

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 Telematikinfrastuktur 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 Telematikinfrastuktur

Übergreifende Spezifikation Spezifikation PKI

Version: 2.8.01 CC
Revision: 198563238177
Stand: 02.0320.05.2020
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
2.8.01 CC	02.03.20.05.20		freigegebenEinarbeitung P21.3	gematik

ENTWURF

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	35
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	37
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	39
78	4.5.1 Typ und Exemplar der Organisation/Einrichtung des Gesundheitswesens	39
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	45
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	50
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	54
102	4.11 Kartenverlust und Deaktivierung von Chipkarten	56
103	5 X.509-Zertifikate	57
104	5.1 eGK – Versichertenkarte	57
105	5.1.1 Definition der Versichertenidentität	57
106	5.1.2 Belegung der Felder im SubjectDN	58
107	5.1.3 X.509-Zertifikatsprofile der eGK	59
108	5.1.3.1 C.CH.AUT und C.CH.AUT_ALT – Authentisierung eGK	59
109	5.1.3.2 C.CH.ENC – Verschlüsselung eGK	61
110	5.1.3.3 C.CH.QES – Qualifizierte Signatur eGK (optional)	63
111	5.1.3.4 C.CH.AUTN – Technische Authentisierung eGK	65
112	5.1.3.5 C.CH.ENCV – Technische Verschlüsselung eGK	66
113	5.2 HBA – Heilberufsausweis	68
114	5.2.1 X.509-Zertifikatsprofile des HBA	68

115	5.2.1.1 C.HP.AUT – Authentisierung HBA	68
116	5.2.1.2 C.HP.ENC – Verschlüsselung HBA	70
117	5.2.1.3 C.HP.QES – Qualifizierte Signatur HBA	72
118	5.3 SMC-B – Ausweis einer Organisation/Einrichtung des Gesundheitswesens	76
119	5.3.1 Definition der Organisationsidentität	76
120	5.3.2 Aufbau Anschriftzone nach [DIN5008]	77
121	5.3.3 Umgang mit überlangen Attributen im SubjectDN	78
122	5.3.4 X.509 Zertifikatsprofile der SMC-B	78
123	5.3.4.1 C.HCI.AUT – Authentisierung SMC-B	78
124	5.3.4.2 C.HCI.ENC – Verschlüsselung SMC-B	80
125	5.3.4.3 C.HCI.OSIG – Signatur SMC-B	82
126	5.4 HSM-B – Ausweis einer Organisation/Einrichtung des Gesundheitswesens	84
127	5.5 gSMC-KT – eHealth Kartenterminal	84
128	5.5.1 Definition der Kartenterminalidentität	84
129	5.5.2 X.509 Zertifikatsprofile der gSMC-KT	85
130	5.5.2.1 C.SMKT.AUT – Identität der gSMC-KT	85
131	5.6 gSMC-K – Konnektor	86
132	5.6.1 Definition und Zuweisung der Konnektoridentität	86
133	5.6.2 Aufbau des SubjectDN	87
134	5.6.3 Statusprüfung von Konnektorzertifikaten	87
135	5.6.4 X.509 Zertifikatsprofile des Konnektors	88
136	5.6.4.1 C.NK.VPN – VPN Authentisierung Netzkonnektor	88
137	5.6.4.2 C.AK.AUT – Authentisierung Anwendungskonnektor	89
138	5.6.4.3 C.SAK.AUT – Authentisierung Signaturdienst	91
139	5.7 VPN-Zugangsdienst	93
140	5.7.1 Definition und Zuweisung der Zugangsdienstidentitäten	93
141	5.7.2 Aufbau des SubjectDN	94
142	5.7.3 X.509 Zertifikatsprofile des Zugangsdienstes	94
143	5.7.3.1 C.VPNK.VPN – VPN Authentisierung Zugangsdienst TI	94
144	5.7.3.2 C.VPNK.VPN-SIS – VPN Authentisierung Zugangsdienst Sicherer Internetzugang	95
145	5.8 ZD – Zentrale Dienste	97
146	5.8.1 Definition der Identität der Zentralen Dienste	97
147	5.8.2 Aufbau des SubjectDN	97
148	5.8.3 X.509 Zertifikatsprofile der Zentralen Dienste	98
149	5.8.3.1 C.ZD.TLS-S Server Authentisierung (chemals C.SF.SSL-S)	98
150	5.9 FD – Fachanwendungsspezifische Dienste	99
151	5.9.1 Definition der Identität der Fachanwendungsspezifischen Dienste	99
152	5.9.2 Aufbau des SubjectDN	100
153	5.9.3 X.509 Zertifikatsprofile der Fachanwendungsspezifischen Dienste	100
154	5.9.3.1 C.FD.TLS-C Client Authentisierung (chemals C.SF.SSL-C)	100
155	5.9.3.2 C.FD.TLS-S Server Authentisierung (chemals C.SF.SSL-S)	102
156	5.9.3.3 C.FD.SIG Signatur Fachdienst	103
157	5.9.3.4 C.FD.AUT Authentisierung Fachdienst	105
158	5.9.3.5 C.FD.ENC Verschlüsselung Fachdienst	107
159	5.10 CM – Clientmodul	108
160	5.10.1 Definition der Identität eines Clientmoduls	108
161	5.10.2 Aufbau des SubjectDN	109

165	5.10.3 X.509 Zertifikatsprofil des Clientmoduls	109
166	5.10.3.1 C.CM.TLS-CS Clientmodul Authentisierung	109
167	5.11 SGD-HSM – Schlüsselgenerierungsdienst-HSM	111
168	5.11.1 Beschreibung der Identität	111
169	5.11.2 X.509 Zertifikatsprofil der SGD-HSM	111
170	5.12 CA – Zertifikatsprofile	113
171	5.12.1 GEM.RCA<n> – Zentrale Root CA_nonQES	113
172	5.12.2 <tsp>. <usage> CA<n> – Aussteller CA_nonQES	115
173	5.12.3 <tsp>.HBA-qCA<n> – Aussteller CA_QES	117
174	5.13 OCSP – Statusauskunftsdienst	119
175	5.13.1 Definition der OCSP-Signer-Identität	119
176	5.13.2 Aufbau des SubjectDN	119
177	5.13.3 X.509-Profil des OCSP-Signer-Zertifikates	119
178	5.13.3.1 C.GEM.OCSP-OCSP-Signer-Zertifikat	119
179	5.14 CRL – Statusauskunftsdienst	121
180	5.14.1 Definition der CRL-Signer-Identität	121
181	5.14.2 Aufbau des SubjectDN	121
182	5.14.3 X.509-Profil des CRL-Signer-Zertifikates	122
183	5.14.3.1 C.GEM.CRL-CRL-Signaturzertifikat	122
184	5.15 TSL – Zertifikatsprofile	123
185	5.15.1 Definition der TSL-Signer-Identität	123
186	5.15.2 Aufbau des SubjectDN	123
187	5.15.3 X.509-Zertifikatsprofil der TSL-Signer-CA	123
188	5.15.4 TSL-Signer-Zertifikat	124
189	5.15.5 TSL-OCSP-Responder-Zertifikat	126
190	6 CV-Zertifikate	127
191	6.1 Festlegungen zur Abgrenzung	127
192	6.2 Namensregeln und -formate	127
193	6.3 Rollen und Profile	128
194	6.3.1 Rollenauthentisierung	128
195	6.3.2 Authentisierung einer Funktionseinheit	134
196	6.4 CV-Zertifikatsprofile der Generation 2	135
197	6.4.1 Berechtigung einer CVC-CA zur Zertifikatserstellung	135
198	6.4.2 Aufbau und Bestandteile der CV-Zertifikate der Generation 2	136
199	6.4.3 Zertifikatsprofil eines CV-Zertifikates für ELC-Schlüssel	137
200	6.4.3.1 Certificate Profile Identifier (CPI)	137
201	6.4.3.2 Certification Authority Reference (CAR)	137
202	6.4.3.3 Öffentlicher Schlüssel	138
203	6.4.3.4 Certificate Holder Reference (CHR)	139
204	6.4.3.5 Certificate Holder Authorization Template (CHAT)	141
205	6.4.3.6 Certificate Effective Date (CED)	142
206	6.4.3.7 Certificate Expiration Date (CXD)	142
207	6.4.3.8 Zu signierende Nachricht M eines CV-Zertifikates der Generation 2	142
208	6.4.4 Struktur und Inhalt eines CV-Zertifikates für ELC-Schlüssel der Generation 2	143
209	143
210	6.4.5 Struktur und Inhalt eines CV-Zertifikates für ELC-Schlüssel der Generation 2	144
211	144
212	6.4.5.1 Struktur und Inhalt von CA-CV-Zertifikaten für ELC-Schlüssel	144

213	6.4.5.2 Struktur und Inhalt von Cross-CV-Zertifikaten für ELC-Schlüssel.....	146
214	6.4.5.3 Struktur und Inhalt von Endnutzer-CV-Zertifikaten für ELC-Schlüssel...	147
215	6.4.6 Flagliste mit Berechtigungen in CV-Zertifikaten für ELC-Schlüssel.....	149
216	7 Festlegung von OIDs.....	155
217	8 Prüfung von Zertifikaten.....	156
218	8.1 Vertrauensraum der TI.....	158
219	8.1.1 TSL im Kontext der ECC-Migration.....	159
220	8.1.2 Initialisierung TI-Vertrauensraum.....	160
221	8.1.2.1 TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“.....	164
222	8.1.3 Geplanter Wechsel TI-Vertrauensanker.....	171
223	8.1.3.1 TUC_PKI_013 „Import TI-Vertrauensanker aus TSL“.....	171
224	8.1.3.2 TSL-Einträge für die Bereitstellung neuer TI-Vertrauensanker.....	175
225	8.1.3.3 Prüfung der TSL nach Wechsel des TI-Vertrauensanker.....	177
226	8.1.4 Ungeplanter Wechsel des TI-Vertrauensanker.....	178
227	8.2 TSL-Prüfung.....	178
228	8.2.1 Erreichbarkeit und Download der TSL.....	178
229	8.2.1.1 TUC_PKI_017 „Lokalisierung TSL-Download-Adressen“.....	178
230	8.2.1.2 TUC_PKI_016 „Download der TSL-Datei“.....	180
231	8.2.2 Vertrauensstatus und Authentifizieren der TSL.....	183
232	8.2.2.1 TUC_PKI_019 „Prüfung der Aktualität der TSL“.....	183
233	8.2.2.2 TUC_PKI_020 „XML-Dokument validieren“.....	191
234	8.2.2.3 TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“.....	192
235	8.2.2.4 TUC_PKI_012 „XML-Signatur-Prüfung“.....	196
236	8.2.3 TSL-Sicherheitsaspekte.....	197
237	8.2.4 TSL-Zeitparameter.....	198
238	8.2.5 ServiceTypeIdentifier „unspecified“.....	198
239	8.3 Zertifikatsprüfung X.509-nonQES.....	199
240	8.3.1 Zertifikatsprüfung in der TI.....	200
241	8.3.1.1 TUC_PKI_018 „Zertifikatsprüfung in der TI“.....	200
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.....	231
250	8.3.2.5 Statusprüfung von eGK-Zertifikaten.....	231
251	8.3.3 Ermittlung von Autorisierungsinformationen.....	231
252	8.3.3.1 Bestätigte Zertifikatsinformationen.....	231
253	8.3.3.2 TUC_PKI_009 „Rollenermittlung“.....	231
254	8.3.3.3 TUC_PKI_007 „Prüfung Zertifikatstyp“.....	234
255	8.3.4 Weitere Prüfungen.....	240
256	8.3.4.1 Umgang mit kritischen Extensions.....	240
257	8.4 Überprüfung der Zertifikate auf Netzwerk- und Transportebene.....	240
258	8.4.1 TLS-Verbindungsaufbau.....	240
259	8.4.2 IPsec-Verbindungsaufbau.....	241
260	8.5 Zertifikatsprüfung X.509-QES.....	241
261	8.5.1 TUC_PKI_030 „QES-Zertifikatsprüfung“.....	242

262	8.5.2 TUC_PKI_036 „BNetzA-VL Aktualisierung“	246
263	8.6 Fehlercodes bei TLS- und Zertifikatsprüfung X.509	250
264	8.7 Zertifikatsprüfung CV-Zertifikate der 2. Generation	259
265	9 OCSP-Statusinformation	262
266	9.1 Statusprüfung	262
267	9.1.1 Schnittstelle I-OCSP-Status-Information	262
268	9.1.1.1 Schnittstellendefinition	263
269	9.1.1.1.1 OCSP-Request	263
270	9.1.1.1.2 OCSP-Response	264
271	9.1.1.2 Umsetzung	264
272	9.1.1.3 Nutzung	265
273	9.1.2 Artefakte	265
274	9.1.2.1 OCSP-Response-Response-Status	265
275	9.1.2.2 OCSP-Response-Zeiten	266
276	9.1.2.3 OCSP-Response-CertStatus	267
277	9.1.2.4 OCSP-Response-CertID	268
278	9.1.2.5 OCSP-Response-Sperrzeitpunkt und Sperrgrund	268
279	9.1.2.6 OCSP-Response-CertHash	268
280	9.1.3 Testunterstützung	268
281	9.1.4 Hardwaremerkmale	268
282	10 Anhang A – Sektorspezifische Ausprägungen der SMC-B-	
283	Zertifikate	269
284	10.1 KZBV	269
285	10.2 KBV	271
286	10.3 DKG	273
287	10.4 GKV-Spitzenverband	275
288	10.5 Apothekerschaft	278
289	10.6 AdV-Umgebung im Auftrag der Kostenträger	280
290	10.7 SMC-B-ORG	281
291	11 Anhang B – Verzeichnisse	285
292	11.1 Abkürzungen	285
293	11.2 Glossar	290
294	11.3 Abbildungsverzeichnis	290
295	11.4 Tabellenverzeichnis	292
296	11.5 Referenzierte Dokumente	300
297	11.5.1 Dokumente der gematik	300
298	11.5.2 Weitere Dokumente	300
299	12 Anhang C – Sektorspezifische Ausprägungen der HBA	
300	Zertifikate	305
301	12.1 BÄK	305

302	12.2 BZÄK	307
303	12.3 BPtK	309
304	12.4 Apothekerschaft	311
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	2 Notation kryptographischer Objekte	19
312	2.1 Basis-Bezeichner	19
313	2.2 Optionale Bezeichnung der technischen Ausprägung	19
314	2.3 Optionales Unterscheidungsmerkmal bei gleicher technischer Ausprägung	
315	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	3 CA-Strukturen	28
326	3.1 Übergreifende Festlegung für CA der TI	28
327	3.1.1 Übersicht der Identitäten/Zertifikate	28
328	3.1.2 Laufzeiten der CA	28
329	3.1.3 Unterstützung verschiedener Schlüsselgenerationen	28
330	3.2 TI-Betriebsumgebungen	29
331	3.2.1 PKI-Sicht auf die Produktivumgebung	30
332	3.2.2 PKI-Sicht auf Test- u. Referenzumgebung (PKI-TeRe)	30
333	3.2.3 Pseudo-QES PKI in Test- u. Referenzumgebung	31
334	3.3 Zentrale Aussteller-CAs in der TI für nonQES-Zertifikate	31
335	3.4 Spezifische Aussteller-CA in der TI	32
336	4 Kodierung von X.509-Identitäten	34
337	4.1 Namensregeln und -formate	34
338	4.1.1 Verarbeitung von Sonderzeichen	34
339	4.1.2 Definition der Subject-DNs für Personen und Komponenten	34

340	4.1.3 SubjectDN von CA-Zertifikaten und von OCSP-Responder-Zertifikaten	34
341	4.2 Schlüssel der Versichertenidentität (eGK)	35
342	4.3 Pseudonym der Versichertenidentität (eGK)	35
343	4.3.1 Versicherten-Pseudonym in X.509-Zertifikaten der eGK	35
344	4.3.2 Eindeutigkeit des Pseudonym.....	35
345	4.3.3 Pseudonym-Erstellungsregel	36
346	4.3.4 Hs-ZW – Herausgeberspezifischer Zufallswert (hs-ZW)	37
347	4.3.5 Kodierung des Pseudonyms	37
348	4.4 Berufsgruppen-ID der Leistungserbringer	39
349	4.4.1 Berufsgruppe des Heilberufers.....	39
350	4.5 ID der Organisation/Einrichtung des Gesundheitswesens.....	39
351	4.5.1 Typ und Exemplar der Organisation/Einrichtung des Gesundheitswesens.....	39
352	4.6 Technische Rolle von Komponenten und Diensten.....	40
353	4.6.1 Technische Rolle im Komponentenzertifikat.....	40
354	4.7 Telematik-ID	41
355	4.7.1 Abbildung der Telematik-ID im X.509-Zertifikat	41
356	4.7.2 Aufbau der Telematik-ID	42
357	4.7.2.1 Sektoraler Präfix	42
358	4.7.2.2 Separator.....	43
359	4.7.2.3 Fortsatz der Telematik-ID.....	43
360	4.8 Kodierung der Zertifikate	44
361	4.8.1 Kodierung der Attribute	44
362	4.8.2 Stringlänge der Attribute.....	45
363	4.8.3 Struktur.....	45
364	4.8.3.1 serialNumber	45
365	4.8.3.2 Admission	46
366	4.8.3.3 CertificatePolicies	48
367	4.8.3.4 CRLDistributionPoints.....	50
368	4.8.3.5 SubjectAltNames.....	50
369	4.9 Erläuterungen zu Zertifikatsprofilen	52
370	4.9.1 Allgemeine Erläuterungen	52
371	4.9.2 Berufs-/Rollenattribute und Sperrbarkeit	52
372	4.9.3 Benennung der Zertifikatsprofile	53
373	4.9.4 Distinguished Name.....	53
374	4.10 Kodierung der Betriebsumgebungen in Zertifikaten	54
375	4.11 Kartenverlust und Deaktivierung von Chipkarten	56
376	5 X.509-Zertifikate	57
377	5.1 eGK – Versichertenkarte.....	57
378	5.1.1 Definition der Versichertenidentität.....	57
379	5.1.2 Belegung der Felder im SubjectDN	58
380	5.1.3 X.509-Zertifikatsprofile der eGK	59
381	5.1.3.1 C.CH.AUT und C.CH.AUT_ALT – Authentisierung eGK.....	59
382	5.1.3.2 C.CH.ENC – Verschlüsselung eGK	61
383	5.1.3.3 C.CH.QES – Qualifizierte Signatur eGK (optional).....	63
384	5.1.3.4 C.CH.AUTN – Technische Authentisierung eGK	65
385	5.1.3.5 C.CH.ENCV – Technische Verschlüsselung eGK.....	66

5.2 HBA – Heilberufsausweis.....	68
5.2.1 X.509 Zertifikatsprofile des HBA	68
5.2.1.1 C.HP.AUT – Authentisierung HBA	68
5.2.1.2 C.HP.ENC – Verschlüsselung HBA	70
5.2.1.3 C.HP.QES – Qualifizierte Signatur HBA	72
5.3 SMC-B – Ausweis einer Organisation/Einrichtung des Gesundheitswesens	76
5.3.1 Definition der Organisationsidentität	76
5.3.2 Aufbau Anschriftzone nach [DIN5008]	77
5.3.3 Umgang mit überlangen Attributen im SubjectDN	78
5.3.4 X.509 Zertifikatsprofile der SMC-B	78
5.3.4.1 C.HCI.AUT – Authentisierung SMC- B	78
5.3.4.2 C.HCI.ENC – Verschlüsselung SMC-B	80
5.3.4.3 C.HCI.OSIG – Signatur SMC-B	82
5.4 HSM-B – Ausweis einer Organisation/Einrichtung des Gesundheitswesens	84
5.5 gSMC-KT – eHealth-Kartenterminal	84
5.5.1 Definition der Kartenterminalidentität	84
5.5.2 X.509 Zertifikatsprofile der gSMC-KT	85
5.5.2.1 C.SMKT.AUT – Identität der gSMC-KT	85
5.6 gSMC-K – Konnektor	86
5.6.1 Definition und Zuweisung der Konnektoridentität	86
5.6.2 Aufbau des SubjectDN	87
5.6.3 Statusprüfung von Konnektorzertifikaten	87
5.6.4 X.509 Zertifikatsprofile des Konnektors	88
5.6.4.1 C.NK.VPN – VPN-Authentisierung Netzkonnektor	88
5.6.4.2 C.AK.AUT – Authentisierung Anwendungskonnektor	89
5.6.4.3 C.SAK.AUT – Authentisierung Signaturdienst	91
5.7 VPN-Zugangsdienst	93
5.7.1 Definition und Zuweisung der Zugangsdienstidentitäten	93
5.7.2 Aufbau des SubjectDN	94
5.7.3 X.509-Zertifikatsprofile des Zugangsdienstes	94
5.7.3.1 C.VPNK.VPN – VPN-Authentisierung Zugangsdienst TI	94
5.7.3.2 C.VPNK.VPN-SIS – VPN-Authentisierung Zugangsdienst Sicherer Internetzugang	95
5.8 ZD – Zentrale Dienste	97
5.8.1 Definition der Identität der Zentralen Dienste	97
5.8.2 Aufbau des SubjectDN	97
5.8.3 X.509 Zertifikatsprofile der Zentralen Dienste	98
5.8.3.1 C.ZD.TLS-S Server-Authentisierung (ehemals C.SF.SSL-S)	98
5.9 FD – Fachanwendungsspezifische Dienste	99
5.9.1 Definition der Identität der Fachanwendungsspezifischen Dienste	99
5.9.2 Aufbau des SubjectDN	100
5.9.3 X.509 Zertifikatsprofile der Fachanwendungsspezifischen Dienste	100
5.9.3.1 C.FD.TLS-C Client-Authentisierung (ehemals C.SF.SSL-C)	100
5.9.3.2 C.FD.TLS-S Server-Authentisierung (ehemals C.SF.SSL-S)	102
5.9.3.3 C.FD.SIG Signatur Fachdienst	103
5.9.3.4 C.FD.AUT Authentisierung Fachdienst	105
5.9.3.5 C.FD.ENC Verschlüsselung Fachdienst	107
5.10 CM – Clientmodul	108

436	5.10.1 Definition der Identität eines Clientmoduls	108
437	5.10.2 Aufbau des SubjectDN	109
438	5.10.3 X.509 Zertifikatsprofil des Clientmoduls	109
439	5.10.3.1 C.CM.TLS-CS Clientmodul-Authentisierung	109
440	5.11 SGD-HSM – Schlüsselgenerierungsdienst-HSM	111
441	5.11.1 Beschreibung der Identität	111
442	5.11.2 X.509 Zertifikatsprofil der SGD-HSM	111
443	5.12 CA - Zertifikatsprofile	113
444	5.12.1 GEM.RCA<n> - Zentrale Root-CA_nonQES	113
445	5.12.2 <tsp>.<usage>-CA<n> - Aussteller-CA_nonQES	115
446	5.12.3 <tsp>.HBA-qCA<n> - Aussteller-CA_QES	117
447	5.13 OCSP – Statusauskunftsdienst	119
448	5.13.1 Definition der OCSP-Signer-Identität	119
449	5.13.2 Aufbau des SubjectDN	119
450	5.13.3 X.509-Profil des OCSP-Signer-Zertifikates	119
451	5.13.3.1 C.GEM.OCSP OCSP-Signer-Zertifikat	119
452	5.14 CRL – Statusauskunftsdienst	121
453	5.14.1 Definition der CRL-Signer-Identität	121
454	5.14.2 Aufbau des SubjectDN	121
455	5.14.3 X.509 Profil des CRL-Signer-Zertifikates	122
456	5.14.3.1 C.GEM.CRL CRL-Signaturzertifikat	122
457	5.15 TSL - Zertifikatsprofile	123
458	5.15.1 Definition der TSL-Signer-Identität	123
459	5.15.2 Aufbau des SubjectDN	123
460	5.15.3 X.509 Zertifikatsprofil der TSL-Signer-CA	123
461	5.15.4 TSL-Signer- Zertifikat	124
462	5.15.5 TSL-OCSP-Responder-Zertifikat	126
463	6 CV-Zertifikate	127
464	6.1 Festlegungen zur Abgrenzung	127
465	6.2 Namensregeln und -formate	127
466	6.3 Rollen und Profile	128
467	6.3.1 Rollenauthentisierung	128
468	6.3.2 Authentisierung einer Funktionseinheit	134
469	6.4 CV-Zertifikatsprofile der Generation 2	135
470	6.4.1 Berechtigung einer CVC-CA zur Zertifikatserstellung	135
471	6.4.2 Aufbau und Bestandteile der CV-Zertifikate der Generation 2	136
472	6.4.3 Zertifikatsprofil eines CV-Zertifikates für ELC-Schlüssel	137
473	6.4.3.1 Certificate Profile Identifier (CPI)	137
474	6.4.3.2 Certification Authority Reference (CAR)	137
475	6.4.3.3 Öffentlicher Schlüssel	138
476	6.4.3.4 Certificate Holder Reference (CHR)	139
477	6.4.3.5 Certificate Holder Authorization Template (CHAT)	141
478	6.4.3.6 Certificate Effective Date (CED)	142
479	6.4.3.7 Certificate Expiration Date (CXD)	142
480	6.4.3.8 Zu signierende Nachricht M eines CV-Zertifikates der Generation 2	142
481	6.4.4 Struktur und Inhalt eines CV-Zertifikates für ELC-Schlüssel der Generation 2	143
482	

483	6.4.5 Struktur und Inhalt eines CV-Zertifikates für ELC-Schlüssel der Generation 2	
484	144
485	6.4.5.1 Struktur und Inhalt von CA CV-Zertifikaten für ELC-Schlüssel	144
486	6.4.5.2 Struktur und Inhalt von Cross-CV-Zertifikaten für ELC-Schlüssel	146
487	6.4.5.3 Struktur und Inhalt von Endnutzer-CV-Zertifikaten für ELC-Schlüssel...	147
488	6.4.6 Flagliste mit Berechtigungen in CV-Zertifikaten für ELC-Schlüssel.....	149
489	7 Festlegung von OIDs.....	155
490	8 Prüfung von Zertifikaten.....	156
491	8.1 Vertrauensraum der TI.....	158
492	8.1.1 TSL im Kontext der ECC-Migration	159
493	8.1.2 Initialisierung TI-Vertrauensraum	160
494	8.1.2.1 TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“.....	164
495	8.1.3 Geplanter Wechsel TI-Vertrauensanker	171
496	8.1.3.1 TUC_PKI_013 „Import TI-Vertrauensanker aus TSL“.....	171
497	8.1.3.2 TSL-Einträge für die Bereitstellung neuer TI-Vertrauensanker	175
498	8.1.3.3 Prüfung der TSL nach Wechsel des TI-Vertrauensanker.....	177
499	8.1.4 Ungeplanter Wechsel des TI-Vertrauensanker	178
500	8.2 TSL-Prüfung	178
501	8.2.1 Erreichbarkeit und Download der TSL.....	178
502	8.2.1.1 TUC_PKI_017 „Lokalisierung TSL Download-Adressen“	178
503	8.2.1.2 TUC_PKI_016 „Download der TSL-Datei“	180
504	8.2.2 Vertrauensstatus und Authentifizieren der TSL	183
505	8.2.2.1 TUC_PKI_019 „Prüfung der Aktualität der TSL“	183
506	8.2.2.2 TUC_PKI_020 „XML-Dokument validieren“	191
507	8.2.2.3 TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“	192
508	8.2.2.4 TUC_PKI_012 „XML-Signatur-Prüfung“	196
509	8.2.3 TSL-Sicherheitsaspekte.....	197
510	8.2.4 TSL-Zeitparameter	198
511	8.2.5 ServiceTypeIdentifier "unspecified"	198
512	8.3 Zertifikatsprüfung X.509 nonQES	199
513	8.3.1 Zertifikatsprüfung in der TI.....	200
514	8.3.1.1 TUC_PKI_018 „Zertifikatsprüfung in der TI“	200
515	8.3.1.2 TUC_PKI_002 „Gültigkeitsprüfung des Zertifikats“.....	208
516	8.3.1.3 TUC_PKI_003 „CA-Zertifikat in TSL-Informationen finden“.....	210
517	8.3.1.4 TUC_PKI_004 „Mathematische Prüfung der Zertifikatssignatur“	213
518	8.3.2 Statusprüfung	216
519	8.3.2.1 TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln“	216
520	8.3.2.2 TUC_PKI_006 „OCSP-Abfrage“	218
521	8.3.2.3 TUC_PKI_021 „CRL-Prüfung“.....	226
522	8.3.2.4 Szenarien für Offline und Timeout von OCSP	231
523	8.3.2.5 Statusprüfung von eGK-Zertifikaten	231
524	8.3.3 Ermittlung von Autorisierungsinformationen	231
525	8.3.3.1 Bestätigte Zertifikatsinformationen	231
526	8.3.3.2 TUC_PKI_009 „Rollenermittlung“	231
527	8.3.3.3 TUC_PKI_007 „Prüfung Zertifikatstyp“.....	234
528	8.3.4 Weitere Prüfungen	240
529	8.3.4.1 Umgang mit kritischen Extensions	240
530	8.4 Überprüfung der Zertifikate auf Netzwerk- und Transportebene	240
531	8.4.1 TLS-Verbindungsaufbau	240

532	8.4.2 IPsec-Verbindungsaufbau	241
533	8.5 Zertifikatsprüfung X.509 QES	241
534	8.5.1 TUC_PKI_030 „QES-Zertifikatsprüfung“	242
535	8.5.2 TUC_PKI_036 „BNetzA-VL Aktualisierung“	246
536	8.6 Fehlercodes bei TSL- und Zertifikatsprüfung X.509	250
537	8.7 Zertifikatsprüfung CV-Zertifikate der 2. Generation	259
538	9 OCSP-Statusinformation	262
539	9.1 Statusprüfung	262
540	9.1.1 Schnittstelle I_OCSP_Status_Information	262
541	9.1.1.1 Schnittstellendefinition	263
542	9.1.1.1.1 OCSP-Request	263
543	9.1.1.1.2 OCSP-Response	264
544	9.1.1.2 Umsetzung	264
545	9.1.1.3 Nutzung	265
546	9.1.2 Artefakte	265
547	9.1.2.1 OCSP-Response – Response Status	265
548	9.1.2.2 OCSP-Response – Zeiten	266
549	9.1.2.3 OCSP-Response – CertStatus	267
550	9.1.2.4 OCSP-Response – CertID	268
551	9.1.2.5 OCSP-Response – Sperrzeitpunkt und Sperrgrund	268
552	9.1.2.6 OCSP-Response – CertHash	268
553	9.1.3 Testunterstützung	268
554	9.1.4 Hardwaremerkmale	268
555	10 Anhang A – Sektorspezifische Ausprägungen der SMC-B-	
556	Zertifikate	269
557	10.1 KZBV	269
558	10.2 KBV	271
559	10.3 DKG	273
560	10.4 GKV-Spitzenverband	275
561	10.5 Apothekerschaft	278
562	10.6 AdV-Umgebung im Auftrag der Kostenträger	280
563	10.7 SMC-B-ORG	281
564	11 Anhang B – Verzeichnisse	285
565	11.1 Abkürzungen	285
566	11.2 Glossar	290
567	11.3 Abbildungsverzeichnis	290
568	11.4 Tabellenverzeichnis	292
569	11.5 Referenzierte Dokumente	300
570	11.5.1 Dokumente der gematik	300
571	11.5.2 Weitere Dokumente	300

572	12 Anhang C – Sektorspezifische Ausprägungen der HBA	
573	Zertifikate.....	305
574	12.1 BÄK	305
575	12.2 BZÄK.....	307
576	12.3 BPtK	309
577	12.4 Apothekerschaft	311
578		

ENTWURF

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 Schutzrechtsinhabern 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].

609 1.5 Methodik

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

614 Sie werden im Dokument wie folgt dargestellt:

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

616 Text / Beschreibung

617 [**<=>**]

618

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

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

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

626

2 Notation kryptographischer Objekte

2.1 Basis-Bezeichner

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

631 **<Objekttyp>.<Objektbesitzer>.<Objektverwendung>**

632 Im weiteren Dokument werden dafür die kürzeren englischen Begriffe verwendet:

633 **<type>.<holder>.<usage>**

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

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

2.2 Optionale Bezeichnung der technischen Ausprägung

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

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

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

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

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

2.3 Optionales Unterscheidungsmerkmal bei gleicher technischer Ausprägung

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

656 Beispiel:

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

658 Ein Anwendungsfall ist bspw., dass Objekte auf Karten in Vorbereitung bzw. zur
659 Unterstützung kommender Kartengenerationen bereits vorgesehen werden und diese in
660 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

677 **Wertebereich von <ID>**

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

681 <X.509v3 ID> ::= ID
682 <card verifiable ID> ::= ID

683 **2.6 Holder (Objektbesitzer)**

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

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

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

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

697

698 **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>

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

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

704

705 Wertebereich von <holder X.509 | SK>

706 <root certification authority> ::= RCA

707 <health professional> ::= HP

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

709 <Clientmodul> ::= CM

710 <health care institution> ::= HCI

711 <security module Kartenterminal> ::= SMKT

712 <Anwendungskonnektor> ::= AK

713 <Netzkonnektor> ::= NK

714 <VPN Zugangsdienst> ::= VPNK

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

716 <Signatur Anwendungs Komponente> ::= SAK

717 <TLS> ::= TLS

718 <Fachdienst VSD> ::= VSD

719 <Zentraler Dienst> ::= ZD

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

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

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

727

728 Wertebereich von <holder CVC>

729 <root certification authority> ::= RCA

730 <certification authority> ::= CA

731 <certification authority eGK> ::= CA_eGK

732 <certification authority HPC> ::= CA_HPC

733 <certification authority SMC> ::= CA_SMC

734 <certification authority SAK> ::= CA_SAK

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

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

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

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

739 <health professional card> ::= HPC

740 <health professional card role> ::= HPC_Role
 741 <health professional card device> ::= HPC_Device
 742 <electronic health card> ::= eGK (elektronische Gesundheitskarte)
 743 <security module card> ::= SMC
 744 <security module card role> ::= SMC_role
 745 <security module card device> ::= SMC_device
 746 <Signatur Anwendungs Komponente> ::= SAK
 747 <Komfort-Merkmal> ::= KM (RFID-Token)
 748 <Kostenträger AdV> ::= KTRADV

749 2.7 Usage (Objektverwendung)

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

753

754 **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>

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

759

760 Wertebereich von <usage X.509 | SK>

761 <qualified electronic signature> ::= QES
 762 <electronic signature> ::= SIG
 763 <electronic signature of an organization> ::= OSIG
 764 <encipherment> ::= ENC

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

796 2.8 n (lfd. Nummer)

797 Bei der Benennung von kryptographischen Objekten erfolgt bei Gleichartigkeit eine
798 Unterscheidung durch Durchnummerieren der Elemente mittels laufender Nummer. Die
799 laufende Nummer wird für alle drei Bereiche Schlüssel, Zertifikat und ID einheitlich
800 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 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

827

828 **Wertebereich von <instance SYM>**

829 <2KeyTripleDES> ::= 2DES

830 <3KeyTripleDES> ::= 3DES

831 <AES mit 128 Bit> ::= AES128

832 <AES mit 256 Bit> ::= AES256

833 2.10 Beispiele zur Umsetzung

834 2.10.1 Beispiele für asymmetrische Objekte

835 **Tabelle 6: Tab_PKI_206 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.R2048
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

836 **2.10.2 Beispiele für symmetrische Objekte**

837 **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.
[<=]

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

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

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

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

881 Ein TSP-X.509 QES MUSS die Schlüsselgeneration RSA gemäß [gemSpec_Krypt#GS-
882 A_4358] unterstützen.
883 [\leq]

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

886 Ein TSP-X.509 QES, der Zertifikate für die Kartengeneration G2.1 erstellt oder
887 verwendet, MUSS die Schlüsselgeneration ECDSA gemäß [gemSpec_Krypt#GS-A_4358]
888 unterstützen.
889 [\leq]

890 **GS-A_5513 - Wahl des Signaturalgorithmus für Zertifikate**

891 Die gematik Root-CA, die TSP-X.509 QES und die TSP-X.509 nonQES MÜSSEN Zertifikate
892 mit dem Signaturalgorithmus der Schlüsselgeneration des Zertifikats signieren.
893 Ausgenommen davon sind die Crosszertifikate der gematik Root-CA.
894 [\leq]

895 **3.2 TI-Betriebsumgebungen**

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

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

Das Diagramm zeigt die Phasen der Produktentwicklung und -produktion, unterteilt in die Bereiche PKI-TeRe und PKI-Prod.

PKI-TeRe (Produktentwicklung) umfasst die Phasen:

- Referenz** (Betriebsumgebung):
 - Referenz-U-n
 - Referenz-U-...
 - Referenz-U-2
 - Referenz-U-1
 - Proof of Concept
 - Entwicklertest
 - Fachtest
- Test** (Betriebsumgebung):
 - Test-U-n
 - Test-U-...
 - Test-U-2
 - Test-U-1
 - Eingangsprüfung
 - Produkttest
 - Produktübergreifender Test
 - Erweiterter Fachtest

PKI-Prod (Produktion) umfasst die Phase:

- Produktion** (Betriebsumgebung):
 - Produktiv-Umgebung
 - Erprobung
 - Vorpilotierung
 - Pilotierung
 - Inbetriebnahmeprüfung
 - **Wirkbetrieb**

Die Phasen sind durch Pfeile verbunden, die die Abfolge von Referenz über Test bis hin zur Produktion zeigen.

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,

970 sowie (3) im `organizationalUnitName` den `<usageName>` = 'VPN-Zugangsdienst'
971 umsetzen.
972 [`<=>`]

973 3.4 Spezifische Aussteller-CA in der TI

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

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

977 Ein TSP-X.509 nonQES und der Anbieter des TSL-Dienstes MÜSSEN für die Beantragung
978 einer Aussteller-CA unterhalb der zentralen gematik-Root-CA die Zertifikatsstruktur
979 gemäß Tab_PKI_212 und einem CA-Namen entsprechend der Tabelle Tab_PKI_213
980 umsetzen.
981 [`<=>`]

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

983 Ein TSP-X.509 nonQES, TSP-X.509 QES und der Anbieter des TSL-Dienstes DÜRFEN aus
984 einer Aussteller-CA mit einem spezifischen Verwendungszweck NICHT weitere EE-
985 Zertifikate für andere Zwecke ausgeben.
986 [`<=>`]

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

988 Ein TSP-X.509 nonQES MUSS für eine Aussteller-CA unterhalb der zentralen gematik-
989 Root-CA (1) die Zertifikatsstruktur gemäß Tab_PKI_212 umsetzen und (2) für die Bildung
990 des `subjectDN` im Feld `subject.commonName` die Einträge aus der Spalte `<usage>` sowie
991 (3) im Feld `organizationalUnitName` die korrespondierenden Einträge aus der Spalte
992 `<usageName>` aus der Tabelle Tab_PKI_213 umsetzen.
993 [`<=>`]

994 **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

995

996

4 Kodierung von X.509-Identitäten

997

4.1 Namensregeln und -formate

998

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

999

1000

4.1.1 Verarbeitung von Sonderzeichen

1001

GS-A_4705 - Verarbeitung von Sonderzeichen in PKI-Komponenten

1002

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., in den einzelnen Namens-elementen zu verarbeiten und darzustellen. Es MUSS dazu ein Zeichensatz gemäß [Common-PKI#Part1] unterstützt werden.

1005

[<=]

1006

1007

Distinguished Names können daher generell mit diesen Sonderzeichen gebildet werden.

1008

Bei Kommunikationspartnern außerhalb Deutschlands kann die Verwendung von

1009

Umlauten zu Problemen führen, z. B. bei der Darstellung von Distinguished Names. Die

1010

zuständigen Instanzen für die Namensgebung müssen diese Problematik berücksichtigen.

1011

Für TI-interne TLS-Server und TLS-Client-Zertifikate können Umlaute und UTF-8-

1012

Codierungen verwendet werden, da auch für diese Komponenten eine Unterstützung

1013

eines Zeichensatzes gemäß [Common-PKI#Part 1] (s. o.) gefordert ist.

1014

4.1.2 Definition der Subject-DNs für Personen und Komponenten

1015

- Definition der Versichertenidentität in Kap 5.1.15.11

1016

- Definition der Organisationsidentität in Kap 5.3.1

1017

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

1018

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

1019

1020

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

1021

1022

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

1023

gematik-Root-CA, TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN bzgl. Aufbau des

1024

SubjectDN in CA-Zertifikaten und OCSP-Responder-Zertifikaten folgende Vorgaben

1025

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

1026

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

1027

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

1028

Attribut organizationName muss enthalten sein und den Namen des TSP enthalten. (d)

1029

Das Attribut countryName muss enthalten sein und das Herkunftsland des TSP (Land der

1030

Anschrift des TSP) enthalten. (e) Die Attribute serialNumber und organizationalUnitName

1031

können enthalten sein, sollen jedoch nur dann verwendet werden, falls sie für die

1032

Eindeutigkeit des subjectDN notwendig sind. (f) Das Attribut organizationIdentifier kann

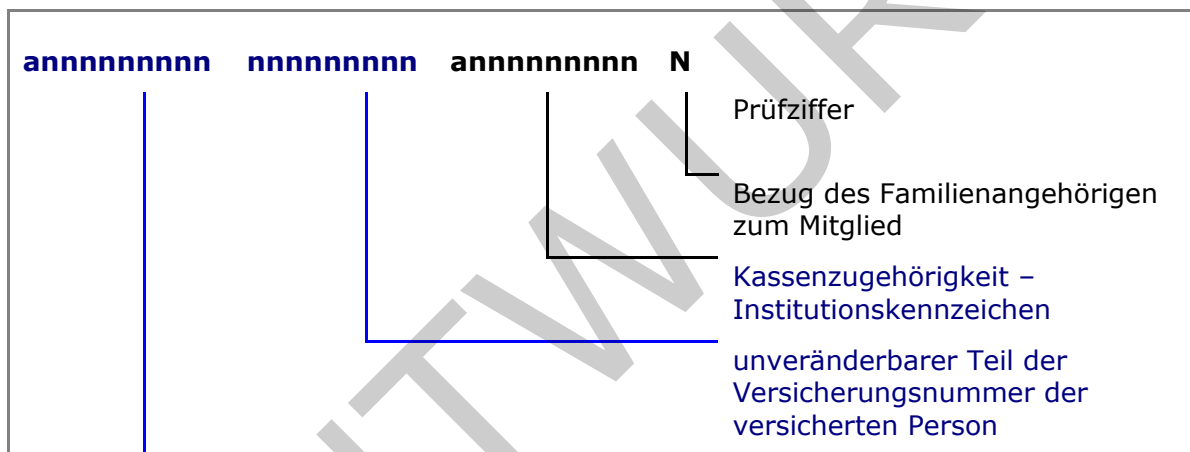
1033 enthalten sein. (g) Darüber hinaus sollen keine weiteren Attribute enthalten sein.
1034 [\leq]

1035 4.2 Schlüssel der Versichertenidentität (eGK)

1036 Gemäß SGB § 290 definieren die Spitzenverbände der Krankenkassen die Struktur der
1037 Krankenversichertennummer, die aus einem unveränderbaren Teil zur Identifikation des
1038 Versicherten und einem veränderbaren Teil, der bundeseinheitliche Angaben zur
1039 Kassenzugehörigkeit enthält.

1040 In den Zertifikaten C.CH.AUT, C.CH.ENC und C.CH.QES der eGK sowie C.CH.AUT_ALT der
1041 alternativen Versichertenidentitäten, wird in zwei OU-Feldern jeweils ein eindeutiger
1042 Schlüssel für den Versicherten sowie die Versicherungs-Institution aufgenommen:

- 1043 • OU = unveränderbarer Teil der KV-Nummer
- 1044 • OU = Institutionskennzeichen



1045 **Abbildung 2: Aufbau der Krankenversichertennummer**

1046 4.3 Pseudonym der Versichertenidentität (eGK)

1047 In den Zertifikaten C.CH.AUTN bzw. C.CH.ENCV der eGK (Schlüssel ohne PIN-Eingabe
1048 nutzbar) wird im Feld `commonName` des `SubjectDN` anstelle der personenbezogenen
1049 Klartextdaten ein Pseudonym verwendet.

1050 4.3.1 Versicherten-Pseudonym in X.509-Zertifikaten der eGK

1051 **GS-A_4572 - Abbildung Pseudonym in X.509-Zertifikaten der eGK**

1052 Der TSP-X.509 nonQES (eGK) MUSS im Feld `commonName` der Zertifikatstypen C.CH.AUTN
1053 bzw. C.CH.ENCV das Pseudonym des Versicherten aufnehmen.
1054 [\leq]

1055 4.3.2 Eindeutigkeit des Pseudonym

1056 Das Pseudonym dient als Ordnungskriterium (Primärschlüssel) für die Ablage von
1057 medizinischen Objekten und muss daher innerhalb der Herausgeber-Domäne über die

1058 Versicherten hinweg eindeutig sein. In Verbindung mit dem Herausgeber ist das
1059 Pseudonym so innerhalb der gesamten TI eindeutig.

1060 **GS-A_4573 - Eindeutigkeit des Pseudonyms innerhalb Herausgeber-Domäne**
1061 Der TSP-X.509 nonQES (eGK) MUSS das im AUTN- und ENCV-Zertifikat des Versicherten
1062 gespeicherte Pseudonym innerhalb der Herausgeber-Domäne (IssuerDomain) eindeutig
1063 gestalten.
1064 [\leq]

1065 4.3.3 Pseudonym-Erstellungsregel

1066 Die Bildung des Pseudonyms erfolgt nach einer Ableitungsregel aus bereits vorliegenden
1067 personenbezogenen Daten (KVNR) sowie durch ein herausgeberspezifisches Geheimnis.
1068 So kann auf den Einsatz eines technisch-organisatorischen Hintergrundsystems zur
1069 Verwaltung der Zuordnung von Pseudonymen zu Klaridentitäten verzichtet werden.

1070 **GS-A_4574 - Pseudonym-Erstellungsregel**
1071 Der TSP-X.509 nonQES (eGK) MUSS das Pseudonym des Versicherten nach folgender
1072 Regel bilden: SHA-256 Hashwert über die Konkatenierung der Datenfelder (1) Nachname
1073 des Versicherten, (2) unveränderbarer Teil der KVNR des Versicherten und (3) einer vom
1074 Herausgeber (Kostenträger) verwendeten Zusatzinformation (herausgeberspezifischer
1075 Zufallswert).
1076
1077 [\leq]
1078

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

1079
1080 Durch Verwendung dieses Verfahrens kann der Nachweis erbracht werden, dass eine
1081 bestimmte KVNR zu einem bestimmten Inhaber und dem entsprechenden
1082 Zertifikatsherausgeber gehört, ohne dass die KVNR in einem (öffentlichen) Zertifikats-
1083 Verzeichnis gespeichert werden muss.

1084 Bei Kenntnis des Nachnamens sowie der KVNR eines Versicherten und sofern der vom
1085 Herausgeber verwendete Zufallswert zur Verfügung gestellt wird, kann das Pseudonym
1086 nachgerechnet werden. Dabei ist ein auch im Negativ-Fall zuverlässiges Prüfungsergebnis
1087 nur möglich, wenn die Anzahl der zu verwendenden Iterationsschritte beschränkt wird.

1088 Beispiel:

1089 Nachname =
1090 „Mustername1“

1091 KVNR (unveränderlicher Teil, 10-stellig, AN) =
1092 „M331784849“

1093 herausgeberspezifischer Zufallswert (16-stellig, h) =
1094 „A32C93C6946314A9“

1095 Konkatenation =
1096 „Mustername1M331784849A32C93C6946314A9“

1097 SHA-256- Hashwert =
1098 "E3F3555165491A7FBE3F355516549E3F3555165902BFAF254518C469E584A793"

1099 Für den `commonName` werden die ersten 20 Hex-Zeichen (Variationsbreite 80 Bit)
1100 verwendet:

1101 `commonName` =
1102 "E3F3555165491A7FBE3F"

1103 **GS-A_4575 - Prüfung auf Eindeutigkeit des Pseudonyms**

1104 Der TSP-X.509 nonQES (eGK) MUSS nach Erzeugung des Pseudonyms prüfen, ob dieses
1105 Pseudonym vom Kartenherausgeber bereits vergeben wurde. Ist dies der Fall, MUSS das
1106 Pseudonym mit inkrementiertem hs-ZW neu generiert und erneut auf Eindeutigkeit
1107 geprüft werden.
1108 [`<=`]

1109 **GS-A_4576 - Pseudonym auf eGK-Ersatzkarten**

1110 Der TSP-X.509 nonQES (eGK) MUSS bei Ausstellung eines eGK-Ersatzausweises
1111 innerhalb der definierten Verwendungsperiode des herstellerspezifischen Zufallswertes
1112 (hs-ZW) dasselbe Pseudonym verwenden wie auf der vorgängigen Karte.
1113 [`<=`]

1114 **GS-A_4577 - Pseudonym auf eGK-Folgekarten**

1115 Der TSP-X.509 nonQES (eGK) MUSS bei Ausstellung eines eGK-Ersatzausweises nach
1116 Ablauf der definierten Verwendungsperiode des hs-ZW oder bei Ausstellung einer
1117 Folgekarte nach Ablauf des Gültigkeitszeitraums der vorgängigen Karte ein neues
1118 Pseudonym auf Grundlage des geänderten hs-ZW vergeben.
1119 [`<=`]

1120 **4.3.4 Hs-ZW – Herausgeberspezifischer Zufallswert (hs-ZW)**

1121 Da der herausgeberspezifische Zufallswert für alle Versicherten eines Herausgebers
1122 identisch ist, muss dieser periodisch, z. B. jährlich gewechselt werden.

1123 **GS-A_4578 - eGK hs-ZW Bildungsregel**

1124 Der eGK-Herausgeber MUSS einen individuellen herausgeberspezifischen Zufallswert (hs-
1125 ZW) aus mindestens 16 Hexadezimal-Ziffern (64 Bit) festlegen, der jeweils kollisionsfrei
1126 zu allen vorherigen hs-ZW dieses eGK-Herausgebers ist.
1127 [`<=`]

1128 **GS-A_4579 - eGK hs-ZW Verwendung/Wechsel**

1129 Der eGK-Herausgeber MUSS den aktuellen hs-ZW für alle Versichertenzertifikate für eine
1130 bestimmte Verwendungsperiode verwenden und mindestens einmal jährlich wechseln.
1131 [`<=`]

1132 **GS-A_4580 - eGK hs-ZW Archivierung**

1133 Der eGK-Herausgeber MUSS alle nicht mehr verwendeten hs-ZW für Zwecke der
1134 Rekonstruktion von Pseudonymen für mindestens 10 Jahre sicher speichern und
1135 berechtigten Teilnehmern der TI verfügbar machen.
1136 [`<=`]

1137 **4.3.5 Kodierung des Pseudonyms**

1138 Für das eGK-Pseudonym gilt folgende Systematik für Erstellung und Verwendung.

1139

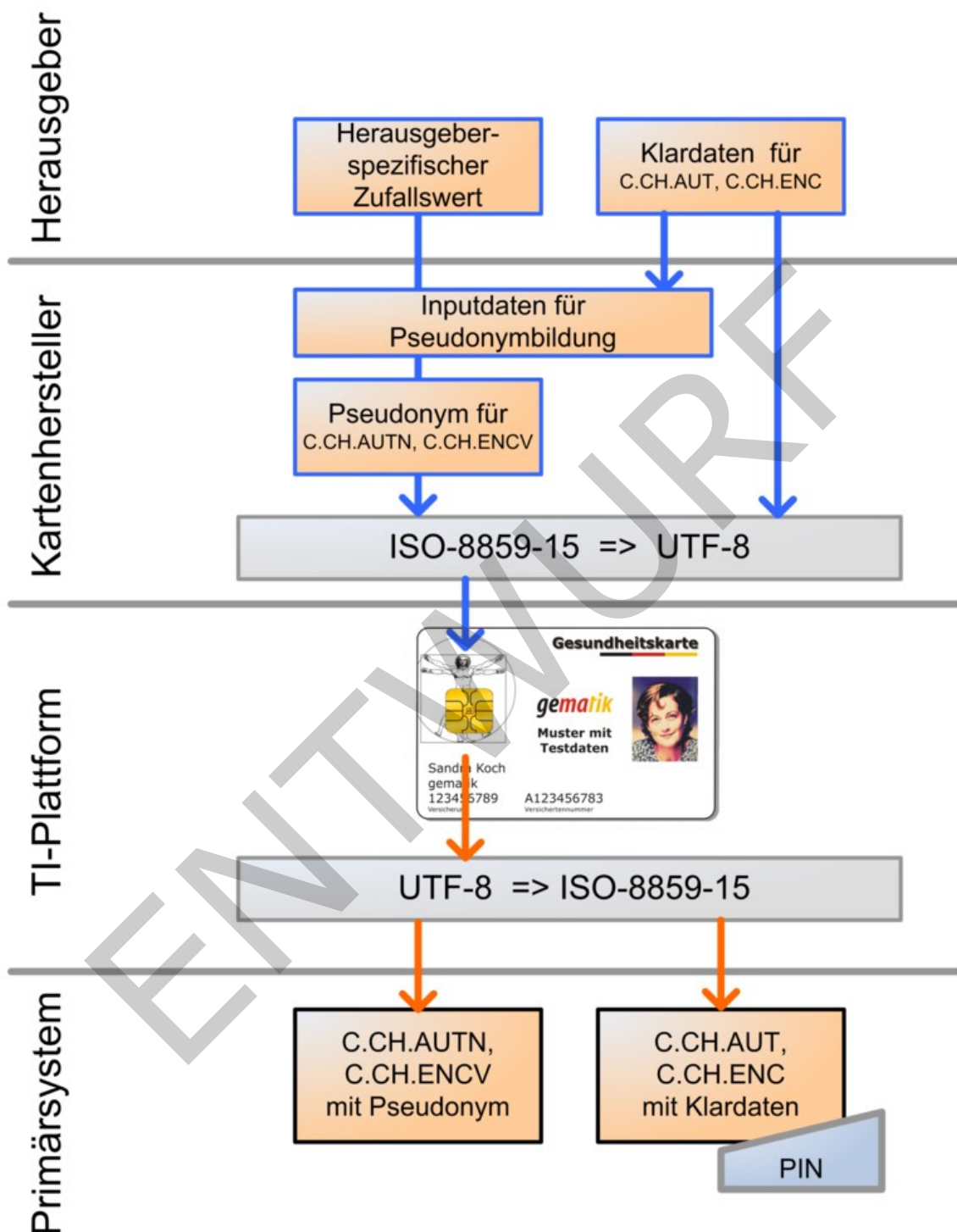


Abbildung 3: Pseudonym Kodierung in X.509-Versichertenzertifikaten

1140

1141

1142

1143

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

Der eGK-Herausgeber MUSS das Pseudonym im UTF-8-Zeichensatz codiert in das Zertifikat der eGK einbringen.
[<=]

4.4 Berufsgruppen-ID der Leistungserbringer

4.4.1 Berufsgruppe des Heilberufers

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

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

GS-A_4583 - Berufsgruppenkennzeichen für HBA

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

GS-A_4584 - Verwendung von Berufsgruppenkennzeichen

TSP-X.509 nonQES und TSP-X.509 QES DÜRFEN NICHT Berufsgruppenkennzeichen, für deren Verwendung sie nicht zugelassen und beauftragt sind, in HBA-Zertifikate einbringen.
[<=]

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.

[<=]

1206 **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

1207 4.7 Telematik-ID

1208 Die Telematik-ID repräsentiert als eineindeutiges Merkmal die Identität eines
1209 Teilnehmers, also eines Leistungserbringers im HBA respektive einer
1210 Organisation/Einrichtung des Gesundheitswesens in einer SMC-B. Die Telematik-ID muss
1211 daher über alle Sektoren hinweg eineindeutig bezogen auf die elektronische Identität der
1212 betroffenen Teilnehmer in der Telematikinfrastruktur sein. Die Zuordnung der Telematik-
1213 ID zum Teilnehmer wird in [gemKPT_PKI_TIP] beschrieben.

1214 Für Ersatzkarten und Austauschkarten wird die Telematik-ID der Originalkarte
1215 verwendet.

1216 Für Folgekarten muss die Telematik-ID nicht identisch zur Vorgängerkarte sein. Der Arzt
1217 und die medizinische Institution können eine neue Telematik-ID beantragen oder auch
1218 die bisherige in der Folgekarte wieder verwenden.

1219 **GS-A_4958 - Neue Telematik-ID bei Folgekarten**

1220 Der Kartenherausgeber MUSS bei der Ausgabe von Folgekarten dem Antragsteller die
1221 Möglichkeit bieten, eine neue Telematik-ID zu beziehen.
1222 [\leq]

1223 **GS-A_4960 - System für Sektorkennzeichen**

1224 Der Gesamtbetriebsverantwortliche der TI MUSS zur Sicherstellung der Eindeutigkeit der
1225 Telematik-ID über die verschiedenen Sektoren des Gesundheitswesens hinweg ein
1226 System für Sektorkennzeichen als Bestandteil (Präfix) der Telematik-ID etablieren und
1227 verwalten.
1228 [\leq]

1229 4.7.1 Abbildung der Telematik-ID im X.509-Zertifikat

1230 Die Telematik-ID wird im Feld **registrationNumber** der Extension Admission hinterlegt,
1231 vgl. Beispiel in Tabelle 12.

1232 **GS-A_4709 - Abbildung der Telematik-ID in Admission-Struktur**

1233 TSP-X.509 nonQES MÜSSEN zur Abbildung der Telematik-ID in HBA- sowie SMC-B-
1234 Zertifikaten eine Admission Extension aufnehmen, die eine oder mehrere Struktur(en)
1235 „ProfessionInfo“ und darin im Feld „registrationNumber“ die Telematik-ID enthalten
1236 muss.
1237 [\leq]

1238 **GS-A_4901 - Einheitliche Admission in Zertifikaten einer Karte**

1239 TSP-X.509 QES und TSP-X.509 nonQES SOLLEN die Admission Extension in allen X.509-
1240 Zertifikaten einer Karte identisch einbringen. In den Herausgabe-Policies können

1241 Ausnahmen hiervon definiert sein.
1242 [\leq]

1243

1244 **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

1245 4.7.2 Aufbau der Telematik-ID

1246 GS-A_4587 - Gesamtlänge der Telematik-ID

1247 Herausgeber von HBA und SMC-B MÜSSEN sicherstellen, dass die Gesamtlänge der
1248 Telematik-ID (Präfix, Separator und Fortsatz) 128 Zeichen nicht überschreitet.
1249 [\leq]

1250

1251 **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

1252 *Anmerkung zur Darstellung des Formats: N=numerisch, AN=alphanumerisch*

1253 4.7.2.1 Sektoraler Präfix

1254 GS-A_4710 - Präfix der Telematik-ID

1255 Herausgeber von HBA und SMC-B MÜSSEN die in Tab_PKI_101 festgelegten Präfixe der
1256 Telematik-ID verwenden.
1257 [\leq]

1258

1259 **Tabelle 14: Tab_PKI_101 Normative Festlegung für das Präfix der Telematik-ID.**

Präfix	Sektor	Zuständige Organisationen
1	Ärzterschaft	BAEK, KBV

2	Zahnärzteschaft	BZÄK, KZBV
3	Apothekerschaft	BAK
4	Psychotherapeutenschaft	BPTK
5	Krankenhaus	DKG
6	(Reserved for future use)	
7	KTR-AdV	
8	Kostenträger	GKV-SV

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) 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.

[<=]

1288 4.8 Kodierung der Zertifikate

1289 4.8.1 Kodierung der Attribute

1290 In diesem Kapitel werden die für alle X.509-Zertifikate einheitlich geltenden Felder und
1291 ihre Kodierung aufgeführt. Ergänzende profilspezifische Kodierungsvorgaben sind bei den
1292 jeweiligen Profilen ausgeführt.

1293 **GS-A_4714 - Kodierung der Attribute in X.509-Zertifikaten**

1294 TSP-X.509 und der Anbieter des TSL-Dienstes MÜSSEN bei der Kodierung der Attribute in
1295 X.509-Zertifikaten die Vorgaben aus Tab_PKI_229 umsetzen. Die Vorgaben sind
1296 unabhängig davon, ob das jeweilige Attribut innerhalb eines issuer (Typ Name)-, subject
1297 (Typ Name)- oder eines extension (Typ Extension)-Elementes im Zertifikat verwendet
1298 wird.

1299 [\leq]

1300

1301 **Tabelle 15: Tab_PKI_229 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
streetAdress {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]	2
organizationIdentifier {id-at 97}	UTF8String [X.520]	-
*) Einschränkung des erlaubten Zeichensatzes auf dedizierte ISO-Subsets gemäß Vorgaben der jeweiligen Kartenherausgeber		

4.8.2 Stringlänge der Attribute

GS-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 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] mehrere unterschiedliche Ausprägungen der Strukturen. Um die Verwendung von Zertifikaten in der TI zu vereinfachen werden spezifisch einschränkende Festlegungen für Extensions 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	<i>medisign</i>
19	<i>atos</i>

1336 Der Nummernraum des Präfixes wird durch die Gesellschaft für Telematikanwendungen
1337 der Gesundheitskarte mbH (gematik) verwaltet.

1338 Im Falle der Clusterung von Diensten besteht evtl. die Notwendigkeit jeder Instanz ein
1339 eigenes Zertifikat auszustellen. Damit die Eindeutigkeit des SubjectDN im jeweiligen
1340 Zertifikat gewährleistet ist, kann die Ausprägung der Instanz in das Feld serialNumber
1341 übernommen werden.

1342 **GS-A_4725 - Eindeutiger SubjectDN durch serialNumber**

1343 Ein TSP-X.509 nonQES KANN die Eindeutigkeit des SubjectDN in einem X.509-Zertifikat
1344 für Zentrale Dienste und Fachanwendungsspezifischen Dienste durch die Verwendung des
1345 Attributes serialNumber {id-at-serialNumber} gewährleisten.

1346 [\leq]

1347 **GS-A_4726 - Verwendung von serialNumber zur Schaffung eindeutiger 1348 SubjectDNs**

1349 TSP-X.509 nonQES MÜSSEN bei Verwendung des Attributs serialNumber in X.509-
1350 Zertifikaten für Zentrale Dienste und Fachanwendungsspezifische Dienste den Inhalt
1351 entsprechend dem folgenden Format aufbauen: Instanz (fünfstellige Dezimalzahl) + "-"
1352 + Unterscheidung Zertifikat (alphanumerischer Wert).

1353 [\leq]

1354 **4.8.3.2 Admission**

1355 Die Extension Admission enthält Angaben zur Registrierung und zu der beruflichen
1356 Zulassung (und somit auch zu daraus ableitbaren Autorisierungsinformationen) sowohl
1357 als Text als auch in Form einer maschinenlesbaren OID.

1358 Für die verschiedenen Zertifikatstypen sind dies jeweils:

- 1359 • die Berufsgruppen (HBA/BA),
- 1360 • der Status als Versicherte/-r (eGK und alternative Versichertenidentitäten),
- 1361 • der Typ der Organisation/Institution (SMC-B) oder
- 1362 • die technische Rolle (Komponentenzertifikate).

1363 Außerdem können die Telematik-ID und die registrierende bzw. zulassende Stelle
1364 (admissionAuthority) in Admission eingetragen werden (in HBA-, BA- und SMC-B-
1365 Zertifikaten).

1366

1367 **GS-A_4717 - TI-spezifische Vorgabe zur Nutzung der Extension Admission**

1368 TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN bei Verwendung der Extension
1369 Admission {id-commonpki-at 3} die Struktur in X.509-Zertifikaten entsprechend
1370 Tab_PKI_226 erstellen.

1371 [\leq]

1372

1373 **Tabelle 17: Tab_PKI_226 Struktur Admission**

#	ASN.1 definition	TI-spezifische Vorgaben
---	------------------	-------------------------

1	id-isismtt-at-admission OBJECT IDENTIFIER ::= {id-isismtt-at 3}	
2	id-isismtt-at-namingAuthorities OBJECT IDENTIFIER ::= {id-isismtt-at 11}	
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	<pre> addProfessionInfo OCTET STRING OPTIONAL } </pre>	

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	<pre> CertificatePolicies ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation </pre>	In allen End-Entity-Zertifikaten MUSS genau ein Element dieser Sequenz enthalten.
2	<pre> PolicyInformation ::= SEQUENCE { </pre>	
3	<pre> policyIdentifier CertPolicyId, </pre>	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	<pre> policyQualifiers SEQUENCE SIZE (1..MAX) OF PolicyQualifierInfo OPTIONAL } </pre>	Enthält das Element PolicyIdentifier die Zertifikatstyp-OID, DARF das Element policyQualifiers NICHT verwendet werden
5	<pre> CertPolicyId ::= OBJECT IDENTIFIER </pre>	

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. [\leq]

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. [\leq]

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. [\leq]

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.

1416 Erläuterung:

1417 Überlange Attribute des Subject Distinguished Name (SubjectDN) werden gekürzt, um
1418 die für sie geltenden Längenvorgaben einzuhalten (s. Tab_PKI_229 „Kodierung der
1419 Attribute in X.509-Zertifikaten"). Sie werden aber in der Extension „SubjectAltNames" in
1420 voller Länge abgebildet.

1421 Felder des „SubjectAltNames" werden als „GeneralName" gespeichert. Für die
1422 Verwendung von überlangen Namen wird der GeneralName-Typ OtherName benutzt.
1423 Dessen Struktur ist wie folgt aufgebaut:

1424

```
1425 OtherName ::= SEQUENCE {
1426     type-id OBJECT IDENTIFIER,
1427     value [0] EXPLICIT ANY DEFINED BY type-id }
1428 }
```

1429 Die type-id entspricht der OID des zu verlängernden Feldes:

- 1430 • commonName {id-at 3}
- 1431 • organizationalUnitName {id-at 11}
- 1432 • organizationName {id-at 10}

1433 Bei Bedarf kann die beschriebene Struktur auch verwendet werden, um Alternativnamen
1434 oder Ergänzungen zum Namen aufzunehmen, welcher im durch ,type-id' bezeichneten
1435 Attribut des SubjectDN enthalten ist, auch wenn dieser nicht gekürzt werden musste.

1436 Für weitere Informationen, siehe auch ITU-T Rec. X.501 | [ISO/IEC9594-2]. Das Format
1437 des value wird entsprechend demjenigen des Attributes festgelegt, bei den Attributen
1438 commonName, organizationalUnitName und organizationName handelt es sich dabei
1439 immer um UTF8String.

1440 4.9 Erläuterungen zu Zertifikatsprofilen

1441 Dieses Kapitel enthält eine Reihe von Erläuterungen und Hilfestellungen zum Verständnis
1442 der in Kapitel 5 dargestellten Zertifikatsprofile sämtlicher X.509-Zertifikate.

1443 4.9.1 Allgemeine Erläuterungen

1444 Die Angabe Kardinalität gibt an, wie oft ein Element in einem Zertifikat enthalten sein
1445 muss. Ein optionales Feld hat so z. B. eine Kardinalität von 0-1. Eine Kardinalität von 1
1446 bezeichnet ein Pflichtfeld, das nur ein Mal auftreten darf.

1447 Die Bezeichner „ZD, FD“ werden in den Festlegungen zu X.509-Zertifikaten als
1448 Kurzbezeichnungen für die Rollen von Zentralen Diensten und
1449 Fachanwendungsspezifischen Diensten verwendet.

1450 Die Attribute einer Berufsgruppe, einer medizinischen Institution oder technischen Rolle
1451 werden in den X.509-Zertifikaten anhand einer maschinenlesbaren OID und einem
1452 textuellen Bezeichner beschrieben. Siehe hierzu auch Kap 4.4 bis 4.6.

1453 Die normative Festlegung der Werte der Felder `professionItems` und `professionOIDs`
1454 erfolgt in den Tabellen Tab_PKI_402, Tab_PKI_403 und Tab_PKI_406 in
1455 [gemSpec_OID#3.5].

1456 Für die Festlegung des Zertifikatstyps in der Extension CertificatePolicies wird eine OID-
1457 Referenz verwendet. Die normative Festlegung der durch diese Referenz dargestellten
1458 OIDs trifft das Dokument [gemSpec_OID# Tab_PKI_405].

1459 4.9.2 Berufs-/Rollenattribute und Sperrbarkeit

1460 **GS-A_4721 - Beantragung Rollenattribute im X.509-Zertifikatsrequest**

1461 Der TSP-X.509 nonQES der Komponenten-PKI MUSS bei der Erstellung von X.509-
1462 Zertifikate für Dienste sicherstellen, dass ein Diensteanbieter nur Zertifikate für die
1463 Rollen beantragen kann, für die dieser Diensteanbieter in der TI von der gematik
1464 zugelassen ist.

1465 [\leq]

1466 **GS-A_4961 - Verwendung zugewiesener Berufs- und Rollenattribute**

1467 Die Kartenherausgeber MÜSSEN genau die Berufs- und Rollenattribute verwenden, die
1468 den zertifizierten Identitäten entweder auf gesetzlicher Grundlage oder durch Zuweisung
1469 einer gesetzlich autorisierten Standesvertretung zugewiesen wurden. Für die codierte
1470 Form dieser Attribute MÜSSEN die von der TI-Plattform verwalteten Berufs- und
1471 Rollencodes verwendet werden.

1472 [\leq]

1473 **GS-A_4722 - Belegung der Felder professionInfos**

1474 Der TSP-X.509 nonQES MUSS bei der Erstellung von X.509-Zertifikaten sicherstellen,
1475 dass die Werte `professionItems` und `professionOIDs` den Festlegungen für den Typ des
1476 beantragten Zertifikats entsprechen.

1477 [\leq]

1478 **GS-A_4724 - Komplettsperrung aller Zertifikate einer Karte**

1479 TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN sicherstellen, dass alle Zertifikate auf
1480 einem Kartenexemplar durch einen Sperrauftrag gesperrt werden können (sofern für die
1481 jeweiligen Zertifikatstypen die Statusinformationsbereitstellungen gefordert sind).

1482 [\leq]

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

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

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

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

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

[<=]

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

```
1529 SubjectDN (String)
1530 C=DE, O=2-29999999999 NOT-VALID, serialNumber=12.80276002791200027011,
1531 CN=Zahnarztpraxis Prof. Dr. Dr. Dr. med. rer. nat. Dip:PN TEST-ONLY
1532
1533 SubjectDN (ASN.1-Codierung)
1534 SEQUENCE {
1535     SET {
1536         SEQUENCE {
1537             OBJECT IDENTIFIER countryName (2 5 4 6)
1538             PrintableString 'DE'
1539         }
1540     }
1541     SET {
1542         SEQUENCE {
1543             OBJECT IDENTIFIER organizationName (2 5 4 10)
1544             UTF8String '2-29999999999 NOT-VALID'
1545         }
1546     }
1547     SET {
1548         SEQUENCE {
1549             OBJECT IDENTIFIER serialNumber (2 5 4 5)
1550             PrintableString '12.80276002791200027011'
1551         }
1552     }
1553     SET {
1554         SEQUENCE {
1555             OBJECT IDENTIFIER commonName (2 5 4 3)
1556             UTF8String
1557             'Zahnarztpraxis Prof. Dr. Dr. Dr. med. rer. nat. '
1558             'Dip:PN TEST-ONLY'
1559         }
1560     }
1561 }
1562
```

1563 4.10 Kodierung der Betriebsumgebungen in Zertifikaten

1564 Zertifikate für Test- und Referenzumgebungen werden je TSP aus genau einer vollständig
1565 separaten Test-PKI ausgestellt. Siehe hierzu auch Kap 3.

1566 **GS-A_4727 - PKI-Separierung von Test- und Produktivumgebung in der TI**

1567 Der TSP-X.509 und der Anbieter des TSL-Dienstes DÜRFEN für die Generierung von EE-
1568 Zertifikaten der Produktivumgebung NICHT eine CA der Testumgebung verwenden.
1569 Umgekehrt DÜRFEN der TSP-X.509 und der Anbieter des TSL-Dienstes für die
1570 Generierung von EE-Zertifikaten der Testumgebung NICHT eine CA der
1571 Produktivumgebung verwenden.
1572 [**<=**]

1573 **GS-A_4588 - CA-Namen für Test-PKI der TI**

1574 Der TSP-X.509 und der Anbieter des TSL-Dienstes MÜSSEN die Namen (CN: und O:)
1575 sämtlicher CAs in der Test-PKI entsprechend den korrespondierenden CAs der
1576 Produktivumgebung vergeben und diese um den String „TEST-ONLY“ im CN-Feld sowie

1577 „NOT-VALID“ im O-Feld ergänzen.
1578 [\leq]

1579 **GS-A_4589 - EE-Namen für Test-PKI der TI**

1580 TSP-X.509 nonQES (außer eGK) und TSP-X.509 QES MÜSSEN die Namen (CN: und O:) der EE-Zertifikate in der Test-PKI entsprechend den korrespondierenden Zertifikatsprofilen der Produktivumgebung verwenden und ergänzen:
1581 (a) für HBA-, Institutions- und Signer-Zertifikate um den String „TEST-ONLY“ im CN-Feld
1582 sowie um den String „NOT-VALID“ im O-Feld,
1583 (b) für Komponentenzertifikate um den String "TEST-ONLY - NOT-VALID" im O-Feld.

1586
1587
1588 [\leq]

1589 Die Fallunterscheidung in GS-A_4589 rührt daher, dass die Markierung als Testzertifikat prominent im Common Name (CN) erfolgen soll, wenn immer dies möglich ist. Falls dem Inhalt des Common Name eine funktionale Bedeutung zukommen kann (z. B. bei einem TLS-Server-Zertifikat mit FQDN im Common Name), muss aber darauf verzichtet werden.
1593 Dies ist bei Zertifikaten für Komponenten (Dienste und Geräte/gSMC) der Fall.

1594 Die folgende Tabelle dient der Detaillierung dieses Sachverhaltes:

1595

1596 **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

1597
1598

1599 **GS-A_4590 - Zertifikatsprofile für Test-PKI**

1600 Der TSP-X.509 und der Anbieter des TSL-Dienstes SOLLEN die Feldattribute (außer CN:
1601 und O:) für sämtliche Zertifikate in der Test-PKI gemäß den korrespondierenden Profilen
1602 der Produktivumgebung setzen.

1603 [\leq]

1604 **4.11 Kartenverlust und Deaktivierung von Chipkarten**

1605 **GS-A_4962 - Verhalten bei Kartenverlust und Änderung persönlicher Daten**

1606 Der Kartenherausgeber MUSS den Zertifikatsnehmer verpflichten, Sperrungen seiner
1607 Karte bzw. seines Sicherheitsmoduls bei dem Kartenherausgeber oder bei einer von ihm
1608 benannten Stelle durchführen zu lassen. Sperrgründe können beispielsweise der Verlust
1609 der Karte bzw. des Sicherheitsmoduls sowie Änderungen zu registrierungsrelevanten
1610 persönlichen Daten sein (z. B. Änderung der Zugehörigkeit zu einer Berufsgruppe).

1611 [\leq]

1612 **GS-A_4963 - Deaktivierung von Chipkarten nach Gültigkeitsende**

1613 Der Kartenherausgeber MUSS Vorgaben definieren, wie eine Chipkarte sowie die
1614 enthaltenen kryptographischen Schlüssel nach Ablauf ihrer definierten Gültigkeitsdauer
1615 dauerhaft unbrauchbar gemacht werden.

1616 [\leq]

1617

5 X.509-Zertifikate

1618 In diesem Kapitel werden die Anforderungen an X.509-Zertifikate formuliert, wobei die
1619 generischen Festlegungen aus Kap. 3 für alle Zertifikatsprofile gelten, soweit anwendbar.

1620 Die Schreibweise der Termini entspricht [Common-PKI].

1621 Bei Verwendung der keyUsage „nonRepudiation“ und „contentCommitment“ wird
1622 technisch dasselbe KeyUsage-Bit gesetzt. In dieser Spezifikation wird einheitlich die
1623 Bezeichnung „nonRepudiation“ verwendet.

1624 Eine Gesamtübersicht aller kryptographischen Identitäten (X.509- und CV-) mit deren
1625 Einsatzfeldern findet sich in [gemKPT_Arch_TIP#AnhB].

1626 **GS-A_4965 - Keine Suspendierung von X.509-Zertifikaten (außer für eGK)**

1627 Ein TSP-X.509 DARF für X.509-Zertifikate – außer denen der eGK – eine Suspendierung
1628 NICHT implementieren.

1629 [\leq]

1630 Die Bedingungen für Sperrung und Suspendierung (nur bei eGK) von Zertifikaten werden
1631 in [gemRL_TSL_SP_CP#5.9] beschrieben.

1632 Für Zertifikate, die auf Karten gespeichert werden, sind Größenbeschränkungen zu
1633 beachten.

1634 **GS-A_5337 - Größenbeschränkung von X.509 Zertifikaten auf Karten**

1635 Ein TSP X.509 (außer ein TSP X.509 für eGK) MUSS sicherstellen, dass die von ihm
1636 erzeugten Zertifikate, die für die Speicherung auf Karten vorgesehen sind, die
1637 Maximalgröße der dafür vorgesehenen Kartenobjekte - gemäß der relevanten
1638 Objektsystemspezifikationen - nicht überschreiten. Wenn zu lange Eingangsdaten
1639 vorliegen sind diese in Abstimmung mit dem Antragsteller/Kartenherausgeber zu ändern.

1640 [\leq]

1641 **5.1 eGK – Versichertenkarte**

1642 Die Festlegungen in diesem Kapitel gelten sowohl für die Zertifikate bzw. Identitäten auf
1643 der eGK selbst als auch für die alternativen Versichertenidentitäten, die nicht auf der
1644 eGK-Smartcard gespeichert sind.

1645 **5.1.1 Definition der Versichertenidentität**

1646 Folgende Datenfelder bilden die Namensidentität des Versicherten

- 1647 1. Vorname des Versicherten
1648 2. Familienname des Versicherten
1649 3. Titel des Versicherten
1650 4. Namenszusatz
1651 5. Vorsatzwort

1652 Diese Daten werden in den folgenden Feldern des **subjectDN** des Versicherten im
1653 Zertifikat abgebildet:

- 1654 • `commonName`
- 1655 • `title`
- 1656 • `givenName`
- 1657 • `surname`

1658 **GS-A_4966 - Nutzung bestehender Versichertendatensätze für eGK-Zertifikate**
1659 Für die Erstellung von Versichertenkarten SOLL der Kartenherausgeber bestehende
1660 Versichertendatensätze für die Registrierung von Zertifikatsnehmern verwenden.
1661 [`<=`]

1662 **5.1.2 Belegung der Felder im SubjectDN**

1663 Die zwei Namenszeilen, die auf die eGK optisch personalisiert werden, bestehen aus
1664 jeweils 28 Zeichen, die beide zusammen mit einem zusätzlichen Leerzeichen als
1665 Trennzeichen den `commonName` des Versicherten bilden. Die Begrenzung auf 64 Zeichen
1666 wird erfüllt.

1667 Für die Bildung der anderen Felder wird der Name des Versicherten in der natürlichen
1668 Schreibweise und Reihenfolge herangezogen.

1669 Titel Vorname Namenszusatz Vorsatzwort Familienname

1670 **GS-A_4967 - Vergabe und Übermittlung eindeutiger Versicherten-ID**
1671 Die Kostenträger MÜSSEN für den Versicherten eine eindeutige ID vergeben und zur
1672 Zertifikatserstellung an den Zertifikatsherausgeber zur Einbringung in die Zertifikate
1673 übermitteln.
1674 [`<=`]

1675 **GS-A_4968 - Erzeugung und Einbringung der KVNR**
1676 Der eGK-Kartenherausgeber MUSS als eindeutigen Identifier des Versicherten die KVNR
1677 gemäß gesetzlicher Vorgaben erzeugen und Festlegungen treffen, welche Anteile der
1678 KVNR in die Versichertenkarten einzubringen sind.
1679 [`<=`]

1680 **GS-A_4592 - Bildung des surname im SubjectDN eGK-Zertifikat**
1681 Der Kartenherausgeber MUSS für das Feld `surname` im SubjectDN der eGK-Zertifikate das
1682 Attribut *Familienname* verwenden und MUSS bei erforderlichen Kürzungen bis zur
1683 maximal zulässigen Länge des Feldes folgende Regel anwenden: (a) ein ggf. vorhandener
1684 dritter Familienname ist ggf. bis auf den Anfangsbuchstaben zu kürzen und die Kürzung
1685 durch einen Punkt kenntlich zu machen. Ist die Kürzung nicht ausreichend, MUSS
1686 zusätzlich gelten: (b) ein zweiter Familienname ist ggf. bis auf den Anfangsbuchstaben zu
1687 kürzen und die Kürzung durch einen Punkt kenntlich zu machen.
1688 [`<=`]

1689 **GS-A_4593 - Bildung des givenName im SubjectDN eGK-Zertifikat**
1690 Der Kartenherausgeber MUSS für das Feld `givenName` im SubjectDN der eGK-Zertifikate
1691 die Attribute *Vorname Namenszusatz Vorsatzwort* verwenden und MUSS bei
1692 erforderlichen Kürzungen bis zur maximal zulässigen Länge des Feldes folgende Regel
1693 anwenden: (a) ein ggf. vorhandener dritter Rufname ist auf den Anfangsbuchstaben zu
1694 verkürzen und die Kürzung durch Punkt kenntlich zu machen. Ist die Kürzung nicht
1695 ausreichend, MUSS zusätzlich gelten: (b) ein zweiter Rufname ist ggf. bis auf den
1696 Anfangsbuchstaben zu kürzen und die Kürzung durch Punkt kenntlich zu machen.
1697 [`<=`]

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.

[<=]

1733 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) Für Zertifikate der eGK: policyIdentifier = <oid_egk_aut> Für Zertifikate der alternativen Versichertenidentitäten: 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
	andere Erweiterungen		0	
signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS- A_4359]		
signature		Wert der Signatur		

1734 **5.1.3.2 C.CH.ENC – Verschlüsselung eGK**

1735 **GS-A_4596 - Umsetzung Zertifikatsprofil C.CH.ENC**

1736 Der TSP-X.509 nonQES (eGK) MUSS C.CH.ENC gemäß Tab_PKI_233 umsetzen.

1737 [**<=**]

1738 **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		

1739 **5.1.3.3 C.CH.QES – Qualifizierte Signatur eGK (optional)**

1740 **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		

1747 **5.1.3.5 C.CH.ENCV - Technische Verschlüsselung eGK**
 1748 **GS-A_4599 - Umsetzung Zertifikatsprofil C.CH.ENCV**
 1749 Der TSP-X.509 nonQES (eGK) MUSS C.CH.ENCV gemäß Tab_PKI_236 umsetzen.
 1750 [**<=**]

1751
 1752 **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		

1753 5.2 HBA – Heilberufsausweis

1754 GS-A_5042 - Kodierung der X.509-Zertifikate für HBA und SMC-B

1755 TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN bei der Herausgabe von Zertifikaten für
1756 HBA und SMC-B die übergreifenden Kodierungsvorschriften aus [gemSpec_PKI#4]
1757 umsetzen.

1758
1759 [<=]

1760 5.2.1 X.509 Zertifikatsprofile des HBA

1761 5.2.1.1 C.HP.AUT – Authentisierung HBA

1762 GS-A_5531-01 - Umsetzung Zertifikatsprofil C.HP.AUT

1763 Der TSP-X.509 nonQES MUSS C.HP.AUT gemäß Tab_PKI_268_1 umsetzen. [<=]

1764 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		
	extensions			critical
	SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Inhabers	1	FALSE
	KeyUsage {2 5 29 15}	<i>Für Schlüsselgeneration RSA:</i> digitalSignature keyEncipherment <i>Für Schlüsselgeneration ECDSA:</i> 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		

1765 *) Sektorspezifische Ausprägungen der HBA-Zertifikate sind dem Anhang C zu
1766 entnehmen.

1767 **) Kodierung in einem SET als einziges Multivalued Relative Distinguished Name
1768 Element (multivaluedRDN) (siehe Hinweis unten unter Zusatzinformationen)

1769 5.2.1.2 C.HP.ENC – Verschlüsselung HBA

1770 GS-A_5532-01 - Umsetzung Zertifikatsprofil C.HP.ENC

1771 Der TSP-X.509 nonQES MUSS C.HP.ENC gemäß Tab_PKI_269_1 umsetzen.[<=]

1772 **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		

1773 *) Sektorspezifische Ausprägungen der HBA-Zertifikate sind dem Anhang C zu
1774 entnehmen.

1775 **) Kodierung in einem SET als einziges Multivalued Relative Distinguished Name
1776 Element (multivaluedRDN) (siehe Hinweis unten unter Zusatzinformationen)

1777 5.2.1.3 C.HP.QES – Qualifizierte Signatur HBA

1778 ~~GS-A_5533 – Umsetzung Zertifikatsprofil C.HP.QES~~

1779 ~~Der TSP-X.509 QES MUSS C.HP.QES gemäß Tab_PKI_270 umsetzen.~~

1780 {<=}

1781 **GS-A_5533-01 - Umsetzung Zertifikatsprofil C.HP.QES**

1782 Der TSP-X.509 QES MUSS C.HP.QES gemäß Tab_PKI_270_1 umsetzen. [<=]

1783 **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>)

1823 *Hinweis: Statt der ICCSN in der Bildungsregel können auch andere TSP-*
1824 *spezifische IDs verwendet werden, die der Länge der ICCSN entsprechen.*

- 1825 • **serialNumber, givenName, surname, title und commonName als SET-**
1826 **OF**

1827 Die Attribute serialNumber, givenName, surname, ggf. title und commonName werden in
1828 einem SET-OF als ein einziges multivaluedRDN kodiert. Die entsprechenden
1829 Kodierungsregeln von X.690 Abs. 11.6 "Set-of components" und RFC_5280 Anhang B
1830 (Reihenfolge im SET) müssen berücksichtigt werden. Attribute im RDN müssen anhand
1831 der String-Länge der Attribut-Werte, in aufsteigender Reihenfolge sortiert, in die
1832 Kodierung einfließen.

1833 **5.3 SMC-B – Ausweis einer Organisation/Einrichtung des** 1834 **Gesundheitswesens**

1835 Die SMC Typ B definiert die Identität einer Organisation oder Einrichtung des
1836 Gesundheitswesens (z. B. Arztpraxis, Krankenhaus, Apotheke, Betriebsstätte nicht-
1837 ärztlicher Psychotherapeut oder auch Geschäftsstellen von Kostenträgern) und wird
1838 deshalb auch „Institutionenkarte“ genannt.

1839 Bzgl. Nutzung bestehender LE-Datensätze für SMC-B-Zertifikate ist die Anforderung GS-
1840 A_4970 (s. Kap. 5.2) zu berücksichtigen.

1841 **5.3.1 Definition der Organisationsidentität**

1842 Der eindeutige Identitätsname der Organisation wird durch folgende Felder gebildet:

- 1843 • **commonName**
1844 • **organizationName**
1845 • **countryName**

1846 Die serialNumber kann weiterhin als technisches Unterscheidungsmerkmal (falls mittels
1847 commonName und organizationName bei einem Issuer keine Eindeutigkeit des Subjects
1848 erreicht werden kann) im SubjectDN dienen.

1849 Der eindeutige Identitätsschlüssel der Organisation oder Einrichtung des
1850 Gesundheitswesens wird durch die Telematik-ID in der Zertifikatserweiterung
1851 „Admission“ abgebildet; s. Abschnitt 4.6.

1852 **GS-A_4971 - Zuordnung von SMC-B zur Institution**

1853 Die Kartenherausgeber MÜSSEN die eindeutige Zuordnung von SMC-B zur berechtigten
1854 Institution sicherstellen.
1855 [**<=**]

1856 Der Zugriff eines Leistungserbringers auf medizinische Daten von Anwendungen der
1857 elektronischen Gesundheitskarte gemäß §291a SGB V mit einer SMC-B darf nur in
1858 Verbindung mit einem HBA erfolgen.

1859 **A_15190 - HBA als Grundlage zur Nutzung von medizinischen Anwendungen**

1860 Die Kartenherausgeber von SMC-B, welche Leistungserbringern den Zugriff auf Daten
1861 von Anwendungen der elektronischen Gesundheitskarte gemäß §291a SGB V ermöglicht,
1862 MÜSSEN mittels organisatorischer oder technischer Maßnahmen sicherstellen, dass der

1863 Nutzer der SMC-B entweder selbst über einen HBA verfügt oder zu einer Institution
1864 gehört, der ein HBA zur Verfügung steht.[<=]

1865 Hinweis 1: Von dieser Regelung sind SM-B für Gesellschafterorganisationen (ohne CVC)
1866 oder Kostenträger (Zugriffsprofil CHA.8 [gemSpec_PKI#Tab_PKI_254]) nicht betroffen,
1867 da sie keinen Zugriff auf die entsprechenden Daten erlauben. Ebenso sind SM-B mit
1868 Zugriffsprofil CHA.1 [gemSpec_PKI#Tab_PKI_254] nicht betroffen, da sie dem Zugriff
1869 des Versicherten selbst in der KTR-AdV-Umgebung dienen.

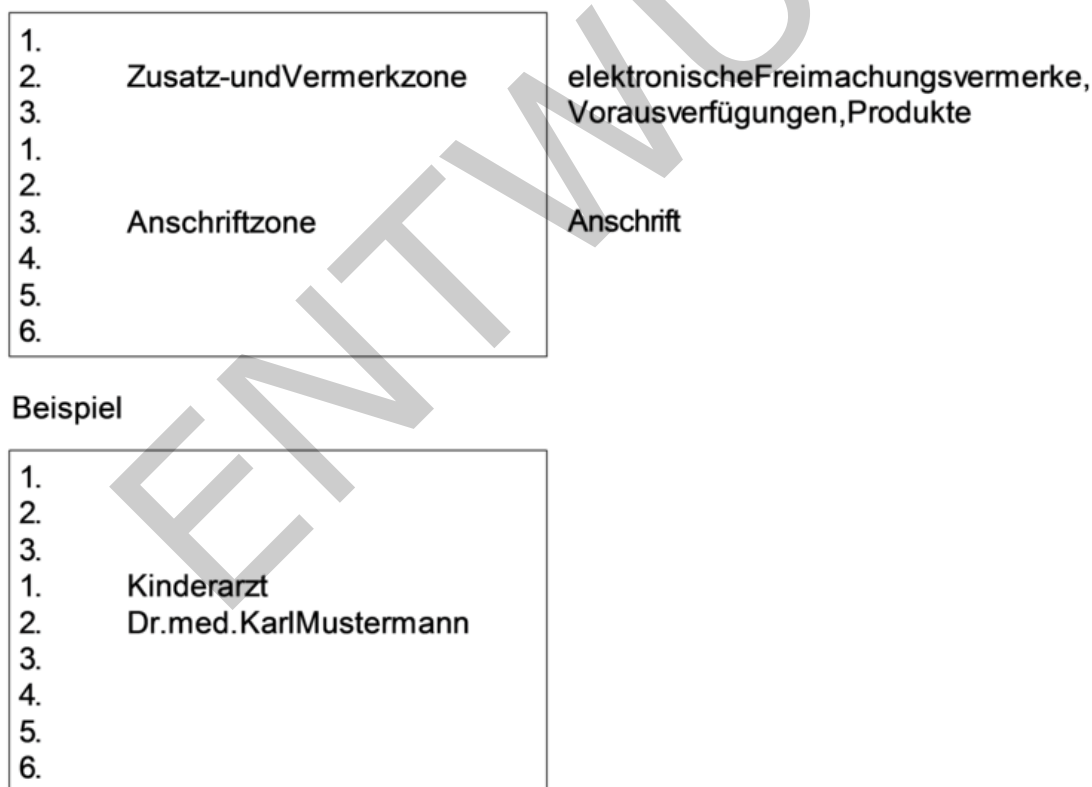
1870 Hinweis 2: Ein HBA im Sinne dieser Anforderung ist ein HBA oder eine HBA-
1871 Vorläuferkarte (HBA-qSig und ZOD_2.0).

1872 5.3.2 Aufbau Anschriftzone nach [DIN5008]

1873 Die ersten zwei Zeilen der Anschriftzone werden für den Inhalt des `commonName`
1874 verwendet.

1875 Der `commonName` beinhaltet somit den „Kurzname“ der Institution, so wie sie sich selbst
1876 auf dem Anschriftenfeld findet. Da dieses Feld von der Institution frei gestaltet werden
1877 kann, ist nachfolgend nur eine exemplarische Variante abgebildet. Die Art der Institution
1878 ist eindeutig in der Admission Extension hinterlegt.

1879



1880

1881

1882

Abbildung 4: Das Anschriftenfeld nach DIN5008

1883 *Hinweis: Für den Sonderfall der „Berufsausübungsgemeinschaften“ (ehemals*
1884 *„Gemeinschaftspraxen“) gilt die Ausnahme, dass die Zeile 2 der Anschriftzone [DIN5008]*
1885 *optional ist. Somit ist Zeile 1 Pflichtfeld, die Zeilen 3 und/oder 4 sind wie Zeile 2 optional,*
1886 *um darüber die Praxisbezeichnung (Bsp. „Praxis Bülowbogen“) mit aufzunehmen.*

1887 **5.3.3 Umgang mit überlangen Attributen im SubjectDN**

1888 Siehe Kapitel 4.8.3.5 „SubjectAltNames“.
1889

1890 **5.3.4 X.509 Zertifikatsprofile der SMC-B**

1891 **5.3.4.1 C.HCI.AUT – Authentisierung SMC- B**

1892 **GS-A_4600 - Umsetzung Zertifikatsprofil C.HCI.AUT**

1893 Der TSP-X.509 nonQES MUSS C.HCI.AUT gemäßTab_PKI_238 umsetzen.
1894 [\leq]

1895

1896 **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 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_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
		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: digitalSignature keyEncipherment Für Schlüsselgeneration ECDSA: digitalSignature	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_aut> 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	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			

1897 *) Sektorspezifische Ausprägungen der SMC-B Zertifikate sind dem Anhang A zu
1898 entnehmen

1899 5.3.4.2 C.HCI.ENC – Verschlüsselung SMC-B

1900 GS-A_4601 - Umsetzung Zertifikatsprofil C.HCI.ENC

1901 Der TSP-X.509 nonQES MUSS C.HCI.ENC gemäß Tab Tab_PKI_239 umsetzen.

1902 [\leq]

1903

1904 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 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_4362] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
extensions				critical
	SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels der Organisation/Einrichtung des Gesundheitswesens	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 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_enc> 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	
		<i>andere Erweiterungen</i>		0	
signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4362]		
signature			Wert der Signatur		

1905 *) Sektorspezifische Ausprägungen der SMC-B Zertifikate sind dem Anhang A zu
1906 entnehmen

1907 5.3.4.3 C.HCI.OSIG – Signatur SMC-B

1908 GS-A_4602 - Umsetzung Zertifikatsprofil C.HCI.OSIG

1909 Der TSP-X.509 nonQES MUSS C.HCI.OSIG gemäß Tab_PKI_240 umsetzen.
1910 [\leq]

1911

1912 **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	
			KeyUsage {2 5 29 15}	nonRepudiation	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_osig> 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	
			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	

		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			

1913 *) Sektorspezifische Ausprägungen der SMC-B Zertifikate sind dem Anhang A zu
1914 entnehmen

1915 5.4 HSM-B – Ausweis einer Organisation/Einrichtung des 1916 Gesundheitswesens

1917 Bestehen höhere Performance-Anforderungen an eine SMC-B (z. B. in Krankenhäusern),
1918 kann als funktionales Äquivalent eine HSM-basierte Lösung eingesetzt werden. Gemäß
1919 Anforderung [gemKPT_PKI_TIP#TIP1-A_2084] sind die X.509-Zertifikate eines HSM-B
1920 entsprechend den Festlegungen der X.509-Zertifikate für SMC-B auszuführen.

1921 5.5 gSMC-KT – eHealth-Kartenterminal

1922 Für gSMC-KT ausgestellte Zertifikate werden nicht statusgeprüft. Für diese Zertifikate
1923 muss ein TSP somit keinen Sperrdienst und keine Statusauskünfte bereitstellen.

1924 Siehe dazu auch Anhang A der [gemRL_TSL_SP_CP#AnhA].

1925 Das Zertifikat eines gSMC-KT enthält nur Informationen über die Identität des SMKT, des
1926 Geräteherstellers sowie des Zertifikateherausgebers. Die Bedeutung des Zertifikats
1927 beschränkt sich auf folgende Aspekte:

- 1928 • die gSMC-KT basiert auf einer hierfür durch die gematik zugelassenen
1929 Chipkartenplattform
- 1930 • das Zertifikat wurde durch einen hierfür durch die gematik zugelassenen TSP-
1931 X.509 nonQES an einen KT-Hersteller ausgestellt

1932 Das Zertifikat eines gSMC-KT repräsentiert nach dem Pairing die Identität eines eHealth-
1933 Kartenterminals.

1934 5.5.1 Definition der Kartenterminalidentität

1935 Die Identität einer gSMC-KT ist durch den *SubjectDN* (*subject distinguishedName*) des
1936 Zertifikats gegeben mit folgendem Aufbau:

- 1937 • **commonName** = [ICCSN des gSMC-KT]
- 1938 • **organizationName** = [Name des Kartenterminal-Herstellers],
- 1939 • **countryName** = [Herkunftsland des Kartenterminal-Herstellers]

1940 **5.5.2 X.509 Zertifikatsprofile der gSMC-KT**

1941 **5.5.2.1 C.SMKT.AUT – Identität der gSMC-KT**

1942 **GS-A_4604 - Umsetzung Zertifikatsprofil C.SMKT.AUT**

1943 Der TSP-X.509 nonQES MUSS C.SMKT.AUT gemäß Tab_PKI_241 umsetzen.

1944 [\leq]

1945

1946 **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		

1947 5.6 gSMC-K – Konnektor

1948 5.6.1 Definition und Zuweisung der Konnektoridentität

1949 Die Identität einer gSMC-K wird durch die ICCSN in Verbindung mit dem Datum der
1950 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

1984 **5.6.4 X.509 Zertifikatsprofile des Konnektors**

1985 **5.6.4.1 C.NK.VPN – VPN-Authentisierung Netzkonnektor**

1986 Die Identität des Netzkonnektors dient der Authentisierung gegenüber den zentralen
1987 Netzwerkdiensten und wird für die Anmeldung an den VPN-Konzentratoren genutzt.

1988 **GS-A_4609 - Umsetzung Zertifikatsprofil C.NK.VPN**

1989 Der TSP-X.509 nonQES MUSS C.NK.VPN gemäß Tab_PKI_242 umsetzen.
1990 [\leq]

1991

1992 **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		

1993
1994
1995

5.6.4.2 C.AK.AUT - Authentisierung Anwendungskonnektor

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

1996 **GS-A_4610 - Umsetzung Zertifikatsprofil C.AK.AUT**
 1997 Der TSP-X.509 nonQES MUSS C.AK.AUT gemäß Tab_PKI_243 umsetzen.
 1998 [\leq]

1999

2000 **Tabelle 36: Tab_PKI_243 Zertifikatsprofil C.AK.AUT Authentisierung**
 2001 **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		

2002 5.6.4.3 C.SAK.AUT - Authentisierung Signaturdienst

2003 Die Identität des Signaturdienstes dient zur Authentisierung gegenüber den
2004 Kartenterminals. Darüber hinaus muss sich der Signaturdienst des Konnektors gegenüber
2005 dem Heilberufsausweis mittels eines CV-Zertifikats (C.SAK.AUTD_CVC) mit einer
2006 spezifischen Rolle (Profil) ausweisen, um Stapelsignaturen durchführen zu können.

2007 GS-A_4611 - Umsetzung Zertifikatsprofil C.SAK.AUT

2008 Der TSP-X.509 nonQES MUSS C.SAK.AUT gemäß Tab_PKI_244 umsetzen.
2009 [<=]

2010

2011 **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

			<i>Für Schlüsselgeneration ECDSA:</i> 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		

2012 5.7 VPN-Zugangsdienst

2013 Der VPN-Zugangsdienst ermöglicht den Konnektoren einerseits einen IPsec-Tunnel über
2014 ein Transportnetz zum VPN-Zugangsdienst und verbindet darüber die Organisationen des
2015 Gesundheitswesens mit dem zentralen Netz der TI, zusätzlich ermöglicht er den
2016 Konnektoren den Aufbau eines separaten IPsec-Tunnels über das Transportnetz, durch
2017 den der sichere Internetzugang erreichbar ist. Für diesen Zweck ist eine separate
2018 kryptographische Identität vorgesehen.

2019 5.7.1 Definition und Zuweisung der Zugangsdienstidentitäten

2020 Die beiden Identitäten des Zugangsdienstes werden durch den jeweiligen FQDN des
2021 Dienstes in Verbindung mit einem zusätzlichen Instanzenkennzeichen gebildet.

2022 Bzgl. Verwendung des FQDN ist die Anforderung GS-A_4720 (s. Kap. 5.9.1) zu
2023 berücksichtigen.

2024 **5.7.2 Aufbau des SubjectDN**

2025 Siehe Tab_PKI_245.

2026 **5.7.3 X.509-Zertifikatsprofile des Zugangsdienstes**

2027 **5.7.3.1 C.VPNK.VPN - VPN-Authentisierung Zugangsdienst TI**

2028 **GS-A_4613 - Umsetzung Zertifikatsprofil C.VPNK.VPN**

2029 Der TSP-X.509 nonQES MUSS C.VPNK.VPN gemäß Tab_PKI_245 umsetzen.
2030 [\leq]

2031

2032 **Tabelle 38: Tab_PKI_245 Zertifikatsprofil C.VPNK.VPN VPN-Authentisierung**
2033 **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.

[<=]

2040
2041

**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		

2042 5.8 ZD – Zentrale Dienste

2043 5.8.1 Definition der Identität der Zentralen Dienste

2044 Die Identität des Zentralen Dienstes wird durch den Fully Qualified Domain Name (FQDN)
2045 des Dienstes in Verbindung mit einem zusätzlichen Instanzenkennzeichen gebildet.

2046 5.8.2 Aufbau des SubjectDN

2047 Siehe Tab_PKI_247.

2048 Die Eindeutigkeit der Identität des Dienstes innerhalb der Telematikinfrastruktur MUSS
2049 bereits durch den Inhalt der folgenden Attribute innerhalb des *SubjectDN* gegeben sein:

- 2050 • **subject.commonName**
- 2051 • **subject.serialNumber**

2052 **5.8.3 X.509 Zertifikatsprofile der Zentralen Dienste**

2053 **5.8.3.1 C.ZD.TLS-S Server-Authentisierung (ehemals C.SF.SSL-S)**

2054 **GS-A_4615 - Umsetzung Zertifikatsprofil C.ZD.TLS-S**

2055 Der TSP-X.509 nonQES MUSS C.ZD.TLS-S gemäß Tab_PKI_247 umsetzen.

2056 [\leq]

2057

2058 **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		

2059 5.9 FD – Fachanwendungsspezifische Dienste

2060 5.9.1 Definition der Identität der Fachanwendungsspezifischen 2061 Dienste

2062 Gemäß übergreifender Definition beinhaltet der Begriff „Fachanwendungsspezifischer
2063 Dienst“ die Fachdienste und Intermediäre.

2064 Als Erweiterung eines fachanwendungsspezifischen Dienstes gelten weiterhin
2065 Clientmodule, die in der Consumerzone (LE-Umgebung) auf den lokalen Systemen
2066 Teilfunktionalitäten des Dienstes bereitstellen oder unterstützen (s. a. Kap. 5.10).

2067 Die Identität des Fachanwendungsspezifischen Dienstes wird durch den Fully Qualified
2068 Domain Name (FQDN) des Dienstes in Verbindung mit einem zusätzlichen
2069 Instanzenkennzeichen gebildet.

2070 **GS-A_4720 - Verwendung registrierter Werte für subjectDN**

2071 Anbieter von zentralen und fachanwendungsspezifischen Diensten in der TI MÜSSEN bei
2072 der Beantragung von X.509-Zertifikaten für den FQDN im **subjectDN** ausschließlich einen
2073 FQDN aus dem zugehörigen Namensraum der TI unter Beachtung des zugewiesenen
2074 Domainnamen verwenden. Dabei MUSS der verwendete FQDN mit dem FQDN der
2075 zugewiesenen Komponente übereinstimmen.
2076 [\leq]

2077 **5.9.2 Aufbau des SubjectDN**

2078 Siehe Tab_PKI_249 oder Tab_PKI_250.

2079 Die Eindeutigkeit der Identität des Dienstes innerhalb der Telematikinfrastruktur MUSS
2080 bereits durch den Inhalt der folgenden Attribute innerhalb des *SubjectDN* gegeben sein:

- 2081 • `subject.commonName`
- 2082 • `subject.serialNumber`

2083 **5.9.3 X.509 Zertifikatsprofile der Fachanwendungsspezifischen**
2084 **Dienste**

2085 **5.9.3.1 C.FD.TLS-C Client-Authentisierung (ehemals C.SF.SSL-C)**

2086 **GS-A_4617 - Umsetzung Zertifikatsprofil C.FD.TLS-C**

2087 Der TSP-X.509 nonQES MUSS C.FD.TLS-C gemäß Tab_PKI_249 umsetzen.
2088 [\leq]

2089

2090 **Tabelle 41: Tab_PKI_249 C.FD.TLS-C Client-Authentisierung Fachanwendungsspezifische**
2091 **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		

2092 **5.9.3.2 C.FD.TLS-S Server-Authentisierung (ehemals C.SF.SSL-S)**

2093 **GS-A_4618 - Umsetzung Zertifikatsprofil C.FD.TLS-S**

2094 Der TSP-X.509 nonQES MUSS C.FD.TLS-S gemäß Tab_PKI_250 umsetzen.

2095 [\leq]

2096

2097 **Tabelle 42: Tab_PKI_250 C.FD.TLS-S Server-Authentisierung**
2098 **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		

2099

2100 5.9.3.3 C.FD.SIG Signatur Fachdienst

2101 A_15172 - Umsetzung Zertifikatsprofil C.FD.SIG

2102 Der TSP-X.509 nonQES MUSS C.FD.SIG gemäß Tab_PKI_251 umsetzen. [<=]

2103

2104

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		

2105

2106 5.9.3.4 C.FD.AUT Authentisierung Fachdienst

2107 A_15591 - Umsetzung Zertifikatsprofil C.FD.AUT

2108 Der TSP-X.509 nonQES MUSS C.FD.AUT gemäß Tab_PKI_275 umsetzen.[<=]

2109

2110 **Tabelle 44: Tab_PKI_275 C.FD.AUT Authentisierung fachanwendungsspezifische**
2111 **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		
			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	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_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 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

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

2112

2113 **5.9.3.5 C.FD.ENC Verschlüsselung Fachdienst**

2114 **A_16213 - Umsetzung Zertifikatsprofil C.FD.ENC**

2115 Der TSP-X.509 nonQES MUSS C.FD.ENC gemäß Tab_PKI_276 umsetzen.[<=]

2116

2117 **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		

2118

2119 5.10 CM – Clientmodul

2120 5.10.1 Definition der Identität eines Clientmoduls

2121 Der Identitätsbereich „Fachanwendungsspezifischer Dienst“ umfasst Dienste und
2122 Intermediäre innerhalb der TI sowie zusätzlich damit in funktionalem Zusammenhang
2123 stehende Clientmodule in der Consumerzone (LE-Umgebung).

Die Identität eines Clientmoduls wird durch den Anbieter des zugehörigen Fachanwendungsspezifischen Dienstes nach dessen eigener Systematik festgelegt. Seitens der TI-Plattform werden hierzu keine Vorgaben definiert, da diese Zertifikate keine Plattformleistung der TI darstellen, sondern die gegenseitige Authentisierung zwischen einem spezifischen Dienst und seinem zugehörigen lokalem Clientmodul unterstützen.

Ein berechtigter Antragsteller für ein C.FD.TLS-* Zertifikat kann auf der Grundlage derselben Berechtigung zusätzlich auch C.CM.TLS-CS-Zertifikate beziehen.

Ein Clientmodul-Zertifikat wird von der CA für Fachdienstzertifikate ausgestellt.

Ein Clientmodul-Zertifikat kann als Exemplar- oder Gattungszertifikat ausgestellt werden.

5.10.2 Aufbau des SubjectDN

Siehe Tab_PKI_267.

Die Eindeutigkeit der Identität des Clientmoduls ist durch den Anbieter des Dienstes nach eigener Systematik sicher zu stellen:

- `subject.commonName`
- `subject.serialNumber`

5.10.3 X.509 Zertifikatsprofil des Clientmoduls

5.10.3.1 C.CM.TLS-CS Clientmodul-Authentisierung

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

Der TSP-X.509 nonQES MUSS C.CM.TLS-CS gemäß Tab_PKI_267 umsetzen.

[<=]

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}	Für Schlüsselgeneration RSA: digitalSignature keyEncipherment Für Schlüsselgeneration ECDSA: 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		

2147

2148

2149 5.11 SGD-HSM – Schlüsselgenerierungsdienst-HSM

2150 5.11.1 Beschreibung der Identität

2151 Ein HSM mit einem speziellen Firmware-Modul ist zentraler Bestandteil eines
2152 Schlüsselgenerierungsdienstes [gemSpec_SGD]. Ein solches als SGD-HSM bezeichnetes
2153 HSM muss eine für einen Client (bspw. ein ePA-Frontend des Versicherten (FdV) oder ein
2154 FM ePA) prüfbare Identität besitzen. Diese Identität wird verwendet um damit öffentliche
2155 ECDH-Schlüssel zu authentisieren, die für die Schlüsselgenerierungsfunktionalität
2156 benötigt werden. Dabei ist es wichtig, dass es verschiedene SGD-HSM gibt, jeweils solche
2157 mit einer Identität entweder vom Typ 1 (oid_sgd1_hsm) und solche vom Typ 2
2158 (oid_sgd2_hsm) (vgl. professionItem in C.SGD-HSM.AUT und [\[gemSpec OID#GS-A_4446\]](#),
2159 und vgl. auch [\[gemSpec SGD#A_17848\]](#)).

2160 Die Identität wird von der Komponenten-PKI ausgegeben. Ein solches Zertifikat wird
2161 jedoch explizit in der TSL aufgeführt (vgl. [\[gemSpec SGD#A_17846\]](#)) und wird daher
2162 von den Clients über einen speziellen Weg geprüft
2163 (vgl. [\[gemSpec SGD#A_17847\]](#)). Durch die direkte Aufführung in der TSL ist die
2164 Identität unabhängig von der Sicherheitsleistung der Komponenten-PKI.

2165 5.11.2 X.509 Zertifikatsprofil der SGD-HSM

2166 A_17844 - Umsetzung Zertifikatsprofil C.SGD-HSM.AUT

2167 Der TSP-X.509 nonQES MUSS das Zertifikatsprofil C.SGD-HSM.AUT nach Tab_PKI_296
2168 umsetzen.

2169
2170 [\leq]

2171 **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		
		extensions			critical
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Dienstes	1	FALSE
		KeyUsage {2 5 29 15}	digitalSignature	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_sgd_hsm_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 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		

2172

2173 5.12 CA - Zertifikatsprofile

2174 **GS-A_4730 - Eindeutige Identifizierung der CA-Zertifikate**

2175 Der TSP-X.509 nonQES und TSP-X.509 QES MUSS bei der Beantragung von X.509-CA-
2176 Zertifikaten sicherstellen, dass der subjectDN die CA eindeutig innerhalb der TI
2177 identifiziert.

2178 [\leq]

2179 **GS-A_4731 - Attribute der CA-Zertifikate**

2180 Der TSP-X.509 nonQES und TSP-X.509 QES SOLL bei der Beantragung von X.509-CA-
2181 Zertifikaten nur die Attribute mit der Kardinalität 1 verwenden.

2182 [\leq]

2183 **GS-A_4732 - Extension der CA-Zertifikate**

2184 Der TSP-X.509 nonQES (eGK) und die gematik Root-CA SOLLEN bei der Erstellung eines
2185 Root- bzw. self-signed CA-Zertifikats die Extension AuthorityKeyIdentifier entfallen
2186 lassen.

2187 [\leq]

2188 Die eindeutige Benennung der CA-Zertifikate im Feld `commonName` erfolgt gemäß Kap. 2.2
2189 nach dem Schema:

2190 `<holder>.<usage>-CA<n>`

2191 (Analog zum Schema `<type>.<holder>.<usage><n>`, welches in Kap. 2.2 beschrieben
2192 wird.)

2193 Der Suffix `<n>` kennzeichnet hierbei die fortlaufende Nummerierung innerhalb eines Typs
2194 von CA-Zertifikaten – beginnend ab dem Wert 1. Dabei wird `<n>` auch bei
2195 Schlüsselgenerations-Wechseln fortgesetzt.

2196

2197 **GS-A_4735 - Namenskonvention für CA-Zertifikate**

2198 Der TSP-X.509 nonQES und TSP-X.509 QES MUSS für jede von ihm betriebene CA die
2199 Namenskonventionen gemäß [GS-A_4588], [GS-A_4590] umsetzen sowie die
2200 Namensbildung im Feld `commonName` nach dem Schema `<holder>.<usage>-CA<n>`
2201 vornehmen.

2202 [\leq]

2203 5.12.1 GEM.RCA<n> - Zentrale Root-CA_nonQES

2204 **GS-A_4736 - Umsetzung Zentrale nonQES-Root-CA-Zertifikat**

2205 Die gematik-Root-CA MUSS die Namenskonvention und Attributsbelegung der Felder für
2206 folgende CA-Zertifikate umsetzen gemäß:

2207 a) Tab_PKI_211 für gematik-Root-CA,

2208 b) Tab_PKI_212 für i) Zentrale Aussteller-CA_nonQES, ii) Aussteller-CA_nonQES, iii)

2209 TSL-Signer-CA. [\leq]

2210

2211 **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
	<i>andere Erweiterungen</i>		0	
	signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
	signature	Wert der Signatur		

2212 **5.12.2 <tsp>.<usage>-CA<n> - Aussteller-CA_nonQES**

2213 **GS-A_4737 - Umsetzung nonQES-CA-Zertifikate**

2214 Der TSP-X.509 nonQES MUSS für die von ihm betriebenen CAs die Attributsbelegung der
2215 Felder gemäß Tab_PKI_212 und die Namenskonvention gemäß Tab_PKI_213 umsetzen.
2216 [**<=>**]

2217

2218 **Tabelle 49: Tab_PKI_212 <tsp>.<usage>-CA<n> –Aussteller- CA_nonQES der TI**

Element	Inhalt	Kar.	
certificate	C.<tsp>.<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	<tsp>.<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		
-----------	-------------------	--	--

2219 *) Für CA-Zertifikate der zentralen PKI wird für <tsp> die Bezeichnung "GEM" und für
2220 <tspName> "gematik GmbH" eingesetzt; für von TSPs betriebene Sub-CAs wird das
2221 jeweilige TSP-Kürzel sowie der vollständige TSP-Name eingefügt.

2222 **) Die erlaubten Werte für <usage> und <usageName> werden in Tab_PKI_213
2223 aufgeführt.

2224 5.12.3 <tsp>.HBA-qCA<n> - Aussteller-CA_QES

2225 GS-A_4948 - Umsetzung QES-CA-Zertifikate

2226 Der TSP-X.509 QES MUSS für die Zertifikate der von ihm betriebenen CAs die
2227 Attributsbelegung der Felder gemäß Tab_PKI_215 umsetzen.

2228 [\leq]

2229

2230 **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		

2231 *) Der Name kann mit oder ohne Leerzeichen vor der laufenden Nr. <n> geschrieben
2232 werden.

5.13 OCSP – Statusauskunftsdienst

5.13.1 Definition der OCSP-Signer-Identität

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

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

Der TSP-X.509 nonQES und der Anbieter des TSL-Dienstes MÜSSEN bei der Beantragung von X.509-OCSP-Signer-Zertifikaten sicherstellen, dass der subjectDN das OCSP-Signer-Zertifikat eindeutig innerhalb der TI identifiziert.

[<=]

GS-A_4739 - Attribute der OCSP-Signer-Zertifikate

Der TSP-X.509 nonQES und der Anbieter des TSL-Dienstes SOLLEN bei der Beantragung von X.509-OCSP-Signer-Zertifikaten nur die Attribute mit der Kardinalität 1 verwenden.

[<=]

GS-A_5514 - Verwendung separater OCSP-Signer-Zertifikate

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

[<=]

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

5.13.2 Aufbau des SubjectDN

Siehe Tab_PKI_253.

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

5.13.3.1 C.GEM.OCSP OCSP-Signer-Zertifikat

GS-A_4741 - Umsetzung Zertifikatsprofil C.GEM.OCSP

Der TSP-X.509 nonQES, die gematik-Root-CA und der TSL-Dienst MÜSSEN C.GEM.OCSP gemäß Tab_PKI_253 umsetzen.

[<=]

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-Diensteanbieters	1	
		countryName	Land der Anschrift des OCSP-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 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		

2267 5.14 CRL – Statusauskunftsdienst

2268 GS-A_5066 - Indirekte CRL gemäß [Common-PKI]

2269 Der TSP-X.509 nonQES für Komponenten MUSS CRLs für X.509-Zertifikate als indirekte
2270 CRLs gemäß [Common-PKI] und [RFC5280#4.2.1.13] unter Verwendung eines
2271 dedizierten CRL-Signers erzeugen.
2272 [\leq]

2273 5.14.1 Definition der CRL-Signer-Identität

2274 Die Identität eines CRL-Signers wird durch den `commonName` gebildet, zur Sicherstellung
2275 der Eindeutigkeit bedarfsweise ergänzt um ein Merkmal im Feld `subject.serialNumber`.

2276 GS-A_4935 - Eindeutige Identifizierung der CRL-Signer-Zertifikate

2277 Der TSP-X.509 nonQES MUSS bei der Beantragung von X.509-CRL-Signer-Zertifikaten
2278 sicherstellen, dass der `subjectDN` das CRL-Signer-Zertifikat eindeutig innerhalb der TI
2279 identifiziert.
2280 [\leq]

2281 GS-A_4936 - Attribute der CRL-Signer-Zertifikate

2282 Der TSP-X.509 nonQES SOLL bei der Beantragung von X.509-CRL-Signer-Zertifikaten nur
2283 die Attribute mit der Kardinalität 1 verwenden.
2284 [\leq]

2285 GS-A_4937 - Ableitung des CRL-Signer-Zertifikates

2286 Ein TSP-X.509 nonQES MUSS das CRL-Signer-Zertifikat der jeweiligen
2287 Schlüsselgeneration für die von ihm be-triebenen CRL-Dienste aus der VPNK-CA
2288 derselben Schlüsselgeneration beziehen.
2289 [\leq]

2290 GS-A_5515 - Bezug separater CRL-Signer-Zertifikate

2291 Ein TSP-X.509 nonQES, der CRL-Dienste betreibt, MUSS für jede unterstützte
2292 Schlüsselgeneration (gemäß [gemSpec_Krypt#GS-A_4357]) jeweils ein separates CRL-
2293 Signer-Zertifikat beziehen.
2294 [\leq]

2295 5.14.2 Aufbau des SubjectDN

2296 Siehe Tab_PKI_214.

2297

2298 **5.14.3 X.509 Profil des CRL-Signer-Zertifikates**

2299 **5.14.3.1 C.GEM.CRL CRL-Signaturzertifikat**

2300 **GS-A_4939 - Umsetzung Zertifikatsprofil C.GEM.CRL**

2301 Der TSP-X.509 nonQES MUSS C.GEM.CRL gemäß Tab_PKI_214 umsetzen.

2302 [\leq]

2303

2304 **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-Dienstanbieters	1	
	countryName	Land der Anschrift des CRL-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 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
	<i>andere Erweiterungen</i>		0	
	signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS- A_4357]		
	signature	Wert der Signatur		

2305 5.15 TSL - Zertifikatsprofile

2306 5.15.1 Definition der TSL-Signer-Identität

2307 Die Identität des TSL-Signers wird durch einen eindeutigen **commonName** bedarfsweise
2308 ergänzt um ein Merkmal im Feld **subject.serialNumber** gebildet.

2309 **GS-A_4742 - Eindeutige Identifizierung der TSL-Signer-Zertifikate**

2310 Der Anbieter des TSL-Dienstes MUSS bei der Beantragung von X.509-TSL-Signer-
2311 Zertifikaten sicherstellen, dass der subjectDN das TSL-Signer-Zertifikat eindeutig
2312 innerhalb der TI identifiziert.

2313 [**<=**]

2314 **GS-A_4743 - Attribute der TSL-Signer-Zertifikate**

2315 Der Anbieter des TSL-Dienstes SOLL bei der Beantragung von X.509-TSL-Signer-
2316 Zertifikaten nur die Attribute mit der Kardinalität 1 verwenden.

2317 [**<=**]

2318 5.15.2 Aufbau des SubjectDN

2319 Siehe Tab_PKI_252_01.

2320 5.15.3 X.509 Zertifikatsprofil der TSL-Signer-CA

2321 **GS-A_4744 - Zentrale TSL-Signer-CA-Zertifikate**

2322 Der Anbieter des TSL-Dienstes MUSS für die von ihm betriebenen TSL-Signer-CAs die
2323 Attributsbelegung der Felder gemäß Tab_PKI_212 und die Namenskonvention für den

2324 TSL-Dienst gemäß Tab_PKI_213 umsetzen.
2325 [\leq]

2326

2327 **A_17686 - TSL-Signer-CA Cross-Zertifikate (ECC-Migration)**

2328 Der TSL-Dienst MUSS für die TSL-Signer-CA der Schlüsselgeneration ECDSA beidseitige
2329 Cross-Zertifikate zu der aktiven TSL-Signer-CA der Schlüsselgeneration RSA bereitstellen
2330 und dabei die folgenden Punkte berücksichtigen:

- 2331 • das bereits existierende Schlüsselmateriale (PublicKey) der TSL-Signer-CA (ECDSA)
2332 wird durch die TSL-Signer-CA (RSA) mit deren PrivateKey signiert und damit das
2333 Cross-Zertifikat mit dem Namen C.GEM.TSL-CA<Index der ECDSA-CA>-
2334 CROSS<Index der RSA-CA> erzeugt
- 2335 • das bereits existierende Schlüsselmateriale (PublicKey) der TSL-Signer-CA (RSA)
2336 wird durch die TSL-Signer-CA (ECDSA) mit deren PrivateKey signiert und damit
2337 das Cross-Zertifikat mit dem Namen C.GEM.TSL-CA<Index der RSA-CA>-
2338 CROSS<Index der ECDSA-CA> erzeugt

2339

2340 [\leq]

2341

2342 **A_17687 - TSL-Signer-CA Cross-Zertifikate – Attributsbelegung (ECC-Migration)**

2343 Der TSL-Dienst MUSS für die zu erstellenden Cross-Zertifikate die Attributsbelegung der
2344 Felder gemäß Tab_PKI_212 umsetzen, wobei Abweichungen bei folgenden Elementen
2345 vorzunehmen sind:

- 2346 • <certificate> = C.GEM.TSL-CA<X>-CROSS<Y>
- 2347 • <commonName> = GEM.TSL-CA<X>-CROSS<Y>

2348 Dabei ist jeweils <X> der Index des zu signierenden TSL-Signer-CA-Schlüssels
2349 (PublicKey) und <Y> der Index des signierenden TSL-Signer-CA-Schlüssels (PrivateKey).

2350

2351 [\leq]

2352 *Beispiele für TSL-Signer-CA Cross-Zertifikate:*

- 2353 • C.GEM.TSL-CA1-CROSS3
2354 Erklärung: Das Cross-Zertifikat ist für TSL-Signer-CA1 (RSA Public Key)
2355 ausgestellt und von TSL-Signer-CA3 (ECDSA) signiert.
- 2356 • C.GEM.TSL-CA3-CROSS1
2357 Erklärung: Das Cross-Zertifikat ist für TSL-Signer-CA3 (ECDSA Public Key)
2358 ausgestellt und von TSL-Signer-CA1 (RSA) signiert.

2359

2360 **5.15.4 TSL-Signer- Zertifikat**

2361 **GS-A_4745-01 - Umsetzung Zertifikatsprofil C.TSL.SIG für TSL-Dienst**

2362 Der TSL-Dienst MUSS das TSL-Signer-Zertifikat C.TSL.SIG gemäß Tab_PKI_252_01
2363 umsetzen.

2364 [\leq]

2365

2366 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		

2367 Hinweis: [ETSI_TS_102_231_V3.1.2], Kap. 6.2 empfiehlt, den Inhalt von
2368 „SchemeOperatorName“ (vgl. [gemSpec_TSL]) als „organizationName“ im Subject
2369 Distinguished Name einzutragen. „SchemeOperatorName“ wiederum MUSS gemäß
2370 [ETSI_TS_102_231_V3.1.2], Kap. 5.3.4 den eingetragenen Namen enthalten. "gematik
2371 Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH" ist aber zu lang für
2372 das Feld „organizationName“, vgl. Kap. 5.3.3: Umgang mit überlangen Attributen im
2373 SubjectDN und Kap. 4.8.3.5: SubjectAltNames.

2374

2375 5.15.5 TSL-OCSP-Responder-Zertifikat

2376 GS-A_4747 - Umsetzung Zertifikatsprofil C.GEM.OCSP für TSL-Dienst

2377 Der TSL-Dienst MUSS für die OCSP-Prüfung des TSL-Signer-Zertifikats ein OCSP-Signer-
2378 Zertifikat C.GEM.OCSP gemäß Tab_PKI_253 umsetzen.

2379
2380 [<=]

2381 GS-A_4918 - Ableitung des OCSP-Signer-Zertifikates für TSL-Dienst

2382 Der TSL-Dienst MUSS das OCSP-Signer-Zertifikat der jeweiligen Schlüsselgeneration
2383 gemäß [RFC6960] von der TSL-Signer-CA derselben Schlüsselgeneration beziehen. [<=]

2384

6 CV-Zertifikate

2385 Dieses Kapitel enthält Anforderungen an die Profilattribute für CV-Zertifikate sowie deren
2386 Verwendung. Hierzu gehört auch die Festlegung von Vorgaben zur Identifizierung der
2387 ausgebenden CA bzw. des Zertifikatsinhabers sowie die Definition von Rollen- und
2388 Geräteprofilen mit denen Zugriffsrechte des Karteninhabers bzw. die Verfügbarkeit von
2389 Funktionseinheiten eines Gerätes verbunden sind.

2390 **GS-A_4972 - Bezug des CV-Zertifikat**

2391 Ein Kartenherausgeber KANN das nicht-personenbezogene CV-Zertifikat nach
2392 entsprechender Registrierung vom TSP-CVC-CA beziehen.
2393 [\leq]

2394 **GS-A_4973 - Ausstellung aller CV-Zertifikate einer Karte durch gleiche CVC-Sub-CA**

2395 Der Kartenherausgeber MUSS sicherstellen, dass alle zu einer Chipkarte gehörenden CV-
2396 Zertifikate durch dieselbe CA der zweiten Ebene erzeugt werden.
2397 [\leq]
2398

2399 **6.1 Festlegungen zur Abgrenzung**

2400 Grundsätzlich sind CV-Zertifikatsprofile zu unterscheiden für

- 2401 • CVC-CAs, die als Herausgeber von CV-Zertifikaten für Endteilnehmer fungieren,
2402 und
- 2403 • Endteilnehmer, d. h. Kartentypen wie eGK, HBA, SM-B und gSMC.

2404 Der öffentliche Root-Schlüssel der PKI für CV-Zertifikate wird direkt als Datenfeld in den
2405 Karten hinterlegt. Die Bereitstellung des öffentlichen Root-Schlüssels in Form eines CV-
2406 Zertifikates ist nicht erforderlich.

2407 **GS-A_4974 - CV-Ausstattung von Smartcards der TI**

2408 Ein Kartenherausgeber, der Smartcards für Einsatzbereiche der TI herausgeben will,
2409 MUSS sicherstellen, dass die Karten über folgende CV-Ausstattung verfügen: (a)
2410 mindestens ein CV-Schlüsselpaar mit zugeordnetem CV-Zertifikat. Es können mehrere
2411 Schlüsselpaare mit jeweils eigenem CV-Zertifikat und unterschiedlichen Profilattributen
2412 enthalten sein, die die Karte für unterschiedliche Funktionen in der TI-
2413 Anwendungslandschaft autorisieren können (b) das CV-CA-Zertifikat der zweiten Ebene
2414 sowie (c) der öffentliche Schlüssel der CV-Root.
2415 [\leq]

2416 **6.2 Namensregeln und -formate**

2417 Anforderungen an Namensregeln und -formate ergeben sich aus der Identifikation von
2418 Herausgebern von CV-Zertifikaten sowie von Zertifikatsinhabern.

2419 Der Herausgeber eines CV-Zertifikats wird über das Datenelement Certificate Authority
2420 Reference (CAR) identifiziert. Anforderungen an die Formatierung und den Inhalt der CAR
2421 sind im Abschnitt 6.4.3.2 beschrieben.

2422 Der Inhaber eines CV-Zertifikats wird im Datenelement Certificate Holder Reference
2423 (CHR) angegeben. Anforderungen an die Formatierung und den Inhalt der CHR sind im
2424 Abschnitt 6.4.3.4 beschrieben.

2425 6.3 Rollen- und gerätebasierte Zugriffsprofile

2426 6.3 Rollen und Profile

2427 In einem CV-Zertifikat einer Chipkarte ist das Zugriffsprofil dieser Chipkarte enthalten.
2428 Dabei wird gemäß [gemKPT_PKI_TIP#5.1] unterschieden zwischen einem Zugriffsprofil
2429 für eine

- 2430 • Authentisierung einer Rolle (CV-Rollen-Zertifikate) bzw. für eine
- 2431 • Authentisierung einer Funktionseinheit eines Gerätes (CV-Gerätezertifikate).

2432 Die technische Umsetzung der Zuordnung zu Zugriffsprofilen in CV-Zertifikaten erfolgt für
2433 Karten der Generation 2 über eine Flagliste, die die Berechtigungen steuert und im Feld
2434 CHAT gespeichert ist (siehe Kapitel 6.4.6).

- 2435 •

2436 6.3.1 Rollenauthentisierung

2437 **GS-A_4620 - Zugriffsprofil einer eGK**

2438 Der Kartenherausgeber MUSS sicherstellen, dass das CV-Rollen-Zertifikat einer eGK als
2439 Zugriffsprofil CHAT.0 den Wert '00 0000 0000 0000' hat.

2440
2441 [\leq]

2442 **GS-A_4621 - Zugriffsprofil von HBA und SM-B (SMC-B, HSM-B)**

2443 Der Kartenherausgeber MUSS sicherstellen, dass bei einem HBA bzw. einer SM-B das
2444 Zugriffsprofil in einem CV-Zertifikat der Rolle des Karteninhabers bzw. der Organisation
2445 gemäß Tabelle Tab_PKI_254 entspricht.

2446 Eine Ausnahme hiervon ist die SM-B für Gesellschafterorganisationen, da sie keine CV-
2447 Rollenzertifikate erhält.

2448 [\leq]

2449 **A_16179 - Zugriffsprofil einer KTR-AdV**

2450 Der Kartenherausgeber für SM-B KTR-AdV MUSS sicherstellen, dass die CV-Rollen-
2451 Zertifikate für eine KTR-AdV jeweils das Zugriffsprofil CHAT.1 bzw. CHAT.0 gemäß
2452 [gemSpec_PKI#Tab_PKI_254] besitzen.

2453 [\leq]

2454 In der folgenden Tabelle werden die Zugriffsprofile im Kontext der sie nutzenden
2455 fachlichen Akteure dargestellt. Der Kern der Tabelle wurde mit den LEOs, Kostenträgern
2456 und dem BMG abgestimmt. Sie bilden die Basis für die Rechtezuweisung auf den
2457 Smartcards der Generation 2.

2458 Die Tabelle enthält auch, welche Organisation als sog. „Qualifizierende Stelle“ (vgl.
2459 Tab_PKI_254) die Berechtigung für die Zugriffsprofile in CV-Zertifikaten vergibt und
2460 damit die Betreiber von CVC-CAs der zweiten Ebene autorisiert, diese Profile in die CV-
2461 Zertifikate einzubringen. Für derzeit nicht verwendete Profile ist diese Zuordnung offen.

2462 Es werden die Zugriffsprofile 0 – 9 für eine Rollenauthentisierung unterschieden:

2463

2464 Tabelle 53: Tab_PKI_254 Zugriffsprofile für eine Rollenauthentisierung

Profile / Akteure / Rollen und OID aus gemSpec_PKI					X.509 Admission Extension	
Zugriffsprofil	Kartentyp	Beschreibung fachlicher Akteur	Fachliche Rolle	Qualifizierende Stelle	profession Item	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.2 A	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.2 ZA	HBA – Zahnarzt	Zahnarzt in einer Institution	Zahnarzt	BZÄK	Zahnärztin/Zahnarzt	oid_zahnarzt
CHAT.2 A	(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 Institution des Arztes	Nicht definiert	Nicht definiert	Nicht definiert	Nicht definiert

CHAT.2 ZA	(H)BA für Mitarbei- ter- (innen) in Zahnarz- t- praxis	Mitarbeiter medizinische Institution (z. B. in Zahnarztpraxis). Der „Mitarbeiter medizinische Institution“ verkörpert gegenüber der TI die Institution des Zahnarztes	Nicht definiert	Nicht definiert	Nicht definiert	Nicht definiert
CHAT.2 A	SMC-B	Mitarbeiter medizinische Institution Arztpraxis (inkl. Praxis ärztlicher Psychotherapeut) mit Autorisierung und Protokollierung gemäß § 291a Abs. 5 Satz 4 SGB V. Der „Mitarbeiter medizinische Institution“ verkörpert gegenüber der TI die Institution des Arztes.	Mitarbeit er Arzt	KV	Betriebsstät- te Arzt	oid_praxis_arzt
CHAT.2 Z 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.	Mitarbeit er Zahnarzt	KZBV	Zahnarztpra- xis	oid_zahnarztprax- is
CHAT.2 A	SMC-B	Mitarbeiter medizinische	Mitarbeit er	DKTIG	Krankenhau- s	oid_krankenhaus

		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.	Krankenhaus			
3						
CHAT.3	HBA – Apotheker	Apotheker in einer öffentlichen Apotheke oder einer Krankenhausapotheke, jeweils mit Sitz in Deutschland.	Apotheker	BAK	Apotheker/in	oid_apotheker
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_pharmazieingenieur oid_apotheken assistent
CHAT.3	SMC-B	Mitarbeiter Apotheke mit Autorisierung und Protokollierung gemäß § 291a Abs.5 Satz 4 SGB V. Der „Mitarbeiter	Mitarbeiter Apotheke	Für den jeweiligen Betriebs-erlaubnis-inhaber zuständige Apotheker	Öffentliche Apotheke	oid_öffentliche_apotheke

		Apotheke" verkörpert gegenüber der TI die Institution des Apothekers.		- kammer		
4						
CHAT.4	HBA – Psychot he- rapeut	Psychotherapeut / Psychologischer Psychotherapeut / Kinder- und Jugendlichen- psychotherapeut	Psychoth e- rapeut	BPTK	Psychothe- rapeut/ in Psycholo- gische/r Psychothe- rapeut/ in Kinder- und Jugendliche n- psychothe- rapeut/-in	oid_psychothera peut oid_ps_psychoth e rapeut oid_kuj_psychot he rapeut
CHAT.4	SMC-B	Institutionskarte eines Psychotherapeuten. Der mit der Karte mögliche Zugriff auf die medizinischen Anwendungen der eGK ist ausschließlich dem Psychotherapeut, dem psychologischen Psychotherapeuten und dem Kinder- und Jugendlichen-psychotherapeuten selbst gestattet und nicht seinen berufsmäßigen Gehilfen.	Mitarbeit er Psychoth e- rapeut	KV	Betriebsstät te Psychothe- rapeut	oid_praxis_psych othe rapeut
5						
CHAT.5	(H)BA sonstige Leistungs- erbringer	Heilmittelerbringer mit (H)BA Hilfsmittelerbringer mit BA	Sonstige Leistungs- erbringer	Nicht definiert	Nicht definiert	Nicht definiert
6						

CHA.6	SMC	Kein fachlicher Akteur - wird nicht verwendet	Nicht definiert	Nicht definiert	Nicht definiert	Nicht definiert
7						
CHAT.7	(H)BA	Rettungsassistent Bei den Akteuren handelt es sich um „Angehörige eines anderen Heilberufs, die für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung“ (§ 291a Abs. 4 Satz 1 Nr. 2e) absolviert haben.	Anderer Heilberuf	Nicht definiert	Rettungsassistent/-in Notfallsanitäter/-in	oid_rettungsassistent oid_notfallsanitaeter
CHAT.7	SMC-B	Mobile Einrichtung Rettungsdienst	Nicht definiert	Nicht definiert	Betriebsstätte Mobile Einrichtung Rettungsdienst	oid_mobile_einrichtung_rettungsdienst
8						
CHAT.8	SMC-B (ohne Zugriff auf med. Daten)	Mitarbeiter von Gesundheitseinrichtungen ohne eigenen HBA oder BA	Mitarbeiter Medizinische Institutionen	Nicht definiert	Nicht definiert	Nicht definiert
CHAT.8		Mitarbeiter von Krankenkassen	Mitarbeiter Kostenträger	GKV-SV	Betriebsstätte Kostenträger	oid_kostentraeger
CHAT.8		Verifikationskarten Kostenträger	Mitarbeiter Kostenträger	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	Nicht definiert	Nicht definiert	Nicht definiert

			Institutio n			
CHAT.9		b) ohne zugeordneten Akteur, sichere Einsatzumgebung für Versicherten	b) Versicherter	Nicht definiert	Nicht definiert	Nicht definiert

2465

2466 6.3.2 Authentisierung einer Funktionseinheit

2467 Es werden die Zugriffsprofile CHAT.51, CHAT.53 – CHAT.55 für eine Authentisierung
2468 einer Funktionseinheit unterschieden (CV-Gerätecertifikate). Es handelt sich dabei um
2469 CV-Zertifikate der Generation 2:

2470

2471 **Tabelle 54: Tab_PKI_255 Zugriffsprofile G2 für eine Authentisierung einer**
2472 **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

2473 *Hinweis 1: Das Zugriffsprofil CHAT.52 war für die SMC-RFID vorgesehen, diese wird*
2474 *derzeit nicht verwendet.*

2475 *Hinweis 2: Ursprünglich wurden auch Zugriffsprofile bzw. CV-Gerätecertifikate für die*
2476 *Generation 1 festgelegt. In der Praxis kommen aber nur CV-Gerätecertifikate der*
2477 *Generation 2 zum Einsatz.*

2478

2479 **GS-A_4622 - Zugriffsprofil einer gSMC-K**

2480 Der Kartenherausgeber MUSS sicherstellen, dass das CV-Gerätecertifikat einer gSMC-K
2481 als Flagliste den Wert '0000 0000 0001' hat (Zugriffsprofil 51 für G2 gemäß
2482 Tab_PKI_918).

2483 [\leq]

2484 **GS-A_5126 - Zugriffsprofil einer gSMC-KT**

2485 Der Kartenherausgeber MUSS sicherstellen, dass das CV-Gerätecertifikat einer gSMC-KT
2486 als Flagliste den Wert '00 0000 0000 0002' hat (Zugriffsprofil 54 für G2 gemäß
2487 Tab_PKI_918).

2488 [\leq]

2489 **GS-A_4623 - Zugriffsprofil eines HBA**

2490 Der Kartenherausgeber MUSS sicherstellen, dass das CV-Gerätezertifikat eines HBA als
2491 Flagliste den Wert '00 0000 0000 000C' hat (Zugriffsprofil 53 für G2 gemäß
2492 Tab_PKI_918).
2493 [\leq]

2494 **GS-A_4624 - Zugriffsprofil einer SM-B**

2495 Der Kartenherausgeber MUSS sicherstellen, dass das CV-Gerätezertifikat einer SM-B als
2496 Flagliste den Wert '00 0000 0000 0004' hat (Zugriffsprofil 55 für G2 gemäß
2497 Tab_PKI_918).
2498 [\leq]

2499 **GS-A_5335 - Zugriffsprofil einer gSMC-K für Administrationszwecke**

2500 Der Kartenherausgeber MUSS sicherstellen, dass die Flagliste des CV-Zertifikats für die
2501 Authentisierung einer gSMC-K gegenüber einem Aktualisierungssystem den Wert '00
2502 0000 0000 0000' hat (Zugriffsprofil 0 für G2 gemäß Tab_PKI_918).
2503 [\leq]

2504 **6.4 CV-Zertifikatsprofile der Generation 2**

2505 Für G2-Karten ist der Einsatz von elliptischen Kurven (ELC) in CV-Zertifikaten
2506 vorgesehen, basierend auf den Festlegungen in [EN 14890-1]. Die CV-Zertifikate
2507 erhalten eine komplett neue Struktur, es erfolgt ein Umstieg von nicht
2508 selbstbeschreibenden, RSA-basierten Zertifikaten auf selbstbeschreibende, ELC-basierte
2509 Zertifikate mit Anhang (Appendix).

2510 Im Gegensatz zu den nicht selbstbeschreibenden Zertifikaten werden die
2511 selbstbeschreibenden Zertifikate durch Konkatenation der Datenobjekte gebildet. Dabei
2512 wird jedem Datenfeld ein Tag und ein Längenfeld vorangestellt, damit jedes Datenfeld
2513 eindeutig interpretiert werden kann (Tag, Length, Value-Prinzip (TLV)). Der zu
2514 signierende Teil ist die Konkatenation der Datenobjekte.

2515 **6.4.1 Berechtigung einer CVC-CA zur Zertifikatserstellung**

2516 TSP-CVC, die zur Ausstellung von CV-Zertifikaten für

- 2517 • genau einen Kartentyp mit einem oder mehreren zugehörigen CV-
2518 Gerätezertifikaten
- 2519 • und genau ein Rollen-Zugriffsprofil (nur bei HBA u. SMC-B)

2520 berechtigt sind, erhalten ein CV-CA-Zertifikat, in dem nur genau diese Zugriffsprofile
2521 über die hinterlegte Flaglist abgebildet sind.

2522 TSP-CVC, die zur Ausstellung von CV-Zertifikaten für mehrere Kartentypen berechtigt
2523 sind, können ein CV-CA-Zertifikat mit kombinierten Zugriffsprofilen nach folgendem
2524 Schema beantragen:

- 2525 • CVC-CA für eGK
2526 Diese CV-Zertifikate sind immer aus einer dedizierten CVC-CA zu erstellen. Eine
2527 Kombination mit anderen Zugriffsprofilen ist nicht zulässig.
- 2528 • CVC-CA für HBA und SMC-B
2529 Die Ausstellung von CV-Zertifikaten dieser Kartentypen in allen
2530 Ausprägungsformen kann durch eine einzige CVC-CA mit kombinierten
2531 Zugriffsprofilen (veroderte Flaglist) erfolgen.

- 2532 • CVC-CA für gSMC-x
2533 Die Ausstellung von CV-Zertifikaten dieser Kartentypen in allen
2534 Ausprägungsformen kann durch eine einzige CVC-CA mit kombinierten
2535 Zugriffsprofilen (veroderte Flaglist) erfolgen.

2536 **GS-A_5213 - CA-Flaglist für CVC-CA eines Profiltyps**

- 2537 Die CVC-Root-CA MUSS bei der Generierung eines CA-Zertifikates
2538 (a) für eine CVC-CA, welche ausschließlich zur Ausstellung von EE-Zertifikaten eines
2539 bestimmten Zugriffsprofils (oder eines spezifischen Tupels aus Geräte- und Rollen-
2540 Zugriffsprofilen) aus Tab_PKI_919, genau die zugeordnete Flaglist aus der Spalte Sub-CA
2541 in das CA-Zertifikat einbringen.
2542 (b) Für eine CVC-CA mit kombinierten Zugriffsprofilen ist die Veroderung der zugehörigen
2543 Flaglisten aus Tab_PKI_919 zulässig für die Zugriffsprofile
2544 (b.1) aller HBA- und SMC-B sowie
2545 (b.2) aller gSMC-K und gSMC-KT.
2546 [\leq]

2547 **6.4.2 Aufbau und Bestandteile der CV-Zertifikate der Generation 2**

2548 Obwohl die Struktur selbstbeschreibend ist, enthalten die CV-Zertifikate einen Certificate
2549 Profile Identifier, der angibt, welche Datenelemente in welcher Reihenfolge in das CV-
2550 Zertifikat einzustellen sind. Im Einzelnen sind das:

- 2551 1. Certificate Profile Identifier (CPI) gemäß 6.4.3.1
2552 2. Certification Authority Reference (CAR) gemäß 6.4.3.2
2553 3. Öffentlicher Schlüssel: Das Datenobjekt zum öffentlichen Schlüssel enthält neben
2554 einer OID, welche den Verwendungszweck des öffentlichen Schlüssels
2555 kennzeichnet, den öffentlichen Punkt Q (siehe [EN 14890-1#Table 234]).
2556 4. Certificate Holder Reference (CHR) gemäß 6.4.3.4
2557 5. Certificate Holder Authorization Template (CHAT): Eine Flagliste
2558 beschreibt gemäß [EN 14890-1#14.9.3.6] die Rechte, die einem
2559 Zertifikatsinhaber nach einer erfolgreichen Authentisierung eingeräumt werden.
2560 6. Certificate Effective Date (CED): Dieses Datenobjekt enthält das Datum des
2561 Inkrafttretens des Zertifikates.
2562 7. Certificate Expiration Date (CXD): Dieses Datenobjekt enthält das Datum mit dem
2563 Gültigkeitsende des Zertifikates.

2564 **Berechtigungssteuerung über die Flagliste im Feld CHAT**

2565 Die Zugriffsberechtigung einer Karte auf die Inhalte einer anderen Karte (Bsp. HBA auf
2566 eGK) kann sehr differenziert über einzelne Bits der sog. Flagliste im Feld CHAT gesteuert
2567 werden.

- 2568 • Im CVC-CA-Zertifikat (ausgestellt durch die CVC-Root-CA) steuert die Flagliste,
2569 welche CV-Berechtigungen durch diese CA ausgestellt werden können.
2570 • Im CV-Zertifikat (ausgestellt durch eine CVC-CA) einer Karte steuert die Flagliste,
2571 über welche Berechtigung diese Karte (d. h. der Karten- und Zertifikatsinhaber)
2572 gegenüber anderen Karten der TI verfügt.

6.4.3 Zertifikatsprofil eines CV-Zertifikates für ELC-Schlüssel

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

6.4.3.1 Certificate Profile Identifier (CPI)

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

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

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

GS-A_4987 - Wert des Card Profile Identifier in G2

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

6.4.3.2 Certification Authority Reference (CAR)

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

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-Schlüsselpaare	'02' für ELC/ECC	letzte 2 Ziffern des Jahres der CA-Schlüsselerzeugung

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

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

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

- 2600 **GS-A_4989 - Länge der Certificate Authority Reference in G2**
 2601 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
 2602 MUSS für die CAR ein acht Oktett langes Wertfeld verwenden.
 2603 [\leq]
- 2604 **GS-A_4990 - Verwendung des Feldes Certificate Authority Reference in G2**
 2605 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
 2606 MUSS das Feld CAR weiter unterteilen in die Konkatenation der Datenelemente CA Name,
 2607 Service-Indikator, CA-spezifische Information, Algorithmenreferenz und Datum sowie
 2608 dabei die Festlegungen bzgl. Länge und zugelassener Werte gemäß Tab_PKI_266
 2609 berücksichtigen.
 2610 [\leq]
- 2611 **GS-A_4991 - Zuordnung von CAR zu Schlüsselpaar des Herausgebers für G2**
 2612 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
 2613 MUSS sicherstellen, dass die Zuordnung zwischen Certificate Authority Reference (CAR)
 2614 und Schlüsselpaar eindeutig ist.
 2615 [\leq]

2616 6.4.3.3 Öffentlicher Schlüssel

2617 Für den Aufbau des öffentlichen Schlüssels gelten die folgenden Anforderungen, konform
 2618 zu [BSI-TR-03110#D.3]:

- 2619 **GS-A_4992 - Datenobjekt für den öffentlichen Schlüssel**
 2620 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
 2621 MUSS den öffentlichen Schlüssel in das Datenobjekt '7F49' einstellen.
 2622 [\leq]

- 2623 **GS-A_4993 - Aufbau eines öffentlichen Schlüssel**
 2624 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
 2625 MUSS in das Wertfeld des Datenobjekt '7F49' des öffentlichen Schlüssels genau zwei
 2626 Datenobjekte eintragen. Dabei MÜSSEN das erste Datenobjekt ein Objektidentifizier
 2627 ODPuK gemäß Tabelle Tab_PKI_901 und das zweite Datenobjekt ein Datenobjekt
 2628 DO '86' mit dem öffentlichen Punkt Q, dessen Wertfeld sich aus Tabelle Tab_PKI_902
 2629 ergibt, sein.
 2630 [\leq]

2631

2632 **Tabelle 56: Tab_PKI_901 Objektidentifizier des öffentlichen Schlüssels eines CV-**
 2633 **Zertifikats der Generation 2**

Verwendungszweck des CV-Zertifikats	Domain- parameter	Objektidentifizier
Transport des öffentlichen Signaturprüf Schlüssels 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	$OID_{PuK} = '06-L06-authS_gemSpec-COS-G2_ecc-with-sha512'$ $OID_{Hex} = '06\ 06\ 2B2403050303'$ $OID_{Dez} = '1.3.36.3.5.3.3'$

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

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

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

6.4.3.4 Certificate Holder Reference (CHR)

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

GS-A_4994 - Datenobjekt für die Certificate Holder Reference

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

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

2662 der Chipkarte besteht.
2663 [\leq]

2664 Bei dem Aufbau und der Belegung des Feldes CHR wird unterschieden zwischen einem
2665 CV-Zertifikat für eine CVC-CA und einem CV-Zertifikat für eine Chipkarte:

2666 **Tabelle 58: Tab_PKI_258 Aufbau CHR**

CV-Zertifikat für	Länge CHR	Inhalt	
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	CHR	Anforderung für CHR
eGK	C.eGK.AUT_CVC.E256	'00 09' ICCSN	Card-G2-A_2363
HBA	C.HPC.AUTR_CVC.R2048	'00 10' ICCSN	Card-G2-A_3385
	C.HPC.AUTR_CVC.E256	'00 06' ICCSN	Card-G2-A_3386
	C.HPC.AUTD_SUK_CVC.E256	'00 09' ICCSN	Card-G2-A_3387
SMC-B	C.SMC.AUTR_CVC.R2048	'00 10' ICCSN	Card-G2-A_3388
	C.SMC.AUTR_CVC.E256	'00 06' ICCSN	Card-G2-A_3389
	C.SMC.AUTD__RPE_CVC.E256	'00 09' ICCSN	Card-G2-A_3390
gSMC-K	C.SMC.AUT_CVC.E256	'00 05' ICCSN	Card-G2-A_3328
	C.SMC.AUT_CVC.E384	'00 06' ICCSN	Card-G2-A_3331

	C.SAK.AUTD_CVC.E256	'00 0A' ICCSN	Card-G2- A_2638
	C.SAK.AUTD_CVC.E384	'00 0F' ICCSN	Card-G2- A_2640
gSMC-KT	C.SMC.AUTD_RPS_CVC.E256	'00 0A' 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	-

2667 *Anmerkung: Die ICCSN der KTR-AdV entspricht der ICCSN der verwendeten SM-B KTR-*
2668 *AdV.*

2669 Eine Chipkarte kann auch mehrere Schlüsselpaare für eine C2C-Authentisierung (und
2670 damit auch mehrere CV-Zertifikate) enthalten. Über die konkrete Belegung von 'xx xx'
2671 wird sichergestellt, dass die Zuordnung von CV-Zertifikat zu einem Schlüsselpaar der
2672 Chipkarte eindeutig ist. Das genaue Vorgehen hierbei wird durch die einzelnen
2673 Spezifikationen der konkreten Chipkarten der TI festgelegt.

2674 **6.4.3.5 Certificate Holder Authorization Template (CHAT)**

2675 Die hier folgenden Anforderungen sind konform zu [EN 14890-1#14.9.3.6].

2676 **GS-A_4996 - Wertfeld des Certificate Holder Authorization Templates**

2677 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2678 MUSS das Certificate Holder Authorization Template in das Datenobjekt '7F4C'
2679 einstellen.
2680 [\leq]

2681 **GS-A_4997 - Aufbau der Certificate Holder Authorization Templates**

2682 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2683 MUSS in das Wertfeld des Datenobjekt '7F4C' genau zwei Datenobjekte eintragen.
2684 Dabei MUSS das zweite Datenobjekt ein Datenobjekt DO'53' gemäß Tabelle
2685 Tab_PKI_910 (bei Anwendung von oid_cvc_fl_ti) oder Tab_PKI_911 (bei Anwendung von
2686 oid_cvc_fl_cms) sein und das erste Datenobjekt einen Objektidentifizier OIDflags gemäß
2687 Tabelle Tab_PKI_904 enthalten, der angibt, wie die Flags im zweiten Datenobjekt zu
2688 interpretieren sind. Die Umsetzung eines bestimmten Berechtigungsprofils MUSS durch
2689 die Kombination der Einzelflags gemäß TAB_PKI_918 erfolgen.
2690 [\leq]

2691

2692 **Tabelle 59: Tab_PKI_904 Mögliche Objektidentifizier OIDflags in Certificate Holder**
2693 **Authorization Templates**

OIDflags
OIDflags = '06-L06-oid_cvc_fl_ti

OID_{flags} = '06-L06- oid_cvc_fl_cms

2694 *Hinweis: Die Festlegung der OID erfolgt in der Spezifikation Festlegung von OIDs*
2695 *[gemSpec_OID#Tab_PKI_408].*

2696 **6.4.3.6 Certificate Effective Date (CED)**

2697 Die hier folgenden Angaben sind konform zu [BSI-TR-03110-3#D.2.1.3].

2698 **GS-A_4998 - Datenobjekt des Certificate Effective Date**

2699 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2700 MUSS das Certificate Effective Date in das Datenobjekt '5F25' einstellen.
2701 [\leq]

2702 **GS-A_4999 - Länge des Certificate Effective Date**

2703 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2704 MUSS für das Certificate Effective Date ein Wertfeld der Länge sechs Oktett einstellen.
2705 [\leq]

2706 **GS-A_5000 - Format des Certificate Effective Date**

2707 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2708 MUSS ein Datum in der Form YYMMDD in unkomprimierter BCD Form in das Wertfeld des
2709 Certificate Effective Date eintragen.
2710 [\leq]

2711 **6.4.3.7 Certificate Expiration Date (CXD)**

2712 Die hier folgenden Angaben sind konform zu [BSI-TR-03110-3#D.2.1.3].

2713 **GS-A_5001 - Datenobjekt des Certificate Expiration Date**

2714 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2715 MUSS das Certificate Expiration Date in das Datenobjekt '5F24' einstellen.
2716 [\leq]

2717 **GS-A_5002 - Länge des Certificate Expiration Date**

2718 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2719 MUSS für das Certificate Expiration Date ein Wertfeld der Länge sechs Oktett einstellen.
2720 [\leq]

2721 **GS-A_5003 - Format des Certificate Expiration Date**

2722 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2723 MUSS ein Datum in der Form YYMMDD in unkomprimierter BCD Form in das Wertfeld des
2724 Certificate Expiration Date eintragen.
2725 [\leq]

2726 **6.4.3.8 Zu signierende Nachricht M eines CV-Zertifikates der Generation** 2727 **2**

2728 **GS-A_5004 - Tag der zu signierenden Nachricht M eines CV-Zertifikates**

2729 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2730 MUSS die zu signierende Nachricht des CV-Zertifikats in das Datenobjekt '7F4E'
2731 einstellen.
2732 [\leq]

2733 **GS-A_5005 - Datenstruktur der zu signierenden Nachricht M eines CV-** 2734 **Zertifikates**

2735 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2736 MUSS die zu signierende Nachricht M des CV-Zertifikats gemäß Tabelle Tab_PKI_905

2737 bilden.
2738 [\leq]

2739

2740 **Tabelle 60: Tab_PKI_905 Zu signierende Nachricht M eines CV-Zertifikates**

M	=	$DO'7F4E'$
$DO'7F4E'$	=	$'7F4E'-L7F4E-($
		$DO'5F29' \quad \quad DO'42' \quad $
		$DO'7F49' \quad \quad DO'5F20' \quad $
		$DO'7F4C' \quad \quad DO'5F25' \quad $
		$DO'5F24'$
		$)$

2741 **6.4.4 Struktur und Inhalt eines CV-Zertifikates für ELC-Schlüssel**
2742 **der Generation 2**

2743 **GS-A_5006 - Signatur des Zertifikatsdatenobjekts**

2744 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2745 MUSS die Signatur der Nachricht M des CV-Zertifikates in Abhängigkeit vom
2746 Domainparameter des privaten Signaturschlüssels PrK des Herausgebers gemäß Tabelle
2747 Tab_PKI_906 erzeugen.
2748 [\leq]

2749

2750 **Tabelle 61: Tab_PKI_906 Signatur der Nachricht M eines CV-Zertifikats**

Domainparameter des privaten Schlüssels PrK	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

2751

2752 **GS-A_5007 - Tag eines Zertifikatsdatenobjekts**

2753 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2754 MUSS die Inhalte des Zertifikatsdatenobjekts in das Datenobjekt $'7F21'$ einstellen.
2755 [\leq]

2756 **GS-A_5008 - Aufbau eines Zertifikatsdatenobjekts**

2757 Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA)
2758 MUSS das CV-Zertifikat als zusammengesetztes Datenobjekt gemäß Tabelle
2759 Tab_PKI_907 erzeugen. Er MUSS dabei sicherstellen, dass das zusammengesetzte
2760 Datenelement genau die beiden primitiven Datenobjekte in der dargestellten Reihenfolge

2761 enthält.
2762 [\leq]

2763

2764 **Tabelle 62: Tab_PKI_907 Struktur und Inhalt eines CV-Zertifikat**

Tag	L	Wert		
'7F21'	L7F21	CV-Zertifikat		
		Tag	L	Wert
		'7F4E'	L7F4E	Nachricht <i>M</i> (gemäß Tabelle 60: Tab_PKI_905 Zu signierende Nachricht <i>M</i> eines CV-Zertifikates) ohne Tag und Längenangabe
		'5F37'	L5F37	Signatur = <i>R</i> <i>S</i> (gemäß Tabelle 61: Tab_PKI_906 Signatur der Nachricht <i>M</i> eines CV-Zertifikats)

2765 6.4.5 Struktur und Inhalt eines CV-Zertifikates für ELC-Schlüssel 2766 der Generation 2

2767 Die nachfolgenden Strukturdiagramme fassen die zuvor beschriebenen Definitionen und
2768 Festlegungen zu den einzelnen Feldern der CV-Zertifikate übersichtlich zusammen,
2769 normativ sind jedoch nur die in den Anforderungen ausgewiesenen Definitionen.

2770 6.4.5.1 Struktur und Inhalt von CA CV-Zertifikaten für ELC-Schlüssel

2771 **Tabelle 63: Tab_PKI_912 CA CV-Zertifikate für 256 bit ELC-Schlüssel, insgesamt**
2772 **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 = R S		

2773

2774

2775

Tabelle 64: Tab_PKI_913 CA CV-Zertifikate für 384 bit ELC-Schlüssel, insgesamt 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	

2776

2777

2778

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	Wert		
			5F29	01	CPI = 70		
			42	08	CAR		
			7F49	818E	öffentlicher Schlüssel		
					Tag	L	Wert
					06	08	2A8648CE3D040304
					86	8181	P2OS(Q, 64)
			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	8180	Signatur = <i>R</i> <i>S</i>				

2779

2780 6.4.5.2 Struktur und Inhalt von Cross-CV-Zertifikaten für ELC-Schlüssel

2781 Ein Cross-CV-Zertifikat ist ein CV-Zertifikat, welches verschiedene Vertrauensräume
2782 verbindet. Eine CVC-Root-CA bestätigt den öffentlichen Schlüssel einer anderen CVC-
2783 Root-CA.

2784 **Tabelle 66: Tab_PKI_937 Cross-CV-Zertifikat für ELC-Schlüssel**

Tag	L	Wert				
´7F21´	*	CV-Zertifikat				
		Tag	L	Wert		
		´7F4E´	*	Nachricht <i>M</i>		
			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				

2785 Anmerkung: Die mit * gefüllten Feldinhalte müssen anhand der in 6.4.5.1 spezifizierten
2786 Zertifikatsprofile für 256/384/512 bit ELC-Schlüssel ermittelt bzw. berechnet werden.

2787 6.4.5.3 Struktur und Inhalt von Endnutzer-CV-Zertifikaten für ELC- 2788 Schlüssel

2789 **Tabelle 67: Tab_PKI_915 Endnutzer-CV-Zertifikate für 256 bit ELC-Schlüssel, insgesamt**
2790 **222 Oktett**

Tag	L	Wert						
7F21	81DA	CV-Zertifikat						
				Tag	L	Wert		
				7F4E	8193	Nachricht M		
						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 = R S	

2791
2792

2793 **Tabelle 68: Tab_PKI_916 Endnutzer-CV-Zertifikate für 384 bit ELC-Schlüssel, insgesamt**
2794 **287 Oktett**

Tag	L	Wert		
7F21	82011A	CV-Zertifikat		
		Tag	L	Wert
		7F4E	81B3	Nachricht M
			Tag	L Wert
			5F29	01 CPI = 70
			42	08 CAR
			7F49	6B öffentlicher Schlüssel
				Tag L Wert
			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	

2795
2796

2797 **Tabelle 69: Tab_PKI_917 Endnutzer-CV-Zertifikate für 512 bit ELC-Schlüssel, insgesamt**
2798 **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				

2799 Der Wert für OID_{Puk} ergibt sich dabei entsprechend Tabelle 57: Tab_PKI_901
2800 Objektidentifizier des öffentlichen Schlüssels eines CV-Zertifikats der Generation 2.

2801 6.4.6 Flagliste mit Berechtigungen in CV-Zertifikaten für ELC- 2802 Schlüssel

2803 Die Flagliste *flagList* im DO '53' innerhalb von CHAT eines CV-Zertifikates erfüllt zwei
2804 Aufgaben: Zum einen zeigt sie in den oberen beiden Bits an, welche Rolle das CV-
2805 Zertifikat in der PKI-Struktur spielt. Die übrigen Bits zeigen an, welche Aktionen nach
2806 einer erfolgreichen Authentisierung freigeschaltet werden. Die Festlegungen zur Rolle
2807 sind konform zu [BSI-TR-03110-3#C.4]. Anders als in [BSI-TR-03110-3#C.4] wird im
2808 Folgenden dem höchstwertigen Bit der Flagliste die Nummer null zugeordnet. In den Bits
2809 b2 bis b55 zeigt ein gesetztes Bit an, dass durch eine erfolgreiche Authentisierung das
2810 Recht erworben wird die zugehörige Aktion durchzuführen. In den Bits b2 bis b55 zeigt
2811 ein gelöscht Bit an, dass auch nach einer erfolgreichen Authentisierung die zugehörige
2812 Aktion nicht freigeschaltet ist.

2813

2814 **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

2815

2816 *Hinweis: Die Rechtedifferenzierung zwischen den Rollen Ärztin/Arzt und*
2817 *Zahnärztin/Zahnarzt ist in die Tabelle Tab_PKI_918 aufgenommen worden: für die*
2818 *beiden Berufsgruppen gibt es unterschiedliche CHAT-Werte gemäß den Zuordnungen der*
2819 *Rechte, die gleichlautend gelten für die entsprechenden Institutionskarten SMC-B der*
2820 *Arztpraxen/Krankenhäuser (CHAT-Wert wie für Ärztin/Arzt) bzw. der Zahnarztpraxen*
2821 *(CHAT-Wert wie für Zahnärztin/Zahnarzt)*

2822

2823 **Tabelle 71: Tab_PKI_918 Abbildung von Rollenberechtigungen Zugriffsprofilen auf**
2824 **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´

2825 *Anmerkung: Zur Berechnung der Sub-CA-Flagliste einer bestimmten Karte muss das*
2826 *Zugriffsprofil der zugehörigen Rolle mit denen des Geräts kombiniert werden (siehe*
2827 *Tab_PKI_919).*

2828
2829 *Beispiel: Ein TSP-CVC ist nur für die Ausgabe von CV-Zertifikaten für Zahnärzte-HBAs*
2830 *zugelassen.*

2831 *Die Flagliste für das Profil CHAT.2ZA des Rollen-Zertifikates lautet* ´00 5D20 DAA0
2832 *8300´.*

2833 *Die Flagliste für das Profil CHAT.53 des Geräte-Zertifikates lautet* ´00 0000 0000
2834 *000C´.*

2835 *Die Kombination, bzw. Veroderung der beiden Flaglisten ergibt* ´00 5D20 DAA0 830C´.

2836 Die Flagliste einer Sub-CA beginnt mit der Bit-Folge '10' (vgl. Tab_PKI_910). Der Wert
2837 für die Flagliste des CA-Zertifikates des TSP-CVC in Tab_PKI_919 lautet '80 5D20
2838 DAA0 830C'.
2839

2840 **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	'80000000000000'
KTR-AdV	CHAT.1 & CHAT.0	'80AE1ACDC1DC04'
gSMC-K / CHAT.51	-	'800000000000001'
gSMC-KT / CHAT.54	-	'800000000000002'
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

2845

7 Festlegung von OIDs

2846 In der vorliegenden Spezifikation wird die Verwendung von OIDs in den
2847 Zertifikatsprofilen der TI-PKI über die Verwendung der OID-Referenznamen geregelt. Die
2848 Zuordnung dieser OID-Referenzen zu den konkreten OID-Werten sowie deren Verwaltung
2849 der OIDs werden im Dokument [gemSpec_OID] normativ beschrieben.

ENTWURF

2850

8 Prüfung von Zertifikaten

2851 Für die Nutzung und Statusprüfung von Zertifikaten in der TI gilt:

- 2852 • Das TSL-Signer-CA-Zertifikat (RSA oder ECDSA) bildet den Vertrauensanker für
2853 die TI.
- 2854 • Das TSL-Signer-CA-Zertifikat (RSA) und das TSL-Signer-CA-Zertifikat (ECDSA)
2855 sind jeweils über Cross-Zertifikate verknüpft.
- 2856 • Jedes Produkt kann immer nur einen der beiden Vertrauensanker aktiv haben. Ein
2857 Wechsel der Vertrauensräume ist über die Cross-Zertifikate möglich.
- 2858 • Eine TSL stellt (i. S. einer Whitelist) den Vertrauensraum für die in der TI
2859 zugelassenen Aussteller-CA dar.
- 2860 • Dabei stellt die TSL(RSA) den Vertrauensraum (RSA) und die TSL(ECC-RSA) den
2861 Vertrauensraum (ECC-RSA) dar. (Hinweis: siehe bzgl. TSL- und Vertrauensraum-
2862 Begrifflichkeiten das Kapitel 8.1.1)
- 2863 • nonQES-Aussteller-CA-Zertifikate werden ausschließlich gegen die TSL geprüft
- 2864 • QES-Aussteller-CA-Zertifikate werden
2865 hinsichtlich ihres VDA-Qualifikationsstatus gemäß [eIDAS] gegen die BNetzA-VL
2866 geprüft. (Vgl. §9 [VDG].)
- 2867 • Als Vertrauensanker für die BNetzA-VL fungieren jeweils die aktuell publizierten
2868 BNetzA-VL-Signer-Zertifikate. Diese werden mittels TSL in die QES-prüfenden
2869 Systeme (Konnektoren) eingebracht und aktualisiert.
- 2870 • End-Entity-Zertifikate werden gegen den OCSP-Dienst der Aussteller-CA geprüft,
2871 außer die Statusprüfung für einen bestimmten Zertifikatstyp ist explizit optional
2872 oder nicht vorgesehen.

2873

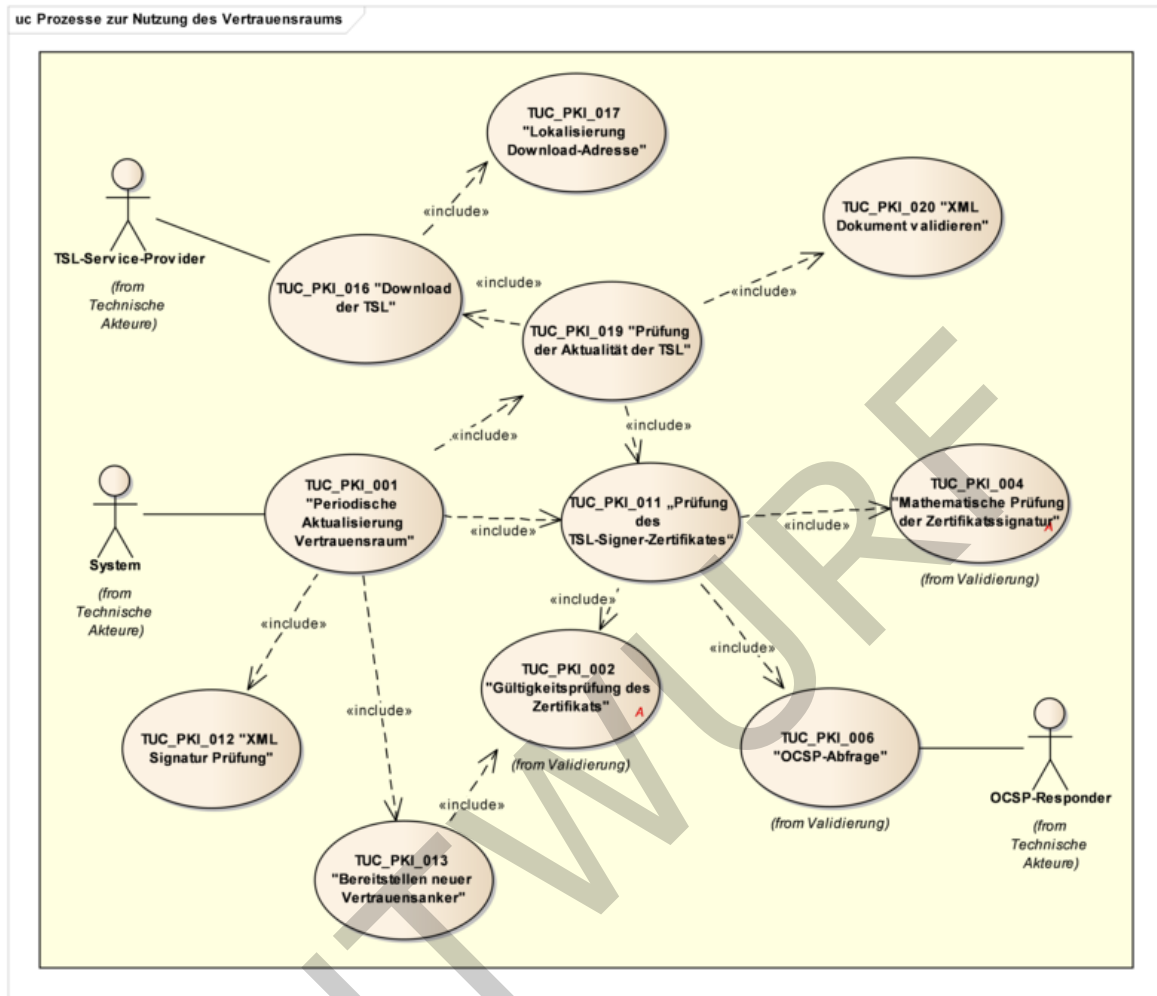


Abbildung 5: Use Case Diagram „Prozesse zur Nutzung des TI-Vertrauensraums“

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

2893 verletztten Vorbedingung, in keinem Fall das Ergebnis eines TUC als positiv
2894 bewertet wird, z. B. eine Prüfung als erfolgreich eingestuft wird.
2895 In welcher Form die Umsetzung von Vorbedingungen erfolgt (z. B. durch explizite
2896 Prüfung, Teilausführung des TUC oder durch Wechsel eines Systemzustands) ist
2897 nicht Gegenstand der TUC-Spezifikation. Ein TUC muss nicht stets
2898 Vorbedingungen haben.

- 2899 • Wird im Ablauf des TUC ein anderer TUC aufgerufen und dieser endet mit einer
2900 Fehlermeldung, so wird auch der aufrufende TUC mit dieser Fehlermeldung
2901 beendet, sofern nichts anderes festgelegt ist. Daher setzen sich die möglichen
2902 Fehlermeldungen eines TUC aus den Fehlerfällen im TUC-Ablauf und allen
2903 Fehlermeldungen der aufgerufenen TUCs zusammen.

2904 Für die Nutzung und die Statusprüfung von nonQES-Zertifikaten im Internet gilt:

2905 Die Zertifikatsprüfung erfolgt gemäß [RFC5280] und gemäß [COMMON-PKI].

- 2906 • Der TI-Vertrauensraum wird im Internet durch die Bereitstellung von OCSP-
2907 Statusauskünften zu allen in der TSL enthaltenen CAs abgebildet.
- 2908 • Mangels einer der TSL entsprechenden Whitelist für zugelassene CAs im Internet
2909 müssen sämtliche nonQES CA- und EE-X.509-Zertifikate der TI im Feld
2910 **authorityInfoAccess** die URL des zugehörigen und im Internet erreichbaren
2911 OCSP-Responders enthalten.
- 2912 • Im Internet erfolgt die Prüfung der nonQES CA- und EE-Zertifikaten (HBA, SMC-B)
2913 entlang des Zertifizierungspfades bis hin zur gematik Root-CA.
- 2914 • Die nonQES-X.509-Zertifikate der temporär zu unterstützenden HBA-
2915 Vorläuferkarten werden auf Basis der dafür etablierten Statusauskunftsdienste
2916 geprüft.

2917 **GS-A_5043 - Auflösung von OCSP-Adressen im Internet**

2918 TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN für Zertifikatstypen, die zusätzlich zur
2919 TI auch im Internet statusgeprüft werden, sicherstellen, dass die im Zertifikat
2920 eingetragene OCSP-Responderadresse im Internet aufgelöst und eine Statusabfrage
2921 erfolgreich durchgeführt werden kann.

2922 [**<=**]

2923 Der TI-Vertrauensraum für QES-Zertifikate wird im Internet nicht gesondert abgebildet.
2924 Die Zertifikate werden gemäß der für QES üblichen Verfahren validiert und statusgeprüft.

2925 Über die Bereitstellung von nonQES-CA- und EE-Zertifikatsinformationen im Internet
2926 hinaus werden durch die Spezifikationen der TI keine Aussagen getroffen über Art und
2927 Umfang von durchzuführenden Schritten im Kontext der Zertifikatsprüfung durch die
2928 Anwendungen im Internet.

2929 **8.1 Vertrauensraum der TI**

2930 Grundlage jeder zertifikatsbasierten Prüfung auf Vertrauenswürdigkeit in der TI ist die
2931 gesicherte Information über den aktuell gültigen TI-Vertrauensraum, gegen den eine
2932 solche Prüfung erfolgt.

2933 Der Vertrauensraum der TI besteht also aus der Menge der CAs (bzw. deren Zertifikate),
2934 die in der TI zugelassen, also als vertrauenswürdig anerkannt sind. Außerdem enthält er
2935 die Einsatzzwecke, für welche die CAs End-Entity-Zertifikate ausgeben dürfen. Dieser TI-
2936 Vertrauensraum wird in der TSL abgebildet.

2937 Die TSL enthält Informationen gemäß [ETSI_TS_102_231#5]. Sie beinhalten neben den
2938 CA-Zertifikaten im TI-Vertrauensraum zusätzliche Angaben, wie z. B. die
2939 Sequenznummer oder die Adressen und Zertifikate der zuständigen OCSP-Responder.
2940 Die TSL spielt also in zertifikatsprüfenden Komponenten die zentrale Rolle.
2941 Konkret bereitgestellt wird die TSL als TSL-Datei in Form einer signierten XML-Datei
2942 gemäß [ETSI_TS_102_231#B].
2943

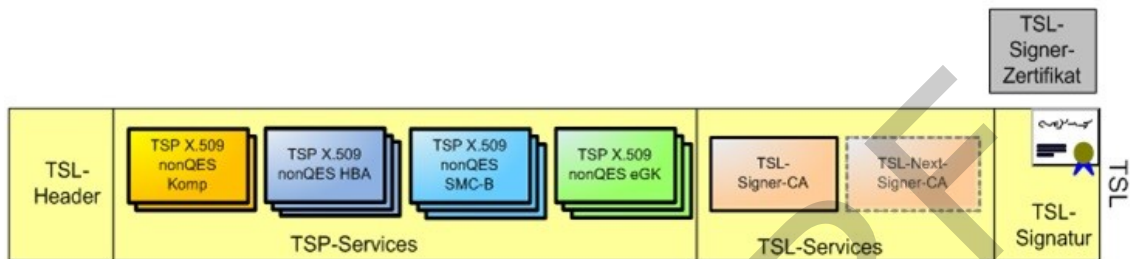


Abbildung 6 : Aufbau der TSL

2944
2945
2946
2947 *Hinweis: Die TSL-Informationen müssen also nicht zwingend in Form der XML-Syntax der*
2948 *TSL-Datei vorgehalten werden. Sie können auch ganz oder teilweise in einen sicheren*
2949 *Speicher des Systems (Truststore) importiert werden.*

2950 Die nachfolgende Gliederung der Teilschritte einer Prüfung orientiert sich an den
2951 Vorgaben des TSL-Standards [ETSI_TS_102_231#H] – mit den Konkretisierungen für die
2952 TI sowie ergänzt um TI-spezifische Erweiterungen der TI-Vertrauensraumprüfung.

2953 Die notwendigen Prüfschritte zur Prüfung des TI-Vertrauensraums werden in Form von
2954 Technischen Use Cases dargestellt:

- 2955 • Initialisierung / Aktualisierung des TI-Vertrauensraumes
- 2956 • Lokalisieren der TSL-Datei
- 2957 • Download der TSL-Datei (ggf. nach vorheriger Aktualitätsprüfung mittels
- 2958 Hashwert-Vergleichsverfahren)
- 2959 • Validierung der TSL-Datei
- 2960 • Prüfung der Integrität und Authentizität der TSL-Datei durch die Prüfung ihrer
- 2961 Signatur

2962 Die bereits im Internet etablierten PKIs der Vorläuferkarten (qSIG, ZOD), die im Rahmen
2963 des Bestandsschutzes zu unterstützen sind, werden in der TI insoweit berücksichtigt,
2964 dass die zugehörigen CAs in den TI-Vertrauensraum (also die TSL) aufgenommen und die
2965 Statusinformationen der zugehörigen EE-Zertifikate durch Nachnutzung des OCSP-
2966 Responder Proxy zur Verfügung gestellt werden (s. Beschreibung in
2967 [gemKPT_Arch_TIP#5.4.13]).

2968 8.1.1 TSL im Kontext der ECC-Migration

2969 Der Vertrauensraum der TI sah bisher nur die Verwendung von RSA-2048 als
2970 Schlüsselalgorithmus vor. Die TSL enthielt daher nur RSA-Zertifikate (im Kontext X.509).

2971 Im Zuge der ECC-Migration müssen alle Produkttypen so umgestellt werden, dass sie
2972 neben RSA-2048 auch ECC-256 unterstützen (vgl. [gemSpec_Krypt#5]). Daher wird
2973 neben der bisher vorhandenen reinen RSA-basierten TSL (im Folgenden „TSL(RSA)“
2974 genannt) eine zweite TSL bereitgestellt, die sowohl die neuen ECDSA-basierten
2975 Zertifikate als auch aus Rückwärtskompatibilitäts-Gründen die weiterhin benötigten RSA-
2976 basierten Zertifikate enthält. Diese zweite neue TSL wird im Folgenden als „**TSL(ECC-
2977 RSA)**“ bezeichnet.

2978 Bis zum vollständigen Abschluss der ECC-Migration werden beide TSL-Varianten vom
2979 TSL-Dienst bereitgestellt. Technisch sind die beiden Varianten unabhängig voneinander.
2980 Der Übergang des Vertrauensraumes von Vertrauensraum (RSA) auf Vertrauensraum
2981 (ECC-RSA) geschieht dabei durch Cross-Zertifizierung der entsprechenden TSL-Signer-
2982 CA-Zertifikate.

2983 Neben dem Download-Punkt für die TSL(RSA) gibt es einen weiteren Download-Punkt für
2984 die TSL(ECC-RSA). Die TSL(RSA) wird weiterhin mit einem RSA-basierten Zertifikat
2985 signiert. Die TSL(ECC-RSA) erhält eine Signatur auf ECDSA-Basis.

2986 Produkttypen, die ausschließlich RSA-Zertifikate verwenden und/oder prüfen, verwenden
2987 die TSL(RSA). Alle Produkttypen, die ECC-Zertifikate nutzen oder validieren, müssen die
2988 TSL(ECC-RSA) verwenden.

2989 Die gematik empfiehlt Anbietern sogenannter Weiterer elektronischer Anwendungen
2990 (aAdG und aAdG-NetG-TI) die Berücksichtigung der für die ECC-Migration aufgeführten
2991 Hinweise und Anforderungen. Letztere sind gekennzeichnet durch die Ergänzung „(ECC-
2992 Migration)“ im Titel der relevanten Anforderungen.

2993 **8.1.2 Initialisierung TI-Vertrauensraum**

2994 Verfügt eine zugelassene Komponente der TI noch nicht über einen aktuell gültigen TI-
2995 Vertrauensanker, muss für dieses Komponentenexemplar eine Initialisierung des TI-
2996 Vertrauensraumes ohne Vorbedingungen durchgeführt werden. Diese besteht aus den
2997 zwei Teilprozessen:

- 2998 • Die sichere Einbringung des TI-Vertrauensankers in Form des aktuell gültigen
2999 TSL-Signer-CA-Zertifikates in die Komponente in einer gesicherten Umgebung des
3000 Herstellers oder Betreibers
- 3001 • Einbringung einer aktuellen TSL in die Komponente durch den Hersteller oder den
3002 Vor-Ort-Administrator

3003 Dies gilt für die Anwendungsfälle

- 3004 • der Erstinbetriebnahme einer Komponente und
- 3005 • der Wiederinbetriebnahme bzw. Systemwiederherstellung zu einem Zeitpunkt, zu
3006 dem die in der Komponente vorhandene TSL nicht mehr gültig und
3007 zwischenzeitlich ein Wechsel des TI-Vertrauensankers erfolgte.

3008 Die folgenden Anforderungen gelten unter den oben genannten Rahmenbedingungen
3009 sowohl für die Initialisierung eines RSA- als auch eines im Rahmen der ECC-Migration
3010 notwendigen ECC-Vertrauensankers.

3011 **GS-A_4640 - Identifizierung/Validierung des TI-Vertrauensankers bei der** 3012 **initialen Einbringung**

3013 Hersteller von Produkttypen der TI, die Zertifikate prüfen, **MÜSSEN** bei der initialen
3014 Einbringung das aktuell gültige TSL-Signer-CA-Zertifikat eindeutig identifizieren und
3015 mittels Fingerprint validieren, bevor dieses Zertifikat als TI-Vertrauensanker in die

3016 Komponente eingebracht werden darf.
3017 [\leq]

3018 **GS-A_4641 - Initiale Einbringung TI-Vertrauensanker**

3019 Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN die initiale Einbringung des
3020 aktuell gültigen TSL-Signer-CA-Zertifikat als TI-Vertrauensanker in die Komponente
3021 nachweislich sicher vor Manipulation vornehmen.
3022 [\leq]

3023 **WA-A_2111 - Initiale Einbringung TI-Vertrauensanker in andere Anwendungen**

3024 Der Anbieter einer aAdG oder aAdG-NetG-TI MUSS sicherstellen, dass die initiale
3025 Einbringung des aktuell gültigen TSL-Signer-CA-Zertifikats als TI-Vertrauensanker in
3026 Dienste der aAdG oder der aAdG-NetG-TI nachweislich sicher vor Manipulation
3027 vorgenommen wird. [\leq]

3028 **GS-A_4748 - Initiale Einbringung TSL-Datei**

3029 Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN die initiale Einbringung der TSL-
3030 Datei in die Komponente nachweislich sicher vor Manipulation vornehmen.
3031 [\leq]

3032 **WA-A_2112 - Initiale Einbringung TSL-Datei**

3033 Der Anbieter einer aAdG oder aAdG-NetG-TI MUSS sicherstellen, dass die initiale
3034 Einbringung der TSL-Datei in Dienste der aAdG oder der aAdG-NetG-TI nachweislich
3035 sicher vor Manipulation vorgenommen wird. [\leq]

3036 Im Abschnitt 8.1.1 werden relevante Punkte zur ECC-Migration erläutert. Daher gilt für
3037 Produkttypen, die auf ECC migriert bzw. im Vertrauensraum (ECC-RSA) betrieben
3038 werden:

3039 **A_17688 - Nutzung des ECC-RSA-Vertrauensraumes (ECC-Migration)**

3040 Die Produkttypen der TI, die ECC-Zertifikate validieren müssen, MÜSSEN das TSL-Signer-
3041 CA-Zertifikat (ECDSA) als TI-Vertrauensanker und die TSL(ECC-RSA) verwenden.
3042
3043 [\leq]

3044 **Nutzung von Cross-Zertifikaten für die Etablierung des ECC-Vertrauensankers:**

3045 Neben den oben in 8.1.2 beschriebenen Festlegungen zum initialen Einbringen eines
3046 neuen Vertrauensankers (auch für ECC-RSA) gibt es eine weitere Möglichkeit zur
3047 Etablierung. Für die von der ECC-Migration betroffenen Produkttypen, die auf Basis eines
3048 bereits etablierten Vertrauensankers (RSA) den neuen Vertrauensanker (ECC-RSA)
3049 (entspricht TSL-Signer-CA-Zertifikat (ECDSA)) etablieren (z.B. Konnektoren), gilt
3050 folgendes:
3051

3052 **A_17689 - Nutzung von Cross-Zertifikaten für Vertrauensraum-Wechsel nach
3053 ECC-RSA (ECC-Migration)**

3054 Die Produkttypen der TI, die einen Vertrauensanker (ECC-RSA) zur Etablierung des
3055 Vertrauensraumes (ECC-RSA) initialisieren, KÖNNEN Cross-Zertifikate verwenden, um
3056 auf Basis ihres bereits etablierten Vertrauensankers (RSA) in den Vertrauensraum (ECC-
3057 RSA) zu wechseln.
3058

3059 [\leq]

3060 **A_17820 - Nutzung von Cross-Zertifikaten für Vertrauensraum-Wechsel nach
3061 RSA (ECC-Migration)**

3062 Die Produkttypen der TI, die einen Vertrauensanker (RSA) zur Etablierung des
3063 Vertrauensraumes (RSA) initialisieren, KÖNNEN Cross-Zertifikate verwenden, um auf
3064 Basis ihres bereits etablierten Vertrauensankers (ECC-RSA) in den Vertrauensraum (RSA)

3065 zu wechseln.
3066 [\leq]

3067 Hinweis: Die Nutzung von Cross-Zertifikaten für den Wechsel des Vertrauensraums ist für
3068 den Konnektor besonders geregelt (s. gemSpec_Kon#A_17837 und A_17784).

3069 **A_17821 - Wechsel des Vertrauensraumes mittels Cross-Zertifikaten (ECC-**
3070 **Migration)**

3071 Die Produkttypen der TI, die den Vertrauensraum mittels Cross-Zertifikates wechseln
3072 (siehe A_17689 und A_17820) MÜSSEN die folgenden Schritte erfolgreich durchlaufen,
3073 um auf den Vertrauensanker des neuen Vertrauensraumes zu wechseln.

3074 Vorbedingung: Das System besitzt zum aktuell etablierten Vertrauensraum den aktuell
3075 aktiven Vertrauensanker (der zu dem benutzten Cross-Zertifikat passend ist).

- 3076 1. Falls eine TSL (aus dem aktuellen Vertrauensraum) bereits im System vorhanden
3077 ist, MUSS das Element TSLSequenceNumber aus dieser TSL ausgelesen und der
3078 Wert im persistenten (sicheren) Speicher des Systems abgelegt werden. Für jeden
3079 TSLSequenceNumber-Nummernkreis (s.u.) wird ein separater Wert geführt.
- 3080 2. Es MUSS das neue Vertrauensanker-Zertifikat (TSL-Signer-CA<X>) in das System
3081 eingelesen werden (auch ggf. als Download realisierbar).
- 3082 3. Es MUSS das Cross-Zertifikates (C.GEM-TSL-CA<X>-CROSS<Y>) in das System
3083 eingelesen werden (auch ggf. als Download realisierbar).
- 3084 4. Es MUSS ein Vergleich des PublicKey im Cross-Zertifikat mit dem PublicKey im
3085 CA-Zertifikat des neuen Vertrauensankers (TSL-Signer-CA<X>) durchgeführt
3086 werden.
- 3087 5. Es MUSS eine Signatur-Prüfung des Cross-Zertifikates gegen den alten
3088 Vertrauensanker im System (TSL-Signer-CA<Y>) durchgeführt werden analog zu
3089 TUC_PKI_004.
- 3090 6. Es MUSS eine neue TSL (passend zum Vertrauensanker TSL-Signer-CA<X>)
3091 analog zu GS-A_4748 eingebracht und danach das Element TSLSequenceNumber
3092 ausgelesen werden. Falls für den TSLSequenceNumber-Nummernkreis der neu
3093 eingebrachten TSL eine TSLSequenceNumber im sicheren Speicher vorliegt, dann
3094 muss die TSLSequenceNumber der neu eingebrachten TSL höher sein, als dieser
3095 Wert.

3096 Wenn einer der Schritte fehlschlägt, MUSS der Vertrauensraum-Wechsel-Prozess
3097 abgebrochen werden und der alte Vertrauensanker (TSL-Signer-CA<Y>) im System
3098 verbleiben.

3099 Nach erfolgreichem Durchlaufen aller Schritte, MUSS der Vertrauensanker (TSL-Signer-
3100 CA<X>) im System etabliert sein.

3101 Erklärungen zu den verwendeten Begriffen:

- 3102 • Vertrauensanker im System vor dem Vertrauensraum-Wechsel: TSL-Signer-
3103 CA<Y>
- 3104 • Vertrauensanker des neuen Vertrauensraumes: TSL-Signer-CA<X>
- 3105 • Verwendetes Cross-Zertifikat: C.GEM-TSL-CA<X>-CROSS<Y>
- 3106 • TSLSequenceNumber – Nummernkreis RSA: 0..9999
- 3107 • TSLSequenceNumber – Nummernkreis ECC-RSA: ab 10000

3108
3109
3110 [\leq]

3111 Für die Zertifikatsprüfung bei der initialen Einbringung und Validierung der TSL gelten die
3112 Bestimmungen für Offline-Anwendungsszenarien aus Kap. 8.3.2.4, d. h. eine
3113 Statusprüfung des TSL-Signatur-Zertifikates erfolgt nicht.

3114 Die in der TI zugelassenen Zertifikate der vertrauenswürdigen Herausgeber (TSPs) sind
3115 in der TSL enthalten. Bei der Initialisierung des TI-Vertrauensraumes wird der Truststore
3116 befüllt, d.h. die Zertifikate können aus der TSL-Datei ausgelesen und z. B. in den
3117 Truststore des Systems importiert werden. Der Status der bezeichneten
3118 Vertrauensdienste wird jeweils im Inhalt des TSL-Elementes „ServiceStatus“ mit einem
3119 URI identifiziert. Die untenstehende Tabelle zeigt die erlaubten Status und erklärt deren
3120 Bedeutung in der TI Für X.509-CA-Zertifikate gibt die Kombination des Inhaltes von
3121 „ServiceStatus“ mit dem Zeitpunkt in „StatusStartingTime“ an,

- 3122 • seit wann ein Zertifikat dem aktuellen TI-X.509-Vertrauensraum angehört (mit
3123 „/inaccord“ markiert), oder
- 3124 • bis wann unter dem CA-Zertifikat EE-Zertifikate ausgestellt werden durften.
- 3125 • „/revoked“: Dies entspricht einer Sperrung gemäß dem Kettenmodell für QES
3126 (s. [gemKPT_PKI_TIP#2.4.3]) oder dem Kompromissmodell für nonQES-
3127 Zertifikate für HBA und SMC-B (s. [gemKPT_PKI_TIP#2.4.2]). Diese erfolgt bei
3128 einer Einstellung des Betriebs aufgrund eines nicht-sicherheitskritischen
3129 Incidents, gegebenenfalls auch nach einem sicherheitskritischen Incident. Vgl.
3130 dazu auch [gemKPT_PKI_TIP#2.3.3.5] „Sperrung von CA-Zertifikaten in der
3131 TSL“ und [gemKPT_PKI_TIP#2.4]. „Gültigkeitsmodelle X.509-Zertifikate“.
3132 Im TUC_PKI_018 "Zertifikatsprüfung in der TI", Schritt 5 wird geprüft, ob
3133 unerlaubt Zertifikate ausgegeben wurden, deren Ausstellungsdatum nach dem
3134 Widerrufsdatum des CA-Zertifikats liegt.
- 3135 • „/expired“: Das CA-Zertifikat ist abgelaufen, es wird aber für die Validierung
3136 von Zertifikaten weiterhin benötigt. Der ServiceStatus wird zur Prüfung von
3137 nonQES-Signaturen nach Kompromissmodell benötigt .

3138 *Hinweis: Gemäß Schalenmodell gesperrte CA-Zertifikate werden aus der TSL entfernt, es*
3139 *wird deshalb kein URI zur Markierung dieser Zertifikate verwendet.*

3140 OCSP-Signer-, CRL-Signer- und CVC-CA-Zertifikate sowie der DNSSEC-Trust-Anchor sind
3141 nur in der aktuellen TSL-Datei enthalten, wenn sie auch gegenwärtig im Einsatz sind. Für
3142 diese Dienstarten ist deshalb „/inaccord“ der einzige erlaubte Status.

3143

3144 **Tabelle 74: Tab_PKI_271 Erlaubte URIs als Inhalte des TSL-Elements ServiceStatus**

URI	Dienstart	Bedeutung
http://uri.etsi.org/TrstSvc/Svcstatus/inaccord	X.509-CA OCSP-Signer CRL-Signer CVC-Root-CA DNSSEC-Trust-Anchor BNetzA-VL-Signer	Der Dienst ist für die TI zugelassen und ist in Betrieb.

	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.

3145

3146 *Hinweis: Der TSL-Dienst darf nur die in Tab_PKI_271 angegebenen URIs für*
3147 *ServiceStatus verwenden.*

3148 **8.1.2.1 TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“**

3149 **GS-A_4642 - TUC_PKI_001: Periodische Aktualisierung TI-Vertrauensraum**

3150 Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_001 zur periodischen
3151 Aktualisierung des TI-Vertrauensraums umsetzen.

3152 [\leq]

3153

3154 **Tabelle 75: TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“**

Element	Beschreibung
Name	TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“

Beschreibung	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 Ein Offline-Modus ist zu berücksichtigen für a) das Mobile-Kartenterminal b) Konnektor ohne Anbindung an die TI Beide verfügen nicht über die automatischen Online-Möglichkeiten zum Bezug von Statusinformationen oder TSL-Aktualisierungen aus der TI.
Anwendungsumfeld	System, das die TSL auswertet
Vorbedingungen	Gültige TSL im System (optional mit Hashwert)
Auslöser	Produkttypspezifischer Trigger Zeitpunkt MUSS durch Facharchitekturen vorgegeben werden. (Standardmäßig ist eine tägliche Prüfung der Aktualität vorzusehen.)
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. [System:] Das verwendete TSL-Signer-Zertifikat wird aus der TSL-Datei extrahiert.4. [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.)5. [System:] Es wird ermittelt, ob in der neuen TSL ein neuer TI-Vertrauensanker vorliegt (TUC_PKI_013 „Import TI-Vertrauensanker aus TSL“).6. [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.
7.
[System:] Der Truststore wird für Zertifikatsprüfung (wieder) bereitgestellt.
8.
[System:] Ende des Use Case

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.

3155

3156

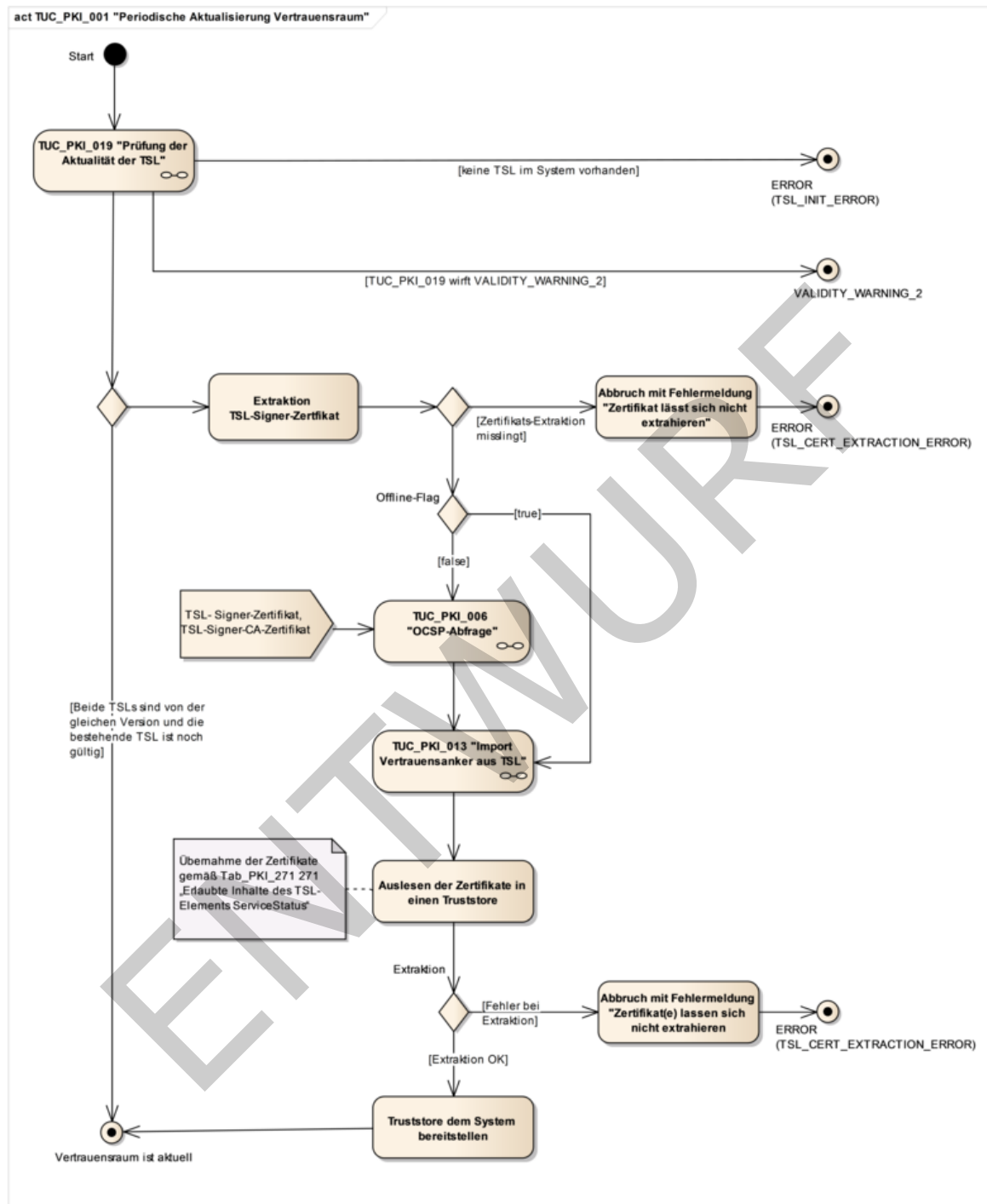


Abbildung 7: Aktivitätsdiagramm TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“

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“

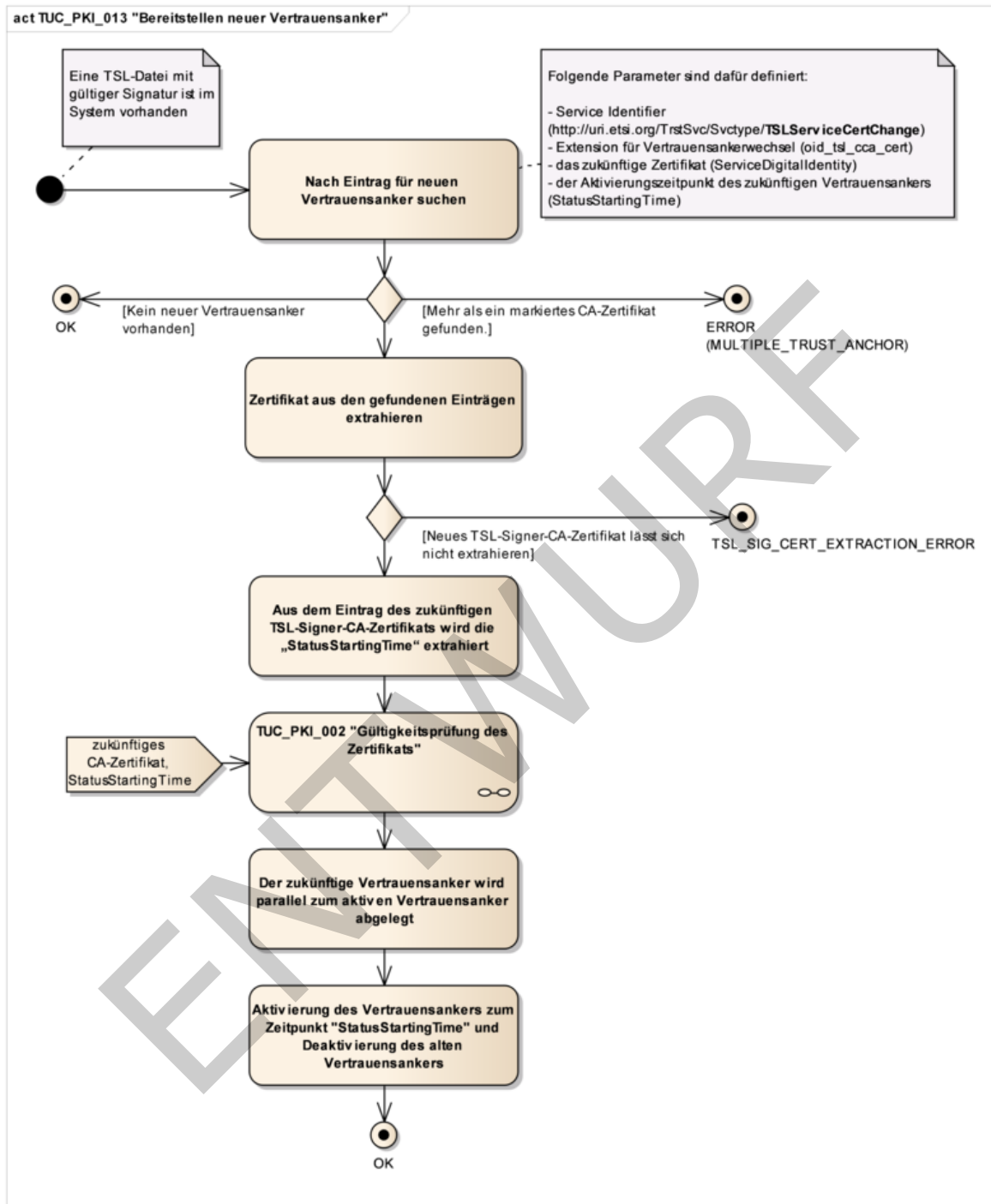
Element	Beschreibung
Name	TUC_PKI_013 „Import neuer TI-Vertrauensanker“
Beschreibung	Als TI-Vertrauensanker gilt das aktuell gültige TSL-Signer-CA-Zertifikat. Das neue TSL-Signer-CA-Zertifikat wird rechtzeitig vor dem geplanten Aktivierungsdatum in die TSL integriert und als zukünftiger TI-Vertrauensanker 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	<p>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.</p> <p>1b. [System:] Es wird mehr als ein markiertes CA-Zertifikat gefunden. (MULTIPLE_TRUST_ANCHOR)</p> <p>2b. [System:] Das TSL-Signer-CA-Zertifikat lässt sich nicht aus der TSL extrahieren. (TSL_SIG_CERT_EXTRACTION_ERROR)</p>
Sicherheitsanforderungen	<p>Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.</p>
Anmerkungen	<p>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.</p>
Zugehörige Diagramme	<p>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.</p>

3175



3176

3177

Abbildung 8: Aktivitätsdiagramm TUC_PKI_013 „Import neuer TI-Vertrauensanker“

3178

8.1.3.2 TSL-Einträge für die Bereitstellung neuer TI-Vertrauensanker

3179

Für den Wechsel auf ein neues TSL-Signer-CA-Zertifikat wird dieses in der TSL

3180

aufgenommen unter Berücksichtigung folgender Rahmenbedingungen:

3181

Die Aufnahme des Zertifikates erfolgt rechtzeitig, also erstmals zu einem Datum, welches

3182

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:

- Innerhalb Element ServiceTypeIdentifier:
URI <http://uri.etsi.org/TrstSvc/Svctype/TSLServiceCertChange>
 - das Zertifikat des neuen TI-Vertrauensankers in ServiceDigitalIdentity
 - Einen durch die gematik vorgegebenen Aktivierungszeitpunkt im Element StatusStartingTime
 - Adresse des OCSP-Responders zur Prüfung von ausgestellten Zertifikaten (TSL-Signer) in ServiceSupplyPoint(s)
 - 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.

3232 **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

3233 In der folgenden Tabelle wird ein (nicht-normatives) Beispiel zu den TSL-Einträgen
3234 dargestellt, die den Wechsel des TI-Vertrauensraumes bewirken.

3235

3236 **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>

```

3237 *Hinweis: Die Authentizität der TSL-Datei ist durch deren Signatur gegeben, die*
3238 *Authentizität des TSL-Download-Punktes wird durch DNSSEC gesichert. Der Download*
3239 *erfolgt deshalb über einfaches HTTP, nicht über HTTPS.*

3240 **8.1.3.3 Prüfung der TSL nach Wechsel des TI-Vertrauensanker**

3241 Ein neuer TI-Vertrauensanker wird mit einem TSL-Eintrag (s. o.) angekündigt.

3242 Sobald der Zeitpunkt für die Aktivierung des neuen TI-Vertrauensankers erreicht ist, wird
3243 der neue TI-Vertrauensanker aktiviert. Zur Ermittlung des Zeitpunktes soll die in der TI
3244 verbindlich geltende Zeitquelle verwendet werden.

3245

3246 **GS-A_4645 - TSL-Signatur ab Aktivierungsdatum neuer TI-Vertrauensanker**

3247 Der TSL-Dienst MUSS ab dem Aktivierungsdatum eines über die TSL publizierten TI-
3248 Vertrauensankers (TSL-Signer-CA-Zertifikat) die TSL mit einem TSL-Signer-Zertifikat

3249 signieren, das von dieser TSL-Signer-CA ausgestellt wurde.
3250 [\leq]

3251 **8.1.4 Ungeplanter Wechsel des TI-Vertrauensanker**

3252 Ein ungeplanter Wechsel des TI-Vertrauensankers kann dann erforderlich werden, wenn
3253 die TSL-Signer-CA korrumpiert wurde. (Nur in Verbindung mit dem missbräuchlichen
3254 Zugang zu den TSL-Download-Punkten kann hieraus ein konkreter Schaden durch
3255 gefälschte TSL-Einträge, die von den auswertenden Komponenten und Systemen nicht
3256 mehr als solche erkennbar sind, für die TI resultieren.)

3257 **8.2 TSL-Prüfung**

3258 **8.2.1 Erreichbarkeit und Download der TSL**

3259 Der TSL-Dienst stellt die jeweils aktuelle TSL an definierten Download-Punkten in der TI
3260 und im Internet bereit. Diese Download-Punkte sind so gewählt, dass sie von allen
3261 Diensten, Systemen und Komponenten in der TI netzwerktechnisch erreicht werden
3262 können.

3263 Die Adressen der TSL-Download-Punkte sind in Form von URI definiert und Bestandteil
3264 jeder TSL.

3265 Die TSL verweist auf die Download-Punkte, wo die jeweils aktuellste Version der TSL
3266 heruntergeladen werden kann (siehe Kap. 8.2.1.1).

3267 Die Lokalisierung der Adresse ist in Abschnitt 8.2.1.1 detailliert beschrieben.

3268 **8.2.1.1 TUC_PKI_017 „Lokalisierung TSL Download-Adressen“**

3269 **GS-A_4646 - TUC_PKI_017: Lokalisierung TSL Download-Adressen**

3270 Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_017 zur Lokalisierung
3271 der Download-Adressen der TSL umsetzen.

3272 [\leq]

3273

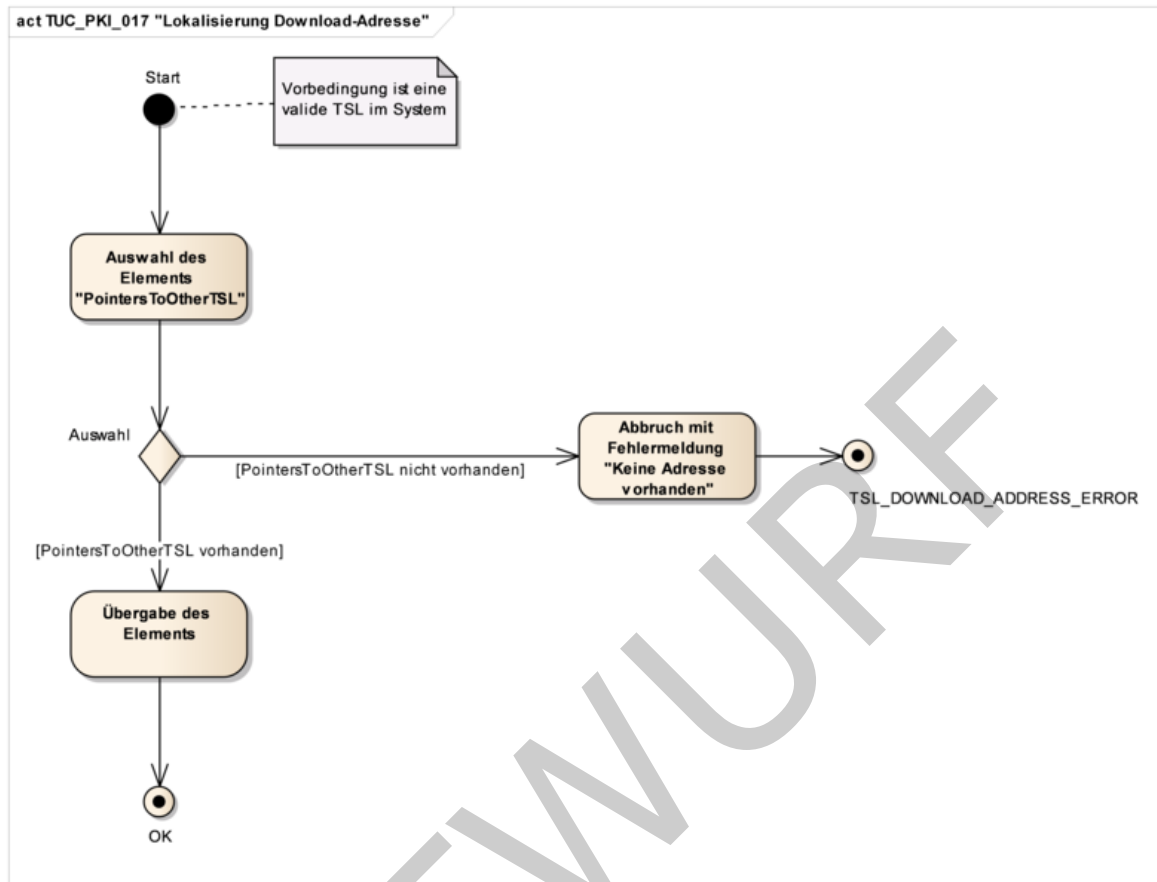
3274 **Tabelle 79: TUC_PKI_017 „Lokalisierung Download-Adressen“**

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.

3275

3276



3277

3278 **Abbildung 9: Aktivitätsdiagramm TUC_PKI_017 „Lokalisierung Download-Adresse“**

3279

3280 **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

3281 Die normative Festlegung der OIDs ist in [gemSpec_OID#3.6] festgelegt.

3282 Die TSL-Dateien und deren Hash-Werte werden vom Anbieter des TSL-Dienstes in der TI
3283 und im Internet zum Download bereitgestellt. Die festgelegten Downloadpunkte sind in
3284 [gemSpec_TSL#A_17680] zu finden.

3285

3286 **8.2.1.2 TUC_PKI_016 „Download der TSL-Datei“**

3287 **GS-A_4647 - TUC_PKI_016: Download der TSL-Datei**

3288 Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_016 zum Download
3289 der TSL-Datei umsetzen.

3290 **[<=]**

3291

3292 **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.

3293
3294

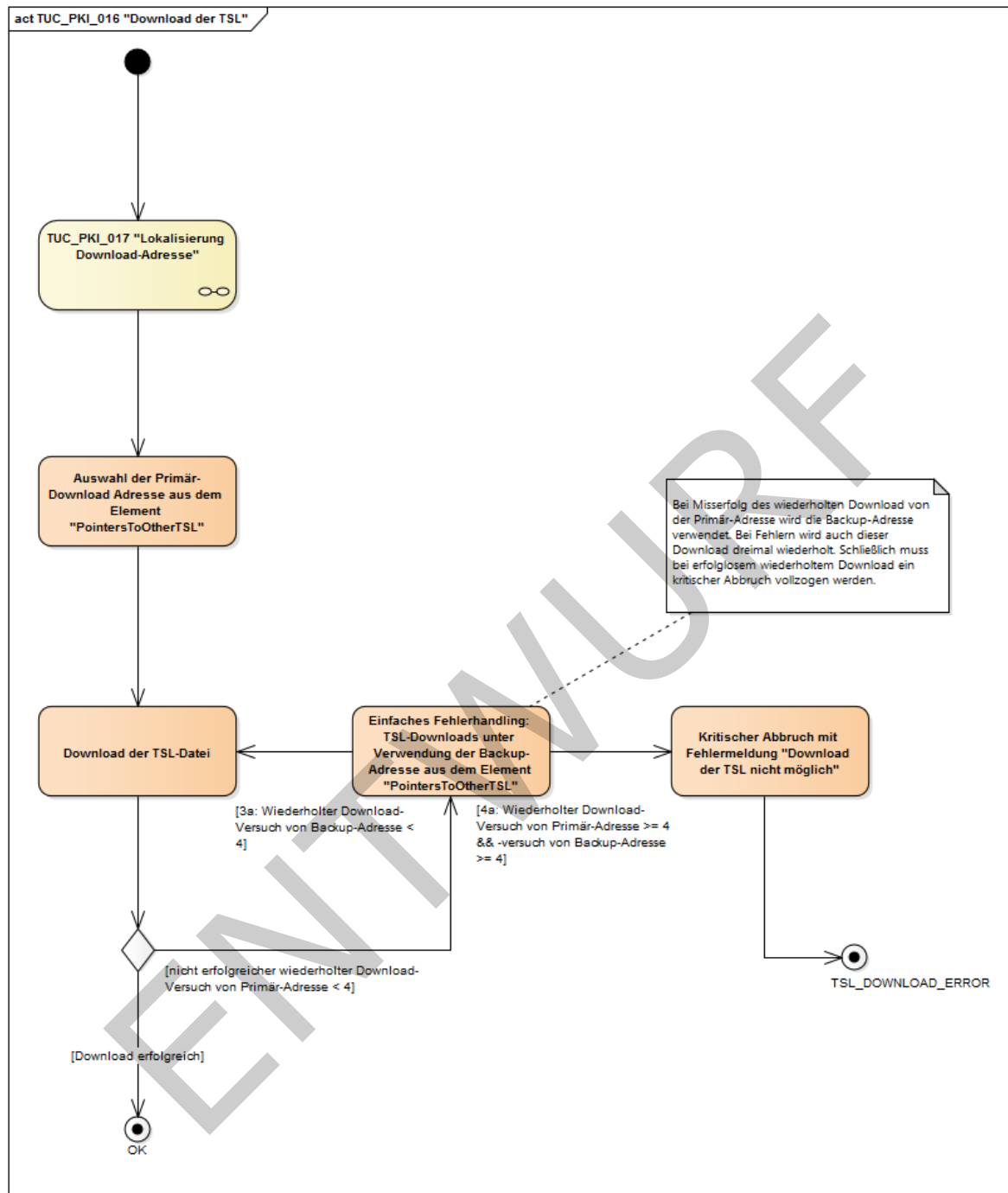


Abbildung 10: Aktivitätsdiagramm TUC_PKI_016 „Download der TSL-Datei“

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.

[<=]

3349 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

3350

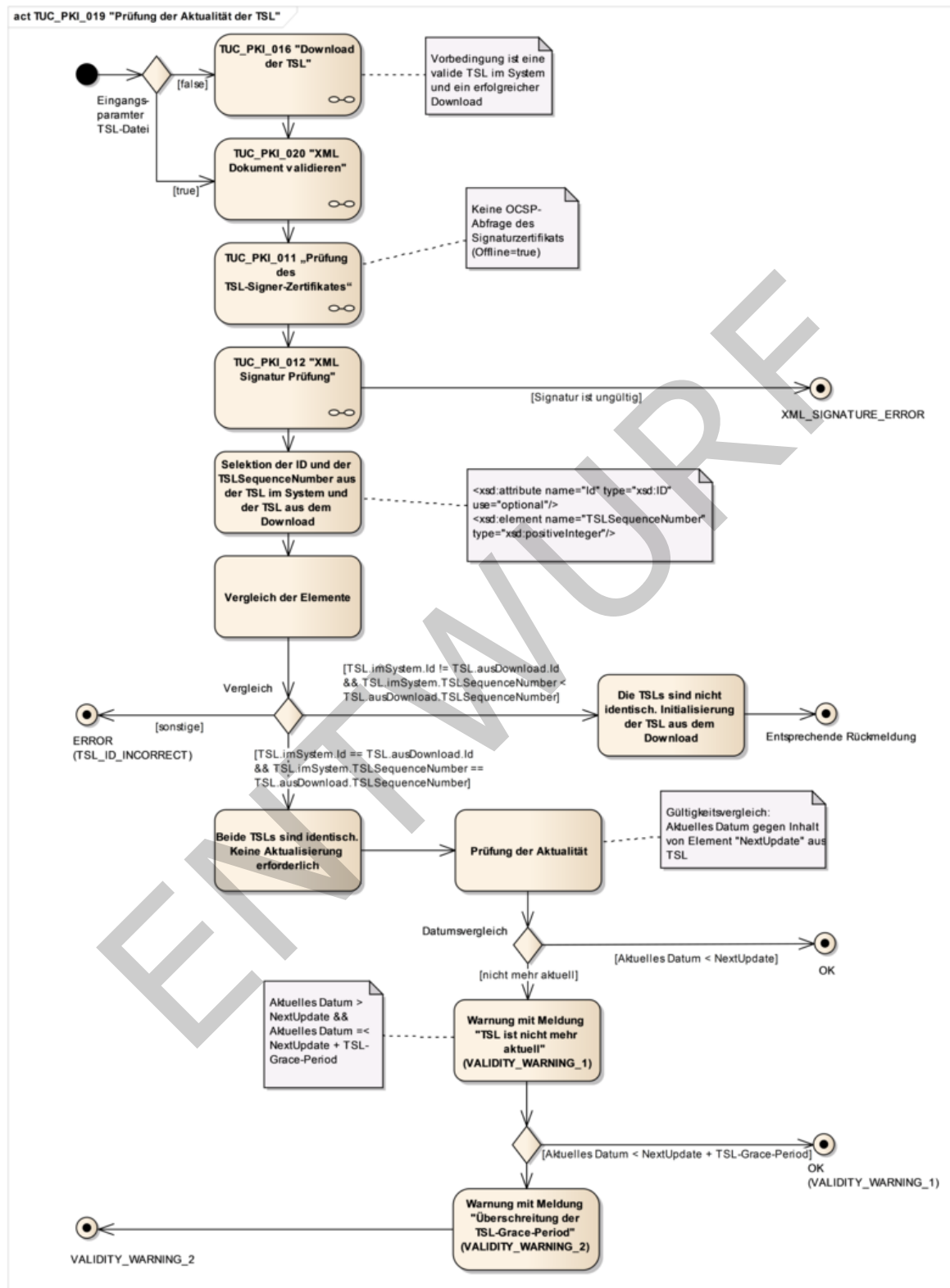


Abbildung 11: Aktivitätsdiagramm TUC_PKI_019 „Prüfung der Aktualität der TSL“

3353 **8.2.2.2 TUC_PKI_020 „XML-Dokument validieren“**

3354 **GS-A_4649 - TUC_PKI_020: XML-Dokument validieren**

3355 Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_020 zur Validierung
3356 eines XML-Dokumentes umsetzen.

3357 [\leq]

3358

3359 **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)

3360 8.2.2.3 TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“

3361 GS-A_4650 - TUC_PKI_011: Prüfung des TSL-Signer-Zertifikates

3362 Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_011 zur Prüfung des
3363 TSL-Signer-Zertifikats umsetzen.

3364 [\leq]

3365

3366 **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“.)

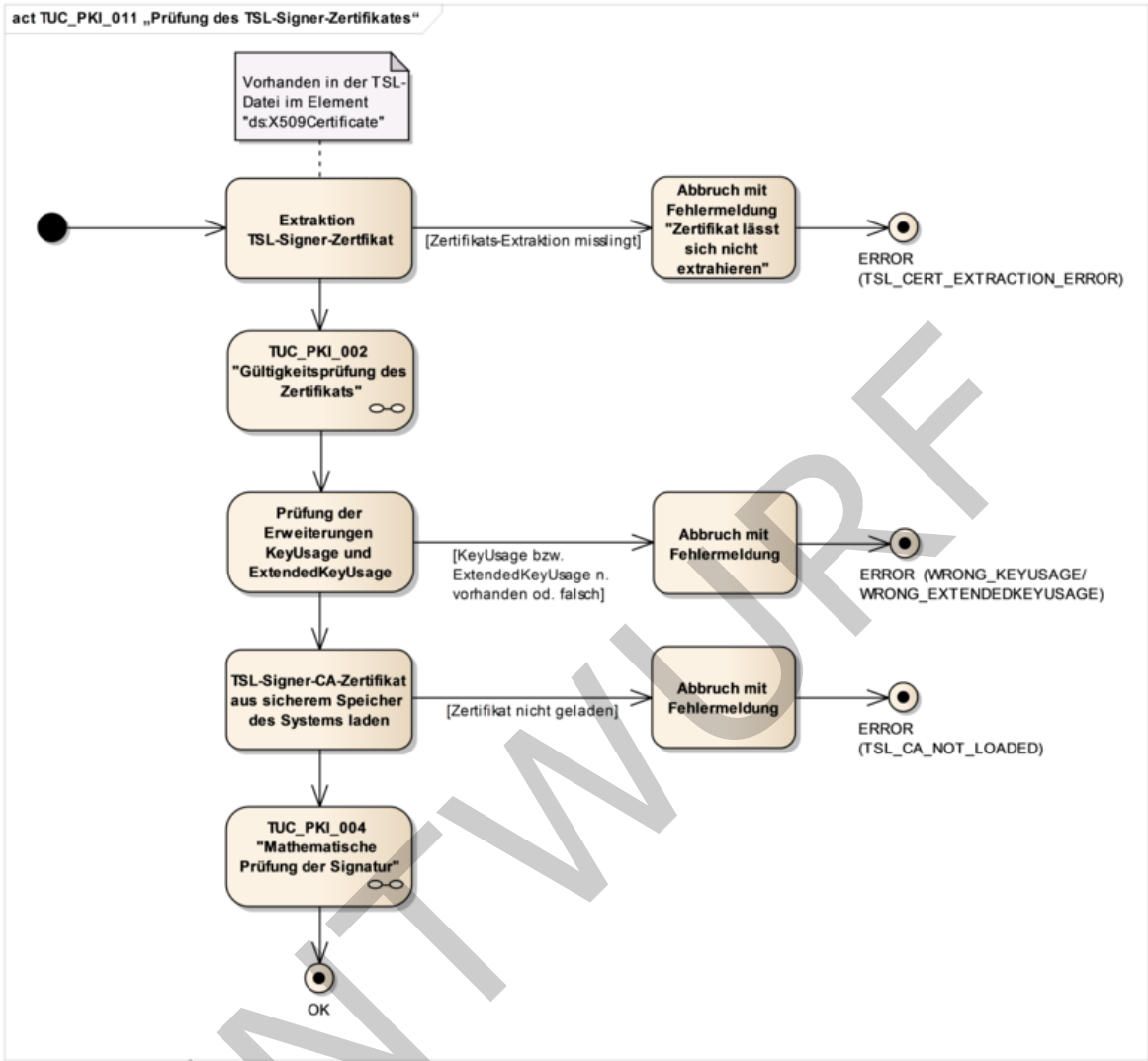
Anwendungsumfeld	System, das die TSL verwendet
Vorbedingungen	TSL-Signer-CA-Zertifikat in einem sicheren Speicher des Systems
Auslöser	TUC_PKI_019 „Prüfung der Aktualität der TSL“
Eingangsdaten	<ul style="list-style-type: none"> • TSL-Datei • Referenzzeitpunkt (Datum optional; bei Nichtangabe Verwendung 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.)

	<p>6. [System:] Ende des Use Case mit Status Rückmeldung</p>
Varianten/Alternativen	
Fehlerfälle	<p>1a. [System:] Das TSL-Signer-Zertifikat lässt sich nicht aus der TSL-Datei extrahieren (TSL_CERT_EXTRACTION_ERROR). 3a. [System:] KeyUsage ist nicht vorhanden bzw. entspricht nicht der vorgesehenen KeyUsage (WRONG_KEYUSAGE). 3a1. [System:] ExtendedKeyUsage entspricht nicht der vorgesehenen ExtendedKeyUsage (WRONG_EXTENDEDKEYUSAGE). 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	<p>Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.</p>

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". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.</p>

3367
3368

3369



3370

3371

3372 **Abbildung 12: Aktivitätsdiagramm TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“**

3373 **8.2.2.4 TUC_PKI_012 „XML-Signatur-Prüfung“**

3374 **GS-A_4651 - TUC_PKI_012: XML-Signatur-Prüfung**

3375 Die Produkttypen der TI, die Zertifikate prüfen MÜSSEN TUC_PKI_012 zur Prüfung der
3376 Signatur einer XML-Datei umsetzen.

3377 [**<=**]

3378

3379 **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].

3380 8.2.3 TSL-Sicherheitsaspekte

3381 Für den TI-Vertrauensanker, das TSL-Signer-CA-Zertifikat, und für die TSL (die
3382 enthaltenen Zertifikate und auch die eigentliche TSL-Datei im XML-Format) gilt ein hoher
3383 Schutzbedarf. Dieser wird dadurch gewährleistet, dass TI-Vertrauensanker und TSL-Datei
3384 initial auf (organisatorisch) abgesichertem Weg in die Komponente, bzw. deren sicheren
3385 Speicher, eingebracht werden. Vor einem Wechsel der TSL (oder des TI-
3386 Vertrauensankers via TSL) müssen immer zwingend Zertifikats- und Signaturprüfungen
3387 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.

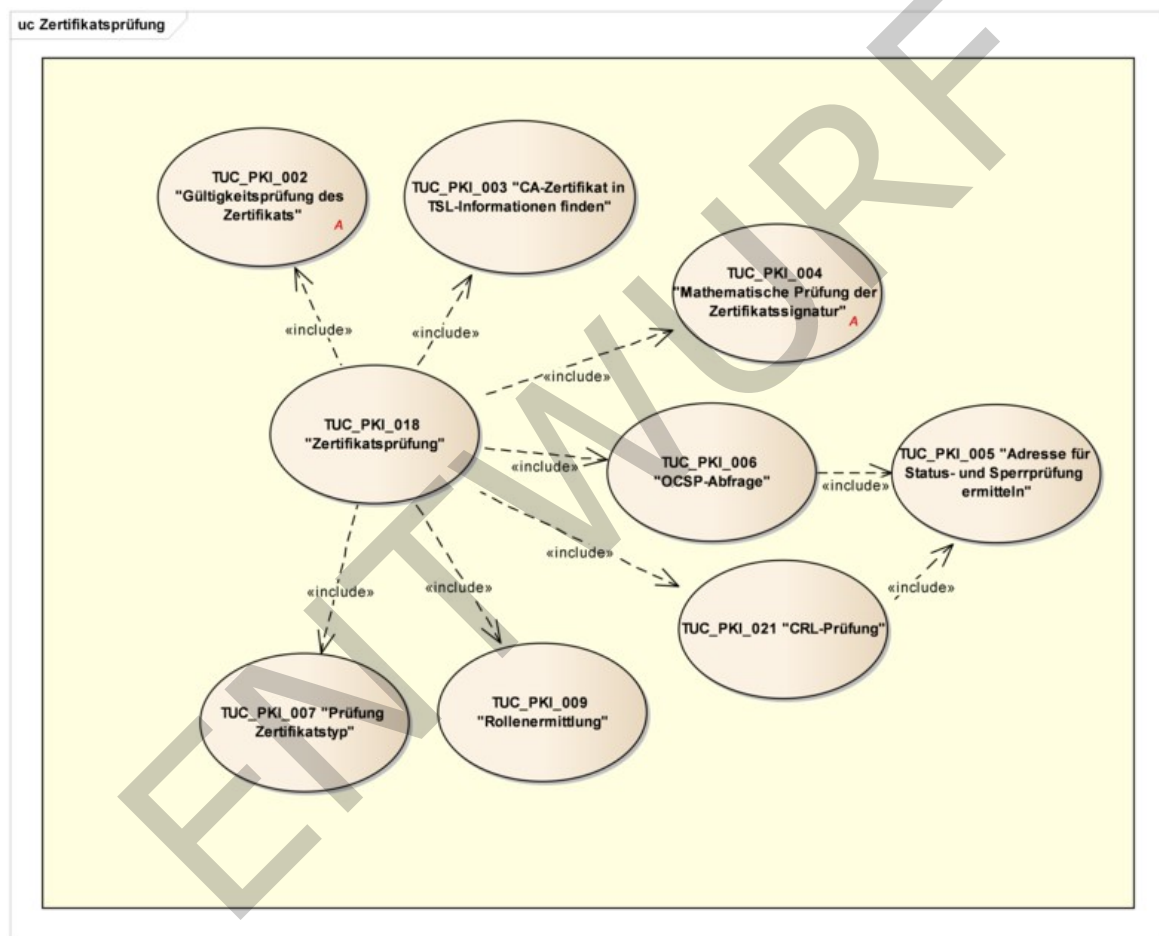


Abbildung 13: Use Case Diagramm „Zertifikatsprüfung“

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)

- 3439 • Abfrage des Sperrstatus des zu prüfenden Zertifikats gegen den im
3440 „ServiceSupplyPoint“ der TSL eingetragenen OCSP-Responder (TUC_PKI_006) und
3441 Prüfung der OCSP-Antwort (Responder-Zertifikat, Sperrstatus)
- 3442 • Rollenermittlung (TUC_PKI_009)
- 3443 • Prüfung Zertifikatstyp (TUC_PKI_007)
- 3444 Bei jeder dieser Prüfungen muss nicht nur die mathematisch-kryptographische
3445 Korrektheit der jeweiligen Mechanismen, sondern auch deren Zulässigkeit mit in die
3446 Prüfung einbezogen werden. Zum Beispiel darf ein Zertifikat, welches nicht mit einem
3447 zugelassenen Hash-Algorithmus signiert ist, nie als gültig eingestuft werden. Für die TI
3448 gültige Hash-Algorithmen siehe [gemSpec_Krypt].
- 3449 Die Verwendung von Informationen aus Zertifikaten kann nur dann erfolgen, wenn das
3450 zugehörige Zertifikat validiert wurde. Somit MUSS eine Zertifikatsprüfung der Ermittlung
3451 bestätigter Zertifikatsinformationen vorangehen.
- 3452 In dem Dokument wird der Begriff „gültiger Zeitraum“ verwendet. Dieser bedeutet, dass
3453 sich der aktuelle Zeitpunkt innerhalb des Gültigkeitszeitraums des Objektes befindet.
- 3454 Die Fachdokumente müssen die entsprechenden Eingangsparameter der Use Cases
3455 berücksichtigen. Die Festlegungen aus den folgenden Dokumenten sind für die
3456 Zertifikatsprüfung verbindlich:
- 3457 • [Common-PKI]: Specifications for Interoperable PKI Applications
- 3458 • [RFC 2560]: X.509 Internet Public Key Infrastructure Online Certificate Status
3459 Protocol – OCSP
- 3460 • [RFC 5280]: Internet X.509 Public Key Infrastructure – Certificate and Certificate
3461 Revocation List (CRL) Profile.

3462 8.3.1 Zertifikatsprüfung in der TI

3463 8.3.1.1 TUC_PKI_018 „Zertifikatsprüfung in der TI“

3464 GS-A_4652 - TUC_PKI_018: Zertifikatsprüfung in der TI

3465 Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_018 zur
3466 Zertifikatsprüfung umsetzen.

3467 [\leq]

3468

3469 **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) • 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 beispielsweise technisch nicht erreichbar ist. • Prüfmodus (OCSP, CRL)
Komponenten	System, OCSP-Responder

Ausgangsdaten	Status der Prüfung, OCSP-Response, im Zertifikat enthaltene Rollen-OIDs
Referenzen	[Common-PKI]

ENTWURF

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. [System] Mathematische Prüfung der Signatur des Zertifikats (TUC_PKI_004 "Mathematische Prüfung der Zertifikatssignatur").5. [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. Der Zeitpunkt des Gültigkeitsbeginns des End-Entity-Zertifikats liegt vor dem
----------------	--

	<p>Zeitpunkt des Statuswechsels.</p> <p>6. [System, Prüfmodus Offline] Falls JA, weiter mit Schritt 8, sonst mit 7.</p> <p>7. [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 Störungssampel (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. [System:] Ermittlung (TUC_PKI_009 "Rollenermittlung") der Rolle</p> <p>9. [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.) mindestens eine OID enthalten.</p> <p>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.</p> <p>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.</p> <p>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).</p> <p>2a1. [System:] intendedExtendedKeyUsage enthält Werte und nicht alle davon sind in der ExtendedKeyUsage enthalten (WRONG_EXTENDEDKEYUSAGE).</p> <p>5a. [System:] Das Ausgabedatum des End-Entity-Zertifikats liegt nach dem Datum des Statuswechsels. Abbruch mit Fehlermeldung (CA_CERTIFICATE_REVOKED_IN_TSL)</p> <p>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 Prüfung wird in diesem Fall durch Aufruf des TUC_PKI_006 durchgeführt, als wäre keine OCSP-Response beigefügt. In den Rückgabewerten dieses TUC wird die Warnmeldung</p>

	(PROVIDED_OCSP_RESPONSE_NOT_VALID) an die aufrufende Funktion übergeben.
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	Gültige Status zu Schritt 5 sind gemäß Tab_PKI_271 inaccord, revoked und expired. 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. Eine Zertifikatsprüfung in der TI gemäß TUC_PKI_018 darf nach Ablauf der TSL- Graceperiod nicht positiv ausfallen (vgl. GS- A_5336).
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_018 "Zertifikatsprüfung". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

3470

3471

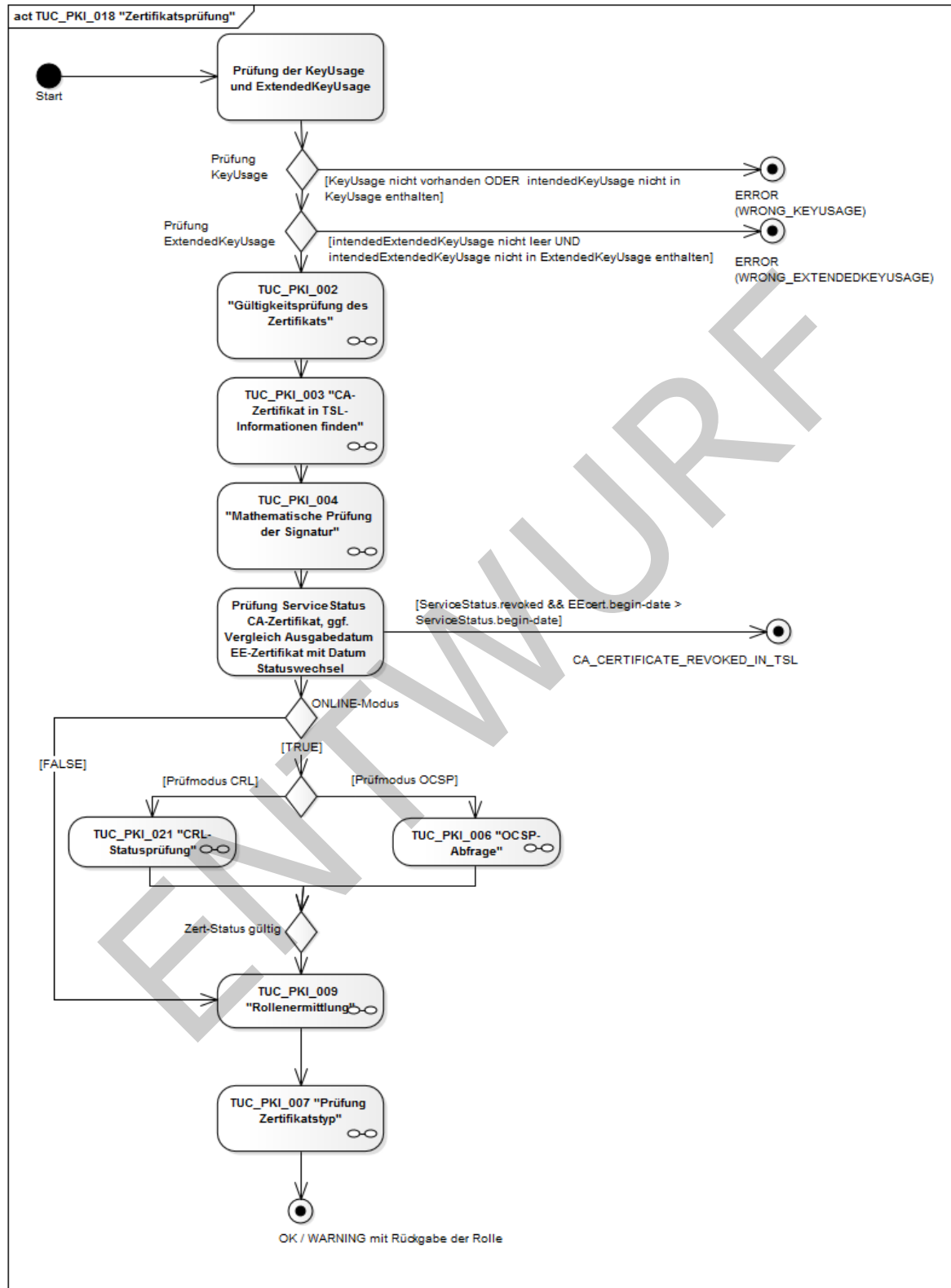


Abbildung 14: Aktivitätsdiagramm TUC_PKI_018 „Zertifikatsprüfung“

8.3.1.2 TUC_PKI_002 „Gültigkeitsprüfung des Zertifikats“

GS-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"
Eingangsdaten	<ul style="list-style-type: none"> Das zu prüfende Zertifikat Referenzzeitpunkt (optional; bei Nichtangabe Verwendung der aktuellen Systemzeit)
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]

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 Zertifikat 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	Der Aufbau der Gültigkeit: wird nicht näher spezifiziert, sondern richtet sich nach referenzierten Standards
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_002 Gültigkeitsprüfung des Zertifikats. Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

3481

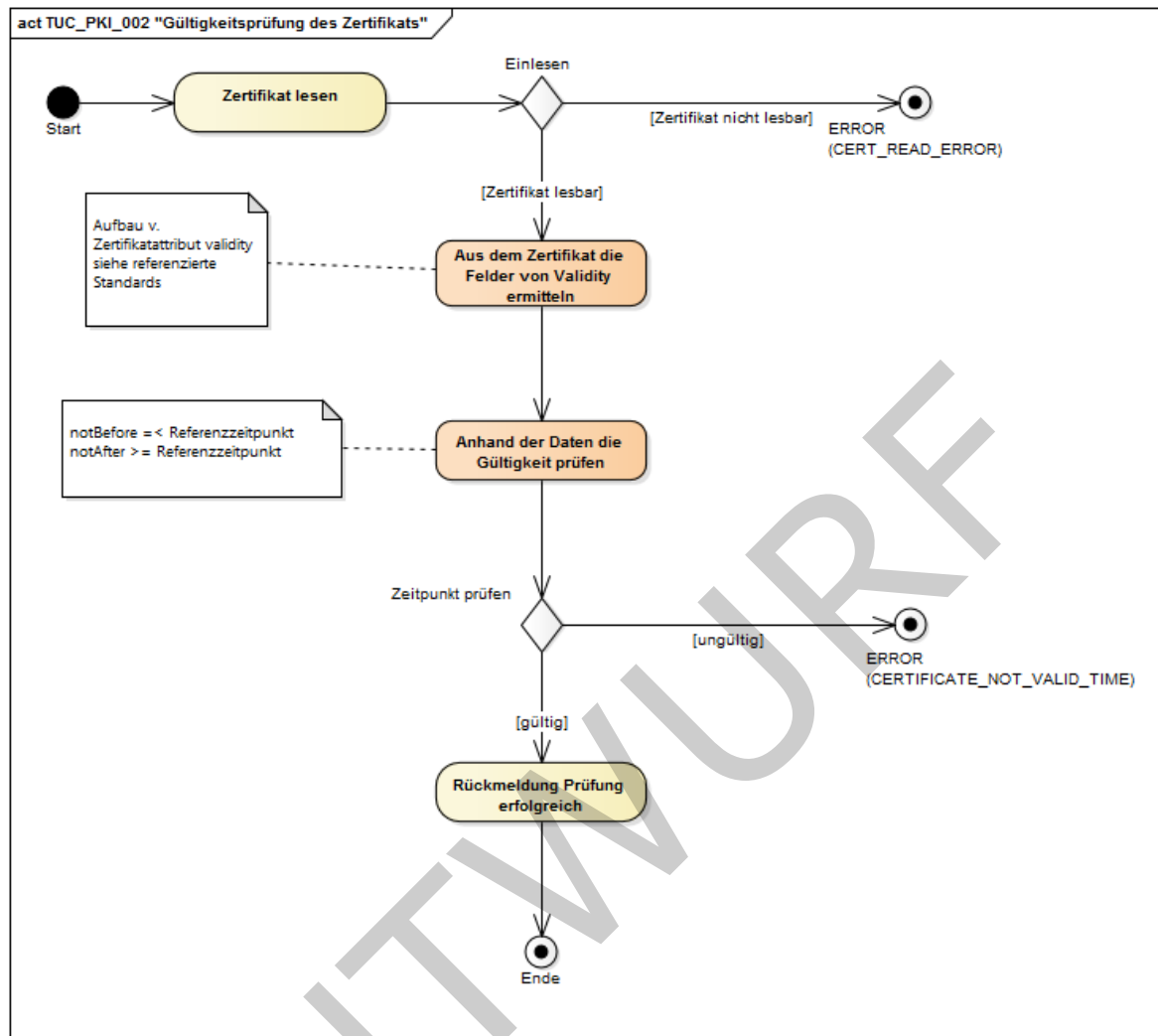


Abbildung 15: Aktivitätsdiagramm TUC_PKI_002 Gültigkeitsprüfung des Zertifikats

8.3.1.3 TUC_PKI_003 „CA-Zertifikat in TSL-Informationen finden“

GS-A_4654 - 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.

[<=]

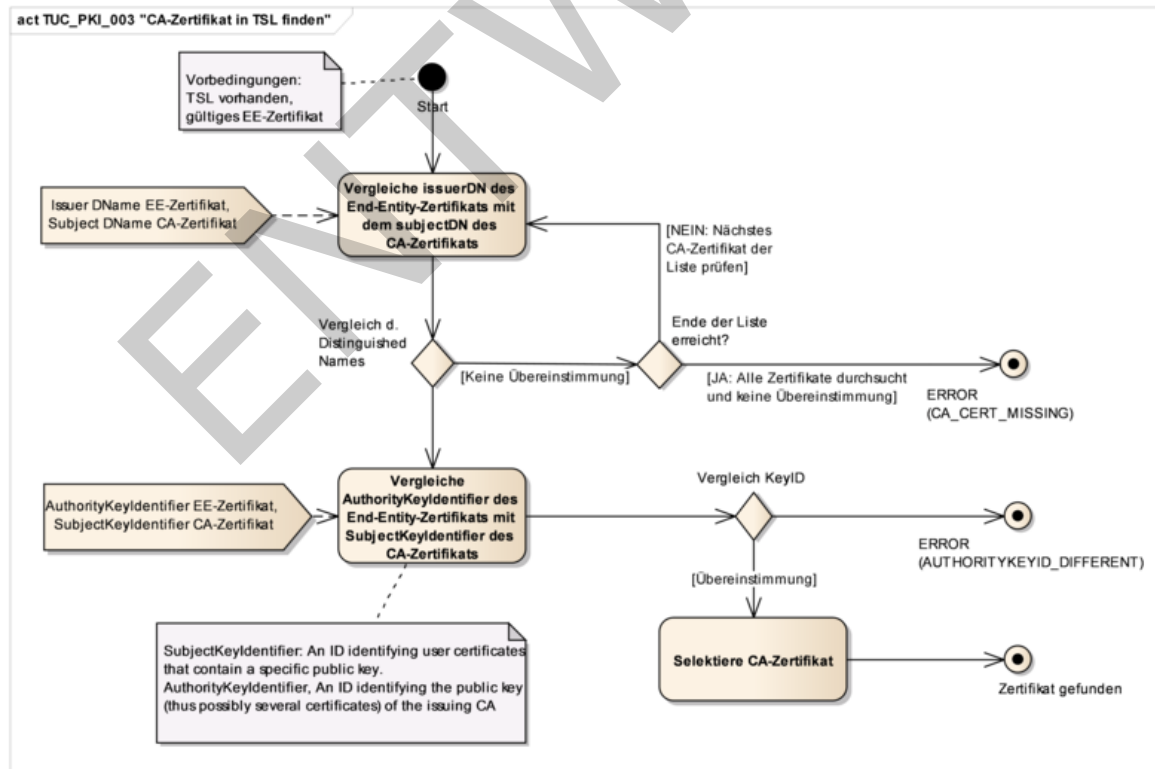
Tabelle 89: TUC_PKI_003 „CA-Zertifikat in TSL-Informationen finden“

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]
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. 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	<ol style="list-style-type: none"> 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.

3491
3492



3493
3494
3495

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 - TUC_PKI_004: Mathematische Prüfung der Zertifikatssignatur

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_004 zur mathematischen Prüfung der Zertifikatssignatur umsetzen.

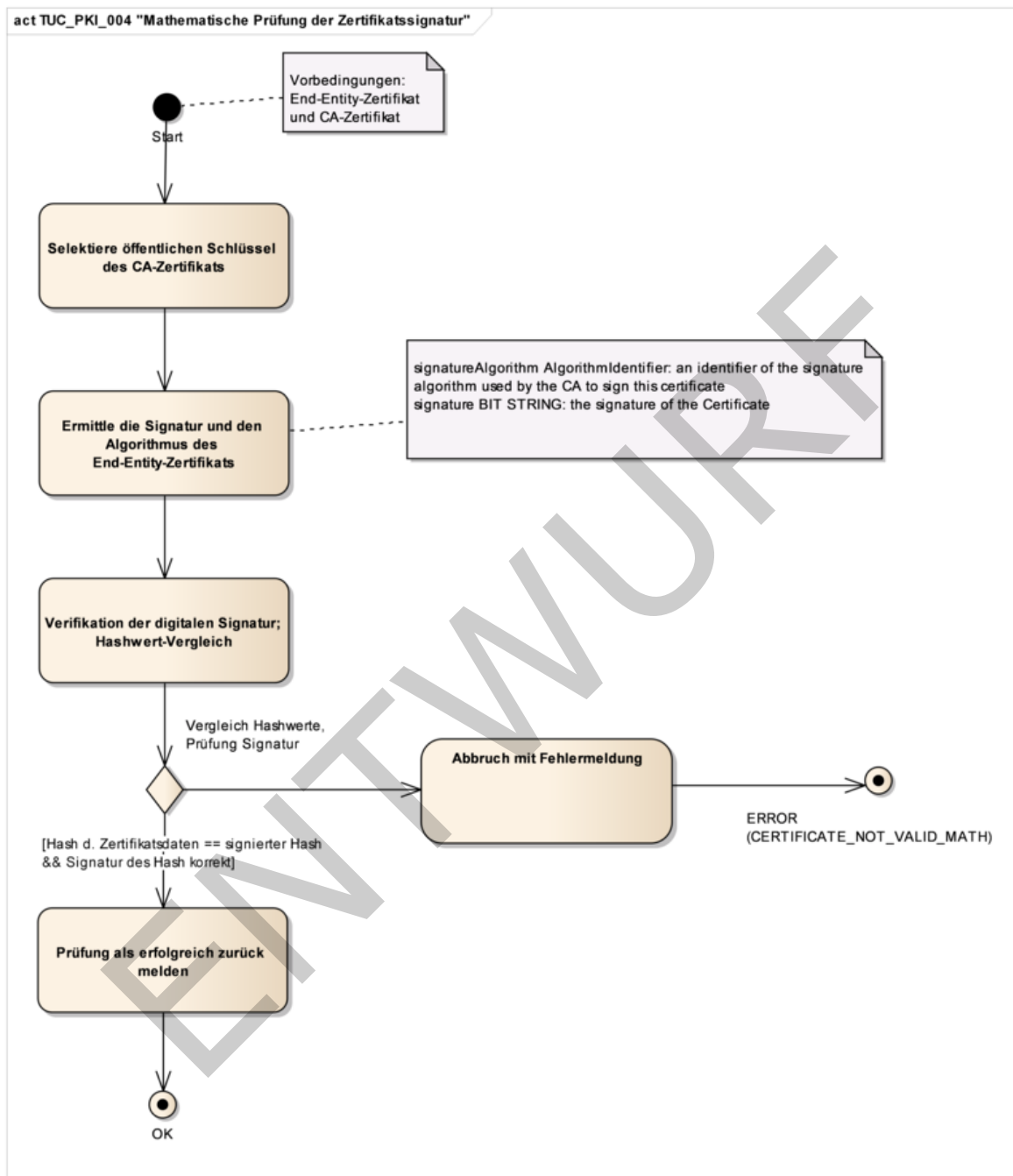
[<=]

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]
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]) 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.

3503
3504



3505
3506
3507

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	<p>1. [System:] (Referenz auf) CA-Zertifikat in TSL-Informationen finden (TUC_PKI_003 "CA-Zertifikat in TSL-Informationen finden")</p> <p>2. [System:] Das Element "ServiceSupplyPoint" (bzw. via referenziertes CA-Zertifikat die Referenz auf den bezeichneten Statusprüfdienst- oder CRL Downloadpunkt) auswählen und URI selektieren.</p> <p>3. [System:] Adresse zurückmelden</p>
Fehlerfälle	<p>1a. [System:] CA kann nicht in den TSL-Informationen ermittelt werden (CA_CERT_MISSING).</p> <p>2a. [System:] Das Element „ServiceSupplyPoint" konnte nicht gefunden werden (SERVICESUPPLYPOINT_MISSING). Weitere Fehlerfälle werden in den jeweiligen referenzierten TUCs beschrieben.</p>
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	<p>Aktivitätsdiagramm TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln".</p> <p>Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.</p>

3516
3517

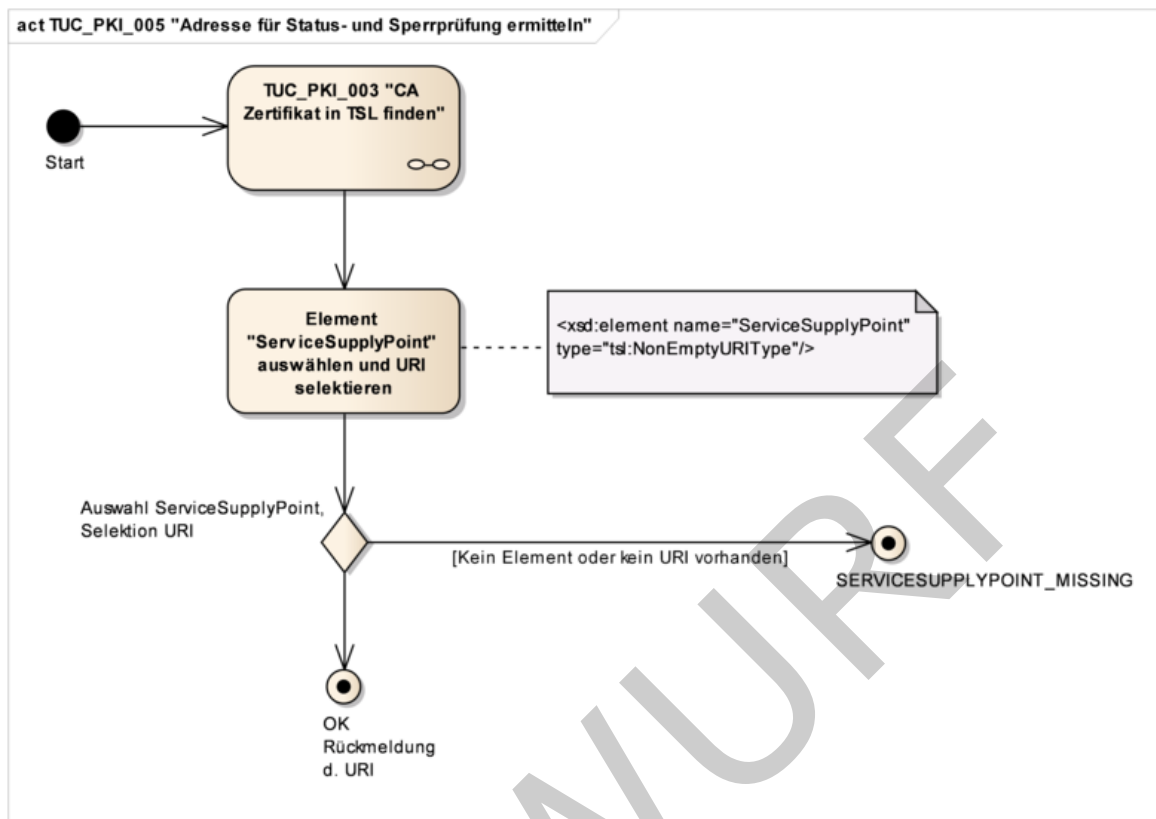


Abbildung 18: Aktivitätsdiagramm TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln“

8.3.2.2 TUC_PKI_006 „OCSP-Abfrage“

GS-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] 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)• 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#Part5#2.3], [RFC2560]/[RFC6960], [RFC5019]

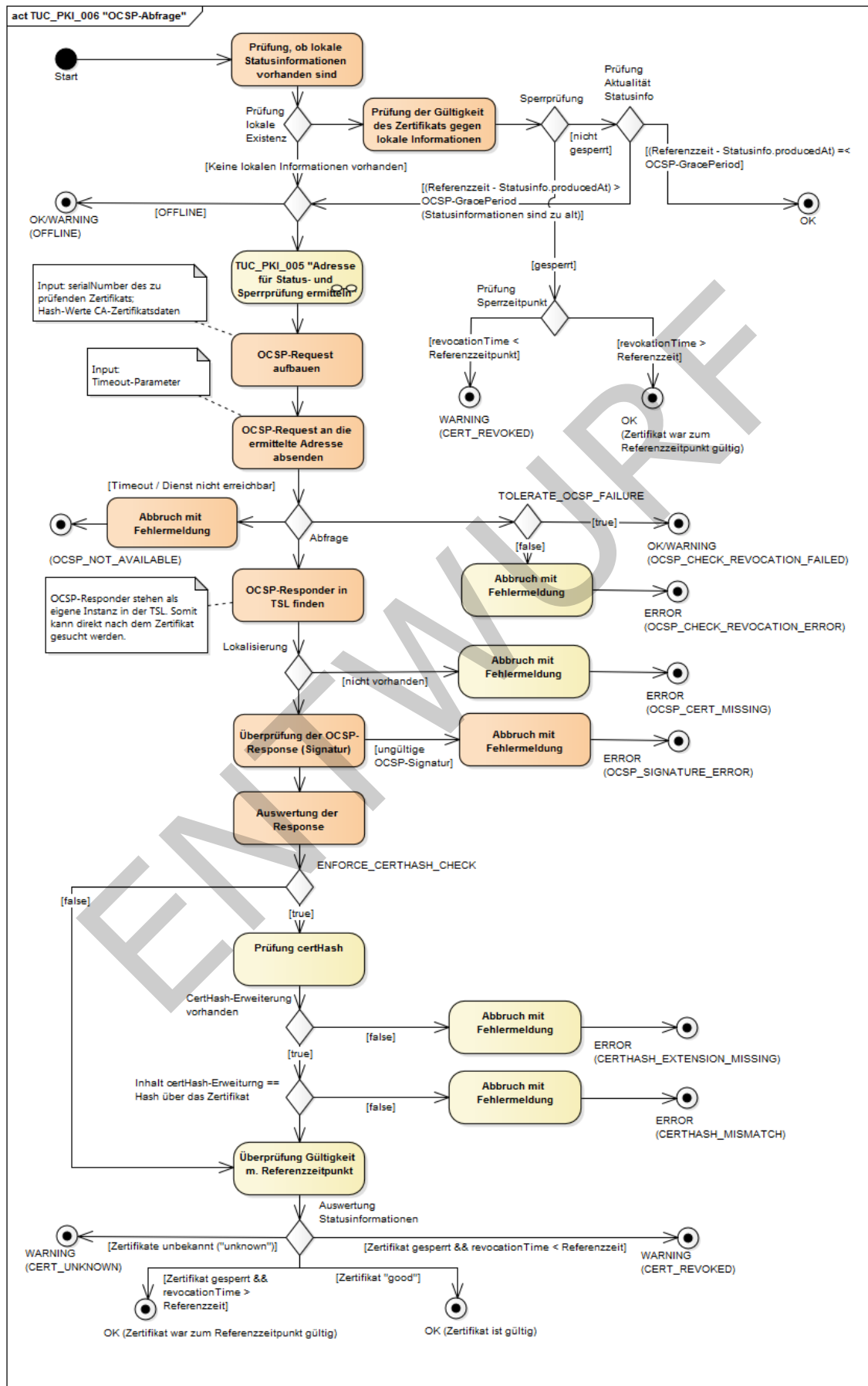
Standardablauf	<ol style="list-style-type: none">1. [System:] Prüfung, ob (zum Referenzzeitpunkt unter Berücksichtigung der OCSP-Graceperiod) gültige Statusinformationen bereits vorliegen (z. B. im lokalen Cache bereitgestellt).2. [System:] Ermittlung der OCSP-Adresse (TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln")3. [System:] Aufbau des OCSP-Request anhand der passenden Zertifikatsdaten4. [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. [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 „ServiceTypeIdentifier“ "http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP" markiert.)6. [System:] Auswertung der OCSP-Response. Dies umfasst die Prüfung von<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. 4.2,• [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]).
----------------	--

7.
[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].
8.
[System:] Überprüfung der Gültigkeit anhand des Referenzzeitpunkts. Der CertStatus "good" wird gemeldet.
9.
[System:] Rückmeldung, dass das Zertifikat gültig ist und Rückgabe der OCSP-Response.
10.
[System:] Ende des UseCase

Varianten/Alternativen	<p>1a. [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. 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#2.1 verarbeitet werden, unabhängig davon, ob das Feld "parameters" der Sequenz AlgorithmIdentifizier innerhalb der CertID mit NULL belegt oder nicht gesetzt ist.</p> <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.</p>
Zugehörige Diagramme	<p>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.</p>



3529 **Abbildung 19: Aktivitätsdiagramm TUC_PKI_006 „OCSP-Abfrage“**

3530 **8.3.2.3 TUC_PKI_021 „CRL-Prüfung“**

3531 **GS-A_4900 - TUC_PKI_021 "CRL-Prüfung"**

3532 Der Konnektor MUSS den TUC_PKI_021 zur Prüfung der Widerrufsinformationen
3533 (Statusprüfung) mittels Zertifikatssperrliste (CRL) umsetzen.

3534 [\leq]

3535

3536 **Tabelle 93: TUC_PKI_021 „CRL-Prüfung“**

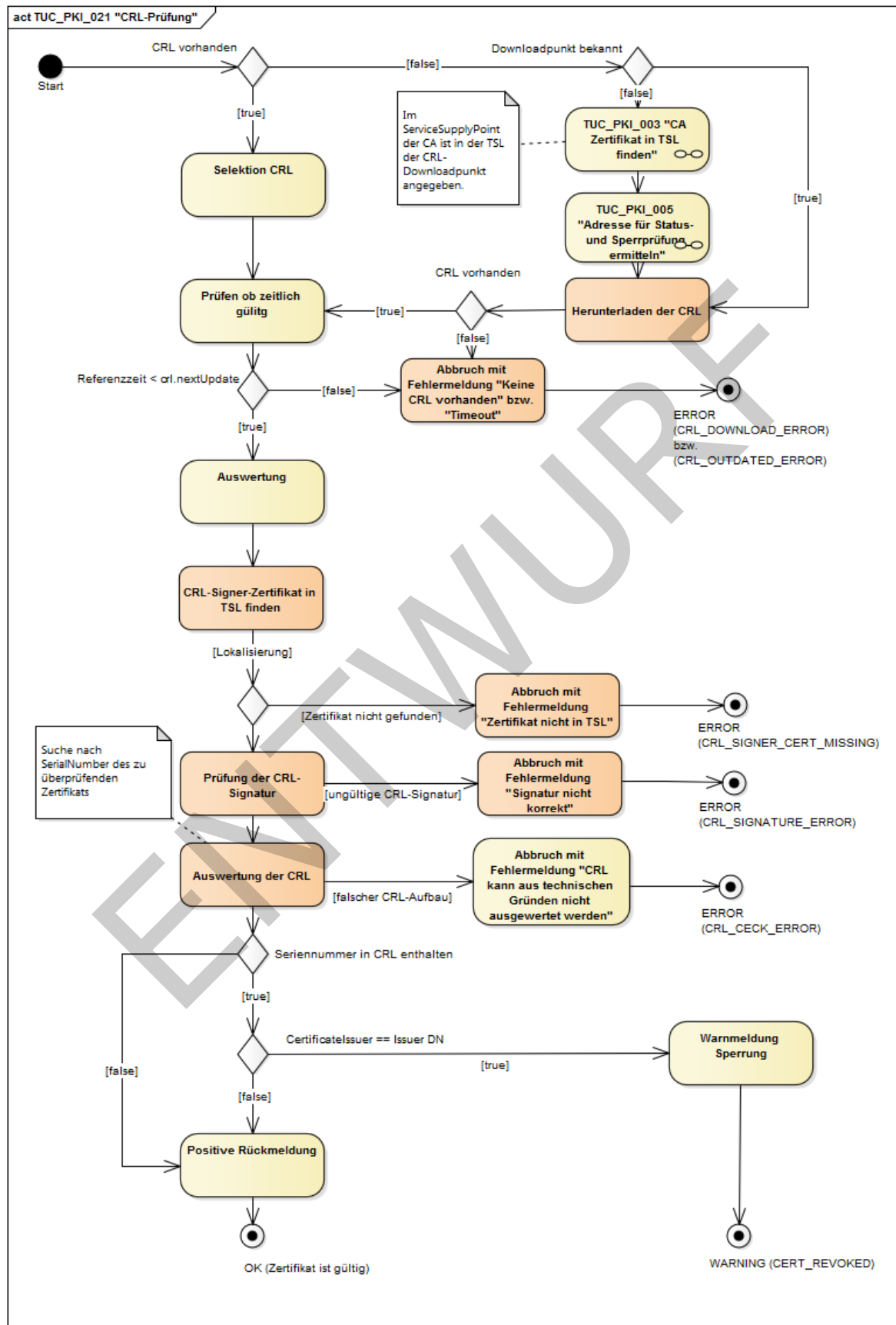
Element	Beschreibung
Name	TUC_PKI_021 „CRL-Prüfung“
Beschreibung	Dieser Use Case beschreibt den Prozess zur Validierung einer CRL (Certificate Revocation List) sowie den Prozess zur Ermittlung der Sperrinformationen zu einem End-Entity-Zertifikat mittels einer CRL.
Anwendungsumfeld	Use Case für den Anwendungsfall 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.]

Standardablauf	<ol style="list-style-type: none">1. [System:] Selektion der CRL2. [System:] Prüfen der zeitlichen Gültigkeit der CRL (Systemzeit < <code>crl.NextUpdate</code>)3. [System:] Auswertung der Art der CRL. Es wird anhand der <code>IssuingDistributionPoint</code>-Erweiterung in der Sperrliste (CRL) geprüft, ob es sich um eine indirekte CRL handelt (<code>indirectCRL-bit</code>). [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.5. [System:] Prüfung der Signatur der CRL6. [System:] Auswertung der CRL-Einträge. Es wird nach der Zertifikatsseriennummer des zu überprüfenden End-Entity-Zertifikats in der CRL gesucht.7. [System:] Falls einer oder mehrere Einträge gefunden wurden, wird die CRL-Entry-Erweiterung „<code>CertificateIssuer</code>“ ausgelesen und deren Inhalt mit dem <code>Issuer-DistinguishedName</code> des End-Entity-Zertifikats verglichen. Nur wenn der Inhalt der <code>CertificateIssuer</code>-Erweiterung mit diesem <code>DistinguishedName</code> übereinstimmt, ist das Zertifikat gesperrt.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. Der Downloadpunkt der CRL ist aus dem Internet erreichbar. Als Übertragungsprotokoll für den allfälligen Download ist „HTTP“ zu verwenden. 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. 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". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.</p>

3537



3539 **Abbildung 20: Aktivitätsdiagramm TUC_PKI_021 „CRL-Prüfung“**

3540 **8.3.2.4 Szenarien für Offline und Timeout von OCSP**

3541 Komponenten und Systeme der Gesundheitstelematik, die ihre Funktion zeitweise oder
3542 ständig ohne Online-Zugang zur TI bereitstellen müssen, können im Offline-Fall keine
3543 Statusauskünfte für Zertifikate von OCSP-Respondern aus der TI erhalten und müssen
3544 somit die Zertifikatsprüfung auf die mathematische Prüfung gegen das Aussteller-CA-
3545 Zertifikat aus der lokal vorliegenden TSL beschränken.

3546 **GS-A_4658 - Zertifikatsprüfung in spezifizierten Offline-Szenarien**

3547 Die Produkttypen der TI, die Zertifikate prüfen und per Spezifikation ihre Funktionen
3548 zeitweise oder ständig offline von der TI erbringen, MÜSSEN für die explizit spezifizierten
3549 Offline-Szenarien bei der Zertifikatsprüfung die TUCs *TUC_PKI_005 OCSP-Adresse*
3550 *ermitteln* und *TUC_PKI_006 OCSP-Abfrage* auslassen.
3551 [**<=**]

3552 **8.3.2.5 Statusprüfung von eGK-Zertifikaten**

3553 Bei eGK-Zertifikaten ist es nicht ausgeschlossen, dass diese suspendiert, also nur
3554 vorübergehend gesperrt werden. Die OCSP-Statusinformationen für eGK-Zertifikate
3555 müssen deshalb in jedem Fall aktuell sein. (Bei Zertifikaten, die dauerhaft gesperrt
3556 werden, können sich Applikation hingegen auf OCSP-Responses, die den Status
3557 „revoked“ enthalten, verlassen, auch wenn diese älter sind. Vgl. *TUC_PKI_006 „OCSP-*
3558 *Abfrage*“)

3559 **GS-A_4943 - Alter der OCSP-Responses für eGK-Zertifikate**

3560 Die Produkttypen der TI, die Zertifikate der elektronischen Gesundheitskarte (eGK)
3561 prüfen, DÜRFEN NICHT OCSP-Responses für die Statusprüfung verwenden, deren Alter
3562 die OCSP-Graceperiod (maximale Caching-Dauer) übersteigt. Dies beinhaltet auch OCSP-
3563 Responses, die den Status „revoked“ enthalten.
3564 [**<=**]

3565 **8.3.3 Ermittlung von Autorisierungsinformationen**

3566 **8.3.3.1 Bestätigte Zertifikatsinformationen**

3567 Das vorliegende Kapitel beschreibt die Ermittlung der folgenden Informationen aus einem
3568 X.509-Zertifikat der Telematikinfrastruktur. Dabei geht es um:

- 3569
 - Zertifikatstypen
- 3570
 - Die Rolle der Zertifikatsidentität

3571 Die in diesem Kapitel beschriebenen Use Cases können durch weitere gematik
3572 Dokumente referenziert werden.

3573 **8.3.3.2 TUC_PKI_009 „Rollenermittlung“**

3574 **GS-A_4660 - TUC_PKI_009: Rollenermittlung**

3575 Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN *TUC_PKI_009* zur Ermittlung der
3576 Rolle der Identität umsetzen.
3577 [**<=**]

3578

3579 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 <code>professionOIDs</code> 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]</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>

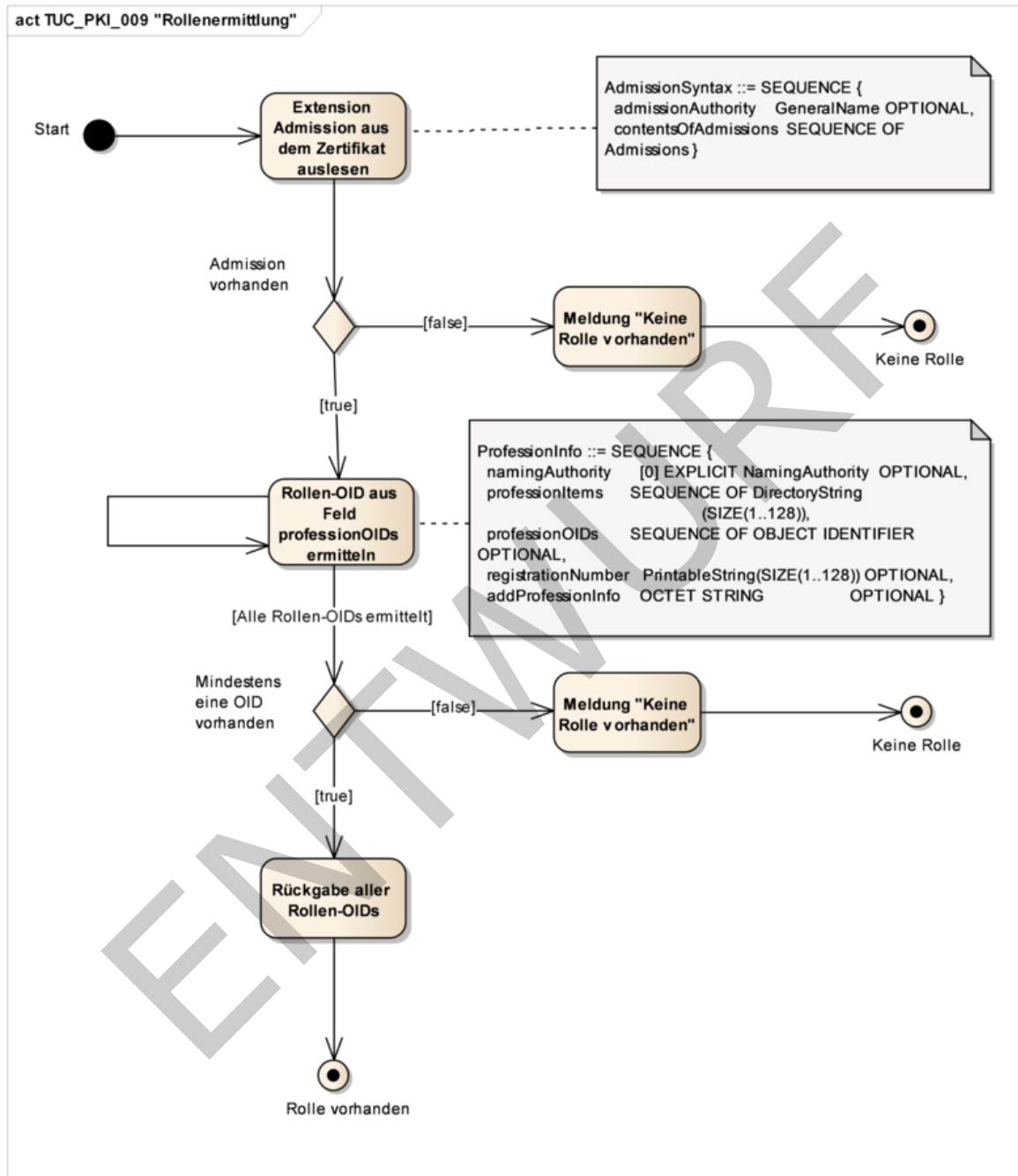


Abbildung 21: Aktivitätsdiagramm TUC_PKI_009 „Rollenermittlung“

8.3.3.3 TUC_PKI_007 „Prüfung Zertifikatstyp“

GS-A_4749 - TUC_PKI_007: Prüfung Zertifikatstyp

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_007 zur Prüfung des Zertifikatstyps umsetzen.

[<=]

3590

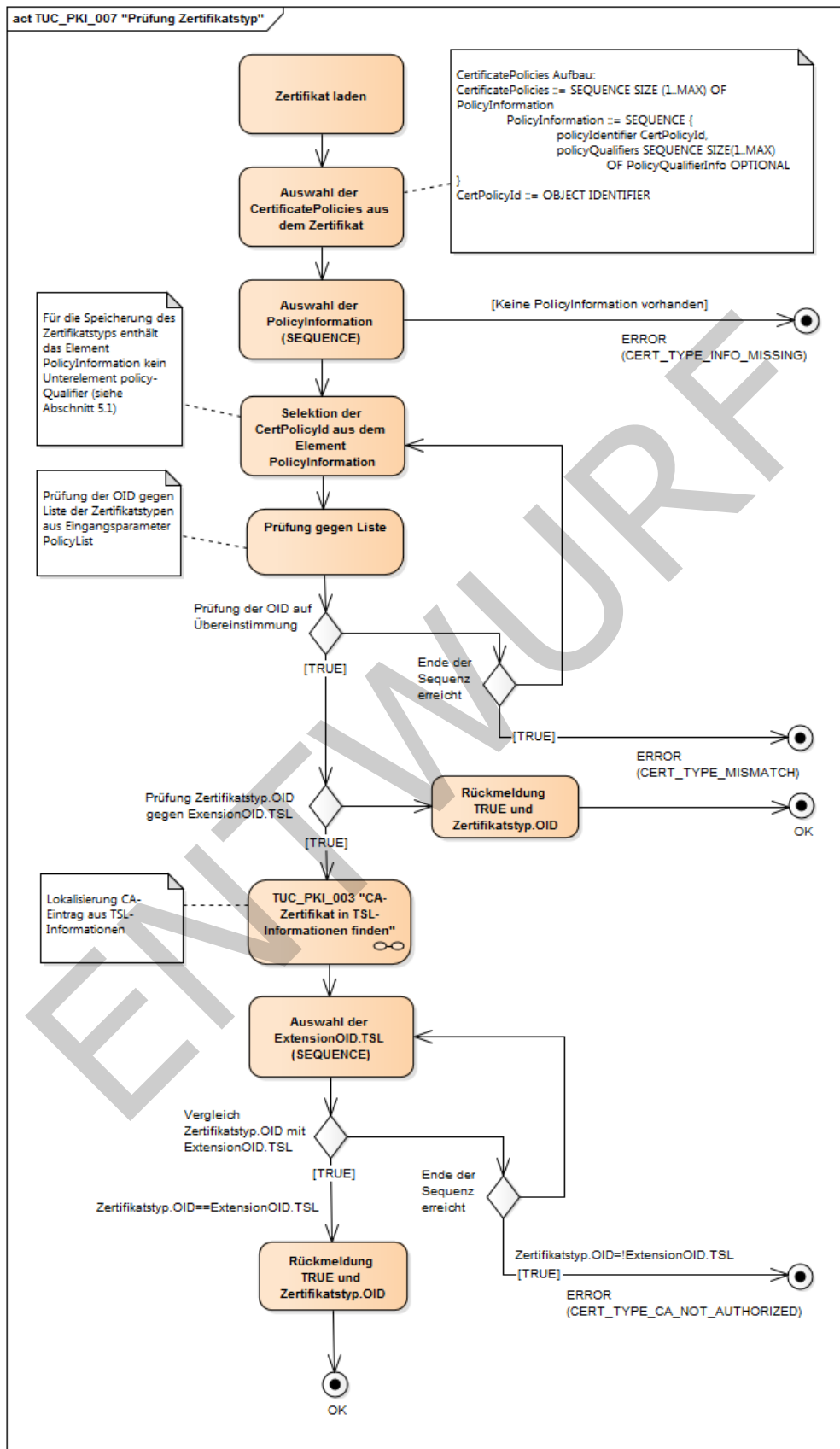
3591 **Tabelle 95: TUC_PKI_007 „Prüfung Zertifikatstyp“**

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. 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>

	<p>Element „ServiceInformationExtensions“ eingefügt, s. [gemSpec_TSL#7.3.2.1].</p>
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 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"). 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	<p>6a. [System:] Keine Übereinstimmung, nächstes Element PolicyInformation des Zertifikates wird analysiert. Wiederholung des Vorgangs ab Schritt 4.</p> <p>7a. Wird die Prüfung der ExtensionOID ausgelassen, endet der Use Case mit der Rückmeldung „Prüfung Zertifikatstyp erfolgreich“ und der Rückgabe der OID des Zertifikatstyps.</p>
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>Der Aufbau der Extension CertificatePolicies ist in Kapitel 4.8.3.3 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>

3592



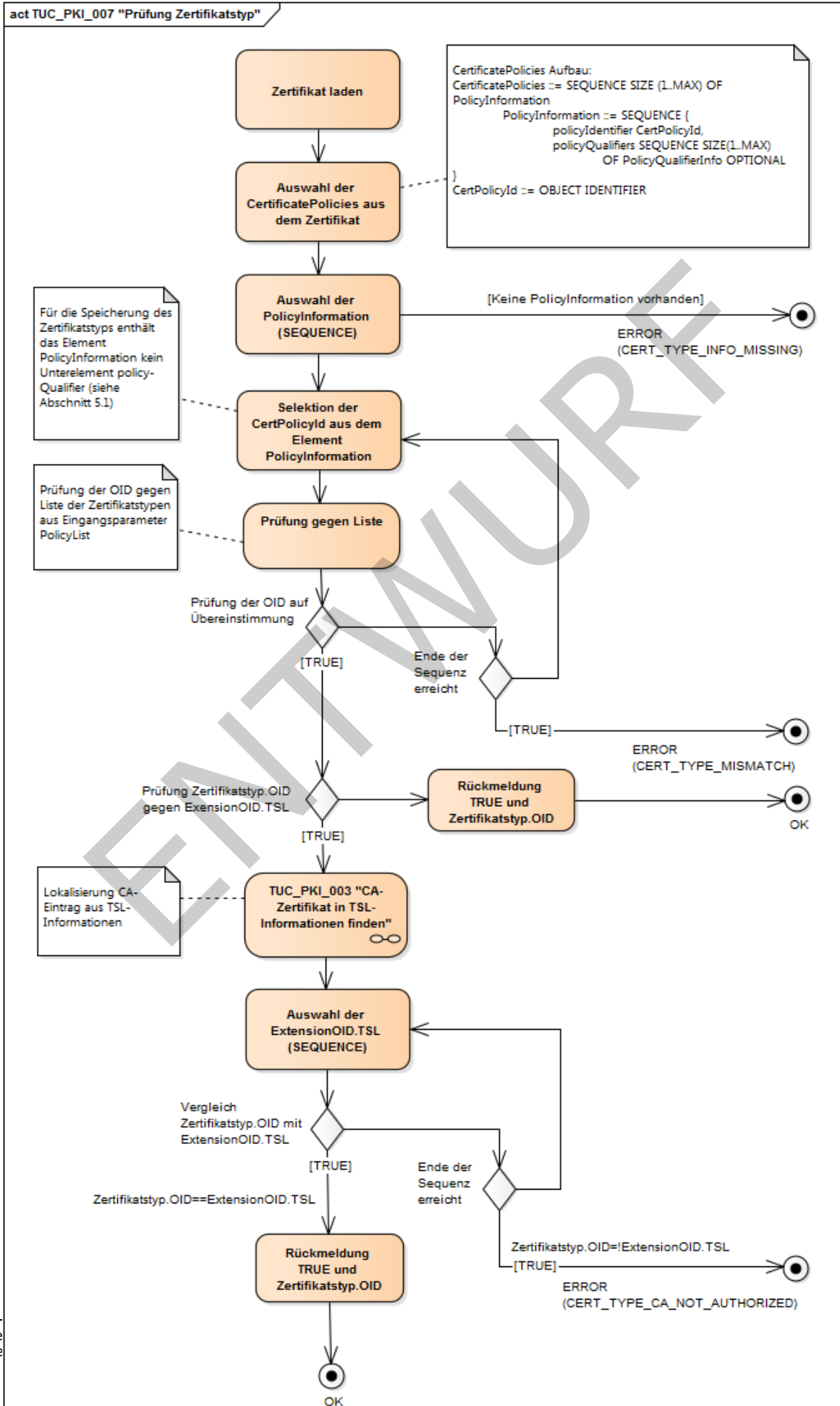


Abbildung 22: Aktivitätsdiagramm TUC_PKI_007 „Prüfung Zertifikatstyp“

8.3.4 Weitere Prüfungen

8.3.4.1 Umgang mit kritischen Extensions

GS-A_4661 - kritische Erweiterungen in Zertifikaten

Zertifikatsprüfenden Komponenten MÜSSEN kritische Zertifikatserweiterungen gemäß [RFC5280] und [Common-PKI] 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.

3621

3622 **GS-A_5077 - FQDN-Prüfung beim TLS-Handshake**

3623 Produkttypen der TI, die beim TLS-Handshake das TLS-Serverzertifikat prüfen, MÜSSEN
3624 sicherstellen, dass für den Verbindungsaufbau der FQDN im Zertifikat C.ZD.TLS-S bzw.
3625 C.FD.TLS-S mit dem der Komponente zugeordneten FQDN übereinstimmt.

3626 [\leq]

3627 **8.4.2 IPsec-Verbindungsaufbau**

3628 **GS-A_5078 - FQDN-Prüfung beim IPsec-Aufbau**

3629 Produkttypen der TI die beim Aufbau einer IPsec-Verbindung das IPsec-Serverzertifikat
3630 prüfen, MÜSSEN sicherstellen, dass der FQDN im Zertifikatattribut *SubjectDN* oder in der
3631 Erweiterung *SubjectAltNames* des Zertifikats C.VPNK.VPN bzw. C.VPNK.VPN-SIS mit dem
3632 der Komponente zugeordneten FQDN übereinstimmt.

3633
3634 [\leq]

3635 **8.5 Zertifikatsprüfung X.509 QES**

3636 Im Folgenden werden die notwendigen Voraussetzungen zur Prüfung von QES-
3637 Zertifikaten dargestellt:

- 3638 1. Die Zertifikatsüberprüfende Komponente muss die Gültigkeit des Zertifikats in
3639 Bezug auf den Signaturerstellungszeitpunkt und dem zu Grunde liegenden
3640 Gültigkeitsmodell überprüfen.
- 3641 2. Die Zertifikatsüberprüfende Komponente muss den Zertifikatsstatus mit dem vom
3642 jeweiligen TSP zur Verfügung gestellten Statusprüfdienst überprüfen.
- 3643 3. Die Zertifikatsüberprüfende Komponente muss auf die Anwendungsbereiche des
3644 Zertifikats und die damit verbundenen Einschränkungen achten.
- 3645 4. Das Schlüsselpaar QES ist ausschließlich für die qualifizierte elektronische
3646 Signatur nach [eIDAS] im Sinne der „Nicht-Abstreitbarkeit“ („nonrepudiation“
3647 bzw. „content commitment“) einzusetzen. Die Schlüsselpaare und Zertifikate
3648 dürfen nur für ihren jeweiligen Anwendungsbereich benutzt werden. Eine
3649 Benutzung außerhalb des zugehörigen Anwendungsbereichs ist nicht zulässig.
- 3650 5. Die Zertifikatsüberprüfende Komponente muss das QES-Zertifikat auf
3651 Vorhandensein der Extension QCStatement und einen darin enthaltenen Wert für
3652 QES-Konformität prüfen.
- 3653 6. Der Überprüfer hat die Sorgfaltspflicht, seine IT-Infrastruktur zu schützen und
3654 muss etwaige Nutzungsbeschränkungen im Zertifikat berücksichtigen.

3655 7. Die zertifikatsprüfende Komponente muss den Qualifikationsstatus des VDA
3656 anhand der von der Bundesnetzagentur bereitgestellten Vertrauensliste (BNetzA-
3657 VL) überprüfen.

3658 Die folgenden Use Cases verdeutlichen die Aktionen des Systems.

3659 Für die QES-Zertifikatsprüfung sind nur der TUC_PKI_030 "QES-Zertifikatsprüfung" und
3660 der TUC_PKI_036 „BNetzA-VL Aktualisierung“ für andere gematik Dokumente
3661 referenzierbar.

3662 **GS-A_4750 - TUC_PKI_030 „QES-Zertifikatsprüfung“**

3663 Alle Produkttypen, die QES-Zertifikate prüfen, MÜSSEN TUC_PKI_030 zur Prüfung der
3664 QES-Zertifikate umsetzen.

3665 [\leq]

3666 **8.5.1 TUC_PKI_030 „QES-Zertifikatsprüfung“**

3667 **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 den in [Common-PKI#Part5] und [Common-PKI#9] beschriebenen Schritten zusammen, sofern sie den Vorgaben von [eIDAS] nicht widersprechen. 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 (refTime): Zeitpunkt, für den das Zertifikat geprüft werden soll • 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
Standardablauf	<ol style="list-style-type: none"> 1. [System] Auslesen und Ausgabe aller gesetzten Elemente der Extension QCStatements des Zertifikates. 2. [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. 3. [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. <i>Hinweis: Für gültige Status siehe Anmerkungszeile zu diesem TUC.</i> 4. [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 <code>http://uri.telematik/TrstSvc/Svctype/TrustedList/schemerules/D E</code>) 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. <i>Hinweis: Details zu den TSL-Einträgen für URLs für OCSP-Responder in der TI unter gemSpec_TSL# TIP1-A_7219</i> 5. [System:] Die abzufragenden Statusinformationen zu QES-Zertifikaten werden unter Verwendung der aus der TSL ermittelten OCSP-Adresse eingeholt. <i>Hinweis: Details zur OCSP-Statusprüfung siehe Anmerkungszeile zu diesem TUC</i> 6. [System:] Ermittlung der Rolle (TUC_PKI_009 "Rollenermittlung") 7. [System:] Ende des Use Case mit Rückgabe des/der im Zertifikat enthaltenen Rollen-OID(s)

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>4a. [System:] Der Offline-Modus ist aktiviert. Es werden keine Statusinformationen eingeholt. (Schritte 4 und 5 entfallen.)</p> <p>5a. [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>5b. [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. 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. [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. [System:] Warnmeldung, dass keine Online-Statusprüfung durchgeführt wurde (NO_OCSP_CHECK).</p> <p>5c. [System:]. Der zuständige OCSP-Responder ist nicht erreichbar. Abbruch mit Fehlermeldung (OCSP_NOT_AVAILABLE).</p> <p>5d. [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>5e. Wenn die in einer OCSP-Response zurückgelieferte 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>5f. [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>
Sicherheitsanforderungen	

Anmerkungen	<p>Gültige Status zu Schritt 1 sind gemäß [ETSI TS 119 612#5.5.4 und #Annex J] <i>granted, accredited, undersupervision, supervisionincessation</i></p> <p>Die Einträge der QES-CA-Zertifikate in der BNetzA-VL besitzen gemäß [ETSI TS 119 612#5.5.1.1] die Extension AdditionalServiceInformation http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatureS.</p> <p>Die Einträge der QES-CA-Zertifikate in der BNetzA-VL besitzen den ServiceTypeIdentifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC.</p> <p>Schritt 2 stellt eine TI-spezifische Sperrprüfung des QES-CA-Zertifikats gemäß Kettenmodell dar. Zusätzlich zu 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:</p> <ul style="list-style-type: none"> • Zur Auswertung der OCSP-Response siehe auch [Common-PKI#Part4#3 und #Part9#4] • Zur Prüfung der certHash-Erweiterung siehe auch [Common-PKI#Part4#3.1.2] und [Common-PKI#Part5#2.3] sowie [gemSpec_Krypt#GS-A_4393] und GS-A_4693 • Zur Prüfung der OCSP-Response auf Integrität (Signatur): Das OCSP-Signer-Zertifikat kann streng gem. RFC6960 von der CA selbst signiert sein oder von einer beliebigen aktuell qualifizierten CA (vgl. gemKPT_PKI_TIP#4.5). Alternativ kann das OCSP-Signer-Zertifikat auch direkt als qualifizierter Dienst in der 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-Response-Signatur als fehlerhaft zu bewerten. In diesem Fall ist auch die OCSP-Response selbst als nicht gültig zu betrachten. • Zur Prüfung des OCSP-Signer-Zertifikats wird ebenfalls das Kettenmodell benutzt (vgl. [ETSI TS 119 172-4]).
Zugehörige Diagramme/Tabelle	

3668 8.5.2 TUC_PKI_036 „BNetzA-VL Aktualisierung“

3669 Der TSL-Dienst stellt die jeweils aktuelle BNetzA-VL an definierten Download-Punkten in
 3670 der TI bereit. Diese Download-Punkte sind so gewählt, dass sie von allen Diensten,
 3671 Systemen und Komponenten in der TI netzwerktechnisch erreicht werden können.

3672 Die Adressen der BNetzA-VL-Download-Punkte sind in Form von URI definiert und
 3673 Bestandteil der TSL (Details s. [gemSpec_TSL#7.5]).

3674 Die Signaturzertifikate der BNetzA-VL sind in der TSL gespeichert und darüber
3675 abgesichert (Details s. [gemSpec_TSL#7.5]).

3676 **GS-A_5484 - TUC_PKI_036 „BNetzA-VL-Aktualisierung“**

3677 Alle Produkttypen, die die BNetzA-VL verwenden, MÜSSEN TUC_PKI_036 zur
3678 Aktualisierung umsetzen.
3679

3680 **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	<p>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.</p> <ol style="list-style-type: none"> 1. [System:] System startet die Aktualisierung der BNetzA-VL 2. [System:] Primäre BNetzA-VL Hash Download-Adresse aus der TSL extrahieren (s. [gemSpec_TSL#7.5]). 3. [System:] Von der im vorherigen Schritt ermittelten Downloadadresse den aktuellen BNetzA-VL Hashwert vom TSL-Dienst herunterladen. 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. 5. [System:] Primäre BNetzA-VL Download-Adresse aus der TSL extrahieren (s. [gemSpec_TSL#7.5]). 6. [System:] Von der ermittelten Downloadadresse die

	<p>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 (falls vorhanden) sicher im System speichern. Ende des Use Cases.</p>
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</p>

	<p>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	

3681
3682
3683 [\leq]

3684 8.6 Fehlercodes bei TSL- und Zertifikatsprüfung X.509

3685 Die folgende Tabelle enthält die in den vorher beschriebenen TUCs zur TSL- und
3686 Zertifikatsprüfung potentiell auftretenden Fehlercodes und ordnet diesen gemäß
3687 [gemSpec_OM] jeweils einen Fehlerkategorie und Fehlerklasse zu.

3688 **GS-A_4751 - Fehlercodes bei TSL- und Zertifikatsprüfung**

3689 Die Produkttypen der TI, die Zertifikate prüfen und die TSL auswerten MÜSSEN die
3690 Fehlercodes gemäß Tab_PKI_274 nutzen. Das Element CompType MUSS belegt werden
3691 mit „[Produkttyp]:PKI“, wobei [Produkttyp] zu ersetzen ist durch den konkreten
3692 Produkttyp in der umzusetzenden Anforderung

3693 [\leq]

3694

3695
3696

Tabelle 99: Tab_PKI_274 Fehlercodes des SubCompTyps PKI bei TSL- und Zertifikatsprüfung

Co de	Sever ity	ErrorT ype	ErrorText	Detail	Meldungskürzel
1001	Error	Technic al	Es liegt keine gültige TSL vor		TSL_INIT_ERROR
1002	Error	Technic al	Zertifikate lassen sich nicht extrahieren		TSL_CERT_EXTRACTION_ERROR
1003	Error	Security	Mehr als ein markierter V-Anker gefunden		MULTIPLE_TRUST_ANCHOR
1004	Error	Technic al	TSL-Signer-CA lässt sich nicht extrahieren		TSL_SIG_CERT_EXTRACTION_ERROR
1005	Error	Technic al	Element „PointersToOtherTSL“ nicht vorhanden		TSL_DOWNLOAD_ADDRESS_ERROR
1006	Error	Technic al	TSL-Download-adressen wiederholt nicht erreichbar		TSL_DOWNLOAD_ERROR
1007	Error	Security	Vergleich der ID und Sequence-Number entspricht nicht der Vergleichs-variante 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 mathematisch nicht gültig.		CERTIFICATE_NOT_VALID_MATH
1026	Error	Technical	Das Element „Service-Supply Point“ konnte nicht gefunden werden.		SERVICESUPPLYPOINT_MISSING

1027	Error	Technical	CA kann nicht in den TSL-Informationen ermittelt werden.	Keine Adresse hinterlegt.	CA_CERT_MISSING
1028	Warning	Technical	Die OCSP-Prüfung konnte nicht durchgeführt werden (1)	TOLERATE_OCSP_FAILURE=true	OCSP_CHECK_REVOCATION_FAILED
1029	Error	Technical	Die OCSP-Prüfung konnte nicht durchgeführt werden (2)	TOLERATE_OCSP_FAILURE=false	OCSP_CHECK_REVOCATION_ERROR
1030	Error	Security	OCSP-Zertifikat nicht in TSL-Informationen enthalten		OCSP_CERT_MISSING
1031	Error	Security	Signatur der Response ist nicht gültig.		OCSP_SIGNATURE_ERROR
1032	Error	Technical	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</i>		OCSP_PROXY_NOT_AVAILABLE

			<i>verwendet. Stattdesse n ist der Fehlercode 1032 zu verwenden .</i>		
103 6	Error	Security	Das Zertifikat ist ungültig. Es wurde nach der Sperrung der aus- gebenden CA ausgestellt .		CA_CERTIFICATE_ REVOKED_IN_TSL
103 9	Warni ng	Security	Warnung, dass Offline- Modus aktiviert ist und keine OCSP- Status- abfrage durch- geführt wurde		NO_OCSP_CHECK
104 0	Error	Security	Bei der Online- status- prüfung ist ENFORCE_ CERTHASH_ _CHECK auf 'true' gesetzt, die OCSP- Response enthält jedoch keine certHash- Erweiterun g		CERTHASH_EXTENSION_ _MISSING

1041	Error	Security	Der certHash in der OCSP-Response stimmt nicht mit dem certHash des vorliegenden Zertifikats überein.		CERTHASH_MISMATCH
1042	Error	Technical	Das TSL-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 Statusinformationen verfügbar sind.		CERT_UNKNOWN
1047	Warning	Security	Das Zertifikat wurde vor oder zum Referenz-		CERT_REVOKED

			zeitpunkt widerrufen .		
1048	Error	Technical	Es ist ein Fehler bei der Prüfung des QC-Statements aufgetreten (z. B. nicht vorhanden, obwohl gefordert).		QC_STATEMENT_ERROR
1050	Warning	Technical	Die einem TUC zur Zertifikatsprüfung beigefügte OCSP-Response zu dem zu prüfenden Zertifikat kann nicht erfolgreich gegen das Zertifikat validiert werden.		PROVIDED_OCSP_RESPONSE_NOT_VALID
1051	Error	Security	Die in einem OCSP-Response zurückgelieferte Nonce stimmt nicht mit der Nonce des OCSP-Requests überein.		OCSP_NONCE_MISMATCH
1052	Error	Security	Attribut-Zertifikat kann dem übergebenen		ATTR_CERT_MISMATCH

			Basis-Zertifikat nicht zugeordnet werden.		
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 Exception-Meldung.		OCSP_STATUS_ERROR
1059	Error	Security	CA-Zertifikat für QES-Zertifikatsprüfung nicht qualifiziert		CA_CERTIFICATE_NOT_QES_QUALIFIED
1060	Error	Technical	Die VL kann nicht		VL_UPDATE_ERROR

			aktualisiert werden.		
106 1	Error	Security	CA (laut TSL) nicht autorisiert für die Herausgabe dieses Zertifikatstyps.		CERT_TYPE_CA_NOT_AUTHORIZED
106 2	Error	Security	Das QES-EE-Zertifikat ist ungültig. Es wurde nach der Sperrung der ausgebenden QES-CA ausgestellt.		CA_CERTIFICATE_REVOKED_IN_BNETZA_VL

3697

3698 8.7 Zertifikatsprüfung CV-Zertifikate der 2. Generation

3699 Die Prüfung von CV-Zertifikaten der Generation 2 beschränkt sich nicht nur auf die
3700 Prüfung der Vertrauenskette und die Signaturprüfung. Zusätzlich werden einige der
3701 verwendeten Schlüsselattribute des CV-Zertifikats und der weiteren CV-Zertifikate in der
3702 Vertrauenskette geprüft bzw. ausgewertet, insbesondere das Certificate Effective Date
3703 (CED) und das Certificate Expiration Date (CXD). Die Prüfung der Signatur eines CV-
3704 Zertifikats erfolgt mittels eines öffentlichen Schlüssels, der vor der Zertifikatsprüfung
3705 ausgewählt wird. Die Prüfschritte erfolgen gemäß Schalenmodell komplett „intern“ durch
3706 das Betriebssystem der prüfenden Chipkarte.

3707 Handelt es sich bei dem Produkttyp der TI, der das CV-Zertifikat prüfen soll, um eine
3708 Chipkarte, dann wird dieser öffentliche Schlüssel durch ein MSE-Set-Kommando der
3709 Karte bekannt gegeben.

3710 GS-A_5009 - Prüfung der mathematischen Korrektheit von CV-Zertifikate der 3711 Generation 2

3712 Die Produkttypen der TI, die CV-Zertifikate prüfen, MÜSSEN bei der Prüfung von CV-
3713 Zertifikaten der Generation 2 die Prüfung der mathematischen Korrektheit vornehmen, d.
3714 h. ob die Signatur des CV-Zertifikats mit dem CV-Zertifikat der ausstellenden TSP-CVC
3715 und ob die Signatur des TSP-CVC -Zertifikats mit dem CV-Zertifikat der ausstellenden
3716 CVC-Root-CA erfolgreich geprüft werden kann.

3717 [\leq]

GS-A_5010 - Prüfung der Signatur eines CV-Zertifikats der Generation 2 mit Hilfe des CV-Zertifikats des Herausgebers

Die Produkttypen der TI, die CV-Zertifikate prüfen, MÜSSEN bei der Prüfung der mathematischen Korrektheit der Signatur eines CV-Zertifikates *C* die im CV-Zertifikat des öffentlichen Schlüssels des Herausgebers enthaltenen Schlüsselattribute dieses öffentlichen Schlüssels anwenden. Die Prüfung MUSS den Vorgaben aus Tabelle TAB_PKI_908 folgen.

[<=]

Tabelle 100: Tab_PKI_908 Prüfung der Signatur eines CV-Zertifikats der Generation 2 mit Hilfe des CV-Zertifikats des Herausgebers

Prüfung der Korrektheit der Signatur eines CV-Zertifikats <i>C</i>
Sei die Nachricht <i>M</i> die gemäß Tabelle Tab_PKI_905 zu signierende Nachricht <i>M</i> des CV-Zertifikates <i>C</i> . Sei Signatur = <i>R</i> <i>S</i> gemäß Tabelle Tab_PKI_906 die Signatur der Nachricht <i>M</i> des CV-Zertifikats <i>C</i> . Sei <i>PuK</i> der im CV-Zertifikat des Herausgebers enthaltene öffentliche Signaturschlüssel des Herausgebers.
Bei der Prüfung der Signatur MUSS der domainParameter des Schlüssels <i>PuK</i> 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 <i>PuK.domainParameter</i> = brainpoolP256r1. B. '61' = 97 hat, gilt <i>PuK.domainParameter</i> = brainpoolP384r1. C. '81' = 129 hat, gilt <i>PuK.domainParameter</i> = 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 <i>C</i> und CV-Zertifikat des Herausgebers nicht miteinander korrespondieren sind, dann ist das CV-Zertifikat <i>C</i> nicht korrekt.

GS-A_5011 - Prüfung der Gültigkeit von CV-Zertifikaten der Generation G2

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN bei der Prüfung von CV-Zertifikaten der Generation 2 die Prüfung der Gültigkeit vornehmen, d. h. die Gültigkeit des CV-Zertifikats gemäß Tabelle TAB_PKI_909 prüfen.

[<=]

Tabelle : Tab_PKI_909 Gültigkeit eines CV-Zertifikats der Generation 2

Gültigkeit eines CV-Zertifikats <i>C</i>
Ein CV-Zertifikat einer CVC-Root-CA ist gültig, wenn <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.
Ein CV-Zertifikat <i>C</i> , das von einem Herausgeber der Generation 2 (TSP-CVC oder CVC-Root-CA) erzeugt wurde, ist gültig, wenn <ul style="list-style-type: none"> das CV-Zertifikat für den öffentlichen Schlüssels des Herausgebers gültig und

- das CV-Zertifikat mathematisch korrekt gebildet ist und
- das Certificate Expiration Date (CXD) des CV-Zertifikats *C* nicht überschritten ist.

In allen anderen Fällen ist das CV-Zertifikat ungültig.

3737

3738

GS-A_5012 - Prüfung von CV-Zertifikaten der Generation 2

3739

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

3740

Prüfung der Gültigkeit des CV-Zertifikats gemäß Schalenmodell vornehmen.

3741

3742

3743

[<=]

3744

9 OCSP-Statusinformation

3745 Dieses Kapitel enthält die Festlegung von Schnittstellen, die durch mehrere Produkttypen
3746 der PKI bereitgestellt werden müssen. Diese Schnittstellen werden in der vorliegenden
3747 Spezifikation beschrieben. Eine wiederholte Darstellung dieser Schnittstellen in den
3748 Spezifikationen der Produkttypen erfolgt nicht, vielmehr wird in diesen Dokumenten auf
3749 die folgenden Beschreibungen verwiesen.

3750 9.1 Statusprüfung

3751 Gemäß [gemKPT_Arch_TIP] ist zur Statusprüfung die Schnittstelle
3752 I_OCSP_Status_Information durch die Produkttypen

- 3753 • TSL-Dienst,
- 3754 • gematik Root-CA
- 3755 • TSP-X.509 nonQES,
- 3756 • TSP-X.509 QES und
- 3757 • OCSP-Responder Proxy

3758 anzubieten. Darüber können Nutzer, wie z. B. Konnektor und VPN-Zugangsdienst,
3759 Statusinformationen zu X.509-Zertifikaten von OCSP-Respondern erhalten. Die
3760 Schnittstelle implementiert die logische Operation check_Revocation_Status mit der der
3761 Sperrstatus eines X.509-Zertifikats ermittelt werden kann (vgl. auch
3762 [gemKPT_PKI_TIP]).

3763 **GS-A_4669 - Umsetzung Statusprüfdienst**

3764 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES, TSP-X.509 QES und
3765 OCSP-Responder Proxy MÜSSEN die Schnittstelle I_OCSP_Status_Information
3766 implementieren.
3767 [**<=**]

3768 Die Algorithmen und Parameter für die Erstellung der Signaturen über die OCSP-
3769 Responses des OCSP werden in [gemSpec_Krypt] festgelegt. Die Statusprüfung von QES-
3770 CA-Zertifikaten erfolgt durch die Prüfung des Vorkommens des Zertifikats in der BNetzA-
3771 VL und des Dienststatus (Servicestatus) der QES-CA in der TSL und BNetzA_VL (s. Kap.
3772 8.5).

3773 9.1.1 Schnittstelle I_OCSP_Status_Information

3774 **GS-A_4670 - Statusprüfdienst über Gültigkeitszeitraum des X.509-Zertifikats**

3775 Die Produkttypen TSL-Dienst, gematik Root-CA und TSP-X.509 nonQES MÜSSEN den
3776 Statusprüfdienst über den gesamten Gültigkeitszeitraum des zu prüfenden Zertifikats
3777 sicherstellen. Darüber hinausgehende Anforderungen an die Verfügbarkeit von
3778 Statusinformationen MÜSSEN in der Policy des Zertifikats herausgebers definiert sein.
3779 [**<=**]

3780 Die gematik Root-CA sowie TSP-X.509 nonQES können Dritte mit der Bereitstellung des
3781 Statusprüfdienstes beauftragen.

GS-A_4672 - Statusprüfdienst QES gemäß den Vorgaben von eIDAS

Der TSP-X.509 QES MUSS für den Statusprüfdienst die Vorgaben gemäß [eIDAS] erfüllen.
[<=]

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 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 Erweiterungen in [Common-PKI].

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.

3824 **GS-A_4674 - OCSP-Requests gemäß [RFC2560] und [Common-PKI]**

3825 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES
3826 MÜSSEN OCSP-Requests gemäß [RFC2560] und [Common-PKI] verarbeiten können.
3827 [\leq]

3828 **GS-A_4957 - Beschränkungen OCSP-Request**

3829 Komponenten (Produkttypen der TI, aAdG und aAdG-NetG-TI), die Zertifikate prüfen,
3830 DÜRFEN (abweichend von [RFC2560]) je OCSP-Request NICHT mehr als den Status für
3831 genau ein Zertifikat abfragen. Ist hierbei die Verwendung der OCSP-Extension „Nonce“
3832 zulässig, DARF diese die Länge von 256 Bit NICHT überschreiten.
3833 [\leq]

3834 **WA-A_2033 - Nutzung der OCSP-Responder der TI**

3835 Eine aAdG oder aAdG-NetG-TI MUSS die OCSP-Responder der TI nutzen. [\leq]

3836 *9.1.1.1.2 OCSP-Response*

3837 Die OCSP-Response ist komplett in [RFC2560] beschrieben, sowie mit Erweiterungen in
3838 [Common-PKI].

3839 Wesentlicher Inhalt ist der Status des angefragten Zertifikats, sowie zeitliches Aussagen
3840 zu dem gelieferten Status und dessen Aktualität. Die Antwort ist signiert. Weitere Details
3841 siehe Abschnitt 9.1.2.2 und folgende.

3842 **GS-A_4675 - OCSP-Responses gemäß [RFC2560]**

3843 Der TSP-X.509 nonQES (eGK) MUSS für Statusauskünfte zu X.509-Zertifikaten OCSP-
3844 Responses gemäß [RFC2560] erzeugen.

3845
3846 [\leq]

3847 **GS-A_4676 - OCSP-Responses gemäß [Common-PKI]**

3848 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES (außer eGK) und
3849 TSP-X.509 QES MÜSSEN für Statusauskünfte zu X.509-Zertifikaten OCSP-Responses
3850 gemäß [Common-PKI] erzeugen.

3851
3852
3853 [\leq]

3854 **GS-A_5124 - OCSP-Responses mit Parameter Nonce [Common-PKI]**

3855 Der TSP-X.509 QES MUSS für Statusauskünfte zu X.509-Zertifikaten den Parameter
3856 „Nonce“ für OCSP-Responses gemäß [Common-PKI] unterstützen.
3857 [\leq]

3858 **9.1.1.2 Umsetzung**

3859 **GS-A_4677 - Spezifikationskonforme OCSP-Responses**

3860 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 QES und TSP-X.509 nonQES
3861 MÜSSEN sicherstellen, dass ihr OCSP-Responder spezifikationskonform antwortet, wenn
3862 der OCSP-Request „well formed“ spezifikationskonform formuliert ist und der Responder
3863 für diesen Service konfiguriert ist.
3864 [\leq]

3865 **GS-A_4678 - Signierte OCSP-Responses**

3866 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 QES und TSP-X.509 nonQES
3867 MÜSSEN sicherstellen, dass ihr OCSP-Responder alle Antworten (Responses) mit
3868 Response-Status 'successful' (0) digital signiert.
3869 [\leq]

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]).

Weiterhin müssen Produkttypen der TI, die OCSP-Responses auswerten, sicherstellen, dass für jede mögliche Ausprägung der zurückgegebenen Parameter eine geordnete Reaktion implementiert wird (vgl. [gemKPT_PKI_TIP#TIP1-A_2149]).

9.1.2 Artefakte

9.1.2.1 OCSP-Response – Response Status

GS-A_4686 - Statusprüfdienst – Response Status

Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN sicherstellen, dass für den Response Status die Werte „successful“, „malformedRequest“, „internalError“, „tryLater“ und „unauthorized“ gemäß Tab_PKI_291 unterstützt werden.

[<=]

Tabelle 101: 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

3912

3913 **GS-A_4687 - Statusprüfdienst – Response Status sigRequired**

3914 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES
3915 MÜSSEN sicherstellen, dass für den Response Status der Wert „sigRequired“ nicht
3916 verwendet wird.

3917 [\leq]

3918 Mit dem Response Status „sigRequired“ fordert der OCSP-Responder explizit, dass die
3919 Anfrage vom OCSP-Client signiert werden muss. Da keine signierten OCSP-Requests in
3920 der TI gefordert sind, darf der Exception Case „sigRequired“ vom OCSP-Responder nicht
3921 verwendet werden.

3922 **9.1.2.2 OCSP-Response - Zeiten**

3923 **GS-A_4688 - Statusprüfdienst – Angabe von Zeitpunkten**

3924 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES
3925 MÜSSEN sicherstellen, dass die Angabe zu den Zeitpunkten `producedAt`, `thisUpdate` und
3926 `nextUpdate` spezifikationskonform gemäß Tab_PKI_292 erfolgt.

3927 [\leq]

3928

3929 **Tabelle 102: 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.

3930 Der Zeitpunkt `nextUpdate` ist nur für OCSP-Antworten sinnvoll, die auf CRLs basieren.

3931

3932 **GS-A_4689 - Statusprüfdienst – Zeitquelle von producedAt**

3933 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES
3934 MÜSSEN sicherstellen, dass der Zeitpunkt `producedAt` auf einer in der TI verbindlichen
3935 Zeitquelle beruht.

3936 [\leq]

GS-A_5215 - Festlegung der zeitlichen Toleranzen in einer OCSP-Response

Produkttypen der TI, die Zertifikate prüfen, MÜSSEN die Angaben zu den Zeitpunkten `producedAt`, `thisUpdate` und `nextUpdate` in der OCSP-Response mit einer Zeit-Toleranz bezüglich der lokalen Systemzeit interpretieren.

Produkttypen der TI, die Zertifikate prüfen, MÜSSEN die folgenden Fälle als gültig akzeptieren, wenn im Rahmen von TUC_PKI_006 eine Online-Abfrage durchgeführt wird:

(a) `producedAt` liegt weniger als (oder ist gleich wie) die Toleranz `t'` gegenüber der Systemzeit bei Erhalt der Response in der Vergangenheit.

(b) `producedAt` liegt weniger als (oder ist gleich wie) die Toleranz `t'` gegenüber der Systemzeit bei Erhalt der Response in der Zukunft.

(c) `thisUpdate` liegt weniger als (oder ist gleich wie) die Toleranz `t'` gegenüber der Systemzeit bei Erhalt der Response in der Zukunft.

(d) `nextUpdate` liegt weniger als (oder ist gleich wie) die Toleranz `t'` gegenüber der Systemzeit bei Erhalt der Response in der Vergangenheit.

Produkttypen der TI, die Zertifikate prüfen, MÜSSEN die Toleranz `t'` auf genau 37,5 Sekunden ansetzen.

[<=]

Hinweis: Das in der Anforderung spezifizierte Verhalten weicht von den Empfehlungen von [RFC2560] / [RFC6960] Kap. 4.2.2.1 zur Prüfung von `thisUpdate` und `nextUpdate` ab.

Das Setzen von Zeittoleranzen (mindestens bezüglich `nextUpdate`) wird aber in [RFC5019], Kap. 4 besprochen: „[...] Clients MAY allow configuration of a small tolerance period for acceptance of responses after `nextUpdate` to handle minor clock differences relative to responders and caches. This tolerance period should be chosen based on the accuracy and precision of time synchronization technology available to the calling application environment. [...]“

9.1.2.3 OCSP-Response - CertStatus

GS-A_4690 - Statusprüfdienst – Status des X.509-Zertifikats

Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN sicherstellen, dass ein OCSP-Responder den Status eines Zertifikats mit einem der drei Werte a) good, b) revoked, c) unknown gemäß Tab_PKI_293 zurückgibt.

[<=]

Tabelle 103: Tab_PKI_293 Status der OCSP Antworten

OCSP Antwort	Bedeutung
good	Der Zustand „good“ sagt aus, dass zum Zeitpunkt <code>thisUpdate</code> 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.

3972 **9.1.2.4 OCSP-Response - CertID**

3973 **GS-A_4691 - Statusprüfdienst – X.509-Zertifikat mit Status „unknown“**

3974 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES
3975 MÜSSEN sicherstellen, dass im Falle eines `certStatus` mit Wert „unknown“ im Feld
3976 `certID` der Struktur `SingleResponse` der Inhalt des `certID`-Feldes in der Struktur
3977 `Request` des OCSP-Requests wiederholt wird.
3978 [`<=`]

3979 **9.1.2.5 OCSP-Response – Sperrzeitpunkt und Sperrgrund**

3980 **GS-A_4692 - Statusprüfdienst – Angabe Sperrzeitpunkt**

3981 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES
3982 MÜSSEN sicherstellen, dass im Falle eines gesperrten X.509-Zertifikats die Angabe des
3983 Sperrzeitpunkts im Teilfeld `revocationTime` in einer OCSP-Response erfolgt.
3984 [`<=`]

3985 **GS-A_5090 - Statusprüfdienst – Keine Angabe von Sperrgründen**

3986 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES
3987 SOLLEN sicherstellen, dass kein Sperrgrund mit der OCSP-Response geliefert wird.
3988 [`<=`]

3989 **9.1.2.6 OCSP-Response – CertHash**

3990 **GS-A_4693 - Statusprüfdienst – Positive Statement**

3991 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES (außer nonQES-
3992 Zertifikaten einer eGK) und TSP-X.509 QES MÜSSEN sicherstellen, dass die von ihnen
3993 betriebenen OCSP-Responder bei OCSP-Antworten immer die private `SingleExtension`
3994 „`certHash`“ [CommonPKI#Part 4, Kapitel 3.1.2] in der OCSP-Response des zu prüfenden
3995 X.509-Zertifikats mitsenden. [`<=`]

3996 **9.1.3 Testunterstützung**

3997 Bei der PKI für X.509-Zertifikate wird zwischen einer Produktiv-PKI und einer Test-PKI
3998 unterschieden.

3999 **GS-A_4694 - Betrieb von OCSP-Responder für Test-PKI-CAs**

4000 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 QES und TSP-X.509 nonQES
4001 MÜSSEN neben OCSP-Respondern für die produktive PKI ebenfalls OCSP-Responder für
4002 die Test-PKI betreiben.
4003 [`<=`]

4004 **9.1.4 Hardwaremerkmale**

4005 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 104: 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> (<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)	1	

	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}	1	FALSE
		professionItem = Beschreibung zu <oid_zahnarztpraxis> gemäß [gemSpec_OID#GS-A_4443]	1	
		professionOID = OID <oid_zahnarztpraxis> gemäß [gemSpec_OID#GS-A_4443]	1	
		registrationNumber = <Telematik-ID gemäss Freigabedaten der zuständigen KZV>	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		

4021

4022

4023 *) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung
4024 ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und
4025 Tab_PKI_240 ist die Kardinalität gleich 0.

4026

4027 Hinweis: In einer früheren Version der vorliegenden Spezifikation war an dieser Stelle
4028 das SMC-B-ORG-Profil des Sektors KZBV zu finden in Form der Tabelle
4029 "Tab_SMCB_KZBV_KZV SMC-B-Zertifikate für KZV (Sektor KZBV)". Dieses Profil ist nun
4030 fachlich unverändert in Kapitel 10.7 mittels der Tabelle "Tab_SMCB_ORG_Gen -
4031 Generisches Zertifikatsprofil" beschrieben.

4032 10.2 KBV

4033 Die nachfolgende Profiltabelle der durch die KBV betreuten Sektoren gilt für die
4034 Sektoren:

- 4035 • Niedergelassene Vertragsärzte (KV)
- 4036 • Niedergelassene Psychologische Psychotherapeuten (KV)
- 4037 • Niedergelassene Kinder- und Jugendlichenpsychotherapeuten (KV)

4038

4039 **Tabelle 105: 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	1	

			„Kurzname“ der Institution, so wie für das Adressfeld definiert.		
		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-Adresse 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 106: 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	signature	siehe Kap 5.3.4		
		issuer	siehe Kap 5.3.4		
		validity	siehe Kap 5.3.4		
		subject			
	commonName	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}	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 107: 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.

Tabelle 108: 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_GKVSV	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 109: Tab_SMCB_TID_GKVSV Aufbau Telematik-ID in SMC-B-Zertifikaten des
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

4070 **10.5 Apothekerschaft**

4071 **Tabelle 110: Tab_SMCB_BAK SMC-B-Zertifikate für Apotheker**

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	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	Familiennamen 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.

4076 **Tabelle 111: Tab_SMCB_TID_BAK Aufbau Telematik-ID in SMC-B-Zertifikaten der**
4077 **Apotheker**

Präfix	Separator	Fortsatz	Weiterer Fortsatz
3 (Apothekerschaft)	-	2 (SMC)	gem. Freigabedaten der Apothekerkammer

4078

4079 **10.6 AdV-Umgebung im Auftrag der Kostenträger**

4080 **Tabelle 112: Tab_SMCB_ADV_KTR SMC-B-Zertifikate für die AdV-Umgebung im Auftrag**
4081 **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		
	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}	nicht belegt	0	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_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	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			

4082

4083 10.7 SMC-B-ORG

4084 Die nachfolgende Profiltabelle gilt für die Zertifikate der SMC-B-ORG und kann als
4085 generisches Zertifikatsprofil von verschiedenen Organisationen zur Herausgabe einer
4086 SMC-B-ORG verwendet werden.

4087 Herausgeberspezifische Ausprägungen zu einzelnen Zertifikatsfeldern sind in der Tabelle
4088 Tab_SMCB_ORG_Herausgeber im Dokument [gemRL_SMC-B_ORG_BP] beschrieben.

4089 **Tabelle 113: 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 [gemRL_SMC-B_ORG_BP#Tab_SMCB_ORG_Herausgeber])	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		
--	-----------	------------------	--	--

- 4090 *) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung
4091 ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und
4092 Tab_PKI_240 ist die Kardinalität gleich 0.
- 4093 Die Verantwortung für die Herausgabe der SMC-B ORG als spezielle Form der SMC-B für
4094 Gesellschafterorganisationen ist im gesonderten Dokument [gemRL_SMC-B_ORG_BP] beschrieben.
- 4095 Die in der Vergangenheit hier gepflegte Tabelle „Tab_SMCB_ORG_Herausgeber -
4096 Herausgeberspezifische Felder im SMC-B-ORG Profil“ finden Sie fortan im Dokument „gemRL_SMC-
4097 B_ORG_BP“ (Berechtigungs-Policy).

4098

11 Anhang B – Verzeichnisse

4099

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

4100 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, für den das Zertifikat auf Gültigkeit geprüft wird und für den die Statusinformationen eingeholt werden. Dabei kann es sich um die aktuelle Systemzeit handeln (z.B. bei TLS-Verbindungsaufbau). Der Referenzzeitpunkt kann auch in der Vergangenheit liegen (z.B. Signaturzeitpunkt bei QES).

4101 Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung
4102 gestellt.

4103 11.3 Abbildungsverzeichnis

4104	Abbildung 1: Betriebsumgebungen aus Sicht der PKI.....	30
4105	Abbildung 2: Aufbau der Krankenversichertennummer.....	35
4106	Abbildung 3: Pseudonym Kodierung in X.509 Versichertenzertifikaten.....	38
4107	Abbildung 4: Das Anschriftenfeld nach DIN5008	77
4108	Abbildung 5: Use Case Diagramm „Prozesse zur Nutzung des TI Vertrauensraums“ ...	157
4109	Abbildung 6 : Aufbau der TSL.....	159

4110	Abbildung 7: Aktivitätsdiagramm TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“	170
4111		
4112	Abbildung 8: Aktivitätsdiagramm TUC_PKI_013 „Import neuer TI-Vertrauensanker“ ..	175
4113	Abbildung 9: Aktivitätsdiagramm TUC_PKI_017 „Lokalisierung Download-Adresse“	180
4114	Abbildung 10: Aktivitätsdiagramm TUC_PKI_016 „Download der TSL-Datei“	183
4115	Abbildung 11: Aktivitätsdiagramm TUC_PKI_019 „Prüfung der Aktualität der TSL“	190
4116	Abbildung 12: Aktivitätsdiagramm TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“	196
4117		
4118	Abbildung 13: Use Case Diagramm „Zertifikatsprüfung“	199
4119	Abbildung 14: Aktivitätsdiagramm TUC_PKI_018 „Zertifikatsprüfung“	207
4120	Abbildung 15: Aktivitätsdiagramm TUC_PKI_002 Gültigkeitsprüfung des Zertifikats ...	210
4121	Abbildung 16: Aktivitätsdiagramm TUC_PKI_003 CA-Zertifikat in TSL-Informationen finden.....	212
4122		
4123	Abbildung 17: Aktivitätsdiagramm TUC_PKI_004 Mathematische Prüfung der Zertifikatssignatur.....	215
4124		
4125	Abbildung 18: Aktivitätsdiagramm TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln“	218
4126		
4127	Abbildung 19: Aktivitätsdiagramm TUC_PKI_006 „OCSP-Abfrage“	226
4128	Abbildung 20: Aktivitätsdiagramm TUC_PKI_021 „CRL-Prüfung“	231
4129	Abbildung 21: Aktivitätsdiagramm TUC_PKI_009 „Rollenermittlung“	234
4130	Abbildung 22: Aktivitätsdiagramm TUC_PKI_007 „Prüfung Zertifikatstyp“	240
4131	Abbildung 1: Betriebsumgebungen aus Sicht der PKI.....	30
4132	Abbildung 2: Aufbau der Krankenversichertennummer.....	35
4133	Abbildung 3: Pseudonym Kodierung in X.509-Versichertenzertifikaten.....	38
4134	Abbildung 4: Das Anschriftenfeld nach DIN5008	77
4135	Abbildung 5: Use Case Diagramm „Prozesse zur Nutzung des TI-Vertrauensraums“ ...	157
4136	Abbildung 6 : Aufbau der TSL.....	159
4137	Abbildung 7: Aktivitätsdiagramm TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“	170
4138		
4139	Abbildung 8: Aktivitätsdiagramm TUC_PKI_013 „Import neuer TI-Vertrauensanker“ ..	175
4140	Abbildung 9: Aktivitätsdiagramm TUC_PKI_017 „Lokalisierung Download-Adresse“	180
4141	Abbildung 10: Aktivitätsdiagramm TUC_PKI_016 „Download der TSL-Datei“	183
4142	Abbildung 11: Aktivitätsdiagramm TUC_PKI_019 „Prüfung der Aktualität der TSL“	190
4143	Abbildung 12: Aktivitätsdiagramm TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“	196
4144		
4145	Abbildung 13: Use Case Diagramm „Zertifikatsprüfung“	199
4146	Abbildung 14: Aktivitätsdiagramm TUC_PKI_018 „Zertifikatsprüfung“	207
4147	Abbildung 15: Aktivitätsdiagramm TUC_PKI_002 Gültigkeitsprüfung des Zertifikats ...	210

4148	Abbildung 16: Aktivitätsdiagramm TUC_PKI_003 CA-Zertifikat in TSL-Informationen	
4149	finden.....	212
4150	Abbildung 17: Aktivitätsdiagramm TUC_PKI_004 Mathematische Prüfung der	
4151	Zertifikatssignatur	215
4152	Abbildung 18: Aktivitätsdiagramm TUC_PKI_005 „Adresse für Status- und Sperrprüfung	
4153	ermitteln“	218
4154	Abbildung 19: Aktivitätsdiagramm TUC_PKI_006 „OCSP-Abfrage“	226
4155	Abbildung 20: Aktivitätsdiagramm TUC_PKI_021 „CRL-Prüfung“	231
4156	Abbildung 21: Aktivitätsdiagramm TUC_PKI_009 „Rollenermittlung“	234
4157	Abbildung 22: Aktivitätsdiagramm TUC_PKI_007 „Prüfung Zertifikatstyp“	240
4158		

4159 11.4 Tabellenverzeichnis

4160	Tabelle 1: Tab_PKI_201 Allgemeine Notationsvorschrift für kryptographische Objekte..	20
4161	Tabelle 2: Tab_PKI_202: Notationsvorgaben für Objekttyp.....	20
4162	Tabelle 3: Tab_PKI_203 Notationsvorgaben für Objektbesitzer	21
4163	Tabelle 4: Tab_PKI_204 Notationsvorgaben für Objektverwendung	23
4164	Tabelle 5: Tab_PKI_205 Notationsvorgaben für Ausprägung	25
4165	Tabelle 6: Tab_PKI_206 Beispiele für asymmetrische Objekte.....	26
4166	Tabelle 7: Tab_PKI_207 Beispiele für symmetrische Objekte	27
4167	Tabelle 8: Tab_PKI_213 Erlaubte Werte für <usage> und <usageName>	32
4168	Tabelle 9: Tab_PKI_221 Berufsgruppenkennzeichnung	39
4169	Tabelle 10: Tab_PKI_222 Institutionstypkennzeichnung.....	40
4170	Tabelle 11: Tab_PKI_230 Kennzeichnung Technische Rolle.....	41
4171	Tabelle 12: Tab_PKI_224 Telematik ID Kennzeichnung	42
4172	Tabelle 13: Tab_PKI_223 Aufbau der Telematik ID	42
4173	Tabelle 14: Tab_PKI_101 Normative Festlegung für das Präfix der Telematik ID.....	42
4174	Tabelle 15: Tab_PKI_229 Kodierung der Attribute in X.509 Zertifikaten	44
4175	Tabelle 16: Tab_PKI_109 Werte für das Präfix <TSP ID>	45
4176	Tabelle 17: Tab_PKI_226 Struktur Admission	46
4177	Tabelle 18: Tab_PKI_227 Struktur CertificatePolicies	48
4178	Tabelle 19: Tab_PKI_228 Struktur SubjectAltName	50
4179	Tabelle 20: Common Name (CN) der End-Entity Zertifikate Test-PKI	55
4180	Tabelle 21: Tab_PKI_231 Personennamen im subjectDN	59
4181	Tabelle 22: Tab_PKI_232 C.CH.AUT und C.CH.AUT_ALT Authentisierung eGK	60
4182	Tabelle 23: Tab_PKI_233 C.CH.ENC Verschlüsselung eGK	61

4183	Tabelle 24: Tab_PKI_234 C.CH.QES Qualifizierte Signatur eGK	63
4184	Tabelle 25: Tab_PKI_235 C.CH.AUTN Technische Authentisierung eGK.....	65
4185	Tabelle 26: Tab_PKI_236 C.CH.ENCV Technische Verschlüsselung eGK	66
4186	Tabelle 27: Tab_PKI_268_1 C.HP.AUT Authentisierung HBA	68
4187	Tabelle 281: Tab_PKI_269_1 C.HP.ENC Verschlüsselung HBA	70
4188	Tabelle 29: Tab_PKI_270_1 C.HP.QES Qualifizierte Signatur HBA.....	72
4189	Tabelle 30: Tab_PKI_238 C.HCI.AUT Authentisierung SMC-B	78
4190	Tabelle 31: Tab_PKI_239 C.HCI.ENC Verschlüsselung SMC-B	80
4191	Tabelle 32: Tab_PKI_240 C.HCI.OSIG Signatur SMC-B	82
4192	Tabelle 33: Tab_PKI_241 C.SMKT.AUT gSMC-KT.....	85
4193	Tabelle 34: Tab_PKI_237 Statusprüfung von Konnektorzertifikaten	87
4194	Tabelle 35: Tab_PKI_242 Zertifikatsprofil C.NK.VPN VPN-Authentisierung Netzkonnektor	
4195	88
4196	Tabelle 36: Tab_PKI_243 Zertifikatsprofil C.AK.AUT Authentisierung	
4197	Anwendungskonnektor.....	90
4198	Tabelle 37: Tab_PKI_244 Zertifikatsprofil C.SAK.AUT Authentisierung SAK	92
4199	Tabelle 38: Tab_PKI_245 Zertifikatsprofil C.VPNK.VPN VPN-Authentisierung	
4200	Zugangsdienst TI	94
4201	Tabelle 39: Tab_PKI_265 Zertifikatsprofil C.VPNK.VPN-SIS VPN-Authentisierung	
4202	Zugangsdienst Sicherer Internetzugang.....	96
4203	Tabelle 40: Tab_PKI_247 C.ZD.TLS-S Server Authentisierung Zentrale Dienste.....	98
4204	Tabelle 41: Tab_PKI_249 C.FD.TLS-C Client Authentisierung Fachanwendungsspezifische	
4205	Dienste.....	100
4206	Tabelle 42: Tab_PKI_250 C.FD.TLS-S Server Authentisierung	
4207	Fachanwendungsspezifische Dienste	102
4208	Tabelle 43: Tab_PKI_251 C.FD.SIG Signatur fachanwendungsspezifische Dienste.....	104
4209	Tabelle 44: Tab_PKI_275 C.FD.AUT Authentisierung fachanwendungsspezifische	
4210	Dienste.....	105
4211	Tabelle 45: Tab_PKI_276 C.FD.ENC Verschlüsselung fachanwendungsspezifische Dienste	
4212	107
4213	Tabelle 46: Tab_PKI_267 C.CM.TLS-CS Clientmodul Authentisierung.....	109
4214	Tabelle 47: Tab_PKI_296 C.SGD-HSM.AUT Authentisierung SGD-HSM	111
4215	Tabelle 48: Tab_PKI_211 GEM.R-CA<n>—Zentrale gematik-Root-CA_nonQES der TI	114
4216	Tabelle 49: Tab_PKI_212 <tsp>.<usage>-CA<n>—Aussteller-CA_nonQES der TI....	115
4217	Tabelle 50: Tab_PKI_253 C.GEM.OCSP Zertifikatsprofil OCSP-Signer	119
4218	Tabelle 51: Tab_PKI_214 C.GEM.CRL Zertifikatsprofil CRL-Signer.....	122
4219	Tabelle 52: Tab_PKI_252_01 C.TSL.SIG Zertifikatsprofil TSL-Signer.....	125
4220	Tabelle 53: Tab_PKI_254 Zugriffsprofile für eine Rollenauthentisierung.....	129

4221	Tabelle 54: Tab_PKI_255 Zugriffsprofile G2 für eine Authentisierung einer	
4222	Funktionseinheit.....	134
4223	Tabelle 55: Tab_PKI_266 Aufbau CAR für Karten der Generation 2.....	137
4224	Tabelle 56: Tab_PKI_901 Objektidentifizier des öffentlichen Schlüssels eines CV-Zertifikats	
4225	der Generation 2.....	138
4226	Tabelle 57: Tab_PKI_902 Punkt Q des öffentlichen Schlüssels eines CV-Zertifikats der	
4227	Generation 2.....	139
4228	Tabelle 58: Tab_PKI_258 Aufbau CHR.....	140
4229	Tabelle 59: Tab_PKI_904 Mögliche Objektidentifizier OID_{flags} in Certificate Holder	
4230	Authorization Templates.....	141
4231	Tabelle 60: Tab_PKI_905 Zu signierende Nachricht M eines CV-Zertifikats.....	143
4232	Tabelle 61: Tab_PKI_906 Signatur der Nachricht M eines CV-Zertifikats.....	143
4233	Tabelle 62: Tab_PKI_907 Struktur und Inhalt eines CV-Zertifikats.....	144
4234	Tabelle 63: Tab_PKI_912 CA CV-Zertifikate für 256-bit ELC-Schlüssel, insgesamt	
4235	220 Oktett.....	144
4236	Tabelle 64: Tab_PKI_913 CA CV-Zertifikate für 384-bit ELC-Schlüssel, insgesamt	
4237	285 Oktett.....	145
4238	Tabelle 65: Tab_PKI_914 CA CV-Zertifikate für 512-bit ELC-Schlüssel, insgesamt	
4239	352 Oktett.....	145
4240	Tabelle 66: Tab_PKI_937 Cross-CV-Zertifikat für ELC-Schlüssel.....	146
4241	Tabelle 67: Tab_PKI_915 Endnutzer CV-Zertifikate für 256-bit ELC-Schlüssel, insgesamt	
4242	222 Oktett.....	147
4243	Tabelle 68: Tab_PKI_916 Endnutzer CV-Zertifikate für 384-bit ELC-Schlüssel, insgesamt	
4244	287 Oktett.....	148
4245	Tabelle 69: Tab_PKI_917 Endnutzer CV-Zertifikate für 512-bit ELC-Schlüssel, insgesamt	
4246	354 Oktett.....	148
4247	Tabelle 70: Tab_PKI_910 TI-PKI, Bedeutung der Bits innerhalb der Flagliste eines CHAT	
4248	149
4249	Tabelle 71: Tab_PKI_918 Abbildung von Rollenberechtigungen Zugriffsprofilen auf	
4250	äquivalente Flaglisten.....	151
4251	Tabelle 72: Tab_PKI_919 Sub-CA-Flaglisten nach Kartentyp (G2) und Zugriffsprofilen.....	153
4252	Tabelle 73: Tab_PKI_911 CMS-PKI, Bedeutung der Bits innerhalb der Flagliste eines	
4253	CHAT.....	154
4254	Tabelle 74: Tab_PKI_271 Erlaubte URIs als Inhalte des TSL-Elements ServiceStatus..	163
4255	Tabelle 75: TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“.....	164
4256	Tabelle 76: TUC_PKI_013 „Import neuer TI-Vertrauensanker“.....	171
4257	Tabelle 77: Gültige Werte für den TI-Vertrauensankerwechsel.....	177
4258	Tabelle 78: Beispiel für den TSL-Eintrag zum Wechsel des TSL-Signer-CA-Zertifikats.....	177
4259	Tabelle 79: TUC_PKI_017 „Lokalisierung Download-Adressen“.....	178
4260	Tabelle 80: Tab_PKI_272 Gültige Werte zur Download-Adresse.....	180

4261	Tabelle 81: TUC_PKI_016 „Download der TSL-Datei“	181
4262	Tabelle 82: TUC_PKI_019 „Prüfung der Aktualität der TSL“	185
4263	Tabelle 83: TUC_PKI_020 „XML-Dokument validieren“	191
4264	Tabelle 84: TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“	192
4265	Tabelle 85: TUC_PKI_012 „XML-Signatur-Prüfung“	196
4266	Tabelle 86: Tab_PKI_294 TSL-Zeitparameter	198
4267	Tabelle 87: TUC_PKI_018 „Zertifikatsprüfung in der TI“	200
4268	Tabelle 88: TUC_PKI_002 „Gültigkeitsprüfung des Zertifikats“	208
4269	Tabelle 89: TUC_PKI_003 „CA-Zertifikat in TSL-Informationen finden“	210
4270	Tabelle 90: TUC_PKI_004 „Mathematische Prüfung der Zertifikatssignatur“	213
4271	Tabelle 91: TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln“	216
4272	Tabelle 92: TUC_PKI_006 „OCSP-Abfrage“	218
4273	Tabelle 93: TUC_PKI_021 „CRL-Prüfung“	226
4274	Tabelle 94: TUC_PKI_009 „Rollenermittlung“	232
4275	Tabelle 95: TUC_PKI_007 „Prüfung Zertifikatstyp“	235
4276	Tabelle 96: Tab_PKI_273 Prüfparameter für TLS-Aufbau	240
4277	Tabelle 97: TUC_PKI_030 „QES-Zertifikatsprüfung“	242
4278	Tabelle 98: TUC_PKI_036 „BNetzA-VL-Aktualisierung“	247
4279	Tabelle 99: Tab_PKI_274 Fehlercodes des SubCompTyps PKI bei TSL- und	
4280	Zertifikatsprüfung	251
4281	Tabelle 100: Tab_PKI_908 Prüfung der Signatur eines CV-Zertifikats der Generation 2	
4282	mit Hilfe des CV-Zertifikats des Herausgebers	260
4283	Tabelle 101: Tab_PKI_291 OCSP-Response-Status-Ergebnisse	265
4284	Tabelle 102: Tab_PKI_292 Zeiten in einer OCSP-Response	266
4285	Tabelle 103: Tab_PKI_293 Status der OCSP-Antworten	267
4286	Tabelle 104: Tab_SMCB_KZBV_ZA SMC-B-Zertifikate für Zahnarzt (Sektor KZBV)	269
4287	Tabelle 105: Tab_SMCB_KV-T SMC-B-Zertifikate für Sektoren der KBV	271
4288	Tabelle 106: Tab_SMCB_DKTIG SMC-B-Zertifikate für Sektor der DKTIG	273
4289	Tabelle 107: Tab_SMCB_TID_DKTIG Aufbau Telematik-ID in SMC-B-Zertifikaten der	
4290	DKTIG	275
4291	Tabelle 108: Tab_SMCB_KTR SMC-B-Zertifikate für Mitarbeiter Kostenträger	275
4292	Tabelle 109: Tab_SMCB_TID_GKVSV Aufbau Telematik-ID in SMC-B-Zertifikaten des	
4293	GKV-SV	277
4294	Tabelle 110: Tab_SMCB_BAK SMC-B-Zertifikate für Apotheker	278
4295	Tabelle 111: Tab_SMCB_TID_BAK Aufbau Telematik-ID in SMC-B-Zertifikaten der	
4296	Apotheker	280
4297	Tabelle 112: Tab_SMCB_ADV_KTR SMC-B-Zertifikate für die Adv-Umgebung im Auftrag	
4298	der Kostenträger	280

4299	Tabelle 113: Tab_SMCB_ORG_Gen – Generisches Zertifikatsprofil für die SMC-B-ORG	282
4300	Tabelle 114: Tab_HBA_BÄK HBA-Zertifikate (AUT, ENC, QES) für BÄK	305
4301	Tabelle 115: Tab_HBA_BZÄK HBA-Zertifikate (AUT, ENC, QES) für BZÄK	307
4302	Tabelle 116: Tab_HBA_BPtK HBA-Zertifikate (AUT, ENC, QES) für BPtK	309
4303	Tabelle 117: Tab_HBA_BAK HBA-Zertifikate (AUT, ENC, QES) für Apotheker	311
4304	Tabelle 1: Tab_PKI_201 Allgemeine Notationsvorschrift für kryptographische Objekte ..	20
4305	Tabelle 2: Tab_PKI_202: Notationsvorgaben für Objekttyp	20
4306	Tabelle 3: Tab_PKI_203 Notationsvorgaben für Objektbesitzer	21
4307	Tabelle 4: Tab_PKI_204 Notationsvorgaben für Objektverwendung	23
4308	Tabelle 5: Tab_PKI_205 Notationsvorgaben für Ausprägung	25
4309	Tabelle 6: Tab_PKI_206 Beispiele für asymmetrische Objekte	26
4310	Tabelle 7: Tab_PKI_207 Beispiele für symmetrische Objekte	27
4311	Tabelle 8: Tab_PKI_213 Erlaubte Werte für <usage> und <usageName>	32
4312	Tabelle 9: Tab_PKI_221 Berufsgruppenkennzeichnung	39
4313	Tabelle 10: Tab_PKI_222 Institutionstypkennzeichnung	40
4314	Tabelle 11: Tab_PKI_230 Kennzeichnung Technische Rolle	41
4315	Tabelle 12: Tab_PKI_224 Telematik-ID-Kennzeichnung	42
4316	Tabelle 13: Tab_PKI_223 Aufbau der Telematik-ID	42
4317	Tabelle 14: Tab_PKI_101 Normative Festlegung für das Präfix der Telematik-ID	42
4318	Tabelle 15: Tab_PKI_229 Kodierung der Attribute in X.509-Zertifikaten	44
4319	Tabelle 16: Tab_PKI_109 Werte für das Präfix <TSP-ID>	45
4320	Tabelle 17: Tab_PKI_226 Struktur Admission	46
4321	Tabelle 18: Tab_PKI_227 Struktur CertificatePolicies	48
4322	Tabelle 19: Tab_PKI_228 Struktur SubjectAltName	50
4323	Tabelle 20: Common Name (CN) der End-Entity-Zertifikate Test-PKI	55
4324	Tabelle 21: Tab_PKI_231 Personennamen im subjectDN	59
4325	Tabelle 22: Tab_PKI_232 C.CH.AUT und C.CH.AUT_ALT Authentisierung eGK	60
4326	Tabelle 23: Tab_PKI_233 C.CH.ENC Verschlüsselung eGK	61
4327	Tabelle 24: Tab_PKI_234 C.CH.QES Qualifizierte Signatur eGK	63
4328	Tabelle 25: Tab_PKI_235 C.CH.AUTN Technische Authentisierung eGK	65
4329	Tabelle 26: Tab_PKI_236 C.CH.ENCV Technische Verschlüsselung eGK	66
4330	Tabelle 27: Tab_PKI_268_1 C.HP.AUT Authentisierung HBA	68
4331	Tabelle 281: Tab_PKI_269_1 C.HP.ENC Verschlüsselung HBA	70
4332	Tabelle 29: Tab_PKI_270_1 C.HP.QES Qualifizierte Signatur HBA	72
4333	Tabelle 30: Tab_PKI_238 C.HCI.AUT Authentisierung SMC-B	78
4334	Tabelle 31: Tab_PKI_239 C.HCI.ENC Verschlüsselung SMC-B	80

4335	Tabelle 32: Tab_PKI_240 C.HCI.OSIG Signatur SMC-B	82
4336	Tabelle 33: Tab_PKI_241 C.SMKT.AUT gSMC-KT.....	85
4337	Tabelle 34: Tab_PKI_237 Statusprüfung von Konnektorzertifikaten	87
4338	Tabelle 35: Tab_PKI_242 Zertifikatsprofil C.NK.VPN VPN-Authentisierung Netzkonnektor	
4339	88
4340	Tabelle 36: Tab_PKI_243 Zertifikatsprofil C.AK.AUT Authentisierung	
4341	Anwendungskonnektor.....	90
4342	Tabelle 37: Tab_PKI_244 Zertifikatsprofil C.SAK.AUT Authentisierung SAK	92
4343	Tabelle 38: Tab_PKI_245 Zertifikatsprofil C.VPNK.VPN VPN-Authentisierung	
4344	Zugangsdienst TI	94
4345	Tabelle 39: Tab_PKI_265 Zertifikatsprofil C.VPNK.VPN-SIS VPN-Authentisierung	
4346	Zugangsdienst Sicherer Internetzugang.....	96
4347	Tabelle 40: Tab_PKI_247 C.ZD.TLS-S Server-Authentisierung Zentrale Dienste.....	98
4348	Tabelle 41: Tab_PKI_249 C.FD.TLS-C Client-Authentisierung Fachanwendungsspezifische	
4349	Dienste.....	100
4350	Tabelle 42: Tab_PKI_250 C.FD.TLS-S Server-Authentisierung	
4351	Fachanwendungsspezifische Dienste	102
4352	Tabelle 43: Tab_PKI_251 C.FD.SIG Signatur fachanwendungsspezifische Dienste	104
4353	Tabelle 44: Tab_PKI_275 C.FD.AUT Authentisierung fachanwendungsspezifische	
4354	Dienste.....	105
4355	Tabelle 45: Tab_PKI_276 C.FD.ENC Verschlüsselung fachanwendungsspezifische Dienste	
4356	107
4357	Tabelle 46: Tab_PKI_267 C.CM.TLS-CS Clientmodul-Authentisierung	109
4358	Tabelle 47: Tab_PKI_296 C.SGD-HSM.AUT Authentisierung SGD-HSM	111
4359	Tabelle 48: Tab_PKI_211 GEM.R-CA<n> – Zentrale gematik Root-CA_nonQES der TI	114
4360	Tabelle 49: Tab_PKI_212 <tsp>.<usage>-CA<n> –Aussteller- CA_nonQES der TI	115
4361	Tabelle 50: Tab_PKI_253 C.GEM.OCSP Zertifikatsprofil OCSP-Signer	119
4362	Tabelle 51: Tab_PKI_214 C.GEM.CRL Zertifikatsprofil CRL-Signer.....	122
4363	Tabelle 52: Tab_PKI_252_01 C.TSL.SIG Zertifikatsprofil TSL-Signer	125
4364	Tabelle 53: Tab_PKI_254 Zugriffsprofile für eine Rollenauthentisierung	129
4365	Tabelle 54: Tab_PKI_255 Zugriffsprofile G2 für eine Authentisierung einer	
4366	Funktionseinheit.....	134
4367	Tabelle 55: Tab_PKI_266 Aufbau CAR für Karten der Generation 2	137
4368	Tabelle 56: Tab_PKI_901 Objektidentifizier des öffentlichen Schlüssels eines CV-Zertifikats	
4369	der Generation 2	138
4370	Tabelle 57: Tab_PKI_902 Punkt Q des öffentlichen Schlüssels eines CV-Zertifikats der	
4371	Generation 2	139
4372	Tabelle 58: Tab_PKI_258 Aufbau CHR.....	140
4373	Tabelle 59: Tab_PKI_904 Mögliche Objektidentifizier OID _{flags} in Certificate Holder	
4374	Authorization Templates.....	141

4375	Tabelle 60: Tab_PKI_905 Zu signierende Nachricht M eines CV-Zertifikates	143
4376	Tabelle 61: Tab_PKI_906 Signatur der Nachricht M eines CV-Zertifikats	143
4377	Tabelle 62: Tab_PKI_907 Struktur und Inhalt eines CV-Zertifikat	144
4378	Tabelle 63: Tab_PKI_912 CA CV-Zertifikate für 256 bit ELC-Schlüssel, insgesamt	
4379	220 Oktett	144
4380	Tabelle 64: Tab_PKI_913 CA CV-Zertifikate für 384 bit ELC-Schlüssel, insgesamt	
4381	285 Oktett	145
4382	Tabelle 65: Tab_PKI_914 CA CV-Zertifikate für 512 bit ELC-Schlüssel, insgesamt	
4383	352 Oktett	145
4384	Tabelle 66: Tab_PKI_937 Cross-CV-Zertifikat für ELC-Schlüssel	146
4385	Tabelle 67: Tab_PKI_915 Endnutzer-CV-Zertifikate für 256 bit ELC-Schlüssel, insgesamt	
4386	222 Oktett	147
4387	Tabelle 68: Tab_PKI_916 Endnutzer-CV-Zertifikate für 384 bit ELC-Schlüssel, insgesamt	
4388	287 Oktett	148
4389	Tabelle 69: Tab_PKI_917 Endnutzer-CV-Zertifikate für 512 bit ELC-Schlüssel, insgesamt	
4390	354 Oktett	148
4391	Tabelle 70: Tab_PKI_910 TI-PKI, Bedeutung der Bits innerhalb der Flagliste eines CHAT	
4392	149
4393	Tabelle 71: Tab_PKI_918 Abbildung von Rollenberechtigungen Zugriffsprofilen auf	
4394	äquivalente Flaglisten	151
4395	Tabelle 72: Tab_PKI_919 Sub-CA-Flaglisten nach Kartentyp (G2) und Zugriffsprofilen	153
4396	Tabelle 73: Tab_PKI_911 CMS-PKI, Bedeutung der Bits innerhalb der Flagliste eines	
4397	CHAT.....	154
4398	Tabelle 74: Tab_PKI_271 Erlaubte URIs als Inhalte des TSL-Elements ServiceStatus..	163
4399	Tabelle 75: TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“	164
4400	Tabelle 76: TUC_PKI_013 „Import neuer TI-Vertrauensanker“	171
4401	Tabelle 77: Gültige Werte für den TI-Vertrauensankerwechsel	177
4402	Tabelle 78: Beispiel für den TSL-Eintrag zum Wechsel des TSL-Signer-CA-Zertifikats .	177
4403	Tabelle 79: TUC_PKI_017 „Lokalisierung Download-Adressen“	178
4404	Tabelle 80: Tab_PKI_272 Gültige Werte zur Download-Adresse.....	180
4405	Tabelle 81: TUC_PKI_016 „Download der TSL-Datei“	181
4406	Tabelle 82: TUC_PKI_019 „Prüfung der Aktualität der TSL“	185
4407	Tabelle 83: TUC_PKI_020 „XML-Dokument validieren“	191
4408	Tabelle 84: TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“	192
4409	Tabelle 85: TUC_PKI_012 „XML-Signatur- Prüfung“	196
4410	Tabelle 86: Tab_PKI_294 TSL Zeitparameter.....	198
4411	Tabelle 87: TUC_PKI_018 „Zertifikatsprüfung in der TI“	200
4412	Tabelle 88: TUC_PKI_002 „Gültigkeitsprüfung des Zertifikats“	208
4413	Tabelle 89: TUC_PKI_003 „CA-Zertifikat in TSL-Informationen finden“	210

4414	Tabelle 90: TUC_PKI_004 „Mathematische Prüfung der Zertifikatssignatur“	213
4415	Tabelle 91: TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln“	216
4416	Tabelle 92: TUC_PKI_006 „OCSP-Abfrage“	218
4417	Tabelle 93: TUC_PKI_021 „CRL-Prüfung“	226
4418	Tabelle 94: TUC_PKI_009 „Rollenermittlung“	232
4419	Tabelle 95: TUC_PKI_007 „Prüfung Zertifikatstyp“	235
4420	Tabelle 96: Tab_PKI_273 Prüfparameter für TLS-Aufbau	240
4421	Tabelle 97: TUC_PKI_030 „QES-Zertifikatsprüfung“	242
4422	Tabelle 98: TUC_PKI_036 „BNetzA-VL Aktualisierung“	247
4423	Tabelle 99: Tab_PKI_274 Fehlercodes des SubCompTyps PKI bei TSL- und	
4424	Zertifikatsprüfung	251
4425	Tabelle 100: Tab_PKI_908 Prüfung der Signatur eines CV-Zertifikats der Generation 2	
4426	mit Hilfe des CV-Zertifikats des Herausgebers	260
4427	Tabelle 101: Tab_PKI_291 OCSP-Response Status Ergebnisse	265
4428	Tabelle 102: Tab_PKI_292 Zeiten in einer OCSP-Response	266
4429	Tabelle 103: Tab_PKI_293 Status der OCSP Antworten	267
4430	Tabelle 104: Tab_SMCB_KZBV_ZA SMC-B-Zertifikate für Zahnarzt (Sektor KZBV)	269
4431	Tabelle 105: Tab_SMCB_KV-T SMC-B-Zertifikate für Sektoren der KBV	271
4432	Tabelle 106: Tab_SMCB_DKTIG SMC-B-Zertifikate für Sektor der DKTIG	273
4433	Tabelle 107: Tab_SMCB_TID_DKTIG Aufbau Telematik-ID in SMC-B-Zertifikaten der	
4434	DKTIG	275
4435	Tabelle 108: Tab_SMCB_KTR SMC-B-Zertifikate für Mitarbeiter Kostenträger	275
4436	Tabelle 109: Tab_SMCB_TID_GKVSV Aufbau Telematik-ID in SMC-B-Zertifikaten des	
4437	GKV-SV	277
4438	Tabelle 110: Tab_SMCB_BAK SMC-B-Zertifikate für Apotheker	278
4439	Tabelle 111: Tab_SMCB_TID_BAK Aufbau Telematik-ID in SMC-B-Zertifikaten der	
4440	Apotheker	280
4441	Tabelle 112: Tab_SMCB_ADV_KTR SMC-B-Zertifikate für die AdV-Umgebung im Auftrag	
4442	der Kostenträger	280
4443	Tabelle 113: Tab_SMCB_ORG_Gen - Generisches Zertifikatsprofil für die SMC-B-ORG	282
4444	Tabelle 114: Tab_HBA_BÄK HBA-Zertifikate (AUT, ENC, QES) für BÄK	305
4445	Tabelle 115: Tab_HBA_BZÄK HBA-Zertifikate (AUT, ENC, QES) für BZÄK	307
4446	Tabelle 116: Tab_HBA_BPtK HBA-Zertifikate (AUT, ENC, QES) für BPtK	309
4447	Tabelle 117: Tab_HBA_BAK HBA-Zertifikate (AUT, ENC, QES) für Apotheker	311
4448		

4449 11.5 Referenzierte Dokumente

4450 11.5.1 Dokumente der gematik

4451 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument
4452 referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der
4453 vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und
4454 Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und
4455 Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht
4456 aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der
4457 aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die
4458 vorliegende Version aufgeführt wird.

4459

[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

4460 11.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
----------	--

[ALGCAT]	Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, vom 11.12.2015 (auch online verfügbar: https://www.bundesanzeiger.de mit dem Suchbegriff „BAnz AT 01.02.2016 B5“)
[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]	T7 & TeleTrust (20.01.2009): Common PKI Spezifikation, Version 2.0 http://www.t7ev.org/themen/entwickler/common-pki-v20-spezifikation.html
[CP-HPC]	Bundesärztekammer et al (06.11.2012): Gemeinsame Policy für die Ausgabe der HPC – Zertifikatsrichtlinie HPC (Version 1.0.5) http://www.bundesaerztekammer.de/downloads/CP_HPC_v1.0.5.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 319 412-2]	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'
[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'
[ETSI TS 119 172-4]	ETSI TS 119 172-4 V0.0.4b (2017-06) 'Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists'
[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/IEC9594-2]	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
[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 (BGBI. I S. 2745), das durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBI. 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.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 TS 101 903 V1.4.2 (2010-12) Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)

[XMLSig]	W3C Recommendation: XML-Signature Syntax and Processing http://www.w3.org/TR/xmlsig-core/

ENTWURF

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 114: 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		

4472
4473

4474 12.2 BZÄK

4475 **Tabelle 115: 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		

4476 **12.3 BPtK**

4477 **Tabelle 116: 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 = „Psychologische/-r Psychotherapeut/-in“ und/oder	1 1-2	FALSE

		professionItem = „Kinder- und Jugendlichenpsychotherapeut/-in“ (siehe [gemSpec_OID#GS-A_4442]) 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)	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		

4478

4479 12.4 Apothekerschaft

4480 **Tabelle 117: 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> 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}	<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 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		

4481