-CA-Zertifikat (RSA) und das TSL-Signer-CA-Zertifikat (ECDSA)
2885 sind jeweils über Cross-Zertifikate verknüpft.
- 2886 • Jedes Produkt kann immer nur einen der beiden Vertrauensanker aktiv haben. Ein
2887 Wechsel der Vertrauensräume ist über die Cross-Zertifikate möglich.
- 2888 • Eine TSL stellt (i. S. einer Whitelist) den Vertrauensraum für die in der TI
2889 zugelassenen Aussteller-CA dar.
- 2890 • Dabei stellt die TSL(RSA) den Vertrauensraum (RSA) und die TSL(ECC-RSA) den
2891 Vertrauensraum (ECC-RSA) dar. (Hinweis: siehe bzgl. TSL- und Vertrauensraum-
2892 Begrifflichkeiten das Kapitel 8.1.1)
- 2893 • nonQES-Aussteller-CA-Zertifikate werden ausschließlich gegen die TSL geprüft
- 2894 • QES-Aussteller-CA-Zertifikate werden
2895 hinsichtlich ihres VDA-Qualifikationsstatus gemäß [eIDAS] gegen die BNetzA-VL
2896 geprüft. (Vgl. §9 [VDG].)
- 2897 • Als Vertrauensanker für die BNetzA-VL fungieren jeweils die aktuell publizierten
2898 BNetzA-VL-Signer-Zertifikate. Diese werden mittels TSL in die QES-prüfenden
2899 Systeme (Konnektoren) eingebracht und aktualisiert.
- 2900 • End-Entity-Zertifikate werden gegen den OCSP-Dienst der Aussteller-CA geprüft,
2901 außer die Statusprüfung für einen bestimmten Zertifikatstyp ist explizit optional
2902 oder nicht vorgesehen.

2903

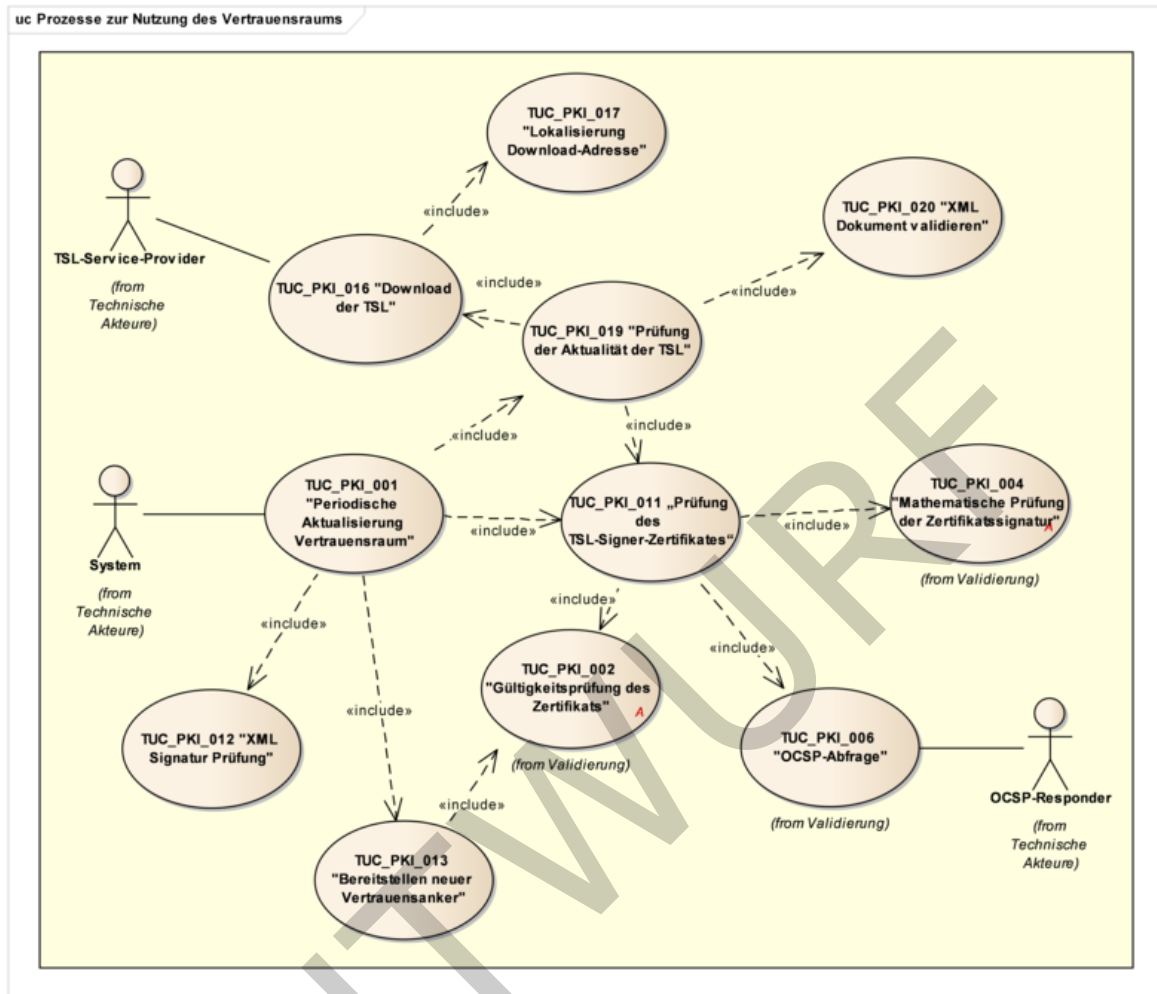


Abbildung 5: Use Case Diagramm „Prozesse zur Nutzung des TI-Vertrauensraums“

Die Funktionalitäten der zertifikatsprüfenden Komponenten werden nachfolgend in „Technischen Use Cases“ (TUCs) beschrieben und spezifiziert. Dabei können in jedem der beschriebenen Schritte eines TUC Fehler auftreten. Übergreifend gilt dazu:

GS-A_4637 - TUCs, Durchführung Fehlerüberprüfung

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN bei der Ausführung eines TUC auf Verarbeitungsfehler prüfen und eine definierte Fehlerbehandlung einleiten.

[<=]

GS-A_4829 - TUCs, Fehlerbehandlung

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN bei der Fehlerbehandlung von TUCs Systemmeldungen ausgeben und der Prozess muss beendet werden, sofern der TUC keine spezifische Fehlerbehandlung beschreibt.

[<=]

Bei der Beschreibung der TUCs sind folgende Punkte zu beachten:

- Die unter „Vorbedingungen“ beschriebenen Bedingungen sind nicht Bestandteil des TUC und werden im Ablauf des TUC nicht explizit geprüft. Stattdessen muss der Kontext aus dem heraus der TUC aufgerufen wird sicherstellen, dass bei einer

2923 verletztten Vorbedingung, in keinem Fall das Ergebnis eines TUC als positiv
2924 bewertet wird, z. B. eine Prüfung als erfolgreich eingestuft wird.
2925 In welcher Form die Umsetzung von Vorbedingungen erfolgt (z. B. durch explizite
2926 Prüfung, Teilausführung des TUC oder durch Wechsel eines Systemzustands) ist
2927 nicht Gegenstand der TUC-Spezifikation. Ein TUC muss nicht stets
2928 Vorbedingungen haben.

- 2929 • Wird im Ablauf des TUC ein anderer TUC aufgerufen und dieser endet mit einer
2930 Fehlermeldung, so wird auch der aufrufende TUC mit dieser Fehlermeldung
2931 beendet, sofern nichts anderes festgelegt ist. Daher setzen sich die möglichen
2932 Fehlermeldungen eines TUC aus den Fehlerfällen im TUC-Ablauf und allen
2933 Fehlermeldungen der aufgerufenen TUCs zusammen.

2934 ~~Für die Nutzung und die Statusprüfung von nonQES-Zertifikaten im Internet gilt:~~

2935 Zur Zertifikatsprüfung werden die Vorgaben aus [gemKPT_PKI_TIP] Kap. 6.5
2936 „Zertifikatsprüfung nonQES“ berücksichtigt.

2937 Die Zertifikatsprüfung erfolgt gemäß [RFC5280] und gemäß [COMMON-PKI].

- 2938 • Der TI-Vertrauensraum wird im Internet durch die Bereitstellung von OCSP-
2939 Statusauskünften zu allen in der TSL enthaltenen CAs abgebildet.
- 2940 • Mangels einer der TSL entsprechenden Whitelist für zugelassene CAs im Internet
2941 müssen sämtliche nonQES CA- und EE-X.509-Zertifikate der TI im Feld
2942 **authorityInfoAccess** die URL des zugehörigen und im Internet erreichbaren
2943 OCSP-Responders enthalten.
- 2944 • Im Internet erfolgt die Prüfung der nonQES CA- und EE-Zertifikaten (HBA, SMC-B)
2945 entlang des Zertifizierungspfades bis hin zur gematik Root-CA.
- 2946 • Die nonQES-X.509-Zertifikate der temporär zu unterstützenden HBA-
2947 Vorläuferkarten werden auf Basis der dafür etablierten Statusauskunftsdienste
2948 geprüft.

2949 **GS-A_5043 - Auflösung von OCSP-Adressen im Internet**

2950 TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN für Zertifikatstypen, die zusätzlich zur
2951 TI auch im Internet statusgeprüft werden, sicherstellen, dass die im Zertifikat
2952 eingetragene OCSP-Responderadresse im Internet aufgelöst und eine Statusabfrage
2953 erfolgreich durchgeführt werden kann.

2954 [**<=**]

2955 Der TI-Vertrauensraum für QES-Zertifikate wird im Internet nicht gesondert abgebildet.
2956 Die Zertifikate werden gemäß der für QES üblichen Verfahren validiert und statusgeprüft.

2957 Über die Bereitstellung von nonQES-CA- und EE-Zertifikatsinformationen im Internet
2958 hinaus werden durch die Spezifikationen der TI keine Aussagen getroffen über Art und
2959 Umfang von durchzuführenden Schritten im Kontext der Zertifikatsprüfung durch die
2960 Anwendungen im Internet.

2961 **8.1 Vertrauensraum der TI**

2962 Grundlage jeder zertifikatsbasierten Prüfung auf Vertrauenswürdigkeit in der TI ist die
2963 gesicherte Information über den aktuell gültigen TI-Vertrauensraum, gegen den eine
2964 solche Prüfung erfolgt.

2965 Der Vertrauensraum der TI besteht also aus der Menge der CAs (bzw. deren Zertifikate),
2966 die in der TI zugelassen, also als vertrauenswürdig anerkannt sind. Außerdem enthält er

2967 die Einsatzzwecke, für welche die CAs End-Entity-Zertifikate ausgeben dürfen. Dieser TI-
2968 Vertrauensraum wird in der TSL abgebildet.

2969 Die TSL enthält Informationen gemäß [ETSI_TS_102_231#5]. Sie beinhalten neben den
2970 CA-Zertifikaten im TI-Vertrauensraum zusätzliche Angaben, wie z. B. die
2971 Sequenznummer oder die Adressen und Zertifikate der zuständigen OCSP-Responder.

2972 Die TSL spielt also in zertifikatsprüfenden Komponenten die zentrale Rolle.

2973 Konkret bereitgestellt wird die TSL als TSL-Datei in Form einer signierten XML-Datei
2974 gemäß [ETSI_TS_102_231#B].

2975

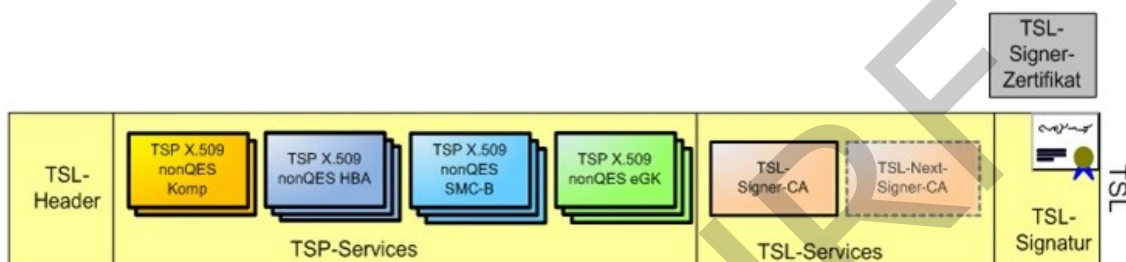


Abbildung 6 : Aufbau der TSL

2976

2977

2978

2979 *Hinweis: Die TSL-Informationen müssen also nicht zwingend in Form der XML-Syntax der*
2980 *TSL-Datei vorgehalten werden. Sie können auch ganz oder teilweise in einen sicheren*
2981 *Speicher des Systems (Truststore) importiert werden.*

2982 Die nachfolgende Gliederung der Teilschritte einer Prüfung orientiert sich an den
2983 Vorgaben des TSL-Standards [ETSI_TS_102_231#H] – mit den Konkretisierungen für die
2984 TI sowie ergänzt um TI-spezifische Erweiterungen der TI-Vertrauensraumprüfung.

2985 Die notwendigen Prüfschritte zur Prüfung des TI-Vertrauensraums werden in Form von
2986 Technischen Use Cases dargestellt:

2987

- 2988 • Initialisierung / Aktualisierung des TI-Vertrauensraumes
- 2989 • Lokalisieren der TSL-Datei
- 2990 • Download der TSL-Datei (ggf. nach vorheriger Aktualitätsprüfung mittels
Hashwert-Vergleichsverfahren)
- 2991 • Validierung der TSL-Datei
- 2992 • Prüfung der Integrität und Authentizität der TSL-Datei durch die Prüfung ihrer
2993 Signatur

2994 Die bereits im Internet etablierten PKIs der Vorläuferkarten (qSIG, ZOD), die im Rahmen
2995 des Bestandsschutzes zu unterstützen sind, werden in der TI insoweit berücksichtigt,
2996 dass die zugehörigen CAs in den TI-Vertrauensraum (also die TSL) aufgenommen und die
2997 Statusinformationen der zugehörigen EE-Zertifikate durch Nachnutzung des OCSP-
2998 Responder Proxy zur Verfügung gestellt werden (s. Beschreibung in
2999 [gemKPT_Arch_TIP#5.4.13]).

8.1.1 TSL im Kontext der ECC-Migration

Der Vertrauensraum der TI sah bisher nur die Verwendung von RSA-2048 als Schlüsselalgorithmus vor. Die TSL enthielt daher nur RSA-Zertifikate (im Kontext X.509).

Im Zuge der ECC-Migration müssen alle Produkttypen so umgestellt werden, dass sie neben RSA-2048 auch ECC-256 unterstützen (vgl. [gemSpec_Krypt#5]). Daher wird neben der bisher vorhandenen reinen RSA-basierten TSL (im Folgenden „TSL(RSA)“ genannt) eine zweite TSL bereitgestellt, die sowohl die neuen ECDSA-basierten Zertifikate als auch aus Rückwärtskompatibilitäts-Gründen die weiterhin benötigten RSA-basierten Zertifikate enthält. Diese zweite neue TSL wird im Folgenden als „**TSL(ECC-RSA)**“ bezeichnet.

Bis zum vollständigen Abschluss der ECC-Migration werden beide TSL-Varianten vom TSL-Dienst bereitgestellt. Technisch sind die beiden Varianten unabhängig voneinander. Der Übergang des Vertrauensraumes von Vertrauensraum (RSA) auf Vertrauensraum (ECC-RSA) geschieht dabei durch Cross-Zertifizierung der entsprechenden TSL-Signer-CA-Zertifikate.

Neben dem Download-Punkt für die TSL(RSA) gibt es einen weiteren Download-Punkt für die TSL(ECC-RSA). Die TSL(RSA) wird weiterhin mit einem RSA-basierten Zertifikat signiert. Die TSL(ECC-RSA) erhält eine Signatur auf ECDSA-Basis.

Produkttypen, die ausschließlich RSA-Zertifikate verwenden und/oder prüfen, verwenden die TSL(RSA). Alle Produkttypen, die ECC-Zertifikate nutzen oder validieren, müssen die TSL(ECC-RSA) verwenden.

Die gematik empfiehlt Anbietern sogenannter Weiterer elektronischer Anwendungen (aAdG und aAdG-NetG-TI) die Berücksichtigung der für die ECC-Migration aufgeführten Hinweise und Anforderungen. Letztere sind gekennzeichnet durch die Ergänzung „(ECC-Migration)“ im Titel der relevanten Anforderungen.

8.1.2 Initialisierung TI-Vertrauensraum

Verfügt eine zugelassene Komponente der TI noch nicht über einen aktuell gültigen TI-Vertrauensanker, muss für dieses Komponentenexemplar eine Initialisierung des TI-Vertrauensraumes ohne Vorbedingungen durchgeführt werden. Diese besteht aus den zwei Teilprozessen:

- Die sichere Einbringung des TI-Vertrauensankers in Form des aktuell gültigen TSL-Signer-CA-Zertifikates in die Komponente in einer gesicherten Umgebung des Herstellers oder Betreibers
- Einbringung einer aktuellen TSL in die Komponente durch den Hersteller oder den Vor-Ort-Administrator

Dies gilt für die Anwendungsfälle

- der Erstinbetriebnahme einer Komponente und
- der Wiederinbetriebnahme bzw. Systemwiederherstellung zu einem Zeitpunkt, zu dem die in der Komponente vorhandene TSL nicht mehr gültig und zwischenzeitlich ein Wechsel des TI-Vertrauensankers erfolgte.

Die folgenden Anforderungen gelten unter den oben genannten Rahmenbedingungen sowohl für die Initialisierung eines RSA- als auch eines im Rahmen der ECC-Migration notwendigen ECC-Vertrauensankers.

GS-A_4640 - Identifizierung/Validierung des TI-Vertrauensankers bei der initialen Einbringung

Hersteller von Produkttypen der TI, die Zertifikate prüfen, MÜSSEN bei der initialen Einbringung das aktuell gültige TSL-Signer-CA-Zertifikat eindeutig identifizieren und mittels Fingerprint validieren, bevor dieses Zertifikat als TI-Vertrauensanker in die Komponente eingebracht werden darf.

[<=]

GS-A_4641 - Initiale Einbringung TI-Vertrauensanker

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN die initiale Einbringung des aktuell gültigen TSL-Signer-CA-Zertifikat als TI-Vertrauensanker in die Komponente nachweislich sicher vor Manipulation vornehmen.

[<=]

WA-A_2111 - Initiale Einbringung TI-Vertrauensanker in andere Anwendungen

Der Anbieter einer aAdG oder aAdG-NetG-TI MUSS sicherstellen, dass die initiale Einbringung des aktuell gültigen TSL-Signer-CA-Zertifikats als TI-Vertrauensanker in Dienste der aAdG oder der aAdG-NetG-TI nachweislich sicher vor Manipulation vorgenommen wird.[<=]

GS-A_4748 - Initiale Einbringung TSL-Datei

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN die initiale Einbringung der TSL-Datei in die Komponente nachweislich sicher vor Manipulation vornehmen.

[<=]

WA-A_2112 - Initiale Einbringung TSL-Datei

Der Anbieter einer aAdG oder aAdG-NetG-TI MUSS sicherstellen, dass die initiale Einbringung der TSL-Datei in Dienste der aAdG oder der aAdG-NetG-TI nachweislich sicher vor Manipulation vorgenommen wird.[<=]

Im Abschnitt 8.1.1 werden relevante Punkte zur ECC-Migration erläutert. Daher gilt für Produkttypen, die auf ECC migriert bzw. im Vertrauensraum (ECC-RSA) betrieben werden:

A_17688 - Nutzung des ECC-RSA-Vertrauensraumes (ECC-Migration)

Die Produkttypen der TI, die ECC-Zertifikate validieren müssen, MÜSSEN das TSL-Signer-CA-Zertifikat (ECDSA) als TI-Vertrauensanker und die TSL(ECC-RSA) verwenden.

[<=]

Nutzung von Cross-Zertifikaten für die Etablierung des ECC-Vertrauensankers:

Neben den oben in 8.1.2 beschriebenen Festlegungen zum initialen Einbringen eines neuen Vertrauensankers (auch für ECC-RSA) gibt es eine weitere Möglichkeit zur Etablierung. Für die von der ECC-Migration betroffenen Produkttypen, die auf Basis eines bereits etablierten Vertrauensankers (RSA) den neuen Vertrauensanker (ECC-RSA) (entspricht TSL-Signer-CA-Zertifikat (ECDSA)) etablieren (z.B. Konnektoren), gilt folgendes:

A_17689 - Nutzung von Cross-Zertifikaten für Vertrauensraum-Wechsel nach ECC-RSA (ECC-Migration)

Die Produkttypen der TI, die einen Vertrauensanker (ECC-RSA) zur Etablierung des Vertrauensraumes (ECC-RSA) initialisieren, KÖNNEN Cross-Zertifikate verwenden, um auf Basis ihres bereits etablierten Vertrauensankers (RSA) in den Vertrauensraum (ECC-RSA) zu wechseln.

[<=]

A_17820 - Nutzung von Cross-Zertifikaten für Vertrauensraum-Wechsel nach RSA (ECC-Migration)

Die Produkttypen der TI, die einen Vertrauensanker (RSA) zur Etablierung des Vertrauensraumes (RSA) initialisieren, KÖNNEN Cross-Zertifikate verwenden, um auf Basis ihres bereits etablierten Vertrauensankers (ECC-RSA) in den Vertrauensraum (RSA) zu wechseln.

[<=]

Hinweis: Die Nutzung von Cross-Zertifikaten für den Wechsel des Vertrauensraumes ist für den Konnektor besonders geregelt (s. gemSpec_Kon#A_17837 und A_17784).

A_17821 - Wechsel des Vertrauensraumes mittels Cross-Zertifikaten (ECC-Migration)

Die Produkttypen der TI, die den Vertrauensraum mittels Cross-Zertifikates wechseln (siehe A_17689 und A_17820) MÜSSEN die folgenden Schritte erfolgreich durchlaufen, um auf den Vertrauensanker des neuen Vertrauensraumes zu wechseln.

Vorbedingung: Das System besitzt zum aktuell etablierten Vertrauensraum den aktuell aktiven Vertrauensanker (der zu dem benutzten Cross-Zertifikat passend ist).

1. Falls eine TSL (aus dem aktuellen Vertrauensraum) bereits im System vorhanden ist, MUSS das Element TSLSequenceNumber aus dieser TSL ausgelesen und der Wert im persistenten (sicheren) Speicher des Systems abgelegt werden. Für jeden TSLSequenceNumber-Nummernkreis (s.u.) wird ein separater Wert geführt.
2. Es MUSS das neue Vertrauensanker-Zertifikat (TSL-Signer-CA<X>) in das System eingelesen werden (auch ggf. als Download realisierbar).
3. Es MUSS das Cross-Zertifikates (C.GEM-TSL-CA<X>-CROSS<Y>) in das System eingelesen werden (auch ggf. als Download realisierbar).
4. Es MUSS ein Vergleich des PublicKey im Cross-Zertifikat mit dem PublicKey im CA-Zertifikat des neuen Vertrauensankers (TSL-Signer-CA<X>) durchgeführt werden.
5. Es MUSS eine Signatur-Prüfung des Cross-Zertifikates gegen den alten Vertrauensanker im System (TSL-Signer-CA<Y>) durchgeführt werden analog zu TUC_PKI_004.
6. Es MUSS eine neue TSL (passend zum Vertrauensanker TSL-Signer-CA<X>) analog zu GS-A_4748 eingebracht und danach das Element TSLSequenceNumber ausgelesen werden. Falls für den TSLSequenceNumber-Nummernkreis der neu eingebrachten TSL eine TSLSequenceNumber im sicheren Speicher vorliegt, dann muss die TSLSequenceNumber der neu eingebrachten TSL höher sein, als dieser Wert.

Wenn einer der Schritte fehlschlägt, MUSS der Vertrauensraum-Wechsel-Prozess abgebrochen werden und der alte Vertrauensanker (TSL-Signer-CA<Y>) im System verbleiben.

Nach erfolgreichem Durchlaufen aller Schritte, MUSS der Vertrauensanker (TSL-Signer-CA<X>) im System etabliert sein.

Erklärungen zu den verwendeten Begriffen:

- Vertrauensanker im System vor dem Vertrauensraum-Wechsel: TSL-Signer-CA<Y>
- Vertrauensanker des neuen Vertrauensraumes: TSL-Signer-CA<X>
- Verwendetes Cross-Zertifikat: C.GEM-TSL-CA<X>-CROSS<Y>
- TSLSequenceNumber – Nummernkreis RSA: 0..9999

- TLSSequenceNumber – Nummernkreis ECC-RSA: ab 10000

[<=]

Für die Zertifikatsprüfung bei der initialen Einbringung und Validierung der TSL gelten die Bestimmungen für Offline-Anwendungsszenarien aus Kap. 8.3.2.4, d. h. eine Statusprüfung des TSL-Signatur-Zertifikates erfolgt nicht.

Die in der TI zugelassenen Zertifikate der vertrauenswürdigen Herausgeber (TSPs) sind in der TSL enthalten. Bei der Initialisierung des TI-Vertrauensraumes wird der Truststore befüllt, d.h. die Zertifikate können aus der TSL-Datei ausgelesen und z. B. in den Truststore des Systems importiert werden. Der Status der bezeichneten Vertrauensdienste wird jeweils im Inhalt des TSL-Elementes „ServiceStatus“ mit einem URI identifiziert. Die untenstehende Tabelle zeigt die erlaubten Status und erklärt deren Bedeutung in der TI Für X.509-CA-Zertifikate gibt die Kombination des Inhaltes von „ServiceStatus“ mit dem Zeitpunkt in „StatusStartingTime“ an,

- seit wann ein Zertifikat dem aktuellen TI-X.509-Vertrauensraum angehört (mit „/inaccord“ markiert), oder
- bis wann unter dem CA-Zertifikat EE-Zertifikate ausgestellt werden durften.
- „/revoked“: Dies entspricht einer Sperrung gemäß dem Kettenmodell für QES (s. [gemKPT_PKI_TIP#2.4.3]) oder dem Kompromissmodell für nonQES-Zertifikate für HBA und SMC-B (s. [gemKPT_PKI_TIP#2.4.2]). Diese erfolgt bei einer Einstellung des Betriebs aufgrund eines nicht-sicherheitskritischen Incidents, gegebenenfalls auch nach einem sicherheitskritischen Incident. Vgl. dazu auch [gemKPT_PKI_TIP#2.3.3.5] „Sperrung von CA-Zertifikaten in der TSL“ und [gemKPT_PKI_TIP#2.4]. „Gültigkeitsmodelle X.509-Zertifikate“. Im TUC_PKI_018 "Zertifikatsprüfung in der TI", Schritt 5 wird geprüft, ob unerlaubt Zertifikate ausgegeben wurden, deren Ausstellungsdatum nach dem Widerrufsdatum des CA-Zertifikats liegt.
- „/expired“: Das CA-Zertifikat ist abgelaufen, es wird aber für die Validierung von Zertifikaten weiterhin benötigt. Der ServiceStatus wird zur Prüfung von nonQES-Signaturen nach Kompromissmodell benötigt .

Hinweis: Gemäß Schalenmodell gesperrte CA-Zertifikate werden aus der TSL entfernt, es wird deshalb kein URI zur Markierung dieser Zertifikate verwendet.

OCSP-Signer-, CRL-Signer- und CVC-CA-Zertifikate sowie der DNSSEC-Trust-Anchor sind nur in der aktuellen TSL-Datei enthalten, wenn sie auch gegenwärtig im Einsatz sind. Für diese Dienstanbieter ist deshalb „/inaccord“ der einzige erlaubte Status.

Tabelle 74: Tab_PKI_271 Erlaubte URIs als Inhalte des TSL-Elements ServiceStatus

URI	Dienst	Bedeutung
http://uri.etsi.org/TrstSvc/Svcstatus/inaccord	X.509-CA OCSP-Signer CRL-Signer CVC-Root-CA DNSSEC-Trust-	Der Dienst ist für die TI zugelassen und ist in Betrieb.

	Anchor BNetzA-VL- Signer Unspecified ServiceType	
http://uri.etsi.org/TrstSvc/Svcstatus/revoked	X.509-CA	Die Zulassung des Dienstes wurde wegen eines nicht-sicherheitskritischen Incidents widerrufen und die CA stellt keine End-Entity-Zertifikate mehr aus. Bis zum Widerrufsdatum (im Element StatusStartingTime) ausgegebene End-Entity-Zertifikate müssen aber normal (also als gültig, falls nicht widerrufen) behandelt werden.
http://uri.etsi.org/TrstSvc/Svcstatus/expired	X.509-CA	Der Dienst war für die TI zugelassen und war bis zum angegebenen Datum (im Element StatusStartingTime) in Betrieb und im TI-Vertrauensraum.

3177

3178 *Hinweis: Der TSL-Dienst darf nur die in Tab_PKI_271 angegebenen URIs für*
3179 *ServiceStatus verwenden.*

3180 **8.1.2.1 TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“**

3181 **GS-A_4642 - TUC_PKI_001: Periodische Aktualisierung TI-Vertrauensraum**

3182 Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_001 zur periodischen
3183 Aktualisierung des TI-Vertrauensraums umsetzen.

3184 [**<=**]

3185

3186 **Tabelle 75: TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“**

Element	Beschreibung
Name	TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“

Beschreibung	<p>Dieser Use Case beschreibt den gesamten Ablauf zur periodischen Aktualisierung des TI-Vertrauensraumes mittels einer TSL-Datei. Dabei verwendet er weitere TUCs, die im Laufe des Kapitels detailliert spezifiziert werden</p> <p>Ein Offline-Modus ist zu berücksichtigen für</p> <ul style="list-style-type: none"> a) das Mobile-Kartenterminal b) Konnektor ohne Anbindung an die TI <p>Beide verfügen nicht über die automatischen Online-Möglichkeiten zum Bezug von Statusinformationen oder TSL-Aktualisierungen aus der TI.</p>
Anwendungsumfeld	System, das die TSL auswertet
Vorbedingungen	Gültige TSL im System (optional mit Hashwert)
Auslöser	<p>Produktypspezifischer Trigger</p> <p>Zeitpunkt MUSS durch Facharchitekturen vorgegeben werden. (Standardmäßig ist eine tägliche Prüfung der Aktualität vorzusehen.)</p>
Eingangsdaten	<ul style="list-style-type: none"> • Neu eingebrachte TSL-Datei (optional) • OCSP-Graceperiod (legt bei der Verwendung von gecachten OCSP-Antworten den maximal zulässigen Zeitraum fest, den die Systemzeit der prüfenden Komponente noch nach dem Zeitpunkt der OCSP-Antwort liegen darf) • Flag für Offline-Modus (Im Offline-Fall kann keine Sperrstatusprüfung des TSL-Signer-Zertifikates durchgeführt werden.)
Komponenten	System, TSL-Download-Punkt, OCSP-Responder
Ausgangsdaten	Status der Initialisierung
Referenzen	[ETSI_TS_102_231]
Standardablauf	<ol style="list-style-type: none"> 1. [System:] System startet die Initialisierung des TI-Vertrauensraums. 2. [System:] Die TSL im System wird auf Aktualität geprüft (TUC_PKI_019 „Prüfung der Aktualität der TSL“). Diese Prüfung erfolgt gegen die neu eingebrachte TSL-Datei als Eingangsparameter oder optional bei Vorhandensein eines TSL-Hashwertes im System über einen Vergleich mit der TSL-Hashwert-Datei am Downloadpunkt. (Ansonsten wird die aktuelle TSL-Datei bei diesem Schritt heruntergeladen.) Die Prüfung ergibt, dass die im System abgelegten TSL-Informationen erneuert werden müssen. 3.

	<p>[System:] Das verwendete TSL-Signer-Zertifikat wird aus der TSL-Datei extrahiert.</p> <p>4.</p> <p>[System:] OCSP-Abfrage für das extrahierte TSL-Signer-Zertifikat durch das System (TUC_PKI_006 "OCSP-Abfrage"). Wenn der zuständige OCSP-Responder die Statusinformation des Zertifikats mit einem Wert „revoked“ oder „unknown“ gemäß GS-A_4690 zurückgibt oder die certHash-Erweiterung fehlt (CERTHASH_EXTENSION_MISSING) bzw. falsch ist (CERTHASH_MISMATCH), darf es nicht zu einer Aktualisierung des TI-Vertrauensraums kommen. (Sämtliche anderen Schritte einer Prüfung des Zertifikates und der XML-Signatur sind im TUC_PKI_019 „Prüfung der Aktualität der TSL“ referenziert, vgl. im Schritt 2.)</p> <p>5.</p> <p>[System:] Es wird ermittelt, ob in der neuen TSL ein neuer TI-Vertrauensanker vorliegt (TUC_PKI_013 „Import TI-Vertrauensanker aus TSL“).</p> <p>6.</p> <p>[System:] Aus den CA-Zertifikaten aus der neuen TSL wird der neue TI-Vertrauensraum gebildet. Dazu werden sie aus der TSL-Datei extrahiert, z. B. in einen System-eigenen Truststore gespeichert und dem System bereitgestellt. Bei der Extraktion der Zertifikate aus der TSL darf keine inhaltliche Überprüfung der Datenfelder oder eine Signaturprüfung des Zertifikats erfolgen. Falls ein solcher Truststore nur den Vertrauensraum der TI enthält, wird er vor der Neubefüllung geleert, so dass anschließend nur die Zertifikate aus der aktuellen TSL dem System zur Verfügung stehen. Falls der Truststore auch für die sichere Speicherung von Zertifikaten benutzt wird, die nicht in der TSL stehen, muss keine komplette Leerung des Truststores erfolgen. Das System muss aber sicherstellen, dass im Truststore nur diejenigen Zertifikate der TI enthalten sind, die den aktuellen Vertrauensraum der TI aufspannen bzw. in der aktuellen TSL-Datei enthalten sind. Die Form des Truststore wird nicht näher spezifiziert, dieser muss nur den gestellten Anforderungen (z. B. bezüglich Sicherheit oder Performance) genügen. Das System muss den TI-Vertrauensraum mit den in der TSL als vertrauenswürdig bezeichneten und für den Produkttyp relevanten CA-Zertifikaten gemäß Tab_PKI_271 „Erlaubte Inhalte des TSL-Elements ServiceStatus“ befüllen.</p> <p>7.</p> <p>[System:] Der Truststore wird für Zertifikatsprüfung (wieder) bereitgestellt.</p> <p>8.</p> <p>[System:] Ende des Use Case</p>
--	--

Varianten/Alternativen	<p>Der Standardablauf stellt die Prüfungen dar, die vollzogen werden müssen. Eine Trennung in zwei Prozesse oder eine Umstrukturierung, bei der alle notwendigen Prüfungen erfolgen, ist zulässig.</p> <p>Im Falle einer aktuellen TSL im System endet der Ablauf nach Schritt 2:</p> <p>2a. [System:] TSL aus Download ist gleich TSL im System; und TSL ist noch gültig.</p> <p>2a.1 [System:] Ende des Use Case</p> <p>3a. [System:] Wenn das Offline-Flag gesetzt ist (offline==true), dann wird mit Schritt 5 fortgesetzt. (Im Offline-Fall kann keine OCSP-Abfrage stattfinden.)</p>
Fehlerfälle/Warnung	<p>2b. [System:] Der TUC_PKI_019 wirft eine VALIDITY_WARNING_2. VALIDITY_WARNING_2 wird als Fehlermeldung ausgegeben. Die weitere Fehlerbehandlung erfolgt unter Beachtung von [GS-A_5336].</p> <p>3b. [System:] Das TSL-Signer-Zertifikat lässt sich nicht aus der TSL-Datei extrahieren (TSL_CERT_EXTRACTION_ERROR). Weitere Fehlerfälle sind in den jeweiligen referenzierten TUCs beschrieben.</p>
Sicherheitsanforderungen	<p>Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.</p>
Anmerkungen	<p>Die Angaben zur Prüfung einer neuen TSL-Datei müssen als vertrauenswürdige Informationen im System schon vorhanden sein. Deshalb muss die OCSP-Adresse zur Prüfung des Signers der neuen TSL-Datei aus der TSL im System ausgelesen werden.</p> <p>Für die Prüfung der ersten TSL-Datei nach einem Vertrauensankerwechsel (entsprechend TUC_PKI_013 „Import TI-Vertrauensanker aus TSL“ und angekündigt mit ServiceTypeIdentifier „http://uri.etsi.org/TrstSvc/Svctype/TSLServiceCertChange“) bedeutet dies, dass die OCSP-Adresse aus dem „TSLServiceCertChange“ Eintrag aus der TSL im System genommen werden muss.</p> <p>Bei der OCSP-Abfrage für das extrahierte TSL-Signer-Zertifikat gemäß TUC_PKI_006 "OCSP-Abfrage" ist es nicht zulässig, im Schritt „Ermittlung der OCSP-Adresse“ (TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln") bereits Daten aus der zu importierenden TSL zu verwenden.</p> <p>Hinweis zur Robustheit der TSL-Verarbeitung: Nach</p>

	erfolgreichen Schema- und Signatur-Prüfungen darf es bei der Verarbeitung der TSL-Elemente nicht mehr zum Abbruch des TUC kommen.
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_001 "Periodische Aktualisierung TI-Vertrauensraum". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

3187

ENTWURF

3188

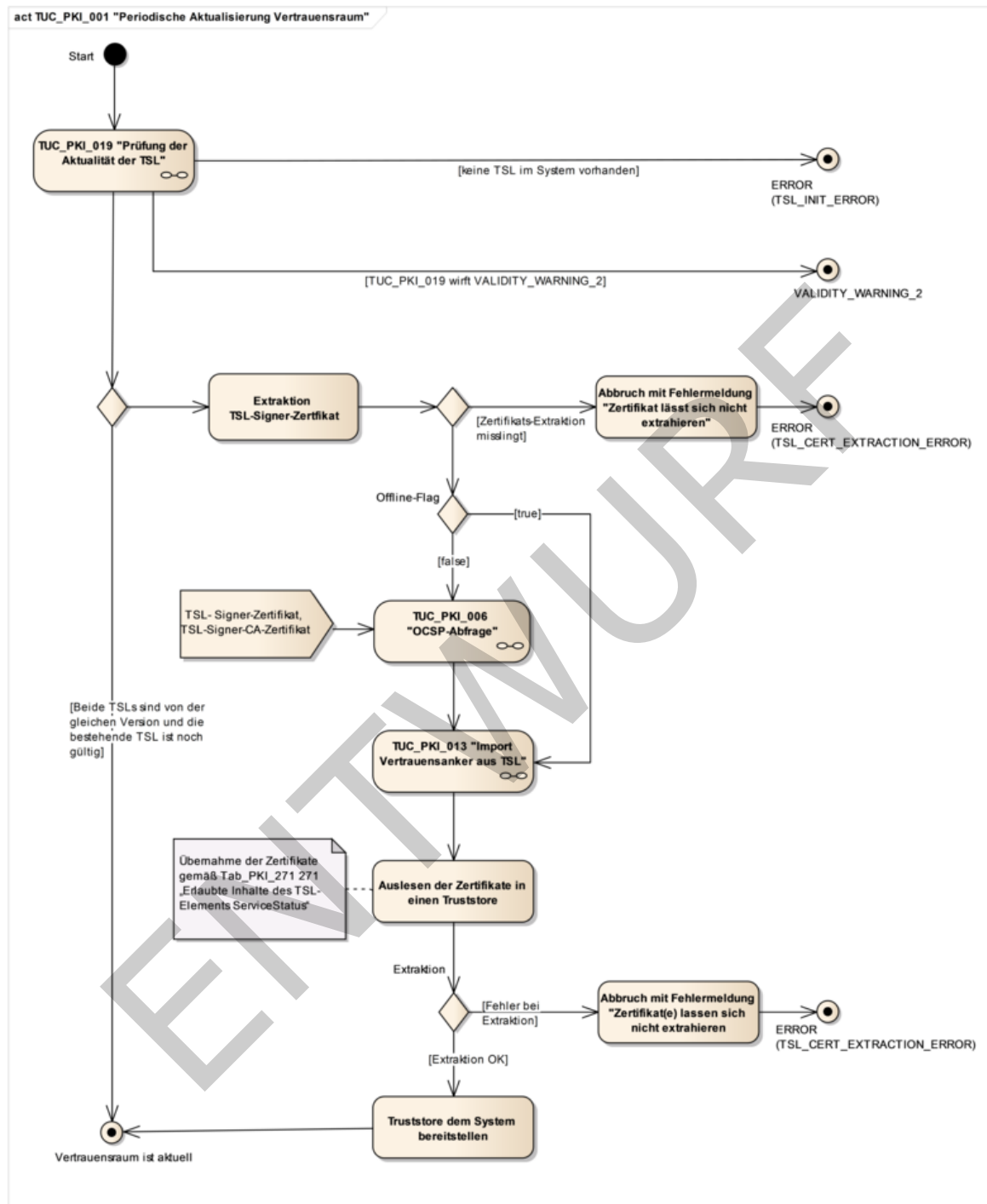


Abbildung 7: Aktivitätsdiagramm TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“

8.1.3 Geplanter Wechsel TI-Vertrauensanker

Im Folgenden werden der Prozess und die Vorgaben zum TI-Vertrauensankerwechsel beschrieben, die sich beim Wechsel innerhalb einer Schlüsselgeneration (RSA bzw. ECDSA) ergeben.

Wird ein Vertrauensankerwechsel im Rahmen der ECC-Migration vorgenommen, so gelten die Hinweise zur ECC-Migration in Kapitel 8.1.

8.1.3.1 TUC_PKI_013 „Import TI-Vertrauensanker aus TSL“

GS-A_4643 - TUC_PKI_013: Import TI-Vertrauensanker aus TSL

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_013 zum Import neuer TI-Vertrauensanker umsetzen.

[<=]

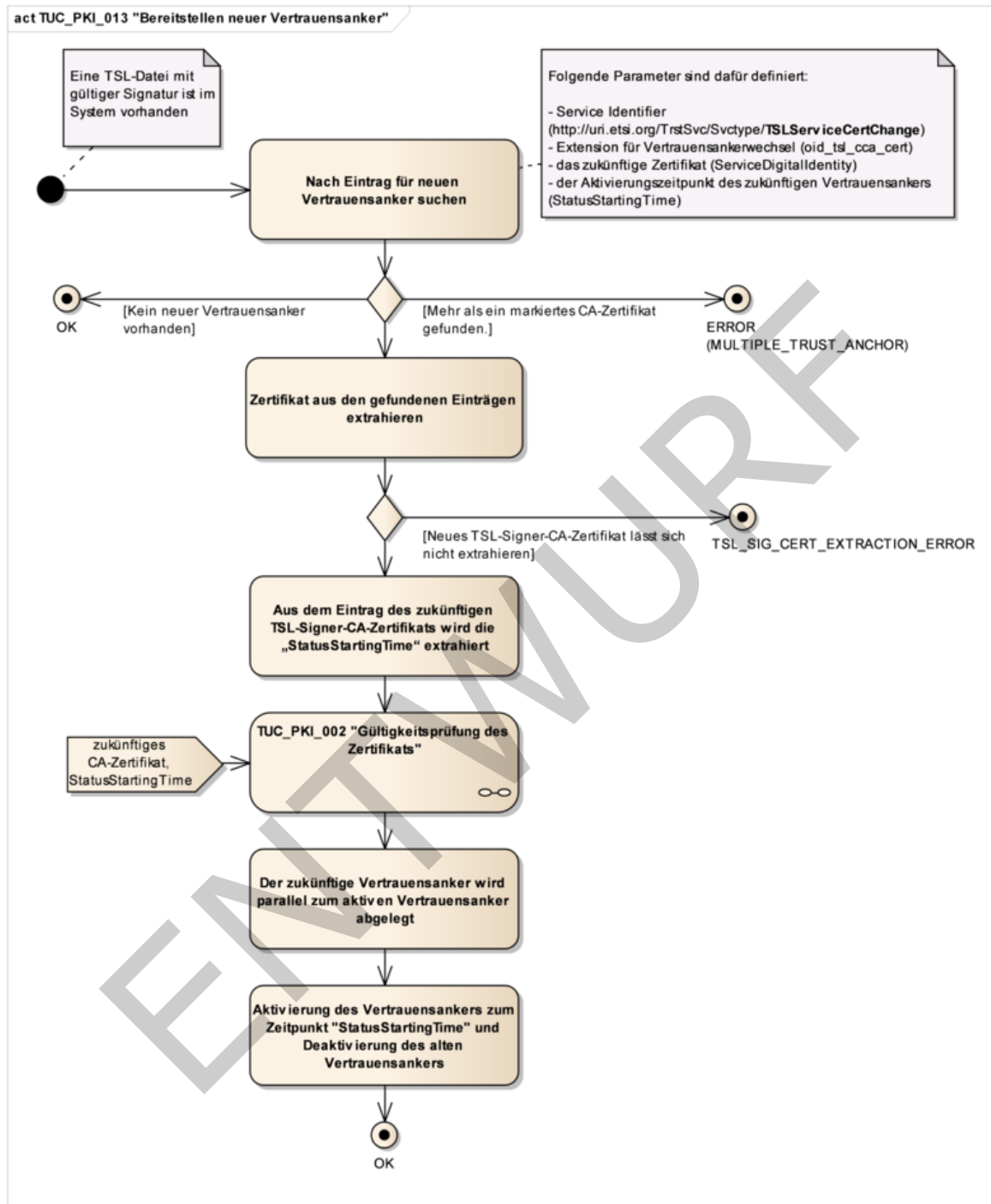
Tabelle 76: TUC_PKI_013 „Import neuer TI-Vertrauensanker“

Element	Beschreibung
Name	TUC_PKI_013 „Import neuer TI-Vertrauensanker“
Beschreibung	Als TI-Vertrauensanker gilt das aktuell gültige TSL-Signer-CA-Zertifikat. Das neue TSL-Signer-CA-Zertifikat wird rechtzeitig vor dem geplanten Aktivierungsdatum in die TSL integriert und als zukünftiger TI-Vertrauensanker markiert. Über diesen Weg wird es an Komponenten und Systeme ausgeliefert. Die Integrität des neuen Schlüssels wird somit durch den gültigen alten gesichert.
Anwendungsumfeld	System, das die TSL verwendet
Vorbedingungen	TSL mit gültiger Signatur
Auslöser	TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“
Eingangsdaten	Neue TSL-Datei (TSL aus dem Download oder manuellen Import)
Komponenten	System
Ausgangsdaten	Status des Prozesses, im Erfolgsfall eine Erweiterung des sicheren Speichers des Systems um den neuen TI-Vertrauensanker und dessen Aktivierungsdatum.

Referenzen	[ETSI_TS_102_231]
Standardablauf	<p>1. [System:] Das System sucht in der TSL nach den Einträgen für den neuen TI-Vertrauensanker. Die Identifikation erfolgt über den in GS-A_4644 bezeichneten ServiceTypeIdentifier-URI. Zusätzlich kann auch der in GS-A_4644 angegebene OID in der ServiceInformationExtension auf korrekte Belegung geprüft werden. Siehe Kapitel 8.1.3.2. Es wird immer das CA-Zertifikat bereitgestellt. Alle anderen Zustände (z. B. wenn nur der unsertifizierte Schlüssel bereitgestellt wird) müssen als Fehler behandelt werden. Parameter: heruntergeladene TSL</p> <p>2. [System:] Aus dem gefundenen Eintrag wird das Zertifikat extrahiert. Ergebnis: zukünftiges TSL-Signer-CA-Zertifikat</p> <p>3. [System:] Aus dem Eintrag des zukünftigen TSL-Signer-CA-Zertifikats wird die „StatusStartingTime“ extrahiert. Ergebnis: StatusStartingTime</p> <p>4. [System:] Für das zukünftige TSL-Signer-CA-Zertifikat wird TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats" durchlaufen. Parameter: zukünftiges TSL-CA-Zertifikat, StatusStartingTime.</p> <p>5. [System:] Der zukünftige TI-Vertrauensanker wird parallel zum aktiven TI-Vertrauensanker abgelegt. Parameter: zukünftiges TSL-Signer-CA-Zertifikat</p> <p>6. [System:] Der zukünftige TI-Vertrauensanker darf nicht vor dem Zeitpunkt „StatusStartingTime“ aktiviert werden. Der zukünftige TI-Vertrauensanker muss spätestens dann aktiviert werden, wenn nach Erreichen der „StatusStartingTime“ ein Update der TSL durchgeführt wird. Bei Aktivierung des zukünftigen TI-Vertrauensankers wird der alte TI-</p>

	Vertrauensanker deaktiviert. Parameter: StatusStartingTime
Varianten/Alternativen	1a. [System:] Es wird kein als neuer TI-Vertrauensanker markiertes CA-Zertifikat gefunden und der Use Case wird beendet.
Fehlerfälle	Ein Abbruch des TUC führt nur dazu, dass kein neuer TI-Vertrauensanker abgelegt wird. Er hat keinen Einfluss auf die Gültigkeit des bestehenden TI-Vertrauensankers oder auf die anderen Schritte der TSL-Aktualisierung. Das System muss dies jedoch protokollieren. 1b. [System:] Es wird mehr als ein markiertes CA-Zertifikat gefunden. (MULTIPLE_TRUST_ANCHOR) 2b. [System:] Das TSL-Signer-CA-Zertifikat lässt sich nicht aus der TSL extrahieren. (TSL_SIG_CERT_EXTRACTION_ERROR)
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	Der Prozess wird unabhängig davon durchlaufen, ob schon ein zukünftiger TI-Vertrauensanker vorliegt oder nicht. Es ist immer nur der zuletzt angekündigte zukünftige TI-Vertrauensanker gültig. Ältere Ankündigungen müssen überschrieben werden. Die Gestaltung des sicheren Speichers des Systems ist durch den Betreiber/Implementierer des Systems zu definieren.
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_013 "Import neuer TI-Vertrauensanker". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

3207



3208

3209

Abbildung 8: Aktivitätsdiagramm TUC_PKI_013 „Import neuer TI-Vertrauensanker“

3210

8.1.3.2 TSL-Einträge für die Bereitstellung neuer TI-Vertrauensanker

3211

Für den Wechsel auf ein neues TSL-Signer-CA-Zertifikat wird dieses in der TSL

3212

aufgenommen unter Berücksichtigung folgender Rahmenbedingungen:

3213

Die Aufnahme des Zertifikates erfolgt rechtzeitig, also erstmals zu einem Datum, welches

3214

eine definierte Zeitspanne vor dem geplanten Aktivierungsdatum liegt. Diese Aufnahme

erfolgt in Abstimmung mit der gematik und unter Einhaltung der üblichen Prozesse der Eintragsverwaltung für Zertifikate in der TSL (s. auch [gemSpec_TSL#6.1.2]). Ab diesem Datum wird das Zertifikat auch in den folgenden TSL-Dateien bis zum Erreichen des Aktivierungszeitpunkts als nächster TI-Vertrauensanker geführt.

Dies wird so gehandhabt, um temporär offline befindliche Komponenten eine als zumutbar angenommene Zeitspanne zur Migration zu gewähren.

Die Integrität des neuen Schlüssels wird durch den alten gesichert. Dazu erzeugt der gematik TSL-Dienst einen TSP-Dienst-Eintrag in der TSL-Datei mit folgenden Eigenschaften (Update-Parameter):

- Service Type Identifier (<http://uri.etsi.org/TrstSvc/Svctype/TSLServiceCertChange>) signalisiert den Verwendungszweck des Eintrags,
`<xsd:element name="ServiceTypeIdentifier" type="tsl:NonEmptyURIType"/>`
- das neue TSL-Signer-CA-Zertifikat (ServiceDigitalIdentity),
`<xsd:element name="X509Certificate" type="xsd:base64Binary"/>`
- der Aktivierungszeitpunkt des neuen TSL-Signer-CA-Zertifikats (StatusStartingTime)
`<xsd:element name="StatusStartingTime" type="xsd:dateTime"/>`
- die Extension für den TI-Vertrauensanker-Wechsel gemäß [gemSpec_OID#3.6] (in ServiceInformationExtension).
`<xsd:element name="ServiceInformationExtensions" type="tsl:ExtensionsListType" minOccurs="0"/>`

Ergänzend dazu gelten die allgemeinen Vorgaben für das Element TSPService wie in [gemSpec_TSL#7.3.2] beschrieben, siehe z. B. TIP1-A_4104 hinsichtlich Eintrag des X.509-Zertifikats oder TIP1-A_4106 bezüglich der Adresse der OCSP-Responder-Adresse.

Als TI-Vertrauensanker wird das TSL-Signer-CA-Zertifikat angesehen. Bei jedem Wechsel wird der vollständige TI-Vertrauensanker in der TSL veröffentlicht.

GS-A_4644 - TSL-Vertrauensankerwechsel

Der TSL-Dienst MUSS für einen TI-Vertrauensankerwechsel die folgenden Einträge aufnehmen:

- (a) Innerhalb Element ServiceTypeIdentifier:
URI <http://uri.etsi.org/TrstSvc/Svctype/TSLServiceCertChange>
 - (b) das Zertifikat des neuen TI-Vertrauensankers in ServiceDigitalIdentity
 - (c) Einen durch die gematik vorgegebenen Aktivierungszeitpunkt im Element StatusStartingTime
 - (d) Adresse des OCSP-Responders zur Prüfung von ausgestellten Zertifikaten (TSL-Signer) in ServiceSupplyPoint(s)
 - (e) die Extension für den TI-Vertrauensankerwechsel {oid_tsl_cca_cert} gemäß [gemSpec_OID#GS-A_4447] (in ServiceInformationExtension)
- [<=]**

Hinweis: Der TSL-Dienst führt das Zertifikat des nächsten TI-Vertrauensankers ab dem erstmaligen Eintrag zusammen mit den anderen Einträgen (a) – (e) in allen folgenden TSL-Dateien bis zu seiner Aktivierung.

Das vorliegende Dokument trifft keine Festlegungen zu den konkret einzutragenden OID-Werten, sondern verwendet stattdessen eine OID-Referenz, die in der Spalte "Inhalt" der Tabelle 82 genannt ist. Die normative Festlegung der OIDs trifft das Dokument [gemSpec_OID], dort ist die Zuordnung zur OID-Referenz ersichtlich.

3264 **Tabelle 77: Gültige Werte für den TI-Vertrauensankerwechsel**

Beschreibung	Ort	Bezeichnung	Format	Inhalt
Eintragsdaten für den Wechsel des TSL-Signer-CA-Zertifikats des TSL-Vertrauensankers	TSL	Change of TSL Signer-CA Certificate	OID	oid_tsl_cca_cert

3265 In der folgenden Tabelle wird ein (nicht-normatives) Beispiel zu den TSL-Einträgen
3266 dargestellt, die den Wechsel des TI-Vertrauensraumes bewirken.

3267

3268 **Tabelle 78: Beispiel für den TSL-Eintrag zum Wechsel des TSL-Signer-CA-Zertifikats**

```

<TSPService>
  <ServiceInformation>
    <ServiceTypeIdentifier>
      http://uri.etsi.org/TrstSvc/Svctype/TSLServiceCertChange
    </ServiceTypeIdentifier>
    <ServiceName>
      <Name xml:lang="DE">{Name des neuen TSL-Vertrauensankers}</Name>
    </ServiceName>
    <ServiceDigitalIdentity>
      <DigitalId>
        <X509Certificate>{Base64-codiertes X.509-Zertifikat}</X509Certificate>
      </DigitalId>
    </ServiceDigitalIdentity>
    <ServiceStatus>http://uri.etsi.org/TrstSvc/Svcstatus/inaccord
  </ServiceStatus>
  <StatusStartingTime>2008-04-01T09:30:47Z</StatusStartingTime>
  <ServiceSupplyPoints>
    <ServiceSupplyPoint>http://pki0locsp02.gematik.net
  </ServiceSupplyPoint>
  </ServiceSupplyPoints>
  <ServiceInformationExtensions>
    <Extension Critical="false">
      <ExtensionOID>{oid_tsl_cca_cert}</ExtensionOID>
      <ExtensionValue>oid_tsl_cca_cert</ExtensionValue>
    </Extension>
  </ServiceInformationExtensions>
</ServiceInformation>
</TSPService>

```

3269 *Hinweis: Die Authentizität der TSL-Datei ist durch deren Signatur gegeben, die*
3270 *Authentizität des TSL-Download-Punktes wird durch DNSSEC gesichert. Der Download*
3271 *erfolgt deshalb über einfaches HTTP, nicht über HTTPS.*

3272 **8.1.3.3 Prüfung der TSL nach Wechsel des TI-Vertrauensanker**

3273 Ein neuer TI-Vertrauensanker wird mit einem TSL-Eintrag (s. o.) angekündigt.

3274 Sobald der Zeitpunkt für die Aktivierung des neuen TI-Vertrauensankers erreicht ist, wird
3275 der neue TI-Vertrauensanker aktiviert. Zur Ermittlung des Zeitpunktes soll die in der TI
3276 verbindlich geltende Zeitquelle verwendet werden.

3277

3278 **GS-A_4645 - TSL-Signatur ab Aktivierungsdatum neuer TI-Vertrauensanker**

3279 Der TSL-Dienst MUSS ab dem Aktivierungsdatum eines über die TSL publizierten TI-
3280 Vertrauensankers (TSL-Signer-CA-Zertifikat) die TSL mit einem TSL-Signer-Zertifikat

3281 signieren, das von dieser TSL-Signer-CA ausgestellt wurde.
3282 [\leq]

3283 8.1.4 Ungeplanter Wechsel des TI-Vertrauensanker

3284 Ein ungeplanter Wechsel des TI-Vertrauensankers kann dann erforderlich werden, wenn
3285 die TSL-Signer-CA korrumpiert wurde. (Nur in Verbindung mit dem missbräuchlichen
3286 Zugang zu den TSL-Download-Punkten kann hieraus ein konkreter Schaden durch
3287 gefälschte TSL-Einträge, die von den auswertenden Komponenten und Systemen nicht
3288 mehr als solche erkennbar sind, für die TI resultieren.)

3289 8.2 TSL-Prüfung

3290 8.2.1 Erreichbarkeit und Download der TSL

3291 Der TSL-Dienst stellt die jeweils aktuelle TSL an definierten Download-Punkten in der TI
3292 und im Internet bereit. Diese Download-Punkte sind so gewählt, dass sie von allen
3293 Diensten, Systemen und Komponenten in der TI netzwerktechnisch erreicht werden
3294 können.

3295 Die Adressen der TSL-Download-Punkte sind in Form von URI definiert und Bestandteil
3296 jeder TSL.

3297 Die TSL verweist auf die Download-Punkte, wo die jeweils aktuellste Version der TSL
3298 heruntergeladen werden kann (siehe Kap. 8.2.1.1).

3299 Die Lokalisierung der Adresse ist in Abschnitt 8.2.1.1 detailliert beschrieben.

3300 8.2.1.1 TUC_PKI_017 „Lokalisierung TSL Download-Adressen“

3301 GS-A_4646 - TUC_PKI_017: Lokalisierung TSL Download-Adressen

3302 Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_017 zur Lokalisierung
3303 der Download-Adressen der TSL umsetzen.

3304 [\leq]

3305

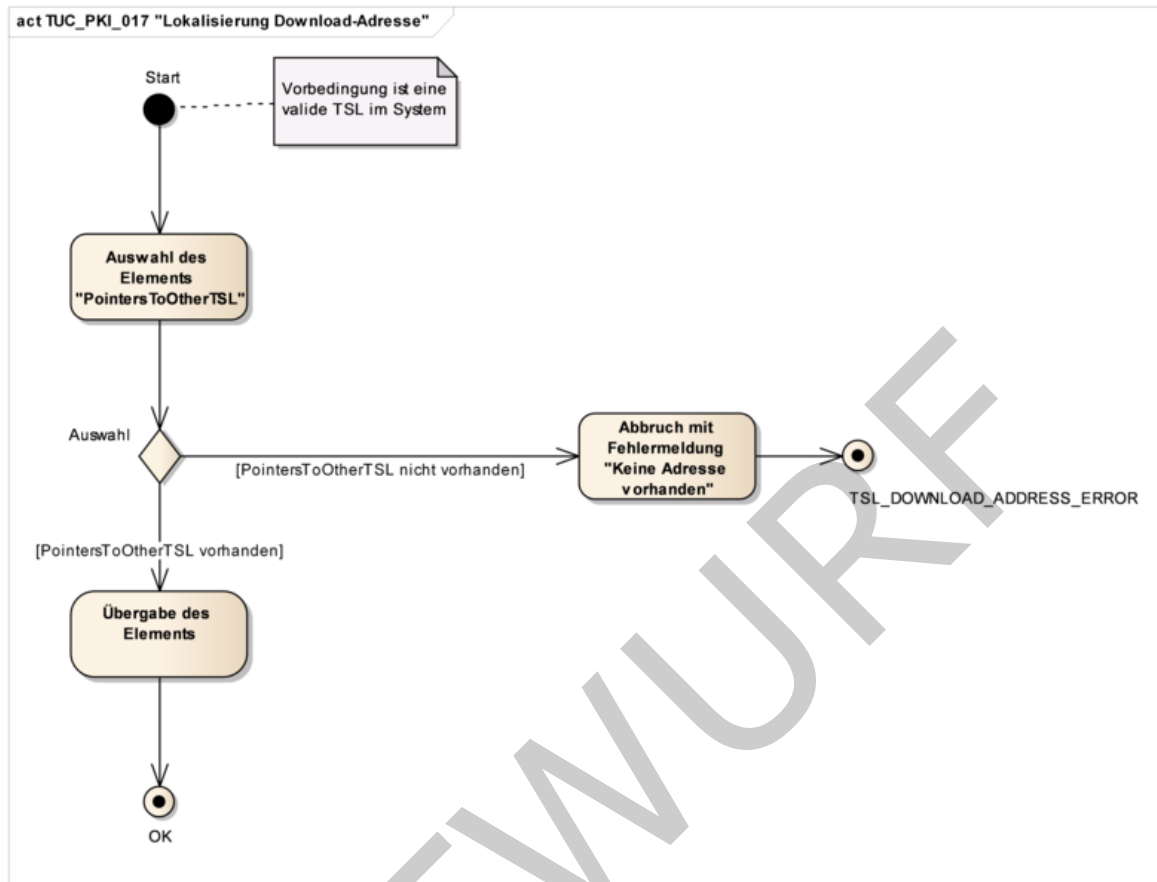
3306 Tabelle 79: TUC_PKI_017 „Lokalisierung Download-Adressen“

Element	Beschreibung
Name	TUC_PKI_017 „Lokalisierung Download-Adressen“
Beschreibung	Die TSL enthält im Element „PointersToOtherTSL“ die Zugriffsadresse für die jeweilige Liste. Zusätzlich ist ein Eintrag für eine Backup-Zugriffsadresse vorhanden. Dieser Use Case beschreibt, wie diese Adressen lokalisiert werden.
Anwendungsumfeld	System, das die TSL verwendet

Vorbedingungen	TSL mit gültiger Signatur
Auslöser	TUC_PKI_016 „Download der TSL“
Eingangsdaten	TSL
Komponenten	System
Ausgangsdaten	PointersToOtherTSL[Primär-Zugriffsadresse, Backup-Zugriffsadresse]
Referenzen	[ETSI_TS_102_231] Annex H und B.2.13
Standardablauf	<ol style="list-style-type: none"> 1. [System:] System startet die Lokalisierung der Adressen 2. [System:] Das Element „PointersToOtherTSL“ wird ausgewählt. 3. [System:] Übergabe des Elements 4. [System:] Ende des Use Cases mit Rückgabe des Adressen-Elements
Fehlerfälle	<ol style="list-style-type: none"> 2a. [System:] Das Element ist nicht vorhanden und der Vorgang wird mit Fehlermeldung abgebrochen. (TSL_DOWNLOAD_ADDRESS_ERROR)
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	Die Kennzeichnung der Adressen in der TSL als primär oder als Backup erfolgt gemäß Tab_PKI_272
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_017 "Lokalisierung Download-Adresse". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

3307

3308



3309

3310 **Abbildung 9: Aktivitätsdiagramm TUC_PKI_017 „Lokalisierung Download-Adresse“**

3311

3312 **Tabelle 80: Tab_PKI_272 Gültige Werte zur Download-Adresse**

Beschreibung	Ort	Bezeichnung	Format	Inhalt
Bezeichner der Eintragsdaten für die Primär-Adresse der TSL	TSL	Primär-Adresse	OID	oid_tsl_p_loc
Bezeichner der Eintragsdaten für die Backup-Adresse der TSL	TSL	Backup-Adresse	OID	oid_tsl_b_loc

3313

Die normative Festlegung der OIDs ist in [gemSpec_OID#3.6] festgelegt.

3314

Die TSL-Dateien und deren Hash-Werte werden vom Anbieter des TSL-Dienstes in der TI und im Internet zum Download bereitgestellt. Die festgelegten Downloadpunkte sind in [gemSpec_TSL#A_17680] zu finden.

3317

3318 **8.2.1.2 TUC_PKI_016 „Download der TSL-Datei“**

3319 **GS-A_4647 - TUC_PKI_016: Download der TSL-Datei**

3320 Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_016 zum Download der TSL-Datei umsetzen.

3322 [**<=**]

3323

3324 **Tabelle 81: TUC_PKI_016 „Download der TSL-Datei“**

Element	Beschreibung
Name	TUC_PKI_016 „Download der TSL-Datei“
Beschreibung	Es wird der Download-Prozess der TSL-Datei und das Verhalten des Systems bei Fehlerfällen, wie nicht erfolgreicher Download bzw. Netzwerkproblemen beschrieben.
Anwendungsumfeld	System, das die TSL verwendet
Vorbedingungen	Lokalisierung der Download-Adresse
Auslöser	TUC_PKI_019 „Prüfung der Aktualität der TSL“
Eingangsdaten	TSL
Komponenten	System, TSL-Download-Punkt
Ausgangsdaten	Status des Prozesses
Referenzen	[ETSI_TS_102_231]
Standardablauf	<ol style="list-style-type: none"> 1. [System:] Das System startet den Prozess zum Download der TSL-Datei. 2. [System:] Lokalisierung der Download-Adresse (TUC_PKI_017 „Lokalisierung TSL Download-Adressen“) 3. [System:] Auswahl der Primär-Adresse gemäß Tab_PKI_272 aus dem Element „PointersToOtherTSL“ und Download der TSL-Datei. Ist der TSL-Download anhand der Primär-Adresse nicht erfolgreich, wird die Backup-Adresse für den Download verwendet. 4. [System:] Ende des Use Case mit entsprechender Rückmeldung.

Varianten/Alternativen	3a. [System:] Bei Fehlern wird ein einfaches Fehlerhandling angestoßen: Der TSL-Download anhand der Primär-Adresse wird dreimal wiederholt. Bei Wiederholung des TSL-Downloads anhand der Backup-Adresse ist analog zu verfahren.
Fehlerfälle	4a. [System:] Sollte der wiederholte Download über keine der Download-Adressen erfolgreich sein, meldet das System einen Fehler und es werden für den Moment keine weiteren Download-Versuche mehr unternommen. (TSL_DOWNLOAD_ERROR)
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_016 "Download der TSL-Datei". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

3325
3326

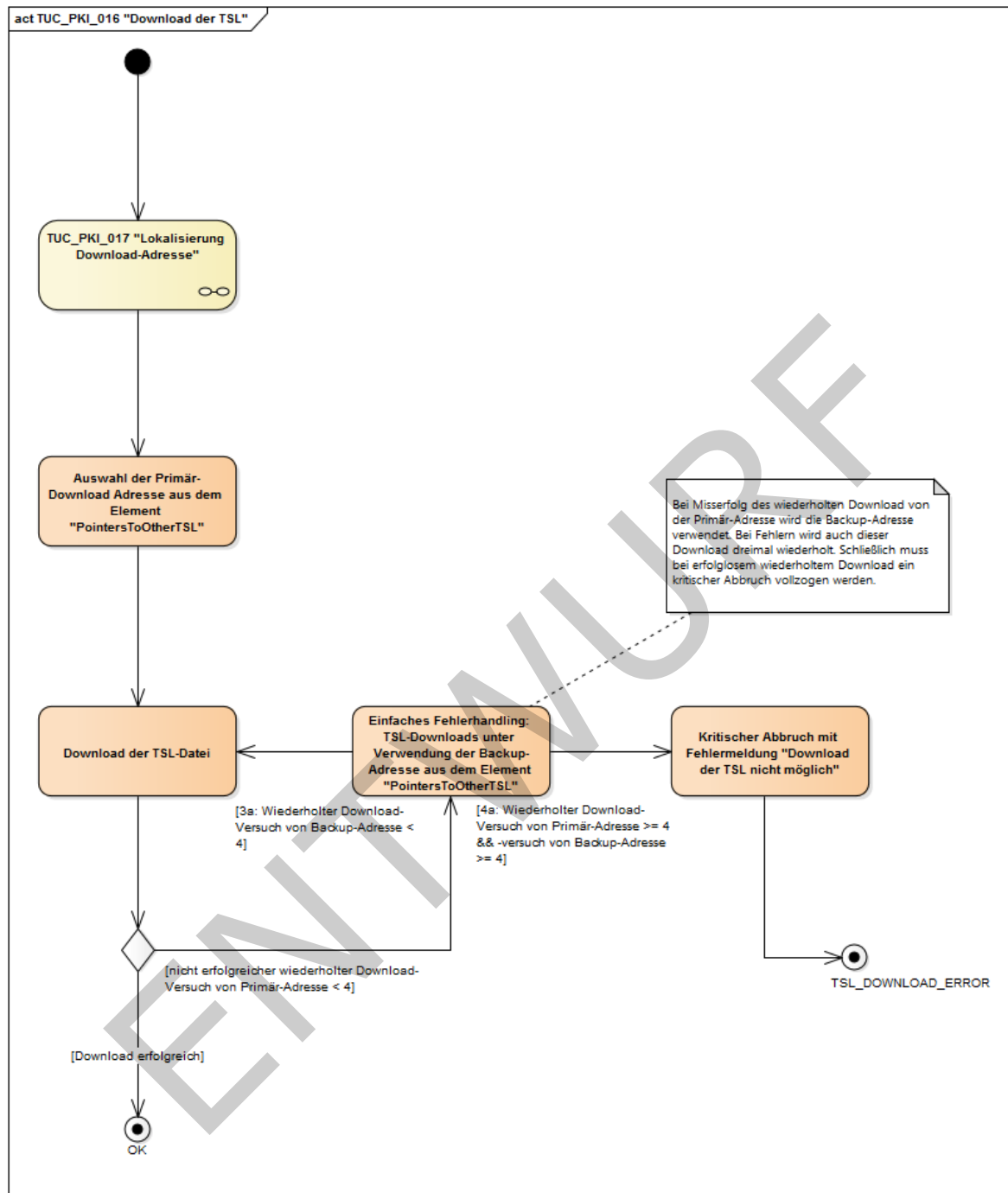


Abbildung 10: Aktivitätsdiagramm TUC_PKI_016 „Download der TSL-Datei“

8.2.2 Vertrauensstatus und Authentifizieren der TSL

8.2.2.1 TUC_PKI_019 „Prüfung der Aktualität der TSL“

Eine TSL-prüfende Komponente oder Anwendung kann den übergreifend festgelegten maximalen Wert der TSL-Graceperiod (30 Tage) mit dem Eingangsparameter TSL-Grace-Period überschreiben. Je nach Kritikalität der prüfenden Anwendung kann die TSL-Grace-Period damit zwischen 0 .. 30 Tagen gewählt werden.

Wird der TUC mit dem Wert „0“ aufgerufen, kann die Bedingung für Validity-Warning-1 nicht erfüllt werden, so dass die TSL mit Überschreitung des „nextUpdate“ auf jeden Fall als „ungültig“ mit der Rückmeldung „VALIDITY_WARNING_2“ reklamiert wird. Damit gilt:

1. OK: nextUpdate > aktuelles Datum
2. VALIDITY_WARNING_1: nextUpdate < aktuelles Datum < (nextUpdate + TSL-Grace-Period)
3. VALIDITY_WARNING_2: nextUpdate < aktuelles Datum > (nextUpdate + TSL-Grace-Period)

Wird VALIDITY_WARNING_2 geworfen, ist der gültige Vertrauensraum der TI nicht verfügbar, d. h. die TSL-Informationen im System sind nicht mehr vertrauenswürdig.

Der Vertrauensraum muss deaktiviert werden und bis zu dessen Re-Etablierung (Import einer gültigen TSL-Datei) darf keine Zertifikatsprüfung „gültig“ ergeben.

Dies kann z. B. durch Leeren des Truststores (Löschen der Zertifikate) erfolgen.

GS-A_5336 - Zertifikatsprüfung nach Ablauf TSL-Graceperiod

Die Produkttypen der TI-Plattform, die Zertifikate prüfen, MÜSSEN nach zeitlichem Ablauf der TSL-Graceperiod oder spätestens ab dem Zeitpunkt der darauf folgenden Prüfung der Aktualität der TSL (TUC_PKI_019) die TSL selbst als nicht mehr gültig bewerten (das TSL-Update-Prüfintervall wird in Tab_PKI_294 festgelegt).

Es steht somit keine valide Basis zur Prüfung von Zertifikaten zur Verfügung.

Die Produkttypen der TI-Plattform, die Zertifikate prüfen, MÜSSEN sicherstellen, dass nach zeitlichem Ablauf der TSL-Graceperiod die Zertifikatsprüfung in der TI (TUC_PKI_018) nicht als positiv bewertet wird. Dies gilt unabhängig vom letzten bekannten Status des (ausstellenden) CA-Zertifikats.

[<=]

Um den regelmäßigen Download der TSL effizient zu gestalten, wird neben der eigentlichen Bereitstellung der TSL-Datei auch jeweils ein SHA256-Hash der TSL-Datei bereitgestellt. Damit kann von TSL-auswertenden Komponenten auf den täglichen Download der TSL verzichtet werden, wenn anhand des zuvor geprüften Hashes festgestellt wird, dass die am Download-Punkt verfügbare TSL identisch mit der zuvor schon eingelesenen und verwendeten TSL ist.

A_17690 - Nutzung der Hash-Datei für TSL (ECC-Migration)

Die Produkttypen der TI, die Zertifikate validieren, und dafür die TSL verwenden, KÖNNEN vorab die Hash-Datei der TSL herunterladen, um zu prüfen, ob die am TSL-Downloadpunkt verfügbare TSL eine andere ist, als die schon zuvor heruntergeladene und bereits ausgewertete TSL. Entspricht der Hash-Wert am Download-Punkt (vgl. [gemSpec_TSL]#6.3.1.2) der bereits heruntergeladenen und ausgewerteten TSL, KANN auf den Download verzichtet werden.

[<=]

GS-A_4648 - TUC_PKI_019: Prüfung der Aktualität der TSL

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_019 zur Prüfung der Aktualität der TSL umsetzen.

[<=]

3381 Tabelle 82: TUC_PKI_019 „Prüfung der Aktualität der TSL“

Element	Beschreibung
Name	TUC_PKI_019 „Prüfung der Aktualität der TSL“
Beschreibung	Das System überprüft (standardmäßig täglich) die Aktualität der TSL. Dies geschieht bei Vorhandensein eines TSL-Hashwertes zunächst anhand eines Vergleichs der TSL-Hashwerte im System und auf dem TSL-Downloadpunkt. Nachfolgend erfolgt ein Vergleich der TSL aus dem System und der TSL aus dem Download: Die jeweilige ID und die jeweilige Sequenznummer der beiden TSL werden dabei verglichen.
Anwendungsumfeld	System, das die TSL auswertet
Vorbedingungen	Eine geprüfte TSL im System
Auslöser	TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“
Eingangsdaten	TSL im System, Hashwert-Datei der TSL im System (optional), neue (nicht über TSL-Download) eingebrachte TSL-Datei (optional), TSL-Grace-Period
Komponenten	System
Ausgangsdaten	Status der Prüfung
Referenzen	[ETSI_TS_102_231]

Standardablauf	<ol style="list-style-type: none">1. [System:] System lädt die aktuelle TSL-Datei herunter (TUC_PKI_016 "Download der TSL-Datei"). Im Folgenden wird diese als neue TSL-Datei bezeichnet.2. [System:] Neue TSL-Datei wird validiert (TUC_PKI_020 „XML-Dokument validieren“) Das entsprechende von der gematik benannte Schema muss verwendet werden.3. [System:] Das TSL-Signer-Zertifikat der neuen TSL-Datei wird geprüft. (TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“).4. [System:] Die Signatur der neuen TSL-Datei muss geprüft werden (TUC_PKI_012 „XML-Signatur-Prüfung“)5. [System:] Aus der TSL im System und der neuen TSL-Datei werden die jeweilige ID und das jeweilige TSLSequenceNumber-Element selektiert.6. [System:] System prüft die ID-Attribute und das TSLSequenceNumber-Element aus Schritt 5 auf Gleichheit. Sind sie identisch, muss keine Aktualisierung erfolgen.7. [System:] Prüfung, ob die TSL im System noch aktuell ist. Dies geschieht anhand des aktuellen Datums und des Elements „NextUpdate“ aus der TSL. Eine TSL wird als aktuell bezeichnet, wenn ihr NextUpdate in der Zukunft liegt.8. [System:] TSL im System ist gültig. Ende des Use Case mit entsprechender Rückmeldung
----------------	---

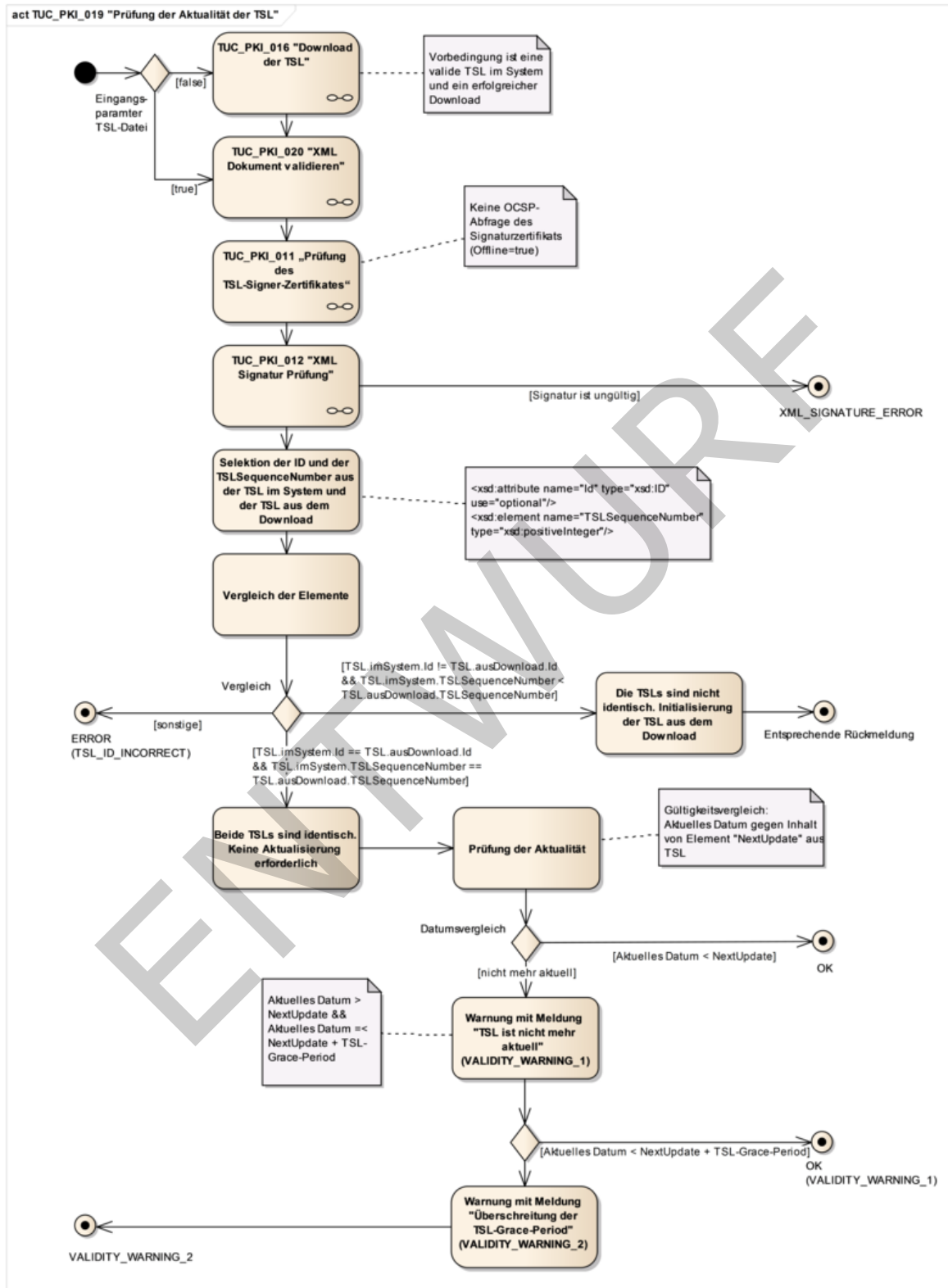
Varianten/Alternativen	<p>1a. [System:] Wenn eine TSL-Datei als Eingangsparameter eingebracht wurde, dann wird diese TSL-Datei verwendet, und es erfolgt kein Download. Im Folgenden wird diese neu eingebrachte TSL als neue TSL-Datei bezeichnet.</p> <p>1b. [System:] Wenn ein TSL-Hashwert als Eingangsparameter im System vorhanden ist, wird die aktuelle Hashwert-Datei der TSL vom TSL Downloadpunkt heruntergeladen. Dazu wird der TSL-Downloadpunkt ermittelt (TUC_PKI_017 „Lokalisierung TSL Download-Adressen“) und von der ermittelten URI statt der Datei mit Endung „*.xml“ die Datei mit Endung „*.sha2“ heruntergeladen.</p> <p>1b1. [System:] Ist der heruntergeladene TSL-Hashwert mit dem Hashwert der aktuell im System gespeicherten TSL identisch, dann wird die im System vorhandene TSL-Datei weiter verwendet und es erfolgt kein TSL-Download. Es wird mit Schritt 7 fortgefahren.</p> <p>1b2. [System:] Falls die Hashwerte verschieden sind oder im System noch kein TSL-Hashwert vorhanden ist, muss eine neue TSL-Datei heruntergeladen werden. Es wird die neue TSL-Hashwert-Datei im System gespeichert und mit Schritt 1 fortgefahren. Variante 1a kann hier nicht wiederholt werden.</p> <p>6a. [System:] Die ID-Attribute aus Schritt 5 sind nicht gleich und das TSLSequenceNumber-Element der TSL im System ist kleiner als die der neuen TSL. Somit ist die TSL im System älter als die die neue TSL.</p> <p>6a1. [System:] Rückmeldung an den aufrufenden Use Case (TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“)</p>
------------------------	--

Fehlerfälle	<p>6b. [System:] Keine der beschriebenen Varianten des Vergleichs der ID und SequenceNumber tritt ein. Ende des Use Case mit Fehlermeldung (TSL_ID_INCORRECT)</p> <p>7a. [System:] Die Aktualitäts-Prüfung ergibt, dass die TSL im System abgelaufen ist (nextUpdate < aktuelles Datum). Das aktuelle Datum liegt aber innerhalb der TSL-Grace-Period (aktuelles Datum < nextUpdate + TSL-Grace-Period). Warnung (VALIDITY_WARNING_1) mit der entsprechenden Meldung. (Die TSL ist nicht mehr aktuell.) Rückmeldung des Warnhinweises.</p> <p>7a1. [System:] Die Aktualitäts-Prüfung ergibt, dass die TSL-Grace-Period überschritten ist (aktuelles Datum > nextUpdate + TSL-Grace-Period). Warnung (VALIDITY_WARNING_2) mit der entsprechenden Meldung, (Ablauf der TSL-Grace-Period, die TSL im System ist nicht mehr vertrauenswürdig und darf nicht als valide Prüfbasis verwendet werden, s. [GS-A_5336]). Rückmeldung des Warnhinweises. Weitere Fehlerfälle sind in den referenzierten Use Cases beschrieben.</p>
Sicherheitsanforderungen	<p>Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.</p>
Anmerkungen	<p>Die ID der TSL-Datei befindet sich als Attribut im Root-Tag des XML-Dokuments. <code><xsd:attribute name="Id" type="xsd:ID" use="optional"/></code> Das Attribut Id wird vom TSL-Service-Provider immer gefüllt. Das Element TSLSequenceNumber beschreibt die Folgenummer der TSL. Sein erstmaliger Inhalt der TSL(RSA) ist gleich 1 und wird jeweils um 1 hoch gezählt. Der erstmalige Wert der TSL(ECC-RSA) ist 10000.</p>

Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_019 "Prüfung der Aktualität der TSL". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.
----------------------	---

ENTWURF

3382



3383

3384

Abbildung 11: Aktivitätsdiagramm TUC_PKI_019 „Prüfung der Aktualität der TSL“

8.2.2.2 TUC_PKI_020 „XML-Dokument validieren“

GS-A_4649 - TUC_PKI_020: XML-Dokument validieren

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_020 zur Validierung eines XML-Dokumentes umsetzen.

[<=]

Tabelle 83: TUC_PKI_020 „XML-Dokument validieren“

Element	Beschreibung
Name	TUC_PKI_020 „XML-Dokument validieren“
Beschreibung	Ein XML-Dokument wird gegen ein XML-Schema validiert.
Anwendungsumfeld	Dieser Use Case wird verwendet, um XML-Dokumente zu validieren. In diesem Dokument betrifft das die Validierung der TSL.
Vorbedingungen	Eine vollständig vorliegende TSL-Datei im XML-Format
Auslöser	TUC_PKI_019 „Prüfung der Aktualität der TSL“
Eingangsdaten	TSL-Datei und TSL-XML-Schema (und alle in ihm referenzierten Schemata). Das System muss sicherstellen, dass zur Validierung nur das von der gematik spezifizierte bzw. benannte Schema benutzt wird.
Komponenten	System
Ausgangsdaten	Entsprechendes Ergebnis der Validierung (Erfolg Misserfolg)
Referenzen	[XML]
Standardablauf	<p>Das System prüft die Wohlgeformtheit des Dokumentes und validiert es gegen das Schema.</p> <ol style="list-style-type: none"> 1. [System:] System startet Prüfung der TSL-Datei. 2. [System:] System prüft Wohlgeformtheit der TSL-Datei. 3. [System:] System validiert die TSL-Datei gegen die Schemata. 4.

	[System:] Ende des Use Case mit positivem Ergebnis
Fehlerfälle	Die übergebenen Schemata könnten selbst invalide oder unvollständig sein. 2a. [System:] Ende des Use Case mit Fehlermeldung (TSL_NOT_WELLFORMED) 3a. [System:] Ende des Use Case mit Fehlermeldung (TSL_SCHEMA_NOT_VALID)

8.2.2.3 TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“

GS-A_4650 - TUC_PKI_011: Prüfung des TSL-Signer-Zertifikates

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_011 zur Prüfung des TSL-Signer-Zertifikats umsetzen.

[<=]

Tabelle 84: TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“

Element	Beschreibung
Name	TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“
Beschreibung	Es wird der Prozess zur Prüfung des TSL-Signer-Zertifikates gegen ein sicher verwahrtes TSL-Signer-CA-Zertifikat spezifiziert. Der Prozess verläuft analog demjenigen für Zertifikatsprüfung im Allgemeinen (TUC_PKI_018 "Zertifikatsprüfung in der TI"), berücksichtigt aber die Besonderheiten des TSL-Signer-Zertifikates. Außerdem erfolgt hier keine Statusprüfung des TSL-Signer-Zertifikates. (Der Aufruf von TUC_PKI_006 „OCSP-Abfrage“ erfolgt in TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“.)
Anwendungsumfeld	System, das die TSL verwendet
Vorbedingungen	TSL-Signer-CA-Zertifikat in einem sicheren Speicher des Systems
Auslöser	TUC_PKI_019 „Prüfung der Aktualität der TSL“

Eingangsdaten	<ul style="list-style-type: none"> • TSL-Datei • Referenzzeitpunkt (Datum optional; bei Nichtangabe Verwendung der aktuellen Systemzeit)
Komponenten	System
Ausgangsdaten	Status der Prüfung
Referenzen	[ETSI_TS_102_231], [XMLSig]
Standardablauf	<ol style="list-style-type: none"> 1. [System:] Das verwendete TSL-Signer-Zertifikat wird aus der TSL-Datei extrahiert. 2. [System] Der Use Case TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats" wird durchlaufen. 3. [System:] Prüfung der Extension KeyUsage auf vorhanden sein. Zudem wird die KeyUsage auf die richtige Belegung (nonRepudiation) geprüft. Weiter wird die ExtendedKeyUsage auf die richtige Belegung mit {id-tsl-kp-tslSigning} geprüft (vgl. Kap. 5.13.1 TSL-Signer-Zertifikat). 4. [System:] Das TSL-Signer-CA-Zertifikat aus dem sicheren Speicher des Systems wird geladen. 5. [System:] Anhand dieses CA-Zertifikates wird die mathematische Prüfung der Signatur des TSL-Signer-Zertifikats durchgeführt (TUC_PKI_004 "Mathematische Prüfung der Zertifikatssignatur"). (Jedes System muss Initial dieses CA-Zertifikat als TI-Vertrauensanker auf sicherem Wege integrieren.) 6. [System:] Ende des Use Case mit Status Rückmeldung
Varianten/Alternativen	

Fehlerfälle	<p>1a. [System:] Das TSL-Signer-Zertifikat lässt sich nicht aus der TSL-Datei extrahieren (TSL_CERT_EXTRACTION_ERROR).</p> <p>3a. [System:] KeyUsage ist nicht vorhanden bzw. entspricht nicht der vorgesehenen KeyUsage (WRONG_KEYUSAGE).</p> <p>3a1. [System:] ExtendedKeyUsage entspricht nicht der vorgesehenen ExtendedKeyUsage (WRONG_EXTENDEDKEYUSAGE).</p> <p>4a. [System:] Das TSL-Signer-CA-Zertifikat kann nicht aus dem sicheren Speicher des Systems geladen werden (TSL_CA_NOT_LOADED).</p> <p>Fehlerfälle sind in den referenzierten Use Cases beschrieben.</p>
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	<p>Die Gestaltung des sicheren Speichers des Systems ist durch den Betreiber des Systems auszuarbeiten.</p> <p>TUC_PKI_018 "Zertifikatsprüfung in der TI" fordert zusätzlich die Ermittlung von Autorisierungsinformationen. Dies wird im vorliegenden Use Case nicht benötigt und kann entfallen.</p> <p>Der Aufruf von TUC_PKI_006 "OCSP-Abfrage erfolgt nicht hier, sondern in TUC_PKI_001 "Periodische Aktualisierung TI-Vertrauensraum".</p>
Zugehörige Diagramme	<p>Aktivitätsdiagramm TUC_PKI_011 "Prüfung des TSL-Signer-Zertifikates".</p> <p>Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.</p>

3399
3400

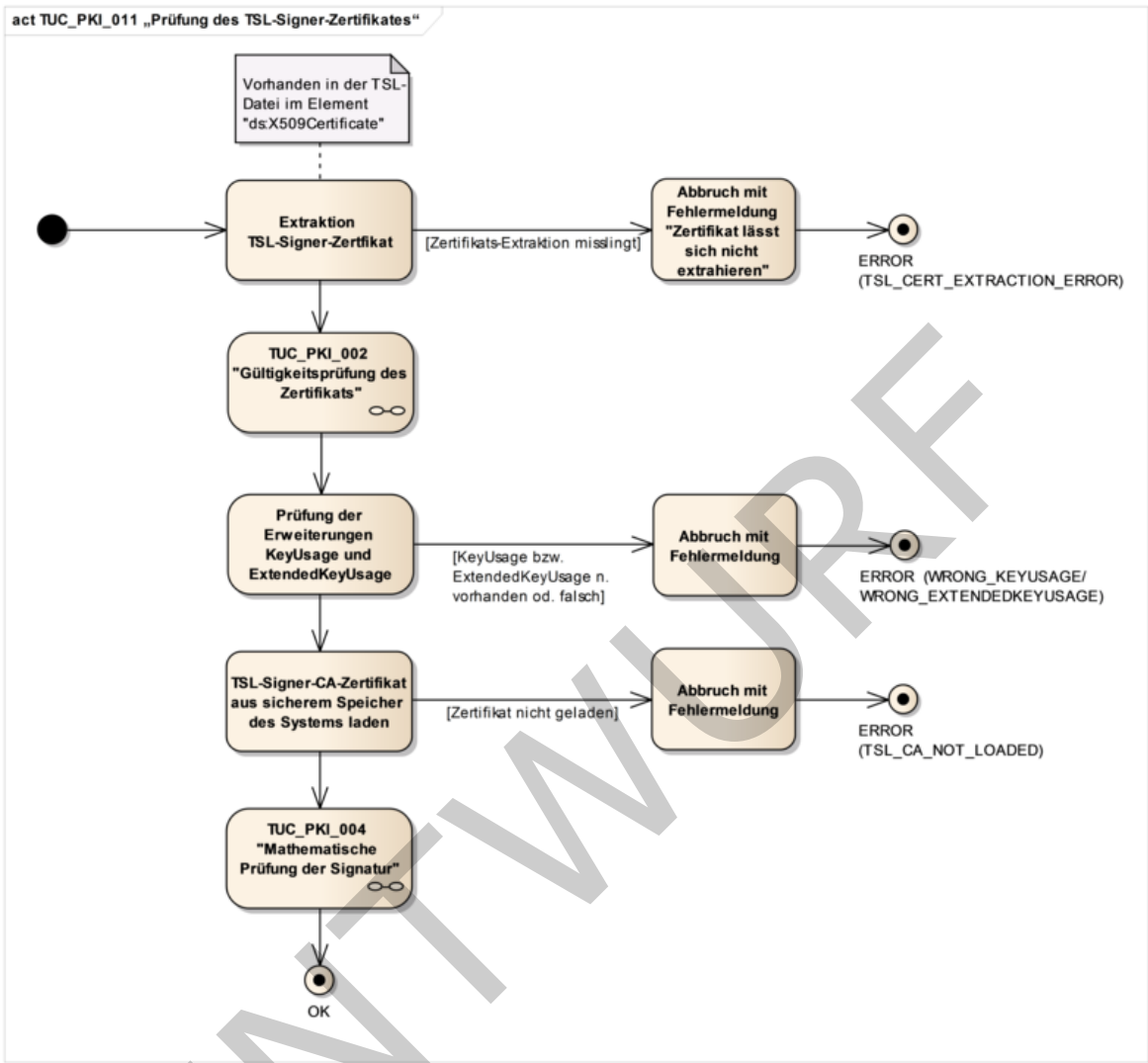


Abbildung 12: Aktivitätsdiagramm TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“

8.2.2.4 TUC_PKI_012 „XML-Signatur-Prüfung“

GS-A_4651 - TUC_PKI_012: XML-Signatur-Prüfung

Die Produkttypen der TI, die Zertifikate prüfen MÜSSEN TUC_PKI_012 zur Prüfung der Signatur einer XML-Datei umsetzen.

[<=]

Tabelle 85: TUC_PKI_012 „XML-Signatur- Prüfung“

Element	Beschreibung
Name	TUC_PKI_012 „XML-Signatur-Prüfung“

Beschreibung	In diesem Use Case wird die Prüfung der XML-Signatur der TSL beschrieben. Die Prüfung wird nicht näher spezifiziert, sondern richtet sich nach den Vorgaben und Standards von W3C.
Anwendungsumfeld	Dieser Use Case umfasst die Prüfung der XML-Signatur und wird durch jedes System verwendet, das eine XML-Signatur prüfen muss.
Vorbedingungen	(Valide) TSL-Datei mit Signatur: Die TSL-Datei wurde Schema-validiert (TUC_PKI_020) Das Signaturzertifikat dieser TSL-Datei muss erfolgreich geprüft worden sein. (TUC_PKI_011).
Auslöser	TUC_PKI_019 „Prüfung der Aktualität der TSL“
Eingangsdaten	signierte XML-Datei und Signaturzertifikat
Komponenten	System
Ausgangsdaten	Status der Prüfung
Referenzen	[XMLSig]
Standardablauf	Der Ablauf richtet sich nach den Vorgaben von W3C.
Fehlerfälle	[System:] Die Signatur ist nicht gültig. Ende des Use Case. Abbruch mit Fehlermeldung (XML_SIGNATURE_ERROR)
Anmerkungen	Vorgaben für die verwendeten Algorithmen und Schlüssellängen der Signatur werden hier nicht getroffen. Siehe dazu [gemSpec_Krypt#GS-A_4371].

3412 **8.2.3 TSL-Sicherheitsaspekte**

3413 Für den TI-Vertrauensanker, das TSL-Signer-CA-Zertifikat, und für die TSL (die
3414 enthaltenen Zertifikate und auch die eigentliche TSL-Datei im XML-Format) gilt ein hoher
3415 Schutzbedarf. Dieser wird dadurch gewährleistet, dass TI-Vertrauensanker und TSL-Datei
3416 initial auf (organisatorisch) abgesichertem Weg in die Komponente, bzw. deren sicheren
3417 Speicher, eingebracht werden. Vor einem Wechsel der TSL (oder des TI-
3418 Vertrauensankers via TSL) müssen immer zwingend Zertifikats- und Signaturprüfungen
3419 durchgeführt werden. Dies garantiert die Authentizität und Integrität der Informationen.

8.2.4 TSL-Zeitparameter

GS-A_4897 - Gültigkeitsdauer einer TSL

Der TSL-Dienst MUSS die Gültigkeitsdauer der TSL gemäß Tab_PKI_294 umsetzen.

Der TSL-Dienst MUSS den Zeitpunkt des resultierenden Gültigkeitsendes der TSL innerhalb des Elementes NextUpdate in der TSL-Datei eintragen.

[<=]

GS-A_4898 - TSL-Grace-Period einer TSL

Produkttypen der TI, die die TSL zur Validierung des TI-Vertrauensraums einsetzen,

MÜSSEN die TSL-Grace-Period gemäß Tab_PKI_294 umsetzen.

[<=]

GS-A_4899 - TSL Update-Prüfintervall

Produkttypen der TI, die die TSL zur Validierung des TI-Vertrauensraums einsetzen, MÜSSEN gemäß den in Tab_PKI_294 festgelegten TSL-Update Intervall prüfen, ob eine aktuellere als die vom System verwendete TSL bereitgestellt wurde.

[<=]

GS-A_5214 - TSL Neuausstellung

Der TSL-Dienst MUSS mindestens 7 Tage vor Ablauf der Gültigkeit der TSL eine neue Version der TSL erstellen.

[<=]

Tabelle 86: Tab_PKI_294 TSL Zeitparameter

Beschreibung	Zeitparameter
Gültigkeitsdauer einer TSL	Ausstellungsdatum + 30 Tage
TSL-Grace-Period für zentrale Dienste und fachanwendungsspezifische Dienste mit Anschluss an das zentrale Netz	0 Tage
TSL-Grace-Period für sonstige Dienste und Komponenten	0-30 Tage
TSL Update-Prüfintervall	24 Stunden

8.2.5 ServiceTypeIdentifier "unspecified"

Die Auswertung der TSL in der TI basiert auf [ETSI_TS_102_231_v3.1.2]. Dort wird der ServiceTypeIdentifier "<http://uri.etsi.org/TrstSvc/Svctype/unspecified>" definiert. Eine Komponente oder ein Dienst der TI muss also mit solch einem Identifier umgehen können. Um diesen Punkt jedoch noch deutlicher sichtbar zu machen wird er mit einer Anforderung in den Vordergrund gestellt.

A_17700 - TSL-Auswertung ServiceTypeIdentifier "unspecified"

Alle Produkttypen der TI, die die TSL auswerten, MÜSSEN TSPService-Einträge verarbeiten können mit dem ServiceTypeIdentifier "

<http://uri.etsi.org/TrstSvc/Svctype/unspecified>". Die Auswertung der TSL darf also nicht fehlschlagen wenn ein solcher ServiceTypeIdentifier in der TI vorgefunden wird.

[<=]

8.3 Zertifikatsprüfung X.509 nonQES

Für die Prüfung der X.509-Zertifikate gelten folgende Vorbedingungen (s. Kapitel 8.1 und 8.2):

- aktuelle TSL liegt vor
- TSL-Datei wurde geprüft
- Der TI-Vertrauensraum wurde initialisiert, der Truststore kann benutzt werden.

Die folgende Use Case Übersicht verdeutlicht die Aktionen des Systems.

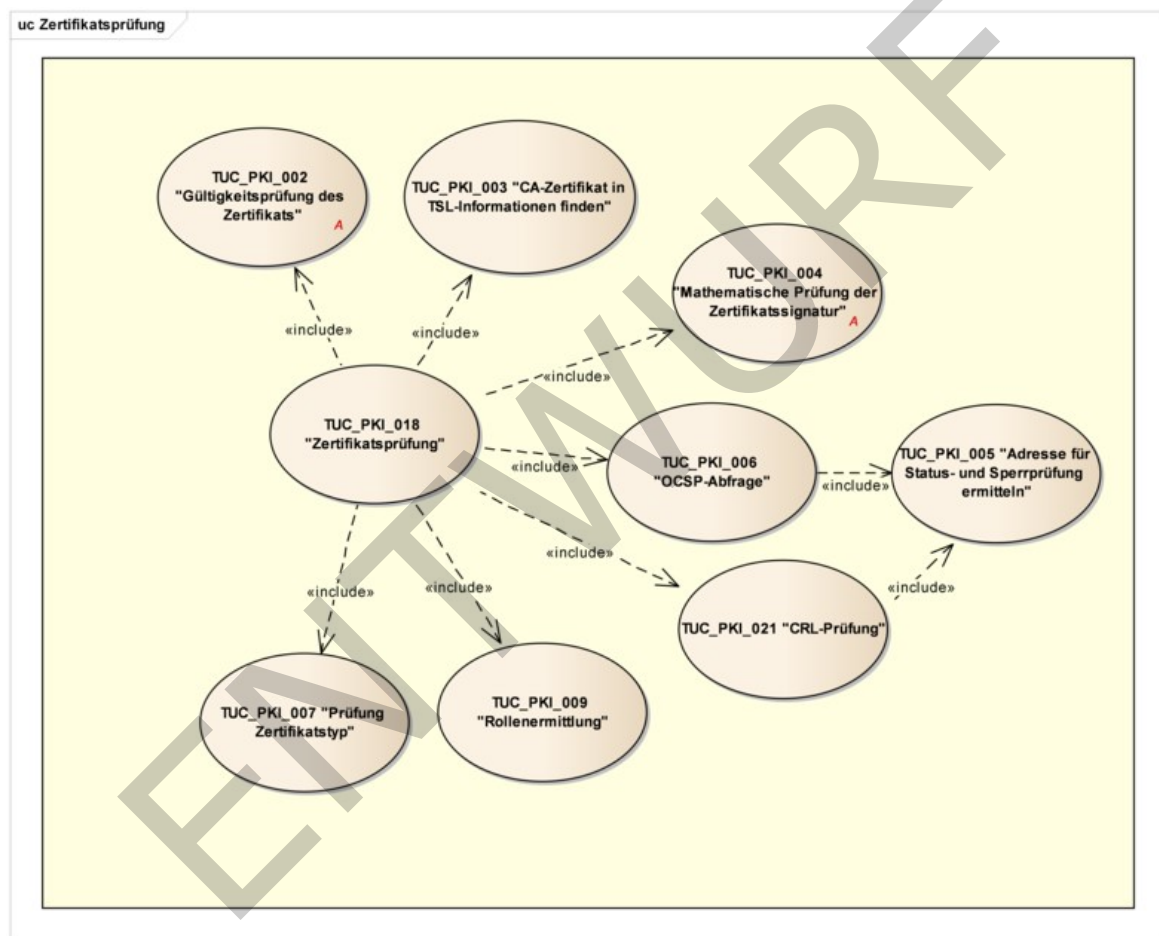


Abbildung 13: Use Case Diagramm „Zertifikatsprüfung“

Die folgenden Schritte sind für eine nonQES-Zertifikatsprüfung durchzuführen:

- Prüfung der Gültigkeit (TUC_PKI_002)
- Prüfung der Identität des Zertifikatsherausgebers (TUC_PKI_003)
- Prüfung der mathematischen Korrektheit des Zertifikats (Signaturprüfung) (TUC_PKI_004)

- Abfrage des Sperrstatus des zu prüfenden Zertifikats gegen den im „ServiceSupplyPoint“ der TSL eingetragenen OCSP-Responder (TUC_PKI_006) und Prüfung der OCSP-Antwort (Responder-Zertifikat, Sperrstatus)
- Rollenermittlung (TUC_PKI_009)
- Prüfung Zertifikatstyp (TUC_PKI_007)

Bei jeder dieser Prüfungen muss nicht nur die mathematisch-kryptographische Korrektheit der jeweiligen Mechanismen, sondern auch deren Zulässigkeit mit in die Prüfung einbezogen werden. Zum Beispiel darf ein Zertifikat, welches nicht mit einem zugelassenen Hash-Algorithmus signiert ist, nie als gültig eingestuft werden. Für die TI gültige Hash-Algorithmen siehe [gemSpec_Krypt].

Die Verwendung von Informationen aus Zertifikaten kann nur dann erfolgen, wenn das zugehörige Zertifikat validiert wurde. Somit MUSS eine Zertifikatsprüfung der Ermittlung bestätigter Zertifikatsinformationen vorangehen.

In dem Dokument wird der Begriff „gültiger Zeitraum“ verwendet. Dieser bedeutet, dass sich der aktuelle Zeitpunkt innerhalb des Gültigkeitszeitraums des Objektes befindet.

Die Fachdokumente müssen die entsprechenden Eingangsparameter der Use Cases berücksichtigen. Die Festlegungen aus den [folgenden Dokumentenstandards](#) [RFC6960], [RFC5280], [RFC5019] und [RFC3370/5754] sowie den spezifischen Eigenschaften der TI sind für die Zertifikatsprüfung verbindlich.

- [\[Common-PKI\]: Specifications for Interoperable PKI Applications](#)
- [\[RFC 2560\]: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP](#)
- [\[RFC 5280\]: Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List \(CRL\) Profile.](#)

8.3.1 Zertifikatsprüfung in der TI

8.3.1.1 TUC_PKI_018 „Zertifikatsprüfung in der TI“

GS-A_4652-01GS-A_4652 - TUC_PKI_018: Zertifikatsprüfung in der TI

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_018 zur Zertifikatsprüfung umsetzen:

[<=>]

Tabelle 87: TUC_PKI_018 „Zertifikatsprüfung in der TI“

Element	Beschreibung
Name	TUC_PKI_018 „Zertifikatsprüfung“
Beschreibung	Dieser Use Case beschreibt die Prüfung nicht-qualifizierter Zertifikate und umfasst die Offline- wie Online-Prüfung.

Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	Eine zeitlich nicht abgelaufene TSL (innerhalb der TSL-Graceperiod) steht als valide Basis zur Prüfung von Zertifikaten zur Verfügung
Auslöser	Zertifikats-Check
Eingangsdaten	<ul style="list-style-type: none"> • Das zu prüfende Zertifikat • Referenzzeitpunkt: Zeitpunkt, für den das Zertifikat geprüft werden soll (optional; bei Nichtangabe Verwendung der aktuellen Systemzeit): Zeitpunkt, für den das Zertifikat geprüft werden soll, s. a. Glossar aus Kap. 11.2 • PolicyList Liste der im aktuellen Aufruf zulässigen Zertifikatstyp-OIDs. Die Liste muss mindestens eine OID enthalten. • Vorgesehene KeyUsage (intendedKeyUsage, mehrere Werte möglich) • Vorgesehene ExtendedKeyUsage (intendedExtendedKeyUsage, mehrere Werte möglich) • OCSP-Graceperiod (legt bei der Verwendung von (gecachten) OCSP-Antworten den maximal zulässige Zeitraum fest, den die Systemzeit der prüfenden Komponente noch nach dem Zeitpunkt der OCSP-Antwort liegen darf (Default: 10 min)) • Offline-Modus (ja/nein) • Beigefügte OCSP-Response zum angefragten Zertifikat (optional; z. B. in der Signatur eingebettet) • Timeout-Parameter (Default: 10s) • TOLERATE_OCSP_FAILURE (true/false, Default: false) - Der Parameter definiert das Verhalten für den Fall, dass die OCSP-Prüfung nicht durchgeführt werden konnte, weil der OCSP-Responder

	<p>beispielsweise technisch nicht erreichbar ist.</p> <ul style="list-style-type: none"> • Prüfmodus (OCSP, CRL)
Komponenten	System, OCSP-Responder
Ausgangsdaten	Status der Prüfung, OCSP-Response, im Zertifikat enthaltene Rollen-OIDs
Referenzen	[Common-PKI] [RFC5280] Kap. 6.1, [X.509] Referenzierte Standards in den aufzurufenden TUCs
Standardablauf	<p>Die Zertifikatsprüfung setzt sich aus folgenden Schritten zusammen:</p> <ol style="list-style-type: none"> 1. [System] Die Gültigkeit des Zertifikats wird geprüft (TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats") . 2. [System] Prüfung der Extension KeyUsage auf Vorhandensein. Zudem wird die KeyUsage und ExtendedKeyUsage (falls vorhanden) auf die richtige Belegung entsprechend der vorgesehenen (intendedKeyUsage bzw. intendedExtendedKeyUsage) KeyUsage geprüft. Die intendedKeyUsage sowie die intendedExtendedKeyUsage können aus einer Liste mehrerer erlaubter Werte bestehen. Es wird geprüft, dass die im Parameter intendedKeyUsage bzw. intendedExtendedKeyUsage übergebenen Werte eine Teilmenge der Werte in der jeweiligen Extension KeyUsage bzw. ExtendedKeyUsage des Zertifikats sind. Da die übergebenen Parameter die Verwendung des Zertifikats im Aufrufkontext widerspiegeln, ist es dabei nicht notwendig, dass diese zu den Werten in der Zertifikatsextension komplett identisch sind. Enthält ein übergebener Parameter keine Werte, so bedeutet dies, dass der Inhalt der Zertifikatsextension nicht relevant ist. 3. [System] Das passende CA-Zertifikat wird in den TSL-Informationen gesucht (TUC_PKI_003 "CA-Zertifikat in TSL-Informationen finden") 4.

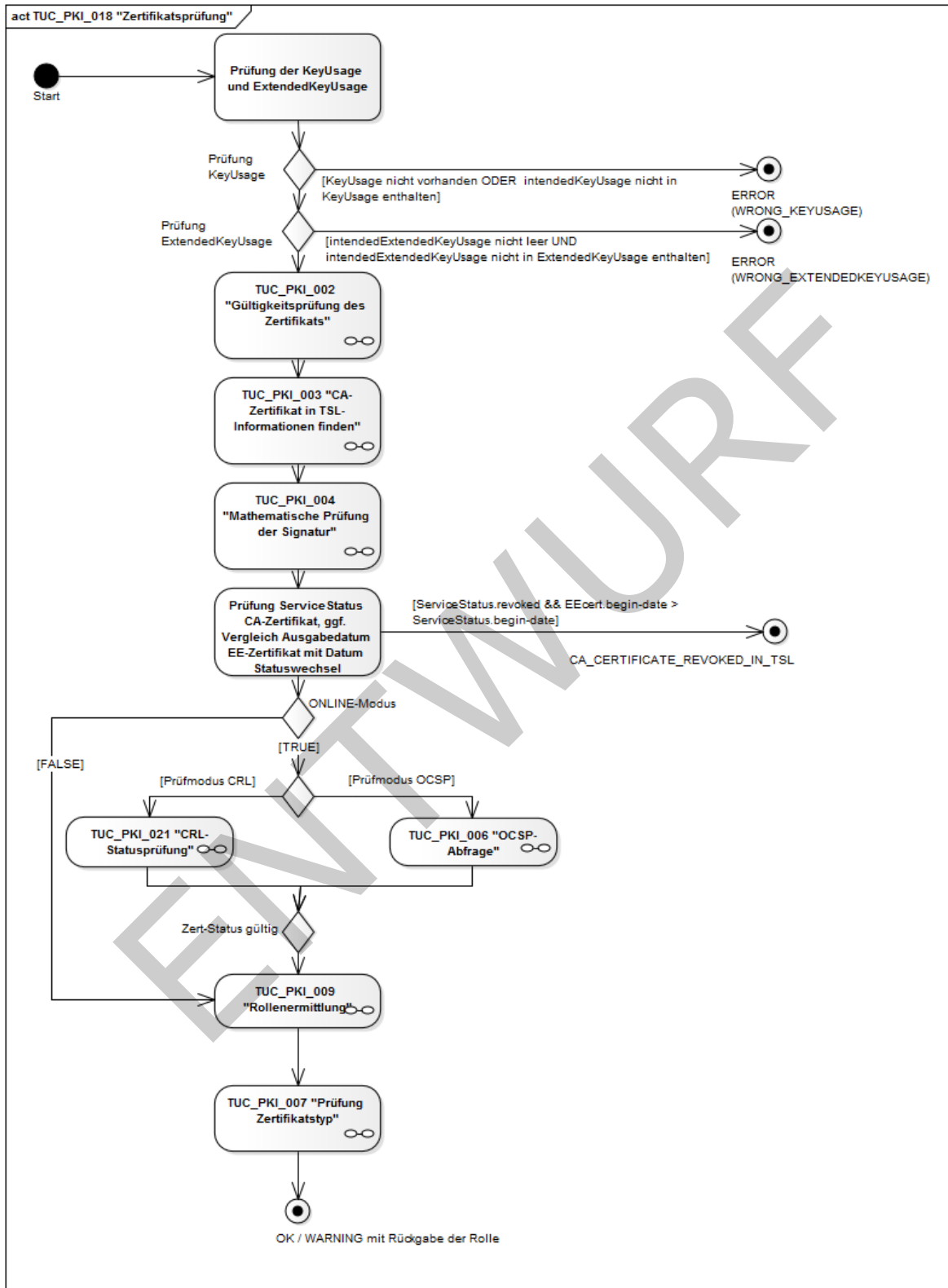
	<p>[System] Mathematische Prüfung der Signatur des Zertifikats (TUC_PKI_004 "Mathematische Prüfung der Zertifikatssignatur").</p> <p>5.</p> <p>[System] Der ServiceStatus (vgl. Tab_PKI_271) des CA-Zertifikats wird geprüft. Im Fall von „revoked“ wird der Zeitpunkt des Gültigkeitsbeginns (Feld "notBefore" gemäß [RFC5280]#4.1.2.5) des End-Entity-Zertifikats mit dem Datum des Statuswechsels (StatusStartingTime) verglichen.</p> <p>Der Zeitpunkt des Gültigkeitsbeginns des End-Entity-Zertifikats liegt vor dem Zeitpunkt des Statuswechsels.</p> <p>6.</p> <p>[System, Prüfmodus Offline] Falls JA, weiter mit Schritt 8, sonst mit 7.</p> <p>7.</p> <p>[System, Prüfmodus OCSP] Statusinformation zum Zertifikat durch Abfrage des zugeordneten OCSP-Dienstes ermitteln (TUC_PKI_006 "OCSP-Abfrage"). TUC_PKI_006 wird für TLS-Zertifikate der Störungsampel (C.ZD.TLS-S mit technischer Rolle oid_stamp) und nonQES-Zertifikate einer eGK mit dem Parameter ENFORCE_CERTHASH_CHECK=false aufgerufen. Für alle anderen Zertifikate wird TUC_PKI_006 mit dem Defaultwert ENFORCE_CERTHASH_CHECK=true aufgerufen.</p> <p>Wenn der zuständige OCSP-Responder die Statusinformation des Zertifikats mit einem Wert „revoked“ oder „unknown“ gemäß GS-A_4690 zurückgibt – Meldungskürzel (CERT_REVOKED) bzw. (CERT_UNKNOWN) gemäß Tab_PKI_274 oder eine wegen ENFORCE_CERTHASH_CHECK=true erforderliche certHash-Erweiterung fehlt (CERTHASH_EXTENSION_MISSING) bzw. falsch ist (CERTHASH_MISMATCH), darf das Zertifikat nicht als gültig bewertet werden.</p> <p>8.</p> <p>[System:] Ermittlung (TUC_PKI_009 "Rollenermittlung") der Rolle</p> <p>9.</p> <p>[System:] Prüfung, ob eine der übergebenen Zertifikatstyp-OIDs (aus der Parameter PolicyList) im Zertifikat enthalten ist (TUC_PKI_007 "Prüfung Zertifikatstyp"). Zur Prüfung muss die Liste (PolicyList s.o.)</p>
--	---

	<p>mindestens eine OID enthalten. 10. [System:] Ende des Use Cases mit Rückgabe des/der im Zertifikat enthaltenen Rollen-OID(s).</p>
Varianten/Alternativen	<p>6a. [System:] Der Offline-Modus ist aktiviert. Es werden keine Statusinformationen zum Zertifikat eingeholt. 7a. [System, Prüfmodus CRL] Prüfung der Sperrinformation des Zertifikates mittels CRL (TUC_PKI_021 "CRL-Prüfung"). Wenn das Zertifikat in der Sperrliste (CRL) enthalten ist – Meldungskürzel (CERT_REVOKED) gemäß Tab_PKI_274, darf das Zertifikat nicht als gültig bewertet werden. 7b [System] Eine OCSP-Response zu dem zu prüfenden Zertifikat wurde im Aufruf mit übergeben. Falls diese zum Referenzzeitpunkt gültig ist, wird nicht der TUC_PKI_006 aufgerufen, sondern die beigefügte OCSP-Response zur weiteren Prüfung verwendet.</p>
Fehlerfälle	<p>2a. [System:] KeyUsage ist nicht vorhanden bzw. nicht alle Werte der intendedKeyUsage in der KeyUsage enthalten (WRONG_KEYUSAGE). 2a1. [System:] intendedExtendedKeyUsage enthält Werte und nicht alle davon sind in der ExtendedKeyUsage enthalten (WRONG_EXTENDEDKEYUSAGE). 5a. [System:] Das Ausgabedatum des End-Entity-Zertifikats liegt nach dem Datum des Statuswechsels. Abbruch mit Fehlermeldung (CA_CERTIFICATE_REVOKED_IN_TSL) 7c. [System] Eine OCSP-Response zu dem zu prüfenden Zertifikat wurde im Aufruf mit übergeben, ergab bei den weiteren Prüfschritten jedoch kein gültiges Ergebnis (Überprüfung und Auswertung der Gültigkeit der OCSP-Response in TUC_PKI_006 schlägt fehl). Eine erneute</p>

	<p>Prüfung wird in diesem Fall durch Aufruf des TUC_PKI_006 durchgeführt, als wäre keine OCSP-Response beigefügt.</p> <p>In den Rückgabewerten dieses TUC wird die Warnmeldung (PROVIDED_OCSP_RESPONSE_NOT_VALID) an die aufrufende Funktion übergeben.</p>
Sicherheitsanforderungen	<p>Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.</p>
Anmerkungen	<p>Gültige Status zu Schritt 5 sind gemäß Tab_PKI_271 inaccord, revoked und expired.</p> <p>Schritt 5 stellt eine Sperrprüfung des CA-Zertifikats (für nonQES-HBA- und SMC-B-Zertifikate) gemäß Ketten- bzw. Kompromissmodell dar. Vgl. Kap. 8.1.1 Initialisierung TI-Vertrauensraum.</p> <p>Eine Zertifikatsprüfung in der TI gemäß TUC_PKI_018 darf nach Ablauf der TSL-Graceperiod nicht positiv ausfallen (vgl. GS-A_5336).</p>
Zugehörige Diagramme	<p>Aktivitätsdiagramm TUC_PKI_018 "Zertifikatsprüfung".</p> <p>Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.</p>

[<=]

3508



3509

3510

Abbildung 14: Aktivitätsdiagramm TUC_PKI_018 „Zertifikatsprüfung“

8.3.1.2 TUC_PKI_002 „Gültigkeitsprüfung des Zertifikats“

GS-A_4653-01GS-A_4653 - TUC_PKI_002: Gültigkeitsprüfung des Zertifikats

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_002 zur Gültigkeitsprüfung des Zertifikates umsetzen:

[\[<=>\]](#)

Tabelle 88: TUC_PKI_002 „Gültigkeitsprüfung des Zertifikats“

Element	Beschreibung
Name	TUC_PKI_002 „Gültigkeitsprüfung des Zertifikats“
Beschreibung	Dieser Use Case beschreibt die Prüfung des Zertifikats auf seine aktuelle zeitliche Gültigkeit. Damit ist der Zeitraum gemeint, der im Feld <i>validity</i> steht. Die Prüfung richtet sich nach referenzierten Standards.
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	Zertifikat vorhanden
Auslöser	Zertifikatsprüfung in der TI, TUC_PKI_013 „Import TI-Vertrauensanker aus TSL“, TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“, TUC_PKI_018 "Zertifikatsprüfung in der TI " TUC_PKI_030 "QES-Zertifikatsprüfung"
Eingangsdaten	<ul style="list-style-type: none"> Das zu prüfende Zertifikat Referenzzeitpunkt (optional; bei Nichtangabe Verwendung der aktuellen Systemzeit): Zeitpunkt, für den das Zertifikat geprüft werden soll, s. a. Glossar aus Kap. 11.2
Komponenten	System
Ausgangsdaten	Status der Prüfung
Referenzen	[Common-PKI#Part1#2—Table-3] , [Common-PKI#Part5#2.2—Table-4, Nr.

	13], [RFC5280#4.1] [eIDAS], [ETSI EN 319 412-5] , [RFC5280]
Standardablauf	<ol style="list-style-type: none"> 1. [System:] Zertifikat lesen 2. [System:] Aus dem Zertifikat das Feld Validity ermitteln und auslesen. 3. [System:] Anhand der ermittelten Daten wird die Gültigkeit geprüft. Dabei kommt folgender Algorithmus zu tragen: notBefore =< Referenzzeitpunkt && notAfter >= Referenzzeitpunkt entspricht einem zeitlich gültigem gültigen Zertifikat. Details siehe [RFC5280] Kap. 4.1.2.5 und 6.1.3 4. [System:] Rückmeldung des Status
Fehlerfälle	<ol style="list-style-type: none"> 1a. [System:] Zertifikat ist nicht lesbar (CERT_READ_ERROR). 3a. [System:] Prüfzeitpunkt nicht innerhalb der Gültigkeitsdauer des Zertifikats (CERTIFICATE_NOT_VALID_TIME).
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	<p>Der Aufbau der Gültigkeit: wird nicht näher spezifiziert, sondern richtet sich nach referenzierten Standards.</p> <p>Die (zeitliche) Gültigkeitsprüfung ist nach [eIDAS] Artikel 28 Satz (1) auch für die QES-Zertifikatsprüfung gemäß TUC_PKI_030 verpflichtend.</p>
Zugehörige Diagramme	<p>Aktivitätsdiagramm TUC_PKI_002 Gültigkeitsprüfung des Zertifikats.</p> <p>Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.</p>

[\[<=\]](#)

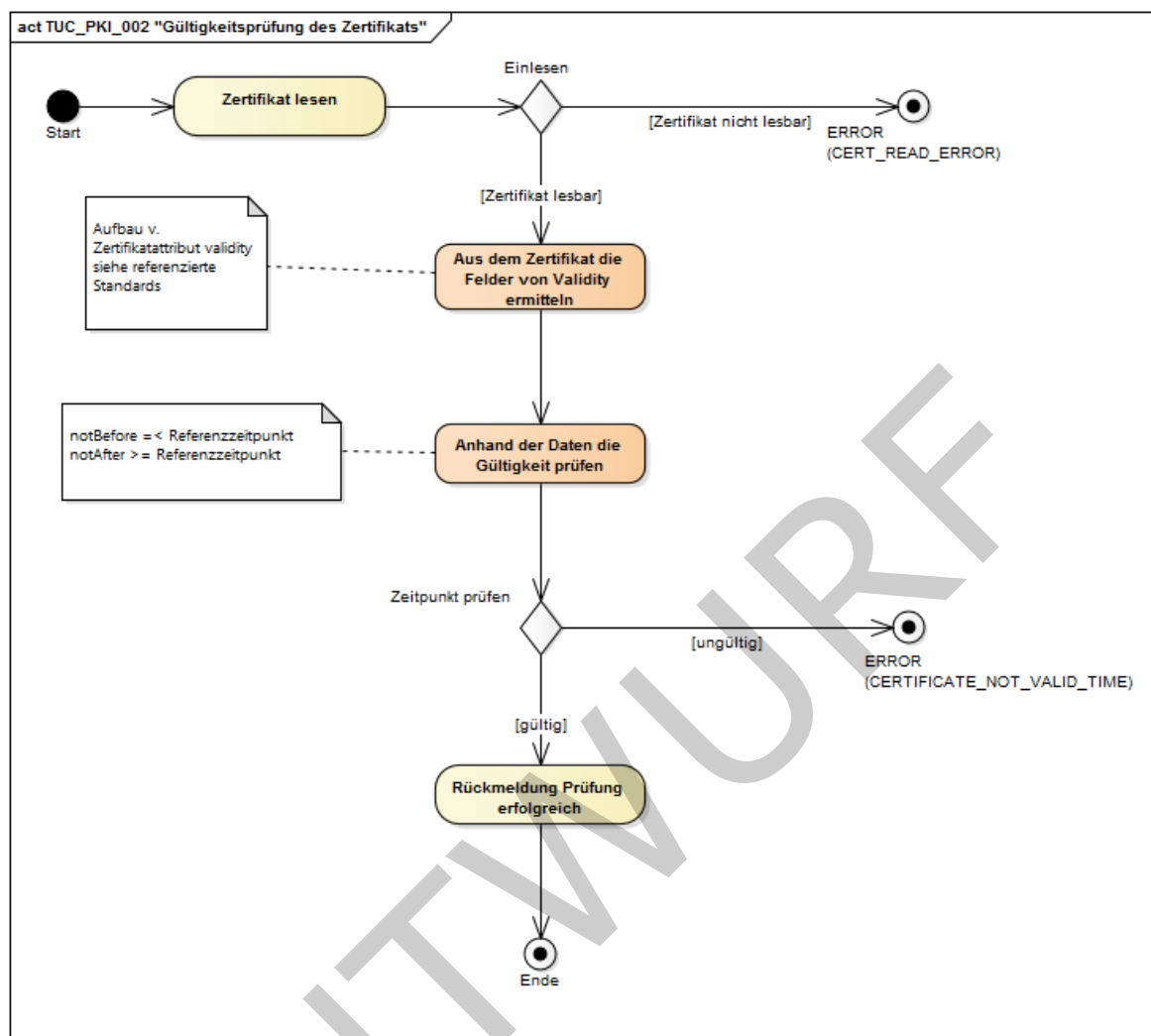


Abbildung 15: Aktivitätsdiagramm TUC_PKI_002 Gültigkeitsprüfung des Zertifikats

8.3.1.3 TUC_PKI_003 „CA-Zertifikat in TSL-Informationen finden“

GS-A_4654-01GS-A_4654 - TUC_PKI_003: CA-Zertifikat finden

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_003 zur Ermittlung des CA-Zertifikats aus den TSL-Informationen umsetzen-

[<=>]

Tabelle 89: TUC_PKI_003 „CA-Zertifikat in TSL-Informationen finden“

Element	Beschreibung
Name	TUC_PKI_003 „CA-Zertifikat in TSL-Informationen finden“

Beschreibung	Anhand der Daten aus dem Zertifikat wird versucht das CA-Zertifikat in der TSL zu finden.
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	Zertifikat innerhalb des definierten Gültigkeitszeitraums Eine TSL mit gültiger Signatur
Auslöser	TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln", TUC_PKI_018 "Zertifikatsprüfung in der TI "
Eingangsdaten	End-Entity-Zertifikatsdaten, TSL-Informationen
Komponenten	System
Ausgangsdaten	Status der Prüfung, (Referenz auf) CA-Zertifikat
Referenzen	[Common-PKI] [ETSI TS 102 231]
Standardablauf	<ol style="list-style-type: none"> 1. [System:] Anhand der End-Entity-Zertifikatsdaten werden die TSL-Informationen durchsucht, um das passende CA-Zertifikat zu finden. Details siehe [ETSI TS 102 231] Kap. 5.5.1 und D.2. 2. [System:] Vergleich 1: IssuerDN des End-Entity-Zertifikats mit dem subjectDN des CA-Zertifikats 3. [System:] Vergleich 2: AuthorityKeyIdentifier des End-Entity-Zertifikats mit SubjectKeyIdentifier des CA-Zertifikats 4. [System:] Selektion (Referenz auf) CA-Zertifikat und Rückgabe
Varianten/Alternativen	<ol style="list-style-type: none"> 2a. [System:] Keine Übereinstimmung. Der Vorgang wird mit einem anderen CA-Zertifikat wiederholt (Iteration)

Fehlerfälle	2b. [System:] Ende der Liste erreicht UND keine Übereinstimmung im DN gefunden. Abbruch des TUC mit Fehlermeldung (CA_CERT_MISSING) 3a. [System:] CA mit passendem DN gefunden, aber Ausstellerschlüssel (SubjectKeyIdentifier) und die Referenz (AuthorityKeyIdentifier) stimmen nicht überein. Abbruch des TUC mit Fehlermeldung (AUTHORITYKEYID_DIFFERENT)
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_003 CA- Zertifikat in TSL-Informationen finden. Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

[<=]

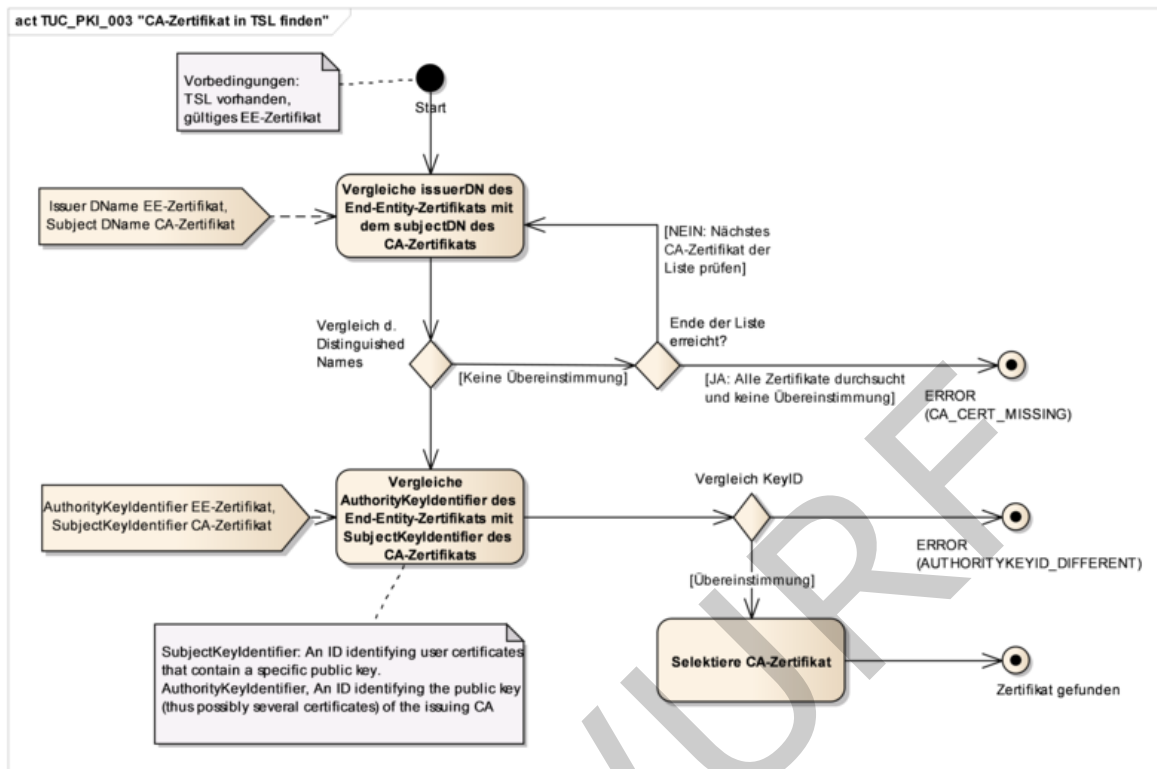


Abbildung 16: Aktivitätsdiagramm TUC_PKI_003 CA-Zertifikat in TSL-Informationen finden

8.3.1.4 TUC_PKI_004 „Mathematische Prüfung der Zertifikatssignatur“

GS-A_4655-01GS-A_4655 - TUC_PKI_004: Mathematische Prüfung der Zertifikatssignatur

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_004 zur mathematischen Prüfung der Zertifikatssignatur umsetzen.

[<=>]

Tabelle 90: TUC_PKI_004 „Mathematische Prüfung der Zertifikatssignatur“

Element	Beschreibung
Name	TUC_PKI_004 „Mathematische Prüfung der Zertifikatssignatur“
Beschreibung	Dieser Use Case beschreibt die mathematische Prüfung der Signatur des End-Entity-Zertifikats mit Hilfe des CA-Zertifikats.
Anwendungsumfeld	System, das Zertifikate verwendet

Vorbedingungen	Gültiges CA-Zertifikat und passendes End-Entity-Zertifikat innerhalb des definierten Gültigkeitszeitraums
Auslöser	TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“, TUC_PKI_013 „Import TI-Vertrauensanker aus TSL“, TUC_PKI_018 "Zertifikatsprüfung in der TI "
Eingangsdaten	End-Entity-Zertifikat, CA-Zertifikat
Komponenten	System
Ausgangsdaten	Status der Prüfung
Referenzen	[Common-PKI]RFC5280]
Standardablauf	<ol style="list-style-type: none"> 1. [System:] Auswahl des öffentlichen Schlüssels des CA-Zertifikats 2. [System:] Die Signatur und der verwendete Algorithmus werden aus dem End-Entity-Zertifikat ausgelesen 3. [System:] Verifikation der Signatur und Hashwert-Vergleich (Verfahren siehe RFC5280) Kap. 6.1) 4. [System:] Rückmeldung an das System
Fehlerfälle	3a. [System:] Die Zertifikats-Signatur ist nicht gültig. Ende des Use Case. Abbruch mit Fehlermeldung (CERTIFICATE_NOT_VALID_MATH)
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	signatureAlgorithm AlgorithmIdentifier: Stellt den verwendeten Signatur-Algorithmus dar, den die CA benutzt hat, um das Zertifikat zu signieren. signature BIT STRING: Die Signatur des Zertifikats.
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_004 Mathematische Prüfung der Zertifikatssignatur. Das Diagramm dient nur der

Veranschaulichung und ist nicht normativ.
Gegebenenfalls enthält es nicht alle
Prüfschritte und Meldungen im Detail.

[<=]

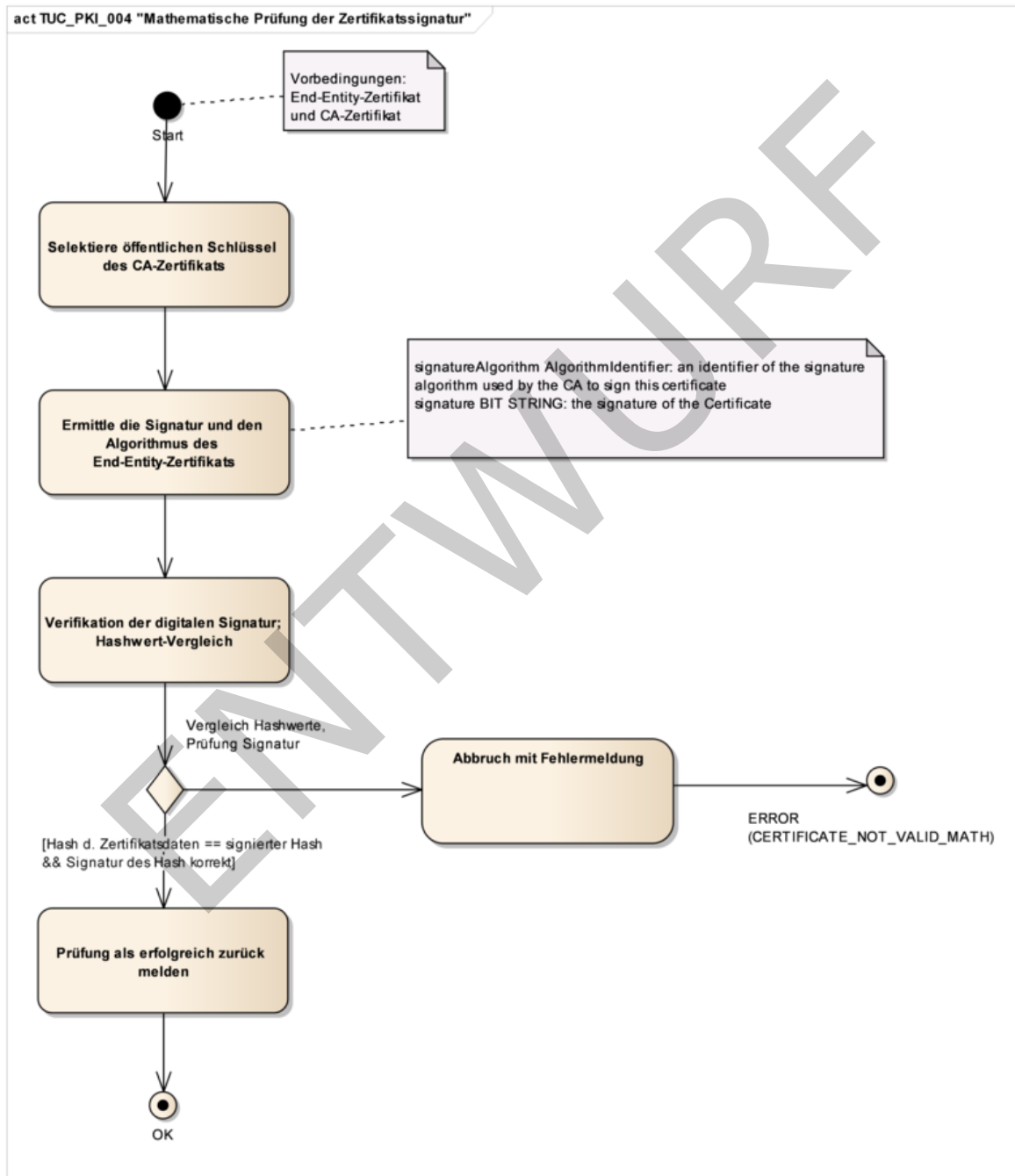


Abbildung 17: Aktivitätsdiagramm TUC_PKI_004 Mathematische Prüfung der Zertifikatssignatur

8.3.2 Statusprüfung

8.3.2.1 TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln“

GS-A_4656 - TUC_PKI_005: Adresse für Status- und Sperrprüfung ermitteln

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_005 zur Ermittlung der Adresse für Status- und Sperrprüfung umsetzen.

[<=]

Tabelle 91: TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln“

Element	Beschreibung
Name	TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln“
Beschreibung	In diesem Use Case wird die Ermittlung der Adresse für Status- und Sperrprüfung beschrieben. Default-mäßig handelt es sich dabei um die Adresse des OCSP-Responders, alternativ um diejenige des CRL-Downloadpunktes. Hierbei wird auf die TSL-Informationen zurückgegriffen. Die Adresse ist im CA-Eintrag der TSL hinterlegt. Für das Verhalten in spezifizierten Offline-Szenarien gilt [GS-A_4658].
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	Eine TSL mit gültiger Signatur
Auslöser	TUC_PKI_006 "OCSP-Abfrage" oder TUC_PKI_021 "CRL-Prüfung"
Eingangsdaten	<ul style="list-style-type: none"> • End-Entity-Zertifikatsdaten • TSL-Informationen
Komponenten	System
Ausgangsdaten	OCSP-Adresse oder Adresse des CRL-Downloadpunktes
Standardablauf	<ol style="list-style-type: none"> 1. [System:] (Referenz auf) CA-Zertifikat in TSL-Informationen finden (TUC_PKI_003 "CA-Zertifikat in TSL-Informationen finden") 2. [System:] Das Element "ServiceSupplyPoint" (bzw. via referenziertes CA-Zertifikat die Referenz auf den bezeichneten Statusprüfdienst- oder CRL Downloadpunkt) auswählen und URI selektieren.

	3. [System:] Adresse zurückmelden
Fehlerfälle	1a. [System:] CA kann nicht in den TSL-Informationen ermittelt werden (CA_CERT_MISSING). 2a. [System:] Das Element „ServiceSupplyPoint“ konnte nicht gefunden werden (SERVICESUPPLYPOINT_MISSING). Weitere Fehlerfälle werden in den jeweiligen referenzierten TUCs beschrieben.
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	Die Adresse des Statusprüfdienstes oder des CRL-Downloadpunktes muss nicht zwingend in der TSL-Datei vorgehalten werden, sondern kann z. B. im Truststore des Systems gespeichert und aufgerufen werden.
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

3567
3568

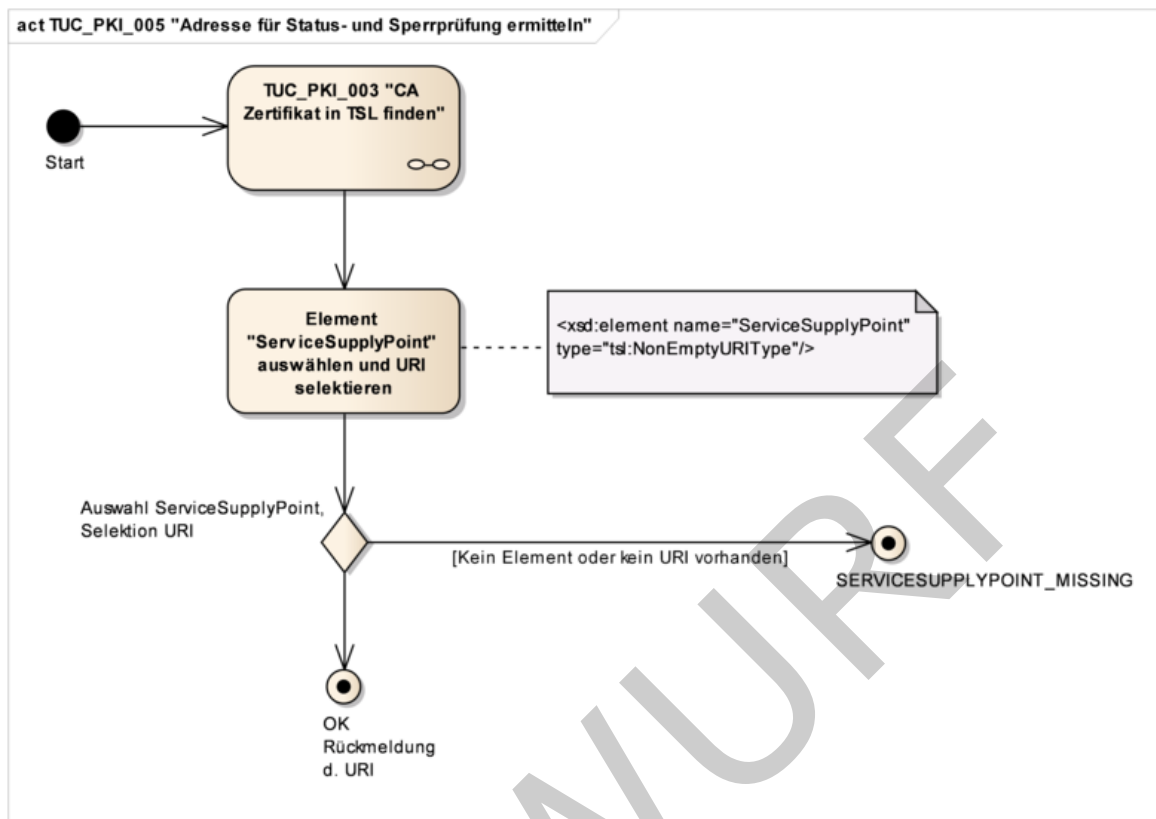


Abbildung 18: Aktivitätsdiagramm TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln“

8.3.2.2 TUC_PKI_006 „OCSP-Abfrage“

GS-A_4657-03GS-A_4657 - TUC_PKI_006: OCSP-Abfrage

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_006 zur OCSP-Abfrage umsetzen.

[<=>]

Tabelle 92: TUC_PKI_006 „OCSP-Abfrage“

Element	Beschreibung
Name	TUC_PKI_006 „OCSP-Abfrage“
Beschreibung	Dieser Use Case beschreibt den Prozess zur OCSP-Prüfung eines Zertifikats. Für das Verhalten in spezifizierten Offline-Szenarien gilt [GS-A_4658]. Der Use Case richtet sich nach den Anforderungen gemäß [Common-PKI#Part5#2.3] aus den referenzierten Standards und nach den spezifischen Eigenschaften der TI.

Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	Zeitlich gültiges End-Entity- und CA-Zertifikat. TSL-Informationen sind vorhanden.
Auslöser	Zertifikats-Check
Eingangsdaten	<ul style="list-style-type: none"> • End-Entity-Zertifikatsdaten • CA-Zertifikatsdaten • TSL-Informationen • Referenzzeitpunkt (optional; bei Nichtangabe Verwendung der aktuellen Systemzeit, vgl. Glossar aus Kapitel 11.2); Zeitpunkt, für den das Zertifikat geprüft werden soll • OCSP-Graceperiod (Default: 10min) • Timeout-Parameter (Default: 10s) • TOLERATE_OCSP_FAILURE (true/false, Default: false) • ENFORCE_CERTHASH_CHECK (true/false, Default: false)
Komponenten	System, OCSP-Responder
Ausgangsdaten	Status der Prüfung OCSP-Response
Referenzen	[Common-PKI-Part 4#3, [Common-PKI-Part 5#2.3], [RFC2560]/[RFC6960], [RFC5019], [RFC3370], [RFC5754]
Standardablauf	<ol style="list-style-type: none"> 1. [System:] Prüfung, ob (zum Referenzzeitpunkt unter Berücksichtigung der OCSP-Graceperiod) gültige Statusinformationen bereits vorliegen (z. B. im lokalen Cache bereitgestellt). 2. [System:] Ermittlung der OCSP-Adresse (TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln") 3. [System:] Aufbau des OCSP-Request anhand der passenden Zertifikatsdaten 4. [System:] Absenden des Request an die ermittelte Adresse Der Timeout-Parameter definiert hier, zu welchem Zeitpunkt das System ein Timeout bei Nichterreichbarkeit des Dienstes meldet. 5.

	<p>[System, OCSP-Responder:] Überprüfung der OCSP-Response (Signatur) auf Integrität. Das dazu benötigte OCSP-Responder-Zertifikat in den TSL-Informationen ermitteln. Die OCSP-Responder-Zertifikate sind alle in den TSL-Informationen enthalten. Somit kann direkt nach dem Zertifikat gesucht werden. (OCSP-Responder sind in der TSL-Datei mit dem „ServiceTypeIdentifizier“ „http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP“ markiert.)</p> <p>6.</p> <p>[System:] Auswertung der OCSP-Response. Dies umfasst die Prüfung von</p> <ul style="list-style-type: none"> • Statuscode („OCSPResponseStatus“) auf Belegung mit ‚0‘ (für „successful“), • Zertifikatsidentifizierungs-Informationen („CertID“) auf Identität mit derjenigen aus dem Request und • Konformität/Plausibilität der Zeitangaben („producedAt“, „thisUpdate“ und (sofern vorhanden) „nextUpdate“). <p>Details siehe</p> <ul style="list-style-type: none"> • [RFC2560]/[RFC6960] Kap. 4.1, 4.2, und 4.4 • [Common PKI] Part 4, Kap. 3, • [Common PKI] Part 5, Kap. 2.3, • [RFC5019], Kap. 4, • [gemSpec_PKI] Kap. 9.1.2 (insb. [GS-A_5215]). <p>7.</p> <p>[System:] Wenn ENFORCE_CERTHASH_CHECK auf ‚true‘ gesetzt ist, wird das End-Entity-Zertifikat mit dem in der certHash-Erweiterung bezeichneten Algorithmus gehasht (vgl. [gemSpec_Krypt#GS-A_4393]). Das Resultat stimmt mit dem gelieferten certificateHash überein. Details siehe [Common PKI#Part4#3.1.2] und [Common PKI#Part5#2.3].</p> <p>8.</p> <p>[System:] Überprüfung der Gültigkeit anhand des Referenzzeitpunkts. Der CertStatus „good“ wird gemeldet.</p> <p>9.</p> <p>[System:] Rückmeldung, dass das Zertifikat gültig ist und Rückgabe der OCSP-Response.</p> <p>10.</p> <p>[System:] Ende des UseCase</p>
Varianten/Alternativen	<p>1a.</p> <p>[System:] Prüfung der Gültigkeit des Zertifikats gegen vorliegende Informationen.</p>

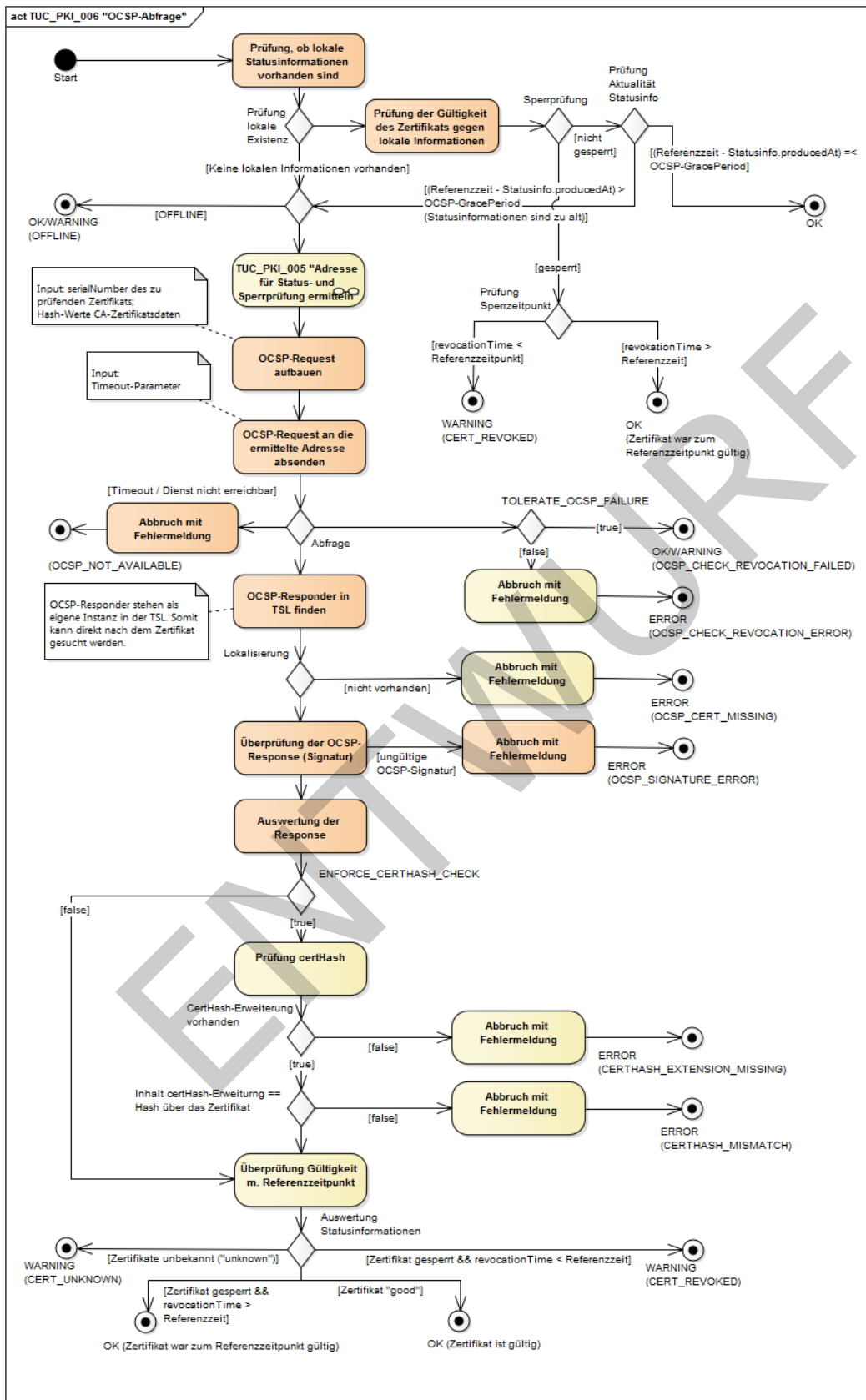
	<p>1a1. [System:] Zertifikat ist gesperrt. Weiter mit Schritt 5, falls die entsprechenden Prüfungen nicht bereits erfolgt sind. Ansonsten Rückmeldung analog 8.</p> <p>1a2. Die Statusinformationen sind zu alt (Zertifikat nicht gesperrt && (Referenzzeit - Statusinfo.producedAt) > OCSP-Graceperiod)). Neue Informationen müssen eingeholt werden. Es geht weiter mit Schritt 2 (Standardablauf).</p> <p>1a3. [System:] Zertifikat ist nicht gesperrt und Statusinformationen sind noch gültig Referenzzeit - Statusinfo.producedAt) <= OCSP-Graceperiod. Rückmeldung: Zertifikat ist gültig.</p> <p>7a. [System:] ENFORCE_CERTHASH_CHECK ist auf 'false' gesetzt. Weiter mit nächstem Schritt. Damit wird eine etwaig vorhandene Erweiterung 'certHash' ignoriert.</p> <p>8a. [System:] Das Zertifikat ist für den Referenzzeitpunkt gültig, obwohl der CertStatus "revoked" gemeldet wird, da "revocationTime" > Referenzzeitpunkt. Rückmeldung Zertifikat ist für den Referenzzeitpunkt gültig und Rückgabe der OCSP-Response.</p> <p>8b. [System:] Zertifikat ist gesperrt und die Referenzzeit liegt nach dem Sperrzeitpunkt (CertStatus revoked UND revocationTime <= des Referenzzeitpunkts). Rückmeldung Zertifikat ist gesperrt und Rückgabe der OCSP-Response. (CERT_REVOKED)</p> <p>8c. [System:] Zertifikat ist unbekannt (Status unknown) Rückmeldung, dass das Zertifikat ungültig ist und Rückgabe der OCSP-Response. (CERT_UNKNOWN)</p>
Fehlerfälle/Warnungen	<p>4a. [System:] Die OCSP-Prüfung konnte nicht durchgeführt werden: Im Falle von TOLERATE_OCSP_FAILURE=true wird als Ergebnis eine Warnung generiert (OCSP_CHECK_REVOCATION_FAILED).</p> <p>4b. [System:] Die OCSP-Prüfung konnte nicht durchgeführt werden: Im Falle von TOLERATE_OCSP_FAILURE=false wird mit einer Fehlermeldung abgebrochen. (OCSP_CHECK_REVOCATION_ERROR)</p> <p>4c. [System:] Der OCSP-Responder ist (unabhängig v. TOLERATE_OCSP_FAILURE) nicht verfügbar. (OCSP_NOT_AVAILABLE)</p> <p>5a. [System:] OCSP-Zertifikat nicht in TSL-Informationen enthalten. Abbruch mit Fehlermeldung. (OCSP_CERT_MISSING)</p>

	<p>5a1. [System:] Signatur der Response ist nicht gültig. Abbruch mit Fehlermeldung (OCSP_SIGNATURE_ERROR)</p> <p>6a. [System:] Die Response enthält einen Statuscode („OCSPResponseStatus“), der ungleich 0 (für „successful“) ist. (Damit zeigt der OCSP-Responder eine Exception an. Z. B. kann der Wert für den Status auf 3 für „tryLater“ gesetzt sein.) Abbruch mit Fehlermeldung (OCSP_STATUS_ERROR)</p> <p>6b. [System:] Die Response enthält einen Statuscode („OCSPResponseStatus“), der gleich 0 („successful“) ist. Die ausgewertete OCSP-Response passt aber nicht zum OCSP-Request (z.B. CertID in OCSP-Request und — Response stimmt gemäß [Common PKI#Part4#3] nicht überein). Abbruch mit Fehlermeldung (OCSP_CHECK_REVOCATION_ERROR)</p> <p>7b. ENFORCE_CERTHASH_CHECK ist auf 'true' gesetzt und die OCSP-Response enthält keine certHash-Erweiterung. (CERTHASH_EXTENSION_MISSING)</p> <p>7c. Der errechnete Zertifikats-Hash stimmt nicht mit demjenigen aus der in der Erweiterung certHash überein. (CERTHASH_MISMATCH)</p>
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	<p>Der genaue Aufbau des OCSP-Requests und der OCSP-Response ist in Kapitel 9 spezifiziert.</p> <p>Zur Abfrage beim OCSP-Responder MUSS ein Timeout-Parameter konfiguriert werden können. Dieser definiert, zu welchem Zeitpunkt das System ein Timeout bei Nichterreichbarkeit des Dienstes meldet.</p> <p>Die OCSP-Graceperiod dient der Performance-Steigerung. Die OCSP-Graceperiod legt bei der Verwendung von OCSP-Antworten (im Cache) deren maximal zulässiges Alter fest (gemessen an der Systemzeit). Ein Zwang, OCSP-Responses über die gesamte Dauer der OCSP-Graceperiod zu cachen, existiert nicht.</p> <p>Anmerkung zu 6b: Die OCSP-Response muss gemäß [Common PKI] Part 4#3 bzw. RFC3370#2.1RFC6960 Kap. 4.2 verarbeitet werden, unabhängig davon, ob das Feld "parameters" der Sequenz AlgorithmIdentifier innerhalb der CertID mit NULL belegt oder nicht gesetzt ist, Details siehe Tab PKI_290 . Der in [RFC5754] Kap. 2 empfohlene SHA2 als Hash-Algorithmus für die Bildung von certID wird nicht von allen OCSP-Responder-Produkten unterstützt.</p>

	Hinweis zum Referenzzeitpunkt (s. auch Glossar aus Kapitel 11.2): Bei der Prüfung von nonQES-Zertifikaten handelt es sich beim jeweiligen Referenzzeitpunkt um die aktuelle Systemzeit. Dadurch vereinfacht sich der Ablauf des TUC: Die Variante 8a ist unter diesen Umständen nicht möglich, sie muss also nicht berücksichtigt werden.
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_006 "OCSP-Abfrage". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

[<=]

ENTWURF



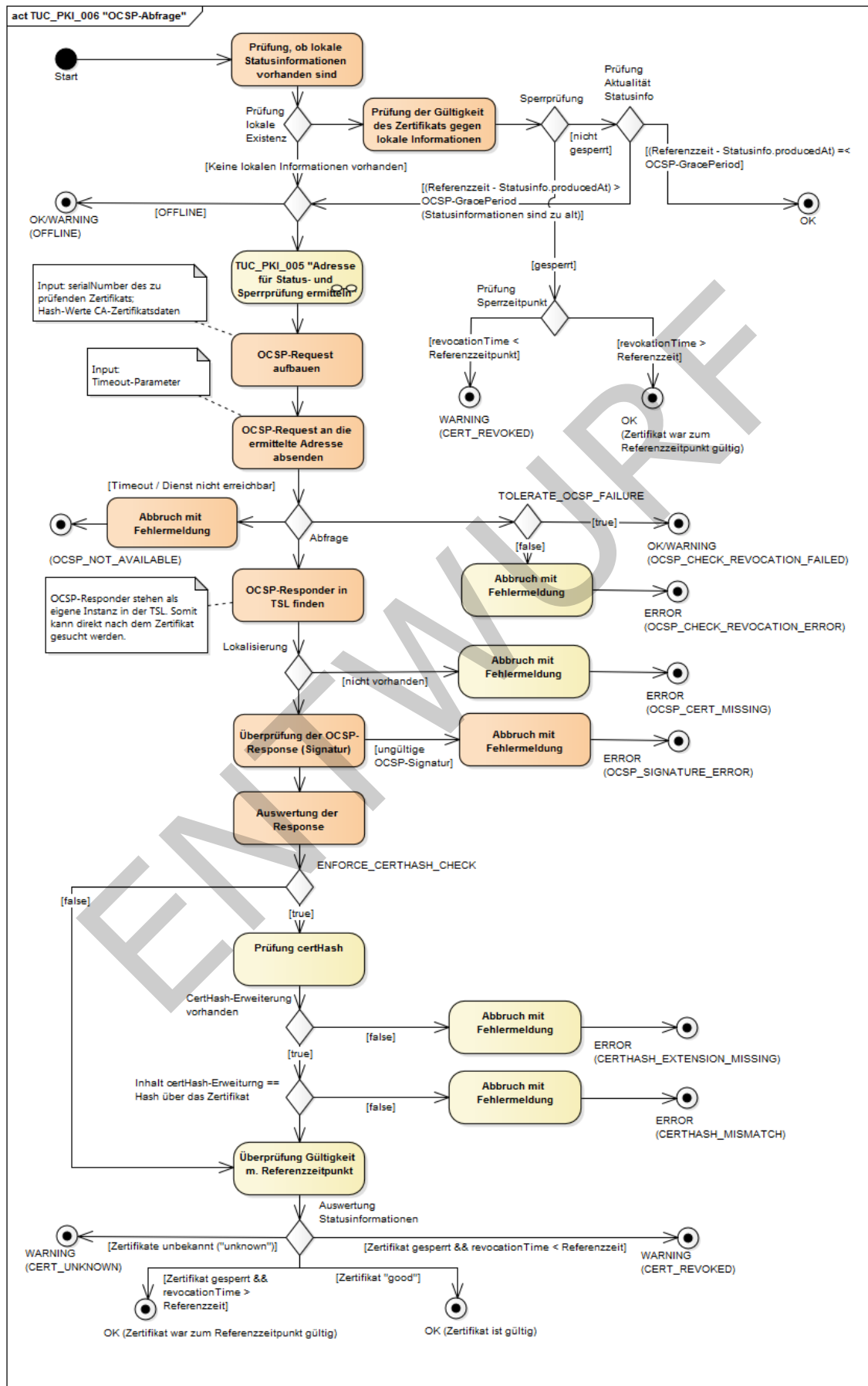


Abbildung 19: Aktivitätsdiagramm TUC_PKI_006 „OCSP-Abfrage“

8.3.2.3 TUC_PKI_021 „CRL-Prüfung“

GS-A_4900-01GS-A_4900 - TUC_PKI_021 "CRL-Prüfung"

Der Konnektor MUSS den TUC_PKI_021 zur Prüfung der Widerrufsinformationen (Statusprüfung) mittels Zertifikatssperrliste (CRL) umsetzen.



Tabelle 93: TUC_PKI_021 „CRL-Prüfung“

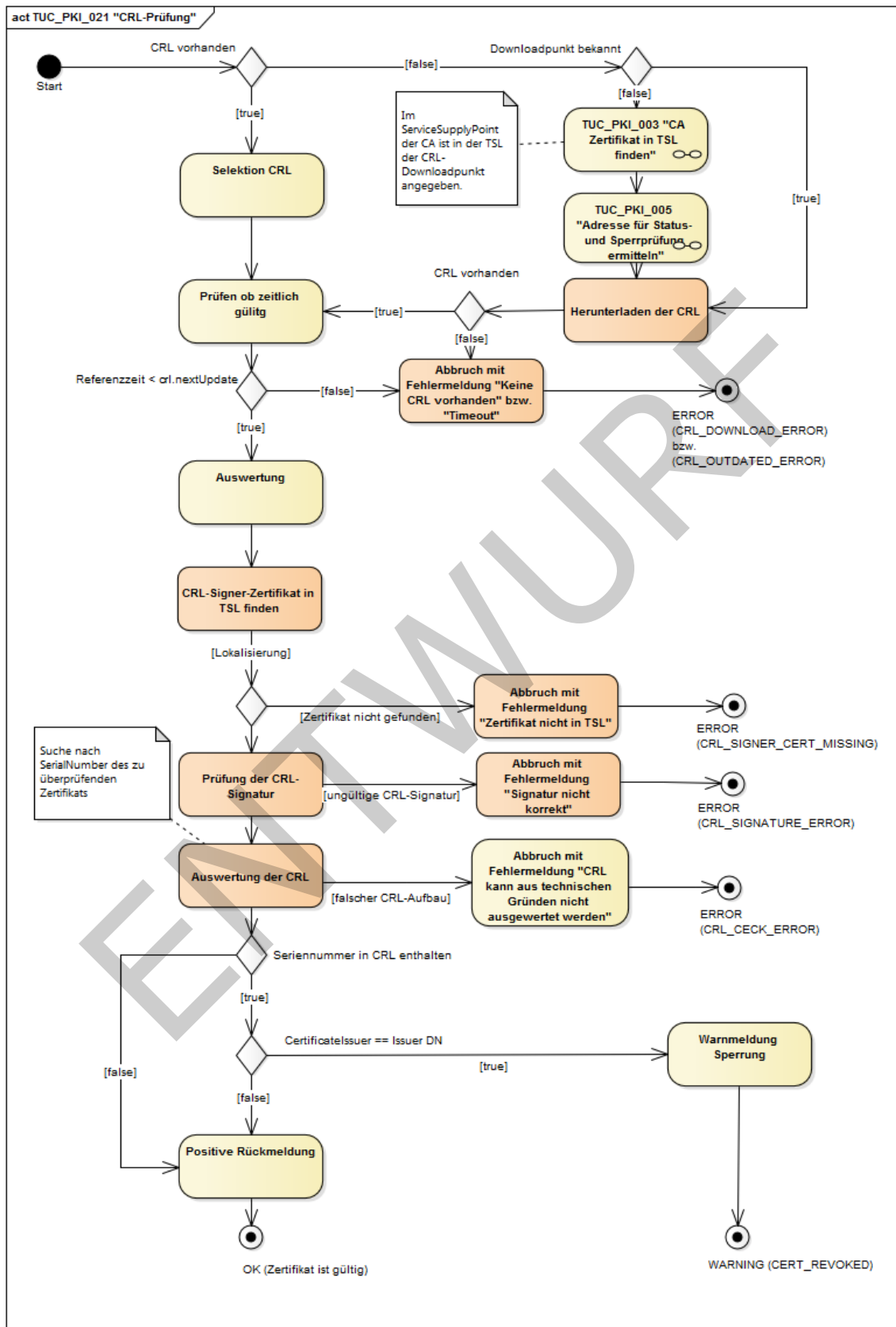
Element	Beschreibung
Name	TUC_PKI_021 „CRL-Prüfung“
Beschreibung	Dieser Use Case beschreibt den Prozess zur Validierung einer CRL (Certificate Revocation List) sowie den Prozess zur Ermittlung der Sperrinformationen zu einem End-Entity-Zertifikat mittels einer CRL. Die Festlegungen aus [RFC5280], [X.509] und den spezifischen Eigenschaften der TI sind verbindlich.
Anwendungsumfeld	Use Case für den Anwendungsfall zur Prüfung der Sperrinformationen eines End-Entity-Zertifikats.
Vorbedingungen	Ein End-Entity-Zertifikat (mathematisch und zeitlich gültig) Eine CRL ist vorhanden oder kann heruntergeladen werden.
Auslöser	TUC_PKI_018 "Zertifikatsprüfung in der TI "
Eingangsdaten	CRL End-Entity-Zertifikatsdaten (Zertifikats-Seriennummer, CertificateIssuer) Timeout-Parameter (alternativ zu CRL) CRL-Downloadpunkt-Adresse (optional, alternativ zu CRL)
Komponenten	System (nur Konnektor)
Ausgangsdaten	Status der Prüfung
Referenzen	[COMMON-PKI#Part1#4], [COMMON-PKI#Part5#2.3], [RFC5280#5.2.5.], [RFC5280#5.3.3.][RFC5280] [X.509]

Standardablauf	<ol style="list-style-type: none">1. [System:] Selektion der CRL2. [System:] Prüfen der zeitlichen Gültigkeit der CRL (Systemzeit < <code>crl.NextUpdate</code>)), s. [RFC5280] Kap. 5.1.2.5.3. [System:] Auswertung der Art der CRL. Es wird anhand der IssuingDistributionPoint-Erweiterung in der Sperrliste (CRL) geprüft, ob es sich um eine indirekte CRL handelt (<code>indirectCRL-bit</code>), s. [RFC5280] Kap. 5.2.5, [X.509] Kap. 7.12..4. [System:] Das zugehörige CRL-Signer-Zertifikat wird in den TSL-Informationen ermittelt. In der TSL-Datei ist der CRL-Signer mit „<code>http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL</code>“ im Element <code>ServiceTypeIdentifier</code> gekennzeichnet, s. [ETSI_TS_102_231_V3.1.2] D.2 ETSI Common Domain URIs.5. [System:] Prüfung der Signatur der CRL, s. [RFC5280] Kap. 6.3.3.6. [System:] Auswertung der CRL-Einträge. Es wird nach der Zertifikatsseriennummer des zu überprüfenden End-Entity-Zertifikats in der CRL gesucht, s. [RFC5280] Kap. 6.3.3.7. [System:] Falls einer oder mehrere Einträge gefunden wurden, wird die CRL-Entry-Erweiterung „<code>CertificateIssuer</code>“ ausgelesen und deren Inhalt mit dem Issuer-DistinguishedName des End-Entity-Zertifikats verglichen. Nur wenn der Inhalt der <code>CertificateIssuer</code>-Erweiterung mit diesem DistinguishedName übereinstimmt, ist das Zertifikat gesperrt, s. [RFC5280] Kap. 6.3.3.8. [System:] Rückmeldung, dass das Zertifikat nicht in der Sperrliste enthalten ist.9. [System:] Ende des Use Case
----------------	--

Varianten/Alternativen	<p>1a. Die CRL ist nicht im System vorhanden und der CRL-Downloadpunkt unbekannt.</p> <p>1a1. [System:] Ermittlung des TSL-Eintrags der CA, welche das End-Entity-Zertifikat herausgegeben hat. (TUC_PKI_003 „CA Zertifikat in TSL finden“)</p> <p>1a2. [System:] Ermittlung des CRL-Downloadpunktes aus dem „Service-SupplyPoint“ des TSL-Service Eintrags (TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln").</p> <p>1a3. [System:] Herunterladen der CRL aus der ermittelten Adresse. Der Timeout-Parameter definiert hier, zu welchem Zeitpunkt das System ein Timeout bei Nichterreichbarkeit des Dienstes meldet.</p> <p>1b. Die CRL ist nicht im System vorhanden, der CRL-Downloadpunkt ist aber schon bekannt.</p> <p>1b1. [System:] Weiter mit 1a3.</p> <p>7a. [System:] Zertifikat ist gesperrt. Rückmeldung an das System. (CERT_REVOKED)</p>
Fehlerfälle	<p>1a3a. [System:] Die CRL kann nicht heruntergeladen werden. (CRL_DOWNLOAD_ERROR)</p> <p>2a. [System:] Die Prüfung der zeitlichen Gültigkeit der CRL ergibt, dass die CRL abgelaufen ist (Systemzeit > crl.NextUpdate) (CRL_OUTDATED_ERROR)</p> <p>3 b. [System:] CRL-Signer-Zertifikat nicht in TSL-Informationen enthalten. Abbruch mit Fehlermeldung. (CRL_SIGNER_CERT_MISSING)</p> <p>4a. [System:] Signatur der CRL ist nicht gültig. (CRL_SIGNATURE_ERROR)</p> <p>5a. [System:] Die CRL ist fehlerhaft aufgebaut und kann nicht geprüft werden. (CRL_CHECK_ERROR)</p> <p>6a. [System:] Die CRL ist fehlerhaft aufgebaut und ihre Einträge können nicht ausgewertet werden. (CRL_CHECK_ERROR)</p> <p>7b. [System:] Die CRL-Einträge sind fehlerhaft aufgebaut und können nicht weiter geprüft werden. (CRL_CHECK_ERROR)</p>

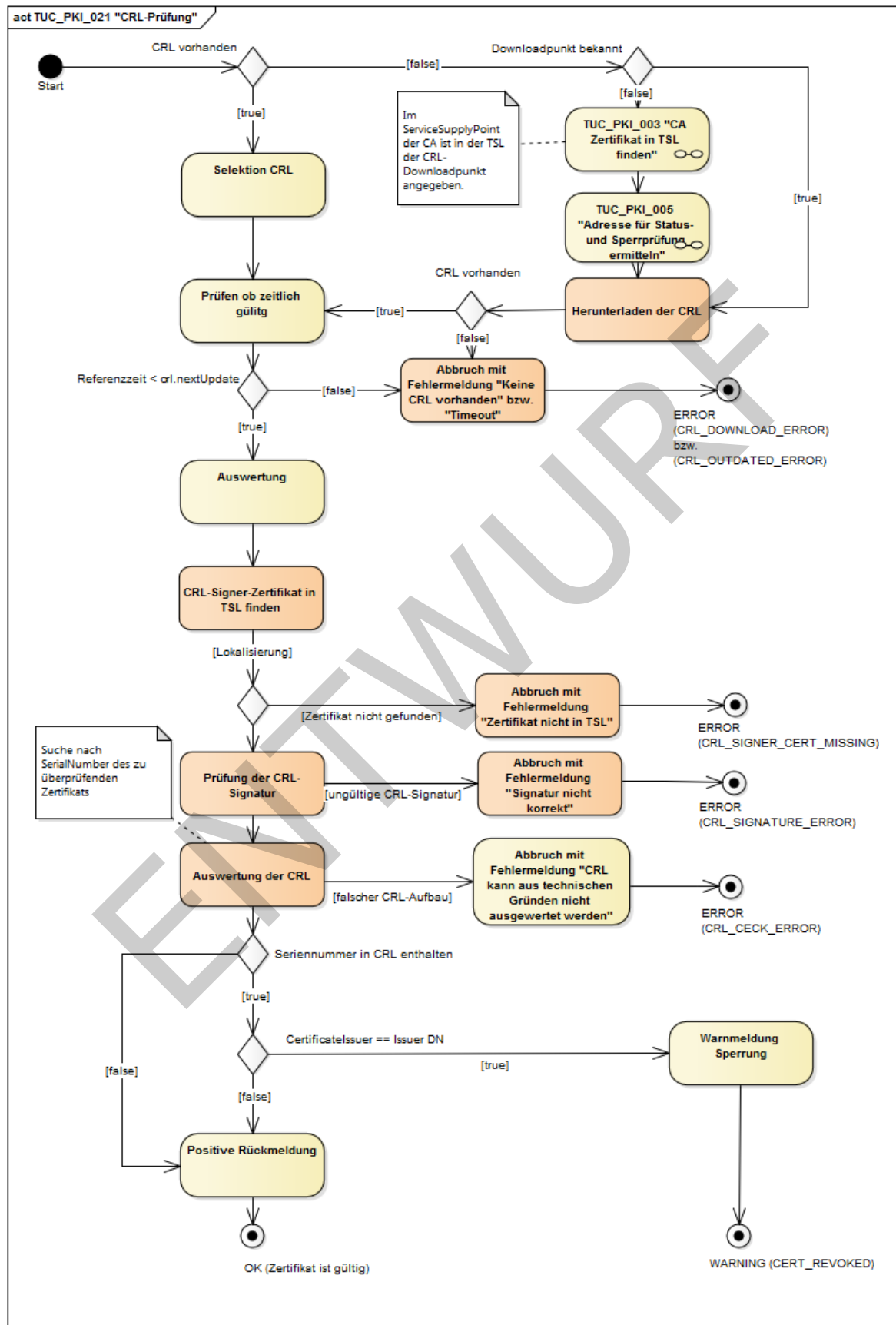
Anmerkungen, Bemerkungen	<p>Dieser TUC kommt z.B. bei der Konzentrador-Zertifikatsprüfung zur Anwendung.</p> <p>Der Downloadpunkt der CRL ist aus dem Internet erreichbar.</p> <p>Als Übertragungsprotokoll für den allfälligen Download ist „HTTP“ zu verwenden.</p> <p>Die Schritte 1-5 beinhalten die Validierung der CRL. Diese können vorgängig durchgeführt werden und müssen also nicht bei jeder einzelnen CRL-Prüfung eines End-Entity-Zertifikats durchlaufen werden, solange gewährleistet ist, dass die CRL zeitlich gültig ist.</p> <p>Die Zertifikats-Extension crlDistributionPoint wird bei der Zertifikatsprüfung von TI-Zertifikaten gemäß TUC_PKI_018/TUC_PKI_021 nicht ausgewertet (vgl. Tab_PKI_245/Tab_PKI_265).</p>
Zugehörige Diagramme	<p>Aktivitätsdiagramm TUC_PKI_021 "CRL-Prüfung".</p> <p>Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.</p>

[<=]



3598

3599



3601 **Abbildung 20: Aktivitätsdiagramm TUC_PKI_021 „CRL-Prüfung“**

3602 **8.3.2.4 Szenarien für Offline und Timeout von OCSP**

3603 Komponenten und Systeme der Gesundheitstelematik, die ihre Funktion zeitweise oder
3604 ständig ohne Online-Zugang zur TI bereitstellen müssen, können im Offline-Fall keine
3605 Statusauskünfte für Zertifikate von OCSP-Respondern aus der TI erhalten und müssen
3606 somit die Zertifikatsprüfung auf die mathematische Prüfung gegen das Aussteller-CA-
3607 Zertifikat aus der lokal vorliegenden TSL beschränken.

3608 **GS-A_4658 - Zertifikatsprüfung in spezifizierten Offline-Szenarien**

3609 Die Produkttypen der TI, die Zertifikate prüfen und per Spezifikation ihre Funktionen
3610 zeitweise oder ständig offline von der TI erbringen, MÜSSEN für die explizit spezifizierten
3611 Offline-Szenarien bei der Zertifikatsprüfung die TUCs *TUC_PKI_005 OCSP-Adresse*
3612 *ermitteln* und *TUC_PKI_006 OCSP-Abfrage* auslassen.
3613 [**<=**]

3614 **8.3.2.5 Statusprüfung von eGK-Zertifikaten**

3615 Bei eGK-Zertifikaten ist es nicht ausgeschlossen, dass diese suspendiert, also nur
3616 vorübergehend gesperrt werden. Die OCSP-Statusinformationen für eGK-Zertifikate
3617 müssen deshalb in jedem Fall aktuell sein. (Bei Zertifikaten, die dauerhaft gesperrt
3618 werden, können sich Applikation hingegen auf OCSP-Responses, die den Status
3619 „revoked“ enthalten, verlassen, auch wenn diese älter sind. Vgl. *TUC_PKI_006 „OCSP-*
3620 *Abfrage*“)

3621 **GS-A_4943 - Alter der OCSP-Responses für eGK-Zertifikate**

3622 Die Produkttypen der TI, die Zertifikate der elektronischen Gesundheitskarte (eGK)
3623 prüfen, DÜRFEN NICHT OCSP-Responses für die Statusprüfung verwenden, deren Alter
3624 die OCSP-Graceperiod (maximale Caching-Dauer) übersteigt. Dies beinhaltet auch OCSP-
3625 Responses, die den Status „revoked“ enthalten.
3626 [**<=**]

3627 **8.3.3 Ermittlung von Autorisierungsinformationen**

3628 **8.3.3.1 Bestätigte Zertifikatsinformationen**

3629 Das vorliegende Kapitel beschreibt die Ermittlung der folgenden Informationen aus einem
3630 X.509-Zertifikat der Telematikinfrastruktur. Dabei geht es um:

- 3631
 - Zertifikatstypen
- 3632
 - Die Rolle der Zertifikatsidentität

3633 Die in diesem Kapitel beschriebenen Use Cases können durch weitere gematik
3634 Dokumente referenziert werden.

3635 **8.3.3.2 TUC_PKI_009 „Rollenermittlung“**

3636 **GS-A_4660-01GS-A_4660 - TUC_PKI_009: Rollenermittlung**

3637 Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN *TUC_PKI_009* zur Ermittlung der
3638 Rolle der Identität umsetzen.
3639 [**<=**]

3640

3641

3642 **Tabelle 94: TUC_PKI_009 „Rollenermittlung“**

Element	Beschreibung
Name	TUC_PKI_009 „Rollenermittlung“
Beschreibung	Die Rolle einer Identität steht im jeweiligen Zertifikat. Dieser Use Case beschreibt die Ermittlung dieser Rolle aus dem Zertifikat. Jede Rolle wird in der Struktur <code>professionInfo</code> als OID gespeichert (siehe Kap 4.4, 4.5, 4.6). In allen Zertifikaten, die eine Rolle besitzen, steht diese in der Extension Admission, aus welcher der OID ausgelesen wird.
Anwendungsumfeld	System, das spezifische Inhalte von Zertifikaten verwendet
Vorbedingungen	Gültiges End-Entity-Zertifikat
Auslöser	Zertifikatsprüfung in der TI, TUC_PKI_018 "Zertifikatsprüfung in der TI ", TUC_PKI_030 "QES-Zertifikatsprüfung"
Eingangsdaten	End-Entity-Zertifikatsdaten
Komponenten	System
Ausgangsdaten	OID der Rolle
Referenzen	[Common-PKI#Part1#3.1]
Standardablauf	<ol style="list-style-type: none"> 1. [System:] Prozess zur Ermittlung der Rolle beginnt 2. [System:] Extension Admission aus dem Zertifikat auslesen. 3. [System] Admission ist vorhanden und die Rolle aus dem Feld <code>professionOIDs</code> ermittelt. Sind weitere Einträge <code>professionInfo</code> enthalten, wird dieser Schritt so oft durchlaufen, bis alle <code>professionOIDs</code> ermittelt sind. 4. [System:] Mindestens eine OID ist vorhanden und wird zurück geliefert. Bei mehreren OID wird die Liste der OID als

	Rückgabewert geliefert. Ende des Use Case mit vorhandener Rolle
Varianten/Alternativen	<p>3a. [System:] Extension Admission ist nicht vorhanden.</p> <p>3a1. [System:] Meldung des Systems, dass keine Rolle vorhanden ist.</p> <p>3a2. [System:] Ende des Use Case ohne Rolle</p> <p>4a. [System:] OID nicht vorhanden</p> <p>4a1. [System:] Meldung des Systems, dass keine Rolle vorhanden ist.</p> <p>4a2. [System:] Ende des Use Case ohne Rolle</p>
Fehlerfälle	Es werden keine spezifischen Fehlerfälle beschrieben.
Anmerkungen	<p>Die Rolle in der Extension Admission befindet sich im Feld professionOIDs und ist als OID abgelegt. Die genaue Festlegung der OID wird im Dokument [gemSpec_OID] spezifiziert.</p> <p>Syntax der Extension Admission siehe [Common-PKI#Part1#3.1]IT-spezifische Festlegungen, insbesondere Tab_PKI_226-01.</p> <p>Die Auswertung der Rolle und wie im Fehlerfall zu verfahren ist, wird in der jeweiligen Produktspezifikation beschrieben.</p>
Zugehörige Diagramme	<p>Aktivitätsdiagramm TUC_PKI_009 „Rollenermittlung“.</p> <p>Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.</p>

[<=]

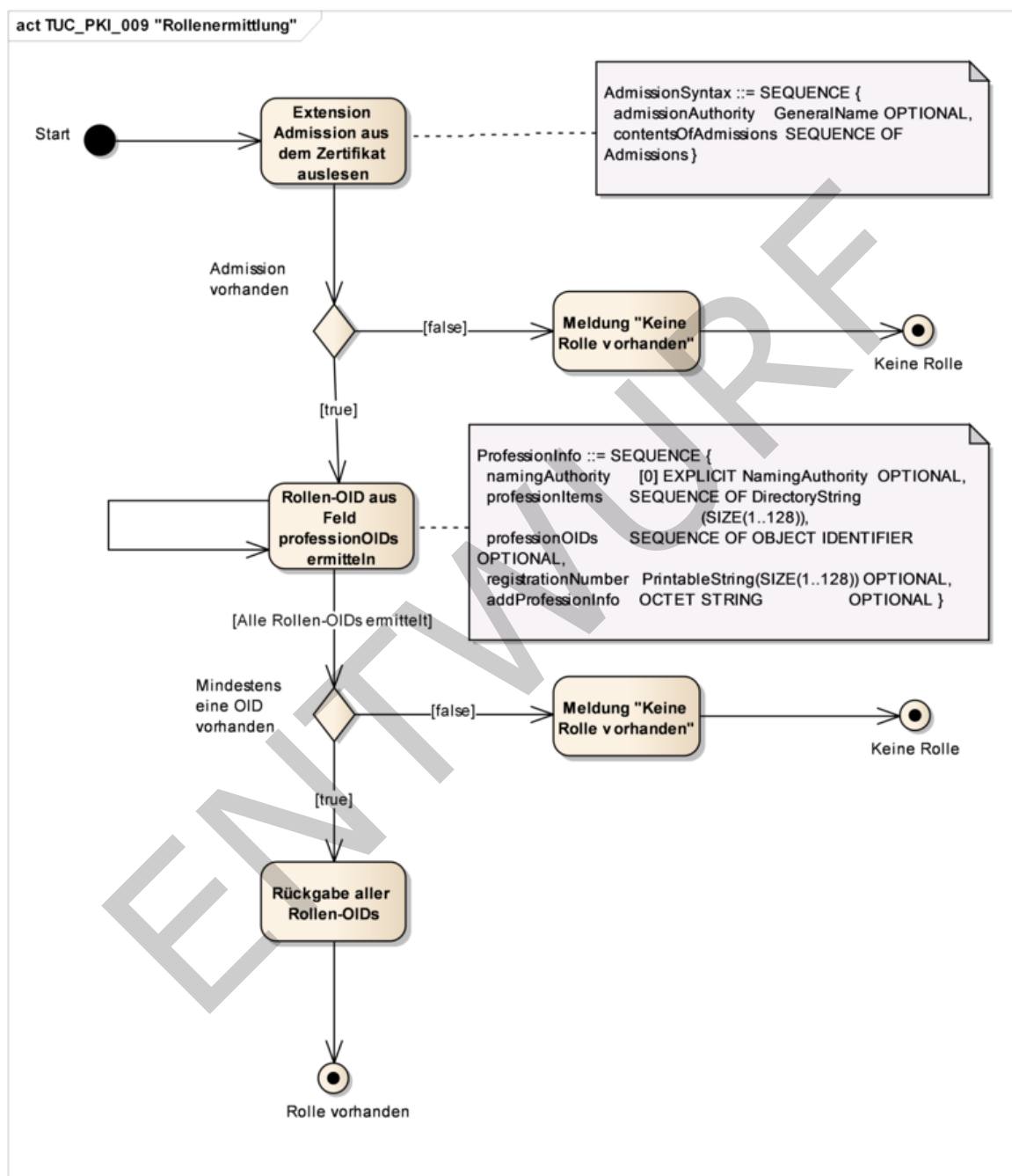


Abbildung 21: Aktivitätsdiagramm TUC_PKI_009 „Rollenermittlung“

8.3.3.3 TUC_PKI_007 „Prüfung Zertifikatstyp“

~~GS-A_4749-01GS-A_4749~~ - TUC_PKI_007: Prüfung Zertifikatstyp

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_007 zur Prüfung des Zertifikatstyps umsetzen.

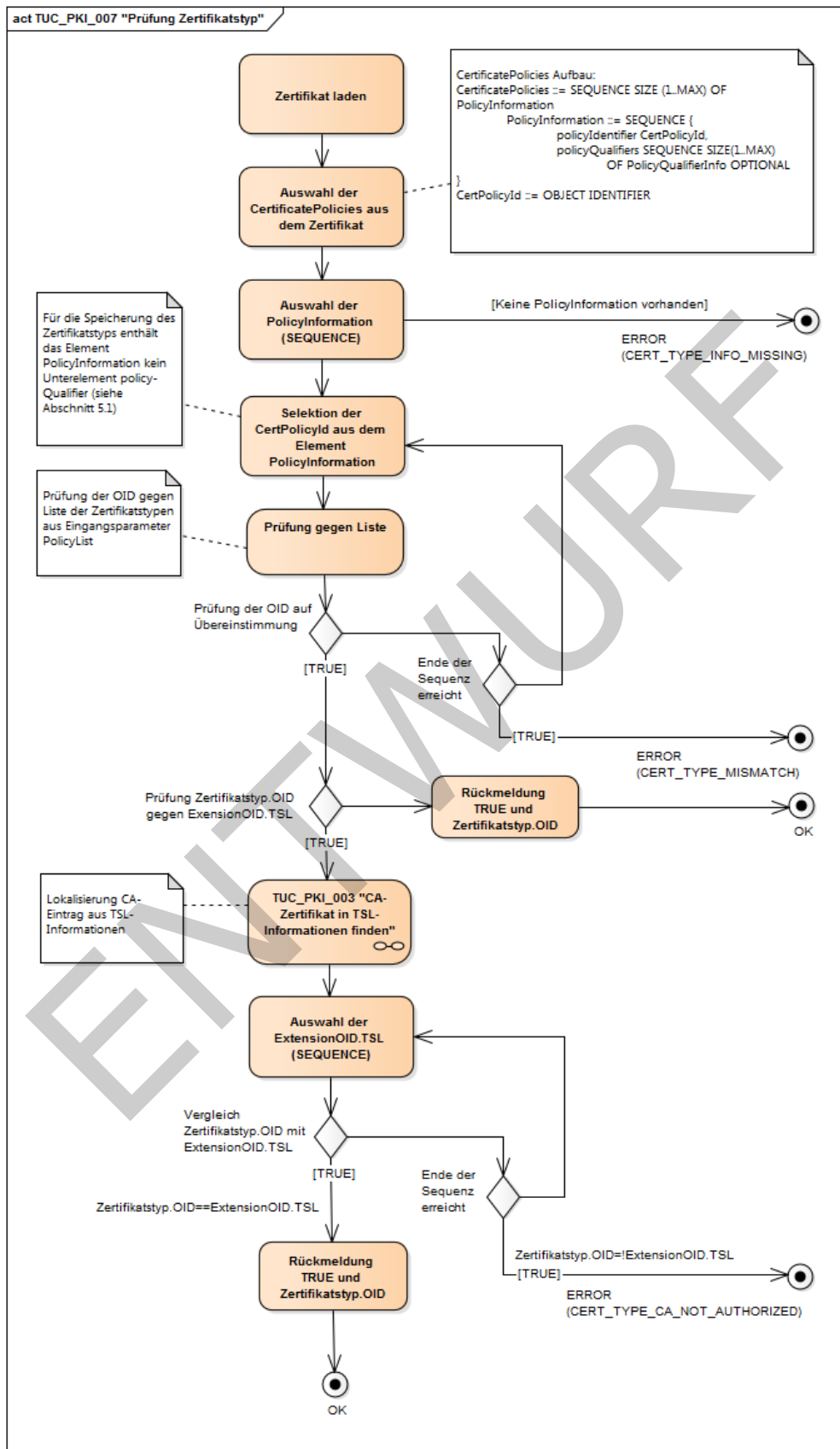
~~[<=]~~

Tabelle 95+ : TUC_PKI_007 „Prüfung Zertifikatstyp“

Element	Beschreibung
Name	TUC_PKI_007 „Prüfung Zertifikatstyp“
Beschreibung	In diesem Use Case wird der Soll-/Ist-Vergleich des Zertifikatstyps im Zuge einer Zertifikatsprüfung beschrieben. Verglichen wird die im Zertifikat hinterlegte Zertifikatstyp-OID (abgelegt in einem Element PolicyIdentifier der X.509-Extension CertificatePolicies) mit der als Eingangsparameter dieses TUC übergebenen Liste der erwarteten Zertifikatstyp-OIDs. Zusätzlich wird die Zertifikatstyp-OID aus dem Zertifikat jeweils mit den in der TSL (TSL-Extension "ServiceInformationExtensions") enthaltenen ExtensionOIDs der CA verglichen, die das Zertifikat ausgestellt hat.
Anwendungsumfeld	System, das spezifische Inhalte von Zertifikaten verwendet
Vorbedingungen	Gültiges End-Entity-Zertifikat Aktuelle TSL-Informationen im System.
Auslöser	TUC_PKI_018 "Zertifikatsprüfung in der TI "
Eingangsdaten	<ul style="list-style-type: none"> Das zu prüfende Zertifikat PolicyList
Komponenten	System
Ausgangsdaten	<ul style="list-style-type: none"> Status der Prüfung OID des Zertifikatstyps
Referenzen	<p>[RFC5280], [Common-PKI#2.2]</p> <p>Für weitere Erläuterungen zum Parameter „PolicyList“ siehe [Common-PKI#Part5], Kapitel 2.2 Validating the Certificate Path.</p> <p>In der TSL werden OIDs für Zertifikatstypen benutzt, um anzuzeigen, welche Typen von Zertifikaten unter einer CA ausgestellt werden dürfen. Diese OIDs werden jeweils im</p>

	Element „ServiceInformationExtensions“ eingefügt, s. [gemSpec_TSL#7.3.2.1]-[RFC5280], [gemSpec_TSL]
Standardablauf	<ol style="list-style-type: none"> 1. [System:] Start des Prozesses zur Ermittlung des Zertifikatstyps. 2. [System:] Zertifikat laden 3. [System:] Auswahl der CertificatePolicies aus dem Zertifikat 4. [System:] Auswahl des Elements PolicyInformation. Es können mehrere Elemente vorkommen, da es eine SEQUENCE ist. In jedem Schritt wird ein Element aus der SEQUENCE entnommen. 5. [System:] Selektion der CertPolicyId aus dem Element PolicyInformation 6. [System:] Prüfung der Zertifikatstyp-OID (nicht jedoch der Policy-OID) aus dem Zertifikat gegen Liste der Zertifikatstyp-OIDs aus dem Parameter PolicyList der Eingangsdaten. 7. [System:] Die Zertifikatstyp-OID ist in PolicyList enthalten. Aus den TSL-Informationen wird der TSL-Eintrag der passenden CA ermittelt, welche das Zertifikat herausgegeben hat. (TUC_PKI_003 "CA Zertifikat in TSL finden"), s. [gemSpec_TSL#7.3.2.1]. 8. [System:] Prüfung der Zertifikatstyp-OID aus dem Zertifikat gegen die im TSL-Eintrag in der TSL-Extension "ServiceInformationExtensions" enthaltenen OIDs. 9. [System:] Die Zertifikatstyp-OID stimmt mit einer ExtensionOID überein. Ende des Use Case mit der Rückgabe der Zertifikatstyp-OID. Mit dem ersten OID-Match wird der Use Case beendet und die gesamte Prüfung als erfolgreich gewertet.
Varianten/Alternativen	<ol style="list-style-type: none"> 6a. [System:] Keine Übereinstimmung, nächstes Element PolicyInformation des Zertifikates wird analysiert. Wiederholung des Vorgangs ab Schritt 4. 7a. Wird die Prüfung der ExtensionOID ausgelassen, endet der Use Case mit der Rückmeldung „Prüfung Zertifikatstyp erfolgreich“ und der Rückgabe der OID des Zertifikatstyps.

Fehlerfälle/Warnungen	<p>4a. [System:] Abbruch und Rückmeldung. Kein Element PolicyIdentifier vorhanden. (CERT_TYPE_INFO_MISSING)</p> <p>7. [System:] Abbruch und Fehlermeldung. Ende der SEQUENCE ist erreicht und es wurde keine Übereinstimmung festgestellt. (CERT_TYPE_MISMATCH)</p> <p>9a. [System:] Es wurde keine Übereinstimmung mit den ExtensionOIDs im Element ServiceInformationExtensions festgestellt. Abbruch mit der Fehlermeldung CERT_TYPE_CA_NOT_AUTHORIZED.</p>
Anmerkungen	<p>Zusätzlich zu [RFC5280] Kap. 4.2.1.4 ist der Aufbau der Extension CertificatePolicies ist in Kapitel 4.8.3.3 TI-spezifisch (Zertifikatstyp-OID) beschrieben. Für die Speicherung des Zertifikatstyps enthält das Element PolicyInformation kein Unterelement policy-Qualifier. Das TSL-Element ServiceInformationExtensions wird detailliert in [gemSpec_TSL#7.3.2.1] beschrieben.</p>
Zugehörige Diagramme	<p>Aktivitätsdiagramm TUC_PKI_007 "Prüfung Zertifikatstyp". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.</p>



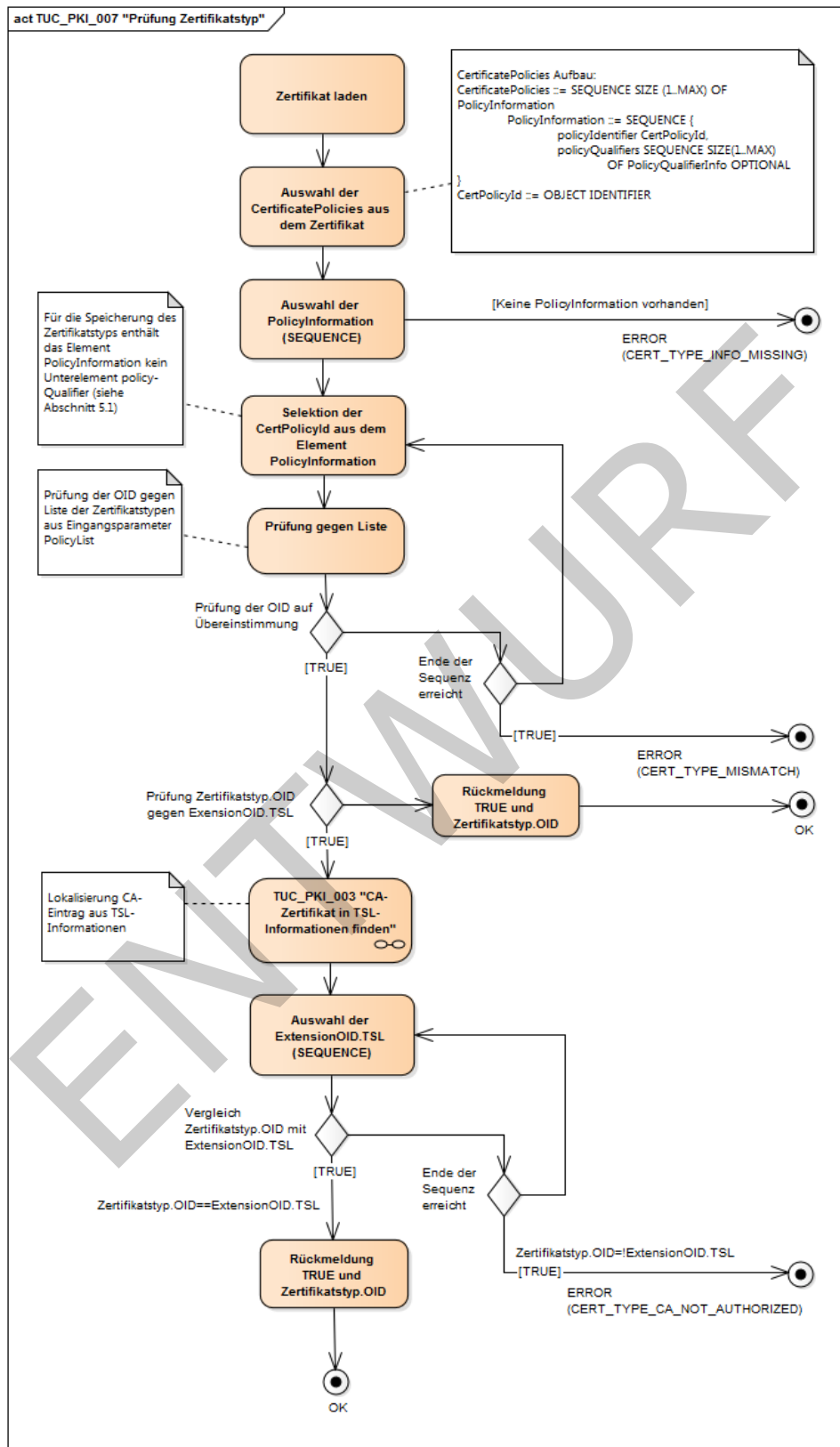


Abbildung 22+ : Aktivitätsdiagramm TUC_PKI_007 „Prüfung Zertifikatstyp“

[<=]

8.3.4 Weitere Prüfungen

8.3.4.1 Umgang mit kritischen Extensions

GS-A_4661-01GS-A_4661 - kritische Erweiterungen in Zertifikaten

Zertifikatsprüfenden Komponenten MÜSSEN kritische Zertifikatserweiterungen gemäß [RFC5280] und [Common-PKI] Kapitel 4.2 verarbeiten.
[<=]

8.4 Überprüfung der Zertifikate auf Netzwerk- und Transportebene

8.4.1 TLS-Verbindungsaufbau

GS-A_4662 - Bedingungen für TLS-Handshake

Produkttypen der TI, die TLS nutzen, MÜSSEN sicherstellen, dass TLS-Applikationsdaten (d. h. TLS-Nutzdaten, wie z. B. die Protokollschicht HTTP, LDAP, SMTP, IMAP oder POP3) nur ausgetauscht werden, wenn im Falle von einseitiger Authentisierung das Serverzertifikat aktuell gültig ist oder im Falle von gegenseitiger Authentisierung beide Zertifikate aktuell gültig sind und zusätzlich in beiden Fällen der TLS-Handshake erfolgreich absolviert wurde.
[<=]

GS-A_4663 - Zertifikats-Prüfparameter für den TLS-Handshake

Produkttypen der TI, die TLS nutzen, MÜSSEN sicherstellen, dass für den TLS-Verbindungsaufbau die in Tab_PKI_273 beschriebene Nutzung der Eingangsdaten-Parameter von TUC_PKI_018 „Zertifikatsprüfung“ für diese Zertifikatsprüfungen verwendet werden.
[<=]

Tabelle 96: Tab_PKI_273 Prüfparameter für TLS-Aufbau

TUC_PKI_018 Eingangsdaten	Beschreibung
Zertifikat	das zu prüfende Zertifikat vom Kommunikationspartner
Referenzzeitpunkt	Aktuelle Systemzeit
Prüfmodus	OCSP
PolicyList	Für den Verwendungszweck TLS zulässige Zertifikatstyp-OID gemäß [gemSpec_OID#Tab_PKI_405]
Vorgesehene KeyUsage	Der Wert MUSS konfigurierbar sein. Die zu konfigurierenden Werte sind in den Zertifikatsprofilen der TLS-nutzenden Komponenten enthalten.

Vorgesehene ExtendedKeyUsage	Der Wert MUSS konfigurierbar sein. Die zu konfigurierenden Werte sind in den Zertifikatsprofilen der TLS-nutzenden Komponenten enthalten.
OCSP-Graceperiod	Der Wert muss konfigurierbar sein.
Offline-Modus	Nein, mit Ausnahme der Komponenten und Dienste, bei denen ein Offline-Modus explizit spezifiziert ist.

3689

3690 **GS-A_5077 - FQDN-Prüfung beim TLS-Handshake**

3691 Produkttypen der TI, die beim TLS-Handshake das TLS-Serverzertifikat prüfen, MÜSSEN
3692 sicherstellen, dass für den Verbindungsaufbau der FQDN im Zertifikat C.ZD.TLS-S bzw.
3693 C.FD.TLS-S mit dem der Komponente zugeordneten FQDN übereinstimmt.

3694 [\leq]

3695 **8.4.2 IPsec-Verbindungsaufbau**

3696 **GS-A_5078 - FQDN-Prüfung beim IPsec-Aufbau**

3697 Produkttypen der TI die beim Aufbau einer IPsec-Verbindung das IPsec-Serverzertifikat
3698 prüfen, MÜSSEN sicherstellen, dass der FQDN im Zertifikatattribut *SubjectDN* oder in der
3699 Erweiterung *SubjectAltNames* des Zertifikats C.VPNK.VPN bzw. C.VPNK.VPN-SIS mit dem
3700 der Komponente zugeordneten FQDN übereinstimmt.

3701
3702 [\leq]

3703 **8.5 Zertifikatsprüfung X.509 QES**

3704 Im Folgenden werden die notwendigen Voraussetzungen zur Prüfung von QES-
3705 Zertifikaten dargestellt:

- 3706 1. Die Zertifikatsüberprüfende Komponente muss die Gültigkeit des Zertifikats in
3707 Bezug auf den Signaturerstellungszeitpunkt und dem zu Grunde liegenden
3708 Gültigkeitsmodell überprüfen.
- 3709 2. Die Zertifikatsüberprüfende Komponente muss den Zertifikatsstatus mit dem vom
3710 jeweiligen TSP zur Verfügung gestellten Statusprüfdienst überprüfen.
- 3711 3. Die Zertifikatsüberprüfende Komponente muss auf die Anwendungsbereiche des
3712 Zertifikats und die damit verbundenen Einschränkungen achten.
- 3713 4. Das Schlüsselpaar QES ist ausschließlich für die qualifizierte elektronische
3714 Signatur nach [eIDAS] im Sinne der „Nicht-Abstreitbarkeit“ („nonrepudiation“
3715 bzw. „content commitment“) einzusetzen. Die Schlüsselpaare und Zertifikate
3716 dürfen nur für ihren jeweiligen Anwendungsbereich benutzt werden. Eine
3717 Benutzung außerhalb des zugehörigen Anwendungsbereichs ist nicht zulässig.
- 3718 5. Die Zertifikatsüberprüfende Komponente muss das QES-Zertifikat auf
3719 Vorhandensein der Extension QCStatement und einen darin enthaltenen Wert für
3720 QES-Konformität prüfen.
- 3721 6. Der Überprüfer hat die Sorgfaltspflicht, seine IT-Infrastruktur zu schützen und
3722 muss etwaige Nutzungsbeschränkungen im Zertifikat berücksichtigen.

7. Die zertifikatsprüfende Komponente muss den Qualifikationsstatus des VDA anhand der von der Bundesnetzagentur bereitgestellten Vertrauensliste (BNetzA-VL) überprüfen.

Die folgenden Use Cases verdeutlichen die Aktionen des Systems.

Für die QES-Zertifikatsprüfung sind nur der TUC_PKI_030 "QES-Zertifikatsprüfung" und der TUC_PKI_036 „BNetzA-VL Aktualisierung“ für andere gematik Dokumente referenzierbar.

8.5.1 TUC_PKI_030 „QES-Zertifikatsprüfung“

~~GS-A_4750-01GS-A_4750~~ - TUC_PKI_030 „QES-Zertifikatsprüfung“

Alle Produkttypen, die QES-Zertifikate prüfen, MÜSSEN TUC_PKI_030 zur Prüfung der QES-Zertifikate umsetzen.

~~{<=>}~~

~~8.5.11.1.1 TUC_PKI_030 „QES-Zertifikatsprüfung“~~

Tabelle 97: TUC_PKI_030 „QES-Zertifikatsprüfung“

Element	Beschreibung
Name	TUC_PKI_030 „QES-Zertifikatsprüfung“
Beschreibung	In diesem Use Case wird die Prüfung von Zertifikaten mit qualifizierter Signatur beschrieben. Die Prüfung von QES-Zertifikaten setzt sich aus und die Sperrprüfung per OCSP entsprechen den in [Common-PKI#Part5] und [Common-PKI#9] beschriebenen Schritten zusammen, sofern sie den gesetzlichen Vorgaben von [eIDAS] nicht widersprechen und relevanten Standards. Die zugrundeliegende Prüfung des Zertifikatspfads (Validation Certificate Path) basiert auf dem Kettenmodell (chain model), siehe Anmerkung [1]. Zusätzlich werden folgende Schritte in diesem Technical Use Case (TUC) durchgeführt.
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	aktuelle TSL-Informationen im Truststore (inkl. OCSP-Adressen in der TI für die zugelassenen VDAs), eine aktuell gültige BNetzA-VL.
Auslöser	Zertifikats-Check
Eingangsdaten	<ul style="list-style-type: none"> QES-Zertifikat Referenzzeitpunkt (refTimeoptional; bei Nichtangabe Verwendung der aktuellen

	<p>Systemzeit): Zeitpunkt, für den das Zertifikat geprüft werden soll, Details siehe Anmerkung [2]</p> <ul style="list-style-type: none"> • Offline-Modus (ja/nein) • Beigefügte OCSP-Response, die zur Prüfung des angefragten QES-Zertifikates erforderlich ist (optional; z. B. in Signatur eingebettet) • Nonce (optional; Wert ausschließlich zur Verwendung bei der OCSP-Prüfung des zu prüfenden QES-Zertifikates) • Timeout-Parameter für OCSP-Abfragen (Default: 10s)
Komponenten	System
Ausgangsdaten	<ul style="list-style-type: none"> • Status der Prüfung • OCSP-Response zum angefragten QES-Zertifikat • im Zertifikat enthaltene Rollen-OIDs • im Zertifikat enthaltene QCStatements-Einträge
Referenzen	<p>[eIDAS], [VDG] [ETSI TS 119 612], [ETSI EN 319 412-5], [ETSI EN 319 412-2], [ETSI EN 319 102-1], [ETSI TS 119 172-4] [RFC5280], [RFC6960], [RFC5019]</p>
Standardablauf	<ol style="list-style-type: none"> 1. [System] Auslesen und Ausgabe aller gesetzten Elemente der Extension QCStatements des Zertifikates- 2, Details siehe Anmerkung [3]. 2. [System:] Prüfung der (zeitlichen) Gültigkeit des Zertifikats mittels TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats", Details siehe Anmerkung [4]. 3. [System] Prüfung der Extension KeyUsage auf Vorhandensein und die richtige Belegung entsprechend [ETSI EN 319 412-2], Details siehe Anmerkung [5]. 4. [System] Anhand der End-Entity-Zertifikate wird die BNetzA-VL durchsucht, um das passende QES-CA-Zertifikat zu finden. Hinweis: Das Verfahren zum Finden des QES-CA-Zertifikates in BNetzA-VL verläuft analog zum Finden des nonQES-CA-Zertifikates in der TSL mittels

~~TUC_PKI_003-~~

35.

[System:] Prüfung, ob das ausstellende QES-CA-Zertifikat für die QES-Prüfung zum Referenzzeitpunkt in der BNetzA-VL gemäß [eIDAS] und [ETSI TS 119 612#5.5.4 und #Annex J] qualifiziert und als gültig gekennzeichnet ist.

~~Hinweis: Für gültige Status, Details siehe Anmerkungszu diesem TUC.~~
4Anmerkung [7].

6.

[System] Prüfung der mathematischen Signaturkorrektheit des Signaturzertifikats zum übergebenen Referenzzeitpunkt gegen das CA-Zertifikat aus Schritt 5 nach dem Kettenmodell, Details siehe Anmerkungen [1], [9].

7.

[System:] Ermittlung der OCSP-Adresse aus dem AIA-Feld des QES-EE-Zertifikates. Dabei handelt es sich um eine öffentlich aufrufbare URL im Internet. Wird für die ermittelte OCSP-URL in der TSL derselbe Wert im InformationValue-Element von AdditionalServiceInformation von BNetzA-VL-Service (mit ServiceTypeIdentifier <http://uri.telematik.TrstSvc/Svctype/TrustedList/schemerules/DE>) gefunden, so wird die dahinter folgende (nach Leerzeichen) URL als Adresse für die OCSP-Anfrage verwendet. Andernfalls wird die zuvor ermittelte OCSP-Adresse aus dem AIA-Feld für die OCSP-Anfrage verwendet.

~~Hinweis: Details zu den TSL-Einträgen für URLs für OCSP-Responder in der TI unter gemSpec_TSL# TIP1-A-7219~~

5siehe Anmerkung [10].

8.

[System:] Die abzufragenden Statusinformationen zu QES-Zertifikaten werden [per OCSP-Requests](#) unter Verwendung der aus der TSL ermittelten OCSP-Adresse [aus Schritt 7](#) eingeholt.

~~Hinweis:~~ 9. Prüfung der OCSP-Response auf Integrität

[System, OCSP-Responder:] Das dazu benötigte OCSP-Responder-Zertifikat (OCSP-Signer-Zertifikat) wird aus dem URI (markiert mit dem ServiceTypeIdentifier

<http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP> oder

<http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC>) in der BNetzA-VL ermittelt. Die Signatur der OCSP-Response wird zum Referenzzeitpunkt mittels des ermittelten OCSP-Signer-Zertifikats geprüft. Falls keiner der URIs vorhanden ist, wird weiter mit Schritt 10 verfahren, siehe Anmerkung [12].

	<p>10. [System, OCSP-Responder:] Das OCSP-Signer-Zertifikat aus dem Feld „certs“ in der OCSP-Response ermitteln. Die Signatur des OCSP-Signer-Zertifikats wird entsprechend mittels des im Schritt 6 validierten QES-CA-Zertifikats geprüft. Die Signatur der OCSP-Response wird anschließend mittels des ermittelten OCSP-Signer-Zertifikats geprüft, siehe Anmerkungen [12].</p> <p>11. [System] Auswertung der OCSP-Response. Dies umfasst die Prüfung gemäß Standards (Details zur OCSP-Statusprüfung siehe Anmerkungszeile zu diesem TUC 6siehe Anmerkung [11])</p> <ul style="list-style-type: none"> • Statuscode („OCSPResponseStatus“) auf Belegung mit „0“ (für „successful“), • Zertifikatsidentifizierungs-Informationen („CertID“) auf Identität mit derjenigen aus dem Request und • Konformität/Plausibilität der Zeitangaben („producedAt“, „thisUpdate“ und (sofern vorhanden) „nextUpdate“). <p>12. [System] Überprüfung der Gültigkeit der Statusinformation anhand des übergebenen Referenzzeitpunkts. Der certStatus „good“ wird gemeldet. Rückmeldung „Das Zertifikat ist gültig“ und Rückgabe der OCSP-Response.</p> <p>13. [System:] Ermittlung der Rolle (TUC_PKI_009 "Rollenermittlung")</p> <p>14. [System:] Ende des Use Case mit Rückgabe des/der im Zertifikat enthaltenen Rollen-OID(s)</p>
Varianten/Alternativen	<p>Der Standardablauf stellt die üblichen Schritte dar, die durchgeführt werden müssen. Eine Trennung in zwei Prozesse oder eine Umstrukturierung, bei der alle notwendigen Schritte erfolgen, ist zulässig.</p> <p>4a7a. [System:] Der Offline-Modus ist aktiviert. Es werden keine Statusinformationen eingeholt. (Schritte 48, 9, 10, 11 und 512 entfallen.)</p> <p>5a) 8a. [System:] Wird im optionalen Parameter Nonce ein Wert übergeben, dann muss für QES-Zertifikate dieser Wert als OCSP-Parameter in den OCSP-Request integriert und im Response geprüft werden.</p> <p>5b8b.</p>

	<p>[System:] Eine OCSP-Response zu dem zu prüfenden Zertifikat wurde im Aufruf mit übergeben. Falls dieses zum Referenzzeitpunkt gültig ist, werden keine OCSP-Requests erzeugt, sondern die beigefügte OCSP-Response zur weiteren Prüfung verwendet.</p>
Fehlerfälle/Warnung	<p>In jedem der beschriebenen Schritte können Fehler auftreten. Diese sind durch das System zu melden und der Prozess muss beendet werden.</p> <p>1a. Ist die Extension QCStatements nicht auslesbar, leer oder enthält keine auslesbaren Elemente, bricht der TUC mit dem Fehler QC_STATEMENT_ERROR ab.</p> <p>3a. [System:] KeyUsage ist nicht vorhanden bzw. entspricht nicht der vorgesehenen keyUsage (WRONG_KEYUSAGE)</p> <p>5a. Ist das QES-CA-Zertifikat in der BNetzA-VL nicht vorhanden oder zum Referenzzeitpunkt nicht mit einem gültigen Status gekennzeichnet, muss der TUC mit einer Fehlermeldung CA_CERTIFICATE_NOT_QES_QUALIFIED abbrechen.</p> <p>3b-5b. [System:] QES-CA-Zertifikat des QES-Zertifikates ist in der BNetzA-VL als revoked gekennzeichnet und QES-Zertifikat ist nach Sperrzeitpunkt erstellt worden. Abbruch mit Fehlermeldung (CA_CERTIFICATE_REVOKED_IN_BNETZA-VL).</p> <p>4a 6a. [System] Die Zertifikats-Signatur ist nicht gültig. Ende des Use Case. Abbruch mit Fehlermeldung (CERTIFICATE_NOT_VALID_MATH)</p> <p>7b. [System:] Warnmeldung, dass keine Online-Statusprüfung durchgeführt wurde (NO_OCSP_CHECK).</p> <p>5e8c. [System:]. Der zuständige OCSP-Responder ist nicht erreichbar. Abbruch mit Fehlermeldung (OCSP_NOT_AVAILABLE).</p> <p>5d8d. [System:] OCSP-Responses zu dem zu prüfenden Zertifikat wurden im Aufruf mit übergeben, ergaben bei den weiteren Prüfschritten jedoch kein gültiges Ergebnis. Eine erneute Prüfung wird in diesem Fall durchgeführt, als wären keine OCSP-Responses beigefügt. In den Rückgabewerten dieses TUC wird die Warnmeldung (PROVIDED_OCSP_RESPONSE_NOT_VALID) an die aufrufende Funktion übergeben.</p> <p>5e8e. Wenn die in einer OCSP-Response zurückgelieferte</p>

	<p>Nonce nicht mit der Nonce des OCSP-Requests für ein QES-Zertifikat übereinstimmt, wird die Prüfung abgebrochen mit der Fehlermeldung OCSP_NONCE_MISMATCH.</p> <p>5f8f.</p> <p>[System:] Nach zeitlichem Ablauf der TSL-Graceperiod ist die aus der TSL zu ermittelnde OCSP-Adresse nicht mehr vertrauenswürdig. Abbruch mit Fehlermeldung (OCSP_CHECK_REVOCATION_ERROR).</p> <p>9a/10a.</p> <p>[System:] OCSP-Signer-Zertifikat nicht in der OCSP-Response enthalten. Abbruch mit Fehlermeldung. (OCSP_CERT_MISSING).</p> <p>9a1/10a1.</p> <p>[System:] Signatur der OCSP-Response ist nicht gültig. Abbruch mit Fehlermeldung (OCSP_SIGNATURE_ERROR)</p> <p>11a.</p> <p>[System:] Die Response enthält einen Statuscode („OCSPResponseStatus“), der ungleich 0 (für „successful“) ist. (Damit zeigt der OCSP-Responder eine Exception an. Beispielsweise kann der Wert für den Status auf 3 für „tryLater“ gesetzt sein.) Abbruch mit Fehlermeldung (OCSP_STATUS_ERROR)</p> <p>11b.</p> <p>[System:] Die Response enthält einen Statuscode („OCSPResponseStatus“), der gleich 0 („successful“) ist. Die ausgewertete OCSP-Response passt aber nicht zum OCSP-Request (z.B. CertID in OCSP-Request und -Response stimmt nicht überein, s. a. Anmerkung [13]). Abbruch mit Fehlermeldung (OCSP_CHECK_REVOCATION_ERROR)</p> <p>12a.</p> <p>[System:] Das Zertifikat ist für den Referenzzeitpunkt gültig, obwohl der CertStatus "revoked" gemeldet wird, da "revocationTime" > Referenzzeitpunkt. Rückmeldung Zertifikat ist für den Referenzzeitpunkt gültig und Rückgabe der OCSP-Response, siehe Anmerkung [14].</p> <p>12b.</p> <p>[System:] Zertifikat ist gesperrt und die Referenzzeit liegt nach dem Sperrzeitpunkt (CertStatus revoked UND revocationTime <= Referenzzeitpunkts). Rückmeldung Zertifikat ist gesperrt und Rückgabe der OCSP-Response. (CERT_REVOKED)</p> <p>12c.</p> <p>[System:] Zertifikat ist unbekannt (Status unknown) Rückmeldung, dass das Zertifikat ungültig ist und Rückgabe der OCSP-Response. (CERT_UNKNOWN)</p> <p>Weitere Fehlerfälle werden in den jeweiligen</p>
--	--

	referenzierten Use Cases beschrieben.
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an die Produkttypen der TI, die QES-Zertifikate prüfen, siehe auch [RFC6960] Kap. 5.
Anmerkungen	<p>Gültige Status zu Folgende Hinweise sollen als Hilfestellung für eine Umsetzung des TUC dienen:</p> <p>[1] Kettenmodell (chain model) für die Validierung von QES-X.509-Zertifikatketten: Alle CA-Zertifikate müssen zum Zeitpunkt der Ausstellung eines QES-EE-Zertifikats gültig sein und das Zertifikat war beim Erstellen der qualifizierten Signatur gültig und nicht von der CA gesperrt, s. Artikel 32, Absatz (1), Satz (b) [eIDAS], Definition Kettenmodell s. [ETSI TR 119 001], Verwendung v. Prüfmodellen s. [ETSI EN 319 102-1] Kap. 5.2.6.4.</p> <p>[2] Weiterführende Informationen siehe Glossar aus Kap. 11.2 und Definition der Zeitparameter aus [gemSpec_Kon] Kap. 4.1.8.1.3.</p> <p>[3] Schritt 1 sind: Im Signaturzertifikat muss mindestens ein QCStatement mit dem OID id-etsi-qcs-QcCompliance. (0.4.0.1862.1.1) enthalten sein. Die QC-Statement-Typen werden in ETSI EN 319 412-5, insbesondere Kap. 5 – Table 2 für QES-Zertifikate, bezüglich der Extension QCStatements des Zertifikates beschrieben.</p> <p>[4] Schritt 2: Die (zeitliche) Gültigkeitsprüfung ist nach [eIDAS] Artikel 28 Satz (1) ANHANG I Buchstabe e) auch für die QES-Zertifikatsprüfung gemäß TUC_PKI_030 verpflichtend, s. a. [ETSI EN 319 412-5] Annex A.1 Buchstabe (e).</p> <p>[5] Schritt 3: Die Prüfung der KeyUsage lehnt sich an [RFC5280] Kap. 4.2.1.3 und [ETSI EN 319 412-2] Kap. 4.3.2 – Table 1 (KeyUsage v. Type A) sowie Tab_PKI_270.</p> <p>[6] Schritt 4: Das Verfahren zum Finden des QES-CA-Zertifikates in BNetzA-VL verläuft analog zum Finden des nonQES-CA-Zertifikates in der TSL mittels TUC_PKI_003.</p> <p>[7] Schritt 5: Gültigkeitsstatus einer QES-CA wird gemäß [ETSI TS 119 612#] Kap. 5.5.4 und #Annex J} durch den Servicestatus granted, accredited, und withdrawn in der BNetzA-VL gekennzeichnet. Pre-eIDAS-relevante Servicestatus (undersupervision, supervisionincession oder accredited) werden in granted bzw. (supervisionceased oder supervisionrevoked) in withdrawn überführt. Historien zum Servicestatus v. VDAs, hinterlegt im Element <u><ServiceHistory></u> in der BNetzA-VL, sind bei der Prüfung der CA zu berücksichtigen.</p>

[8] Die Einträge der QES-CA-Zertifikate in der BNetzA-VL besitzen gemäß [ETSI TS 119 612#] Kap. 5.5.1.1]9.4 die Extension additionalServiceInformation

<http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/For eSignatures>.

~~Die Einträge der QES-CA-Zertifikate in der BNetzA-VL besitzen den ServiceTypeIdentifier~~

~~<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>.~~

~~Schritt 2 stellt eine TI-spezifische Sperrprüfung des QES-CA-Zertifikats gemäß Kettenmodell dar.~~

~~Zusätzlich~~

[9] Schritt 6: Die Prüfung der Korrektheit der digitalen Signatur des Signaturzertifikats ist z.B. gemäß FDP_DAU.2/QES aus [BSI-CC-PP-0098] ein Bestandteil der QES-Prüfung, welcher sich nicht aus TUC_PKI_004 ableiten lässt.

[10] Schritt 7:

- Details zu den TSL-Einträgen für URLs für OCSP-Responder in der TI unter gemSpec_TSL#TIP1-A_7219. Das Verfahren zur Weiterleitung der OCSP-Anfrage an die zuvor ermittelte OCSP-Adresse aus dem AIA-Feld ist analog zur Weiterleitung von OCSP-Anfragen für QES-Zertifikate der Vorläuferkarten (HBAqSig/ZOD2).
- Die Bereitstellung von Statusprüfdiensten durch die VDAs richtet sich nach den Vorgaben gemäß [eIDAS#] Artikel 24, Abs. (2) Buchstabe (k), Abs. (3) und (4)] ~~muss Schritt 5 folgende Anforderungen bei der QES-spezifischen Statusprüfungen erfüllen: (3) und (4). Die technische Umsetzung des Statusprüfdienstes per OCSP basiert auf [RFC6960].~~
- ~~Zur Auswertung der OCSP-Response siehe auch [Common-PKI#Part4#3 und #Part9#4]~~

~~Zur~~[11] Schritt 11: Die Response enthält einen Statuscode („OCSPResponseStatus“), der gleich 0 („successful“) ist:

- Die Prüfung der certHash-Erweiterung ~~siehe auch [Common-PKI#Part4#3.1.2] und [Common-PKI#Part5#2.3] sowie richtet sich nach GS-A_4693 und [gemSpec_Krypt#GS-A_4393] und GS-A_4693~~
- Die Auswertung der OCSP-Responses (Signatur der OCSP-Responses) gemäß [RFC6960] Kap. 4.1, 4.2 und 4.4 und Kap. 9.1.2 aus [gemSpec_PKI]

[12] Schritt 9, 10: Zur Prüfung der OCSP-Response auf Integrität (Signatur):

1. Die gematik trifft hierzu keine Vorgabe zum Prüfmodell für die Validierung der Signatur von im TUC verwendeten OCSP-Signer-Zertifikaten.
2. Schritt 9: Das OCSP-Signer-Zertifikat kann ~~streng gem.~~ gemäß [RFC6960] von der ausstellenden QES-CA selbst signiert sein oder von einer beliebigen aktuell qualifizierten CA (vgl. gemKPT_PKI_TIP#4.5). ~~Alternativ kann das OCSP-Signer-Zertifikat auch In~~ Bezug auf die Anmerkung aus [ETSI TS 119 612] Kap. 5.5.1.1 (a) NOTE - können OCSP-Signer-Zertifikate aufgrund der Komplexitätsreduzierung nicht direkt als qualifizierter DienstStatusprüfdienst in der die BNetzA-VL eingetragen sein (~~diese werden mit dem ServiceTypeIdentifier~~ "http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP" gekennzeichnet). Genau dann wenn keine dieser Bedingungen zutrifft ist die OCSP-s. URIs in Schritt 9), siehe Schritt 10.
- 1.3. Schritt 10: Falls keiner der URIs in der BNetzA-VL vorhanden ist, muss die Prüfung der Signatur der Response ~~Signatur als fehlerhaft zu bewerten. In diesem Fall ist auch die OCSP-Response selbst als nicht gültig zu betrachten.~~ technisch gemäß [RFC6960] mittels des OCSP-Signer-Zertifikats erfolgen, welches von der ausstellenden QES-CA selbst signiert und im Feld „certs“ der „BasicOCSPResponse“ hinterlegt ist (Festlegung dazu siehe Vorgabe aus Kapitel 9.1.2.7). Der Vertrauensstatus des OCSP-Signer-Zertifikats muss somit über die BNetzA-VL prüfbar sein

~~Zur Prüfung des OCSP-Signer-Zertifikats wird ebenfalls das Kettenmodell benutzt (vgl. [ETSI TS 119 172-4]).~~ [13] Schritt 11b: Die OCSP-Response muss gemäß [RFC6960] Kap. 4.2 verarbeitet werden, unabhängig davon, ob das Feld "parameters" der Sequenz AlgorithmIdentifier innerhalb der CertID mit NULL belegt oder nicht gesetzt ist, siehe Tab_PKI_290. Der in [RFC5754] Kap. 2 empfohlene SHA2 als HashAlgorithmus für die Bildung von certID wird nicht von allen OCSP-Responder-Produkten unterstützt.

[14] Schritt 12a: Falls die Referenzzeit nicht übergeben wird, wird die aktuelle Systemzeit verwendet. Die Variante 12a. ist unter diesen

	Umständen nicht möglich; sie wird also nicht berücksichtigt.
Zugehörige Diagramme/Tabelle	

[<=]

8.5.2 TUC_PKI_036 „BNetzA-VL Aktualisierung“

Der TSL-Dienst stellt die jeweils aktuelle BNetzA-VL an definierten Download-Punkten in der TI bereit. Diese Download-Punkte sind so gewählt, dass sie von allen Diensten, Systemen und Komponenten in der TI netzwerktechnisch erreicht werden können.

Die Adressen der BNetzA-VL-Download-Punkte sind in Form von URI definiert und Bestandteil der TSL (Details s. [gemSpec_TSL#7.5]).

Die Signaturzertifikate der BNetzA-VL sind in der TSL gespeichert und darüber abgesichert (Details s. [gemSpec_TSL#7.5]).

GS-A_5484 - TUC_PKI_036 „BNetzA-VL-Aktualisierung“

Alle Produkttypen, die die BNetzA-VL verwenden, MÜSSEN TUC_PKI_036 zur Aktualisierung umsetzen.

Tabelle 98: TUC_PKI_036 „BNetzA-VL Aktualisierung“

Element	Beschreibung
Name	TUC_PKI_036 „BNetzA-VL Aktualisierung“
Beschreibung	Dieser Use Case beschreibt die Aktualisierung der im System gespeicherten BNetzA-VL.
Anwendungsumfeld	System, das die BNetzA-VL verwendet
Vorbedingungen	Eine aktuell gültige TSL im System
Auslöser	Produktypspezifischer Trigger
Eingangsdaten	<ul style="list-style-type: none"> optional: neu eingebrachte BNetzA-VL-Datei
Komponenten	System
Ausgangsdaten	Status des Prozesses
Referenzen	[ETSI_TS_119_612] [XML] [XMLSig]
Standardablauf	Der Standardablauf stellt die Prüfungen dar, die vollzogen werden müssen. Die Reihenfolge der Schritte ist aber nicht normativ. Eine Trennung in zwei Prozesse oder eine Umstrukturierung, bei der alle notwendigen Prüfungen erfolgen, ist zulässig. 1. [System:] System startet die Aktualisierung der BNetzA-VL

	<p>2. [System:] Primäre BNetzA-VL Hash Download-Adresse aus der TSL extrahieren (s. [gemSpec_TSL#7.5]).</p> <p>3. [System:] Von der im vorherigen Schritt ermittelten Downloadadresse den aktuellen BNetzA-VL Hashwert vom TSL-Dienst herunterladen.</p> <p>4. [System:] Heruntergeladenen BNetzA-VL Hashwert mit dem Hashwert der aktuell im System gespeicherten BNetzA-VL (falls vorhanden) vergleichen. Falls die Hashwerte verschieden sind oder im System noch keine BNetzA-VL vorhanden ist muss die BNetzA-VL im System aktualisiert werden.</p> <p>5. [System:] Primäre BNetzA-VL Download-Adresse aus der TSL extrahieren (s. [gemSpec_TSL#7.5]).</p> <p>6. [System:] Von der ermittelten Downloadadresse die aktuelle BNetzA-VL vom TSL-Dienst herunterladen.</p> <p>7. [System:] Die Wohlgeformtheit der BNetzA-VL-Datei prüfen.</p> <p>8. [System:] Die BNetzA-VL-Datei gegen das XML-Schema gem. [ETSI_TS_119_612#Annex C.2] validieren.</p> <p>9. [System:] Die Aktualität der BNetzA-VL prüfen. Dies geschieht anhand des aktuellen Datums und des Elements „NextUpdate“ aus der BNetzA-VL. Die BNetzA-VL wird als aktuell bezeichnet, wenn ihr NextUpdate nicht in der Vergangenheit liegt.</p> <p>10. [System:] Das verwendete BNetzA-VL-Signer-Zertifikat aus der BNetzA-VL-Datei extrahieren.</p> <p>11. [System:] Prüfen ob das BNetzA-VL-Signerzertifikat in der TSL enthalten ist. Die Identifizierung des Zertifikats erfolgt durch</p> <ul style="list-style-type: none">• Suche nach einem TSPService mit ServiceTypeIdentifier für „BNetzA-VL“ gem. [gemSpec_TSL#7.3.2] und• Vergleich des Elements X509Certificate in zugehöriger DigitalId mit dem BNetzA-VL-Signer-Zertifikat aus Schritt 10 <p>12. [System:] Die XML-Signatur der BNetzA-VL-Datei mittels in der TSL gefundenem BNetzA-VL-Signerzertifikat gem. [XAdES] prüfen.</p> <p>13. [System:] Die aktualisierte BNetzA-VL und deren Hashwert</p>
--	---

	(falls vorhanden) sicher im System speichern. Ende des Use Cases.
Varianten/Alternativen	<p>1a. System:] Wenn eine BNetzA-VL-Datei als Eingangsparameter eingebracht wurde, dann wird diese Datei validiert und geprüft. Weiter mit Schritt 7.</p> <p>2a. [System:] Das Element ist nicht vorhanden. Weiter mit Schritt 3a.2</p> <p>3a. [System:] Das Herunterladen von der primären Downloadadresse schlägt fehl.</p> <p>3a.1 [System:] Das Herunterladen wird bis zu drei Mal wiederholt versucht (insgesamt wird der Vorgang also maximal vier Mal ausgeführt). Falls erfolgreich, weiter mit Schritt 4.</p> <p>3a.2 [System:] Backup BNetzA-VL Hash Download-Adresse aus der TSL extrahieren (s. [gemSpec_TSL#7.5]). Falls nicht erfolgreich, weiter mit Schritt 5.</p> <p>3a.3 [System:] Das Herunterladen wird von der Backup Downloadadresse ausgeführt. Falls erfolgreich, weiter mit Schritt 4.</p> <p>3a.4 [System:] Das Herunterladen von der Backup Downloadadresse wird bis zu drei Mal wiederholt versucht (insgesamt wird der Vorgang also maximal vier Mal ausgeführt). Falls erfolgreich, weiter mit Schritt 4. Falls nicht erfolgreich, weiter mit Schritt 5.</p> <p>4a. [System:] Die verglichenen Hashwerte sind identisch. In diesem Fall ist die im System gespeicherte BNetzA-VL aktuell. Ende des Use Cases ohne Fehler.</p> <p>5b. [System:] Das Element ist nicht vorhanden. Weiter mit Schritt 6a.2</p> <p>6a. [System:] Das Herunterladen von der primären Downloadadresse schlägt fehl.</p> <p>6a.1 [System:] Das Herunterladen wird bis zu drei Mal wiederholt versucht (insgesamt wird der Vorgang also maximal vier Mal ausgeführt). Falls erfolgreich, weiter mit Schritt 7.</p> <p>6a.2 [System:] Backup BNetzA-VL Download-Adresse aus der TSL extrahieren (s. [gemSpec_TSL#7.5]).</p> <p>6a.3 [System:] Das Herunterladen wird von der Backup Downloadadresse ausgeführt. Falls erfolgreich, weiter mit Schritt 7.</p>

	<p>6a.4 [System:] Das Herunterladen von der Backup Downloadadresse wird bis zu drei Mal wiederholt versucht (insgesamt wird der Vorgang also maximal vier Mal ausgeführt). Falls erfolgreich, weiter mit Schritt 7.</p>
Fehlerfälle	<p>Ein Abbruch des TUC führt nur dazu, dass keine neue BNetzA-VL gespeichert wird. Er hat keinen Einfluss auf die Gültigkeit der bestehenden BNetzA-VL. Das System muss dies jedoch protokollieren.</p> <p>6a.2a [System:] Das Element ist nicht vorhanden. Ende des Use Case mit der Fehlermeldung VL_UPDATE_ERROR.</p> <p>6a.4a [System:] Das Herunterladen der BNetzA-VL ist fehlgeschlagen. Ende des Use Cases mit der Fehlermeldung VL_UPDATE_ERROR.</p> <p>7a. [System:] Die XML-Datei ist nicht wohlgeformt. Ende des Use Cases mit der Fehlermeldung VL_UPDATE_ERROR.</p> <p>8a. [System:] Die XML-Schema-Validierung liefert einen Fehler. Ende des Use Cases mit der Fehlermeldung VL_UPDATE_ERROR.</p> <p>9a. [System:] Die Aktualitäts-Prüfung ergibt, dass die BNetzA-VL abgelaufen ist (nextUpdate < aktuelles Datum). Ende des Use Cases mit der Fehlermeldung VL_UPDATE_ERROR.</p> <p>10a. [System:] Das BNetzA-VL-Signer-Zertifikat lässt sich nicht aus der BNetzA-VL-Datei extrahieren. Ende des Use Cases mit der Fehlermeldung VL_UPDATE_ERROR.</p> <p>11a. BNetzA-VL-Signerzertifikat ist nicht in der TSL enthalten. Ende des Use Case mit der Fehlermeldung VL_UPDATE_ERROR.</p> <p>12a. [System:] Die Signatur ist nicht gültig. Ende des Use Cases mit der Fehlermeldung XML_SIGNATURE_ERROR.</p>
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	Das BNetzA-VL-Signer-Zertifikat wird vor Aufnahme in die TSL geprüft (s. [gemSpec_TSL#6.3]). Diese Prüfschritte werden darum nach dem Download innerhalb der TI nicht wiederholt.
Zugehörige Diagramme	

3754
3755
3756

[<=]

3757 8.6 Fehlercodes bei TSL- und Zertifikatsprüfung X.509

3758 Die folgende Tabelle enthält die in den vorher beschriebenen TUCs zur TSL- und
3759 Zertifikatsprüfung potentiell auftretenden Fehlercodes und ordnet diesen gemäß
3760 [gemSpec_OM] jeweils einen Fehlerkategorie und Fehlerklasse zu.

3761 **GS-A_4751 - Fehlercodes bei TSL- und Zertifikatsprüfung**

3762 Die Produkttypen der TI, die Zertifikate prüfen und die TSL auswerten MÜSSEN die
3763 Fehlercodes gemäß Tab_PKI_274 nutzen. Das Element CompType MUSS belegt werden
3764 mit „[Produkttyp]:PKI“, wobei [Produkttyp] zu ersetzen ist durch den konkreten
3765 Produkttyp in der umzusetzenden Anforderung
3766 [\leq]

3767

3768 **Tabelle 99: Tab_PKI_274 Fehlercodes des SubCompTyps PKI bei TSL- und**
3769 **Zertifikatsprüfung**

Co de	Sever ity	ErrorT ype	ErrorText	Detail	Meldungskürzel
100 1	Error	Technic al	Es liegt keine gültige TSL vor		TSL_INIT_ERROR
100 2	Error	Technic al	Zertifikate lassen sich nicht extrahiere n		TSL_CERT_EXTRACTION _ERROR
100 3	Error	Security	Mehr als ein markierter V-Anker gefunden		MULTIPLE_TRUST_ANCHOR
100 4	Error	Technic al	TSL- Signer- CA lässt sich nicht extrahiere n		TSL_SIG_CERT _EXTRACTION_ERROR
100 5	Error	Technic al	Element „PointersT o OtherTSL“ nicht vorhanden		TSL_DOWNLOAD _ADDRESS_ERROR
100 6	Error	Technic al	TSL- Download- adressen wiederholt		TSL_DOWNLOAD_ERROR

			nicht erreichbar		
1007	Error	Security	Vergleich der ID und Sequence-Number entspricht nicht der Vergleichsvariante 6a		TSL_ID_INCORRECT
1008	Warning	Security	Die TSL ist nicht mehr aktuell		VALIDITY_WARNING_1
1009	Warning	Security	Überschreitung des Elements NextUpdate um TSL-Grace-Period		VALIDITY_WARNING_2
1010	Warning	Security	<i>Veraltet: Diese Warnmeldung ist redundant zu VALIDITY_WARNING_1 (Code 1008). Sie soll deshalb nicht mehr verwendet werden.</i>		TSL_NEXTUPDATE_EXPIRED
1011	Error	Technical	TSL-Datei nicht wellformed		TSL_NOT_WELLFORMED
1012	Error	Technical	Schemata der TSL-Datei nicht korrekt		TSL_SCHEMA_NOT_VALID

1013	Error	Security	Signatur ist nicht gültig		XML_SIGNATURE_ERROR
1016	Error	Security	KeyUsage ist nicht vorhanden bzw. entspricht nicht der vorgesehenen KeyUsage		WRONG_KEYUSAGE
1017	Error	Security	Extended-KeyUsage entspricht nicht der vorgesehenen Extended-KeyUsage		WRONG_EXTENDEDKEYUSAGE
1018	Error	Security	Zertifikats-typ-OID stimmt nicht überein		CERT_TYPE_MISMATCH
1019	Error	Technical	Zertifikat nicht lesbar		CERT_READ_ERROR
1021	Error	Security	Zertifikat ist zeitlich nicht gültig		CERTIFICATE_NOT_VALID_TIME
1023	Error	Security	Authority-Key-Identifizier des End-Entity-Zertifikats von Subject-Key-Identifizier des CA-Zertifikats unterschiedlich		AUTHORITYKEYID_DIFFERENT
1024	Error	Security	Zertifikats-Signatur ist mathe-		CERTIFICATE_NOT_VALID_MATH

			matisch nicht gültig.		
102 6	Error	Technic al	Das Element „Service- Supply Point“ konnte nicht gefunden werden.		SERVICESUPPLYPOINT _MISSING
102 7	Error	Technic al	CA kann nicht in den TSL- Infor- mationen ermittelt werden.	Keine Adresse hinterlegt.	CA_CERT_MISSING
102 8	Warni ng	Technic al	Die OCSP- Prüfung konnte nicht durchgeföh rt werden (1)	TOLERATE_ OCSP _FAILURE=t rue	OCSP_CHECK_ REVOCATION_FAILED
102 9	Error	Technic al	Die OCSP- Prüfung konnte nicht durchgeföh rt werden (2)	TOLERATE_ OCSP _FAILURE=f alse	OCSP_CHECK_ REVOCATION_ERROR
103 0	Error	Security	OCSP- Zertifikat nicht in TSL- Infor- mationen enthalten		OCSP_CERT_MISSING
103 1	Error	Security	Signatur der Response ist nicht gültig.		OCSP_SIGNATURE_ERROR
103 2	Error	Technic al	OCSP- Responder nicht verfügbar		OCSP_NOT_AVAILABLE

1033	Error	Security	Kein Element Policy-Information vorhanden		CERT_TYPE_INFO_MISSING
1034	Error	Technical	<i>Veraltet: Diese Fehlermeldung wird nicht mehr verwendet. Stattdessen ist der Fehlercode 1032 zu verwenden.</i>		OCSP_PROXY_NOT_AVAILABLE
1036	Error	Security	Das Zertifikat ist ungültig. Es wurde nach der Sperrung der ausgebenden CA ausgestellt.		CA_CERTIFICATE_REVOKED_IN_TSL
1039	Warning	Security	Warnung, dass Offline-Modus aktiviert ist und keine OCSP-Statusabfrage durchgeführt wurde		NO_OCSP_CHECK
1040	Error	Security	Bei der Online-statusprüfung ist ENFORCE_CERTHASH		CERTHASH_EXTENSION_MISSING

			_CHECK auf 'true' gesetzt, die OCSP-Response enthält jedoch keine certHash-Erweiterung		
1041	Error	Security	Der certHash in der OCSP-Response stimmt nicht mit dem certHash des vorliegenden Zertifikats überein.		CERTHASH_MISMATCH
1042	Error	Technical	Das TLS-SignerCA-Zertifikat kann nicht aus dem sicheren Speicher des Systems geladen werden.		TSL_CA_NOT_LOADED
1043	Error	Technical	CRL kann aus technischen Gründen nicht ausgewertet werden.		CRL_CHECK_ERROR
1044	Warning	Technical	Warnung, dass zum angefragten Zertifikat keine		CERT_UNKNOWN

			Status- infor- mationen verfügbar sind.		
104 7	Warni ng	Security	Das Zertifikat wurde vor oder zum Referenz- zeitpunkt widerrufen .		CERT_REVOKED
104 8	Error	Technic al	Es ist ein Fehler bei der Prüfung des QC- Statement s aufgetrete n (z. B. nicht vorhanden , obwohl gefordert).		QC_STATEMENT_ERROR
105 0	Warni ng	Technic al	Die einem TUC zur Zertifikats- prüfung beigefügte OCSP- Response zu dem zu prüfenden Zertifikat kann nicht erfolgreich gegen das Zertifikat validiert werden.		PROVIDED_OCSP_RESPONSE _NOT_VALID
105 1	Error	Security	Die in einem OCSP- Response zurück- gelieferte Nonce		OCSP_NONCE_MISMATCH

			stimmt nicht mit der Nonce des OCSP-Requests überein.		
1052	Error	Security	Attribut-Zertifikat kann dem übergebenen Basis-Zertifikat nicht zugeordnet werden.		ATTR_CERT_MISMATCH
1053	Error	Technical	Die CRL kann nicht heruntergeladen werden.		CRL_DOWNLOAD_ERROR
1054	Error	Technical	Eine verwendete CRL ist zum aktuellen Zeitpunkt nicht mehr gültig.		CRL_OUTDATED_ERROR
1055	Error	Security	CRL-Signer-Zertifikat nicht in TSL-Informationen enthalten		CRL_SIGNER_CERT_MISSING
1057	Error	Security	Signatur der CRL ist nicht gültig.		CRL_SIGNATURE_ERROR
1058	Error	Technical	Die OCSP-Response enthält eine		OCSP_STATUS_ERROR

			Exception-Meldung.		
1059	Error	Security	CA-Zertifikat für QES-Zertifikatsprüfung nicht qualifiziert		CA_CERTIFICATE_NOT_QES_QUALIFIED
1060	Error	Technical	Die VL kann nicht aktualisiert werden.		VL_UPDATE_ERROR
1061	Error	Security	CA (laut TSL) nicht autorisiert für die Herausgabe dieses Zertifikatsyps.		CERT_TYPE_CA_NOT_AUTHORIZED
1062	Error	Security	Das QES-EE-Zertifikat ist ungültig. Es wurde nach der Sperrung der ausgebenden QES-CA ausgestellt.		CA_CERTIFICATE_REVOKED_IN_BNETZA_VL

3770

3771 8.7 Zertifikatsprüfung CV-Zertifikate der 2. Generation

3772 Die Prüfung von CV-Zertifikaten der Generation 2 beschränkt sich nicht nur auf die
3773 Prüfung der Vertrauenskette und die Signaturprüfung. Zusätzlich werden einige der
3774 verwendeten Schlüsselattribute des CV-Zertifikats und der weiteren CV-Zertifikate in der
3775 Vertrauenskette geprüft bzw. ausgewertet, insbesondere das Certificate Effective Date
3776 (CED) und das Certificate Expiration Date (CXD). Die Prüfung der Signatur eines CV-
3777 Zertifikats erfolgt mittels eines öffentlichen Schlüssels, der vor der Zertifikatsprüfung
3778 ausgewählt wird. Die Prüfschritte erfolgen gemäß Schalenmodell komplett „intern“ durch
3779 das Betriebssystem der prüfenden Chipkarte.

3780 Handelt es sich bei dem Produkttyp der TI, der das CV-Zertifikat prüfen soll, um eine
3781 Chipkarte, dann wird dieser öffentliche Schlüssel durch ein MSE-Set-Kommando der
3782 Karte bekannt gegeben.

3783 **GS-A_5009 - Prüfung der mathematischen Korrektheit von CV-Zertifikate der**
3784 **Generation 2**

3785 Die Produkttypen der TI, die CV-Zertifikate prüfen, MÜSSEN bei der Prüfung von CV-
3786 Zertifikaten der Generation 2 die Prüfung der mathematischen Korrektheit vornehmen, d.
3787 h. ob die Signatur des CV-Zertifikats mit dem CV-Zertifikat der ausstellenden TSP-CVC
3788 und ob die Signatur des TSP-CVC -Zertifikats mit dem CV-Zertifikat der ausstellenden
3789 CVC-Root-CA erfolgreich geprüft werden kann.

3790 [\leq]

3791 **GS-A_5010 - Prüfung der Signatur eines CV-Zertifikats der Generation 2 mit**
3792 **Hilfe des CV-Zertifikats des Herausgebers**

3793 Die Produkttypen der TI, die CV-Zertifikate prüfen, MÜSSEN bei der Prüfung der
3794 mathematischen Korrektheit der Signatur eines CV-Zertifikates C die im CV-Zertifikat des
3795 öffentlichen Schlüssels des Herausgebers enthaltenen Schlüsselattribute dieses
3796 öffentlichen Schlüssels anwenden. Die Prüfung MUSS den Vorgaben aus Tabelle
3797 TAB_PKI_908 folgen.

3798 [\leq]

3799

3800 **Tabelle 100: Tab_PKI_908 Prüfung der Signatur eines CV-Zertifikats der Generation 2**
3801 **mit Hilfe des CV-Zertifikats des Herausgebers**

Prüfung der Korrektheit der Signatur eines CV-Zertifikats C

Sei die Nachricht M die gemäß Tabelle Tab_PKI_905 zu signierende Nachricht M des
CV-Zertifikates C.
Sei Signatur = R || S gemäß Tabelle Tab_PKI_906 die Signatur der Nachricht M des
CV-Zertifikats C.
Sei PuK der im CV-Zertifikat des Herausgebers enthaltene öffentliche Signaturschlüssel
des Herausgebers.

Bei der Prüfung der Signatur MUSS der domainParameter des Schlüssels PuK gemäß
des CV-Zertifikats des Herausgebers genutzt werden (gemäß Tab_PKI_901).
Falls das Wertfeld von DO '86' im CV-Zertifikat des Herausgebers eine Länge von
A. '41' = 65 hat, gilt PuK.domainParameter = brainpoolP256r1.
B. '61' = 97 hat, gilt PuK.domainParameter = brainpoolP384r1.
C. '81' = 129 hat, gilt PuK.domainParameter = brainpoolP512r1.

Bei der Prüfung der Signatur MUSS das Hashverfahren gemäß dem domainParameter
genutzt werden (gemäß Tab_PKI_906).

Falls CAR und CHAT aus CV-Zertifikat C und CV-Zertifikat des Herausgebers nicht
miteinander korrespondieren sind, dann ist das CV-Zertifikat C nicht korrekt.

3802

3803 **GS-A_5011 - Prüfung der Gültigkeit von CV-Zertifikaten der Generation G2**

3804 Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN bei der Prüfung von CV-
3805 Zertifikaten der Generation 2 die Prüfung der Gültigkeit vornehmen, d. h. die Gültigkeit
3806 des CV-Zertifikats gemäß Tabelle TAB_PKI_909 prüfen.

3807 [\leq]

3808

3809

Tabelle 101: Tab_PKI_909 Gültigkeit eines CV-Zertifikats der Generation 2

Gültigkeit eines CV-Zertifikats C
<p>Ein CV-Zertifikat einer CVC-Root-CA ist gültig, wenn</p> <ul style="list-style-type: none"> • das CV-Zertifikat mathematisch korrekt gebildet ist und • das Certificate Expiration Date (CXD) des CV-Zertifikats noch nicht überschritten ist.
<p>Ein CV-Zertifikat C, das von einem Herausgeber der Generation 2 (TSP-CVC oder CVC-Root-CA) erzeugt wurde, ist gültig, wenn</p> <ul style="list-style-type: none"> • das CV-Zertifikat für den öffentlichen Schlüssel des Herausgebers gültig und • das CV-Zertifikat mathematisch korrekt gebildet ist und • das Certificate Expiration Date (CXD) des CV-Zertifikats C nicht überschritten ist.
<p>In allen anderen Fällen ist das CV-Zertifikat ungültig.</p>

3810

3811

GS-A_5012 - Prüfung von CV-Zertifikaten der Generation 2

3812

Die Produkttypen der TI, die CV-Zertifikate prüfen, MÜSSEN bei der Prüfung von CV-Zertifikaten der Generation 2 die Prüfung der mathematischen Korrektheit und die Prüfung der Gültigkeit des CV-Zertifikats gemäß Schalenmodell vornehmen.

3813

3814

3815

3816

[<=]

9 OCSP-Statusinformation

Dieses Kapitel enthält die Festlegung von Schnittstellen, die durch mehrere Produkttypen der PKI bereitgestellt werden müssen. Diese Schnittstellen werden in der vorliegenden Spezifikation beschrieben. Eine wiederholte Darstellung dieser Schnittstellen in den Spezifikationen der Produkttypen erfolgt nicht, vielmehr wird in diesen Dokumenten auf die folgenden Beschreibungen verwiesen.

9.1 Statusprüfung

Gemäß [gemKPT_Arch_TIP] ist zur Statusprüfung die Schnittstelle I_OCSP_Status_Information durch die Produkttypen

- TSL-Dienst,
- gematik Root-CA
- TSP-X.509 nonQES,
- TSP-X.509 QES und
- OCSP-Responder Proxy

anzubieten. Darüber können Nutzer, wie z. B. Konnektor und VPN-Zugangsdienst, Statusinformationen zu X.509-Zertifikaten von OCSP-Respondern erhalten. Die Schnittstelle implementiert die logische Operation check_Revocation_Status mit der der Sperrstatus eines X.509-Zertifikats ermittelt werden kann (vgl. auch [gemKPT_PKI_TIP]).

GS-A_4669 - Umsetzung Statusprüfdienst

Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES, TSP-X.509 QES und OCSP-Responder Proxy MÜSSEN die Schnittstelle I_OCSP_Status_Information implementieren.

[<=]

Die Algorithmen und Parameter für die Erstellung der Signaturen über die OCSP-Responses des OCSP werden in [gemSpec_Krypt] festgelegt. Die Statusprüfung von QES-CA-Zertifikaten erfolgt durch die Prüfung des Vorkommens des Zertifikats der QES-CA in der BNetzA-VL und des Dienststatus (Servicestatus) der QES-CA in der TSL und BNetzA_VL (s. Kap. 8.5). Anhand der gemäß TIP1-A_7219 aus der TSL ermittelten OCSP-Adressen werden Statusinformationen angefragter QES-Zertifikate eingeholt.

9.1.1 Schnittstelle I_OCSP_Status_Information

GS-A_4670 - Statusprüfdienst über Gültigkeitszeitraum des X.509-Zertifikats

Die Produkttypen TSL-Dienst, gematik Root-CA und TSP-X.509 nonQES MÜSSEN den Statusprüfdienst über den gesamten Gültigkeitszeitraum des zu prüfenden Zertifikats sicherstellen. Darüber hinausgehende Anforderungen an die Verfügbarkeit von Statusinformationen MÜSSEN in der Policy des Zertifikatsherausgebers definiert sein.

[<=]

Die gematik Root-CA sowie TSP-X.509 nonQES können Dritte mit der Bereitstellung des Statusprüfdienstes beauftragen.

GS-A_4672-01 - Statusprüfdienst QES gemäß den Vorgaben von eIDAS und Standards

~~GS-A_4672 - Statusprüfdienst QES gemäß den Vorgaben von eIDAS~~ Der TSP-X.509 QES MUSS für den Statusprüfdienst die Vorgaben gemäß [eIDAS] und [VDG§16] sowie den technischen Anforderungen nach [RFC6960] erfüllen.

[<=]

Abweichungen von [RFC6960] werden detailliert in [gemKPT_PKI_TIP#4.5] beschrieben.

GS-A_5050 - gematik-Root-CA Statusprüfdienst im Internet

Die gematik Root-CA MUSS im Internet einen OCSP-Dienst für die Statusauskünfte der CAs zur Verfügung stellen, die Zertifikate zur Verwendung in HBA und SMC-B und eGK bzw. alternative Versichertenidentitäten herausgeben.

[<=]

GS-A_5052 - gematik Root-CA Zertifikatsstatus

Die gematik Root-CA MUSS sicherstellen, dass die Zertifikatsstatusinformation zu einem X.509-CA-Zertifikat im Internet identisch ist zum Status dieses CA-Zertifikates in der TSL.

[<=]

GS-A_5053 - TI-Zertifikatstypen im Internet

Der TSP-X.509 nonQES für HBA, eGK oder SMC-B MUSS Zertifikatsstatusinformationen zu den ausgestellten X.509-Zertifikaten im Internet bereitstellen.

[<=]

Hinweis: Für einen TSP-X.509 nonQES eGK ist es in Abstimmung mit der gematik bis maximal 06/2020 zulässig, noch keine Zertifikatsstatusinformationen im Internet bereitzustellen.

GS-A_5051 - TSP-X.509 nonQES Zertifikatsstatus

Der TSP-X.509 nonQES für HBA oder SMC-B MUSS sicherstellen, dass die Zertifikatsstatusinformation zu einem X.509-Zertifikat in der TI und im Internet identisch ist.

[<=]

9.1.1.1 Schnittstellendefinition

Gemäß [gemKPT_PKI_TIP#TIP1-A_2140] muss die Schnittstelle zur Statusprüfung von nonQES-Zertifikaten der eGK und der alternativen Versichertenidentitäten technisch nach [RFC6960] implementiert werden. Bei allen anderen X.509-Zertifikaten, in denen die CertHash-Erweiterung (Positive Statement) obligatorisch verwendet wird, erfolgt die Statusprüfung zusätzlich gemäß GS-A_4693.

- ~~• von nonQES-Zertifikaten der eGK und der alternativen Versichertenidentitäten nach [RFC2560] implementiert werden und~~
- ~~• bei allen anderen X.509-Zertifikaten gemäß [Common-PKI] implementiert werden, wobei die CertHash-Erweiterung (PositiveStatement) obligatorisch verwendet werden muss.~~

9.1.1.1.1 OCSP-Request

Der OCSP-Request ist komplett in [RFC2560] beschrieben, sowie mit- und Erweiterungen in [Common-PKI] sind komplett in [RFC6960] beschrieben. Die certHash-Erweiterung (außer nonQES-Zertifikaten einer eGK) wird gemäß GS-A_4693 umgesetzt.

Wesentliches Merkmal zur Identifizierung des Zertifikats ist dessen Seriennummer. Der Herausgeber des Zertifikats wird über Hashwerte seines öffentlichen Schlüssels und seines Namens identifiziert. OCSP-Requests können gemäß den Standards signiert sein, dies wird (s. a. Abschnitt 9.1.2.1) in der TI allerdings nicht gefordert und deshalb diese Signaturen auch nicht geprüft.

GS-A_4674-01 - OCSP-Requests gemäß Standards

~~GS-A_4674 - OCSP-Requests gemäß [RFC2560] und [Common-PKI]~~ Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN OCSP-Requests gemäß [RFC2560] und [Common-PKI]-RFC6960] unter obligatorischer Verwendung der CertHash-Erweiterung verarbeiten können. Der Parameter certID MUSS gemäß Tab_PKI_290 gebildet werden.

[<=]

Tabelle 102: Tab_PKI_290 Struktur certID in OCSP-Request/Response

#	Asn.1 Definition	TI-spezifische Vorgaben
1	CertID ::= SEQUENCE {	
2	hashAlgorithm AlgorithmIdentifier OPTIONAL, {DIGEST-ALGORITHM, {...}}	hashAlgorithm ist der zur Erzeugung der Hashwerte issuerNameHash und issuerKeyHash verwendete Hash-Algorithmus. Default SHA1 gemäß [RFC5019] Kap. 2.1.1 und [RFC3370] Kap. 2.1.1, optional SHA2 gemäß [RFC5754] Kap. 2. Das Setzen AlgorithmIdentifier mit oder ohne NULL ist optional.
3	issuerNameHash OCTET STRING,	Hash of issuer's DN.
4	issuerKeyHash OCTET STRING,	Hash of issuer's public key
5	serialNumber CertificateSerialNumber	serialNumber is the serial number of the certificate

GS-A_4957-01GS-A_4957 - Beschränkungen OCSP-Request

Komponenten (Produkttypen der TI, aAdG und aAdG-NetG-TI), die Zertifikate prüfen, DÜRFEN (abweichend von [RFC2560]RFC6960]) je OCSP-Request NICHT mehr als den Status für genau ein Zertifikat abfragen. Ist hierbei die Verwendung der OCSP-Extension „Nonce“ zulässig, DARF diese die Länge von 256 Bit NICHT überschreiten.

[<=]

WA-A_2033 - Nutzung der OCSP-Responder der TI

Eine aAdG oder aAdG-NetG-TI MUSS die OCSP-Responder der TI nutzen.[<=]

9.1.1.1.2 OCSP-Response

Die OCSP-Response ~~ist und ihre Extension sind~~ komplett in [RFC2560]RFC6960 beschrieben, ~~sowie mit Erweiterungen in [Common-PKI]~~. Die certHash-Erweiterung (außer nonQES-Zertifikaten einer eGK) wird gemäß GS-A_4693 umgesetzt.

Wesentlicher Inhalt ist der Status des angefragten Zertifikats, sowie zeitliches Aussagen zu dem gelieferten Status und dessen Aktualität. Die Antwort ist signiert. Weitere Details siehe Abschnitt 9.1.2.2 und folgende.

GS-A_4675-01 - OCSP-Responses zu eGK-Zertifikaten gemäß Standards

~~GS-A_4675-OCSP-Responses gemäß [RFC2560]~~Der TSP-X.509 nonQES (eGK) MUSS für Statusauskünfte zu X.509-Zertifikaten OCSP-Responses gemäß [RFC2560]RFC6960 und [RFC5280] erzeugen.

[<=]

GS-A_4676-01 - OCSP-Responses gemäß Standards

~~GS-A_4676-OCSP-Responses gemäß [Common-PKI]~~Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES (außer eGK) und TSP-X.509 QES MÜSSEN für Statusauskünfte zu X.509-Zertifikaten OCSP-Responses gemäß [Common-PKI]RFC6960 und [RFC5280] unter obligatorischer Verwendung der CertHash-Erweiterung erzeugen. Der Parameter certID MUSS gemäß Tab_PKI_290 gebildet werden.

[<=]

GS-A_5124-01 - OCSP-Responses mit Parameter Nonce gemäß [RFC6960]

~~GS-A_5124-OCSP-Responses mit Parameter Nonce [Common-PKI]~~Der TSP-X.509 QES MUSS für Statusauskünfte zu X.509-Zertifikaten den Parameter „Nonce“ für OCSP-Responses gemäß [Common-Tab_PKI]_289 unterstützen.

[<=]

Tabelle 103: Tab_PKI_289 Struktur Nonce

#	Asn.1 Definition		TI-spezifische Vorgaben
1	id-pkix-ocsp	OBJECT IDENTIFIER ::= {id-ad-ocsp}	Siehe [RFC6960#4.4.1, B.1 und B.2]
2	id-pkix-ocsp-nonce	OBJECT IDENTIFIER ::= {id-pkix-ocsp 2}	Referenzen siehe oben
3		Nonce ::= OCTET STRING	optional

[<=]

Ergänzend zu [RFC6960] kann der OCSP-Client anhand der Festlegung gemäß Tab_PKI_289 jeden Rückgabewert analysieren. Nicht alle Standard-OCSP-Responder unterstützen diese Nonce-Erweiterung.

9.1.1.2 Umsetzung

GS-A_4677 - Spezifikationskonforme OCSP-Responses

Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN sicherstellen, dass ihr OCSP-Responder spezifikationskonform antwortet, wenn der OCSP-Request „well formed“ spezifikationskonform formuliert ist und der Responder für diesen Service konfiguriert ist.

[<=]

GS-A_4678 - Signierte OCSP-Responses

Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN sicherstellen, dass ihr OCSP-Responder alle Antworten (Responses) mit Response-Status 'successful' (0) digital signiert.

[<=]

GS-A_4679 - Signatur zu Statusauskünften von nonQES-Zertifikaten

Die Produkttypen TSL-Dienst, gematik Root-CA, und TSP-X.509 nonQES MÜSSEN zur Erzeugung von Signaturen über OCSP-Responses mit Statusauskünften zu nicht-qualifizierten X.509-Zertifikaten ein Schlüsselpaar einsetzen, für das ein nicht-qualifiziertes X.509-Zertifikat ausgestellt wurde.

[<=]

GS-A_5517 - Schlüsselgenerationen der OCSP-Signer-Zertifikate

Die Produkttypen TSL-Dienst, gematik Root-CA und TSP-X.509 nonQES MÜSSEN sicherstellen, dass zum Signieren von OCSP-Responses für Zertifikate einer bestimmten Schlüsselgeneration, ausschließlich ein OCSP-Signer-Zertifikat derselben Schlüsselgeneration (gemäß [gemSpec_Krypt#GS-A_4357] bzw. [gemSpec_Krypt#GS-A_4358]) verwendet wird.

[<=]

GS-A_4684 - Auslassung der Signaturprüfung bei OCSP-Requests

Zur Gewährleistung der Performance MÜSSEN die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 QES und TSP-X.509 nonQES OCSP-Responder so konfigurieren, dass signierte Requests wie unsignierte Requests behandelt werden und die Signaturprüfung der Requests entfällt.

[<=]

GS-A_4685 - Statusprüfdienst - Steigerung der Performance

Die Produkttypen TSL-Dienst, gematik Root-CA und TSP-X.509 nonQES SOLLEN Methoden des Response-Caching anwenden, um die Performance des Statusprüfdienstes zu steigern.

[<=]

9.1.1.3 Nutzung

Gemäß [gemKPT_PKI_TIP] müssen anfragende Komponenten sicherstellen, dass je OCSP-Request nicht mehr als der Status für ein X.509-Zertifikat abgefragt wird (vgl. [gemKPT_PKI_TIP#TIP1-A_2144]).

4007 Weiterhin müssen Produkttypen der TI, die OCSP-Responses auswerten, sicherstellen,
4008 dass für jede mögliche Ausprägung der zurückgegebenen Parameter eine geordnete
4009 Reaktion implementiert wird (vgl. [gemKPT_PKI_TIP#TIP1-A_2149]).

4010 9.1.2 Artefakte

4011 9.1.2.1 OCSP-Response – Response Status

4012 GS-A_4686 - Statusprüfdienst – Response Status

4013 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES
4014 MÜSSEN sicherstellen, dass für den Response Status die Werte „successful“,
4015 „malformedRequest“, „internalError“, „tryLater“ und „unauthorized“ gemäß Tab_PKI_291
4016 unterstützt werden.
4017 [\leq]

4018

4019 **Tabelle 104: Tab_PKI_291 OCSP-Response Status Ergebnisse**

Ergebnis Anfrage	Bedeutung
successful	Erfolgreiche Bearbeitung einer Anfrage
malformed Request	Wegen fehlerhaftem Anfrageformat konnte keine erfolgreiche Bearbeitung der Anfrage erfolgen.
internalError	Auftretung eines internen Fehlers beim OCSP-Server
tryLater	Nicht-Verfügbarkeit des OCSP-Servers (temporär)
unauthorized	Der Client ist nicht berechtigt

4020

4021 GS-A_4687 - Statusprüfdienst – Response Status sigRequired

4022 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES
4023 MÜSSEN sicherstellen, dass für den Response Status der Wert „sigRequired“ nicht
4024 verwendet wird.
4025 [\leq]

4026 Mit dem Response Status „sigRequired“ fordert der OCSP-Responder explizit, dass die
4027 Anfrage vom OCSP-Client signiert werden muss. Da keine signierten OCSP-Requests in
4028 der TI gefordert sind, darf der Exception Case „sigRequired“ vom OCSP-Responder nicht
4029 verwendet werden.

4030 9.1.2.2 OCSP-Response - Zeiten

4031 GS-A_4688 - Statusprüfdienst – Angabe von Zeitpunkten

4032 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES
4033 MÜSSEN sicherstellen, dass die Angabe zu den Zeitpunkten `producedAt`, `thisUpdate` und
4034 `nextUpdate` spezifikationskonform gemäß Tab_PKI_292 erfolgt.
4035 [\leq]

4036

4037 **Tabelle 105: Tab_PKI_292 Zeiten in einer OCSP-Response**

Zeiten	Bedeutung
--------	-----------

thisUpdate	„thisUpdate“ enthält den Zeitpunkt, für den die gemachte Aussage gültig ist. Es gibt den Zeitpunkt an zu der die Statusinformation als korrekt angesehen wurde.
nextUpdate	„nextUpdate“ enthält die Zeit, wann neue Informationen über das angefragte Zertifikat verfügbar sein werden. OCSP-Antworten, die keinen „nextUpdate“ Zeitpunkt enthalten, zeigen an, dass jederzeit neuere Statusinformationen zu Zertifikaten vorhanden sein können.
producedAt	Der Zeitpunkt der Signierung einer OCSP-Response.

4038 Der Zeitpunkt **nextUpdate** ist nur für OCSP-Antworten sinnvoll, die auf CRLs basieren.

4039

4040 **GS-A_4689 - Statusprüfdienst – Zeitquelle von producedAt**

4041 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES
4042 MÜSSEN sicherstellen, dass der Zeitpunkt **producedAt** auf einer in der TI verbindlichen
4043 Zeitquelle beruht.

4044 [**<=**]

4045 **GS-A_5215 - Festlegung der zeitlichen Toleranzen in einer OCSP-Response**

4046 Produkttypen der TI, die Zertifikate prüfen, MÜSSEN die Angaben zu den Zeitpunkten
4047 **producedAt**, **thisUpdate** und **nextUpdate** in der OCSP-Response mit einer Zeit-Toleranz
4048 bezüglich der lokalen Systemzeit interpretieren.

4049 Produkttypen der TI, die Zertifikate prüfen, MÜSSEN die folgenden Fälle als gültig
4050 akzeptieren, wenn im Rahmen von TUC_PKI_006
4051 eine Online-Abfrage durchgeführt wird:

4052 (a) **producedAt** liegt weniger als (oder ist gleich wie) die Toleranz ,t' gegenüber der
4053 Systemzeit bei Erhalt der Response in der Vergangenheit.

4054 (b) **producedAt** liegt weniger als (oder ist gleich wie) die Toleranz ,t' gegenüber der
4055 Systemzeit bei Erhalt der Response in der Zukunft.

4056 (c) **thisUpdate** liegt weniger als (oder ist gleich wie) die Toleranz ,t' gegenüber der
4057 Systemzeit bei Erhalt der Response in der Zukunft.

4058 (d) **nextUpdate** liegt weniger als (oder ist gleich wie) die Toleranz ,t' gegenüber der
4059 Systemzeit bei Erhalt der Response in der Vergangenheit.

4060 Produkttypen der TI, die Zertifikate prüfen, MÜSSEN die Toleranz ,t' auf genau 37,5
4061 Sekunden ansetzen.

4062 [**<=**]

4063 *Hinweis: Das in der Anforderung spezifizierte Verhalten weicht von den Empfehlungen*
4064 *von [RFC2560] / [RFC6960] Kap. 4.2.2.1 zur Prüfung von thisUpdate und nextUpdate*
4065 *ab.*

4066 *Das Setzen von Zeittoleranzen (mindestens bezüglich nextUpdate) wird aber in*
4067 *[RFC5019], Kap. 4 besprochen: „[...] Clients MAY allow configuration of a small tolerance*
4068 *period for acceptance of responses after nextUpdate to handle minor clock differences*
4069 *relative to responders and caches. This tolerance period should be chosen based on the*
4070 *accuracy and precision of time synchronization technology available to the calling*
4071 *application environment. [...]”*

4072 **9.1.2.3 OCSP-Response - CertStatus**

4073 **GS-A_4690 - Statusprüfdienst – Status des X.509-Zertifikats**

4074 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES
4075 MÜSSEN sicherstellen, dass ein OCSP-Responder den Status eines Zertifikats mit einem

4076 der drei Werte a) good, b) revoked, c) unknown gemäß Tab_PKI_293 zurückgibt.
4077 [\leq]

4078

4079 **Tabelle 106: Tab_PKI_293 Status der OCSP Antworten**

OCSP Antwort	Bedeutung
good	Der Zustand „good“ sagt aus, dass zum Zeitpunkt thisUpdate das Zertifikat nicht gesperrt war. Good sagt aber nichts über die Gültigkeitsdauer und Existenz des Zertifikates aus.
revoked	Der Zustand „revoked“ sagt aus, dass das Zertifikat von der zugehörigen Zertifizierungsstelle ausgestellt wurde, dem OCSP-Responder bekannt ist und temporär oder endgültig gesperrt ist.
unknown	Diese Antwort bedeutet, dass der OCSP-Responder das nachgefragte Zertifikat nicht kennt. Entweder ist dieser von der entsprechenden CA nicht für die Beantwortung von Statusabfragen autorisiert oder es können keine Informationen zu dem Zertifikat gefunden werden.

4080 **9.1.2.4 OCSP-Response - CertID**

4081 **GS-A_4691 - Statusprüfdienst – X.509-Zertifikat mit Status „unknown“**

4082 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES
4083 MÜSSEN sicherstellen, dass im Falle eines certStatus mit Wert „unknown“ im Feld
4084 certID der Struktur SingleResponse der Inhalt des certID-Feldes in der Struktur
4085 Request des OCSP-Requests wiederholt wird.

4086 [\leq]

4087 **9.1.2.5 OCSP-Response – Sperrzeitpunkt und Sperrgrund**

4088 **GS-A_4692 - Statusprüfdienst – Angabe Sperrzeitpunkt**

4089 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES
4090 MÜSSEN sicherstellen, dass im Falle eines gesperrten X.509-Zertifikats die Angabe des
4091 Sperrzeitpunkts im Teilfeld revocationTime in einer OCSP-Response erfolgt.

4092 [\leq]

4093 **GS-A_5090 - Statusprüfdienst – Keine Angabe von Sperrgründen**

4094 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES
4095 SOLLEN sicherstellen, dass kein Sperrgrund mit der OCSP-Response geliefert wird.

4096 [\leq]

4097 **9.1.2.6 OCSP-Response – CertHash**

4098 **GS-A_4693-01GS-A_4693 - Statusprüfdienst – Positive Statement**

4099 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES (außer nonQES-
4100 Zertifikaten einer eGK) und TSP-X.509 QES MÜSSEN sicherstellen, dass die von ihnen
4101 betriebenen OCSP-Responder bei OCSP-Antworten immer die private
4102 SingleExtensionOCSP-Extension „certHash“ [CommonPKI#Part 4, Kapitel 3.1.2] gemäß
4103 Tab_PKI_288 in der OCSP-Response des zu prüfenden X.509-Zertifikats mitsenden. [\leq]

4104

Tabelle 107: Tab_PKI_288 Struktur certHash

#	Asn.1 Definition	TI-spezifische Vorgaben
1	id-commonpki-at-certHash OBJECT IDENTIFIER ::= {1 3 36 8 3 13}	
2	CertHash ::= SEQUENCE {	
3	hashAlgorithm AlgorithmIdentifier,	Algorithmus-Identifizier zur Berechnung des Hash-Wertes, Details siehe [gemSpec_Krypt#GS-A_4393].
4	certificateHash OCTET STRING }	Hash-Wert über das DER-kodierte angefragte Zertifikat.

[<=]

9.1.2.7 OCSP-Response – Responder-Zertifikate

A_19500 - Statusprüfdienst – Hinterlegung OCSP-Signer-Zertifikat

Der TSP-X_509 QES MUSS für Statusauskünfte zu X.509-Zertifikaten das für die Überprüfung der OCSP-Response auf Integrität (mathematische Korrektheitsprüfung der Signatur) benötigte OCSP-Signer-Zertifikat im Feld „certs“ der zu übermittelnden „BasisOCSPResponse“ gemäß [RFC6960] hinterlegen. [<=]

9.1.3 Testunterstützung

Bei der PKI für X.509-Zertifikate wird zwischen einer Produktiv-PKI und einer Test-PKI unterschieden.

GS-A_4694 - Betrieb von OCSP-Responder für Test-PKI-CAs

Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN neben OCSP-Respondern für die produktive PKI ebenfalls OCSP-Responder für die Test-PKI betreiben.

[<=]

9.1.4 Hardwaremerkmale

Die Statusprüfung setzt keine besonderen Hardwaremerkmale voraus.

10 Anhang A – Sektorspezifische Ausprägungen der SMC-B-Zertifikate

Die nachfolgenden Profiltabellen der Sektoren referenzieren auf die Festlegungen aus Kap. 5.3.4 für alle sektorübergreifenden Attribute und ergänzen/ersetzen diese um sektorspezifische Ausprägungen.

Die Profiltabellen gelten einheitlich für die Zertifikate:

- C.HCI.AUT
- C.HCI.ENC
- C.HCI.OSIG

*Hinweis: Während der Erprobungsphase ORS1 enthielten die Zertifikate im Feld **CertificatePolicies** zusätzlich die Policy-OID der „Policy für SMC-B Zertifikate während Erprobung“. Die während der Erprobungsphase ausgegebenen Zertifikate behalten ihre Gültigkeit bis zu ihrem zeitlichen Ablauf.*

10.1 KZBV

Tabelle 108: Tab_SMCB_KZBV_ZA SMC-B-Zertifikate für Zahnarzt (Sektor KZBV)

Element		Inhalt	Kar.	
certificate		C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
	tbsCertificate			
	version	siehe Kap 5.3.4		
	serialNumber	siehe Kap 5.3.4		
	signature	siehe Kap 5.3.4		
	issuer	siehe Kap 5.3.4		
	validity	siehe Kap 5.3.4		
	subject			
	commonName	Gemäß Freigabedaten der zuständigen KZV	1	
	title	nicht belegt	0	
	givenName	nicht belegt	0	
	surName	nicht belegt	0	
	serialNumber	TI-weit eindeutiger Identifier der Karte in der Form: <TSP-ID>.<ICCSN>	1	

			(<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)		
		organizationalUnitName	nicht belegt	0	
		organizationName	Telematik-ID gemäss Freigabedaten der zuständigen KZV	1	
		streetAddress	nicht belegt	0	
		postalCode	nicht belegt	0	
		localityName	nicht belegt	0	
		stateOrProvinceName	nicht belegt	0	
		countryName	siehe Kap 5.3.4	1	
		andere Attribute		0	
		subjectPublicKeyInfo	siehe Kap 5.3.4		
		extensions			critical
		SubjectKeyIdentifier {2 5 29 14}	siehe Kap 5.3.4	1	FALSE
		KeyUsage {2 5 29 15}	siehe Kap 5.3.4	1	TRUE
		SubjectAltNames {2 5 29 17}	rfc822Name type-id= {2 5 4 3}; value= ggf. überlange Institutionsnamen, Alternativnamen oder Ergänzungen	0-1 0-1	FALSE
		BasicConstraints {2 5 29 19}	siehe Kap 5.3.4	1	TRUE
		CertificatePolicies {2 5 29 32}	siehe Kap 5.3.4 zusätzlich: policyQualifierInfo	1 0	FALSE
		CRLDistributionPoints {2 5 29 31}	CDP des TSP für das betreffende Zertifikat	1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap 5.3.4	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	siehe Kap 5.3.4	1	FALSE
		Admission {1 3 36 8 3 3}	admissionAuthority = {0=<von der KZBV benannte attributbestätigende Stelle – zuständige KZV>,C=DE} professionItem = Beschreibung zu <oid_zahnarztpraxis> gemäß [gemSpec_OID#GS-A_4443] professionOID = OID <oid_zahnarztpraxis> gemäß [gemSpec_OID#GS-A_4443] registrationNumber = <Telematik-ID	1 1 1 1	FALSE

			gemäß Freigabedaten der zuständigen KZV>		
		ExtendedKeyUsage {2 5 29 37}	siehe Kap 5.3.4	*)	FALSE
		andere Erweiterungen		0	
		signatureAlgorithm	siehe Kap 5.3.4		
		signature	siehe Kap 5.3.4		

4140

4141

4142 *) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung
4143 ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und
4144 Tab_PKI_240 ist die Kardinalität gleich 0.

4145

4146 Hinweis: In einer früheren Version der vorliegenden Spezifikation war an dieser Stelle
4147 das SMC-B-ORG-Profil des Sektors KZBV zu finden in Form der Tabelle
4148 "Tab_SMCB_KZBV_KZV SMC-B-Zertifikate für KZV (Sektor KZBV)". Dieses Profil ist nun
4149 fachlich unverändert in Kapitel 10.7 mittels der Tabelle "Tab_SMCB_ORG_Gen -
4150 Generisches Zertifikatsprofil" beschrieben.

4151 10.2 KBV

4152 Die nachfolgende Profiltabelle der durch die KBV betreuten Sektoren gilt für die
4153 Sektoren:

- 4154 • Niedergelassene Vertragsärzte (KV)
- 4155 • Niedergelassene Psychologische Psychotherapeuten (KV)
- 4156 • Niedergelassene Kinder- und Jugendlichenpsychotherapeuten (KV)

4157

4158 **Tabelle 109: Tab_SMCB_KV-T SMC-B-Zertifikate für Sektoren der KBV**

Element	Inhalt	Kar.	
certificate	C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
tbsCertificate			
version	siehe Kap 5.3.4		
serialNumber	siehe Kap 5.3.4		
signature	siehe Kap 5.3.4		
issuer	siehe Kap 5.3.4		
validity	siehe Kap 5.3.4		
subject			

		commonName	Erste zwei Zeilen der Anschriftenzone (DIN5008), somit „Kurzname“ der Institution, so wie für das Anschriftenfeld definiert.	1	
		title	Titel des Verantwortlichen/Inhabers	0-1	
		givenName	Vorname des Verantwortlichen/Inhabers (mehrere Vornamen sind durch Blank oder Bindestrich getrennt)	0-1	
		surName	Familiennamen des Verantwortlichen/Inhabers	0-1	
		serialNumber	nicht belegt	0	
		organizationalUnitName	nicht belegt	0	
		organizationName	9-stellige Betriebsstättennummer (z.B. „121234512“) der Praxis als eindeutige Nummer. Für privat abrechnende Ärzte wird hier eine 10-stellige Ersatznummer eingefügt.	1	
		streetAddress	Strassen-Anschrift der Institution (mehrere Wörter sind durch Blank getrennt)	0-1	
		postalCode	Postleitzahl des Ortes der Institution (Deutsche PLZ werden 5-stellig abgebildet)	0-1	
		localityName	Stadt des Institut-Standortes	0-1	
		stateOrProvinceName	Bundesland des Institut-Standortes	0-1	
		countryName	siehe Kap 5.3.4	1	
		andere Attribute		0	
		subjectPublicKeyInfo	siehe Kap 5.3.4		
		extensions			critical
		SubjectKeyIdentifier {2 5 29 14}	siehe Kap 5.3.4	1	FALSE
		KeyUsage {2 5 29 15}	siehe Kap 5.3.4	1	TRUE
		SubjectAltNames {2 5 29 17}	siehe Kap 5.3.4	0-1	FALSE
		BasicConstraints {2 5 29 19}	siehe Kap 5.3.4	1	TRUE
		CertificatePolicies {2 5 29 32}	siehe Kap 5.3.4	1	FALSE
		CRLDistributionPoints {2 5 29 31}	CDP des TSP für das betreffende Zertifikat	1	FALSE

	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap 5.3.4	1	FALSE
	AuthorityKeyIdentifier {2 5 29 35}	siehe Kap 5.3.4	1	FALSE
	Admission {1 3 36 8 3 3}	admissionAuthority: nicht gesetzt professionItem = Beschreibung zu <oid_praxis_arzt> bzw. <oid_praxis_psychotherapeut> gemäss [gemSpec_OID#GS-A_4443] professionOID = OID <oid_praxis_arzt> bzw. <oid_praxis_psychotherapeut> gemäss [gemSpec_OID#GS-A_4443] registrationNumber <Telematik-ID gemäß Freigabedaten der KBV> (Es wird genau eine Admission- Struktur verwendet, mit je genau einem Element: professionInfo, professionItem, registrationNumber)	0 1 1 1	FALSE
	ExtendedKeyUsage {2 5 29 37}	siehe Kap 5.3.4	*)	FALSE
	andere Erweiterungen		0	
	signatureAlgorithm	siehe Kap 5.3.4		
	signature	siehe Kap 5.3.4		

*) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und Tab_PKI_240 ist die Kardinalität gleich 0.

Hinweis: Ein weiteres Zertifikatsprofil im Verantwortungsbereich der KBV ist das Profil der SMC-B-ORG mit KBV-Ausprägung. Dieses ist mittels der Tabelle "Tab_SMCB_ORG_Gen - Generisches Zertifikatsprofil" in Kapitel 10.7 beschrieben.

10.3 DKG

Die nachfolgende Profiltabelle der DKTIG gilt für den Sektor:

- Krankenhäuser (DKTIG)

Tabelle 110: Tab_SMCB_DKTIG SMC-B-Zertifikate für Sektor der DKTIG

Element	Inhalt	Kar.	
certificate	C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
tbsCertificate			
version	siehe Kap 5.3.4		

		serialNumber	siehe Kap 5.3.4		
		signature	siehe Kap 5.3.4		
		issuer	siehe Kap 5.3.4		
		validity	siehe Kap 5.3.4		
		subject			
		commonName	Gemäss Freigabedaten der DKTIG.	1	
		title	nicht belegt	0	
		givenName	nicht belegt	0	
		surName	nicht belegt	0	
		serialNumber	TI-weit eindeutiger Identifier der Karte in der Form: <TSP-ID>.<ICCSN> (<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)	1	
		organizationalUnitName	nicht belegt	0	
		organizationName	abgeleitet aus dem Institutionskennzeichen eines Krankenhauses	0-1	
		streetAddress	Strassen-Anschrift der Institution (mehrere Wörter sind durch Blank getrennt)	1	
		postalCode	Postleitzahl des Ortes der Institution (Deutsche PLZ werden 5-stellig abgebildet)	1	
		localityName	Stadt des Institut-Standortes	1	
		stateOrProvinceName	Bundesland des Institut-Standortes	1	
		countryName	siehe Kap 5.3.4	1	
		andere Attribute		0	
		subjectPublicKeyInfo	siehe Kap 5.3.4		
		extensions			critical
		SubjectKeyIdentifier {2 5 29 14}	siehe Kap 5.3.4	1	FALSE
		KeyUsage {2 5 29 15}	siehe Kap 5.3.4	1	TRUE
		SubjectAltNames {2 5 29 17}	siehe Kap 5.3.4	0-1	FALSE
		BasicConstraints {2 5 29 19}	siehe Kap 5.3.4	1	TRUE
		CertificatePolicies {2 5 29 32}	siehe Kap 5.3.4	1	FALSE

	CRLDistributionPoints {2 5 29 31}	siehe Kap 5.3.4	0-1	FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap 5.3.4	1	FALSE
	AuthorityKeyIdentifier {2 5 29 35}	siehe Kap 5.3.4	1	FALSE
	Admission {1 3 36 8 3 3}	admissionAuthority = {0=<von der DKG benannte attributbestätigende Stelle>,C=DE} professionItem = Beschreibung zu <Krankenhaus> gemäss [gemSpec_OID#GS-A_4443] professionOID = OID <oid_krankenhaus> gemäss [gemSpec_OID#GS-A_4443] registrationNumber = siehe Tabelle Tab_SMCB_TID_DKTIG	1 1 1 1	FALSE
	ExtendedKeyUsage {2 5 29 37}	siehe Kap 5.3.4	*)	FALSE
	andere Erweiterungen		0	
	signatureAlgorithm	siehe Kap 5.3.4		
	signature	siehe Kap 5.3.4		

*) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und Tab_PKI_240 ist die Kardinalität gleich 0.

Tabelle 111: Tab_SMCB_TID_DKTIG Aufbau Telematik-ID in SMC-B-Zertifikaten der DKTIG

Präfix s. Kap 4.7.2.1	Separator s. Kap 4.7.2.2	Fortsatz s. Kap 4.7.2.3
Krankenhaus		SMC-B Kennzeichen + Institutsindividuelle Kennzeichnung
5	-	2 <gem. Freigabedaten der DKTIG>

10.4 GKV-Spitzenverband

Die nachfolgende Profiltabelle des GKV-Spitzenverbandes gilt für Betriebsstätten bzw. Geschäftsstellen der gesetzlichen Krankenkassen.

4181 **Tabelle 112: Tab_SMCB_KTR SMC-B-Zertifikate für Mitarbeiter Kostenträger**

Element		Inhalt	Kar.	
certificate		C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
	tbsCertificate			
	version	siehe Kap 5.3.4		
	serialNumber	siehe Kap 5.3.4		
	signature	siehe Kap 5.3.4		
	issuer	siehe Kap 5.3.4		
	validity	siehe Kap 5.3.4		
	subject			
	commonName	Kurzbezeichnung der Krankenkasse gemäß Freigabedaten des GKV-SV	1	
	title	nicht belegt	0	
	givenName	nicht belegt	0	
	surName	nicht belegt	0	
	serialNumber	TI-weit eindeutiger Identifier der Karte in der Form: <TSP-ID>.<ICCSN> (<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)	1	
	organizationalUnitName	nicht belegt	0	
	organizationName	8-stellige eindeutige Betriebsnummer (BBNR) der Krankenkassenhauptverwaltung gemäß Freigabedaten des GKV-SV	1	
	streetAddress	Straßenanschrift und Hausnummer des Krankenkassenhauptsitzes gemäß Freigabedaten des GKV-SV	1	
	postalCode	Postleitzahl des Krankenkassenhauptsitzes gemäß Freigabedaten des GKV-SV (Deutsche PLZ werden 5-stellig abgebildet)	1	
	localityName	Stadt des Krankenkassenhauptsitzes gemäß Freigabedaten des GKV-SV	1	
	stateOrProvinceName	nicht belegt	0	
	countryName	siehe Kap 5.3.4		
	andere Attribute	siehe Kap 5.3.4		
	subjectPublicKeyInfo	siehe Kap 5.3.4		

extensions			critical
SubjectKeyIdentifier {2 5 29 14}	siehe Kap 5.3.4		FALSE
KeyUsage {2 5 29 15}	siehe Kap 5.3.4		TRUE
SubjectAltNames {2 5 29 17}	otherName (s. Tab_PKI_228) type-id= {2 5 4 3}; value=ggf. überlange Bezeichnung der Krankenkasse oder Ergänzungen	0-1	FALSE
BasicConstraints {2 5 29 19}	siehe Kap 5.3.4		TRUE
CertificatePolicies {2 5 29 32}	siehe Kap 5.3.4		FALSE
CRLDistributionPoints {2 5 29 31}	nicht belegt	0	FALSE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap 5.3.4		FALSE
AuthorityKeyIdentifier {2 5 29 35}	siehe Kap 5.3.4		FALSE
Admission {1 3 36 8 3 3}	admissionAuthority = {O=GKV- Spitzenverband,C=DE} professionItem = Beschreibung zu <oid_kostentraeger> gemäß [gemSpec_OID#GS-A_4443] professionOID = OID <oid_kostentraeger> gemäß [gemSpec_OID#GS-A_4443] registrationNumber = siehe Tabelle Tab_SMCB_TID_GKVS	1 1 1 1	FALSE
ExtendedKeyUsage {2 5 29 37}	siehe Kap 5.3.4	*)	FALSE
andere Erweiterungen		0	
signatureAlgorithm	siehe Kap 5.3.4		
signature	siehe Kap 5.3.4		

*) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung
ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und
Tab_PKI_240 ist die Kardinalität gleich 0.

4186 **Tabelle 113: Tab_SMCB_TID_GKVSV Aufbau Telematik-ID in SMC-B-Zertifikaten des**
4187 **GKV-SV**

Präfix s. Kap 4.7.2.1	Separator s. Kap 4.7.2.2	Fortsatz s. Kap 4.7.2.3
8 (Kostenträger)	-	8-stellige eindeutige Betriebsnummer (BBNR) des GKV-SV

4188

4189 10.5 Apothekerschaft

4190 **Tabelle 114: Tab_SMCB_BAK SMC-B-Zertifikate für Apotheker**

Element		Inhalt	Kar.	
certificate		C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
<div> <div>tbsCertificate</div> <div> <div>version</div> <div>serialNumber</div> <div>signature</div> <div>issuer</div> <div>validity</div> <div>subject</div> <div> <div>commonName</div> <div>title</div> <div>givenName</div> <div>surName</div> <div>serialNumber</div> <div>organizationalUnitName</div> <div>organizationName</div> </div> </div> </div>				
	version	siehe Kap 5.3.4		
	serialNumber	siehe Kap 5.3.4		
	signature	siehe Kap 5.3.4		
	issuer	siehe Kap 5.3.4		
	validity	siehe Kap 5.3.4		
	subject			
	commonName	Name der Apotheke	1	
	title	siehe Kap 5.3.4		
	givenName	Vorname des Verantwortlichen/Inhabers (mehrere Vornamen sind durch Blank oder Bindestrich getrennt) <i>Hinweis: bei mehreren Personen bleibt das Feld leer</i>	0-1	
	surName	Familienname des Verantwortlichen/Inhabers <i>Hinweis: bei mehreren Personen bleibt das Feld leer</i>	0-1	
	serialNumber	TI-weit eindeutiger Identifier der Karte in der Form: <TSP-ID>.<ICCSN> (<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)	0-1	
	organizationalUnitName	nicht belegt	0	
	organizationName	Telematik-ID der Institution gemäß Freigabedaten der Apothekerkammer	1	

			streetAddress	Strassen-Anschrift der Institution (mehrere Wörter sind durch Blank getrennt)	1	
			postalCode	Postleitzahl des Ortes der Institution (Deutsche PLZ werden 5-stellig abgebildet)	1	
			localityName	Stadt des Apotheken-Standortes	1	
			stateOrProvinceName	Bundesland des Apotheken-Standortes	1	
			countryName	siehe Kap 5.3.4		
			andere Attribute	siehe Kap 5.3.4		
			subjectPublicKeyInfo	siehe Kap 5.3.4		
			extensions			critical
			SubjectKeyIdentifier {2 5 29 14}	siehe Kap 5.3.4		FALSE
			KeyUsage {2 5 29 15}	siehe Kap 5.3.4		TRUE
			SubjectAltNames {2 5 29 17}	ggf. überlange Institutionsnamen, Alternativnamen oder Ergänzungen	0-1	FALSE
			BasicConstraints {2 5 29 19}	siehe Kap 5.3.4		TRUE
			CertificatePolicies {2 5 29 32}	siehe Kap 5.3.4		FALSE
			CRLDistributionPoints {2 5 29 31}	nicht belegt	0	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap 5.3.4		FALSE
			AuthorityKeyIdentifier {2 5 29 35}	siehe Kap 5.3.4		FALSE
			Admission {1 3 36 8 3 3}	admissionAuthority = {O=<von der BAK benannte attributbestätigende Stelle >,>,C=DE} professionItem = Beschreibung zu <oid_oeffentliche_apotheke> gemäß [gemSpec_OID#GS-A_4443] professionOID = OID <oid_oeffentliche_apotheke> gemäß [gemSpec_OID#GS-A_4443] registrationNumber = <Telematik-ID der Institution gemäß Freigabedaten der Apothekerkammer>	0-1 1 1 1	FALSE
			ExtendedKeyUsage {2 5 29 37}	siehe Kap 5.3.4	*)	FALSE

		andere Erweiterungen	siehe Kap 5.3.4		
		signatureAlgorithm	siehe Kap 5.3.4		
		signature	siehe Kap 5.3.4		

*) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und Tab_PKI_240 ist die Kardinalität gleich 0.

Tabelle 115: Tab_SMCB_TID_BAK Aufbau Telematik-ID in SMC-B-Zertifikaten der Apotheker

Präfix	Separator	Fortsatz	Weiterer Fortsatz
3 (Apothekerschaft)	-	2 (SMC)	gem. Freigabedaten der Apothekerkammer

10.6 AdV-Umgebung im Auftrag der Kostenträger

Tabelle 116: Tab_SMCB_ADV_KTR SMC-B-Zertifikate für die AdV-Umgebung im Auftrag der Kostenträger

Element	Inhalt *)	Kar.	
certificate	C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
tbsCertificate			
version	siehe Kap 5.3.4		
serialNumber	siehe Kap 5.3.4		
signature	siehe Kap 5.3.4		
issuer	siehe Kap 5.3.4		
validity	siehe Kap 5.3.4		
subject			
commonName	Herausgebende Krankenkasse	1	
title	nicht belegt	0	
givenName	nicht belegt	0	
surName	nicht belegt	0	
serialNumber	nicht belegt	0	
organizationalUnitName	nicht belegt	0	
organizationName	siehe Kap 5.3.4	0-1	
streetAddress	siehe Kap 5.3.4	0-1	

		postalCode	siehe Kap 5.3.4	0-1	
		localityName	siehe Kap 5.3.4	0-1	
		stateOrProvinceName	nicht belegt	0	
		countryName	siehe Kap 5.3.4	1	
		andere Attribute		0	
		subjectPublicKeyInfo	siehe Kap 5.3.4		critical
		extensions			
		SubjectKeyIdentifier {2 5 29 14}	siehe Kap 5.3.4	1	
		KeyUsage {2 5 29 15}	siehe Kap 5.3.4	1	
		SubjectAltNames {2 5 29 17}	siehe Kap 5.3.4	0-1	
		BasicConstraints {2 5 29 19}	siehe Kap 5.3.4	1	
		CertificatePolicies {2 5 29 32}	siehe Kap 5.3.4	1	
		CRLDistributionPoints {2 5 29 31}	nicht belegt	0	
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap 5.3.4	1	
		AuthorityKeyIdentifier {2 5 29 35}	siehe Kap 5.3.4	1	
		Admission {1 3 36 8 3 3}	admissionAuthority : nicht gesetzt professionItem = Beschreibung zu <oid_adv_ktr> gemäss [gemSpec_OID#GS-A_4443] professionOID = OID < oid_adv_ktr> gemäss [gemSpec_OID#GS-A_4443] registrationNumber = Telematik-ID der Institution	0 1 1 1	
		ExtendedKeyUsage {2 5 29 37}	siehe Kap 5.3.4		FALSE
		andere Erweiterungen		0	
		signatureAlgorithm	siehe Kap 5.3.4		
		signature	siehe Kap 5.3.4		

4201

4202 **10.7 SMC-B-ORG**

4203 Die nachfolgende Profiltabelle gilt für die Zertifikate der SMC-B-ORG und kann als
4204 generisches Zertifikatsprofil von verschiedenen Organisationen zur Herausgabe einer
4205 SMC-B-ORG verwendet werden.

4206 Herausgeberspezifische Ausprägungen zu einzelnen Zertifikatsfeldern sind in der Tabelle
4207 Tab_SMCB_ORG_Herausgeber im Dokument [gemRL_SMC-B_ORG_BP] beschrieben.

4208 **Tabelle 117: Tab_SMCB_ORG_Gen - Generisches Zertifikatsprofil für die SMC-B-ORG**

Element		Inhalt *)	Kar.	
certificate		C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
	tbsCertificate			
	version	siehe Kap. 5.3.4		
	serialNumber	siehe Kap. 5.3.4		
	signature	siehe Kap. 5.3.4		
	issuer	siehe Kap. 5.3.4		
	validity	siehe Kap. 5.3.4		
	subject			
	commonName	Kurzbezeichnung gemäß Freigabedaten der zuständigen Organisation (Herausgeberspezifische Ausprägung siehe [gemRL_SMC-B_ORG_BP#Tab_SMCB_ORG_Herausgeber])	1	
	title	nicht belegt	0	
	givenName	nicht belegt	0	
	surName	nicht belegt	0	
	serialNumber	TI-weit eindeutiger Identifier der Karte in der Form: <TSP-ID>.<ICCSN> (<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)	1	
	organizationalUnitName	nicht belegt	0	
	organizationName	siehe Kap. 5.3.4 (Herausgeberspezifische Ausprägung siehe [gemRL_SMC-B_ORG_BP#Tab_SMCB_ORG_Herausgeber])	0-1	
	streetAddress	nicht belegt	0	
	postalCode	nicht belegt	0	
	localityName	nicht belegt	0	
	stateOrProvinceName	nicht belegt	0	
	countryName	siehe Kap. 5.3.4	1	

	andere Attribute		0	
	subjectPublicKeyInfo	siehe Kap. 5.3.4		
	extensions			critical
	SubjectKeyIdentifier {2 5 29 14}	siehe Kap. 5.3.4	1	FALSE
	KeyUsage {2 5 29 15}	siehe Kap. 5.3.4	1	TRUE
	SubjectAltNames {2 5 29 17}	Komplettangabe zur betreffenden Organisation (Herausgeberspezifische Ausprägung siehe [gemRL_SMC-B_ORG_BP#Tab_SMCB_ORG_Herausgeber])	0-1	FALSE
	BasicConstraints {2 5 29 19}	siehe Kap. 5.3.4	1	TRUE
	CertificatePolicies {2 5 29 32}	siehe Kap. 5.3.4	1	FALSE
	CRLDistributionPoints {2 5 29 31}	siehe Kap. 5.3.4 (Herausgeberspezifische Ausprägung siehe gemRL_SMC-B_ORG_BP#Tab_SMCB_ORG_Herausgeber)	0-1	FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap. 5.3.4	1	FALSE
	AuthorityKeyIdentifier {2 5 29 35}	siehe Kap. 5.3.4	1	FALSE
	Admission {1 3 36 8 3 3}	admissionAuthority = {O=<zuständige Registrierungsstelle>,C=DE} (Herausgeberspezifische Ausprägung siehe [gemRL_SMC-B_ORG_BP#Tab_SMCB_ORG_Herausgeber]) professionItem = Beschreibung der Institution gemäß [gemSpec_OID#GS-A_4443] (Herausgeberspezifische Ausprägung siehe [gemRL_SMC-B_ORG_BP#Tab_SMCB_ORG_Herausgeber]) professionOID = OID der Institution gemäß [gemSpec_OID#GS-A_4443] (Herausgeberspezifische Ausprägung siehe [gemRL_SMC-B_ORG_BP#Tab_SMCB_ORG_Herausgeber]) registrationNumber = Telematik-ID gemäß Freigabedaten der zuständigen Organisation (Herausgeberspezifische Ausprägung siehe	1 1 1 1	FALSE

		[gemRL_SMC-B_ORG_BP#Tab_SMCB_ORG_Herausgeber])		
	ExtendedKeyUsage {2 5 29 37}	siehe Kap. 5.3.4	*)	FALSE
	andere Erweiterungen		0	
	signatureAlgorithm	siehe Kap. 5.3.4		
	signature	siehe Kap. 5.3.4		

*) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und Tab_PKI_240 ist die Kardinalität gleich 0.

Die Verantwortung für die Herausgabe der SMC-B ORG als spezielle Form der SMC-B für Gesellschafterorganisationen ist im gesonderten Dokument [gemRL_SMC-B_ORG_BP] beschrieben.

Die in der Vergangenheit hier gepflegte Tabelle „Tab_SMCB_ORG_Herausgeber - Herausgeberspezifische Felder im SMC-B-ORG Profil“ finden Sie fortan im Dokument „gemRL_SMC-B_ORG_BP“ (Berechtigungs-Policy).

10.8 Weitere Leistungserbringerinstitutionen

Tabelle 118: Tab_PKI_286 Generisches Zertifikatsprofil für die SMC-B - Weitere Leistungserbringerinstitution

Element	Inhalt *)	Kar.	
certificate	C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
tbsCertificate			
version	siehe Kap. 5.3.4		
serialNumber	siehe Kap. 5.3.4		
signature	siehe Kap. 5.3.4		
issuer	siehe Kap. 5.3.4		
validity	siehe Kap. 5.3.4		
subject			
commonName	Kurzbezeichnung gemäß Freigabedaten der zuständigen Betriebsstätten und Leistungserbringerinstitution I	1	
title	nicht belegt	0	
givenName	nicht belegt	0	

	surName	nicht belegt	0	
	serialNumber	TI-weit eindeutiger Identifier der Karte in der Form: <TSP-ID>.<ICCSN> (<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)	1	
	organizationalUnitName	nicht belegt	0	
	organizationName	siehe Kap. 5.3.4 (Herausgeberspezifische Ausprägung siehe [gemRL_SMC-B_Herausgabepolicy])	0-1	
	streetAddress	siehe Kap. 5.3.4	0-1	
	postalCode	siehe Kap. 5.3.4	0-1	
	localityName	siehe Kap. 5.3.4	0-1	
	stateOrProvinceName	siehe Kap. 5.3.4	0-1	
	countryName	siehe Kap. 5.3.4	1	
	andere Attribute		0	
	subjectPublicKeyInfo	siehe Kap. 5.3.4		
	extensions			critical
	SubjectKeyIdentifier {2 5 29 14}	siehe Kap. 5.3.4	1	FALSE
	KeyUsage {2 5 29 15}	siehe Kap. 5.3.4	1	TRUE
	SubjectAltNames {2 5 29 17}	Komplettangabe zur betreffenden Organisation	0-1	FALSE
	BasicConstraints {2 5 29 19}	siehe Kap. 5.3.4	1	TRUE
	CertificatePolicies {2 5 29 32}	siehe Kap. 5.3.4	1	FALSE
	CRLDistributionPoints {2 5 29 31}	siehe Kap. 5.3.4	0-1	FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap. 5.3.4	1	FALSE
	AuthorityKeyIdentifier {2 5 29 35}	siehe Kap. 5.3.4	1	FALSE
	Admission {1 3 36 8 3 3}	admissionAuthority = {O=<zuständige bestätigende Organisation>,C=DE} professionItem = Genau eine Beschreibung zu <oid institution_pflege> bzw.	1 1	FALSE

		<p><oid_institution_pflege> bzw. <oid_geburtshilfe> bzw. <oid_institution_pflege> bzw. <oid_praxis_physiotherapeut> bzw. <oid_institution_augenoptiker> bzw. <oid_institution_hoerakustiker> bzw. <oid_institution_orthopaedieschuhmacher> bzw. <oid_institution_orthopaedietechniker> bzw. <oid_institution_zahntechniker> bzw. <oid_rettungsleitstellen> bzw. <oid_sanitaetsdienst_bundeswehr gemäß [gemSpec_OID#GS-A_4443-01]</p> <p>professionOID = Genau eine OID der Berufsgruppe <oid_institution_pflege> bzw. <oid_institution_pflege> bzw. <oid_geburtshilfe> bzw. <oid_institution_pflege> bzw. <oid_praxis_physiotherapeut> bzw. <oid_institution_augenoptiker> bzw. <oid_institution_hoerakustiker> bzw. <oid_institution_orthopaedieschuhmacher> bzw. <oid_institution_orthopaedietechniker> bzw. <oid_institution_zahntechniker> bzw. <oid_rettungsleitstellen> bzw. <oid_sanitaetsdienst_bundeswehr gemäß [gemSpec_OID#GS-A_4443-01]</p> <p>registrationNumber = Telematik-ID gemäß Freigabedaten der zuständigen bestätigenden Organisation gemäß Tab_PKI_101-01 (entsprechend dem Präfix 9, 10 oder 11)</p>	1	
	ExtendedKeyUsage {2.5.29.37}	siehe Kap. 5.3.4	*)	FALSE
	andere Erweiterungen		0	
	signatureAlgorithm	siehe Kap. 5.3.4		
	signature	siehe Kap. 5.3.4		

*) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung
ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und
Tab_PKI_240 ist die Kardinalität gleich 0.

10.9 Weitere Ärztliche Institutionen

4228
4229

**Tabelle 119: Tab_PKI_288 Generisches Zertifikatsprofil für die SMC-B - Weitere
Ärztliche Institutionen**

Element		Inhalt *)	Kar.	
certificate		C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
	tbsCertificate			
	version	siehe Kap. 5.3.4		
	serialNumber	siehe Kap. 5.3.4		
	signature	siehe Kap. 5.3.4		
	issuer	siehe Kap. 5.3.4		
	validity	siehe Kap. 5.3.4		
	subject			
	commonName	Kurzbezeichnung gemäß Freigabedaten der zuständigen Organisation	1	
	title	nicht belegt	0	
	givenName	nicht belegt	0	
	surName	nicht belegt	0	
	serialNumber	TI-weit eindeutiger Identifier der Karte in der Form: <TSP-ID>.<ICCSN> (<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)	1	
	organizationalUnitName	nicht belegt	0	
	organizationName	siehe Kap. 5.3.4	0-1	
	streetAddress	siehe Kap. 5.3.4	0-1	
	postalCode	siehe Kap. 5.3.4	0-1	
	localityName	siehe Kap. 5.3.4	0-1	
	stateOrProvinceName	siehe Kap. 5.3.4	0-1	
	countryName	siehe Kap. 5.3.4	1	
	andere Attribute		0	
	subjectPublicKeyInfo	siehe Kap. 5.3.4		

extensions			critical
SubjectKeyIdentifier {2 5 29 14}	siehe Kap. 5.3.4	1	FALSE
KeyUsage {2 5 29 15}	siehe Kap. 5.3.4	1	TRUE
SubjectAltNames {2 5 29 17}	Komplettangabe zur betreffenden Organisation	0-1	FALSE
BasicConstraints {2 5 29 19}	siehe Kap. 5.3.4	1	TRUE
CertificatePolicies {2 5 29 32}	siehe Kap. 5.3.4	1	FALSE
CRLDistributionPoints {2 5 29 31}	siehe Kap. 5.3.4	0-1	FALSE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap. 5.3.4	1	FALSE
AuthorityKeyIdentifier {2 5 29 35}	siehe Kap. 5.3.4	1	FALSE
Admission {1 3 36 8 3 3}	<p>admissionAuthority = {O=<zuständige bestätigende Organisation>,C=DE}</p> <p>professionItem = Genau eine Beschreibung zu <oid_gesundheitsdienst> <oid_arbeitsmedizin> <oid_vorsorge_reha> gemäß [gemSpec_OID#GS-A_4443]</p> <p>professionOID = Genau eine OID der Berufsgruppe <oid_gesundheitsdienst> <oid_arbeitsmedizin> <oid_vorsorge_reha> gemäß [gemSpec_OID#GS-A_4443]</p> <p>registrationNumber = Telematik-ID gemäß Freigabedaten der zuständigen bestätigenden Organisation gemäß Tab_PKI_101-01 (entsprechend dem Präfix 9, 10 oder 11)</p>	<p>1</p> <p>1</p> <p>1</p>	FALSE
ExtendedKeyUsage {2 5 29 37}	siehe Kap. 5.3.4	*)	FALSE
andere Erweiterungen		0	
signatureAlgorithm	siehe Kap. 5.3.4		

	signature	siehe Kap. 5.3.4		
--	-----------	------------------	--	--

*) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und Tab_PKI_240 ist die Kardinalität gleich 0.

ENTWURF

4234

11 Anhang B – Verzeichnisse

4235

11.1 Abkürzungen

Kürzel	Erläuterung
aAdG	andere Anwendungen des Gesundheitswesens (mit Zugriff auf Dienste der TI)
aAdG-NetG	aAndere Anwendungen des Gesundheitswesens ohne Zugriff auf Dienste der TI in angeschlossenen Netzen des Gesundheitswesens
aAdG-NetG-TI	andere Anwendungen des Gesundheitswesens mit Zugriff auf Dienste der TI aus angeschlossenen Netzen des Gesundheitswesens
AES	Advanced Encryption Standard
AK	Anwendungskonnektor
AN	alphanumerisch
AUT	Authentisierung (Authentication)
AUTN	Technisches Authentisierungszertifikat für Nachrichten
AVS	Apothekenverwaltungssystem (Primärsystem der Apotheker)
BAEK/BÄK	Bundesärztekammer
BAK	Bundesapothekerkammer
BCD	Binary coded decimal
BMG	Bundesministerium für Gesundheit
BNetzA	Bundesnetzagentur
BNetzA-VL	Vertrauensliste (TSL) der Bundesnetzagentur
BPTK	Bundespsychotherapeutenkammer
BSI	Bundesamt für Sicherheit in der Informationstechnik
BZÄK	Bundeszahnärztekammer

C2C	card to card
CA	certification authority
CAMS	Card Application Management System
CAR	Certificate Authority Reference
CC	Common Criteria
CED	Certificate Effective Date
CH	Card Holder
CHA	Certificate Holder Authorisation
CHAT	Certificate Holder Authorization Template
CHR	Certificate Holder Reference
CMS	Karten Management System, Card Management System
CP	Certificate Policy
CPI	Certificate Profile Identifier
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CV	Card Verifiable
CVC	Card Verifiable Certificate
CVC-CA	CA für CV-Zertifikate
CV-Zertifikate	Card Verifiable-Zertifikate
CXD	Certificate Expiration Date
DES	Data Encryption Standard
DIMDI	Deutsches Institut für Medizinische Dokumentation und Information
DKG	Deutsche Krankenhausgesellschaft
DKTIG	Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH

DN	Distinguished Name
DNS	Domain Name Service
DNs	Distinguished Names
EE	End Entity
eGK	Elektronische Gesundheitskarte
ePA	Elektronische Patientenakte
ENC	Verschlüsselung (Encryption)
ENCV	Technisches Verschlüsselungszertifikat für Verordnungen
ETSI	Europäisches Institut für Telekommunikationsnormen
FdV	Frontend des Versicherten
FIPS-140 2	Federal Information Processing Standard 140 2
FQDN	Fully Qualified Domain Name
FM	Fachmodul
GBSM	Gerätebezogenes Sicherheitsmodul
GKV	Gesetzliche Krankenversicherung
gSMC	Gerätebezogene Security Module Card
HBA	Heilberufsausweis
HCI	Health Care Institution
HP	Health Professional
HPC	Health Professional Card
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ICCSN	ICC Serial Number
ID	Identität (Identity)

IK	Individual Key
IPSec	Internet Protocol Security
ISM	Information Security Management
ISO	International Standard Organization
KBV	Kassenärztliche Bundesvereinigung
KIS	Krankenhausinformationssystem (Primärsystem der Krankenhäuser)
KT	Kartenterminal
KTR	Kostenträger
KV	Kassenärztliche Vereinigung
KVK	Krankenversichertenkarte
KVNR	Krankenversichertennummer
KZBV	Kassenzahnärztliche Bundesvereinigung
LÄK	Landesärztekammer
LDAP	Lightweight Directory Access Protocol
LEO	Leistungserbringer-Organisation
LZÄK	Landeszahnärztekammer
MAC	Message Authentication Code
MON	Monitoring
NK	Netzkonnektor
OCSP	Online Certificate Status Protocol
OCSP-R	OCSP-Responder
OID	Object Identifier
OSIG	Organizational Signature
PIN	Personal Identification Number

PKI	Public Key Infrastructure
PKIX	PKI nach X.509 Standard der IETF
PrK	Private Key
PuK	Public Key
PVS	Praxisverwaltungssystem (Primärsystem des Arztes)
QES	Qualifizierte elektronische Signatur
RA	Registration Authority
RCA	Root-CA
RFC	Request For Comment
RSA	Rivest Shamir Adleman (Verfahren)
SAK	Signaturanwendungskomponente
SGB	Sozialgesetzbuch
SGD	Schlüsselgenerierungsdienst
SHA	Secure Hash Algorithm
SIG	Elektronische Signatur
SLA	Service Level Agreement
SM	Security Module
SMC-B	Sicherheitsmodul vom Typ B <medizinische Institution>
SMC	Security Module Card
gSMC-K	Security Module Card Konnektor als <holder>
SM-KT-Zertifikat	X.509-Komponentenzertifikat zu einem SM-KT
SubjectDN	Subject Distinguished Name
TCL	Trusted Component List
TI	Telematikinfrastuktur

TLS	Transport Layer Security
TSL	Trust-service Status List
TSP	Trust Service Provider
VDA	Vertrauensdiensteanbieter
VPN	Virtual Private Network
XML	Extensible Markup Language
ZOD	Zahnärzte Online Deutschland

4236 11.2 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.
Referenzzeitpunkt, Referenzzeit	„Referenzzeit(punkt)“ entspricht „refTime“ in [Common-PKI#Part5] und den Corrigenda dazu (Version 1.2.1 vom 14.06.2014). Es handelt sich um den Zeitpunkt aus einem übergebenen Zeitparameter , für den das Zertifikat auf Gültigkeit geprüft wird und für den die Statusinformationen eingeholt werden. Dabei kann es sich um die aktuelle Systemzeit „current time“ gemäß [RFC5280] Kap. 6.1.3 für nonQES nach dem Schalenmodell (PKIX shell model) handeln (z.B. bei TLS-Verbindungsaufbau). Der Referenzzeitpunkt kann auch in der Vergangenheit liegen (z.B. Signaturzeitpunkt bei QES): Der Signaturzeitpunkt für QES bezüglich des Ketten- für QES-Zertifikate für HBA bzw. Kompromissmodells für nonQES-Zertifikate für HBA und SMC-B (s. [gemKPT_PKI_TIP#2.4.2])

4237 Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung
4238 gestellt.

4239 11.3 Abbildungsverzeichnis

4240	Abbildung 1: Betriebsumgebungen aus Sicht der PKI	30
4241	Abbildung 2: Aufbau der Krankenversichertennummer	35
4242	Abbildung 3: Pseudonym Kodierung in X.509 Versichertenzertifikaten	38
4243	Abbildung 4: Das Anschriftenfeld nach DIN5008	78

4244	Abbildung 5: Use Case Diagramm „Prozesse zur Nutzung des TI-Vertrauensraums“ ...	161
4245	Abbildung 6 : Aufbau der TSL.....	163
4246	Abbildung 7: Aktivitätsdiagramm TUC_PKI_001 „Periodische Aktualisierung TI-	
4247	Vertrauensraum“.....	173
4248	Abbildung 8: Aktivitätsdiagramm TUC_PKI_013 „Import neuer TI-Vertrauensanker“ ..	177
4249	Abbildung 9: Aktivitätsdiagramm TUC_PKI_017 „Lokalisierung Download-Adresse“	182
4250	Abbildung 10: Aktivitätsdiagramm TUC_PKI_016 „Download der TSL-Datei“	185
4251	Abbildung 11: Aktivitätsdiagramm TUC_PKI_019 „Prüfung der Aktualität der TSL“	192
4252	Abbildung 12: Aktivitätsdiagramm TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“	
4253	197
4254	Abbildung 13: Use Case Diagramm „Zertifikatsprüfung“	200
4255	Abbildung 14: Aktivitätsdiagramm TUC_PKI_018 „Zertifikatsprüfung“	207
4256	Abbildung 15: Aktivitätsdiagramm TUC_PKI_002 Gültigkeitsprüfung des Zertifikats ...	210
4257	Abbildung 16: Aktivitätsdiagramm TUC_PKI_003 CA-Zertifikat in TSL-Informationen	
4258	finden.....	213
4259	Abbildung 17: Aktivitätsdiagramm TUC_PKI_004 Mathematische Prüfung der	
4260	Zertifikatssignatur.....	215
4261	Abbildung 18: Aktivitätsdiagramm TUC_PKI_005 „Adresse für Status- und Sperrprüfung	
4262	ermitteln“	218
4263	Abbildung 19: Aktivitätsdiagramm TUC_PKI_006 „OCSP-Abfrage“	226
4264	Abbildung 20: Aktivitätsdiagramm TUC_PKI_021 „CRL-Prüfung“	232
4265	Abbildung 21: Aktivitätsdiagramm TUC_PKI_009 „Rollenermittlung“	235
4266	Abbildung 22: Aktivitätsdiagramm TUC_PKI_007 „Prüfung Zertifikatstyp“	240
4267	Abbildung 1: Betriebsumgebungen aus Sicht der PKI.....	30
4268	Abbildung 2: Aufbau der Krankenversicherungsnummer.....	35
4269	Abbildung 3: Pseudonym Kodierung in X.509-Versichertenzertifikaten.....	38
4270	Abbildung 4: Das Anschriftenfeld nach DIN5008	78
4271	Abbildung 5: Use Case Diagramm „Prozesse zur Nutzung des TI-Vertrauensraums“ ...	161
4272	Abbildung 6 : Aufbau der TSL.....	163
4273	Abbildung 7: Aktivitätsdiagramm TUC_PKI_001 „Periodische Aktualisierung TI-	
4274	Vertrauensraum“.....	173
4275	Abbildung 8: Aktivitätsdiagramm TUC_PKI_013 „Import neuer TI-Vertrauensanker“ ..	177
4276	Abbildung 9: Aktivitätsdiagramm TUC_PKI_017 „Lokalisierung Download-Adresse“	182
4277	Abbildung 10: Aktivitätsdiagramm TUC_PKI_016 „Download der TSL-Datei“	185
4278	Abbildung 11: Aktivitätsdiagramm TUC_PKI_019 „Prüfung der Aktualität der TSL“	192
4279	Abbildung 12: Aktivitätsdiagramm TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“	
4280	197
4281	Abbildung 13: Use Case Diagramm „Zertifikatsprüfung“	200

4282	Abbildung 14: Aktivitätsdiagramm TUC_PKI_018 „Zertifikatsprüfung“	207
4283	Abbildung 15: Aktivitätsdiagramm TUC_PKI_002 Gültigkeitsprüfung des Zertifikats ...	210
4284	Abbildung 16: Aktivitätsdiagramm TUC_PKI_003 CA-Zertifikat in TSL-Informationen	
4285	finden.....	213
4286	Abbildung 17: Aktivitätsdiagramm TUC_PKI_004 Mathematische Prüfung der	
4287	Zertifikatssignatur	215
4288	Abbildung 18: Aktivitätsdiagramm TUC_PKI_005 „Adresse für Status- und Sperrprüfung	
4289	ermitteln“	218
4290	Abbildung 19: Aktivitätsdiagramm TUC_PKI_006 „OCSP-Abfrage“	226
4291	Abbildung 20: Aktivitätsdiagramm TUC_PKI_021 „CRL-Prüfung“	232
4292	Abbildung 21: Aktivitätsdiagramm TUC_PKI_009 „Rollenermittlung“	235
4293	Abbildung 22 : Aktivitätsdiagramm TUC_PKI_007 „Prüfung Zertifikatstyp“	240
4294		

4295 11.4 Tabellenverzeichnis

4296	Tabelle 1: Tab_PKI_201 Allgemeine Notationsvorschrift für kryptographische Objekte..	20
4297	Tabelle 2: Tab_PKI_202: Notationsvorgaben für Objekttyp.....	20
4298	Tabelle 3: Tab_PKI_203 Notationsvorgaben für Objektbesitzer	21
4299	Tabelle 4: Tab_PKI_204 Notationsvorgaben für Objektverwendung	23
4300	Tabelle 5: Tab_PKI_205 Notationsvorgaben für Ausprägung	25
4301	Tabelle 6: Tab_PKI_206 Beispiele für asymmetrische Objekte.....	26
4302	Tabelle 7: Tab_PKI_207 Beispiele für symmetrische Objekte	27
4303	Tabelle 8: Tab_PKI_213 Erlaubte Werte für <usage> und <usageName>	32
4304	Tabelle 9: Tab_PKI_221 Berufsgruppenkennzeichnung	39
4305	Tabelle 10: Tab_PKI_222 Institutionstypkennzeichnung	40
4306	Tabelle 11: Tab_PKI_230 Kennzeichnung Technische Rolle	41
4307	Tabelle 12: Tab_PKI_224 Telematik ID-Kennzeichnung	42
4308	Tabelle 13: Tab_PKI_223 Aufbau der Telematik ID	42
4309	Tabelle 14: Tab_PKI_101 Normative Festlegung für das Präfix der Telematik ID.....	43
4310	Tabelle 15: Tab_PKI_229 Kodierung der Attribute in X.509 Zertifikaten	44
4311	Tabelle 16: Tab_PKI_109 Werte für das Präfix <TSP-ID>	46
4312	Tabelle 17: Tab_PKI_226 Struktur Admission	47
4313	Tabelle 18: Tab_PKI_227 Struktur CertificatePolicies	48
4314	Tabelle 19: Tab_PKI_228 Struktur SubjectAltName	51
4315	Tabelle 20: Common Name (CN) der End-Entity Zertifikate Test-PKI	55
4316	Tabelle 21: Tab_PKI_231 Personennamen im subjectDN	60

4317	Tabelle 22: Tab_PKI_232 C.CH.AUT und C.CH.AUT_ALT Authentisierung eGK	61
4318	Tabelle 23: Tab_PKI_233 C.CH.ENC Verschlüsselung eGK	62
4319	Tabelle 24: Tab_PKI_234 C.CH.QES Qualifizierte Signatur eGK	64
4320	Tabelle 25: Tab_PKI_235 C.CH.AUTN Technische Authentisierung eGK	66
4321	Tabelle 26: Tab_PKI_236 C.CH.ENCV Technische Verschlüsselung eGK	67
4322	Tabelle 27: Tab_PKI_268_1 C.HP.AUT Authentisierung HBA	69
4323	Tabelle 281: Tab_PKI_269_1 C.HP.ENC Verschlüsselung HBA	71
4324	Tabelle 29: Tab_PKI_270_1 C.HP.QES Qualifizierte Signatur HBA	73
4325	Tabelle 30: Tab_PKI_238 C.HCI.AUT Authentisierung SMC-B	79
4326	Tabelle 31: Tab_PKI_239 C.HCI.ENC Verschlüsselung SMC-B	81
4327	Tabelle 32: Tab_PKI_240 C.HCI.OSIG Signatur SMC-B	83
4328	Tabelle 33: Tab_PKI_241 C.SMKT.AUT gSMC-KT	86
4329	Tabelle 34: Tab_PKI_237 Statusprüfung von Konnektorzertifikaten	88
4330	Tabelle 35: Tab_PKI_242 Zertifikatsprofil C.NK.VPN VPN-Authentisierung Netzkonnektor	
4331	89
4332	Tabelle 36: Tab_PKI_243 Zertifikatsprofil C.AK.AUT Authentisierung	
4333	Anwendungskonnektor	91
4334	Tabelle 37: Tab_PKI_244 Zertifikatsprofil C.SAK.AUT Authentisierung SAK	93
4335	Tabelle 38: Tab_PKI_245 Zertifikatsprofil C.VPNK.VPN VPN-Authentisierung	
4336	Zugangsdienst TI	95
4337	Tabelle 39: Tab_PKI_265 Zertifikatsprofil C.VPNK.VPN-SIS VPN-Authentisierung	
4338	Zugangsdienst Sicherer Internetzugang	97
4339	Tabelle 40: Tab_PKI_247 C.ZD.TLS-S Server Authentisierung Zentrale Dienste	99
4340	Tabelle 41: Tab_PKI_249 C.FD.TLS-C Client Authentisierung Fachanwendungsspezifische	
4341	Dienste	101
4342	Tabelle 42: Tab_PKI_250 C.FD.TLS-S Server Authentisierung	
4343	Fachanwendungsspezifische Dienste	103
4344	Tabelle 43: Tab_PKI_251 C.FD.SIG Signatur fachanwendungsspezifische Dienste	105
4345	Tabelle 44: Tab_PKI_275 C.FD.AUT Authentisierung fachanwendungsspezifische	
4346	Dienste	106
4347	Tabelle 45: Tab_PKI_276 C.FD.ENC Verschlüsselung fachanwendungsspezifische Dienste	
4348	108
4349	Tabelle 46: Tab_PKI_267 C.CM.TLS-CS Clientmodul Authentisierung	110
4350	Tabelle 47: Tab_PKI_296 C.SGD-HSM.AUT Authentisierung SGD-HSM	112
4351	Tabelle 48: Tab_PKI_211 GEM-R-CA<n>—Zentrale gematik-Root-CA_nonQES der TI	115
4352	Tabelle 49: Tab_PKI_212 <tsp>.<usage>-CA<n>—Aussteller-CA_nonQES der TI	116
4353	Tabelle 50: Tab_PKI_253 C.GEM.OCSP Zertifikatsprofil OCSP-Signer	120
4354	Tabelle 51: Tab_PKI_214 C.GEM.CRL Zertifikatsprofil CRL-Signer	123
4355	Tabelle 52: Tab_PKI_252_01 C.TSL.SIG Zertifikatsprofil TSL-Signer	126

4356	Tabelle 53: Tab_PKI_254 Zugriffsprofile für eine Rollenauthentisierung	130
4357	Tabelle 54: Tab_PKI_255 Zugriffsprofile G2 für eine Authentisierung einer	
4358	Funktionseinheit.....	137
4359	Tabelle 55: Tab_PKI_266 Aufbau CAR für Karten der Generation 2	140
4360	Tabelle 56: Tab_PKI_901 Objektidentifizier des öffentlichen Schlüssels eines CV-Zertifikats	
4361	der Generation 2	142
4362	Tabelle 57: Tab_PKI_902 Punkt Q des öffentlichen Schlüssels eines CV-Zertifikats der	
4363	Generation 2	142
4364	Tabelle 58: Tab_PKI_258 Aufbau CHR	143
4365	Tabelle 59: Tab_PKI_904 Mögliche Objektidentifizier OID_{flags} in Certificate Holder	
4366	Authorization Templates.....	145
4367	Tabelle 60: Tab_PKI_905 Zu signierende Nachricht M eines CV-Zertifikates	146
4368	Tabelle 61: Tab_PKI_906 Signatur der Nachricht M eines CV-Zertifikats	146
4369	Tabelle 62: Tab_PKI_907 Struktur und Inhalt eines CV-Zertifikat	147
4370	Tabelle 63: Tab_PKI_912 CA CV-Zertifikate für 256-bit ELC-Schlüssel, insgesamt	
4371	220 Oktett	148
4372	Tabelle 64: Tab_PKI_913 CA CV-Zertifikate für 384-bit ELC-Schlüssel, insgesamt	
4373	285 Oktett	148
4374	Tabelle 65: Tab_PKI_914 CA CV-Zertifikate für 512-bit ELC-Schlüssel, insgesamt	
4375	352 Oktett	149
4376	Tabelle 66: Tab_PKI_937 Cross-CV-Zertifikat für ELC-Schlüssel	150
4377	Tabelle 67: Tab_PKI_915 Endnutzer-CV-Zertifikate für 256-bit ELC-Schlüssel, insgesamt	
4378	222 Oktett	151
4379	Tabelle 68: Tab_PKI_916 Endnutzer-CV-Zertifikate für 384-bit ELC-Schlüssel, insgesamt	
4380	287 Oktett	151
4381	Tabelle 69: Tab_PKI_917 Endnutzer-CV-Zertifikate für 512-bit ELC-Schlüssel, insgesamt	
4382	354 Oktett	152
4383	Tabelle 70: Tab_PKI_910 TI-PKI, Bedeutung der Bits innerhalb der Flagliste eines CHAT	
4384	153
4385	Tabelle 71: Tab_PKI_918 Abbildung von Rollenberechtigungen-Zugriffsprofilen auf	
4386	äquivalente Flaglisten	155
4387	Tabelle 72: Tab_PKI_919 Sub-CA-Flaglisten nach Kartentyp (G2) und Zugriffsprofilen	
4388	Tabelle 73: Tab_PKI_911 CMS-PKI, Bedeutung der Bits innerhalb der Flagliste eines	
4389	CHAT.....	157
4390	Tabelle 74: Tab_PKI_271 Erlaubte URIs als Inhalte des TSL-Elements ServiceStatus..	167
4391	Tabelle 75: TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“	168
4392	Tabelle 76: TUC_PKI_013 „Import neuer TI-Vertrauensanker“	174
4393	Tabelle 77: Gültige Werte für den TI-Vertrauensankerwechsel	179
4394	Tabelle 78: Beispiel für den TSL-Eintrag zum Wechsel des TSL-Signer-CA-Zertifikats ..	179
4395	Tabelle 79: TUC_PKI_017 „Lokalisierung Download-Adressen“	180

4396	Tabelle 80: Tab_PKI_272 Gültige Werte zur Download-Adresse.....	182
4397	Tabelle 81: TUC_PKI_016 „Download der TSL-Datei“	183
4398	Tabelle 82: TUC_PKI_019 „Prüfung der Aktualität der TSL“	187
4399	Tabelle 83: TUC_PKI_020 „XML-Dokument validieren“	193
4400	Tabelle 84: TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“	194
4401	Tabelle 85: TUC_PKI_012 „XML-Signatur-Prüfung“	197
4402	Tabelle 86: Tab_PKI_294 TSL-Zeitparameter	199
4403	Tabelle 87: TUC_PKI_018 „Zertifikatsprüfung in der TI“	201
4404	Tabelle 88: TUC_PKI_002 „Gültigkeitsprüfung des Zertifikats“	208
4405	Tabelle 89: TUC_PKI_003 „CA-Zertifikat in TSL-Informationen finden“	210
4406	Tabelle 90: TUC_PKI_004 „Mathematische Prüfung der Zertifikatssignatur“	213
4407	Tabelle 91: TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln“	216
4408	Tabelle 92: TUC_PKI_006 „OCSP-Abfrage“	218
4409	Tabelle 93: TUC_PKI_021 „CRL-Prüfung“	226
4410	Tabelle 94: TUC_PKI_009 „Rollenermittlung“	233
4411	Tabelle 95: TUC_PKI_007 „Prüfung Zertifikatstyp“	236
4412	Tabelle 96: Tab_PKI_273 Prüfparameter für TLS-Aufbau	241
4413	Tabelle 97: TUC_PKI_030 „QES-Zertifikatsprüfung“	243
4414	Tabelle 98: TUC_PKI_036 „BNetzA-VL-Aktualisierung“	252
4415	Tabelle 99: Tab_PKI_274 Fehlercodes des SubCompTyps PKI bei TSL- und	
4416	Zertifikatsprüfung	256
4417	Tabelle 100: Tab_PKI_908 Prüfung der Signatur eines CV-Zertifikats der Generation 2	
4418	mit Hilfe des CV-Zertifikats des Herausgebers	265
4419	Tabelle 101: Tab_PKI_291 OCSP-Response-Status-Ergebnisse	272
4420	Tabelle 102: Tab_PKI_292 Zeiten in einer OCSP-Response	272
4421	Tabelle 103: Tab_PKI_293 Status der OCSP-Antworten	274
4422	Tabelle 104: Tab_SMCB_KZBV_ZA SMC-B-Zertifikate für Zahnarzt (Sektor KZBV)	276
4423	Tabelle 105: Tab_SMCB_KV-T SMC-B-Zertifikate für Sektoren der KBV	278
4424	Tabelle 106: Tab_SMCB_DKTIG SMC-B-Zertifikate für Sektor der DKTIG	280
4425	Tabelle 107: Tab_SMCB_TID_DKTIG Aufbau Telematik-ID in SMC-B-Zertifikaten der	
4426	DKTIG	282
4427	Tabelle 108: Tab_SMCB_KTR SMC-B-Zertifikate für Mitarbeiter Kostenträger	283
4428	Tabelle 109: Tab_SMCB_TID_GKVSV Aufbau Telematik-ID in SMC-B-Zertifikaten des	
4429	GKV-SV	285
4430	Tabelle 110: Tab_SMCB_BAK SMC-B-Zertifikate für Apotheker	285
4431	Tabelle 111: Tab_SMCB_TID_BAK Aufbau Telematik-ID in SMC-B-Zertifikaten der	
4432	Apotheker	287

4433	Tabelle 112: Tab_SMCB_ADV_KTR SMC-B-Zertifikate für die Adv-Umgebung im Auftrag	
4434	der Kostenträger	287
4435	Tabelle 113: Tab_SMCB_ORG_Gen – Generisches Zertifikatsprofil für die SMC-B-ORG	289
4436	Tabelle 114: Tab_HBA_BÄK HBA-Zertifikate (AUT, ENC, QES) für BÄK	317
4437	Tabelle 115: Tab_HBA_BZÄK HBA-Zertifikate (AUT, ENC, QES) für BZÄK	319
4438	Tabelle 116: Tab_HBA_BPtK HBA-Zertifikate (AUT, ENC, QES) für BPtK	321
4439	Tabelle 117: Tab_HBA_BAK HBA-Zertifikate (AUT, ENC, QES) für Apotheker	323
4440	Tabelle 1: Tab_PKI_201 Allgemeine Notationsvorschrift für kryptographische Objekte ..	20
4441	Tabelle 2: Tab_PKI_202: Notationsvorgaben für Objekttyp	20
4442	Tabelle 3: Tab_PKI_203 Notationsvorgaben für Objektbesitzer	21
4443	Tabelle 4: Tab_PKI_204 Notationsvorgaben für Objektverwendung	23
4444	Tabelle 5: Tab_PKI_205-01 Notationsvorgaben für Ausprägung	25
4445	Tabelle 6: Tab_PKI_206-01 Beispiele für asymmetrische Objekte	26
4446	Tabelle 7: Tab_PKI_207 Beispiele für symmetrische Objekte	27
4447	Tabelle 8: Tab_PKI_213 Erlaubte Werte für <usage> und <usageName>	32
4448	Tabelle 9: Tab_PKI_221 Berufsgruppenkennzeichnung	39
4449	Tabelle 10: Tab_PKI_222 Institutionstypkennzeichnung	40
4450	Tabelle 11: Tab_PKI_230 Kennzeichnung Technische Rolle	41
4451	Tabelle 12: Tab_PKI_224 Telematik-ID-Kennzeichnung	42
4452	Tabelle 13: Tab_PKI_223 Aufbau der Telematik-ID	42
4453	Tabelle 14: Tab_PKI_101-01 Normative Festlegung für das Präfix der Telematik-ID	43
4454	Tabelle 15: Tab_PKI_229-01 Kodierung der Attribute in X.509-Zertifikaten	44
4455	Tabelle 16: Tab_PKI_109 Werte für das Präfix <TSP-ID>	46
4456	Tabelle 17: Tab_PKI_226-01 Struktur Admission	47
4457	Tabelle 18: Tab_PKI_227 Struktur CertificatePolicies	48
4458	Tabelle 19: Tab_PKI_228 Struktur SubjectAltName	51
4459	Tabelle 20: Common Name (CN) der End-Entity-Zertifikate Test-PKI	55
4460	Tabelle 21: Tab_PKI_231 Personennamen im subjectDN	60
4461	Tabelle 22: Tab_PKI_232 C.CH.AUT und C.CH.AUT_ALT Authentisierung eGK	61
4462	Tabelle 23: Tab_PKI_233 C.CH.ENC Verschlüsselung eGK	62
4463	Tabelle 24: Tab_PKI_234 C.CH.QES Qualifizierte Signatur eGK	64
4464	Tabelle 25: Tab_PKI_235 C.CH.AUTN Technische Authentisierung eGK	66
4465	Tabelle 26: Tab_PKI_236 C.CH.ENCV Technische Verschlüsselung eGK	67
4466	Tabelle 27: Tab_PKI_268_1 C.HP.AUT Authentisierung HBA	69
4467	Tabelle 281: Tab_PKI_269_1 C.HP.ENC Verschlüsselung HBA	71
4468	Tabelle 29: Tab_PKI_270_1 C.HP.QES Qualifizierte Signatur HBA	73

4469	Tabelle 30: Tab_PKI_238 C.HCI.AUT Authentisierung SMC-B	79
4470	Tabelle 31: Tab_PKI_239 C.HCI.ENC Verschlüsselung SMC-B	81
4471	Tabelle 32: Tab_PKI_240 C.HCI.OSIG Signatur SMC-B	83
4472	Tabelle 33: Tab_PKI_241 C.SMKT.AUT gSMC-KT.....	86
4473	Tabelle 34: Tab_PKI_237 Statusprüfung von Konnektorzertifikaten	88
4474	Tabelle 35: Tab_PKI_242 Zertifikatsprofil C.NK.VPN VPN-Authentisierung Netzkonnektor	
4475	89
4476	Tabelle 36: Tab_PKI_243 Zertifikatsprofil C.AK.AUT Authentisierung	
4477	Anwendungskonnektor.....	91
4478	Tabelle 37: Tab_PKI_244 Zertifikatsprofil C.SAK.AUT Authentisierung SAK.....	93
4479	Tabelle 38: Tab_PKI_245 Zertifikatsprofil C.VPNK.VPN VPN-Authentisierung	
4480	Zugangsdienst TI	95
4481	Tabelle 39: Tab_PKI_265 Zertifikatsprofil C.VPNK.VPN-SIS VPN-Authentisierung	
4482	Zugangsdienst Sicherer Internetzugang.....	97
4483	Tabelle 40: Tab_PKI_247 C.ZD.TLS-S Server-Authentisierung Zentrale Dienste.....	99
4484	Tabelle 41: Tab_PKI_249 C.FD.TLS-C Client-Authentisierung Fachanwendungsspezifische	
4485	Dienste.....	101
4486	Tabelle 42: Tab_PKI_250 C.FD.TLS-S Server-Authentisierung	
4487	Fachanwendungsspezifische Dienste	103
4488	Tabelle 43: Tab_PKI_251 C.FD.SIG Signatur fachanwendungsspezifische Dienste	105
4489	Tabelle 44: Tab_PKI_275 C.FD.AUT Authentisierung fachanwendungsspezifische	
4490	Dienste.....	106
4491	Tabelle 45: Tab_PKI_276 C.FD.ENC Verschlüsselung fachanwendungsspezifische Dienste	
4492	108
4493	Tabelle 46: Tab_PKI_267 C.CM.TLS-CS Clientmodul-Authentisierung	110
4494	Tabelle 47: Tab_PKI_296 C.SGD-HSM.AUT Authentisierung SGD-HSM	112
4495	Tabelle 48: Tab_PKI_211 GEM.R-CA<n> – Zentrale gematik Root-CA_nonQES der TI	115
4496	Tabelle 49: Tab_PKI_212 <tsp>.<usage>-CA<n> –Aussteller- CA_nonQES der TI	116
4497	Tabelle 50: Tab_PKI_253 C.GEM.OCSP Zertifikatsprofil OCSP-Signer	120
4498	Tabelle 51: Tab_PKI_214 C.GEM.CRL Zertifikatsprofil CRL-Signer.....	123
4499	Tabelle 52: Tab_PKI_252_01 C.TSL.SIG Zertifikatsprofil TSL-Signer	126
4500	Tabelle 53: Tab_PKI_254 Zugriffsprofile für eine Rollenauthentisierung	130
4501	Tabelle 54: Tab_PKI_255 Zugriffsprofile G2 für eine Authentisierung einer	
4502	Funktionseinheit.....	137
4503	Tabelle 55: Tab_PKI_266 Aufbau CAR für Karten der Generation 2	140
4504	Tabelle 56: Tab_PKI_901 Objektidentifizier des öffentlichen Schlüssels eines CV-Zertifikats	
4505	der Generation 2.....	142
4506	Tabelle 57: Tab_PKI_902 Punkt Q des öffentlichen Schlüssels eines CV-Zertifikats der	
4507	Generation 2	142
4508	Tabelle 58: Tab_PKI_258 Aufbau CHR.....	143

4509	Tabelle 59: Tab_PKI_904 Mögliche Objektidentifizier OID_{flags} in Certificate Holder	
4510	Authorization Templates.....	145
4511	Tabelle 60: Tab_PKI_905 Zu signierende Nachricht M eines CV-Zertifikates	146
4512	Tabelle 61: Tab_PKI_906 Signatur der Nachricht M eines CV-Zertifikats	146
4513	Tabelle 62: Tab_PKI_907 Struktur und Inhalt eines CV-Zertifikat	147
4514	Tabelle 63: Tab_PKI_912 CA CV-Zertifikate für 256 bit ELC-Schlüssel, insgesamt	
4515	220 Oktett	148
4516	Tabelle 64: Tab_PKI_913 CA CV-Zertifikate für 384 bit ELC-Schlüssel, insgesamt	
4517	285 Oktett	148
4518	Tabelle 65: Tab_PKI_914 CA CV-Zertifikate für 512 bit ELC-Schlüssel, insgesamt	
4519	352 Oktett	149
4520	Tabelle 66: Tab_PKI_937 Cross-CV-Zertifikat für ELC-Schlüssel	150
4521	Tabelle 67: Tab_PKI_915 Endnutzer-CV-Zertifikate für 256 bit ELC-Schlüssel, insgesamt	
4522	222 Oktett	151
4523	Tabelle 68: Tab_PKI_916 Endnutzer-CV-Zertifikate für 384 bit ELC-Schlüssel, insgesamt	
4524	287 Oktett	151
4525	Tabelle 69: Tab_PKI_917 Endnutzer-CV-Zertifikate für 512 bit ELC-Schlüssel, insgesamt	
4526	354 Oktett	152
4527	Tabelle 70: Tab_PKI_910 TI-PKI, Bedeutung der Bits innerhalb der Flagliste eines CHAT	
4528	153
4529	Tabelle 71: Tab_PKI_918 Abbildung von Rollenberechtigungen Zugriffsprofilen auf	
4530	äquivalente Flaglisten	155
4531	Tabelle 72: Tab_PKI_919 Sub-CA-Flaglisten nach Kartentyp (G2) und Zugriffsprofilen	156
4532	Tabelle 73: Tab_PKI_911 CMS-PKI, Bedeutung der Bits innerhalb der Flagliste eines	
4533	CHAT.....	157
4534	Tabelle 74: Tab_PKI_271 Erlaubte URIs als Inhalte des TSL-Elements ServiceStatus..	167
4535	Tabelle 75: TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“	168
4536	Tabelle 76: TUC_PKI_013 „Import neuer TI-Vertrauensanker“	174
4537	Tabelle 77: Gültige Werte für den TI-Vertrauensankerwechsel	179
4538	Tabelle 78: Beispiel für den TSL-Eintrag zum Wechsel des TSL-Signer-CA-Zertifikats .	179
4539	Tabelle 79: TUC_PKI_017 „Lokalisierung Download-Adressen“	180
4540	Tabelle 80: Tab_PKI_272 Gültige Werte zur Download-Adresse.....	182
4541	Tabelle 81: TUC_PKI_016 „Download der TSL-Datei“	183
4542	Tabelle 82: TUC_PKI_019 „Prüfung der Aktualität der TSL“	187
4543	Tabelle 83: TUC_PKI_020 „XML-Dokument validieren“	193
4544	Tabelle 84: TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“	194
4545	Tabelle 85: TUC_PKI_012 „XML-Signatur- Prüfung“	197
4546	Tabelle 86: Tab_PKI_294 TSL Zeitparameter.....	199
4547	Tabelle 87: TUC_PKI_018 „Zertifikatsprüfung in der TI“	201

4548	Tabelle 88: TUC_PKI_002 „Gültigkeitsprüfung des Zertifikats“	208
4549	Tabelle 89: TUC_PKI_003 „CA-Zertifikat in TSL-Informationen finden“	210
4550	Tabelle 90: TUC_PKI_004 „Mathematische Prüfung der Zertifikatssignatur“	213
4551	Tabelle 91: TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln“	216
4552	Tabelle 92: TUC_PKI_006 „OCSP-Abfrage“	218
4553	Tabelle 93: TUC_PKI_021 „CRL-Prüfung“	226
4554	Tabelle 94: TUC_PKI_009 „Rollenermittlung“	233
4555	Tabelle 95 : TUC_PKI_007 „Prüfung Zertifikatstyp“	236
4556	Tabelle 96: Tab_PKI_273 Prüfparameter für TLS-Aufbau	241
4557	Tabelle 97: TUC_PKI_030 „QES-Zertifikatsprüfung“	243
4558	Tabelle 98: TUC_PKI_036 „BNetzA-VL Aktualisierung“	252
4559	Tabelle 99: Tab_PKI_274 Fehlercodes des SubCompTyps PKI bei TSL- und	
4560	Zertifikatsprüfung	256
4561	Tabelle 100: Tab_PKI_908 Prüfung der Signatur eines CV-Zertifikats der Generation 2	
4562	mit Hilfe des CV-Zertifikats des Herausgebers	265
4563	Tabelle 101: Tab_PKI_909 Gültigkeit eines CV-Zertifikats der Generation 2	266
4564	Tabelle 102: Tab_PKI_290 Struktur certID in OCSP-Request/Response	269
4565	Tabelle 103: Tab_PKI_289 Struktur Nonce	270
4566	Tabelle 104: Tab_PKI_291 OCSP-Response Status Ergebnisse	272
4567	Tabelle 105: Tab_PKI_292 Zeiten in einer OCSP-Response	272
4568	Tabelle 106: Tab_PKI_293 Status der OCSP Antworten	274
4569	Tabelle 107: Tab_PKI_288 Struktur certHash	275
4570	Tabelle 108: Tab_SMCB_KZBV_ZA SMC-B-Zertifikate für Zahnarzt (Sektor KZBV)	276
4571	Tabelle 109: Tab_SMCB_KV-T SMC-B-Zertifikate für Sektoren der KBV	278
4572	Tabelle 110: Tab_SMCB_DKTIG SMC-B-Zertifikate für Sektor der DKTIG	280
4573	Tabelle 111: Tab_SMCB_TID_DKTIG Aufbau Telematik-ID in SMC-B-Zertifikaten der	
4574	DKTIG	282
4575	Tabelle 112: Tab_SMCB_KTR SMC-B-Zertifikate für Mitarbeiter Kostenträger	283
4576	Tabelle 113: Tab_SMCB_TID_GKVSV Aufbau Telematik-ID in SMC-B-Zertifikaten des	
4577	GKV-SV	285
4578	Tabelle 114: Tab_SMCB_BAK SMC-B-Zertifikate für Apotheker	285
4579	Tabelle 115: Tab_SMCB_TID_BAK Aufbau Telematik-ID in SMC-B-Zertifikaten der	
4580	Apotheker	287
4581	Tabelle 116: Tab_SMCB_ADV_KTR SMC-B-Zertifikate für die AdV-Umgebung im Auftrag	
4582	der Kostenträger	287
4583	Tabelle 117: Tab_SMCB_ORG_Gen - Generisches Zertifikatsprofil für die SMC-B-ORG	289
4584	Tabelle 118: Tab_PKI_286 Generisches Zertifikatsprofil für die SMC-B - Weitere	
4585	Leistungserbringerinstitution	291

Tabelle 119: Tab_PKI_288 Generisches Zertifikatsprofil für die SMC-B - Weitere Ärztliche Institutionen.....	294
Tabelle 120: Tab_HBA_BÄK HBA-Zertifikate (AUT, ENC, QES) für BÄK	317
Tabelle 121: Tab_HBA_BZÄK HBA-Zertifikate (AUT, ENC, QES) für BZÄK	319
Tabelle 122: Tab_HBA_BPtK HBA-Zertifikate (AUT, ENC, QES) für BPtK	321
Tabelle 123: Tab_HBA_BAK HBA-Zertifikate (AUT, ENC, QES) für Apotheker.....	323
Tabelle 124: Tab_PKI_285 Generisches Zertifikatsprofil (C.HP.AUT, C.HP.ENC, C.HP.QES) für BA - Weitere Leistungserbringer.....	326

11.5 Referenzierte Dokumente

11.5.1 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 jeweils gültige Versionsnummern sind in der aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar
[gemKPT_Arch_TIP]	gematik: Architektur der TI-Plattform
[gemKPT_PKI_TIP]	gematik: Konzept PKI der TI-Plattform
[gemRL_TSL_SP_CP]	gematik: Certificate Policy - Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL
[gemSpec_COS]	gematik: Spezifikation des Card Operating System (COS), Elektrische Schnittstelle
[gemSpec_CVC_Root]	gematik: Spezifikation CVC-Root
[gemSpec_Krypt]	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_OID]	gematik: Spezifikation Festlegung von OIDs

[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_TSL]	gematik: Spezifikation TSL-Dienst

4606

11.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ALGCAT] SOG-IS]	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“) SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms. Version 1.1, June 2018. https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.1.pdf
[BSI-TR-03110]	BSI, Advanced Security Mechanisms for Machine Readable Travel Documents, Version 2.10, 20.03.2012 https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03110/index_hm.html
[BSI-TR-03111]	BSI (2012): Elliptic Curve Cryptography, Version 2.0 https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03111/index_hm.html
[Common - PKI] [BSI-CC-PP-0098]	T7 & TeleTrust (20.01.2009): Common PKI Spezifikation, Version 2.0 http://www.t7ev.org/themen/entwickler/common-pki-v20-spezifikation.htm BSI (03.07.2019): Common Criteria Schutzprofil (Protection Profile) Schutzprofil 2: Anforderungen an den Konnektor. Version 1.4
[CP-HPC]	Bundesapothekerkammer, Bundesärztekammer et al (06.11.2012):, Bundespsychotherapeutenkammer, Bundeszahnärztekammer (24.09.2018): Gemeinsame Policy für die Ausgabe der HPCHeilberufsausweise – Zertifikatsrichtlinie HPCHeilberufsausweis (Version 12.0.50) http://www.bundesaerztekammer.de/downloads/CP_HPC_v1.0.5.pdf https://www.abda.de/fileadmin/user_upload/assets/Telematik/CP_HPC_v2.0.0.pdf
[DIN5008]	DIN 5008 (2005): Schreib- und Gestaltungsregeln für die Textverarbeitung

[eIDAS]	Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
[EN 14890-1]	EN 14890-1 (Draft: February 2007) Application Interface for smart cards used as secure signature Creation Devices - Part 1: Basic services
[ETSI EN 319 412-1]	ETSI (Februar 2016): ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Overview and common data structures, Version 1.1.1
[ETSI EN 319 412-2]	ETSI (Februar 2016): ETSI EN 319 412-2 V2.1.1 'Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons', Version 2.1.1
[ETSI EN 319 412-5]	ETSI (2017-11): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.
[ETSI TS 102 231 v3.1.2]	ETSI (Dezember 2009): ETSI Technical Specification TS 102 231 ('Provision of harmonized Trust Service Provider (TSP) status information') Version 3.1.2
[ETSI TS 119 612]	ETSI (July 2015): ETSI TS 119 612 V2.1.1 'Electronic Signatures and Infrastructures (ESI); Trusted Lists', Version 2.1.1
[ETSI EN 119 001]	ETSI (2016-03): Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations, Version 1.2.1
[ETSI EN 319 102-1]	ETSI (2016-05): Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation, Version 1.1.1
[ETSI TS 119 172-4]	ETSI (2019-08-04): ETSI TS 119 172-4 V0.0.4b (2017-06) Final draft for approval 'Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists', Version 0.0.7
[FIPS 180 -4]	Federal Information Processing Standards Publication 180-4 Secure Hash Standard (SHS), March 2012 http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf
[ISO/IEC 9594-2]	ISO/IEC 9594-2:2008-12 Information technology - Open Systems Interconnection - The Directory: Models

[ISO3166-1]	ISO/IEC 3166-1:1997 Codes for the representations of names of countries – Part 1: Country codes
[ISO8859-1]	ISO/IEC 8859-1 (1998): Information technology - 8-bit single-byte coded graphic character sets - Part 1: Latin alphabet No. 1
[ISO9796-2]	ISO9796-2: 2002 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://tools.ietf.org/html/rfc2109
[RFC2560]	RFC 2560 (Juni 1999): X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP http://tools.ietf.org/html/rfc2560
[RFC3629]	RFC 3629 (November 2003): UTF-8, a transformation format of ISO 10646 http://tools.ietf.org/html/rfc3629
[RFC3739]	RFC 3739 (March 2004): Internet X.509 Public Key Infrastructure Qualified Certificates Profile http://tools.ietf.org/html/rfc3739
[RFC4514]	RFC 4514 (Juni 2006): Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names http://tools.ietf.org/html/rfc4514
[RFC5019]	RFC 5019 (September 2007): The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments http://tools.ietf.org/html/rfc5019
[RFC5280]	RFC 5280 (Mai 2008): Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile http://tools.ietf.org/html/rfc5280
[RFC6960]	RFC 6960 (Juni 2013): X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP https://tools.ietf.org/html/rfc6960
[RFC5754]	RFC5754 (Jan. 2010): Using SHA2 Algorithms with Cryptographic Message Syntax https://tools.ietf.org/html/rfc5754

[RFC3370]	RFC3370 (August 2002): Cryptographic Message Syntax (CMS) Algorithms https://tools.ietf.org/html/rfc3370
[SGB V]	BGBI. I S.2477 (20.12.1988): Sozialgesetzbuch, Fünftes Buch Zuletzt geändert durch Art. 4 G v. 14.4.2010 I 410 Gesetzliche Krankenversicherung
[VDG]	"Vertrauensdienstegesetz vom 18. Juli 2017 (BGBl. I S. 2745), das durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist" Stand: Geändert durch Art. 2 G v. 18.7.2017 I 2745 https://www.gesetze-im-internet.de/vdg/BJNR274510017.html
[X.509]	ITU-T X.509 (10/2019): SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY, Directory, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks http://www.itu.int/rec/T-REC-X.509/
[X.520]	ITU-T X.520 (10/2012): SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY, Directory, Information technology – Open Systems Interconnection – The Directory: Selected attribute types http://www.itu.int/rec/T-REC-X.520/
[X.521]	ITU-T X.521 (10/2012): SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY, Directory, Information technology – Open Systems Interconnection – The Directory: Selected object classes http://www.itu.int/rec/T-REC-X.521/
[XML]	World Wide Web Consortium (2006): Extensible Markup Language (XML) 1.0 http://www.w3.org/TR/REC-xml/
[XAdES]	ETSI (2010-12): ETSI TS 101 903 V1.4.2 (2010-12) Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES), Version 1.4.2
[XMLSig]	W3C Recommendation: XML-Signature Syntax and Processing http://www.w3.org/TR/xmlsig-core/

12 Anhang C – Sektorspezifische Ausprägungen der HBA Zertifikate

Die nachfolgenden Profiltabellen der Sektoren referenzieren auf die Festlegungen aus Kap. 5.2.1 für alle sektorübergreifenden Attribute und ergänzen/ersetzen diese um sektorspezifische Ausprägungen.

Die Profiltabellen gelten einheitlich für die Zertifikate:

- C.HP.AUT
- C.HP.ENC
- C.HP.QES

12.1 BÄK

Tabelle 120: Tab_HBA_BÄK HBA-Zertifikate (AUT, ENC, QES) für BÄK

Element		Inhalt	Kar.	
certificate		C.HP.AUT, C.HP.ENC, C.HP.QES		
	tbsCertificate			
	version	siehe Kap. 5.2.1		
	serialNumber	siehe Kap. 5.2.1		
	signature	siehe Kap. 5.2.1		
	issuer	siehe Kap. 5.2.1		
	validity	siehe Kap. 5.2.1		
	subject			
	commonName	siehe Kap. 5.2.1		
	title	siehe Kap. 5.2.1		
	givenName	siehe Kap. 5.2.1		
	surName	siehe Kap. 5.2.1		
	serialNumber	siehe Kap. 5.2.1		
	organizationalUnitName	siehe Kap. 5.2.1		

			organizationName	siehe Kap. 5.2.1		
			countryName	siehe Kap. 5.2.1		
			andere Attribute	siehe Kap. 5.2.1		
			subjectPublicKeyInfo	siehe Kap. 5.2.1		
			extensions			critical
			SubjectKeyIdentifier {2 5 29 14}	siehe Kap. 5.2.1		FALSE
			KeyUsage {2 5 29 15}	siehe Kap. 5.2.1		TRUE
			SubjectAltNames {2 5 29 17}	siehe Kap. 5.2.1		FALSE
			BasicConstraints {2 5 29 19}	siehe Kap. 5.2.1		TRUE
			CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = http://www.e- arzteausweis.de/ policies/EE_policy.html policyIdentifier = Zertifikatstyp-OID gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <id-etsi-qcp-natural- qscd> {0.4.0.194112.1.2} (nur für QES) policyIdentifier = 1.3.6.1.4.1.42675.1.1: CPME European eID-Policy for Physicans policyIdentifier = <OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP- spezifischen Zertifikatsrichtlinie	1 0-1 1 (1) 1 0-1 0-1	FALSE
			CRLDistributionPoints {2 5 29 31}	siehe Kap. 5.2.1		FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap. 5.2.1		FALSE
			AuthorityKeyIdentifier {2 5 29 35}	siehe Kap. 5.2.1		FALSE
			Admission {1 3 36 8 3 3}	admissionAuthority = {O=<zuständige bestätigende Ärztekammer>,C=DE} professionItem = „Ärztin/Arzt“ (siehe [gemSpec_OID#GS-A_4442]) professionOID = <oid_arzt> (siehe [gemSpec_OID#GS-A_4442]) registrationNumber = Telematik-ID des Inhabers	1 1 1 1	FALSE

	ExtendedKeyUsage {2 5 29 37}	siehe Kap. 5.2.1		FALSE
	ValidityModel {1 3 6 1 4 1 8301 3 5}	siehe Kap. 5.2.1		FALSE
	QCStatements {1 3 6 1 5 5 7 1 3}	siehe Kap. 5.2.1		FALSE
	additionalInformation {1 3 36 8 3 15}	siehe Kap. 5.2.1		FALSE
	Restriction {1 3 36 8 3 8}	siehe Kap. 5.2.1		FALSE
	andere Erweiterungen	siehe Kap. 5.2.1		
signatureAlgorithm		siehe Kap. 5.2.1		
signature		siehe Kap. 5.2.1		

4618
4619

4620 12.2 BZÄK

4621 **Tabelle 121: Tab_HBA_BZÄK HBA-Zertifikate (AUT, ENC, QES) für BZÄK**

Element		Inhalt *)	Kar.	
certificate		C.HP.AUT, C.HP.ENC, C.HP.QES		
	tbsCertificate			
	version	siehe Kap. 5.2.1		
	serialNumber	siehe Kap. 5.2.1		
	signature	siehe Kap. 5.2.1		
	issuer	siehe Kap. 5.2.1		
	validity	siehe Kap. 5.2.1		
	subject			
	commonName	siehe Kap. 5.2.1		
	title	siehe Kap. 5.2.1		
	givenName	siehe Kap. 5.2.1		
	surName	siehe Kap. 5.2.1		

			serialNumber	siehe Kap. 5.2.1		
			organizationalUnitName	siehe Kap. 5.2.1		
			organizationName	siehe Kap. 5.2.1		
			countryName	siehe Kap. 5.2.1		
			andere Attribute	siehe Kap. 5.2.1		
			subjectPublicKeyInfo	siehe Kap. 5.2.1		
			extensions			critical
			SubjectKeyIdentifier {2 5 29 14}	siehe Kap. 5.2.1		FALSE
			KeyUsage {2 5 29 15}	siehe Kap. 5.2.1		TRUE
			SubjectAltNames {2 5 29 17}	siehe Kap. 5.2.1		FALSE
			BasicConstraints {2 5 29 19}	siehe Kap. 5.2.1		TRUE
			CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = http://policies.bzaek.de policyIdentifier = Zertifikatstyp-OID gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <id-etsi-qcp-natural- qscd> {0.4.0.194112.1.2} (nur für QES) policyIdentifier = <OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP- spezifischen Zertifikatsrichtlinie	1 0-1 1 (1) 0-1 0-1	FALSE
			CRLDistributionPoints {2 5 29 31}	CDP der ausstellenden CA für AUT und ENC zwingend, ... für QES optional	1 0-1	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap. 5.2.1		FALSE
			AuthorityKeyIdentifier {2 5 29 35}	siehe Kap. 5.2.1		FALSE
			Admission {1 3 36 8 3 3}	admissionAuthority = {O=< zuständige Landeszahnärztekammer>,C=DE} professionItem = „Zahnärztin/Zahnarzt“ (siehe [gemSpec_OID#GS-A_4442]) professionOID = <oid_zahnarzt> (siehe [gemSpec_OID#GS-A_4442])	1 1 1	FALSE

			registrationNumber = Telematik-ID des Inhabers	1	
		ExtendedKeyUsage {2 5 29 37}	siehe Kap. 5.2.1		FALSE
		ValidityModel {1 3 6 1 4 1 8301 3 5}	siehe Kap. 5.2.1		FALSE
		QCStatements {1 3 6 1 5 5 7 1 3}	siehe Kap. 5.2.1		FALSE
		additionalInformation {1 3 36 8 3 15}	siehe Kap. 5.2.1		FALSE
		Restriction {1 3 36 8 3 8}	siehe Kap. 5.2.1		FALSE
		andere Erweiterungen	siehe Kap. 5.2.1		
		signatureAlgorithm	siehe Kap. 5.2.1		
		signature	siehe Kap. 5.2.1		

4622 **12.3 BPtK**

4623 **Tabelle 122: Tab_HBA_BPtK HBA-Zertifikate (AUT, ENC, QES) für BPtK**

Element		Inhalt *)	Kar.	
certificate		C.HP.AUT, C.HP.ENC, C.HP.QES		
	tbsCertificate			
	version	siehe Kap. 5.2.1		
	serialNumber	siehe Kap. 5.2.1		
	signature	siehe Kap. 5.2.1		
	issuer	siehe Kap. 5.2.1		
	validity	siehe Kap. 5.2.1		
	subject			
	commonName	siehe Kap. 5.2.1		
	title	siehe Kap. 5.2.1		
	givenName	siehe Kap. 5.2.1		
	surName	siehe Kap. 5.2.1		

	serialNumber	siehe Kap. 5.2.1		
	organizationalUnitName	siehe Kap. 5.2.1		
	organizationName	siehe Kap. 5.2.1		
	countryName	siehe Kap. 5.2.1		
	andere Attribute	siehe Kap. 5.2.1		
	subjectPublicKeyInfo	siehe Kap. 5.2.1		
	extensions			critical
	SubjectKeyIdentifier {2 5 29 14}	siehe Kap. 5.2.1		FALSE
	KeyUsage {2 5 29 15}	siehe Kap. 5.2.1		TRUE
	SubjectAltNames {2 5 29 17}	siehe Kap. 5.2.1		FALSE
	BasicConstraints {2 5 29 19}	siehe Kap. 5.2.1		TRUE
	CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = http://www.e- psychotherapeu tenausweis.de/policies/EE_policy.html policyIdentifier = Zertifikatstyp-OID gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <id-etsi-qcp-natural-qscd> {0.4.0.194112.1.2} (nur für QES) policyIdentifier = <OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP- spezifischen Zertifikatsrichtlinie	1 0-1 1 (1) 0-1 0-1	FALSE
	CRLDistributionPoints {2 5 29 31}	siehe Kap. 5.2.1		FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap. 5.2.1		FALSE
	AuthorityKeyIdentifier {2 5 29 35}	siehe Kap. 5.2.1		FALSE
	Admission {1 3 36 8 3 3}	admissionAuthority = {O=<zuständige Landespsychotherapeutenkammer>,C=DE} Eine oder zwei professionInfo-Elemente bestehend aus: professionItem = „Psychotherapeut/-in“ oder professionItem = „Psychologische/-r	1 1-2	FALSE

		<p>Psychotherapeut/-in" und/oder professionItem = „Kinder- und Jugendlichenpsychotherapeut/-in" (siehe [gemSpec_OID#GS-A_4442]) professionOID = <oid_psychotherapeut> oder professionOID = <oid_ps_psychotherapeut> und/oder professionOID = <oid_kuj_psychotherapeut> (siehe [gemSpec_OID#GS-A_4442]) registrationNumber = Telematik-ID des Inhabers... ... für AUT und ENC zwingend, ... für QES optional (Diese muss dann in mindestens einem professionInfo-Element aufgeführt sein)</p>	1 0-1	
	ExtendedKeyUsage {2 5 29 37}	siehe Kap. 5.2.1		FALSE
	ValidityModel {1 3 6 1 4 1 8301 3 5}	siehe Kap. 5.2.1		FALSE
	QCStatements {1 3 6 1 5 5 7 1 3}	siehe Kap. 5.2.1		FALSE
	additionalInformation {1 3 36 8 3 15}	siehe Kap. 5.2.1		FALSE
	Restriction {1 3 36 8 3 8}	siehe Kap. 5.2.1		FALSE
	andere Erweiterungen	siehe Kap. 5.2.1		
	signatureAlgorithm	siehe Kap. 5.2.1		
	signature	siehe Kap. 5.2.1		

4624

4625 12.4 Apothekerschaft

4626 **Tabelle 123: Tab_HBA_BAK HBA-Zertifikate (AUT, ENC, QES) für Apotheker**

Element	Inhalt	Kar.	
certificate	C.HP.AUT, C.HP.ENC, C.HP.QES		
tbsCertificate			
version	siehe Kap. 5.2.1		
serialNumber	siehe Kap. 5.2.1		
signature	siehe Kap. 5.2.1		
issuer	siehe Kap. 5.2.1		

			validity	siehe Kap. 5.2.1		
			subject			
			commonName	siehe Kap. 5.2.1		
			title	siehe Kap. 5.2.1		
			givenName	siehe Kap. 5.2.1		
			surName	siehe Kap. 5.2.1		
			serialNumber	siehe Kap. 5.2.1		
			organizationalUnitName	siehe Kap. 5.2.1		
			organizationName	siehe Kap. 5.2.1		
			countryName	siehe Kap. 5.2.1		
			andere Attribute	siehe Kap. 5.2.1		
			subjectPublicKeyInfo	siehe Kap. 5.2.1		
			extensions			critical
			SubjectKeyIdentifier {2 5 29 14}	siehe Kap. 5.2.1		FALSE
			KeyUsage {2 5 29 15}	siehe Kap. 5.2.1		TRUE
			SubjectAltNames {2 5 29 17}	siehe Kap. 5.2.1		FALSE
			BasicConstraints {2 5 29 19}	siehe Kap. 5.2.1		TRUE
			CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = https://www.abda.de/themen/positionen- und-initiativen/telematik/hba/ policyIdentifier = Zertifikatstyp-OID gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <id-etsi-qcp-natural-qscd> {0.4.0.194112.1.2} (nur für QES) policyIdentifier = <OID der TSP-spezifischen Policy>	1 0-1 1 (1) 0-1 0-1	FALSE

		policyQualifierInfo = URL der TSP-spezifischen Zertifikatsrichtlinie		
	CRLDistributionPoints {2 5 29 31}	siehe Kap. 5.2.1		FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap. 5.2.1		FALSE
	AuthorityKeyIdentifier {2 5 29 35}	siehe Kap. 5.2.1		FALSE
	Admission {1 3 36 8 3 3}	<p>admissionAuthority = (O= <Apothekerkammer Bezeichnung>, C=DE)</p> <p>professionItem = Genau eine Beschreibung zu <oid_apotheker> bzw. <oid_apothekerassistent> bzw. <oid_pharmazieingenieur> bzw. <oid_apothekenassistent>. gemäß [gemSpec_OID#GS-A_4442]</p> <p>professionOID = Genau eine OID der Berufsgruppe <oid_apotheker> bzw. <oid_apothekerassistent> bzw. <oid_pharmazieingenieur> bzw. <oid_apothekenassistent> gemäß [gemSpec_OID#GS-A_4442]</p> <p>registrationNumber = Telematik-ID des Inhabers für AUT und ENC zwingend, ... für QES optional</p>	<p>1</p> <p>1</p> <p>1</p> <p>1</p> <p>0-1</p>	FALSE
	ExtendedKeyUsage {2 5 29 37}	siehe Kap. 5.2.1		FALSE
	additionalInformation	siehe Kap. 5.2.1		FALSE
	Restriction	siehe Kap. 5.2.1		FALSE
	andere Erweiterungen	siehe Kap. 5.2.1		
	signatureAlgorithm	siehe Kap. 5.2.1		
	signature	siehe Kap. 5.2.1		

12.5 Weitere Leistungserbringer

Tabelle 124: Tab_PKI_285 Generisches Zertifikatsprofil (C.HP.AUT, C.HP.ENC, C.HP.QES)
für BA - Weitere Leistungserbringer

Element		Inhalt	Kar.	
certificate		C.HP.AUT, C.HP.ENC, C.HP.QES		
	tbsCertificate			
	version	siehe Kap. 5.2.1		
	serialNumber	siehe Kap. 5.2.1		
	signature	siehe Kap. 5.2.1		
	issuer	siehe Kap. 5.2.1		
	validity	siehe Kap. 5.2.1		
	subject			
	commonName	siehe Kap. 5.2.1		
	title	siehe Kap. 5.2.1		
	givenName	siehe Kap. 5.2.1		
	surName	siehe Kap. 5.2.1		
	serialNumber	siehe Kap. 5.2.1		
	organizationalUnitName	siehe Kap. 5.2.1		
	organizationName	siehe Kap. 5.2.1		
	countryName	siehe Kap. 5.2.1		
	andere Attribute	siehe Kap. 5.2.1		
	subjectPublicKeyInfo	siehe Kap. 5.2.1		
	extensions			critical
	SubjectKeyIdentifier {2 5 29 14}	siehe Kap. 5.2.1		FALSE

	KeyUsage {2 5 29 15}	siehe Kap. 5.2.1		TRUE
	SubjectAltNames {2 5 29 17}	siehe Kap. 5.2.1		FALSE
	BasicConstraints {2 5 29 19}	siehe Kap. 5.2.1		TRUE
	CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = http://www.e- arztasweis.de/ policies/EE_policy.html policyIdentifier = Zertifikatstyp-OID gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <id-etsi-qcp-natural-qscd> {0.4.0.194112.1.2} (nur für QES) policyIdentifier = 1.3.6.1.4.1.42675.1.1: CPME European eID-Policy for Physicans policyIdentifier = <OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP- spezifischen Zertifikatsrichtlinie	1 0-1 1 (1) 1 0-1 0-1	FALSE
	CRLDistributionPoints {2 5 29 31}	siehe Kap. 5.2.1		FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap. 5.2.1		FALSE
	AuthorityKeyIdentifier {2 5 29 35}	siehe Kap. 5.2.1		FALSE
	Admission {1 3 36 8 3 3}	admissionAuthority = {O=<zuständige bestätigende Organisation>, C=DE} professionItem = Genau eine Beschreibung zu <oid_altenpfleger> bzw. <oid_pflegefachkraft> bzw. <oid_hebamme> bzw. <oid_physiotherapeut> bzw. <oid_augenoptiker> bzw. <oid_hoerakustiker> bzw. <oid_orthopaedieschuhmacher> bzw. <oid_orthopaedietechniker> bzw. <oid_zahntechniker> gemäß [gemSpec_OID#GS-A_4442] professionOID = Genau eine OID der Berufsgruppe: <oid_altenpfleger> bzw. <oid_pflegefachkraft> bzw. <oid_hebamme> bzw. <oid_physiotherapeut> bzw. <oid_augenoptiker> bzw. <oid_hoerakustiker> bzw. <oid_orthopaedieschuhmacher> bzw.	1 1 1	FALSE

			<p><oid_orthopaedietechniker> bzw. <oid_zahntechniker> gemäß [gemSpec_OID#GS-A_4442]</p> <p>registrationNumber = Telematik-ID des Inhabers gemäß Tab_PKI_101-01 (entsprechend dem Präfix 9, 10 oder 11)</p>		
		ExtendedKeyUsage {2 5 29 37}	siehe Kap. 5.2.1		FALSE
		ValidityModel {1 3 6 1 4 1 8301 3 5}	siehe Kap. 5.2.1		FALSE
		QCStatements {1 3 6 1 5 5 7 1 3}	siehe Kap. 5.2.1		FALSE
		additionalInformation {1 3 36 8 3 15}	siehe Kap. 5.2.1		FALSE
		Restriction {1 3 36 8 3 8}	siehe Kap. 5.2.1		FALSE
		andere Erweiterungen	siehe Kap. 5.2.1		
		signatureAlgorithm	siehe Kap. 5.2.1		
		signature	siehe Kap. 5.2.1		

4631