

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

## Elektronische Gesundheitskarte und Telematikinfrastruktur

# Konzept PKI der TI- Plattform

Version: 2.99.0 CC  
Revision: 198482230662  
Stand: 02.0330.04.2020  
Status: zur Abstimmung freigegeben  
Klassifizierung: öffentlich\_Entwurf  
Referenzierung: gemKPT\_PKI\_TIP

26

## Dokumentinformationen

### Änderungen zur Vorversion

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

30

### Dokumentenhistorie

Version	Datum	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
2.0.0	02.08.17		Überarbeitung Online-Produktivbetrieb (Stufe 2.1)	gematik
	06.12.17		Ausbau LE-AdV	gematik
2.1.0	18.12.17		Änderungen lt. OPB1 R1.6.4-0, Ausbau LE-AdV-Anteile	gematik
2.2.0	14.05.18		Einarbeitung P15.2, P15.3, P15.4	gematik
2.3.0	26.10.18		Einarbeitung P15.9	gematik
2.4.0	18.12.18		Einarbeitung P15.11, 17.1	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, 16.1/2	gematik
2.8.0	02.03.20		Einarbeitung P21.1	gematik
2.89.0 CC	02.0330.04.20		freigegeben Anpassungen gemäß Änderungsliste P22.1 und Scope-Themen aus Systemdesign R4.0.0	gematik

## Inhaltsverzeichnis

33	<b>1 Einordnung des Dokumentes .....</b>	<b>11</b>
34	<b>1.1 Zielsetzung .....</b>	<b>11</b>
35	<b>1.2 Zielgruppe .....</b>	<b>11</b>
36	<b>1.3 Geltungsbereich .....</b>	<b>11</b>
37	<b>1.4 Methodik .....</b>	<b>12</b>
38	<b>2 Konzeptionelle Grundlagen .....</b>	<b>13</b>
39	<b>2.1 Einführung PKI der TI .....</b>	<b>13</b>
40	<b>2.2 Basisfunktionen der PKI .....</b>	<b>13</b>
41	<b>2.3 Vertrauensmodelle in der PKI der TI .....</b>	<b>14</b>
42	2.3.1 Vertrauensmodell für QES .....	14
43	2.3.2 Vertrauensraum mittels TSL .....	15
44	2.3.2.1 TSL in der TI im Kontext ECC Migration .....	15
45	2.3.3 Vertrauensraum mittels TSL – Umsetzung in der TI .....	16
46	2.3.3.1 Bereitstellung der TSL als Vertrauensraum der TI .....	16
47	2.3.3.2 Struktur, Signatur und Inhalt der TSL .....	16
48	2.3.3.3 Gültigkeit und Auswertung der TSL .....	20
49	2.3.3.4 Initialisierung/Reinitialisierung des Vertrauensraums .....	21
50	2.3.3.5 Sperrung von CA-Zertifikaten in der TSL .....	22
51	2.3.3.6 Aktualisierung des Vertrauensraumes .....	25
52	2.3.3.7 Vertrauensankerwechsel .....	25
53	2.3.4 Vertrauensmodell der nonQES TI-Zertifikate im Internet .....	26
54	2.3.5 Vertrauensmodell von Zertifikaten der HBA-Vorläuferkarten in der TI .....	26
55	2.3.6 Vertrauensmodell CVC .....	27
56	<b>2.4 Gültigkeitsmodelle X.509-Zertifikate .....</b>	<b>28</b>
57	2.4.1 PKIX-Schalenmodell .....	28
58	2.4.2 Kompromissmodell .....	29
59	2.4.3 QES-Kettenmodell .....	29
60	<b>2.5 Zertifikatstypen in der TI und deren Verwendung .....</b>	<b>29</b>
61	2.5.1 X.509-Zertifikate für Identitäten der TI .....	29
62	2.5.2 CV-Zertifikate für Karten in der TI .....	30
63	<b>2.6 Verantwortliche Instanzen .....</b>	<b>31</b>
64	<b>2.7 Teilnehmer in der PKI .....</b>	<b>32</b>
65	2.7.1 Trust Service Provider (TSP) .....	32
66	2.7.2 Registrierungsstellen .....	34
67	2.7.3 Kartenherausgeber .....	34
68	2.7.3.1 HBA-Herausgeber .....	36
69	2.7.3.2 eGK-Herausgeber .....	37
70	2.7.3.3 Herausgeber der SMC-B .....	37
71	2.7.3.4 Herausgeber von gSMC-K und gSMC-KT .....	38
72	2.7.3.5 Herausgeber von Prüfkarten .....	38
73	2.7.4 Anbieter TSL-Dienst .....	38
74	2.7.5 Zertifikatsantragsteller .....	38
75	2.7.6 Zertifikatsnehmer .....	39

76	2.7.7 Zertifikatsnutzer .....	39
77	2.7.8 gematik .....	39
78	2.7.9 Andere Teilnehmer .....	39
79	2.7.9.1 Rollenvergabestelle .....	39
80	2.7.9.2 Attributsbestätigende Stellen .....	40
81	<b>2.8 Identifikation von Akteuren .....</b>	<b>41</b>
82	2.8.1 Krankenversichertennummer .....	41
83	2.8.2 Telematik-ID .....	42
84	<b>2.9 Lebenszyklus von Zertifikaten .....</b>	<b>43</b>
85	2.9.1 Definition der Begriffe .....	43
86	2.9.2 Lebenszyklus für Zertifikate ohne Status-Eigenschaft .....	44
87	2.9.3 Lebenszyklus für Zertifikate mit Statureigenschaft .....	44
88	2.9.4 Staging der Zertifikate im Kartenterminal .....	44
89	2.9.5 Staging der Zertifikate des Konnektors .....	45
90	2.9.6 Verantwortlichkeiten für den Zertifikats-Lebenszyklus .....	45
91	2.9.6.1 gematik .....	46
92	2.9.6.2 TSP .....	46
93	2.9.6.3 Kartenherausgeber .....	47
94	2.9.6.4 Kartenhersteller .....	47
95	2.9.6.5 Hersteller einer Komponente .....	47
96	2.9.6.6 Betreiber einer Komponente .....	47
97	2.9.7 Gültigkeitszeiträume für Schlüssel .....	48
98	<b>3 CA-Strukturen .....</b>	<b>49</b>
99	<b>3.1 Einführung .....</b>	<b>49</b>
100	3.1.1 Übersicht Identitäten/Zertifikate .....	49
101	<b>3.2 TSP-übergreifende CA-Struktur .....</b>	<b>52</b>
102	3.2.1 nonQES-CA-Struktur für zentralisierte PKI .....	53
103	3.2.1.1 gematik Root-CA (im Kontext nonQES X.509-Zertifikate) .....	53
104	3.2.1.2 Komponenten- und Dienste-CA .....	54
105	3.2.1.3 Bereitstellung OCSP-Signer .....	54
106	3.2.1.4 Bereitstellung CRL-Signer .....	55
107	3.2.1.5 TSL-Signer-CA .....	55
108	3.2.1.6 gematik CVC-Root-CA .....	55
109	3.2.1.7 CVC-CA .....	55
110	<b>3.3 HBA-spezifische CA-Strukturen .....</b>	<b>56</b>
111	3.3.1 QES-CA-Struktur für HBA-QES .....	56
112	3.3.2 nonQES-CA-Struktur für ENC, AUT, OSIG, CV .....	56
113	3.3.3 Sektorneutrale CA für HBA, BA und SMC-B .....	57
114	<b>4 Statusprüfung bei X.509-Zertifikaten .....</b>	<b>59</b>
115	<b>4.1 Einführung .....</b>	<b>59</b>
116	<b>4.2 Eingangsanforderungen .....</b>	<b>59</b>
117	<b>4.3 Methoden der Statusprüfung .....</b>	<b>59</b>
118	4.3.1 Dezentrale Statusprüfung mittels CRL .....	59
119	4.3.2 Serverbasierte Statusprüfung mittels OCSP .....	59
120	4.3.3 Sonderfälle der Statusprüfung .....	60
121	<b>4.4 Logisches Konzept der OCSP-Dienste .....</b>	<b>60</b>
122	4.4.1 OCSP-Festlegungen .....	61

123	4.4.2 OCSP-Responder-Adresse.....	61
124	4.4.3 OCSP-Request.....	62
125	4.4.4 OCSP-Response.....	62
126	4.4.4.1 Zertifikatsstatus.....	62
127	4.4.4.2 Zeitpunkte in der OCSP-Response.....	62
128	4.4.4.3 Gültigkeitsdauer eines OCSP-Response (nonQES).....	63
129	4.4.4.4 Signatur der OCSP-Responses.....	63
130	4.4.4.5 Fehlermeldungen in der OCSP-Response.....	64
131	<b>4.5 OCSP-Dienste.....</b>	<b>64</b>
132	4.5.1 OCSP-Responder Proxy.....	65
133	4.5.2 Einsatz von HSM.....	66
134	<b>5 CVC-Grundlagen und CVC-Hierarchie.....</b>	<b>67</b>
135	<b>5.1 Funktion von CV-Zertifikaten.....</b>	<b>67</b>
136	<b>5.2 Hierarchie der CV-Zertifikate.....</b>	<b>68</b>
137	<b>5.3 Prozesse und Verantwortlichkeiten im Kontext CV-Zertifikate.....</b>	<b>68</b>
138	<b>5.4 Aufbau und Inhalt von CV-Zertifikaten für G1-Karten.....</b>	<b>69</b>
139	5.4.1 Zugriffsprofile.....	69
140	<b>5.5 Aufbau und Inhalt von CV-Zertifikaten für G2-Karten.....</b>	<b>69</b>
141	5.5.1 Aufbau und Inhalt.....	69
142	5.5.2 Zugriffsprofile.....	70
143	<b>5.6 Gültigkeitsmodell und Prüfung der CV-Zertifikate für G2-Karten.....</b>	<b>70</b>
144	<b>5.7 Konzeptionelle Grundlagen der Zertifikatserneuerung bei CV-Zertifikaten</b>	
145	<b>der G2-Karten.....</b>	<b>71</b>
146	5.7.1 Definition Gültigkeitsdauer, Zertifikatserneuerung und Sperrbarkeit.....	71
147	5.7.2 Infrastruktur zur Zertifikatserneuerung.....	71
148	<b>6 Zertifikatsprüfung.....</b>	<b>72</b>
149	<b>6.1 Grundlagen.....</b>	<b>72</b>
150	<b>6.2 Abgrenzung.....</b>	<b>72</b>
151	<b>6.3 Vertrauensraumprüfung in der TI.....</b>	<b>72</b>
152	6.3.1 Ablaufschritte der Vertrauensraumprüfung.....	72
153	<b>6.4 Vertrauensraumprüfung im Internet.....</b>	<b>74</b>
154	<b>6.5 Zertifikatsprüfung (nonQES).....</b>	<b>74</b>
155	6.5.1 Konzeptionelle Festlegungen zur Zertifikatsprüfung.....	74
156	6.5.2 Ablaufschritte der Zertifikatsprüfung.....	75
157	6.5.3 Weitere Prüfungen und Auswertungen.....	76
158	<b>6.6 QES-Zertifikatsprüfung.....</b>	<b>80</b>
159	6.6.1 Konzeptionelle Festlegungen zur QES-Zertifikatsprüfung.....	80
160	6.6.2 Ablaufschritte der QES-Zertifikatsprüfung.....	80
161	<b>6.7 Festlegungen zur Durchführung.....</b>	<b>82</b>
162	6.7.1 Durchführung von Zertifikatsprüfungen.....	82
163	6.7.2 Spezialfälle der Zertifikatsprüfung.....	82
164	6.7.3 Bedingungen für eine erfolgreiche Zertifikatsprüfung.....	83
165	<b>7 Betriebliche Aspekte der PKI.....</b>	<b>85</b>

166	<b>7.1 Einführung.....</b>	<b>85</b>
167	7.1.1 Rollen.....	85
168	7.1.2 Authentisierung der Rolleninhaber.....	85
169	<b>7.2 Zulassung von TSP in den Vertrauensraum der TI.....</b>	<b>86</b>
170	7.2.1 Zulassung von TSP X.509 zur Aufnahme in die TSL.....	86
171	7.2.2 Zulassung von CVC-CAs der zweiten Ebene.....	87
172	<b>7.3 TSP-Dienste im Rahmen des X.509-Zertifikatslebenszyklus.....</b>	<b>87</b>
173	7.3.1 Registrierungsdienst.....	87
174	7.3.2 Erstellungsdienst.....	89
175	7.3.3 Statusprüfdienst.....	89
176	7.3.4 Sperrdienst.....	90
177	<b>7.4 Verzeichnisdienst der TI.....</b>	<b>91</b>
178	7.4.1 Geltungsbereich.....	91
179	7.4.2 Datenmodell.....	91
180	7.4.2.1 Basisdaten (zertifikatsbasiert).....	91
181	7.4.2.2 Fachanwendungsdaten (optional).....	92
182	7.4.3 Lifecyclemanagement für Verzeichniseinträge.....	92
183	7.4.4 Aufbau und Außensicht.....	92
184	7.4.4.1 Autorisierung.....	92
185	7.4.4.2 Sichtbarkeit in der TI.....	93
186	<b>8 Anhang A – Verzeichnisse.....</b>	<b>94</b>
187	8.1 Abkürzungen.....	94
188	8.2 Glossar.....	99
189	8.3 Abbildungsverzeichnis.....	99
190	8.4 Tabellenverzeichnis.....	99
191	8.5 Referenzierte Dokumente.....	100
192	8.5.1 Dokumente der gematik.....	100
193	8.5.2 Weitere Dokumente.....	101
194	<b>1 Einordnung des Dokumentes.....</b>	<b>11</b>
195	1.1 Zielsetzung.....	11
196	1.2 Zielgruppe.....	11
197	1.3 Geltungsbereich.....	11
198	1.4 Methodik.....	12
199	<b>2 Konzeptionelle Grundlagen.....</b>	<b>13</b>
200	2.1 Einführung PKI der TI.....	13
201	2.2 Basisfunktionen der PKI.....	13
202	2.3 Vertrauensmodelle in der PKI der TI.....	14
203	2.3.1 Vertrauensmodell für QES.....	14
204	2.3.2 Vertrauensraum mittels TSL.....	15
205	2.3.2.1 TSL in der TI im Kontext ECC-Migration.....	15
206	2.3.3 Vertrauensraum mittels TSL – Umsetzung in der TI.....	16
207	2.3.3.1 Bereitstellung der TSL als Vertrauensraum der TI.....	16
208	2.3.3.2 Struktur, Signatur und Inhalt der TSL.....	16

209	2.3.3.3 Gültigkeit und Auswertung der TSL .....	20
210	2.3.3.4 Initialisierung/Reinitialisierung des Vertrauensraums .....	21
211	2.3.3.5 Sperrung von CA-Zertifikaten in der TSL .....	22
212	2.3.3.6 Aktualisierung des Vertrauensraumes .....	25
213	2.3.3.7 Vertrauensankerwechsel .....	25
214	2.3.4 Vertrauensmodell der nonQES TI-Zertifikate im Internet .....	26
215	2.3.5 Vertrauensmodell von Zertifikaten der HBA-Vorläuferkarten in der TI .....	26
216	2.3.6 Vertrauensmodell CVC .....	27
217	<b>2.4 Gültigkeitsmodelle X.509-Zertifikate .....</b>	<b>28</b>
218	2.4.1 PKIX-Schalenmodell .....	28
219	2.4.2 Kompromissmodell .....	29
220	2.4.3 QES-Kettenmodell .....	29
221	<b>2.5 Zertifikatstypen in der TI und deren Verwendung .....</b>	<b>29</b>
222	2.5.1 X.509-Zertifikate für Identitäten der TI .....	29
223	2.5.2 CV-Zertifikate für Karten in der TI .....	30
224	<b>2.6 Verantwortliche Instanzen .....</b>	<b>31</b>
225	<b>2.7 Teilnehmer in der PKI .....</b>	<b>32</b>
226	2.7.1 Trust Service Provider (TSP) .....	32
227	2.7.2 Registrierungsstellen .....	34
228	2.7.3 Kartenherausgeber .....	34
229	2.7.3.1 HBA-Herausgeber .....	36
230	2.7.3.2 eGK-Herausgeber .....	37
231	2.7.3.3 Herausgeber der SMC-B .....	37
232	2.7.3.4 Herausgeber von gSMC-K und gSMC-KT .....	38
233	2.7.3.5 Herausgeber von Prüfkarten .....	38
234	2.7.4 Anbieter TSL-Dienst .....	38
235	2.7.5 Zertifikatsantragsteller .....	38
236	2.7.6 Zertifikatsnehmer .....	39
237	2.7.7 Zertifikatsnutzer .....	39
238	2.7.8 gematik .....	39
239	2.7.9 Andere Teilnehmer .....	39
240	2.7.9.1 Rollenvergabestelle .....	39
241	2.7.9.2 Attributsbestätigende Stellen .....	40
242	<b>2.8 Identifikation von Akteuren .....</b>	<b>41</b>
243	2.8.1 Krankenversichertennummer .....	41
244	2.8.2 Telematik-ID .....	42
245	<b>2.9 Lebenszyklus von Zertifikaten .....</b>	<b>43</b>
246	2.9.1 Definition der Begriffe .....	43
247	2.9.2 Lebenszyklus für Zertifikate ohne Status-Eigenschaft .....	44
248	2.9.3 Lebenszyklus für Zertifikate mit Statureigenschaft .....	44
249	2.9.4 Staging der Zertifikate im Kartenterminal .....	44
250	2.9.5 Staging der Zertifikate des Konnektors .....	45
251	2.9.6 Verantwortlichkeiten für den Zertifikats-Lebenszyklus .....	45
252	2.9.6.1 gematik .....	46
253	2.9.6.2 TSP .....	46
254	2.9.6.3 Kartenherausgeber .....	47
255	2.9.6.4 Kartenhersteller .....	47
256	2.9.6.5 Hersteller einer Komponente .....	47
257	2.9.6.6 Betreiber einer Komponente .....	47
258	2.9.7 Gültigkeitszeiträume für Schlüssel .....	48



259	<b>3 CA-Strukturen .....</b>	<b>49</b>
260	<b>3.1 Einführung .....</b>	<b>49</b>
261	3.1.1 Übersicht Identitäten/Zertifikate .....	49
262	<b>3.2 TSP-übergreifende CA-Struktur .....</b>	<b>52</b>
263	3.2.1 nonQES-CA-Struktur für zentralisierte PKI .....	53
264	3.2.1.1 gematik Root-CA (im Kontext nonQES X.509-Zertifikate) .....	53
265	3.2.1.2 Komponenten- und Dienste-CA .....	54
266	3.2.1.3 Bereitstellung OCSP-Signer .....	54
267	3.2.1.4 Bereitstellung CRL-Signer .....	55
268	3.2.1.5 TSL Signer-CA .....	55
269	3.2.1.6 gematik CVC-Root-CA .....	55
270	3.2.1.7 CVC-CA .....	55
271	<b>3.3 HBA-spezifische CA-Strukturen .....</b>	<b>56</b>
272	3.3.1 QES-CA-Struktur für HBA-QES .....	56
273	3.3.2 nonQES-CA-Struktur für ENC, AUT, OSIG, CV .....	56
274	3.3.3 Sektorneutrale CA für HBA, BA und SMC-B .....	57
275	<b>4 Statusprüfung bei X.509-Zertifikaten .....</b>	<b>59</b>
276	<b>4.1 Einführung .....</b>	<b>59</b>
277	<b>4.2 Eingangsanforderungen .....</b>	<b>59</b>
278	<b>4.3 Methoden der Statusprüfung .....</b>	<b>59</b>
279	4.3.1 Dezentrale Statusprüfung mittels CRL .....	59
280	4.3.2 Serverbasierte Statusprüfung mittels OCSP .....	59
281	4.3.3 Sonderfälle der Statusprüfung .....	60
282	<b>4.4 Logisches Konzept der OCSP-Dienste .....</b>	<b>60</b>
283	4.4.1 OCSP Festlegungen .....	61
284	4.4.2 OCSP-Responder-Adresse .....	61
285	4.4.3 OCSP-Request .....	62
286	4.4.4 OCSP-Response .....	62
287	4.4.4.1 Zertifikatsstatus .....	62
288	4.4.4.2 Zeitpunkte in der OCSP-Response .....	62
289	4.4.4.3 Gültigkeitsdauer eines OCSP-Response (nonQES) .....	63
290	4.4.4.4 Signatur der OCSP-Responses .....	63
291	4.4.4.5 Fehlermeldungen in der OCSP-Response .....	64
292	<b>4.5 OCSP-Dienste .....</b>	<b>64</b>
293	4.5.1 OCSP-Responder Proxy .....	65
294	4.5.2 Einsatz von HSM .....	66
295	<b>5 CVC-Grundlagen und CVC-Hierarchie .....</b>	<b>67</b>
296	<b>5.1 Funktion von CV-Zertifikaten .....</b>	<b>67</b>
297	<b>5.2 Hierarchie der CV-Zertifikate .....</b>	<b>68</b>
298	<b>5.3 Prozesse und Verantwortlichkeiten im Kontext CV-Zertifikate .....</b>	<b>68</b>
299	<b>5.4 Aufbau und Inhalt von CV-Zertifikaten für G1-Karten .....</b>	<b>69</b>
300	5.4.1 Zugriffsprofile .....	69
301	<b>5.5 Aufbau und Inhalt von CV-Zertifikaten für G2-Karten .....</b>	<b>69</b>
302	5.5.1 Aufbau und Inhalt .....	69
303	5.5.2 Zugriffsprofile .....	70



304	<b>5.6 Gültigkeitsmodell und Prüfung der CV-Zertifikate für G2-Karten .....</b>	<b>70</b>
305	<b>5.7 Konzeptionelle Grundlagen der Zertifikatserneuerung bei CV-Zertifikaten</b>	
306	<b>der G2-Karten.....</b>	<b>71</b>
307	5.7.1 Definition Gültigkeitsdauer, Zertifikatserneuerung und Sperrbarkeit .....	71
308	5.7.2 Infrastruktur zur Zertifikatserneuerung .....	71
309	<b>6 Zertifikatsprüfung.....</b>	<b>72</b>
310	<b>6.1 Grundlagen.....</b>	<b>72</b>
311	<b>6.2 Abgrenzung .....</b>	<b>72</b>
312	<b>6.3 Vertrauensraumprüfung in der TI.....</b>	<b>72</b>
313	6.3.1 Ablaufschritte der Vertrauensraumprüfung.....	72
314	<b>6.4 Vertrauensraumprüfung im Internet .....</b>	<b>74</b>
315	<b>6.5 Zertifikatsprüfung (nonQES) .....</b>	<b>74</b>
316	6.5.1 Konzeptionelle Festlegungen zur Zertifikatsprüfung.....	74
317	6.5.2 Ablaufschritte der Zertifikatsprüfung .....	75
318	6.5.3 Weitere Prüfungen und Auswertungen.....	76
319	<b>6.6 QES-Zertifikatsprüfung .....</b>	<b>80</b>
320	6.6.1 Konzeptionelle Festlegungen zur QES-Zertifikatsprüfung.....	80
321	6.6.2 Ablaufschritte der QES-Zertifikatsprüfung .....	80
322	<b>6.7 Festlegungen zur Durchführung .....</b>	<b>82</b>
323	6.7.1 Durchführung von Zertifikatsprüfungen .....	82
324	6.7.2 Spezialfälle der Zertifikatsprüfung .....	82
325	6.7.3 Bedingungen für eine erfolgreiche Zertifikatsprüfung.....	83
326	<b>7 Betriebliche Aspekte der PKI .....</b>	<b>85</b>
327	<b>7.1 Einführung.....</b>	<b>85</b>
328	7.1.1 Rollen.....	85
329	7.1.2 Authentisierung der Rolleninhaber .....	85
330	<b>7.2 Zulassung von TSP in den Vertrauensraum der TI .....</b>	<b>86</b>
331	7.2.1 Zulassung von TSP-X.509 zur Aufnahme in die TSL.....	86
332	7.2.2 Zulassung von CVC-CAs der zweiten Ebene.....	87
333	<b>7.3 TSP-Dienste im Rahmen des X.509-Zertifikatslebenszyklus .....</b>	<b>87</b>
334	7.3.1 Registrierungsdienst.....	87
335	7.3.2 Erstellungsdienst.....	89
336	7.3.3 Statusprüfdienst .....	89
337	7.3.4 Sperrdienst .....	90
338	<b>7.4 Verzeichnisdienst der TI.....</b>	<b>91</b>
339	7.4.1 Geltungsbereich.....	91
340	7.4.2 Datenmodell.....	91
341	7.4.2.1 Basisdaten (zertifikatsbasiert) .....	91
342	7.4.2.2 Fachanwendungsdaten (optional) .....	92
343	7.4.3 Lifecyclemanagement für Verzeichniseinträge.....	92
344	7.4.4 Aufbau und Außensicht .....	92
345	7.4.4.1 Autorisierung.....	92
346	7.4.4.2 Sichtbarkeit in der TI .....	93
347	<b>8 Anhang A – Verzeichnisse .....</b>	<b>94</b>

348	<b>8.1 Abkürzungen .....</b>	<b>94</b>
349	<b>8.2 Glossar .....</b>	<b>99</b>
350	<b>8.3 Abbildungsverzeichnis.....</b>	<b>99</b>
351	<b>8.4 Tabellenverzeichnis .....</b>	<b>99</b>
352	<b>8.5 Referenzierte Dokumente.....</b>	<b>100</b>
353	8.5.1 Dokumente der gematik.....	100
354	8.5.2 Weitere Dokumente.....	101
355		

ENTWURF

---

## 1 Einordnung des Dokumentes

---

### 1.1 Zielsetzung

Das vorliegende Konzept der PKI legt die Anforderungen an die Erstellung und Verwaltung der Zertifikate der TI-Plattform fest, einschließlich deren Prüfung sowie der Grundlagen des zugehörigen Vertrauensraums.

Durch den Bestandsschutz sind wesentliche Aspekte der TI bereits gesetzt und orientieren sich somit an der bereits für den Basis-Rollout umgesetzten Architektur. Dazu zählen bspw. der Einsatz einer Trust-service Status List (TSL) als zentraler Vertrauensraum der X.509-PKI sowie der Einsatz einer hierarchischen Root-Struktur bei den CV-Zertifikaten.

Im Konzept werden Optimierungen für die gewachsenen, komplexen CA-Strukturen der PKI-Anbieter dargestellt, ebenso Optimierungen bzgl. der zugehörigen OCSP-Strukturen.

Nach den einführenden Kapiteln werden folgende Themen behandelt:

**Kap. 2** beschreibt konzeptionelle Grundlagen, v. a. hinsichtlich der Vertrauensmodelle der TI und der relevanten Teilnehmer der PKI der TI.

**Kap. 3** beschreibt Optimierungen der CA-Strukturen, um mehr Flexibilität, weniger Komplexität und eine verbesserte Wirtschaftlichkeit zu erreichen.

**Kap. 4** schildert die Grundlagen der Statusprüfung bei X.509-Zertifikaten mittels OCSP als Standardprotokoll und zeigt Optimierungsmöglichkeiten in der Architektur auf.

**Kap. 5** beschreibt die Besonderheiten von CV-Zertifikaten.

**Kap. 6** skizziert die Grundlagen der Prüfung von X.509-Zertifikaten und des zugrundeliegenden Vertrauensraums inkl. der Besonderheiten bei der Prüfung qualifizierter Zertifikate.

**Kap. 7** skizziert die wesentlichen betrieblichen PKI-Prozesse.

### 1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter von Produkten der TI.

### 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*

392 *allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu*  
393 *tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder*  
394 *Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen*  
395 *Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik*  
396 *GmbH übernimmt insofern keinerlei Gewährleistungen.*

### 397 **1.4 Methodik**

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

402 Sie werden im Dokument wie folgt dargestellt:

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

404 Text / Beschreibung

405 [**<=**]

406

407 Dabei umfasst die Anforderung sämtliche zwischen der Afo-ID und der Textmarke  
408 angeführten Inhalte.  
409

---

## 2 Konzeptionelle Grundlagen

---

### 2.1 Einführung PKI der TI

Die TI-Plattform muss Komponenten und Funktionen zur Verfügung stellen, um in den Geschäftsprozessen des Gesundheitswesens die folgenden Elementarfunktionen anbieten zu können:

- Authentisierung von Akteuren gegenüber Systemen, Komponenten und Diensten der TI über eine verbindlich registrierte Zuordnung von Schlüssel mit einem Akteur; diese Funktion adressiert den Aspekt der Authentizität.
- Erstellung und Prüfung von digitalen Signaturen, die die bewusste willentliche Veranlassung durch einen bestimmten Akteur in Form einer Signatur über die fragliche Transaktion/Daten dokumentieren; die Signaturfunktion adressiert den Aspekt der Nichtabstreitbarkeit der signierten Transaktion.
- Erstellung und Prüfung von digitalen Signaturen, die den Zustand eines Datums zum Zeitpunkt dieses Signaturvorgangs in Form einer Signatur dokumentieren; die Signaturfunktion adressiert den Aspekt der Integrität des signierten Datums.
- Ver- und Entschlüsselung von Daten, die besonderen Vertraulichkeitsanforderungen unterliegen bei Speicherung und Transport; die Verschlüsselung adressiert den Aspekt der Vertraulichkeit.

Die angeführten Funktionen werden auf der Grundlage asymmetrischer kryptographischer Verfahren bereitgestellt, sind in ein technisches und organisatorisches Regelwerk eingebunden und bilden in Summe die Public Key Infrastructure (PKI) der TI.

#### **TIP1-A\_2030 - Bereitstellung von Sicherheitsgrundfunktionen auf Krypto-Basis**

Die TI-Plattform MUSS kryptographisch basierte Verfahren zur Umsetzung der Schutzziele Authentizität, Nichtabstreitbarkeit, Integrität und Vertraulichkeit bereitstellen.

[<=]

Nutzer der PKI sind die Akteure im Gesundheitswesen – natürliche und juristische Personen der Heil-, Pflege- und Hilfsmittelversorgung, Gesellschafterorganisationen, technische Infrastrukturkomponenten der TI selbst und schließlich Anwendungs- und Fachdienste der Leistungserbringer und Kostenträger.

#### **TIP1-A\_2032 - Abbildung von Akteuren auf elektronische Identitäten der TI**

Die TI-Plattform MUSS die technisch sichere Abbildung von Akteuren auf elektronische Identitäten der TI in Form von Soft- oder Hardware-Sicherheitsmodulen (z.B. Chipkarten, HSM) realisieren.

[<=]

Die architektonische Einordnung der PKI erfolgt im Konzept „Architektur der TI-Plattform“ [gemKPT\_Arch\_TIP].

### 2.2 Basisfunktionen der PKI

Aus Anwendungs- und Nutzersicht stellt die PKI eine Reihe von Basisfunktionen zur Verfügung:

- Bereitstellung und Lifecycle Management des TI-Vertrauensraums
- Identifikation von Personen, Institutionen und technischen Komponenten
- Registrierung von Zertifikatsantragstellern
- Erzeugung und Bereitstellung von Endnutzerzertifikaten für
  - nonQES-Zertifikate
  - QES-Zertifikate nach [eIDAS]
- Zertifikatssperrung durch Zertifikatsnehmer und attributbestätigende Stellen
- Zertifikatssperrung durch Herausgeber und gematik als „Policy Authority“
- Suchen und Abrufen von Zertifikaten aus Verzeichnissen
- Abruf von Zertifikatsstatusinformationen (Sperrinformationen)
- Beantragung, Produktion und Auslieferung von Zertifikaten

Durch die gesicherte und verbindliche Zuordnung von Akteuren zu kryptographischen Schlüsseln wird die elektronische Identität des Akteurs etabliert, so dass dieser in den elektronischen Geschäftsprozessen der TI zuverlässig authentifiziert werden kann und über die Möglichkeiten zu vertraulicher Kommunikation verfügt.

## **TIP1-A\_2033 - PKI-Dienste-Implementierung nach internationalen Standards**

Die TI-Plattform SOLL die Konzeption der PKI-Dienste gemäß den internationalen Standards implementieren.

[<=]

## **2.3 Vertrauensmodelle in der PKI der TI**

Ein definierter PKI-Vertrauensraum für die Anwendungsbereiche der Gesundheitskarte bildet den Kern der kryptographisch abgesicherten Geschäftsprozesse des Gesundheitswesens. Gemäß der regulatorischen Hoheit der unterschiedlichen Anwendungsfelder müssen zu deren Abbildung innerhalb und außerhalb der TI verschiedene Vertrauensmodelle implementiert werden für:

- Zertifikate für die Erstellung qualifizierter elektronischer Signaturen (QES), die speziell für die Anwendungsbereiche der Gesundheitskarte zusätzlich unter den Bestimmungen des SGB implementiert werden.
- Digitale Zertifikate, für deren Einsatz innerhalb der TI und des Internets die Regularien einerseits der gematik sowie andererseits die der Vertretungsorganisationen von Leistungserbringern und Kostenträgern bestimmend sind.
- Digitale Zertifikate, die im Kontext des zeitlich begrenzten Bestandsschutzes der HBA-Vorläuferkarten bereits im Feld im Einsatz sind, und deren Funktionsweise (soweit technisch unterstützt) auch innerhalb der TI unterstützt werden soll.

### **2.3.1 Vertrauensmodell für QES**

Qualifizierte Vertrauensdienste gemäß [eIDAS] müssen in der Vertrauensliste (VL) des jeweils zuständigen Mitgliedstaates publiziert werden (siehe [eIDAS], Artikel 22 und EU-Durchführungsbeschluss 2015/1505 dazu). Dies beinhaltet auch das Führen einer Historie, z.B. wird bei einem gesperrten Dienst aufgeführt, bis wann dieser über einen gültigen Qualifikationsstatus verfügte.

Die Bundesnetzagentur (BNetzA) ist gemäß [VDG] für die deutsche Vertrauensliste (BNetzA-VL) zuständig. Die BNetzA-VL gibt somit offiziell vor, ob ein Vertrauensdienst (d.h. eine CA und deren Zertifikat) zu einem bestimmten Zeitpunkt über einen gültigen Status zur Ausgabe von QES-Zertifikaten verfügte. Der TSL-Dienst lädt diese Liste deshalb regelmäßig vom Download-Punkt der BNetzA herunter und stellt diese – analog zur TSL – in der TI den QES-validierenden Komponenten (also den Konnektoren) zur Verfügung.

Die Zertifikate zur Signierung der BNetzA-VL werden in die „List of Trusted Lists“ der Europäischen Kommission (EU-LOTL) eingetragen, und die BNetzA-VL darf nur unter Verwendung eines dieser offiziell publizierten Zertifikate signiert werden. Der TSL-Dienst nimmt diese Zertifikate deshalb mit einer speziellen Markierung versehen in die TSL auf (siehe auch Kapitel 2.3.3 „Vertrauensraum mittels TSL – Umsetzung in der TI“), und die QES-validierenden Komponenten entnehmen die BNetzA-Signer-Zertifikate der aktuellen TSL, um die Signatur der BNetzA-VL zu prüfen.

#### **TIP1-A\_2034 - QES-PKI**

Die TI-Plattform MUSS eine PKI für QES-Zertifikate in der TI gemäß [eIDAS] umsetzen. [<=]

### **2.3.2 Vertrauensraum mittels TSL**

Die vertrauenswürdigen Aussteller-CAs für X.509-Zertifikate werden in einer TSL einem einheitlichen Vertrauensraum unterstellt. Für die Implementierung wird das Konzept der „Trust-service Status List“ (TSL) gewählt. Dabei werden die Vertrauensinformationen der teilnehmenden Zertifikatsaussteller, der Trust Service Provider (TSP), in einer signierten XML-Datei abgelegt. Es gilt bei den nonQES-CA-Zertifikaten der TSL ihre Aufnahme in die TSL als hinreichendes Indiz für die Vertrauenswürdigkeit. Das Konzept der TSL ist durch ETSI normiert. Details sind in [ETSI\_TS\_102\_231\_V3.1.2] zu finden.

#### **2.3.2.1 TSL in der TI im Kontext ECC-Migration**

Der in der TI etablierte Vertrauensraum mittels TSL wird von der ausschließlichen Nutzung von RSA im Rahmen der ECC-Migration auf die Verwendung von ECDSA-Zertifikaten erweitert. Dazu wird neben der bereits aufgebauten TSL(RSA) eine zweite TSL(ECC-RSA) etabliert, die neben den neuen ECC-Elementen aus Rückwärtskompatibilitäts-Gründen auch die RSA-Elemente enthält. Die TSL(ECC-RSA) wird von auf ECC migrierten oder zu migrierenden TI-Produkttypen als Vertrauensraum-Repräsentation verwendet.

Sowohl die TSL(RSA) als auch die TSL(ECC-RSA) stellen für sich genommen eigene TI-Vertrauensräume dar. Die im Folgenden beschriebenen Darstellungen beziehen sich (auch, wenn im Singular beschrieben) auf beide Varianten.

Bezüglich eines TI-Vertrauensraumes (RSA oder ECC-RSA) gibt es immer genau einen Vertrauensanker, der durch das entsprechend aktive TSL-Signer-CA-Zertifikat derselben Schlüsselgeneration (RSA oder ECDSA) abgebildet ist:

- Vertrauensanker RSA: TSL-Signer-CA-Zertifikat (RSA)
- Vertrauensanker ECC-RSA: TSL-Signer-CA-Zertifikat (ECDSA)



### 2.3.3 Vertrauensraum mittels TSL – Umsetzung in der TI

In der TI wird mittels einer TSL ein einheitlicher Vertrauensraum der X.509-PKI umgesetzt. Für den Einsatz in der TI zugelassene TSP-X.509 werden in die TSL der gematik aufgenommen. Im Rahmen der Zertifikatsprüfung muss ermittelt werden, ob die Aussteller-CA in der TSL vorhanden ist.

Eine detaillierte Darstellung der Prüflogik bei der Zertifikatsprüfung erfolgt in Kap 6.

Hinweis: Die TSL hat in der TI neben der Etablierung des Vertrauensraumes zusätzlich die Funktion, als vertrauenswürdiges Medium PKI-bezogene Zusatzinformationen zur Zertifikatsprüfung innerhalb der TI zu transportieren. Damit wird der sichere Betrieb unterstützt. Bei den Artefakten handelt es sich aktuell um:

- BNetzA-VL-Signer-Zertifikate und die Download-Punkte der BNetzA-VL innerhalb der TI
- Root-CA-Zertifikate der CVC-Root und deren Cross-Zertifikate
- DNSSEC-Trustanchor der TI

#### 2.3.3.1 Bereitstellung der TSL als Vertrauensraum der TI

##### TIP1-A\_2038 - Vertrauensraum mittels TSL

Die TI-Plattform MUSS für die Implementierung des Vertrauensraums das Konzept einer „Trust-service Status List“ (TSL) umsetzen.

[<=]

##### TIP1-A\_2039 - Bereitstellung des TSL-Dienstes

Die TI-Plattform MUSS einen TSL-Dienst bereitstellen.

[<=]

##### TIP1-A\_2683 - Bereitstellung nonQES-PKI in der TI

Die TI-Plattform MUSS eine PKI für nonQES-Zertifikate in der TI umsetzen.

[<=]

##### TIP1-A\_2037 - Bereitstellung Vertrauensraum

Die TI-Plattform MUSS für alle X.509-nonQES-Zertifikate einen Vertrauensraum mit einer für die Kartenarten (1) eGK, (2) HBA, (3) SMC entsprechenden Policy umsetzen.

[<=]

##### TIP1-A\_2054 - Downloadbarkeit der TSL

Der TSL-Dienst MUSS für die TSL als zentralen Vertrauensraum mehrere, voneinander unabhängige Downloadpunkte implementieren und publizieren, um die TSL hochverfügbar bereitzustellen.

[<=]

##### TIP1-A\_2055 - Bereitstellung der TSL im Internet

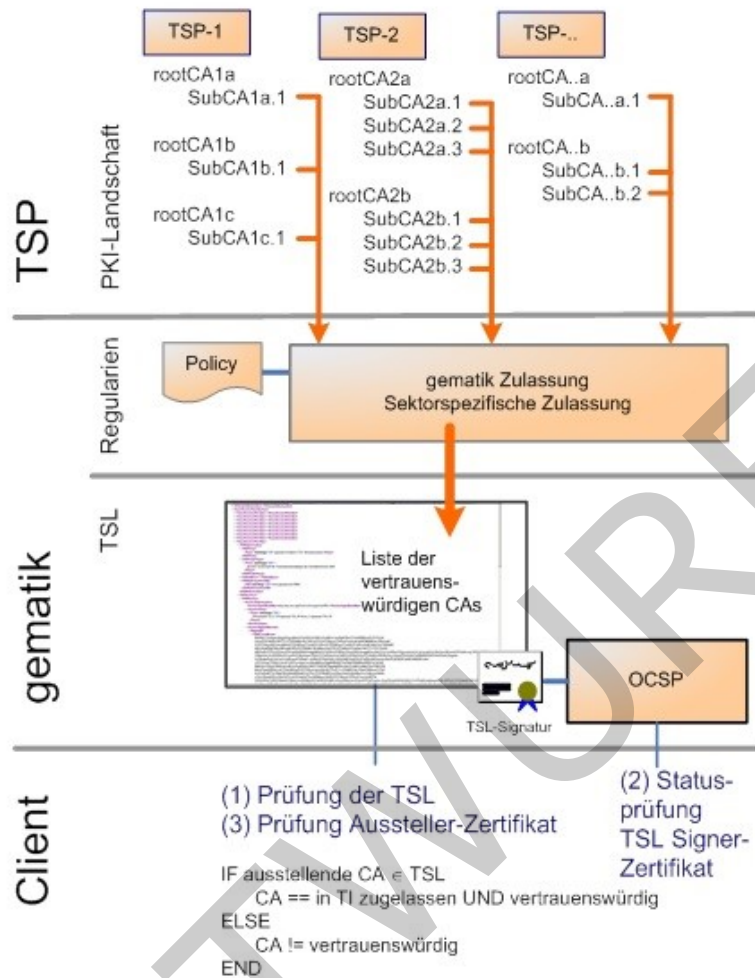
Die TI-Plattform MUSS die TSL als zentralen Vertrauensraum in der TI und im Internet zum Download bereitstellen.

[<=]

In der TSL-Umsetzung vor Bestandsaufnahme wurde für die Komponentenzertifikate eine eigene, separate TSL bereitgestellt, die als „Infrastruktur-TSL“ oder „Trusted Component List“ (TCL) bezeichnet wurde. Nun erfolgt die Zusammenfassung in eine Liste für die Aussteller von Personen-/Organisationszertifikaten und Komponentenzertifikaten.

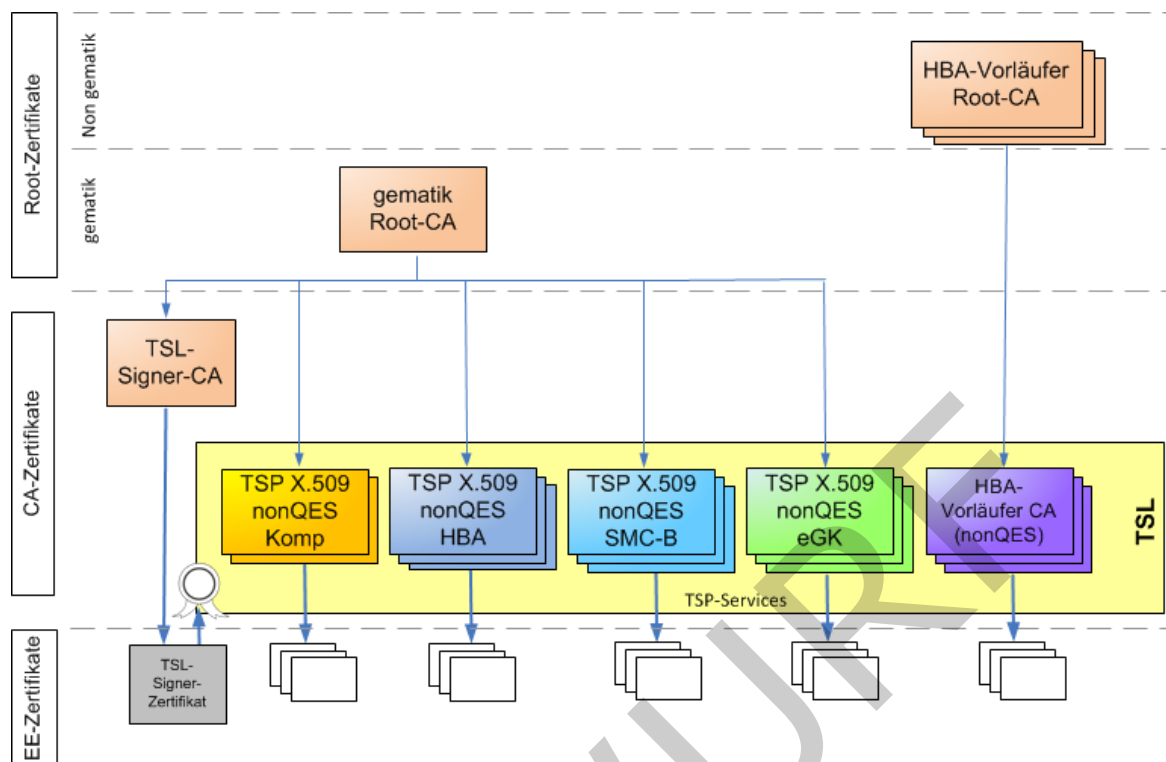
#### 2.3.3.2 Struktur, Signatur und Inhalt der TSL

Die folgende Abbildung verdeutlicht die Anwendung der TSL in der TI.



**Abbildung 1: TSL-Modell**

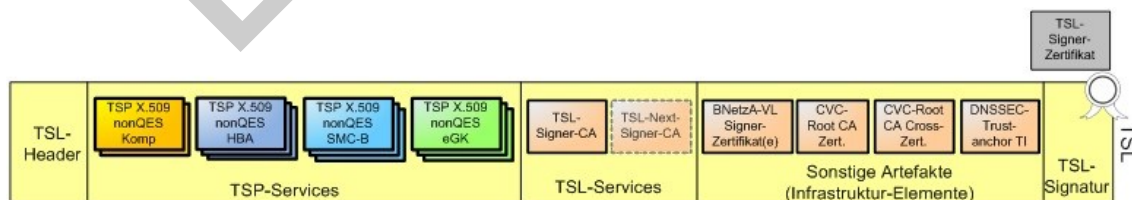
Abbildung 2 zeigt die grundsätzlichen Hierarchiestufen der Zertifikate und soll verdeutlichen, dass jeweils die CA-Zertifikate in die TSL als Vertrauensraum aufzunehmen sind, unabhängig davon, ob diese aus einer übergeordneten Root-CA abgeleitet sind oder es sich um sog. „self-signed“ CAs handelt.



**Abbildung 2: Zertifikathierarchien und deren Abbildung in der TSL**

In Abbildung 3 ist der interne Aufbau der TSL gezeigt. Nach Verwaltungsinformationen im TSL-Header werden die CA-Zertifikate der TSP-X.509, ob self-signed oder aus übergeordneter Root, als „TSP-Services“ in die TSL aufgenommen. „TSP-Services“ sind die Zertifikate, die zur Absicherung der TSL selbst erforderlich sind, z. B. das TSL-Signer-CA-Zertifikat. Im Falle der Aktualisierung des Vertrauensankers wird auch der neue, zukünftige Vertrauensanker aufgenommen. Das TSL-Signerzertifikat ist in die XML-Signatur der TSL eingebettet. Das TSL-Signerzertifikat wird ausgegeben von der TSL-Signer-CA, die wiederum von der gematik Root-CA zertifiziert wird.

Neben diesen Basis-Elementen, werden in der TSL auch noch weitere Infrastruktur-Elemente als Artefakte (siehe auch Hinweis in Kapitel 2.3.3 „Vertrauensraum mittels TSL – Umsetzung in der TI“) mitgeführt. Dazu gehören vor allem auch die publizierten Signer-Zertifikate der BNetzA-VL (siehe auch Kapitel 2.3.1 „Vertrauensmodell für QES“).



**Abbildung 3: Aufbau der TSL**

### TIP1-A\_2041 - Format der TSL nach [ETSI\_TS\_102\_231\_V3.1.2]

Der TSL-Dienst MUSS als technisches Format für die TSL das ETSI-Format nach [ETSI\_TS\_102\_231\_V3.1.2] „Provision of harmonized Trust-service status information“

606 umsetzen.

607 [ $\leq$ ]

### 608 **TIP1-A\_2040 - Signatur der TSL durch TSL-Signerzertifikat**

609 Der TSL-Dienst MUSS jede zu publizierende TSL mit einem TSL-Signerzertifikat signieren

610 [ $\leq$ ]

### 611 **TIP1-A\_2042 - In TSL aufzunehmende Infos zu Zertifikatsherausgebern**

612 Der TSL-Dienst MUSS in die TSL die folgenden Informationen bzgl. der einzelnen

613 zugelassenen Zertifikatsherausgeber aufnehmen: (a) CA-Zertifikat, (b)

614 Bereitstellungspunkt für Statusauskunft per OCSP (ggf. auch mehrere), (c)

615 Signaturzertifikat des OCSP-Responders, (d) Kennung der für diesen

616 Zertifikatsherausgeber erlaubten Zertifikatstypen.

617 [ $\leq$ ]

### 618 **TIP1-A\_2043 - Aufnahme von zugelassenen CAs in die TSL**

619 Der TSL-Dienst MUSS das Aussteller-CA-Zertifikat einer CA, der innerhalb der TI ein

620 vertrauenswürdiger Status zugewiesen werden soll, in die TSL aufnehmen.

621 [ $\leq$ ]

### 622 **TIP1-A\_2045 - Entfernen von abgelaufenen nonQES-CA-Zertifikaten aus der TSL**

623 Der TSL-Dienst MUSS nonQES-CA-Zertifikate aus der TSL entfernen, sobald das

624 Aussteller-CA-Zertifikat zeitlich abgelaufen ist.

625 [ $\leq$ ]

### 626 **TIP1-A\_2046 - Prüfung der Vertrauenswürdigkeit von Aussteller-CAs**

627 Die TI-Plattform MUSS zur Feststellung der Vertrauenswürdigkeit einer Aussteller-CA zu

628 einem gegebenen EE-Zertifikat prüfen, ob diese Aussteller-CA als Eintrag in der TSL

629 vorhanden und zu diesem Zeitpunkt als gültig gekennzeichnet ist.

630 [ $\leq$ ]

631 Im Rahmen der Zertifikatsprüfung wird dann nicht das Root-Zertifikat geprüft, sondern

632 nur der direkte Schritt zum CA-Zertifikat. Es müssen bei einer mehrstufigen Hierarchie

633 nur die Zertifikate der ausstellenden CAs in die TSL aufgenommen werden, egal ob es

634 sich dabei um self-signed-CA- oder Sub-CA-Zertifikate aus einer übergeordneten Root

635 handelt.

### 636 **TIP1-A\_2047 - Kennzeichnung des Status von Aussteller-CAs in TSL**

637 Der TSL-Dienst MUSS für jedes enthaltene Aussteller-CA-Zertifikat in der TSL ein

638 Statuskennzeichen pflegen, in welchem der Status dieser CA dokumentiert ist und ab

639 welchem Zeitpunkt (Datum) dieser Status gelten soll.

640 [ $\leq$ ]

### 2.3.3.3 Gültigkeit und Auswertung der TSL

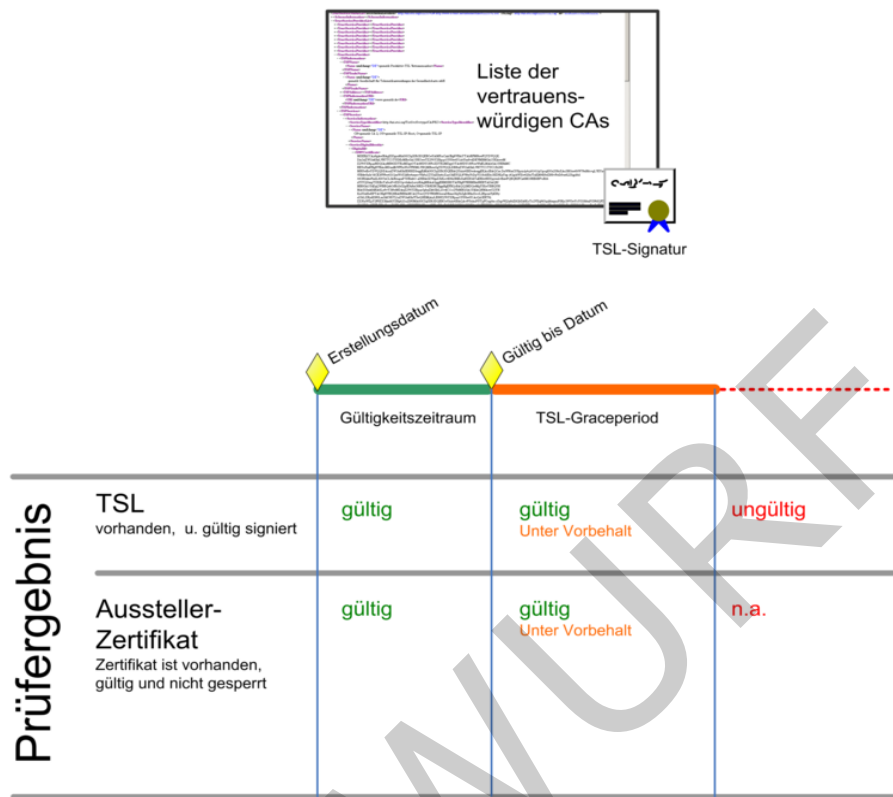


Abbildung 4: Gültigkeitszeiträume TSL

#### TIP1-A\_2048 - Bereitstellung von TSL-Signer-CA- und -Signerzertifikat

Der TSL-Dienst MUSS den signaturprüfenden Komponenten das TSL-Signer-CA-Zertifikat, das TSL-Signerzertifikat und die URL des zugehörigen OCSP-Responder bereitstellen, um die Prüfung des Vertrauensraumes im Rahmen einer Zertifikatsprüfung zu ermöglichen. [ <= ]

#### TIP1-A\_2049 - Bereitstellung von Metainformationen zur TSL

Der TSL-Dienst MUSS in die TSL folgende Informationen zur Liste selbst bereitstellen, um die Aktualität der Liste auswertbar zu machen (a) Erstellungsdatum, ab dem die Liste als „aktuell“ gilt, (b) Geplantes Updatedatum, an dem die Liste durch eine neue Version aktualisiert werden soll, (c) inkrementelle Sequenznummer der Liste [ <= ]

#### TIP1-A\_2050 - Gültigkeit der TSL unter Vorbehalt

Die Produkttypen der TI-Plattform, die Zertifikate prüfen, MÜSSEN eine nicht mehr aktuelle TSL bis zu einem darüber hinausgehenden Zeitpunkt weiterhin als gültig unter Vorbehalt auswerten. Der Vorbehalt MUSS in einer Warnmeldung an die aufrufende Funktion bei der Zertifikatsprüfung mit dem Hinweis geliefert werden, dass die Prüfung gegen eine abgelaufene TSL erfolgte. [ <= ]

Der Zeitraum nach Ablauf des Gültigkeitszeitraums der TSL, in dem gemäß [TIP1-A\_2050] die TSL als „gültig unter Vorbehalt“ betrachtet wird, wird im Weiteren als „TSL-Graceperiod“ bezeichnet.

#### **TIP1-A\_2051 - CA-Zertifikatsprüfung innerhalb TSL-Graceperiod**

Die Produkttypen der TI-Plattform, die Zertifikate prüfen, MÜSSEN eine TSL-Graceperiod konfigurierbar implementieren, innerhalb der die Prüfung eines enthaltenen und nicht gesperrten Aussteller-CA-Zertifikates ein Gültig-Ergebnis in Verbindung mit einer Warnmeldung liefern muss. Ein Defaultwert der TSL-Graceperiod MUSS in den Produkttypen voreingestellt sein.

[<=]

#### **TIP1-A\_2489 - CA-Zertifikatsprüfung nach Ablauf TSL-Graceperiod**

Die Produkttypen der TI-Plattform, die Zertifikate prüfen, MÜSSEN nach zeitlichem Ablauf der TSL-Graceperiod bei der Prüfung eines Aussteller-CA-Zertifikates unabhängig vom Status dieses CA-Zertifikates ein Ungültig-Ergebnis der Zertifikatsprüfung in Verbindung mit einer Fehlermeldung liefern, da die TSL selbst als ungültig bewertet werden muss und damit keine valide Prüfbasis zur Verfügung steht.

[<=]

Im Ergebnis bedeutet dies innerhalb der TSL-Graceperiod ein positives Prüfergebnis „unter Vorbehalt“ – also ein verringertes Vertrauensniveau, das dem prüfenden Client eine Ermessensentscheidung für das weitere Vorgehen ermöglicht.

#### **TIP1-A\_2053 - Folgerungen des TSL-Prüfergebnisses Gültig unter Vorbehalt**

Die Produkttypen der TI-Plattform, die Zertifikate prüfen, MÜSSEN die semantischen Folgerungen eines TSL-Prüfergebnisses „Gültig unter Vorbehalt (Ablaufdatum < aktueller Zeitpunkt < (Ablaufdatum + TSL-Graceperiod))“ gemäß den eigenen Schutzbedarfen definieren und umsetzen.

[<=]

#### **TIP1-A\_2072 - Prüfung auf Aktualität der TSL**

Alle zertifikatsprüfenden Komponenten in der TI-Plattform MÜSSEN in einem definierten Prüfintervall das Vorhandensein einer aktualisierten TSL prüfen und anhand eines optionalen Hashvergleichsverfahrens oder der Sequenznummer in der TSL entscheiden, ob die im Trust Store vorhandene TSL beibehalten wird oder durch eine neuere Version (höhere Sequenznummer) vom Verteilpunkt ersetzt werden muss.

[<=]

### **2.3.3.4 Initialisierung/Reinitialisierung des Vertrauensraums**

Die Etablierung des Vertrauensraums durch den initialen Download der TSL ist relevant für die Fälle:

- Erstinbetriebnahme einer Komponente in der TI
- Wiederanlauf bzw. Systemwiederherstellung zu einem Zeitpunkt, zu dem die in der Komponente vorhandene TSL definitiv nicht mehr gültig ist:

#### **TIP1-A\_2056 - Sichere Einbringung des Vertrauensankers**

Die TI-Plattform MUSS sicherstellen, dass in alle zertifikatsprüfenden Komponenten bei der Erstinbetriebnahme der Vertrauensanker in Form des TSL-Signer-CA-Zertifikates sicher eingebracht wird.

[<=]



## **TIP1-A\_2435 - Verifikation des Vertrauensankers**

Die TI-Plattform MUSS sicherstellen, dass bei allen zertifikatsprüfenden Komponenten im Zuge der Erstinbetriebnahme der initial eingebrachte Vertrauensanker (TSL-Signer-CA-Zertifikat) durch einen Berechtigten verifiziert wird.

[<=]

## **TIP1-A\_2057 - Identifizierung und Verifizierung des TSL-Signer-CA-Zertifikates**

Die TI-Plattform MUSS für die Bereitstellung und Übermittlung des TSL-Signer-CA-Zertifikates Verfahren zur Verfügung stellen, die eine sichere Identifizierung und Verifizierung genau dieses Zertifikates gewährleisten.

[<=]

## **TIP1-A\_2058 - Schutz vor Überschreiben des TSL-Signer-CA-Zertifikates**

Zertifikatsprüfende Komponenten in der TI-Plattform MÜSSEN sicherstellen, dass das TSL-Signer-CA-Zertifikat im komponenteninternen Trust Store durch einen geeigneten Schutzmechanismus vor missbräuchlichem Überschreiben oder Manipulation abgesichert wird.

[<=]

Nach Implementierung des Vertrauensankers in der Komponente erfolgt in einem nächsten Schritt der Import der aktuell gültigen TSL, deren Prüfung gegen das TSL-Signer-CA-Zertifikat sowie das darauf folgende Einlesen aller Ausstellerzertifikate der TSL und deren Abspeicherung in einem sicheren Speicherbereich (Trust Store) der Komponente.

Die Verfahren zum Import von TSL-Signer-CA-Zertifikat, dessen Fingerprint sowie auch der TSL selbst müssen berücksichtigen, dass die Komponente bis zum erfolgreichen Abschluss dieses Verfahrens noch keine Verbindung in die TI aufbauen kann – somit die Elemente über das Internet bezogen und offline in die Komponenten eingebracht werden müssen.

Nach erfolgreichem Abschluss der o.g. Schritte ist die Komponente bis zum Zeitpunkt des nächsten Updates wieder korrekt konfiguriert für Zertifikatsprüfungen und automatische TSL-Aktualisierungen.

## **TIP1-A\_2059 - Speicherung der TSL in lokalem Trust Store**

Alle zertifikatsprüfenden Komponenten in der TI-Plattform MÜSSEN die Inhalte der TSL nach erfolgreicher Vertrauensraum- und syntaktischer Prüfung in einem lokalen Trust Store sicher speichern und zum weiteren Abruf lokal zugreifbar halten.

[<=]

Vorgaben zum lokalen Trust Store werden in den produkttypspezifischen Spezifikationen der jeweiligen Komponenten getroffen.

## **2.3.3.5 Sperrung von CA-Zertifikaten in der TSL**

Bei einem Widerruf der TI-Zulassung von Root-CA- oder Aussteller-CA-Zertifikaten werden anhand der Kritikalität des zugrundeliegenden Incidents zwei Sperrgründe unterschieden.

### **Sicherheitskritischer Incident**

Mögliche Gründe, die einen sicherheitskritischen Incident darstellen (nicht abschließend):

- Festgestellte oder mögliche Kompromittierung des CA-Schlüssels
- Sicherheitsprobleme oder -verstöße beim TSP-X.509 hinsichtlich Betriebsprozessen, Sicherheitsinfrastrukturen und Verfahrensabläufen



- Kenntnis von Änderungen an sicherheitskritischen Prozessen oder Infrastrukturen, die nicht in Form einer Änderungsmitteilung inklusive eines Sicherheitsgutachtens bei der gematik eingereicht wurden
- Änderungsmitteilung des TSP-X.509 bezüglich sicherheitskritischer Aspekte seiner Zulassung, die keine positive Einschätzung durch ein Sicherheitsgutachten nachweisen konnte

Diese Fälle werden im Rahmen des TI-übergreifenden Notfallmanagements gemäß [gemRL\_Betr\_TI] koordiniert. Der TSP-X.509 hat diese Fälle als Incident der Priorität 1 mit der Kennzeichnung „TI-Notfall“ zu klassifizieren und zur Koordination der Notfallbewältigung an den Servicebetriebsverantwortlichen der TI-Plattform (SBV) zu eskalieren. Weitere Vorgaben zur TI-Notfallbewältigung und -vorsorge befinden sich in [gemRL\_Betr\_TI].

Der SBV wird in Abstimmung mit den Beteiligten (Herausgeber, TSP/VDA für QES, ggf. BNetzA), geeignete Maßnahmen herbeiführen.

Wird eine Massensperrung notwendig, erfolgt in diesen Fällen der Entzug des Vertrauensstatus durch Setzen eines Sperrdatums, und/oder der Entfernung des Aussteller-CA-Zertifikates aus der TSL zu einem festgelegten Zeitpunkt. Mit Verteilung der aktualisierten TSL in die Trust Stores der dezentralen Komponenten und Fachdienste verlieren sowohl die CA wie auch sämtliche EE-Zertifikate dieser CA ihre Funktion in der TI. Hierbei ist es unerheblich, ob die EE-Zertifikate durch die CA vorgängig gesperrt wurden oder nicht.

## **TIP1-A\_2061 - Entzug des Vertrauensstatus einer CA bei sicherheitskritischen Incidents**

Die TI-Plattform MUSS einer CA den Vertrauensstatus entziehen, wenn während des Gültigkeitszeitraumes des CA-Zertifikats Ereignisse eintreten, die eine Gewährleistung der technischen und/oder organisatorischen Sicherheit der CA hinsichtlich Registrierungs-, Erstellungs- und Sperrdienste nicht mehr ermöglichen oder auch nur substantiell in Frage stellen. Im Ergebnis MÜSSEN sowohl das CA-Zertifikat wie auch die darauf basierenden EE-Zertifikate bei einer Zertifikatsprüfung als ungültig ausgewiesen werden. [ $\leq$ ]

## **TIP1-A\_2062 - Entfernen von CA-Zertifikaten aus der TSL**

Der TSL-Dienst MUSS ein gesperrtes Aussteller-CA-Zertifikat je nach Weisung des Servicebetriebsverantwortlichen der TI-Plattform zum festgelegten Termin entweder (a) mit einem Sperrdatum versehen oder (b) aus der TSL entfernen und umgehend eine aktualisierte TSL publizieren. [ $\leq$ ]

## **Nicht-sicherheitskritischer Incident**

Neben den sicherheitskritischen Umständen, die einen Entzug der Zulassung in Verbindung mit einer sofortigen Entfernung einer betroffenen Aussteller-CA aus der TSL erfordern, gibt es weitere Kriterien, die zwar einen Entzug der Zulassung zur Folge haben, jedoch die Sicherheit von TI und deren Anwendungen nicht gefährden.

Mögliche Gründe, die zu einem nicht-sicherheitskritischen Incident führen (nicht abschließend):

- TSP-X.509 stellt den Betrieb gänzlich ein
- TSP-X.509 stellt den Betrieb der betreffenden CA ein
- Ungeplante Zerstörung des privaten CA-Schlüssels ohne Möglichkeit zur Rekonstruktion

Bei nonQES-CAs für HBA und SMC-B wird eine solche Sperrung gemäß Kompromissmodell (s. Kap. 2.4.2) umgesetzt, indem diese CAs in der TSL auf den Status „revoked“ gesetzt werden.

Andere nonQES-CAs stellen nach einem nicht-sicherheitskritischen Incident ebenfalls nicht mehr EE-Zertifikate aus, sie verbleiben aber als normal gültig („inaccord“) in der TSL, solange gültige Zertifikate im Umlauf sind und sicher statusgeprüft werden können. Die Einhaltung dieser Vorgabe wird organisatorisch gewährleistet.

#### **TIP1-A\_2064 - Entzug Vertrauensstatus einer CA bei nicht-sicherheitskritischen Incidents**

Die gematik MUSS einer CA den Vertrauensstatus entziehen, wenn während des Gültigkeitszeitraumes des CA-Zertifikats Ereignisse eintreten, die gegen die Zulassungsvorgaben verstoßen, nicht aber die Sicherheit der TI und Anwendungen in Frage stellen. Im Ergebnis werden die von dieser CA bereits ausgestellten EE-Zertifikate bei einer Zertifikatsprüfung weiterhin als gültig ausgewiesen, nicht jedoch neu ausgestellte EE-Zertifikate dieser CA.

[<=]

#### **TIP1-A\_2065 - Umgang mit widerrufenen CA-Zertifikaten in der TSL**

Der TSL-Dienst MUSS Aussteller-CA-Zertifikate, deren Zulassung durch die gematik aufgrund nicht-sicherheitskritischer Incidents widerrufen wurde, mit einem entsprechenden „revoked“-Status sowie dem Datum dieses Statuswechsels versehen und diese Angaben bis zum regulären Ablaufdatum des betreffenden CA-Zertifikates in der aktuellen TSL mitführen.

[<=]

#### **TIP1-A\_2066 - Verhinderung der Neuausstellung von EE-Zertifikaten bei Incidents**

Ein TSP-X.509nonQES MUSS ab dem Zeitpunkt der Feststellung eines nicht-sicherheitskritischen Incidents sicherstellen, dass von der betroffenen CA keine neuen EE-Zertifikate für den Einsatz in der TI ausgestellt werden.

[<=]

#### **TIP1-A\_2067 - Operabilität von EE-Zertifikaten widerrufener CAs**

TSP-X.509QES und TSP-X.509nonQES MÜSSEN sicherstellen, dass in den Fällen nicht-sicherheitskritischer Incidents bereits ausgegebene EE-Zertifikate weiterhin bis zu ihrem regulären Ablauf in der TI operabel bleiben. Hierbei MUSS er für diese Zertifikate weiterhin einen OCSP- und Sperrdienst in der vereinbarten Dienstgüte aufrecht erhalten.

[<=]

#### **TIP1-A\_2068 - Bewertung widerrufener CA-Zertifikate in der TSL**

Alle zertifikatsprüfenden Komponenten in der TI-Plattform MÜSSEN bei der Prüfung von Aussteller-CA-Zertifikaten in der TSL den Status überprüfen. Ist der „revoked“-Status gesetzt, MUSS die Prüfroutine anhand des zugehörigen Datums auswerten, ob das zu prüfende EE-Zertifikat nach dem Statuswechsel der CA ausgegeben wurde. In diesem Fall MUSS die Prüfung ein negatives Ergebnis zurückliefern. Liegt das Ausgabedatum des EE-Zertifikates vor dem Statuswechsel der CA auf „revoked“, MUSS das Aussteller-CA-Zertifikat als gültig zurückgemeldet werden.

[<=]

### **Übergreifende Festlegungen**

#### **TIP1-A\_2069 - Bestätigung des Widerrufs von CA-Zertifikaten in der TSL**

Bei dem Widerruf einer CA-Zulassung durch die gematik MUSS der betroffene TSP-X.509nonQES den Widerruf sowie die korrekte Durchführung der Auflagen (z. B. Sperrung von CA- und EE-Zertifikaten oder Sicherstellung des weiteren Betriebs von OCSP- und Sperrdienst) schriftlich gegenüber der gematik dokumentieren und die

852 Umsetzung bestätigen.  
853 [ $\leq$ ]

#### 854 2.3.3.6 Aktualisierung des Vertrauensraumes

855 Der TSL-Dienst publiziert periodisch eine neue TSL mit einer bestimmten Gültigkeitsdauer  
856 (siehe Abbildung 4). Dezentrale Komponenten, zentrale Dienste und Fachdienste müssen  
857 die jeweils aktuelle TSL herunterladen, um die Prüfung der Ausstellerzertifikate  
858 durchführen zu können. Die Abhängigkeit der Prüfergebnisse vom Alter der TSL ist in  
859 Abbildung 4 dargestellt.

#### 860 TIP1-A\_2070 - Regelmäßige Neu-Ausstellung der TSL

861 Der TSL-Dienst MUSS eine neue TSL regelmäßig in Abhängigkeit des „Gültig bis Datum“  
862 mit einer neuen Sequenznummer ausstellen, signieren und an den definierten  
863 Downloadpunkten bereitstellen – unabhängig davon, ob sich der Inhalt der TSL geändert  
864 hat oder nicht.  
865 [ $\leq$ ]

866 Änderungen im Inhalt der TSL können sich ergeben durch:

- 867 • Initiale Aufnahme eines TSP-X.509nonQES mit erstem CA-Zertifikat
- 868 • Aufnahme neuer CA-Zertifikate für einen bereits enthaltenen TSP-X.509nonQES
- 869 • Update bestehender Aussteller-CA-Zertifikate nach Ablauf deren  
870 Gültigkeitszeitraumes
- 871 • Wechsel des Status eines bestehenden Aussteller-CA-Zertifikates auf „revoked“  
872 wegen eines nicht-sicherheitskritischen Wegfalls der Zulassung für den TSP-  
873 X.509nonQES und die betreffende CA ab einem bestimmten Datum.
- 874 • Entfernen eines Aussteller-CA-Zertifikates im Status „revoked“ nach Ablauf des  
875 regulären Gültigkeitszeitraumes
- 876 • Entfernen eines Aussteller-CA-Zertifikats aufgrund eines sicherheitskritischen  
877 Incidents
- 878 • Aufnahme oder Entfernung von BNetzA-VL-Signerzertifikaten aufgrund  
879 Änderungen der EU-LOTL

#### 880 2.3.3.7 Vertrauensankerwechsel

881 Die TSL-Signer-CA als initialer Vertrauensanker der TSL – und damit der TI-PKI –  
882 unterliegt wie alle anderen CAs einem definierten Lifecycle sowie ungeplanten  
883 Randbedingungen, d.h. es müssen technische und organisatorische Prozesse konzipiert  
884 werden, für

- 885 • Wechsel des TSL-Signerzertifikates zum Ende des Gültigkeitszeitraums (incl.  
886 Wechsel der CA-Schlüssel)
- 887 • Wechsel des TSL-Signerzertifikates aufgrund Kompromittierung der CA-Schlüssel
- 888 • Wechsel von Algorithmen aufgrund der Entwicklung in der Kryptoanalyse

889 Der Wechsel des Vertrauensankers erfolgt über die TSL selbst. Das jeweils aktuelle TSL-  
890 Signer-CA-Zertifikat ist sowohl in den dezentralen Komponenten ausgerollt, wie auch als  
891 Eintrag in der TSL hinterlegt.

892 Ein Vertrauensankerwechsel stellt den Wechsel des TSL-Signer-CA-Zertifikates für einen  
893 TI-Vertrauensraum innerhalb einer Schlüsselgeneration (RSA oder ECDSA) dar. Ein  
894 Vertrauensankerwechsel zum Übergang (Migration) auf eine andere Schlüsselgeneration

895 muss über andere Mechanismen (Initialisierung eines neuen Vertrauensankers z.B. über  
896 Cross-Zertifikate) realisiert werden.

897 **TIP1-A\_2074 - Neuausstellung und Verteilung des Vertrauensankers**

898 Der TSL-Dienst MUSS rechtzeitig vor Ablauf des aktuellen TSL-Signer-CA-Zertifikates die  
899 Neuausstellung eines Folgezertifikates durchführen und dieses als „zukünftigen  
900 Vertrauensanker“ mittels der TSL an die zertifikatsprüfenden Komponenten verteilen.  
901 [ $\leq$ ]

902 **TIP1-A\_2075 - Import des neuen Vertrauensankers in Trust Store**

903 In der TI-Plattform MÜSSEN alle zertifikatsprüfenden Komponenten bei einem geplanten  
904 Wechsel des zentralen Vertrauensankers (TSL-Signer-CA-Zertifikat) bereits vor Ablauf  
905 des bestehenden Vertrauensankers das zukünftige Zertifikat in ihren lokalen Trust Store  
906 importieren und zum Aktivierungsdatum das alte mit dem neuen TSL-Signer-CA-  
907 Zertifikat ersetzen.  
908 [ $\leq$ ]

909 Ab dem Aktivierungsdatum werden die publizierten TSL dann mit einem TSL-  
910 Signerzertifikat signiert, das von der neuen TSL-Signer-CA ausgestellt wurde. Damit ist  
911 der Wechsel des Vertrauensankers abgeschlossen.

912 Im Falle einer Kompromittierung der CA-Schlüssel oder eines anderen Vorfalls, der eine  
913 sofortige Sperrung der TSL-Signer-CA erfordert, kann das oben beschriebene Verfahren  
914 nicht angewendet werden. Je nach Zeitpunkt des Bekanntwerdens ist in diesem Fall  
915 bereits die Authentizität der aktuellen oder der zukünftigen TSL selbst in Frage gestellt,  
916 so dass auch ein darin enthaltener „zukünftiger Vertrauensanker“ als nicht-authentisch  
917 verdächtig werden muss.

918 Als Lösung für diese Situation muss im gemäß [gemSpec\_DS\_Anbieter] geforderten  
919 Notfallkonzept für die jeweilige Komponente die Reinitialisierung des Vertrauensraumes  
920 in der Komponente durch einen organisatorisch-technischen Prozess ausgearbeitet  
921 werden. Je nach Bewertung des Incidents durch den Servicebetriebsverantwortlichen der  
922 TI-Plattform (SBV) können u. U. bestimmte PKI-Dienste nicht bereitstehen. Als Folge  
923 muss bspw. der operative Betrieb einer Arztpraxis oder eines Krankenhauses auf Basis  
924 der letzten publizierten TSL weitergeführt werden. In den betrieblichen Prozessen sind  
925 geeignete Maßnahmen zu definieren und über SLAs abzusichern, die eine Reinitialisierung  
926 innerhalb eines möglichst kurzen Zeitraums ermöglichen.

927 **2.3.4 Vertrauensmodell der nonQES TI-Zertifikate im Internet**

928 Zur Unterstützung der HBA- und SMC-B Karten im Internet müssen die TSP-X.509 eine  
929 Reihe von Leistungen sowohl innerhalb der TI wie auch zusätzlich im Internet  
930 bereitstellen.

931 **TIP1-A\_5130 - Unterstützung von HBA- und SMC-B Zertifikaten im Internet**

932 Die TI-Plattform MUSS geeignete Maßnahmen implementieren, um die Statusauskünfte  
933 für nonQES X.509-Zertifikate im Internet bereitzustellen und diese gesichert mit den  
934 Statusauskünften in der TI zu synchronisieren.  
935 [ $\leq$ ]

936 **2.3.5 Vertrauensmodell von Zertifikaten der HBA-Vorläuferkarten**  
937 **in der TI**

938 Zur Unterstützung der HBA-Vorläuferkarten qSIG- und ZOD-Karten auch innerhalb der TI  
939 müssen weitere Anforderungen berücksichtigt werden:

**TIP1-A\_5131 - CA-Zertifikate der HBA-Vorläuferkarten im TI-Vertrauensraum**

Die TI-Plattform MUSS die zugehörigen CA-Zertifikate sowie OCSP-Signatur-Zertifikate von zu unterstützenden HBA-Vorläuferkarten (qSIG, ZOD) unter Einhaltung eines geregelten Registrierungsverfahrens in den Vertrauensraum der TI aufnehmen.

[<=]

**TIP1-A\_5282 - OCSP-Auskünfte der HBA-Vorläuferkarten innerhalb der TI**

Die TI-Plattform MUSS die im Internet verfügbaren OCSP-Dienste von bereits zugelassenen Anbietern der HBA-Vorläuferkarten (qSIG-Karten, ZOD-Karten) innerhalb der TI verwenden.

[<=]

Die bereits im Internet etablierten PKIs der HBA-Vorläuferkarten (qSIG, ZOD), die im Rahmen des Bestandsschutzes zu unterstützen sind, werden in der TI insoweit berücksichtigt, dass die zugehörigen CAs in den TI-Vertrauensraum (also die TSL) aufgenommen und die im Internet verfügbaren Statusinformationen der zugehörigen EE-Zertifikate in der TI zur Verfügung gestellt werden.

**2.3.6 Vertrauensmodell CVC**

CV-Zertifikate dienen der gesicherten Card-to-Card-Authentisierung unabhängig von Online-Infrastrukturen. Vor diesem Hintergrund muss abweichend von dem Vertrauensmodell für X.509-Zertifikate der Vertrauensanker für CV-Zertifikate innerhalb der Karten selbst etabliert sein.

Karten der TI müssen über folgende CV-Ausstattung verfügen:

- mindestens ein CV-Schlüsselpaar mit zugeordnetem CV-Zertifikat. Es können mehrere Schlüsselpaare mit jeweils eigenem CV-Zertifikat und unterschiedlichen Profilattributen enthalten sein, die die Karte für unterschiedliche Funktionen in der TI-Anwendungslandschaft autorisieren können
- das CV-CA-Zertifikat der zweiten Ebene sowie
- der CV-Root-PuK als Vertrauensanker der C2C-Authentisierung

Anmerkung: Für die Kartengeneration 2 werden die CV-Zertifikate auf ECC-basierte Kryptographie umgestellt. Eine Cross-Zertifizierung, die üblicherweise benutzt wird, um die Verbindung zwischen zwei Zertifizierungsstellen herzustellen, kann nicht ohne Weiteres technologieübergreifend zwischen RSA-basierten und ECC-basierten Zertifikaten genutzt werden. Daher ist auch eine eigene, separate CVC-PKI für Kartengeneration 2 mit einer zweiten, separaten CVC-Root-CA notwendig.

**TIP1-A\_2077 - Umsetzung 2-stufiger CA-Hierarchie bei CVC-PKI**

Die TI-Plattform MUSS das Vertrauensmodell für die Card-to-Card-Authentisierung über eine CVC-PKI mit 2-stufiger CA-Hierarchie umsetzen.

[<=]

**TIP1-A\_5132 - Bereitstellung einer CVC-Root-CA zur Nutzung für G2-Karten**

Die TI-Plattform MUSS eine CVC-Root-CA betreiben, von der alle Sub-CAs zur Ausgabe von CV-Zertifikaten für G2-Karten (Verwendung in der TI) abgeleitet werden.

[<=]



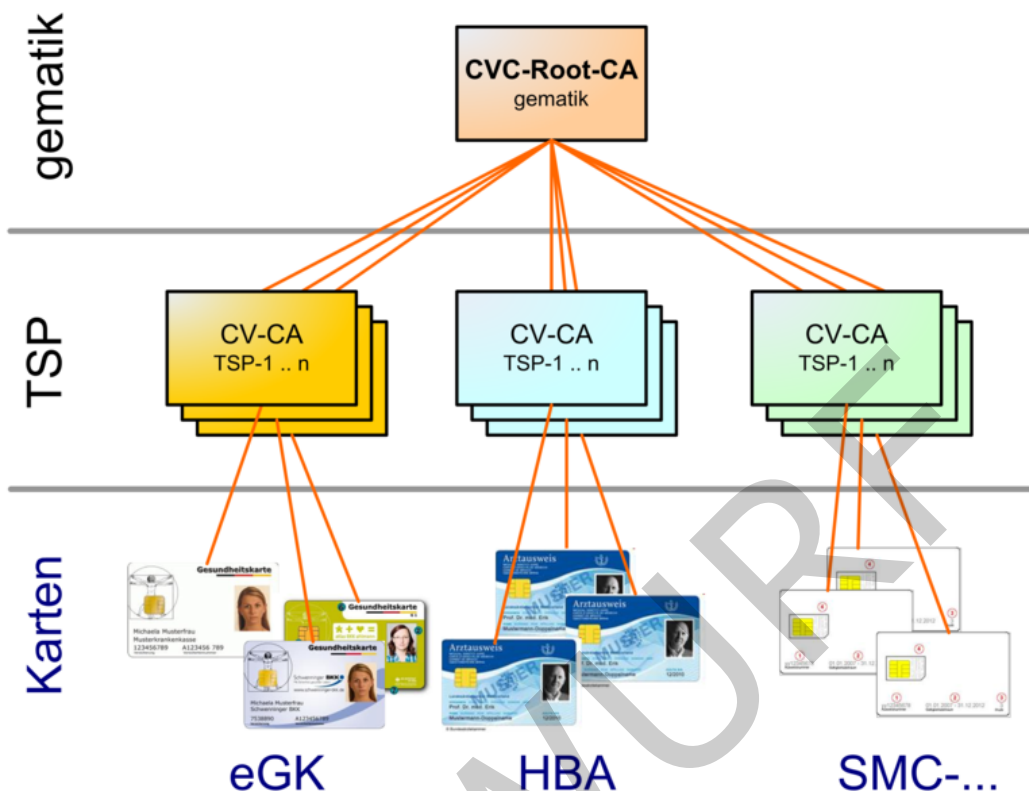


Abbildung 5: Hierarchie der CVC-PKI (je Kartengeneration)

## 2.4 Gültigkeitsmodelle X.509-Zertifikate

Geht es beim Vertrauensmodell darum, Zertifikate auf einen vertrauenswürdigen Anker oder gemeinsamen Vertrauensraum zurückzuführen, geht es beim Gültigkeitsmodell um die Feststellung, ob das Zertifikat in seiner Nutzung als gültig angesehen werden kann.

Zertifikate müssen zu einem bestimmten Prüfzeitpunkt gültig bzw. gültig gewesen sein, d. h., nicht gesperrt oder abgelaufen sein. Der Prüfzeitpunkt hängt vom verwendeten Gültigkeitsmodell ab. Üblicherweise wird die Gültigkeit von Signaturen zum Zwecke der Authentisierung zur aktuellen Jetzt-Zeit geprüft, während Signaturen für Dokumente auf den Zeitpunkt der Erstellung der Signatur geprüft werden.

### 2.4.1 PKIX-Schalenmodell

Gemäß PKI-Standard X.509 ist das Schalenmodell, auch PKIX-Modell genannt, standardisiert. Dabei müssen alle Zertifikate der Zertifikatskette zum Prüfzeitpunkt gültig sein. Jedes untergeordnete Zertifikat muss in seiner zeitlichen Gültigkeit innerhalb der Gültigkeit des übergeordneten Zertifikats sein, damit ein gültiger Zertifizierungspfad zustande kommen kann und die Prüfung mit einem positiven Gültig-Ergebnis abschließt.

Damit Root- und Aussteller-CAs über längere Perioden im Einsatz bleiben können, muss ihre Gültigkeitsdauer (Laufzeit) deutlich länger sein als diejenige der EE-Zertifikate.

Für die Nutzung in der TI reicht das Vorhandensein des Aussteller-CA-Zertifikats in der TSL als Nachweis der Vertrauenswürdigkeit aus. Die weitergehenden Prüfschritte bis zur

1004 Root-CA des Aussteller-CA-Zertifikates wurden vorgängig als Voraussetzung für die  
1005 Zulassung der Aussteller-CA erfolgreich durchgeführt.

1006 In der TI erfolgt die Gültigkeitsprüfung aller X.509-Zertifikate für Komponenten (Geräte  
1007 und Dienste) gemäß PKIX-Schalenmodell.

1008 Auch die nonQES-X.509-Zertifikate der eGK werden nach PKIX-Schalenmodell geprüft.

### 1009 **2.4.2 Kompromissmodell**

1010 Für sämtliche nonQES-X.509-Zertifikate des HBA sowie der SMC-B gilt einheitlich das  
1011 Gültigkeitsmodell nach dem sog. Kompromissmodell [baekValidityModel], in dem nach  
1012 dem Kettenmodell geprüft wird, jedoch die Gültigkeitszeiträume der Zertifikate nach dem  
1013 Schalenmodell gesetzt werden.

1014 Zur TI-spezifischen Sperrung von CA-Zertifikaten gemäß Ketten- oder Kompromissmodell  
1015 siehe Kapitel 2.3.3.5 „Sperrung von CA-Zertifikaten in der TSL“.

### 1016 **2.4.3 QES-Kettenmodell**

1017 Bei der Prüfung von qualifizierten elektronischen Signaturen (QES) ist innerhalb der TI  
1018 der Zeitpunkt der Signaturerstellung entscheidend. Zu diesem Zeitpunkt MUSS das  
1019 verwendete qualifizierte EE-Zertifikat gültig gewesen sein (vgl. [eIDAS] Art. 32 Absatz  
1020 1b). Diese Voraussetzung ist bereits gegeben, wenn zum Zeitpunkt der Ausstellung des  
1021 EE-Zertifikates die übergeordneten Aussteller-CA-Zertifikate gültig waren.

1022 Die Signatur mit einem in diesem Sinne gültigen EE-Zertifikat ist somit gültig, auch wenn  
1023 zum Signaturzeitpunkt die Aussteller-Sub-CA bereits zeitlich abgelaufen oder gesperrt  
1024 sind – aber zum Zeitpunkt der Erstellung des EE-Zertifikates noch gültig waren.

1025 Zur TI-spezifischen Sperrung von CA-Zertifikaten gemäß Ketten- oder Kompromissmodell  
1026 siehe Kapitel 2.3.3.5 „Sperrung von CA-Zertifikaten in der TSL“.

## 1027 **2.5 Zertifikatstypen in der TI und deren Verwendung**

### 1028 **2.5.1 X.509-Zertifikate für Identitäten der TI**

- 1029 • QES-Zertifikate zur Nutzung von QES (zur verbesserten Beweiseignung der  
1030 Dokumente) mit dem HBA und als optionale Nutzung mit der eGK.
- 1031 • Signaturzertifikate (SIG) zur Signatur von Informationsobjekten mit  
1032 Sicherheitsfunktionen in der TI (bspw. TSL, OCSP-Response, Code-Signatur,  
1033 Signatur von Zertifikaten durch ausstellende CA)
- 1034 • Signaturzertifikate (AUT, AUTN, AUT\_ALT) zur Sicherstellung von Integrität und  
1035 Authentizität im nicht-qualifizierten Kontext der Identitäten für Personen,  
1036 Organisationen und Komponenten
- 1037 • Verschlüsselungszertifikate (ENC, ENCV) für Ver- und Entschlüsselung  
1038 identitätsbezogener Daten für Personen, Organisationen und Komponenten

### 1039 **TIP1-A\_4451 - Bereitstellung von X.509-Zertifikaten durch TSP-X.509**

1040 Die TI-Plattform MUSS TSPs bereitstellen, die nonQES-X.509-Zertifikate ausgeben und  
1041 die dafür notwendigen Prozesse und Schnittstellen anbieten.

1042 [**<=**]



**TIP1-A\_5133 - HBA- und SMC-B CA-Statusinformationen im Internet**

Die gematik Root-CA MUSS CA-Statusinformationen für folgende Zertifikate

- (a) C.HP.AUT,
- (b) C.HP.ENC,
- (c) C.HCI.AUT,
- (d) C.HCI.ENC sowie C.HCI.OSIG

in einem OCSP-Dienst im Internet zur Verfügung stellen.

[<=]

**TIP1-A\_5141 - Bereitstellung CA-Zertifikate und Fingerprints im Internet**

Die gematik Root-CA MUSS CA-Zertifikate sowie deren Fingerprint (für Zertifikate, die im Internet prüfbar sein müssen) im Internet zur Verfügung stellen.

[<=]

**TIP1-A\_5134 - HBA- und SMC-B Statusinformationen im Internet**

Ein TSP-X.509 nonQES MUSS die Statusinformationen für folgende Zertifikate

- (a) C.HP.AUT,
- (b) C.HP.ENC,
- (c) C.HCI.AUT,
- (d) C.HCI.ENC sowie C.HCI.OSIG in einem OCSP-Dienst im Internet zur Verfügung stellen.

[<=]

**TIP1-A\_2436 - Gültigkeitsdauer der X.509-Zertifikate**

Die TI-Plattform MUSS für alle in der TI verwendeten X.509-Zertifikate einen Gültigkeitszeitraum in Form eines kalendarischen Datums „Nicht zu verwenden vor“ und „Nicht mehr verwenden nach“ zur Verfügung stellen.

[<=]

**TIP1-A\_4452 - Sperrung von Karten durch Sperrung der X.509-Zertifikate**

Die TI-Plattform MUSS die Sperrung von in der TI verwendeten Smartcards über die Sperrung der darauf befindlichen X.509-Zertifikate umsetzen.

[<=]

**TIP1-A\_2437 - Sperrung von X.509-Zertifikaten**

Die TI-Plattform MUSS für alle in der TI verwendeten X.509-Zertifikate, für die aus dem Anwendungskontext eine Statusprüfung gefordert ist, die Verfügbarkeit von Sperrprozessen und Statusauskünften sicherstellen, einschließlich der erforderlichen technischen und organisatorischen Schnittstellen.

[<=]

Die X.509-Zertifikate enthalten entsprechend ihres Einsatzbereiches unterschiedliche Verwendungszwecke. Die Ausprägung des Verwendungszwecks wird in den Zertifikatsprofilen beschrieben, die erlaubten Verwendungszwecke werden in der Policy definiert.

**TIP1-A\_2490 - Verwendungszweck von X.509-Zertifikaten**

Ein TSP-X.509 MUSS sicherstellen, dass jedes für den Einsatz in der TI ausgestellte X.509-Zertifikat einen Verwendungszweck gemäß [RFC5280] enthält.

[<=]

**2.5.2 CV-Zertifikate für Karten in der TI**

- Zertifikate für Card-to-Card-Authentisierung und Autorisierung zwischen eGK und SMC-B, HBA sowie KTR-AdV (CV-Rollenzertifikate)

- 1090 • Zertifikate für Card-to-Card-Authentisierung und Autorisierung für
- 1091 gerätespezifische Funktionen (gSMC-K, gSMC-KT, SMC-B, HBA – CV-
- 1092 Gerätezertifikate)

## 1093 2.6 Verantwortliche Instanzen

1094 Abbildung 6: Zuordnung der Verantwortlichkeiten für die Zertifikate zeigt die Aufteilung  
 1095 in sogenannte Verantwortungsdomänen (mögliche optionale Ausprägungsformen von  
 1096 Identitäten und Zertifikaten sind nicht berücksichtigt).

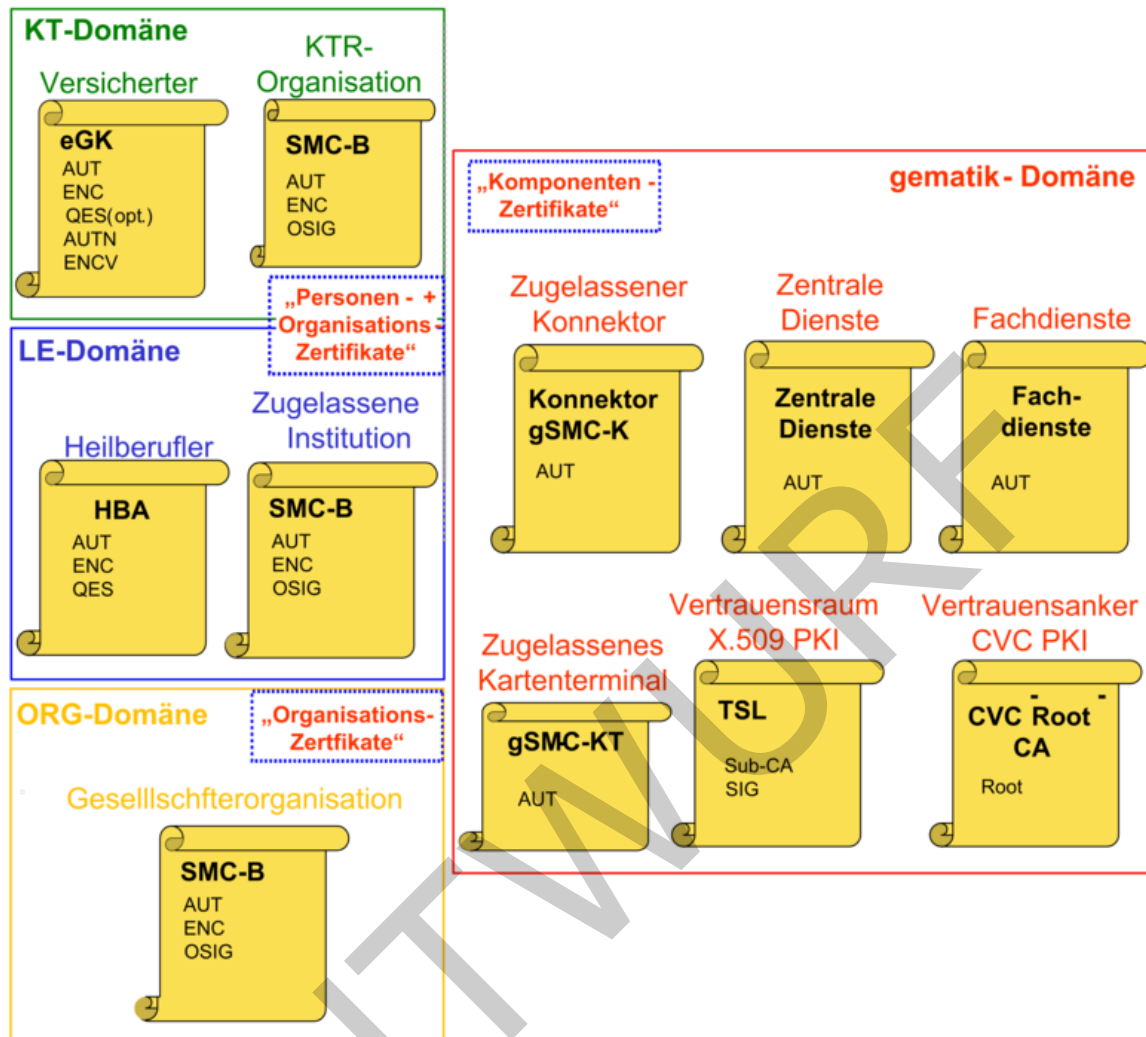
### 1097 **TIP1-A\_2081 - Spezifikation von Komponenten- und Dienstzertifikaten**

1098 Die TI-Plattform MUSS Zertifikate für Komponenten, zentrale Dienste und  
 1099 fachanwendungsspezifische Dienste sowie für Root-CAs, Aussteller-CA-Zertifikate sowie  
 1100 daraus abgeleitete EE-Zertifikate bereitstellen.

1101 [ $\leq$ ]

1102 Anmerkung zu SMC-B: Im Dokument wird der Begriff SMC-B übergreifend verwendet, um  
 1103 damit sowohl die Ausprägung als Karte (SMC-B) als auch die Ausprägung mittels eines  
 1104 HSM, das sogenannte HSM-B, zu beschreiben. Die HSM-B kann in Szenarien zum Einsatz  
 1105 kommen, in denen die Performance von Chipkarten nicht ausreichend ist, bspw. in  
 1106 Krankenhäusern. Funktional muss ein HSM-B vollständig einer SMC-B entsprechen, d. h.  
 1107 sowohl hinsichtlich CV-Zertifikaten wie auch hinsichtlich X.509-Zertifikaten.

1108



1109

1110

1111

Abbildung 6: Zuordnung der Verantwortlichkeiten für die Zertifikate

**TIP1-A\_2084 - Vorgaben für HSM-B als SMC-B Ersatz**

Ein HSM-B MUSS funktional vollständig eine (oder mehrere) SMC-B abbilden können, d. h. sich aus Sicht der Primäranwendung hinsichtlich CV- und X.509-Zertifikaten verhalten wie eine (hochperformante) SMC-B.

[&lt;=]

**2.7 Teilnehmer in der PKI**

Die Teilnehmer und deren Aufgaben werden beschrieben. Den Teilnehmern können Rollen zugewiesen werden. Die Rollendefinition und -zuordnung selbst sind nicht Gegenstand dieses Abschnittes.

**2.7.1 Trust Service Provider (TSP)**

Trust Service Provider (TSP) stellen für den Einsatz in der Telematikinfrastruktur X.509- und CV-Zertifikate aus für natürliche und juristische Personen sowie für zentrale Dienste,

1124 fachanwendungsspezifische Dienste und technische Komponenten. Neben anderen  
1125 Aufgaben sind TSP somit immer auch Zertifikatsherausgeber.

1126 In [gemKPT\_Arch\_TIP] sind als TSP-Produkttypen definiert:

- 1127 • gematik Root-CA
- 1128 • TSP-X.509QES (auch als VDA für QES bezeichnet)
- 1129 • TSP-X.509nonQES
- 1130 • TSP-CVC
- 1131 • CVC-Root-CA

1132 Folgende Namenskonvention gilt für TSP als Adressaten für spezifische Anforderungen,  
1133 die im vorliegenden Konzept definiert werden:

- 1134 • TSP  
1135 Gesamtheit aller TSP, die Zertifikate in irgendeiner Form herausgeben und/oder  
1136 zertifikatsrelevante Dienste betreiben (Produkttypen 1) 2) 3) 4) und 5))
- 1137 • TSP-X.509  
1138 Übergreifende Bezeichnung für alle Herausgeber von X.509-Zertifikaten  
1139 (Produkttypen 1) 2) und 3))

### 1140 **TIP1-A\_2085 - Forderung nach CP und CPS des TSP**

1141 Ein TSP-X.509 MUSS Festlegungen für Identifizierung, Registrierung, Herausgabe,  
1142 Verlängerung und Sperrung von Zertifikaten in seiner Certificate Policy (CP) und seinem  
1143 Certification Practice Statement (CPS) treffen sowie technisch und organisatorisch  
1144 umsetzen, wobei seine Certificate Policy nicht im Widerspruch zur übergreifenden  
1145 Certificate Policy der gematik bzw. der gemeinsamen HPC-Policy (für HBA-Zertifikate)  
1146 stehen darf.

1147 [ $\leq$ ]

### 1148 **TIP1-A\_2086 - Zulassung von TSPs und Nachweis der Sicherheit**

1149 Ein TSP MUSS durch die gematik zugelassen sein, um in der TI Zertifikate herausgeben  
1150 zu dürfen und muss dafür die Umsetzung der für ihn geltenden Sicherheitsanforderungen  
1151 in einem Sicherheitskonzept beschreiben.

1152 [ $\leq$ ]

1153 In bestimmten Fällen sind einige der Zertifikatsprofile für einen TSP optional, wie z.B. die  
1154 alternativen Versichertenidentitäten für den TSP-X.509 nonQES eGK. Die Realisierung der  
1155 optionalen Zertifikatsprofile wird im Rahmen des Zulassungsverfahrens festgelegt.

1156

### 1157 **TIP1-A\_4453 - Sektorspezifische Zulassung von TSPs**

1158 TSP-X.509QES und TSP-X.509nonQES für Zertifikate der Leistungserbringer MÜSSEN  
1159 eine sektorspezifische Zulassung erfolgreich durchlaufen haben, um in der TI Zertifikate  
1160 herausgeben zu dürfen. Diese sektorspezifische Zulassung MUSS mindestens folgende  
1161 Inhalte umfassen:

- 1162 (1) Antrags- und Ausgabeprozess,
- 1163 (2) Bestätigung der Sektorattribute,
- 1164 (3) Produktionsfreigabe.

1165 [ $\leq$ ]

1166 TSP stehen mit den verantwortlichen Kartenherausgebern in enger Zusammenarbeit  
1167 (s. a. Kapitel 2.7.3.1). Zusätzlich zu der Erfüllung der Sicherheitsanforderungen muss der  
1168 TSP von der für die jeweiligen Zertifikate zuständigen Organisation für die Eintragung  
1169 von bestimmten Rollen in X.509- bzw. eines bestimmten Profils in die CV-Zertifikate

berechtigt werden. Die für die jeweiligen Berufs- bzw. Institutionsbezeichnungen zuständigen Organisationen legen Bedingungen für die Berechtigungserteilung fest.

Ein TSP-X.509 erstellt im Auftrag in der TI genutzte nonQES- bzw. QES-Zertifikate.

#### **TIP1-A\_2089 - Grundaufgaben des TSP im Rahmen des Zertifikats-Lebenszyklus**

In der Rolle als Zertifikatsherausgeber MUSS ein TSP-X.509QES oder ein TSP-X.509nonQES in seinem Verantwortungsbereich

(a) die eindeutige Zuordnung von Zertifikaten zu Personen, zu ihren Rollen in der TI und zu Institutionen organisatorisch sicherstellen,

(b) die Endnutzerzertifikate sicher gemäß den für ihn geltenden

Sicherheitsanforderungen erzeugen und dem Zertifikatsnutzer bereitstellen,

(c) für die identitätsbezogenen Endnutzerzertifikate die Zertifikatsantragsteller sicher gemäß den für ihn geltenden Sicherheitsanforderungen registrieren und dazu

dokumentierte Registrierungsprozesse implementieren,

(d) für die identitätsbezogenen Endnutzerzertifikate den Zertifikatsnehmern gemäß den für ihn geltenden Sicherheitsanforderungen die Möglichkeit zur Sperrung ihrer Zertifikate anbieten und dazu dokumentierte Sperrprozesse implementieren.

[<=]

#### **TIP1-A\_2090 - Einbringung der Telematik-ID in HBA/SMC-B gemäß Profil**

Wird ein TSP-X.509QES und TSP-X.509nonQES zur Zertifikatserstellung für HBA bzw. SMC-B beauftragt, MUSS er die dem Antragsteller zugeordnete Telematik-ID in das dafür laut Zertifikatsprofil vorgesehene Feld der X.509-Zertifikate für HBA bzw. SMC-B speichern.

[<=]

#### **TIP1-A\_2091 - Einbringung der KVNR in eGK und alternative Versichertenidentitäten gemäß Profil**

Wird ein TSP-X.509QES und TSP-X.509nonQES zur Zertifikatserstellung für die eGK oder die alternativen Versichertenidentitäten beauftragt, MUSS er die dem Antragsteller zugeordnete Krankenversicherungsnummer in das dafür laut Zertifikatsprofil vorgesehene Feld der X.509-Zertifikate für die eGK speichern.

[<=]

Die Vergabe und Zuordnung von Telematik-ID und Krankenversicherungsnummer zu Akteuren und die Nutzung dieser IDs werden im Abschnitt 2.8 beschrieben.

### **2.7.2 Registrierungsstellen**

Registrierungsstellen führen die Registrierungen von Zertifikatsnehmern durch, d. h. sie prüfen die eingereichten Zertifikatsanträge, erfassen deren Daten zur Zertifikatserstellung, archivieren die Anträge über definierte Zeiträume. Weiterhin nehmen die Registrierungsstellen auch Sperranträge entgegen, veranlassen die operative Sperrung von Zertifikaten und betreiben eine Hotline für die von ihnen bereitgestellten Dienste.

Registrierungsstellen bilden die Kundenschnittstelle einer PKI zu den Zertifikatsnehmern.

### **2.7.3 Kartenherausgeber**

Kartenherausgeber (Gesellschafterorganisationen (ORG), Leistungserbringerorganisationen (LEOs), Kostenträger (KTR) und Gerätehersteller) sind

1215 für die Herausgabe von eGK, HBA, SMC-B, gSMC-K und gSMC-KT zuständig. Die gematik  
1216 ist für die Herausgabe von Prüfkarten zuständig.

1217 **TIP1-A\_2094 - Rollenautorisierung von TSP durch Kartenherausgeber**

1218 Die Kartenherausgeber MÜSSEN die von ihnen beauftragten TSP (im Falle von eGK,  
1219 gSMC-K und gSMC-KT) bzw. zugelassenen TSP (im Falle von SMC-B und HBA) bzgl. der  
1220 Einbringung von Zertifikatsattributen für Rollen (Zugriffsprofile) in die Zertifikate  
1221 autorisieren.

1222 [ $\leq$ ]

1223 **TIP1-A\_2098 - Umsetzung von Sperraufträgen durch Berechtigte**

1224 TSP-X.509QES und TSP-X.509nonQES MÜSSEN für die von ihm herausgegebenen  
1225 Zertifikate Sperraufträge umsetzen, unter Anwendung der Berechtigungen gemäß  
1226 Tab\_PKI\_107 sowie nach Authentifizierung und Berechtigungsprüfung der  
1227 beauftragenden Person oder Organisationseinheit.

1228 [ $\leq$ ]

1229

1230 **Tabelle 1: Tab\_PKI\_107 Übersicht der PKI-spezifischen Sperrgründe**

Sperrberechtigte Stellen *)	Zertifikate der Kartenarten									
			HBA	HBA	SMC-B	SMC-B	SMC-B	SMC-B		
	Prüfkarte eGK	eGK (**)	QES	non-QES	LEI	ORG	KTR	KTR-AdV	gSMC-K	FD, ZD
LE			1a	1a	1a					
med. Institution					1a					
Hersteller									1b	
Anbieter **)										1b, 3
Herausgebende LEO **) ****)			2,5	2,5	2,5	2				
Zertifikatsnehmende LEO **) ****)						1a				
GKV-Spitzenverband **)						1a	2			
KTR **)		1a, 2					1a	2		
gematik	1a		3	3	3	3	3	3	1c,3	1c,3
BNetzA			4							

- 1231 1a) Jederzeit ohne Angabe von Gründen
- 1232 1b) Eventgetriggert im Rahmen eines definierten Incident-Prozesses mit den zuständigen  
1233 und betroffenen Parteien
- 1234 1c) Jederzeit ohne Angabe von Gründen für Zertifikate, die für den Produkttyp Service  
1235 Monitoring erstellt wurden
- 1236 2) Wegfall oder Entzug geforderter Eigenschaften des Antragstellers gemäß  
1237 Ausgabepolicy
- 1238 3) Wegfall oder Entzug geforderter Eigenschaften des TSP gemäß gematik-Zulassung
- 1239 4) Verlust des Qualifikationsstatus des VDA für QES gemäß [eIDAS]
- 1240 5) Wegfall oder Entzug geforderter Eigenschaften des VDA für QES /TSP gemäß Sektor-  
1241 Zulassung
- 1242
- 1243 \*) Berechtigung für organisatorische Sperrungen gilt nur für den jeweiligen Herausgeber  
1244 der Zertifikate
- 1245 \*\*) In herausgeberspezifischen Policies können weitere Sperrgründe definiert sein.
- 1246 \*\*\*) incl. alternative Versichertenidentitäten
- 1247 \*\*\*\*) Wenn bei einer SMC-B ORG die herausgebende LEO identisch mit der  
1248 zertifikatsnehmenden LEO ist, so kann sie ihre eigenen Zertifikate jederzeit ohne Angabe  
1249 von Gründen sperren.

1250

## 1251 **TIP1-A\_2099 - Beschreibung von Herausgabeprozessen in Ausgabepolicy**

1252 Der Kartenherausgeber MUSS für die Beantragung, Herausgabe und Sperrung der in  
1253 seinem Verantwortungsbereich befindlichen Karten und deren Zertifikate die dafür  
1254 notwendigen Prozesse in einer Ausgabepolicy beschreiben und deren Umsetzung  
1255 sicherstellen.

1256 [ $\leq$ ]

## 1257 **TIP1-A\_2100 - Verfahrensimplementierung zur Berechtigungsprüfung**

1258 TSP-X.509QES und TSP-X.509nonQES MÜSSEN die vom Kartenherausgeber  
1259 vorgegebenen technischen und organisatorischen Verfahren implementieren, um die  
1260 Berechtigung von Antragstellern für Sperraufträge nach den Regularien der  
1261 Ausgabepolicy der betreffenden Zertifikate nachvollziehbar prüfen zu können.

1262 [ $\leq$ ]

1263 Kartenherausgeber haben je nach Kartenart unterschiedliche Aufgaben.

## 1264 **2.7.3.1 HBA-Herausgeber**

1265 Die Herausgabe von HBA und HBA-Zertifikaten liegt gemäß des Landesheilverberufsgesetzes  
1266 im Verantwortungsbereich der Kammer auf Landesebene.

1267 Im Kontext der TI wird der Sammelbegriff „Leistungserbringerorganisation (LEO)“  
1268 verwendet.

## 1269 **TIP1-A\_2103 - Prüfung der Berufsgruppenzugehörigkeit**

1270 Der Herausgeber des HBA MUSS die Zugehörigkeit des Antragstellers zu einer  
1271 bestimmten Berufsgruppe (wie z. B. „Ärztin/Arzt“, „Apotheker/Apothekerin“) prüfen und  
1272 dem TSP übermitteln, damit dieser die Information in den Zertifikaten speichert.

1273 [ $\leq$ ]

1274 Es gelten die folgenden Verantwortungsbereiche:



- 1275 • Landesärztekammern (bzw. auch Bezirksärztekammern in Rheinland-Pfalz) sind  
1276 verantwortlich für die Herausgabe des HBA für Ärzte (inklusive ärztliche  
1277 Psychotherapeuten),
- 1278 • LZÄK für Zahnärzte
- 1279 • LAK für Akteure im Apotheken- und Pharmaziebereich,
- 1280 • Bundespsychotherapeutenkammer (BPTK) für nicht-ärztliche Psychotherapeuten,  
1281 d. h.
- 1282 • Psychologische Psychotherapeuten sowie
- 1283 • Kinder- und Jugendlichen-Psychotherapeuten
- 1284 • eGBR für sonstige Berufe der medizinischen Versorgung, Notfallversorgung und  
1285 der Versorgung mit Heil- und Hilfsmitteln

### 1286 **2.7.3.2 eGK-Herausgeber**

1287 Die Kostenträger sind für die eGK-Herausgabe verantwortlich.

1288 Jeder Versicherte erhält im Rahmen des Versicherungsverhältnisses eine eGK, der eine  
1289 eindeutige ID durch bereits definierte und genutzte Verfahren zugeordnet ist.

1290 Darüber hinaus kann jeder Versicherte auf Antrag alternative Versichertenidentitäten  
1291 erhalten. Diese sind für bestimmte Fachanwendungen (derzeit nur für ePA vorgesehen)  
1292 alternativ zur eGK verwendbar. Im Rahmen der gematik-Spezifikationen werden die  
1293 alternativen Versichertenidentitäten ebenfalls der Kartenart eGK zugeordnet.

### 1294 **2.7.3.3 Herausgeber der SMC-B**

1295 Herausgabe und Erstellung von SMC-B erfolgen in der Verantwortungsdomäne der  
1296 jeweiligen Sektororganisationen und von Kostenträgern, die jeweils auch für die  
1297 eindeutige Identifizierung der Institutionen und deren Zuordnung zu einer bestimmten  
1298 SMC-B verantwortlich sind.

1299 Zu unterscheiden sind dabei drei Ausprägungen der SMC-B:

- 1300 • SMC-B einer Gesellschafterorganisation  
1301 (Diese erlaubt keinen Zugriff auf eGKs)
- 1302 • SMC-B einer medizinischen Institution bzw. Leistungserbringerinstitution
- 1303 • SMC-B eines Kostenträgers

1304 Die Verantwortung für die Herausgabe der SMC-B ORG als spezielle Form der SMC-B für  
1305 Gesellschafterorganisationen ist im gesonderten Dokument [gemRL\_SMC-B\_ORG\_BP]  
1306 beschrieben.

1307

1308 Die Herausgabe der SMC-B des Krankenhaussektors liegt im Verantwortungsbereich der  
1309 Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH (DKTIG).

1310 Verantwortlich für die Herausgabe der SMC-B der anderen Sektoren sind:

- 1311 • Kassenärztliche Vereinigungen (KVen) für die Betriebsstätten ihrer Mitglieder:
- 1312 • Betriebstätte Vertragsarzt (inklusive ärztliche Psychotherapeuten) mit  
1313 Zulassung gemäß [Ärzte-ZV] oder
- 1314 • Betriebstätte nicht-ärztlicher Vertragspsychotherapeut mit Zulassung gemäß  
1315 [Ärzte-ZV]

- 1316 • Für den jeweiligen Vertragszahnarzt/Vertragszahnarztpraxis zuständige KZV:  
1317 Zahnarztpraxis mit vertragszahnärztlicher Zulassung (die jeweils zuständige KZV  
1318 ist zudem berechtigt, auch SMC-B für Zahnärzte auszugeben, die sich im  
1319 Zulassungsverfahren zur vertragszahnärztlichen Zulassung befinden). Die  
1320 abschließenden Regelungen zur Antragsberechtigung werden von der jeweils  
1321 zuständigen KZV festgelegt. Die TSP-Sektorzulassung im Bereich  
1322 Vertragszahnärzteschaft für SMC-B Profil 2ZA wird von der KZBV durchgeführt.
- 1323 • Offen: ausschließlich privatabrechnende Ärzte
- 1324 • BZÄK: Zahnarztpraxis privat
- 1325 • Für den jeweiligen Betriebserlaubnisinhaber zuständige Apothekerkammer.
- 1326 • GKV-Spitzenverband: Betriebsstätten bzw. Geschäftsstellen der Kostenträger  
1327 (gesetzlich),
- 1328 • Kostenträger für AdV in Umgebungen in ihrem Auftrag (KTR-AdV)

#### 1329 **2.7.3.4 Herausgeber von gSMC-K und gSMC-KT**

1330 Gerätehersteller sind für die Herausgabe von gerätebezogenen Sicherheitsmodulen  
1331 (gSMC-K, gSMC-KT) zuständig. Sie veranlassen die Erstellung und Herausgabe einer  
1332 gSMC-K bzw. gSMC-KT. Zu Geräteherstellern gehören beispielsweise  
1333 Kartenterminalhersteller.

#### 1334 **2.7.3.5 Herausgeber von Prüfkarten**

1335 Die gematik ist für die Herausgabe von Prüfkarten eGK verantwortlich. Eine Prüfkarte  
1336 eGK ist keinem Versicherten zugeordnet. Sie wird für eine fiktive Person ausgestellt und  
1337 ausschließlich im Rahmen eines Installationstests verwendet. Informationen zur  
1338 Personalisierung befinden sich im Dokument [gemSpec\_PK\_eGK].

#### 1340 **A\_13539 - Auditrecht für Herausgabeprozesse der Prüfkarten**

1341 Der Kartenherausgeber von Prüfkarten eGK MUSS dem GKV-Spitzenverband als  
1342 Eigentümer des Test.IK (welche auf einer Prüfkarte eGK das Institutionskennzeichen  
1343 eines realen Kostenträger ersetzt) ein Auditrecht auf die Prozesse zur Herausgabe der  
1344 Prüfkarte eGK gewähren.[<=]

#### 1345 **2.7.4 Anbieter TSL-Dienst**

1346 Die technische Umsetzung zur Bereitstellung der TSL mittels TSL-Dienst erfolgt durch  
1347 den Anbieter des TSL-Dienstes. Seine Aufgaben umfassen die Erzeugung, Verwaltung  
1348 und Veröffentlichung der TSL im Rahmen eines TSL-Dienstes (s.a. Abschnitt 2.3.2).

#### 1349 **2.7.5 Zertifikatsantragsteller**

1350 Antragsteller ist immer eine natürliche Person, die entweder für sich selbst oder für eine  
1351 juristische Person, für die sie vertretungsberechtigt ist, einen Zertifikatsantrag bei einem  
1352 TSP stellt.

1353 Die folgenden Akteure sind Beispiele für die oben genannten natürlichen oder juristischen  
1354 Personen:

- 1355 • Gesellschafterorganisationen,

- 1356 • Leistungserbringer,
- 1357 • medizinische Institutionen,
- 1358 • Kostenträger,
- 1359 • Gerätehersteller,
- 1360 • Diensteanbieter.

### 1361 **TIP1-A\_4454 - Einbringung registrierter Zulassungsdaten in X.509-Zertifikate**

1362 Die TI-Plattform MUSS sicherstellen, dass Zertifikatsantragsteller, die eine Zulassung  
1363 durchlaufen, die im Rahmen der Zulassung registrierten relevanten Daten in die  
1364 Zertifikate einbringen lassen.  
1365 [ $\leq$ ]

## 1366 **2.7.6 Zertifikatsnehmer**

1367 Zertifikatsnehmer sind natürliche und juristische Personen sowie zentrale Dienste,  
1368 fachanwendungsspezifische Dienste und technische Komponenten, für die ein TSP-  
1369 X.509QES und TSP-X.509nonQES Zertifikate ausstellt.

1370 Bei personenbezogenen Zertifikaten sind Antragsteller und Zertifikatsnehmer identisch.

1371 Bei organisations- bzw. gerätebezogenen Zertifikaten können Antragsteller und  
1372 Zertifikatsnehmer verschieden sein, wie das folgende Beispiel zeigt. Im Krankenhaus-  
1373 Sektor ist die juristische Person Krankenhaus der Zertifikatsnehmer, weil für sie die  
1374 Zertifikate auf der SMC-B ausgestellt werden. Der Antragsteller ist eine natürliche  
1375 Person, die bei der Antragstellung über die dieser Person zustehende Vertretungsmacht  
1376 für das Krankenhaus verfügt.

## 1377 **2.7.7 Zertifikatsnutzer**

1378 Der Zertifikatsnutzer nutzt Zertifikate anderer Zertifikatsnehmer, bspw. im Rahmen einer  
1379 Signaturprüfung. Er vertraut dabei – in den Grenzen der zugehörigen Ausgabepolicy –  
1380 auf die Gültigkeit der Zertifikatsinhalte. Dazu muss der Zertifikatsnutzer selbst kein  
1381 Zertifikat besitzen. Deshalb gelten für ihn gesonderte Festlegungen in der Policy.

## 1382 **2.7.8 gematik**

1383 Die gematik fungiert als Zulassungsinstanz für TSP sowie für den Anbieter des TSL-  
1384 Dienstes und legt die Sicherheitsanforderungen fest.

1385 In Aufgabenteilung und engen Absprachen mit den Leistungserbringerorganisationen und  
1386 Kostenträgern spezifiziert die gematik X.509- und CV-Zertifikate für den Einsatz in der  
1387 TI.

## 1388 **2.7.9 Andere Teilnehmer**

### 1389 **2.7.9.1 Rollenvergabestelle**

1390 In personenbezogenen bzw. institutionsbezogenen Zertifikaten wird die fachliche Rolle  
1391 (eine oder mehrere) eines Antragstellers im Zertifikat durch den entsprechenden Object  
1392 Identifier (OID), die Berufs- bzw. Institutionsbezeichnung sowie die Bezeichnung der  
1393 berufsattributbestätigenden Stelle beschrieben.

1394 Die Sicherstellung der TI-weit eindeutigen Zuordnung von berufsfachlichen Rollen und  
1395 deren Berechtigungen zu den technisch in den Zertifikaten verwendeten Rollenattributen  
1396 obliegt der Rollenvergabestelle, die diese Aufgabe in Zusammenarbeit mit den  
1397 Teilnehmerorganisationen umsetzt.

1398 **TIP1-A\_2110 - Definition eines Systems für Rollenattribute**

1399 Die TI-Plattform MUSS ein System für Rollenattribute und den Zugriff auf diese  
1400 definieren.

1401 [ $\leq$ ]

1402 **TIP1-A\_2111 - Definition und Koordination von Rollen für Akteure**

1403 Die Rollenvergabestelle MUSS die Definition der Rollen für technische und fachliche  
1404 Akteure der TI mit den Teilnehmerorganisationen LEO, Kostenträger und gematik  
1405 koordinieren und in eindeutige Rollenbezeichnungen überführen.

1406 [ $\leq$ ]

1407 **TIP1-A\_2112 - Überführung von Rollen in OIDs**

1408 Die Rollenvergabestelle MUSS die vereinbarten Rollen mittels eines Registrars in  
1409 eindeutige OIDs überführen und diese in der TI verwalten und in der TI verfügbar  
1410 machen.

1411 [ $\leq$ ]

1412 **TIP1-A\_2113 - Verwendung der zugewiesenen Rollenattribute**

1413 Alle Zertifikatsherausgeber MÜSSEN sicherstellen, dass bei der Zertifikatserstellung den  
1414 EE-Zertifikaten nur genau die Rollenattribute zugewiesen werden, für die die  
1415 Antragsteller gemäß Ausgabepolicy berechtigt sind.

1416 [ $\leq$ ]

1417 **2.7.9.2 Attributsbestätigende Stellen**

1418 Attributsbestätigende Stellen sind standesrechtlich legitimierte Organisationen, welche  
1419 die geschützten Attribute in X.509-Zertifikaten gegenüber dem TSP-X.509QES und TSP-  
1420 X.509nonQES bestätigen. Die Berufsgruppenattribute eines HBA-Inhabers sowie die  
1421 Institutionsattribute eines SMC-B-Inhabers können nur bei vorliegender Bestätigung  
1422 dieser Stellen in X.509-Zertifikaten aufgenommen werden.

1423

1424 **TIP1-A\_2114 - Attributbestätigende Stelle für HBA-Berufsgruppenattribut**

1425 HBA-Kartenherausgeber MÜSSEN das Berufsgruppenattribut für die Zertifikate ihrer  
1426 Mitglieder bestätigen und die Produktion des HBA gemäß ihrer Ausgabepolicy freigeben.

1427 [ $\leq$ ]

1428 **TIP1-A\_4455 - Attributbestätigende Stelle für SMC-B-Institutionsattribut**

1429 SMC-B-Kartenherausgeber MÜSSEN das Institutionsattribut für die Zertifikate ihrer  
1430 Mitglieder bestätigen und die Produktion der SMC-B gemäß ihrer Ausgabepolicy  
1431 freigeben.

1432 [ $\leq$ ]

1433 **Hinweis:** Das Institutionsattribut wird nur bei SMC-B für medizinische Institutionen  
1434 gesetzt.

1435 Bei einer SMC-B für Gesellschafterorganisationen verhält sich die Attributbestätigung  
1436 aber analog dazu: Der Kartenherausgeber (z.B. KZBV) bestätigt, dass es sich bei der  
1437 SMC-B-haltenden Stelle um eine Gesellschafterorganisation handelt (z.B. KZV).

1438 Angelehnt an die Berufsgruppen- und Institutionsattribute werden in technischen X.509-  
1439 Zertifikaten die technischen Rollen der Komponenten und Dienste bestätigt.

**TIP1-A\_4456 - Bestätigende Stelle für technische Rollen**

Herausgeber von gSMC-K/gSMC-KT respektive Dienstanbieter MÜSSEN die technische Rolle für die Zertifikate ihrer Komponenten bzw. Dienste bestätigen.

[<=]

**2.8 Identifikation von Akteuren**

Als Teilprozess der Registrierung ist die zuverlässige und eindeutige Identifikation aller an der TI beteiligten Akteure zwingend notwendig. Hierbei werden eindeutige Identifikationsmerkmale der realen Identitäten und daran gekoppelte eindeutige technische Identifikationsmerkmale benötigt. Die Authentisierung erfolgt durch die Nutzung von personen-, instituts-, organisations- bzw. gerätebezogenen Endnutzerzertifikaten, die kryptographische Identitäten mit den realen Identitäten verknüpft (s. a. Tabelle der kryptographischen Identitäten der TI-Plattform in [gemKPT\_Arch\_TIP#AnhB]) und auf Chipkarten oder anderen sicheren Systemen gespeichert sind. Die folgenden Chipkarten bzw. anderen sicheren Systeme sind definiert:

- Die eGK und die alternativen Versichertenidentitäten zur eindeutigen Identifikation und Authentifizierung des Versicherten,
- der HBA zur eindeutigen Identifikation und Authentifizierung des Leistungserbringers,
- die SMC-B zur eindeutigen Authentifizierung einer Organisation des Gesundheitswesens (medizinische Institution, Gesellschafterorganisation oder Kostenträger) und damit der Gesamtheit deren Mitarbeiter,
- die gSMC zur eindeutigen Authentifizierung von Geräten.

Die eindeutigen Identitäten von natürlichen (Versicherte, Leistungserbringer) bzw. juristischen Personen (medizinische Institutionen, Gesellschafterorganisations- und Kostenträrgeschäftsstellen) werden über die Krankenversichertennummer des Versicherten und die Telematik-ID eines Leistungserbringers bzw. einer medizinischen Institution oder Organisation des Gesundheitswesens repräsentiert.

**2.8.1 Krankenversichertennummer**

Zur Feststellung der Versichertenidentität wird die Krankenversichertennummer (KVNR) als eindeutige ID verwendet. Die Struktur der KVNR ist im [SGB V] im §290 festgelegt.

Die Spitzenverbände der Krankenkassen haben in Abstimmung mit dem BMG das Verfahren festgelegt, mit dem der unveränderbare Teil der KVNR erzeugt wird. Der unveränderbare Teil der KVNR ist zusammen mit weiteren personenbezogenen Daten des Versicherten in bestimmten Zertifikaten der eGK und der alternativen Versichertenidentitäten enthalten.

Zu den X.509-Zertifikaten auf der eGK gehören die Zertifikate C.CH.AUT, C.CH.ENC, C.CH.QES (optional), C.CH.AUTN und C.CH.ENCV. Zu den X.509-Zertifikaten der alternativen Versichertenidentitäten gehört das Zertifikat C.CH.AUT\_ALT. Über das die Zertifikate C.CH.AUT und C.CH.AUT\_ALT kann sich der Versicherte in der TI authentisieren.

Für bestimmte Anwendungsfälle werden die Zertifikate C.CH.AUTN bzw. C.CH.ENCV verwendet, die anstelle der persönlichen Identifikationsdaten ein Pseudonym des Versicherten enthalten. Die versichertenindividuellen Pseudonyme werden durch den

1484 jeweiligen Kostenträger berechnet. Die Pseudonyme werden mit kryptographischen  
1485 Verfahren aus dem unveränderbaren Teil der KVNR, dem Nachnamen des Versicherten  
1486 und einer vom Herausgeber (Kostenträger) generierten Zusatzinformation  
1487 (herausgeberspezifischer Zufallswert) gebildet.

## 1488 2.8.2 Telematik-ID

1489 Die eindeutige elektronische Identifizierung der Teilnehmer der TI (Leistungserbringer  
1490 als HBA-Halter bzw. medizinische Institutionen inklusive Einzelpraxen und  
1491 Berufsausübungsgemeinschaften, Gesellschafterorganisations- und  
1492 Kostenträgersgeschäftsstellen als Halterinnen von SMC-B) erfolgt über die Telematik-ID.  
1493 Die Sektoren des Gesundheitswesens verwalten jeweils einen Nummernkreis und weisen  
1494 den Akteuren, für die sie zuständig sind, eine Telematik-ID zu. Die Granularität der  
1495 Abbildung der existierenden Teilnehmer auf elektronische Identitäten obliegt den  
1496 einzelnen Sektoren bzw. den konkreten Teilnehmern. So kann sich eine reale Institution  
1497 auch in unterschiedliche elektronische Identitäten aufteilen, mit jeweils eigenen SMC-B  
1498 und Telematik-IDs.

1499 Um die Profibildung über mehrere Karten zu verhindern, kann die Telematik-ID mit  
1500 jedem Kartenwechsel zu einer Folgekarte geändert werden.

1501 Wird sie geändert, ändert sich auch die durch die Telematik-ID repräsentierte  
1502 elektronische Identität in der TI.

1503

### 1504 A\_18481 - Eineindeutigkeit der Telematik-ID

1505 Der Kartenherausgeber MUSS sicherstellen, dass die Telematik-ID bezogen auf die  
1506 elektronische Identität der betroffenen Teilnehmer in der Telematikinfrastruktur  
1507 eineindeutig ist. [ <= ]

*Für den HBA sind noch nicht alle Details bzgl. der Sicherstellung der  
Eineindeutigkeit der Telematik-ID in der TI geklärt. Ggf. notwendige  
Anpassungen hierzu erfolgen in einer Folgeversion dieses  
Dokumentes.*

1508 *Für den HBA sind noch nicht alle Details bzgl. der Sicherstellung der Eineindeutigkeit der*  
1509 *Telematik-ID in der TI geklärt. Ggf. notwendige Anpassungen hierzu erfolgen in einer Folgeversion*  
1510 *dieses Dokumentes.*

1511

### 1512 A\_18482 - Keine Neuvergabe einer Telematik-ID für mindestens 5 Jahre

1513 Ein Kartenherausgeber MUSS sicherstellen, dass eine Neuvergabe einer einmal  
1514 vergebenen Telematik-ID für mindestens 5 Jahre ausgeschlossen wird. [ <= ]

1515

1516 Die Trennung von den folgenden sektorspezifischen Festlegungen (Fortsatz) erfolgt durch  
1517 ein Trennzeichen (Separator). Die Verantwortung für die Eindeutigkeit des  
1518 sektorspezifischen Teils der Telematik-ID (Fortsatz) liegt bei dem jeweiligen Sektor; für  
1519 die Details dieses Teils gibt es keine normativen Vorgaben von der gematik. Eine  
1520 Begrenzung gibt es nur durch die festgelegte Länge des entsprechenden Feldes (128  
1521 Zeichen).

1522 Basierend auf den bisherigen Festlegungen der an der Vergabe der Telematik-ID  
1523 beteiligten Organisationen wurden den einzelnen Sektoren Kennzeichen in Form von  
1524 Präfixen zugeordnet, um in Verbindung mit der Telematik-ID eine eindeutige  
1525 Identifizierung über alle Sektoren hinweg gewährleisten zu können.



**TIP1-A\_2124 - Verwendung der Telematik-ID**

Ein Kartenherausgeber MUSS sicherstellen, dass als Präfix der Telematik-ID nur diejenige natürliche Zahl gesetzt wird, welche dem Sektor zugeordnet ist, den der Kartenherausgeber vertritt.

[<=]

**2.9 Lebenszyklus von Zertifikaten**

In diesem Kapitel wird der Lebenszyklus von X.509-Zertifikaten und CV-Zertifikaten beschrieben und es werden die dabei verwendeten Begriffe definiert.

Es gibt zwei verschiedene Ausprägungen des Lebenszyklus. Unterscheidungsmerkmal ist dabei, ob eine Statusprüfung erfolgt.

**2.9.1 Definition der Begriffe****Definition: Generierung**

Im Kontext von X.509-Zertifikaten und CV-Zertifikaten bezeichnet der Begriff „Generierung“ die Erzeugung eines Zertifikats, bei der eine elektronische Signatur einer Aussteller-CA über den öffentlichen Schlüssel und die Identitätsdaten des Antragstellers gebildet wird.

Das Zertifikat wird über den öffentlichen Schlüssel eines Schlüsselpaares ausgestellt, das die elektronische Identität der Person, Organisation oder technischen Komponente kryptographisch abbildet und gegenüber Anwendungen der TI authentifiziert.

**Definition: Staging**

Im Kontext von X.509-Zertifikaten und CV-Zertifikaten bezeichnet der Begriff „Staging“ die sichere Einbringung von kryptographischem Schlüssel und Zertifikaten in die betreffende Karte (eGK, HBA, ...) bzw. technische Komponente.

In dieser Phase des Zertifikatslebenszyklus kommen Dienste zur Schlüsselverteilung, zur Schlüsselinstallation und u. U. zur Schlüsselspeicherung zur Anwendung.

**Definition: Publizierung**

Der Terminus Publizierung bezeichnet die Veröffentlichung von Zertifikaten in einem Online-Verzeichnisdienst, so dass der Status des Zertifikates durch Komponenten und Anwendungen der TI geprüft werden kann.

Die Publizierung kann optional eine vorgängige Freischaltung in einem gesonderten organisatorischen Verfahren einschließen.

Für CV-Zertifikate ist die Publizierung nicht relevant.

**Definition: Sperrung**

Im Kontext von X.509-Zertifikaten bezeichnet der Begriff „Sperrung“ die Änderung des Status eines Zertifikats von „gültig“ auf „gesperrt“ in dem zugeordneten Statusprüfdienst.

Eine Sperrung von CV-Zertifikaten ist technisch nicht möglich.

Die Sperrung wird von dem Sperrberechtigten initiiert und von dem TSP-X.509QES und TSP-X.509nonQES umgesetzt.

Nach der Sperrung eines Zertifikats hat eine Zertifikatsprüfung als Ergebnis sinngemäß „Zertifikat ungültig seit <Datum>“.



1567 Es gibt zwei mögliche Varianten der Sperrung:

- 1568 • Suspendierung
- 1569 • endgültige Sperrung

1570 Es wird von einer Suspendierung gesprochen, falls die Sperrung nicht endgültig ist, d. h.  
1571 falls der Status des Zertifikats wieder von „ungültig“ auf „gültig“ geändert werden kann.

1572 Der Prozess des Widerrufs einer Suspendierung wird als Desuspendierung bezeichnet.

1573 Im Fall einer endgültigen Sperrung ist die Änderung des Zertifikatsstatus „gesperrt“ nicht  
1574 mehr möglich.

### 1575 **Definition: Gültigkeitsende**

1576 Im Kontext von X.509-Zertifikaten bezeichnet der Begriff „Gültigkeitsende“ den Ablauf  
1577 des im Zertifikat angegebenen Gültigkeitszeitraums.

1578 Die CV-Zertifikate der Kartengeneration 2 verfügen über ein steuerbares Gültigkeitsende,  
1579 nach dessen Überschreitung eine C2C-Authentisierung für die betreffende Karte nicht  
1580 mehr möglich ist.

1581 Nach dem Gültigkeitsende hat eine Zertifikatsprüfung ein negatives Ergebnis „Zertifikat  
1582 ungültig seit <Datum>“. Das Zertifikat darf danach durch verarbeitende Komponenten  
1583 nicht mehr akzeptiert werden.

## 1584 **2.9.2 Lebenszyklus für Zertifikate ohne Status-Eigenschaft**

1585 Der Lebenszyklus von CV-Zertifikaten sowie von X.509-Zertifikaten, für die in der  
1586 Telematikinfrastruktur kein Statusprüfdienst gefordert ist, gliedert sich durch folgende  
1587 Übergänge:

- 1588 • Generierung
- 1589 • Staging
- 1590 • Gültigkeitsende (nur für X.509-Zertifikate und CV-Zertifikate für G2-Karten)

## 1591 **2.9.3 Lebenszyklus für Zertifikate mit Statuseigenschaft**

1592 Der Lebenszyklus von X.509-Zertifikaten, für die in der Telematikinfrastruktur ein  
1593 Statusprüfdienst angeboten wird, gliedert sich durch folgende Übergänge:

- 1594 • Generierung
- 1595 • Staging
- 1596 • Publizierung
- 1597 • Sperrung
- 1598 • Gültigkeitsende

## 1599 **2.9.4 Staging der Zertifikate im Kartenterminal**

1600 Der Kartenterminalhersteller ist Antragsteller für die Zertifikate der gSMC-KT und liefert  
1601 das Gerät einschließlich des gerätebezogenen Sicherheitsmoduls des Kartenterminals  
1602 (gSMC-KT) inklusive Zertifikat aus. Der Kartenterminalhersteller ist der für die gSMC-KT  
1603 verantwortliche Kartenherausgeber.

1604 Zu diesem Zeitpunkt gibt es keinen Zusammenhang zwischen dem Zertifikat der gSMC-  
1605 KT und der Identität irgendeines eHealth-Kartenterminals.

## 1606 2.9.5 Staging der Zertifikate des Konnektors

1607 Der Konnektorhersteller ist Antragsteller für die Zertifikate der gSMC-K und liefert das  
1608 Gerät einschließlich des gerätebezogenen Sicherheitsmoduls (gSMC-K) aus.

1609 Die Zuordnung von Geräteidentität zu den Konnektorzertifikaten erfolgt durch die Inhalte  
1610 des Subject-DN der Zertifikate.

## 1611 2.9.6 Verantwortlichkeiten für den Zertifikats-Lebenszyklus

1612 HINWEIS: Die nachfolgende Übersicht dient dem besseren Verständnis der beteiligten  
1613 Rollen über den gesamten Lebenszyklus der Zertifikate.

1614 Im Rahmen der PKI kann das notwendige Vertrauen in die Authentizität der Identitäten  
1615 nur durch eine verbindlich definierte Verantwortungs- und Haftungsregelung über die  
1616 Erstellungs-, Staging- und Betriebsprozesse der folgenden Organisationen erreicht  
1617 werden:

- 1618 • gematik
- 1619 • TSP (Anbieter einer Aussteller-CA und/oder CVC-Sub-CA)
- 1620 • Kartenherausgeber
- 1621 • Kartenhersteller
- 1622 • Hersteller einer Komponente
- 1623 • Anbieter einer Komponente
- 1624 • Karteninhaber

1625 Für ein einzelnes Zertifikat haben die genannten Organisationen jeweils die  
1626 Verantwortung für verschiedene Stationen im Lebenszyklus. Die folgende Tabelle zeigt  
1627 die Verantwortlichkeiten in Bezug auf ein Zertifikat:

1628

1629 **Tabelle 2: Verantwortlichkeiten in Bezug auf ein Zertifikat**

Lebenszyklus-Zertifikat	Verantwortlich
Generierung	TSP
Staging	Hersteller
Publizierung	Anbieter oder Hersteller, je nach Komponente (in Zusammenarbeit mit dem TSP-X.509QES und TSP-X.509nonQES)
Veranlassung Sperrung	bei Komponenten: Anbieter, Hersteller, gematik bei Personen/Organisationen: Karteninhaber, Herausgeber, ggf. attributsbestätigende oder zuständige Stelle (z.B. bei Kammerwechsel).

Durchführung Sperrung	TSP
-----------------------	-----

1630

1631 Im Folgenden werden die Verantwortlichkeiten der Organisationen bzgl. des operativen  
 1632 Betriebs der PKI beschrieben. Dabei gilt, dass ein Anbieter einen Dienstleister (Betreiber)  
 1633 mit der Durchführung der genannten Aufgaben beauftragen kann. Die Verantwortung für  
 1634 die korrekte Durchführung der Aufgaben hat aber weiterhin der Anbieter.

#### 1635 **Besonderheiten des Kartenterminals**

1636 Da das gSMC-KT-Zertifikat keinen Verweis auf ein bestimmtes Gerät enthält, wird für  
 1637 diese Zertifikate die Rolle des Herstellers von dem Herausgeber der gSMC-KT  
 1638 eingenommen.

1639 Die Rolle des Betreibers wird bei Kartenterminals durch den Karteninhaber des gSMC-KT,  
 1640 (die Organisation, die das Kartenterminal in seiner Umgebung einsetzt) eingenommen.

#### 1641 **Besonderheiten des Konnektors**

1642 Die Rolle des Betreibers wird bei Konnektoren durch die Organisation des  
 1643 Gesundheitswesens ausgeübt, die einen Konnektor nutzt.

### 1644 **2.9.6.1 gematik**

1645 Die gematik hat die Verantwortung für die Zulassung von TSP, für die Erstellung und  
 1646 Verteilung der TSL und damit auch für das Einbringen der TSP-Zertifikate in die TSL und  
 1647 ggf. deren Entfernen aus der TSL sowie für den Betrieb der CVC-Root-CA.

1648 Die gematik hat die Verantwortung für zentral betriebene PKI-Dienste und die  
 1649 Herausgabe von Prüfkarten eGK.

1650 Die gematik kann das Sperren von Komponentenzertifikaten initiieren (bspw. beim  
 1651 Entzug von Zulassungen oder Kompromittierung zentraler Dienste), während die  
 1652 Durchführung der Sperrung bei den TSP-X.509QES und TSP-X.509nonQES liegt.

1653 Die gematik verantwortet Spezifikationen und übergreifende Policies.

1654 Die gematik ist oberste Instanz für Sicherheit in der TI und Incidenthandling.

### 1655 **2.9.6.2 TSP**

1656 Ein TSP muss von der gematik zugelassen werden (und ggf. weitere sektorspezifische  
 1657 Zulassungen durchlaufen haben), um als TSP Zertifikate für den Einsatz in der TI  
 1658 generieren zu dürfen.

1659 Ein TSP generiert ein Zertifikat auf Antrag durch den berechtigten Anbieter/Hersteller,  
 1660 Kostenträger, Leistungserbringer oder medizinische Institution.

1661 TSP-X.509QES und TSP-X.509nonQES müssen für bestimmte Zertifikatstypen einen  
 1662 OSCP-Responder betreiben, über den Statusabfragen zu allen von diesem TSP  
 1663 generierten X.509-Zertifikaten beantwortet werden.

1664 TSP-X.509QES und TSP-X.509nonQES führen Sperrungen von X.509-Zertifikaten auf  
 1665 Veranlassung durch berechnigte Anbieter/Hersteller, Versicherte, Kostenträger,  
 1666 Leistungserbringer oder medizinische Institutionen durch. Die gematik kann in den im  
 1667 vorigen Abschnitt genannten Fällen sperrberechtigt sein.

1668 Leistungserbringerorganisationen sind in der Rolle als attributsbestätigende Stelle  
 1669 ebenfalls sperrberechtigt.

### 2.9.6.3 Kartenherausgeber

Der Kartenherausgeber ist dafür verantwortlich, dass die durch ihn vertretenen Personen oder Institutionen/Organisationen die Möglichkeit haben, die für sie vorgesehenen Karten zu erhalten.

Der Kartenherausgeber sorgt dafür, dass bei der Erzeugung der Karten nur durch die gematik zugelassene initialisierte Karten und TSPs eingesetzt werden.

Der Kartenherausgeber bestätigt die Richtigkeit der auf der Karte hinterlegten Attribute.

Der Kartenherausgeber nimmt diese Verantwortung durch eine eigene Zulassung oder eine Beauftragung der beteiligten Akteure wahr.

### 2.9.6.4 Kartenhersteller

Der Kartenhersteller ist bei der Produktion der Chipkarte für die sichere Einbringung der korrekten Schlüssel und Zertifikate in die Karte verantwortlich. Dazu gehören:

- ein oder mehrere X.509-Endnutzerzertifikate
- zu den X.509-Endnutzerzertifikaten zugehörige private Schlüssel
- ggf. ein oder mehrere CV-Zertifikate der Chipkarte
- ggf. zu den CV-Zertifikaten der Chipkarte zugehörige private Schlüssel
- ggf. zu den CV-Zertifikaten der Chipkarte zugehöriges CV-CA-Zertifikat und öffentlicher Schlüssel der CVC-Root-CA

### 2.9.6.5 Hersteller einer Komponente

#### ***Hersteller Kartenterminal***

Der Kartenterminalhersteller agiert als Kartenherausgeber und ist verantwortlich für die Bereitstellung des für das Kartenterminal benötigten gerätespezifischen Sicherheitsmoduls gSMC-KT.

#### ***Hersteller eines Konnektors***

Der Konnektorhersteller agiert als Kartenherausgeber. Er tritt als Sperrberechtigter auf und muss dafür die vorgesehenen Schnittstellen des TSP-X.509nonQES nutzen.

### 2.9.6.6 Betreiber einer Komponente

#### ***Organisation, die das eHealth-Kartenterminal einsetzt***

Eine Organisation, die ein eHealth-Kartenterminal einsetzt, bezieht das für dessen Betrieb benötigte gSMC-KT entweder direkt von einem Kartenherausgeber oder zusammen mit dem Kartenterminal von dessen Hersteller.

#### ***Organisation des Gesundheitswesens, die einen Konnektor betreibt***

Die Organisation lässt einen Konnektor aufbauen und installieren.

Die Organisation muss die Verwaltungsinformationen zu den Zertifikaten der Identität (gSMC-K) seiner Konnektoren sicher speichern. Diese Daten muss sie im Rahmen einer ggf. notwendigen Sperrung der Zertifikate zur Identifikation bereithalten.

#### ***Anbieter eines zentralen oder fachanwendungsspezifischen Dienstes***

Der Anbieter muss sich als solcher von der gematik zulassen.

Der Anbieter muss für jeden in der TI etablierten Fachdienst die notwendigen Komponentenzertifikate bei einem TSP-X.509nonQES beantragen.

1710 Der Anbieter tritt als Sperrberechtigter auf und muss dafür die vorgesehenen  
1711 Schnittstellen des TSP nutzen.

### 1712 **2.9.7 Gültigkeitszeiträume für Schlüssel**

1713 Die Gültigkeit kryptographischer Schlüssel in der TI wird nicht unmittelbar, sondern über  
1714 die Gültigkeitszeiträume der darüber ausgestellten Zertifikate definiert. Daher ist die  
1715 Rezertifizierung bereits vorgängig verwendeter ‚alter‘ Schlüssel nicht zulässig.

1716 Durch Vorgaben der Herausgeber-Policy kann die konkrete Einsatzdauer von privaten CA-  
1717 Schlüsseln zusätzlich eingeschränkt werden.

#### 1718 **TIP1-A\_2492 - Rezertifizierung kryptographischer Schlüssel**

1719 Ein TSP-X.509 MUSS für die Ausstellung von Folgezertifikaten für eine gegebene  
1720 kryptographische Identität der TI neue kryptographische Schlüssel erzeugen und  
1721 verwenden.

1722 [ $\leq$ ]

ENTWURF

1723

## 3 CA-Strukturen

1724

### 3.1 Einführung

1725

1726

1727

Ausgehend von der Art der benötigten Zertifikate, ihrer funktionalen Zuordnung zu bestimmten Trägermedien sowie der jeweiligen Zuständigkeitsdomäne wird eine CA-Struktur entwickelt, die folgenden Kernanforderungen gerecht wird:

1728

- Funktionelle Abdeckung aller benötigten Ausstelleridentitäten

1729

- Wirtschaftliche Optimierung einer übergreifenden CA-Struktur

1730

- Flexibilität hinsichtlich des marktoffenen Anbietermodells für spezifische CAs

1731

#### 3.1.1 Übersicht Identitäten/Zertifikate

1732

1733

Zugunsten der Übersichtlichkeit sind in der Tabelle folgende Ausprägungen der jeweiligen Zertifikate NICHT explizit dargestellt:

1734

- Zertifikate für zusätzliche Betriebsumgebungen (Referenz-BU, Test-BU, ...)

1735

- Ausprägung innerhalb der Kartenarten (Testkarten, Entwicklerkarten, ...)

1736

1737

1738

1739

**Hinweis:** In den Spalten der Tabelle sind die Verantwortungsdomänen der Identitätselemente unterschieden. Zur Hervorhebung sind die Zertifikate für qualifizierte Signaturen in einer gesonderten Spalte unter der Verantwortungsdomäne der BNetzA aufgeführt.

1740

Optionale Zertifikate sind in Klammern gesetzt.

1741

1742

**Tabelle 3: Übersicht Identitätselemente und Verantwortungsdomänen**

Dezentrale Komponenten	gematik	LEO	KTR	BNetzA
Prüfkarte eGK	AUT, ENC AUT-N, ENC-V CVC			
eGK			AUT, ENC AUT-N, ENC-V CVC	(QES)
alternative Versichertenidentitäten			AUT_ALT	
HBA (alle Sektoren)		AUT, ENC AUTO CVC		QES (Attribut)

SMC-B/HSM-B medizinische Institution		AUT, ENC, OSIG, CVC		
SMC-B/HSM-B Gesellschafterorganisation		AUT, ENC, OSIG, CVC	AUT, ENC, OSIG, CVC	
SMC-B ORG Gesellschaften ohne CVC	AUT, ENC, OSIG	AUT, ENC, OSIG	AUT, ENC, OSIG	
SMC-B/HSM-B Kostenträger			AUT, ENC, OSIG, CVC	
gSMC-K (NK)	IPsec			
gSMC-K (AK)	TLS			
gSMC-K (SAK)	TLS CVC			
gSMC-KT	TLS			
Zentrale Dienste	gematik	LEO	KTR	BNetzA
VPN-Zugangsdienst	IPsec (TI) IPsec (SIS)			
weitere Zentrale Dienste	TLS-Server			
Fachanwendungsspezi- fische Dienste (derzeit nur VSDM)	gematik	LEO	KTR	BNetzA
Fachdienste	TLS-Client TLS-Server			
Intermediär	TLS-Client TLS-Server			
Infrastruktur	gematik	LEO	KTR	BNetzA
TSL	SIG			
OCSP	SIG	SIG	SIG	



qOCSP				QES
qOCSP-Proxy				n.a.
CRL	SIG			
Dezentrale Komponenten	gematik	LEO	KTR	BNetzA
eGK			AUT, ENC AUT-N, ENC-V CVC	(QES
HBA (alle Sektoren)		AUT, ENC AUTO CVC		QES (Attribut)
SMC-B	CVC	AUT, ENC, OSIG, CVC	AUT, ENC, OSIG, CVC	
HSM-B	CVC	AUT, ENC OSIG, CVC	AUT, ENC, OSIG, CVC	
gSMC-K (NK)	IPSEC			
gSMC-K (AK)	TLS			
gSMC-K (SAK)	TLS CVC			
gSMC-KT	TLS			
Zentrale Dienste	gematik	LEO	KTR	BNetzA
VPN-Zugangsdienst	IPSEC (TI) IPSEC (SIS)			
weitere Zentrale Dienste	TLS-Server			

Fachanwendungsspezifische Dienste (derzeit nur VSDM)	gematik	LEO	KTR	BNetzA
Fachdienste	TLS-Client TLS-Server			
Intermediär	TLS-Client TLS-Server			
Clientmodul	TLS-Clientmodul			
Infrastruktur	gematik	LEO	KTR	BNetzA
TSL	SIG			
OCSP	SIG	SIG	SIG	
qOCSP				(QES)*)
qOCSP-Proxy				n.a.
CRL	SIG			

1743 \*) OCSP-Signer-Zertifikate von VDA für QES müssen konform zu [eIDAS] sein.

### 1744 3.2 TSP-übergreifende CA-Struktur

1745 Zur Etablierung einer einheitlich geregelten PKI für nonQES-Zertifikate stellt die gematik  
1746 als Policy-Authority eine zentrale Root-CA für alle zertifikatsausgebenden TSP bereit.  
1747 Entsprechend müssen alle nonQES-X.509 Aussteller-CA-Zertifikate in der TI durch die  
1748 gematik Root-CA signiert sein.

1749 Aufbau, Betrieb und Management der TI-CAs sind aufgrund der hohen Qualitäts- und  
1750 Sicherheitsanforderungen mit erheblichen Kosten verbunden. Deshalb werden CAs, die  
1751 nicht unmittelbar der wettbewerblichen Differenzierung dienen, zusammengefasst und als  
1752 Infrastrukturdienste der gematik bereitgestellt.

1753

1754 **Hinweis:** Die hier vorgestellte Lösung belässt sowohl den Sektoren wie auch einzelnen  
1755 TSP die Möglichkeit zum Weiterbetrieb vorhandener- (eGK-CAs) resp. zur Etablierung  
1756 eigener Sub-CA-Strukturen unterhalb der gematik Root-CA. Die Policy-Konformität und  
1757 technische Interoperabilität muss der Anbieter gegenüber der gematik nachweisen.

#### 1758 TIP1-A\_2127 - Zusammenfassung gleichrangiger CA-Instanzen

1759 Die TI-Plattform SOLL funktional gleichrangige Aussteller-CA-Instanzen Sektor- und auch  
1760 TSP-übergreifend zusammenfassen.

1761 [ $\leq$ ]

Eine CA setzt für das Ausstellen von Zertifikaten ein Schlüsselpaar mit einer festen Schlüssellänge ein. Dieses Schlüsselpaar wird nur mit einem bestimmten kryptographischen Algorithmus genutzt. Bei der Erneuerung des Schlüsselpaares sind Versionswechsel und Wechsel der Schlüsselgeneration zu unterscheiden. Bei einem Versionswechsel werden die Schlüssellänge und der Algorithmus nicht verändert.

Im Gegensatz dazu wird bei einem Wechsel der Schlüsselgeneration die Schlüssellänge oder der Algorithmus verändert. Dies kann durch neue kryptographische Vorgaben für CAs (vgl. auch [gemSpec\_Krypt#GS-A\_5079]) notwendig werden.

Für eine Übergangszeit werden in der TI verschiedene Schlüsselgenerationen parallel unterstützt, um einen schrittweisen Übergang zur neuen Schlüsselgeneration zu ermöglichen. Die Schlüssel der alten Schlüsselgeneration und damit die zugehörigen Zertifikate dürfen nach Ablauf der Übergangszeit nicht mehr verwendet werden.

#### **TIP1-A\_6878 - Parallele Unterstützung verschiedener Schlüsselgenerationen**

Die gematik Root-CA MUSS in der TI jeweils die in [gemSpec\_Krypt] vorgegebenen Schlüsselgenerationen während einer Übergangszeit (s. [gemSpec\_Krypt#GS-A\_4357, GS-A\_5079]) parallel unterstützen.

[<=]

#### **TIP1-A\_7022 - Unterstützung mindestens einer Schlüsselgeneration**

Die TSP-X.509 QES und TSPX.509 nonQES MÜSSEN in der TI mindestens eine der in [gemSpec\_Krypt] vorgegebenen Schlüsselgenerationen (s. [gemSpec\_Krypt#GS-A\_4357, GS-A\_4358, GS-A\_5079]) unterstützen.

[<=]

### **3.2.1 nonQES-CA-Struktur für zentralisierte PKI**

Für alle nachfolgend dargestellten CA, die von der gematik für Sektor- und TSP-unabhängige Dienste bereitgestellt werden, gilt:

**Herausgeber:** gematik

**Anbieter:** gematik

**Zulassung:** gematik

**Policy:** gematik, HBA-Herausgeber, BA-Herausgeber

**Schnittstellen:** Für die Kartenherausgeber werden Prozessschnittstellen zur gematik sowie zu den TSP auf der Grundlage der jeweiligen Herausgabe-Policy etabliert. Für die TSP-X.509 sowie Kartenpersonalisierer werden in den Spezifikationen die erforderlichen technischen Schnittstellen für Beantragung und Auslieferung der X.509-Zertifikate definiert.

#### **3.2.1.1 gematik Root-CA (im Kontext nonQES X.509-Zertifikate)**

Die "gematik Root-CA" ist der gemeinsame Anker aller nonQES-X.509-Zertifikate, die von der gematik für Sektor- und TSP-unabhängige Dienste bereitgestellt werden. Das Zertifikatsportfolio dieser zentralisierten PKI, das u. a. auch die AUT-/ENC-Zertifikate des HBA und BA enthält, wird berechtigten Zertifikatsantragstellern über eine Online-Schnittstelle zur Verfügung gestellt.

Die zentrale Root-CA-Instanz der TI wird „gematik Root-CA“ genannt.

Weiterhin wird die Zertifizierung von öffentlichen Aussteller-CA-Schlüsseln durch die gematik Root-CA im Sinne des marktoffenen Anbietermodells anderen in der TI

1806 zugelassenen ZDA und TSP angeboten. Hierfür stellt die gematik ein geeignetes  
1807 organisatorisches Verfahren sowie der Anbieter der gematik Root-CA die erforderlichen  
1808 technischen Schnittstellen und Funktionen bereit.

## 1809 **TIP1-A\_2438 - X.509 nonQES gematik Root-CA**

1810 Die TI-Plattform MUSS in der TI eine zentrale X.509 nonQES-Root-CA unter der  
1811 Bezeichnung „gematik Root-CA“ bereitstellen.  
1812 [ $\leq$ ]

## 1813 **TIP1-A\_2439 - Policy der gematik Root-CA**

1814 Die gematik Root-CA MUSS die Regularien (Policy) vollständig beschreiben, unter denen  
1815 die Zertifizierung von Sub-CA-Schlüsseln durch die gematik Root-CA erfolgt.  
1816 [ $\leq$ ]

## 1817 **TIP1-A\_2128 - Lifecycle der gematik Root-CA**

1818 Die gematik Root-CA MUSS vollständig offline initialisiert und betrieben werden.  
1819 [ $\leq$ ]

## 1820 **TIP1-A\_2129 - Sichere Signierung von Sub-CA-Zertifikaten**

1821 Der Anbieter der gematik Root-CA MUSS sicherstellen, dass die Signierung von Sub-CA-  
1822 Zertifikaten der gematik Root-CA in einem geregelten und auditierten offline-Verfahren  
1823 und unter Einhaltung aller Vorgaben des Sicherheits- und Betriebskonzeptes erfolgt.  
1824 [ $\leq$ ]

## 1825 **TIP1-A\_2440 - Aufgaben der gematik Root-CA**

1826 Die gematik Root-CA MUSS Sub-CA-Zertifikate ausstellen, ggf. sperren und  
1827 Statusinformationen zur Verfügung stellen für die nonQES-X.509-Aussteller-CAs. Dies  
1828 umfasst die Einsatzbereiche:  
1829 a) nonQES HBA, BA,  
1830 b) SMC-B,  
1831 c) Komponenten und Dienste,  
1832 d) TSL-Signer,  
1833 e) nonQES eGK.  
1834 [ $\leq$ ]

## 1835 **TIP1-A\_2441 - Sub-CA unterhalb der gematik Root-CA**

1836 Ein TSP-X.509nonQES MUSS seine Sub-CA-Zertifikate von der gematik Root-CA  
1837 ableiten. [ $\leq$ ]

## 1838 **3.2.1.2 Komponenten- und Dienste-CA**

1839 Die Komponentenzertifikate (technische Identitäten) werden zentral durch die PKI der  
1840 gematik bereitgestellt.

- 1841 • Geräte in den dezentralen Systemen (Konnektor, Kartenterminal, ...)
- 1842 • Zentrale Dienste (VPN-Zugangsdienst, KSR,...)
- 1843 • Fachanwendungsspezifische Dienste (Fachdienste, Intermediär, ...)

1844 Für die Zertifikate des VPN-Zugangsdienstes muss eine eigene CA bereitgestellt werden,  
1845 da speziell für die VPN-Zertifikate eine Statusprüfung per CRL vorgesehen ist.  
1846 Entsprechend muss ein CRL-Prüfpfad zu dieser CA in der TSL definiert werden.

## 1847 **3.2.1.3 Bereitstellung OCSP-Signer**

1848 TSP-X.509nonQES und der Anbieter TSL-Dienst müssen OCSP-Signer-Zertifikate für ihre  
1849 eigenen nonQES OCSP-Responder-Instanzen erzeugen.

1850 OCSP-Signer-Zertifikate werden nicht von einer dedizierten OCSP-Signer-CA signiert,  
1851 sondern wie in Kap. 4.5 beschrieben.

#### 1852 **3.2.1.4 Bereitstellung CRL-Signer**

1853 TSP-X.509nonQES, die Statusprüfdienste als CRL bereitstellen, müssen CRL-Signer-  
1854 Zertifikate zur Signatur von CRLs für die Sperrauskünfte der von ihnen ausgegebenen  
1855 C.VPNK.VPN und C.VPNK.VPN-SIS Zertifikate beziehen.

1856 CRL-Signer-Zertifikate werden ausschließlich von der VPNK-CA, also nicht von einer  
1857 dedizierten CRL-Signer-CA signiert.

#### 1858 **3.2.1.5 TSL Signer-CA**

1859 Die TSL-Signer-Zertifikate sind originärer Bestandteil des TSL-Dienstes, der den  
1860 Vertrauensraum der gesamten TI etabliert. Sie werden ausgestellt von der TSL-Signer-  
1861 CA, die wiederum von der gematik Root-CA abgeleitet wird.

1862 Im Rahmen der ECC-Migration werden separate TSL-Signer-CAs sowohl für den TI-  
1863 Vertrauensraum (RSA) als auch für den TI-Vertrauensraum (ECC-RSA) benötigt.

#### 1864 **3.2.1.6 gematik CVC-Root-CA**

1865 Die gematik CVC-Root-CA bildet den Vertrauensanker aller CV-Zertifikate für die Card-to-  
1866 Card-Authentisierung in der TI. Von dieser Root müssen TSP-CVC eine Sub-CA  
1867 beantragen, um eigene CV-Zertifikate erzeugen zu können.

##### 1868 **TIP1-A\_2443 - gematik CVC-Root-CA**

1869 Die TI-Plattform MUSS in der TI eine zentrale CVC-Root-CA unter der Bezeichnung  
1870 „gematik CVC-Root-CA“ bereitstellen.  
1871 [<=]

##### 1872 **TIP1-A\_2444 - Regularien der gematik CVC-Root-CA**

1873 Die TI-Plattform MUSS die Regularien zur gematik CVC-Root-CA vollständig beschreiben,  
1874 unter denen die Ausstellung von CVC-CA-Zertifikaten der zweiten Ebene erfolgt.  
1875 [<=]

##### 1876 **TIP1-A\_2130 - Lifecycle der gematik CVC-Root-CA**

1877 Die TI-Plattform MUSS den Lifecycle der gematik CVC-Root-CA vollständig offline  
1878 gestalten.  
1879 [<=]

##### 1880 **TIP1-A\_2131 - Sichere Signierung von CVC-Sub-CA-Zertifikaten**

1881 Die CVC-Root-CA MUSS sicherstellen, dass die Signierung von Sub-CA-Zertifikaten für in  
1882 der TI zugelassene TSP-CVC in einem geregelten und auditierten offline-Verfahren und  
1883 unter Einhaltung aller Vorgaben des Sicherheits- und Betriebskonzeptes erfolgt.  
1884 [<=]

#### 1885 **3.2.1.7 CVC-CA**

1886 Die TSP-unabhängige Bereitstellung einer Sub-CVC-CA ist geeignet die Kosten seitens  
1887 der ZDA/TSP und letztlich der Kartenherausgeber zu senken.

##### 1888 **TIP1-A\_2132 - Signierung von CVC-Sub-CA-Zertifikaten**

1889 Ein TSP-CVC MUSS seine CVC-Sub-CA bei der gematik CVC-Root-CA zertifizieren lassen,  
1890 um CV-Zertifikate für zugelassene Kartenherausgeber erstellen zu können.  
1891 [<=]

1892 Für eGK-Hersteller ist der eigene Betrieb einer CVC-Sub-CA eine performante und somit  
 1893 auch wirtschaftliche Lösung. Für die kleinvolumigen Kartenarten (alle außer eGK) fördert  
 1894 die Bereitstellung eines zentralen CVC-Dienstes den Wettbewerb durch eine verringerte  
 1895 Marktzugangsbarriere und führt somit indirekt auch zu einer Kostenreduktion.

### 1896 3.3 HBA-spezifische CA-Strukturen

1897 Es werden generische CA-Strukturen für einen TSP beschrieben, der HBA-Zertifikate für  
 1898 einen Sektor ausgeben möchte.

1899 Die Darstellung erfolgt getrennt nach nonQES- und QES-Anforderungen.

1900 Die Implementierung mit erforderlichem CA-Lifecycle-Management und zugehörigen  
 1901 Policy- und Vertragswerken zwischen den Akteuren sind hier generisch dargestellt.

1902 Vor diesem Hintergrund werden dann Synergien und Besonderheiten einer einheitlichen  
 1903 CA-Ausprägung für alle Sektoren aufgezeigt.

#### 1904 3.3.1 QES-CA-Struktur für HBA-QES

##### 1905 **TIP1-A\_2134 - gültiger Qualifikationsstatus**

1906 Ein TSP-X.509 QES als Zertifikatsherausgeber für QES-Zertifikate MUSS für den Betrieb  
 1907 seiner QES-Dienste deren gültigen Qualifikationsstatus gemäß [eIDAS] nachweisen.  
 1908 [ $\leq$ ]

1909 Verantwortlich für die HBA-Bereitstellung für Leistungserbringer registrierter  
 1910 Berufsgruppen sind die Registerorganisationen der Berufsstände. Für zugelassene Ärzte  
 1911 z. B. die Landesärztekammern, etc.

1912 Die das Berufsgruppenattribut verwaltende Registerorganisation wird weiterhin neutral  
 1913 als LEO bezeichnet (funktionale Anforderungen an CA-Strukturen über alle LEO  
 1914 identisch).

1915 HBA-Herausgeber: LEO

1916 **Anbieter:** am Markt agierender VDA für QES

1917 **Zulassung:** LEO, gematik

1918 **Prüfinstanz:** beauftragte Konformitätsbewertungsstelle für QES; LEO oder beauftragter  
 1919 Dienstleister für HBA-Prozesse und nonQES; gematik für Kartenplattform

1920 **Policy:** LEO, gematik

1921 HBA-Produktionsfreigabe: LEO

1922 Für die Bereitstellung von Berufsausweisen (BA), für bislang nicht in einer Kammer  
 1923 verwaltete Berufe (Notfall-, Heil- und Pflegeberufe), ist eine zuständige  
 1924 Registerorganisation in Planung (eGBR), die zu gegebener Zeit die entsprechenden  
 1925 Anforderungen an den BA formulieren wird.

#### 1926 3.3.2 nonQES-CA-Struktur für ENC, AUT, OSIG, CV

1927 Neben der Herausgabe der zwingend an einen VDA gebundenen QES-Zertifikate sind für  
 1928 die HBA-Produktion nonQES-Zertifikate erforderlich. Diese werden durch den VDA für  
 1929 QES selbst bereitgestellt.

### 1930 3.3.3 Sektorneutrale CA für HBA, BA und SMC-B

1931 Die verschiedenen Ärztekammern auf Landesebene, die eigenverantwortlichen  
 1932 Ärztekammern auf Bezirksebene, die Zahnärztekammern, die Apothekerkammern und  
 1933 die Psychotherapeutenkammern auf Landesebene regeln selbst die notwendigen  
 1934 Herausgabeprozesse des HBA, zum Beispiel die Zusammenarbeit mit anderen  
 1935 Heilberufskammern oder Vertragsbindung mit VDA im Rahmen der Kartenproduktion.

1936 Um alle relevanten Geschäftsprozesse über die Anwendungen der TI abbilden zu können,  
 1937 müssen insgesamt folgende Akteure mit elektronischen Identitäten (HBA, BA SMC-B)  
 1938 versehen werden:

- 1939 • Alle Sektoren mit ihren berufsständischen Vertretungen bzw.  
 1940 Leistungserbringerorganisationen (LEO)
- 1941 • Einrichtungen der Kostenträger
- 1942 • Perspektivisch alle Gesellschafterorganisationen (Gesellschafter der gematik und  
 1943 durch diese Gesellschafter vertretene Organisationen)
- 1944 • Perspektivisch zusätzliche Akteure, die keiner approbierten und durch eine  
 1945 Ständevertretung repräsentierten Berufsgruppen angehören, sondern anderen –  
 1946 den sog. Nicht-verkammerten – Berufen im Notfall-, Pflege- und Heilbereich  
 1947 angehören. Hierbei bestehen zahlreiche und vielfältige Kommunikations- und  
 1948 Datenschnittstellen zum Versicherten, zu Ärzten und Krankenhäusern sowie bei  
 1949 der Versorgung des Versicherten mit Heil- und Hilfsmitteln sowie therapeutischen  
 1950 Maßnahmen. Zukünftig besteht also Bedarf zu deren vollständigen Einbindung in  
 1951 die TI.  
 1952 Um eine geregelte Versorgung dieser Berufsgruppen mit elektronischen  
 1953 Berufsausweisen (HBA) zu ermöglichen, wurde auf Beschluss der  
 1954 Gesundheitsminister der Länder die Etablierung eines länderübergreifenden  
 1955 Registers (eGBR) beschlossen, das die Rolle vergleichbar einer Ärztekammer  
 1956 übernehmen und deshalb im folgenden Text auch unter dem Begriff LEO  
 1957 subsumiert wird ). Das eGBR ist derzeit im Aufbau befindlich und aktuell ist noch  
 1958 keine belastbare Spezifikation verfügbar.

1959 Aus funktionaler Sicht der TI unterscheiden sich die Akteure der Sektoren in ihrer  
 1960 Repräsentation (HBA, BA, SMC-B) in folgenden Punkten:

- 1961 • X.509-Zertifikate in der Extension admission
- 1962 • Berufsbezeichnung (HBA) oder Beschreibung der Institution/Betriebsstätte (SMC-  
 1963 B) – textuell (im Attribut professionItem) und maschinenlesbar (im Attribut  
 1964 professionOID)
- 1965 • Zuständige Stelle zur Verwaltung des Berufsattributes (herausgebende LEO)
- 1966 • Die bereits etablierte Liste der zugelassenen Berufsbezeichnungen<sup>(Diese Liste enthält</sup>  
 1967 bereits eine Reihe von Nicht-Arztberufen, ist jedoch nicht vollständig.) und Identifier zur Verwendung in  
 1968 Zertifikaten muss bedarfsgerecht erweitert werden (Hoheit: LEO, DIMDI, gematik)

1969 Zur Erfüllung aller funktionalen Anforderungen an die sektorspezifischen Ausprägungen  
 1970 hinsichtlich optischer und elektrischer Eigenschaften (Authentisierung, Autorisierung)  
 1971 ergeben sich keine sektorspezifischen Anforderungen an die zugrunde liegende PKI. Vor  
 1972 diesem Hintergrund und angesichts der Anforderungen nach Reduktion der Komplexität  
 1973 bei gleichzeitig verbesserter Wirtschaftlichkeit der Systemarchitektur erfolgt die  
 1974 Bündelung der CA-Strukturen zu einer übergreifenden LEO-PKI.

1975 Für Ausgabeprozesse und Policy gelten folgende Zuordnungen:



- 1976 • für den HBA gelten die Festlegungen der gemeinsamen Policy (CP) der LEO [CP-  
1977 HPC]  
1978 Ggf. unabdingbar sektorspezifische Ausprägungen können als solche ausgewiesen  
1979 und in die gemeinsame Policy aufgenommen werden.  
1980 Für das QES-Zertifikat gelten darüber hinaus die gesetzlichen Regelungen für VDA  
1981 für QES.
- 1982 • für den BA muss eine entsprechende Policy durch das eGBR erstellt werden.
- 1983 • für die nicht-personenbezogenen Zertifikate der Geräte und Dienste in der TI gilt  
1984 die CP der gematik [gemRL\_TSL\_SP\_CP].

ENTWURF

1985

---

## 4 Statusprüfung bei X.509-Zertifikaten

---

1986

### 4.1 Einführung

1987  
1988  
1989  
1990  
1991  
1992

X.509-Zertifikate werden mit einer definierten Gültigkeitsdauer ausgestellt, während der sich Bedingungen einstellen können, die eine weitere Verwendung des Zertifikates bis zum Laufzeitende nicht erlauben (Kartenverlust, Wegfall kritischer Berufsattribute im Zertifikat, Schlüsselkompromittierung, Kompromittierung der CA, ...). Vor diesem Hintergrund sind zeitnahe Auskunftsdienste über den Sperrstatus eines jeden Zertifikates elementar für die Verlässlichkeit der auf die Gültigkeit vertrauenden Geschäftsprozesse.

1993

### 4.2 Eingangsanforderungen

1994  
1995  
1996  
1997

Eine der elementaren Anforderung an jeden Herausgeber von Zertifikaten in der TI besteht in der Bereitstellung von Sperrinformationen zu jedem Zertifikat über den Zeitraum der Zertifikatslaufzeit sowie über einen zu definierenden Zeitraum nach Ablauf der Gültigkeit des Zertifikates für Zwecke der Zertifikats- und Signaturprüfung.

1998

### 4.3 Methoden der Statusprüfung

1999

#### 4.3.1 Dezentrale Statusprüfung mittels CRL

2000  
2001  
2002  
2003  
2004  
2005  
2006  
2007  
2008  
2009  
2010  
2011  
2012  
2013

In der TI werden CRLs für Zwecke der Zertifikatsstatusprüfung ausschließlich für die Statusprüfung der Zertifikate C.VPNK.VPN und C.VPNK.VPN-SIS verwendet. Hierzu lädt der Konnektor regelmäßig eine im Internet verfügbare CRL und prüft den Sperrstatus des Konzentrazertifikates.

Der Status aller anderen X.509-Zertifikate – sofern eine Statusprüfung für den betreffenden Zertifikatstyp definiert ist – wird über OCSP geprüft.

**TIP1-A\_4457 - Statusprüfung von X.509-Zertifikaten des VPN-Zugangsdienstes**

Die TI-Plattform MUSS die Statusprüfung der X.509-Zertifikate ID.VPNK.VPN bzw. ID.VPNK.VPN-SIS des VPN-Zugangsdienstes über im Internet verfügbare CRLs bereitstellen. Die TI-Plattform MUSS ebenfalls für die Verteilung der Sperrinformationen der eben genannten Zertifikate über OCSP im Internet Statusinformationen zur Verfügung stellen.

[<=]

2014

#### 4.3.2 Serverbasierte Statusprüfung mittels OCSP

2015  
2016  
2017  
2018  
2019

Bei der Abfrage per *Online Certificate Status Protocol* (OCSP) erfolgt die Statusprüfung für ein bestimmtes Zertifikat serverbasiert und bedarfsgesteuert genau in dem Moment, der für die Client-Anwendung zur Statusauswertung relevant ist.

Ein OCSP-Responder kann seine Informationen über verschiedene Quellen, wie der internen CA-Datenbank, aus einer LDAP-Datenbank oder einer CRL beziehen. Die

2020 Gültigkeitsangaben der originären Statusauskunft werden in der Antwort der OCSP-  
2021 Response an den Client für weitere Auswertungen zurückgemeldet.  
2022 Jede OCSP-Response, welche Zertifikatsstatusinformationen enthält, wird vom OCSP-  
2023 Responder signiert übermittelt, so dass auch die Authentizität des OCSP-Responder und  
2024 die Integrität der Response geprüft werden kann.

### 2025 4.3.3 Sonderfälle der Statusprüfung

2026 Einen Sonderfall bilden die Komponenten für den Verbindungsaufbau in die TI bzw. das  
2027 Internet, die die vom Netzzugangspunkt angebotenen Zertifikate noch nicht per OCSP  
2028 gegen einen innerhalb der TI befindlichen OCSP-Responder prüfen können.

2029 Für dieses Szenario bieten sich folgende Lösungen:

- 2030 • Bereitstellung entsprechender OCSP-Responder über das Internet –  
2031 vorausgesetzt, die Netzzugangskomponenten verfügen über Internetzugang.
- 2032 • Rückgriff auf eine CRL-basierte Statusprüfung, wobei ein Update der CRL  
2033 • erst nach erfolgreichem Zugang zur TI oder  
2034 • vor Zugang zur TI via Internet (Voraussetzung s.o.) erfolgen kann
- 2035 • Implementierung einer organisatorischen Lösung zur Deaktivierung eines nicht  
2036 mehr vertrauenswürdigen Zugangspunktes.

2037 Die Entscheidung wurde zugunsten der CRL-basierten Statusprüfung getroffen. Als  
2038 alternatives Verfahren werden Sperrauskünfte per OCSP ebenfalls im  
2039 Internet bereitgestellt.

2040 Die Ermittlung des CRL Distribution Point (CDP) erfolgt analog der Ermittlung der OCSP-  
2041 Adresse über einen Eintrag in der TSL (ServiceSupplyPoint) zur korrespondierenden CA.

#### 2042 **TIP1-A\_5448 - Zuordnung von CRL- und OCSP-Adressen in der TSL**

2043 Die TI-Plattform MUSS der in der TI zugelassenen CA zur Ausstellung von Zertifikaten für  
2044 den VPN-Zugangsdienst innerhalb der TSL-Datenstruktur den zur  
2045 Zertifikatsstatusprüfung per CRL zu verwendenden CRL Distribution Point (CDP) und  
2046 die per OCSP zu verwendenden OCSP-Adressen zuordnen. Diese Adresse können von  
2047 denjenigen in den zu prüfenden Zertifikaten abweichen.

2048 [ $\leq$ ]

#### 2049 **TIP1-A\_4458 - Statusprüfung der ID.VPNK.VPN und ID.VPNK.VPN-SIS** 2050 **(Zugangspunkt TI bzw. Sicherer Internetzugang)**

2051 Produkttypen der TI, die die Zertifikate der Identitäten ID.VPNK.VPN bzw. ID.VPNK.VPN-  
2052 SIS prüfen, MÜSSEN den Sperrstatus dieser Zertifikate per CRL oder OCSP prüfen.

2053 [ $\leq$ ]

### 2054 4.4 Logisches Konzept der OCSP-Dienste

2055 Der OCSP-Client richtet die Anfrage zum Status eines bestimmten Zertifikates an den  
2056 entsprechenden OCSP-Responder, um zu prüfen, ob das entsprechende Zertifikat  
2057 bekannt ist und nicht zwischenzeitlich gesperrt wurde. Dieser OCSP-Responder ermittelt  
2058 den fraglichen Status aus den Datenbeständen einer oder mehrerer ausstellender CAs  
2059 und liefert dem Client die Antworten „good“, „revoked since <date>“ oder „unknown“.

#### 4.4.1 OCSP Festlegungen

##### **TIP1-A\_2140-01TIP1-A\_2140 - Standard für OCSP-Dienste**

TSP-X.509QES und TSP-X.509nonQES MÜSSEN für alle X.509-Zertifikate (außer denen für eGK) OCSP-Dienste in der TI gemäß [~~Common PKI~~RFC6960] und [RFC5280] unter obligatorischer Verwendung der CertHash-Erweiterung (Positive Statement) implementieren.

[<=]

Abweichungen von [RFC6960] werden detailliert im Abschnitt 4.5 beschrieben. Die certHash-Erweiterung (außer nonQES-Zertifikaten einer eGK) wird gemäß GS-A\_4693 umgesetzt.

##### **TIP1-A\_2493-01TIP1-A\_2493 - Standard für OCSP-Dienste für eGK**

TSP-X.509QES und TSP-X.509nonQES MÜSSEN für alle X.509-Zertifikate der eGK OCSP-Dienste in der TI gemäß [~~RFC2560~~RFC6960] und [RFC5280] implementieren.

[<=]

#### 4.4.2 OCSP-Responder-Adresse

##### **TIP1-A\_2138 - Einbringung der OCSP-Adresse ins Zertifikat**

TSP-X.509QES und TSP-X.509nonQES MÜSSEN für jedes von ihnen ausgestellte X.509-Zertifikat einer in der TI zugelassenen CA die Adresse des zur ausgebenden CA zugehörigen OCSP-Responders in das Zertifikat einbringen. Ausnahmen hiervon bilden Zertifikate, für die per Definition keine Statusprüfung vorgesehen ist.

[<=]

##### **TIP1-A\_2142 - Zuordnung von OCSP-Adressen in der TSL**

Die TI-Plattform MUSS jeder in der TI zugelassenen CA innerhalb der TSL-Datenstruktur für Zertifikatsstatusanfragen zu verwendende OCSP-Responder-Adresse(n) zuordnen. Diese Adressen können von denjenigen in den zu prüfenden Zertifikaten abweichen.

[<=]

Die Anwendungen innerhalb der TI prüfen für nonQES-Zertifikate zunächst den Vertrauensstatus der ausgebenden CA über die Einträge der TSL. Als Rückmeldung dieser Prüfung wird (im positiven Fall) die tatsächlich zu verwendende OCSP-Adresse zur Prüfung des Zertifikatsstatus geliefert; eine Auswertung der in den Zertifikaten ausgewiesenen Adressinformation findet nicht statt. Die eigentliche Statusanfrage kann somit an eine andere OCSP-Responder-Adresse gerichtet werden als im Zertifikat hinterlegt. Diese Funktionalität der TSL bietet die Möglichkeit für eine flexible Gestaltung der OCSP-Dienste innerhalb der TI.

Für QES-Zertifikate wird für Statusprüfungen innerhalb der TI zunächst die OCSP-Adresse für das Internet aus dem EE-Zertifikat extrahiert und mittels einer in der TSL hinterlegten Übersetzungstabelle der zuständige OCSP-Responder in der TI ermittelt.

Die Anwendungen außerhalb der TI im Internet prüfen den Vertrauensstatus des Zertifikates direkt über die eingetragene URI der OCSP-Adresse im EE-Zertifikat selbst, da im Internet die Umsetzung des TI-Vertrauensraumes über OCSP-Dienste realisiert wird. Die Statusanfragen zu den EE- wie auch den CA-Zertifikaten des Zertifizierungspfades werden somit jeweils an diejenige OCSP-Responder-Adresse gerichtet, die im Zertifikat hinterlegt ist.

**TIP1-A\_5137 - Auflösung von OCSP-Adressen im Internet**

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

[<=]

**4.4.3 OCSP-Request****TIP1-A\_2143-01TIP1-A\_2143 - Umgang mit signierten OCSP-Requests**

TSP-X.509QES und TSP-X.509nonQES MÜSSEN sicherstellen, dass die von ihm betriebenen OCSP-Responder signierte Requests nach [RFC2560] sowie [Common-PKI]RFC6960] beantworten. Aus Gründen der Performance MUSS der OCSP-Responder signierte Requests wie unsignierte Requests behandeln, d.h. die Signaturprüfung entfallen lassen.

[<=]

**TIP1-A\_2144-01TIP1-A\_2144 - Anzahl Zertifikate je OCSP-Request**

Die TI-Plattform MUSS sicherstellen, dass je OCSP-Request nicht mehr als der Status für genau ein Zertifikat abgefragt werden darf (abweichend von [RFC2560],RFC6960], wonach je Request die Status mehrerer Zertifikate angefordert werden kann).

[<=]

**4.4.4 OCSP-Response**

Bei der Anwendungsentwicklung muss berücksichtigt werden, dass eine OCSP-Response gemäß [RFC2560] nicht alle Aspekte einer Zertifikatsprüfung abdeckt. Die OCSP-Response gibt lediglich den Sperrstatus eines Zertifikates zurück. Weitere Zeitparameter der OCSP-Response sowie der im Zertifikat hinterlegte Gültigkeitszeitraum müssen von einer Client-Anwendung zur Auswertung herangezogen werden.

Weiterhin ist die Prüfung der ausstellenden CA-Hierarchie über den gesamten Validierungspfad nicht Gegenstand einer OCSP-Response. Aus dem Ergebnis der Pfadvalidierung ergibt sich, ob ein Zertifikat von einer zugelassenen CA ausgestellt wurde.

**4.4.4.1 Zertifikatsstatus**

Die Status der OCSP-Responses sind in [RFC2560#2.2] zu finden.

**4.4.4.2 Zeitpunkte in der OCSP-Response**

Für die Auswertungslogik in den Komponenten und Fachanwendungen sind die zeitlichen Angaben zum Zertifikatsstatus von entscheidender Bedeutung.

**TIP1-A\_2145 - Zeitpunkt in OCSP-Response auf Basis verbindlicher Zeitquelle**

Der OCSP-Dienst MUSS sicherstellen, dass die OCSP-Response den Zeitpunkt, zu dem der Status des angefragten Zertifikates festgestellt wurde, enthält. Dieser Zeitpunkt muss auf einer in der TI verbindlich geltenden Zeitquelle beruhen.

[<=]

Zusätzlich bestimmen weitere Parameter die semantische Bedeutung dieses Zeitpunktes:

- 2146 • Die Datensätze in der Datenbasis des OCSP-Dienstes können aus  
2147 unterschiedlichen Quellen stammen, die ihrerseits von unterschiedlicher Aktualität  
2148 sind, je nach Latenzzeit zwischen Statusänderung durch die CA und Eintreffen der  
2149 Änderungsmeldung in der Datenbasis des OCSP-Responders.  
2150 Bsp-1: OCSP-Responder und CA verwenden die selbe Datenbank  
2151 Bsp-2: DB des OCSP-Responders wird monatlich mit CRL synchronisiert
- 2152 • Der Zeitpunkt der Sperrung eines Zertifikates ist relevant, weil Statusabfragen  
2153 sich auf Signaturen beziehen können, die vor oder nach einer möglichen Sperrung  
2154 erfolgt sind.

2155 Folgende Zeitspanne kann in der OCSP-Response nicht enthalten sein, sie muss vom  
2156 auswertenden Client selbst ermittelt und nach eigenen Kriterien bewertet werden:

- 2157 • Laufzeit der Response-Daten, d.h. zulässige Zeitspanne zwischen Response-  
2158 Signatur sowie Eintreffen und Auswertung in der Client-Anwendung

2159 Um zu verhindern, dass bspw. auf Basis alter CRLs veraltete Statusauskünfte verteilt  
2160 werden, müssen Statusänderungen unmittelbar im OCSP-Dienst umgesetzt werden.

#### 2161 **TIP1-A\_4459 - Aktualität von OCSP-Responses**

2162 Der OCSP-Dienst MUSS die Aktualität von OCSP-Responses sicherstellen.

2163 [ $\leq$ ]

#### 2164 **4.4.4.3 Gültigkeitsdauer eines OCSP-Response (nonQES)**

2165 Innerhalb welcher Zeitspanne eine Statusauskunft genutzt werden kann, ist wesentlich  
2166 abhängig von dem Schutzbedarf des durch die zu validierende Signatur bestätigten  
2167 Sachverhalts. Während in diesem Sinne hochkritische Signaturen immer eine quasi-  
2168 Echtzeitprüfung bis zur CA-Datenbasis erfordern, genügt für weniger kritische  
2169 Anwendungen ggf. auch eine Statusauskunft, die bereits einen Tag alt ist.

2170 Ferner ermöglicht die Festlegung der zulässigen Nutzungsdauer von OCSP-Responses das  
2171 Zwischenspeichern und Wiederverwenden dieser Responses im lokalen Cache einer  
2172 Komponente oder in einem vorgeschalteten OCSP-Proxy. Das Caching verfolgt die Ziele:

- 2173 • Verkürzung der Response-Laufzeiten
- 2174 • Reduzierung der Netzlast
- 2175 • Implementierung dedizierter OCSP-Proxy (hochperformant, hochverfügbar,  
2176 skalierbar)

#### 2177 **4.4.4.4 Signatur der OCSP-Responses**

##### 2178 **TIP1-A\_2146 - Signatur der OCSP-Response**

2179 Der OCSP-Dienst MUSS jede Antwort eines OCSP-Responders gemäß [RFC2560]  
2180 signieren.

2181 [ $\leq$ ]

##### 2182 **TIP1-A\_2147 - Signatur der nonQES-OCSP-Response**

2183 Der OCSP-Dienst MUSS die Signatur einer Statusantwort für ein nonQES-Zertifikat durch  
2184 einen OCSP-Responder mit einem nonQES-Zertifikat erzeugen.

2185 [ $\leq$ ]

##### 2186 **TIP1-A\_2148 - Performance-Erhöhung bei OCSP durch Caching**

2187 Der OCSP-Dienst SOLL die Performance durch Methoden des Response-Caching steigern.

2188 [ $\leq$ ]



#### 4.4.4.5 Fehlermeldungen in der OCSP-Response

##### **TIP1-A\_2149 - Auswertung von OCSP-Responses**

Die Produkttypen der TI-Plattform, die OCSP-Responses auswerten, MÜSSEN für jede mögliche Ausprägung der zurückgelieferten Parameter (Exception Cases, Zeiten, Fehlercodes) eine geordnete Reaktion implementieren.

[<=]

##### **TIP1-A\_2150 - Ausschluss der Anforderung signierter OCSP-Requests**

Der OCSP-Dienst DARF NICHT mit einem Fehlercode antworten, der den Client zur Übermittlung eines signierten Requests auffordert, da innerhalb der TI keine signierten OCSP-Requests gefordert sind.

[<=]

#### 4.5 OCSP-Dienste

Analog zur gewählten CA-Struktur in der TI ist auch die Architektur der OCSP-Dienste optimiert unter den Prämissen Komplexitätsreduktion, Wirtschaftlichkeit und Flexibilität.

Der RFC6960 sieht vor, dass ein OCSP-Signer-Zertifikat von derselben CA signiert sein sollte [RFC6960#4.2.2.2], die auch die End-Entity-Zertifikate ausstellt. Dies soll sicherstellen, dass die OCSP-Response von der prüfenden Instanz validiert werden kann. Für Zertifikate, die nach dem Kompromiss- oder Kettenmodell ausgestellt wurden, kann diese Vorgabe jedoch nicht immer erfüllt werden, denn eine Signatur muss unter Umständen auch dann noch prüfbar sein, wenn das CA-Zertifikat zeitlich abgelaufen ist oder gesperrt wurde.

In diesem Fall müssen für nonQES-Zertifikate die OCSP-Statusauskünfte durch eine andere CA übernommen werden.

##### **TIP1-A\_2446 - Signaturzertifikate für OCSP-Responder in der TI**

Produkttypen der TI, die nonQES-Statusauskünfte per OCSP bereitstellen, SOLLEN für ihre nonQES-OCSP-Responder die Signaturzertifikate gemäß [RFC6960] erstellen. Ausgenommen davon sind nach Kompromissmodell ausgestellte Zertifikate für die kein gültiges Signaturzertifikat mehr verfügbar ist. Für diese wird die OCSP-Statusauskunft durch eine andere CA übernommen und ggf. die Prüfbarkeit über die TSL sichergestellt.

[<=]

*Hinweis: Bereits von der OCSP-Signer-CA der gematik bezogene OCSP-Signer-Zertifikate der Schlüsselgeneration „RSA“ können weiter verwendet werden.*

OCSP-Dienste für QES-Zertifikate müssen den Vorgaben von [eIDAS] genügen. Dies beinhaltet Konformität der OCSP-Zertifikatsprofile mit [RFC6960]. Wegen der Ausstellung der End-Entity-Zertifikate nach Kettenmodell kann wie oben erläutert die Vorgabe in [RFC6960#4.2.2.2] zur Ableitung der OCSP-Signer-Zertifikate nicht streng erfüllt werden.

Durch die Forderung nach der dauerhaften Prüfbarkeit für qualifizierte Signaturen auch bei Beendigung des Betriebs können folgende Fälle eintreten (vgl. [VDG§16]):

- die Bereitstellung der OCSP-Statusauskünfte wird von einer anderen qualifizierten CA übernommen. Diese qualifizierte CA kann auch von einem anderen qualifizierten Vertrauensdiensteanbieter betrieben werden oder
- die Bereitstellung der OCSP-Statusauskünfte wird von der Bundesnetzagentur übernommen. Für diesen Zweck stellt die Bundesnetzagentur ein dauerhaftes Verzeichnis (DAVE) bereit.



Je nach den Umständen der Beendigung des TSP-Dienstes oder der Einstellung des CA-Betriebs kann der Fall eintreten, dass unter der im End-Entity-Zertifikat hinterlegten OCSP-Responder-Adresse für das Internet keine Auskünfte mehr erteilt werden. In diesem Fall kann als Alternative für eine OCSP-Statusprüfung im Internet der zuständige OCSP-Responder aus der BNetzA-VL ermittelt werden. Das Verfahren dazu wird durch die BNetzA im Einvernehmen mit den VDAs festgelegt. Innerhalb der TI wird der zuständige OCSP-Responder über die Übersetzungstabelle in der TSL identifiziert (s.a. Kap. 4.4.2).

Durch die mögliche Übernahme der OCSP-Statusauskünfte durch einen anderen TSP muss es abweichend von RFC6960 erlaubt sein, dass das OCSP-Signer-Zertifikat aus einer beliebigen, auf Basis der BNetzA-VL qualifizierten CA abgeleitet ist. Unter Umständen ist auch dies nicht realisierbar und dann wird das OCSP-Signer-Zertifikat selbst direkt als qualifizierter Dienst in die BNetzA-VL eingebracht. Dieser Fall muss darum bei der QES-Zertifikatsprüfung berücksichtigt werden (s. Kap. 6.6.2 ).

#### 4.5.1 OCSP-Responder Proxy

Zur Statusprüfung von X.509-Zertifikaten werden die zuständigen OCSP-Responder in der TI betrieben. Ausnahmen hiervon sind die OCSP-Responder

- für Zertifikate der HBA-Vorläuferkarten

Diese werden nicht in der TI betrieben. Um deren Abfrage innerhalb der TI zu ermöglichen, wird ein OCSP-Responder Proxy bereitgestellt.

Ein solcher Proxy verfügt über keine eigene Signaturidentität, somit benötigt er kein X.509-Zertifikat. Aus diesem Grund erfolgt die Erwähnung nur der Vollständigkeit halber hinsichtlich OCSP-Dienste innerhalb der TI.

Die Verfügbarkeit der OCSP-Responder für Zertifikate der HBA-Vorläuferkarten muss für Zertifikatsstatusprüfungen innerhalb der TI durch einen Proxy sichergestellt werden.

##### TIP1-A\_2159 - Leistung des OCSP-Responder Proxy

Der OCSP-Responder Proxy MUSS die OCSP-Statusauskunft für Zertifikate der HBA-Vorläuferkarten in der TI verfügbar machen.

[<=]

##### TIP1-A\_2160 - Erreichbarkeit des OCSP-Responder Proxy

Der OCSP-Responder Proxy MUSS in der TI durch alle Komponenten und Dienste erreichbar sein.

[<=]

2268

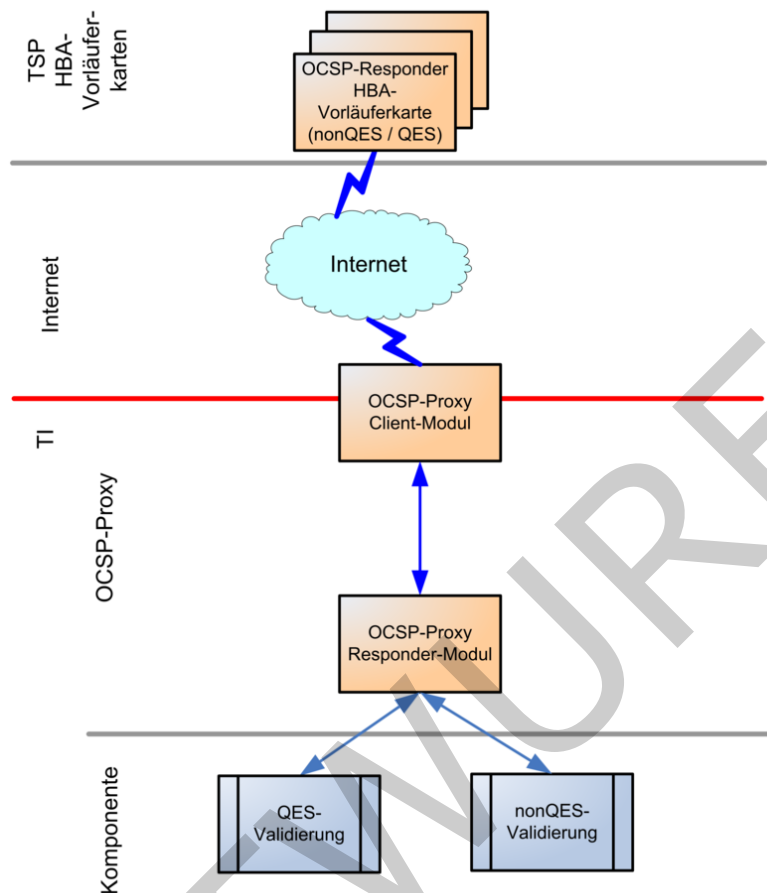


Abbildung 7: OCSP-Responder Proxy

2269

2270

2271

2272

## 2273 4.5.2 Einsatz von HSM

### 2274 TIP1-A\_2163 - Einsatz von HSMs zur Signatur von OCSP-Responses

2275 Der OCSP-Dienst KANN zur Signatur von OCSP-Responses ein HSM verwenden, sofern es  
 2276 die Anforderungen im jeweiligen Umfeld (nonQES, QES) erfüllt.

2277 [ $\leq$ ]

2278

## 5 CVC-Grundlagen und CVC-Hierarchie

2279

### 5.1 Funktion von CV-Zertifikaten

2280  
2281  
2282  
2283

Chipkarten der TI enthalten für die Authentisierung entsprechende Schlüsselpaare und zugehörige CV-Zertifikate. Durch eine Card-to-Card-Authentisierung (kurz: C2C-Authentisierung) weist eine Chipkarte ihre Echtheit gegenüber der anderen Chipkarte nach.

2284  
2285  
2286  
2287  
2288  
2289  
2290

Der Vertrauensanker der CVC-PKI ist der öffentliche Schlüssel der übergeordneten CVC-Root-CA, die zentral für die gesamte TI-Kartenfamilie im Verantwortungsbereich der gematik betrieben wird. Die Verifikation eines CV-Zertifikates erfolgt intern durch das Betriebssystem der Chipkarten, somit muss sich auch der Vertrauensanker innerhalb der Chipkarte befinden. Die Sub-CVC-CAs werden vom TSP-CVC betrieben und stellen im Auftrag der Kartenherausgeber die eigentlichen CV-Zertifikate über die kartenindividuellen Schlüssel einer Chipkarte aus.

2291  
2292  
2293  
2294  
2295  
2296

Neben verschiedenen technischen Parametern enthält ein CV-Zertifikat einer Chipkarte zur eindeutigen Identifizierung die ICCSN dieser Chipkarte und ein Zugriffsprofil. Bei korrekter Vergabe der ICCSN identifiziert diese die Chipkarte weltweit eindeutig. Über das in einem CV-Zertifikat enthaltene Zugriffsprofil wird festgelegt, welche konkreten Rechte bezüglich der Zugriffe auf Daten oder der Ausführbarkeit weiterer Funktionen in einer Chipkarte nach der C2C-Authentisierung erlangt werden. Dabei wird zwischen

2297  
2298

- Zugriffsprofilen für eine Authentisierung einer Rolle (in sog. CV-Rollen-Zertifikaten) und

2299  
2300

- Zugriffsprofilen für eine Authentisierung einer Funktionseinheit der Chipkarte (in sog. CV-Geräte-Zertifikaten)

2301

unterschieden. Funktionseinheiten sind bspw. SAK und Remote-PIN-Sender.

2302  
2303

Gemäß den derzeit definierten Anwendungen ist folgende Zuordnung dieser Zertifikatsarten auf die in der TI vorhandenen konkreten Chipkarten bindend:

2304

- eGKs enthalten nur CV-Rollenzertifikate.

2305

- gSMC-Ks und gSMC-KTs enthalten nur CV-Gerätezertifikate.

2306  
2307

- HBAs und SMC-Bs enthalten sowohl CV-Rollenzertifikate als auch CV-Geräte-Zertifikate.

2308

- Die KTR-AdV enthält zusätzlich zur SM-B ein zweites CV-Rollenzertifikat.

2309

#### **TIP1-A\_2164 - Abbildung des Zugriffsprofils in CV-Rollenzertifikaten**

2310  
2311  
2312  
2313

Die TI-Plattform MUSS sicherstellen, dass für ein CV-Rollenzertifikat, das in einer eGK, einem HBA oder einer SMC-B enthalten ist, das Zugriffsprofil angegeben wird, in welcher Rolle der Karteninhaber (Person bzw. Organisation) an der TI teilnimmt.

**[<=]**

2314  
2315  
2316

Über die in dem CV-Rollenzertifikat enthaltene Rolle wird festgelegt, welche Zugriffsrechte der Karteninhaber nach einer C2C-Authentisierung auf die in der anderen Chipkarte gespeicherten Daten erhält.

2317

#### **TIP1-A\_2165 - Abbildung des Zugriffsprofils in CV-Gerätezertifikaten**

2318  
2319

Die TI-Plattform MUSS sicherstellen, dass für ein CV-Gerätezertifikat, das in einem HBA, einer SMC-B oder einer gSMC-K(T) enthalten ist, das für die jeweilige Funktionseinheit

2320 der Karte definierte Zugriffsprofil implementiert wird.  
2321 [=]

## 2322 5.2 Hierarchie der CV-Zertifikate

2323 Gemäß des Vertrauensmodells der CVC-PKI ergibt sich die bereits in Abbildung 5  
2324 skizzierte 2-stufige Hierarchie der CVC-PKI.

### 2325 **TIP1-A\_2167 - Ausstellung von CV-Kartenzertifikaten durch CVC-Sub-CA**

2326 Die TI-Plattform MUSS sicherstellen, dass die EE-CV-Zertifikate über die  
2327 kartenindividuellen CV-Schlüssel einer Chipkarte (eGK, HBA, SMC) durch eine CVC-CA  
2328 der zweiten Ebene ausgestellt werden.  
2329 [=]

2330 Eine Chipkarte der TI kann über mehrere Rollen und somit über mehrere CV-  
2331 Schlüsselpaare mit zugeordneten CV-Zertifikaten verfügen. Zur Speicherplatzoptimierung  
2332 gilt jedoch, dass alle CV-Zertifikate einer Chipkarte von derselben CVC-CA ausgestellt  
2333 werden.

## 2334 5.3 Prozesse und Verantwortlichkeiten im Kontext CV-Zertifikate

2335 Die von der TI-Plattform zu definierenden Sicherheitsziele können nicht nur durch  
2336 Sicherheitsmaßnahmen bei einem der an der Produktion beteiligten Organisationen  
2337 erreicht werden. Es ist vielmehr eine zwischen den Beteiligten abgestimmte  
2338 Zusammenarbeit notwendig. Aus Sicht der TI-Plattform ist die CVC-CA stellvertretend für  
2339 alle Beteiligten für die Einhaltung der Anforderungen verantwortlich.

### 2340 **TIP1-A\_2169 - Definition von Ausgabepolicy und Betriebsvorgaben für CVC-Root-CA**

2341 Die TI-Plattform MUSS für die CVC-Root-CA eine Ausgabepolicy sowie Vorgaben für den  
2342 Betrieb dieser CA definieren und deren Einhaltung durch geeignete Maßnahmen  
2343 sicherstellen.  
2344 [=]

### 2346 **TIP1-A\_2170 - Definition von Betriebsvorgaben für CVC-Sub-CAs**

2347 Die TI-Plattform MUSS für die Zertifizierung von Sub-CVC-CA über alle TSP-CVC  
2348 einheitlich geltende Vorgaben für den Betrieb dieser CA definieren und deren Einhaltung  
2349 durch geeignete Maßnahmen sicherstellen.  
2350 [=]

### 2351 **TIP1-A\_2171 - Erstellung Ausgabepolicy durch TSP-CVC**

2352 Ein TSP-CVC MUSS für die Produktion von EE-CV-Zertifikaten eine Ausgabepolicy  
2353 erstellen, die nicht im Widerspruch zu den übergeordneten Ausgabepolicies stehen darf.  
2354 [=]

### 2355 **TIP1-A\_2172 - Erstellung Sicherheitskonzept Zertifikatsprozess durch TSP-CVC**

2356 Ein TSP-CVC MUSS für den Betrieb einer Sub-CVC-CA in einem Sicherheitskonzept den  
2357 Gesamtprozess von der Beantragung bis zur Einbringung des CV-Zertifikates in eine  
2358 Chipkarte beschreiben und die Einhaltung der beschriebenen Maßnahmen auf Verlangen  
2359 der TI-Plattform nachweisen. Sind mehrere Organisationen an diesem Prozess beteiligt,  
2360 sind die technischen und organisatorischen Schnittstellen sowie deren Absicherung zu  
2361 beschreiben – ggf. auch durch Referenzierung der Sicherheitskonzepte der beteiligten  
2362 Organisationen.  
2363 [=]

## 5.4 Aufbau und Inhalt von CV-Zertifikaten für G1-Karten

### 5.4.1 Zugriffsprofile

In einem CV-Zertifikat einer Chipkarte ist ein Zugriffsprofil dieser Chipkarte enthalten. Dabei wird gemäß Kap. 5.1 unterschieden zwischen einem Zugriffsprofil für die Authentisierung einer Rolle (CV-Rollenzertifikate) bzw. für die Authentisierung einer Funktionseinheit eines Gerätes (CV-Gerätezertifikate).

Bei einem Zugriffsprofil für eine Rollenauthentisierung weist eine Chipkarte nach einer C2C-Authentikation mit dem CV-Zertifikat gegenüber der anderen Karte nach, dass sie eine bestimmte Rolle hat.

Bei einem Zugriffsprofil für eine Authentisierung einer Funktionseinheit eines Gerätes weist eine Chipkarte nach einer C2C-Authentikation mit dem CV-Zertifikat gegenüber der anderen Karte nach, dass sie die zugehörige Funktionseinheit enthält.

## 5.5 Aufbau und Inhalt von CV-Zertifikaten für G2-Karten

### 5.5.1 Aufbau und Inhalt

Im Folgenden sind tabellarisch der Aufbau der CV-Zertifikate der Kartengeneration 2 sowie die Bedeutung der einzelnen Felder dargestellt.

#### **TIP1-A\_5138 - Struktur der CV-Zertifikate der Kartengeneration 2**

Die TI-Plattform MUSS CV-Zertifikate der Kartengeneration 2 gemäß der in Tab\_PKI\_108 definierten Struktur bereitstellen.

[<=]

**Tabelle 4: Tab\_PKI\_108 Informationen für ein CV-Zertifikat G2**

CPI	CAR	Öffentl. Punkt Q	OID- PuK	CHR	CHAT	CED	CXD
-----	-----	---------------------	-------------	-----	------	-----	-----

**Tabelle 5: Übersicht Felder eines CV-Zertifikats**

Feld	Inhalt
CPI	Certificate Profile Identifier: Dieser legt die genaue Struktur der Nachricht fest, über die die Signatur berechnet wird.
CAR	Certification Authority Reference: Eindeutiger Bezeichner des Schlüsselpaares, mit dessen privatem Schlüssel die CVC-CA das CV-Zertifikat signiert hat.
Öffentl. Punkt Q	Öffentlicher Punkt Q des öffentlichen Schlüssels, für den das CV-Zertifikat berechnet wird.

OIDPuK	OID des Algorithmus, mit dem der öffentliche Schlüssel des Zertifikatsinhabers (CVC-CA oder Chipkarte) genutzt werden kann.
CHR	Certificate Holder Reference: Eindeutiger Bezeichner des Schlüsselpaars des Zertifikatsinhabers, dessen öffentlichen Schlüssel in dem CV-Zertifikat enthalten ist.
CHAT	Certificate Holder Authorisation Template: Legt die Rolle des Zertifikatsinhabers fest.
CED	Certificate Effective Date: Ausgabezeitpunkt, ab wann das Zertifikat gültig ist
CXD	Certificate Expiration Date: Zeitpunkt für das Gültigkeitsende

2388

## 2389 5.5.2 Zugriffsprofile

2390 Anders als bei Karten der Generation 1 wird die Rolle eines Zertifikatsinhabers nicht  
 2391 durch den Inhalt eines CHA-Feldes ausgedrückt, sondern durch Abbildung in einer  
 2392 Berechtigungsmatrix, die wesentlich mehr unterschiedliche Zugriffsprofile ermöglicht.  
 2393 Dies erfolgt in Anlehnung an die [BSI-TR-03110 Part3]. Das generelle Prinzip der  
 2394 Zugriffsprofile für Rollen- bzw. Funktionseinheitsauthentisierung und dass diese im CV-  
 2395 Zertifikat hinterlegt werden, bleibt dagegen erhalten.

## 2396 5.6 Gültigkeitsmodell und Prüfung der CV-Zertifikate für G2-Karten

2397 Die Zertifikatsprüfung von CV-Zertifikaten ist vereinfacht gegenüber der Prüfung von  
 2398 X.509-Zertifikaten.

2399 CV-Zertifikate sind für einen offline-Einsatz konzipiert, somit entfallen eine  
 2400 Sperrmöglichkeit und dadurch auch die Notwendigkeit der Sperrstatusprüfung.

2401 Die Prüfung der CV-Zertifikate besteht aus der Prüfung der zeitlichen Gültigkeit und der  
 2402 Prüfung der mathematischen Korrektheit der Signatur in der Zertifikatskette. Die  
 2403 Prüfschritte erfolgen nach dem Schalenmodell komplett „intern“ durch das  
 2404 Betriebssystem der prüfenden Chipkarte.

2405 Die Chipkarte enthält zur zeitlichen Gültigkeitsprüfung eine Zeitvariable. Die CV-  
 2406 Zertifikate enthalten einen Ausgabezeitpunkt und ein Gültigkeitsende. Weitere  
 2407 Ausführungen siehe Folgekapitel 5.8.

### 2408 TIP1-A\_5139 - Prüfung von CV-Zertifikaten der Kartengeneration 2

2409 Die TI-Plattform MUSS eine Prüfmöglichkeit für CV-Zertifikate der Kartengeneration 2  
 2410 bereitstellen.

2411 [ $\leq$ ]

2412 Um die Nutzung der CV-Zertifikate der Kartengeneration 2 zu begrenzen, müssen Start-  
 2413 und Endedatum der Gültigkeit aufgenommen werden.

2414 Nach Ablauf des Gültigkeitszeitraums kann keine erfolgreiche C2C-Authentisierung mehr  
 2415 durchgeführt werden. Im Gegensatz zu den CV-Zertifikaten für G1-Karten sollen für die

2416 CV-Zertifikate der G2-Karten eine Zertifikatserneuerung implementiert und damit die  
2417 Gültigkeitsdauer verlängert werden.

2418 **TIP1-A\_5140 - Gültigkeitsdauer bei CV-Zertifikaten der Kartengeneration 2**  
2419 Die TI-Plattform MUSS die Gültigkeitsdauer von CV-Zertifikaten der Kartengeneration 2  
2420 beschränken.  
2421 [ $\leq$ ]

## 2422 **5.7 Konzeptionelle Grundlagen der Zertifikatserneuerung bei CV-** 2423 **Zertifikaten der G2-Karten**

### 2424 **5.7.1 Definition Gültigkeitsdauer, Zertifikatserneuerung und** 2425 **Sperrbarkeit**

2426 CV-Zertifikate der Kartengeneration 2 enthalten als Neuerung gegenüber CV-Zertifikaten  
2427 der Kartengeneration 1 ein Ausgabedatum sowie ein Ablaufdatum, der Zeitraum  
2428 dazwischen entspricht der Gültigkeitsdauer. Nur in diesem zeitlich eingegrenzten Bereich  
2429 ist ein CV-Zertifikatsimport und damit eine C2C-Authentisierung erfolgreich möglich. Wird  
2430 beabsichtigt, dem Zertifikatsinhaber auch nach Gültigkeitsende weiterhin die im CV-  
2431 Zertifikat enthaltene Rolle basierend auf dem bestehenden Schlüsselpaar zuzuweisen, so  
2432 ist ein neues CV-Zertifikat auf Basis des bestehenden öffentlichen Schlüssels  
2433 auszustellen, welches sich vom alten CV-Zertifikat nur durch geändertes Ausgabedatum  
2434 sowie Ablaufdatum unterscheidet.

2435 Die Neuausstellung der CV-Zertifikate wird auch als Zertifikatserneuerung bezeichnet.

2436 Eine Sperrung von CV-Zertifikaten vergleichbar mit dem Vorgehen bei X.509-Zertifikaten  
2437 ist (wie schon bei CV-Zertifikaten der Kartengeneration 1) nicht vorgesehen.

2438 Aus Sicht einer CVC-CA werden solange neue CV-Zertifikate für einen dedizierten  
2439 öffentlichen Schlüssel erstellt und zur Distribution angeboten, bis das Ende der Gültigkeit  
2440 des Schlüsselpaares erreicht ist oder die weitere Zertifikatserneuerung unterbunden wird.  
2441 Letzteres entspricht einer „Sperrung“ des Schlüsselpaares.

2442 Für neu ausgestellte Karten müssen in jedem Fall neue Schlüsselpaare generiert werden.

2443 Ein vorgezogenes Gültigkeitsende für die CV-Zertifikate der Kartengeneration 2 ist nur  
2444 für Karten notwendig, die mit Zugriffsrechten auf andere Karten ausgestattet sind, um  
2445 damit deren Missbrauchspotential einzugrenzen. Da die eGK über keine Zugriffsrechte  
2446 verfügt, kann die Gültigkeitsdauer des eGK-CV-Zertifikats die gesamte Laufzeit der  
2447 Kartengültigkeit umfassen.

### 2448 **5.7.2 Infrastruktur zur Zertifikatserneuerung**

2449 Die erneuerten CV-Zertifikate auf Basis der bestehenden Schlüssel werden von der CVC-  
2450 CA ausgestellt. Dazu muss die Karte einen Request an die CA stellen und die dort  
2451 erzeugten neuen Zertifikate müssen zurück zur Karte transportiert werden. Technisch ist  
2452 dafür eine Schnittstelle bei der CVC-CA notwendig, sowie eine „Prozesssteuernde  
2453 Instanz“. Diese Infrastruktur muss aufgebaut werden und zu einem definierten Zeitpunkt  
2454  $t_0$  bundesweit bereitstehen.



2455

---

## 6 Zertifikatsprüfung

---

2456

### 6.1 Grundlagen

2457

Die Zertifikatsprüfung gliedert sich in zwei wesentliche Schritte:

2458

- Prüfung des Vertrauensraums

2459

- Prüfung des eigentlichen Zertifikats

2460

### 6.2 Abgrenzung

2461

Die TI-Plattform stellt einen Dienst zur Prüfung von Zertifikaten bereit, der in der Architektur der TI-Plattform als Dienst „Prüfung\_Zertifikat“ beschrieben wird. Die Beschreibung der Schnittstellen und zugehörigen Operationen dieses Dienstes erfolgt in [gemKPT\_Arch\_TIP].

2462

2463

2464

2465

Im PKI-Konzept wird die Zertifikatsprüfung auf konzeptioneller Ebene beschrieben. Es werden, in Form von sogenannten „Ablaufschritten“, die Teilschritte der Vertrauensraum- und der Zertifikatsprüfung grob beschrieben inkl. der besonderen Merkmale der Prüfung qualifizierter Zertifikate

2466

2467

2468

2469

Für die Zertifikatsprüfung im Internet gilt die Vorgehensweise nach [\[Common-PKI\]-den Standards \[RFC5280\] und \[RFC6960\]](#).

2470

2471

Die zertifikatsprüfenden Komponenten müssen in ihren Spezifikationen die jeweiligen Besonderheiten der Zertifikatsprüfung selbst festlegen, wie z. B. der Wegfall von Statusprüfungen bei bestimmten Komponenten.

2472

2473

2474

Die Zertifikatsprüfung bei CV-Zertifikaten wird in Kap. 5.5 beschrieben.

2475

### 6.3 Vertrauensraumprüfung in der TI

2476

Bevor für ein Zertifikat als Teil der Zertifikatsprüfung die Zugehörigkeit zum Vertrauensraum der TI geprüft werden kann, muss zunächst die TSL als Ausprägung des Vertrauensraums bezogen und geprüft werden, um dann in einem sicheren Speicherbereich (Trust Store) abgelegt zu werden. Erst dann darf sie als valide Quelle für die o. g. „Zugehörigkeitsprüfung“ genutzt werden.

2477

2478

2479

2480

2481

#### 6.3.1 Ablaufschritte der Vertrauensraumprüfung

2482

##### TIP1-A\_2174 - Ablaufschritte der Vertrauensraumprüfung

2483

Die TI-Plattform MUSS die Prüfung des TI-Vertrauensraums entsprechend der in Tab\_PKI\_104 definierten Ablaufschritte umsetzen.

2484

2485

[<=]

2486

2487 **Tabelle 6: Tab\_PKI\_104 Ablaufschritte der Vertrauensraumprüfung**

<b>Ablaufschritte der Vertrauensraumprüfung</b> <b>Anmerkung: Die Sequenz der Ablaufschritte ist funktional hergeleitet, kann jedoch auch anders gestaltet werden, sofern das Ergebnis der Prüfung qualitativ äquivalent ist.</b>	
Ablaufschritt 1	Download der TSL
Beschreibung	Download der aktuellen Liste vom relevanten Verteilpunkt
Vorbedingung	Adresse des Verteilpunktes bekannt
Anmerkungen	Die Adresse wird im Regelfall aus der vorliegenden TSL ermittelt, initial wird die Adresse z. B. manuell konfiguriert oder die TSL organisatorisch bereitgestellt
Ablaufschritt 2a	Aktualitätsprüfung
Beschreibung	Prüfung, ob die herunterzuladende TSL neuer als die letzte vorhandene ist und noch innerhalb der Gültigkeitsperiode liegt
Vorbedingung	TSL im System
Anmerkungen	eine „abgelaufene“ TSL wird nicht als ungültig betrachtet
Ablaufschritt 2b	Schemaprüfung der TSL
Beschreibung	XML-Schemaprüfung
Vorbedingungen	heruntergeladene TSL, XML-Schema der TSL
Anmerkungen	das XML-Schema der TSL muss spezifiziert und benannt sein
Ablaufschritt 3	Prüfung des Signaturzertifikats
Beschreibung	Prüfung der Gültigkeit und des Vertrauensstatus des TSL-Signerzertifikats gegen sicher verwahrten TSL-Signer-CA-Schlüssel
Vorbedingung	vorliegender, sicher verwahrter TSL-Signer-CA-Schlüssel
Anmerkungen	diese Zertifikatsprüfung erfolgt gemäß den Festlegungen in Kap. 6.4
Ablaufschritt 4	Prüfung der XML-Signatur
Beschreibung	Standard Signaturprüfung einer XML-Signatur gemäß W3C-Vorgaben
Vorbedingung	erfolgreich validiertes TSL-Signerzertifikat
Anmerkungen	Vorgaben für Algorithmen und Schlüssellängen der Signatur müssen übergreifend getroffen werden

2488

## 2489 6.4 Vertrauensraumprüfung im Internet

2490 Der Vertrauensraum für die in der TI gültigen CA- und EE-Zertifikate wird im Internet  
2491 dadurch gebildet, dass für genau diese Zertifikate ein OCSP-Dienst zur Verfügung gestellt  
2492 wird. Die Prüfung erfolgt dabei nach den Vorgaben von [Common-PKI].

## 2493 6.5 Zertifikatsprüfung (nonQES)

### 2494 6.5.1 Konzeptionelle Festlegungen zur Zertifikatsprüfung

2495 Nachdem die TSL als Quelle des Vertrauensraums bezogen, geprüft, ausgewertet und in  
2496 einen Trust Store eingebracht wurde, kann sie als valide Quelle für die Ablaufschritte der  
2497 eigentlichen Zertifikatsprüfung verwendet werden.

2498 Die Zertifikatsprüfung orientiert sich an den [TI-spezifischen Anforderungen und den](#)  
2499 [Vorgaben der gängigen Standards \[RFC5280\] und \[Common-PKI\], RFC6960](#). Da als  
2500 zentraler Vertrauensanker kein übergeordnetes Root-Zertifikat verwendet wird, entfällt  
2501 die sonst übliche Bildung eines kompletten Zertifikatspfades von Endnutzerzertifikat über  
2502 CA-Zertifikat bis zum Root-Zertifikat und die Prüfung jedes dieser Zertifikate mittels der  
2503 üblichen Prüfschritte, um damit das Endnutzerzertifikat auf einen vertrauenswürdigen  
2504 Anker zurückzuführen. Stattdessen wird die TSL als Quelle des Vertrauensraums  
2505 verwendet. Daher reicht es aus, für die Prüfung der Vertrauenskette das CA-Zertifikat in  
2506 der TSL zu finden.

2507 Als Optimierung gegenüber [\[Common-PKI\], RFC6960](#) wird die Signaturprüfung des  
2508 OCSP-Signerzertifikats nicht nach den kompletten Prüfschritten durchgeführt. Das TSL-  
2509 Konzept erlaubt die OCSP-Signerzertifikate der TSP in die TSL aufzunehmen.

2510 Bis auf eine Ausnahme werden Statusauskünfte ausschließlich über OCSP-Dienste  
2511 realisiert, um die maximale Aktualität der Statusauskünfte gewährleisten zu können. Die  
2512 o.g. Ausnahme betrifft die Zertifikate des Zugangsdienstes (C.VPNK.VPN, C.VPNK.VPN-  
2513 SIS) und ist im Kapitel 4.3.3 beschrieben. Zur Vereinfachung der nachfolgenden  
2514 Darstellungen der Ablaufschritte der Zertifikatsprüfung (nonQES) wird generell von  
2515 OCSP-Diensten gesprochen.

2516 Zur Sperrstatusprüfung in der TI wird ausschließlich OCSP verwendet. Als Sonderfall  
2517 werden die Zertifikate des VPN-Zugangsdienstes (C.VPNK.VPN, C.VPNK.VPN-SIS) im  
2518 Internet gegen eine CRL geprüft (s.a. Kapitel 4.3.3).

2519 Entsprechend dem Vorgehen bei OCSP wird auch die Prüfung des CRL-Signerzertifikats  
2520 nur auf das Vorhandensein in der TSL geprüft.

2521 In der nachfolgenden Darstellung der Ablaufschritte der Zertifikatsprüfung (nonQES) wird  
2522 nur der Standardfall einer OCSP-Statusprüfung berücksichtigt.

2523 Aus Gründen der Lastreduzierung und Performancesteigerung ist es prinzipiell möglich,  
2524 OCSP-Responses zwischenspeichern und zu diesem Zweck einen OCSP-Cache  
2525 anzulegen. Anhand der Anforderungen der jeweiligen Anwendung, die eine  
2526 Zertifikatsprüfung nutzt, um bspw. Eine Signatur zu prüfen, muss diese festlegen, wie  
2527 aktuell eine Sperrinformation sein muss und daraus abgeleitet, welche maximale Dauer  
2528 für das Caching erlaubt sein soll.

2529 Es ist möglich, der Zertifikatsprüfung den Zeitpunkt mitzugeben, für den diese Prüfung  
2530 relevant sein soll, dieser wird auch als „Referenzzeitpunkt“ bezeichnet. Dies kann die  
2531 aktuelle Systemzeit sein, wenn die Prüfung zum Zeitpunkt „Jetzt“ erfolgen soll, um bspw.  
2532 Ein Verschlüsselungszertifikat des Kommunikationspartner zu prüfen, aber auch ein

2533 Zeitpunkt in der Vergangenheit, wie bspw. Im Rahmen einer Signaturprüfung der  
 2534 Zeitpunkt der Signaturerstellung, der sich aus der Signatur entnehmen lässt.

## 2535 6.5.2 Ablaufschritte der Zertifikatsprüfung

### 2536 TIP1-A\_2175 - Ablaufschritte der Zertifikatsprüfung nonQES

2537 Die TI-Plattform MUSS die Prüfung von Zertifikaten entsprechend der in Tab\_PKI\_105  
 2538 definierten Ablaufschritte umsetzen.

2539 [ $\leq$ ]

2540

2541 **Tabelle 7: Tab\_PKI\_105 Ablaufschritte der Zertifikatsprüfung**

<b>Ablaufschritte der Zertifikatsprüfung nonQES</b>	
<b>Anmerkung:</b> Die Sequenz der Ablaufschritte ist funktional hergeleitet, kann jedoch auch anders gestaltet werden, sofern das Ergebnis der Prüfung qualitativ äquivalent ist.	
Ablaufschritt 1	Prüfung der Vertrauenskette
Beschreibung	Prüfung, ob das zugehörige Ausstellerzertifikat in der TSL enthalten ist
Vorbedingung	TSL-Informationen in sicherem Speicher vorhanden
Anmerkungen	Die Prüfung erfolgt über den Vergleich von „Aussteller im Endnutzerzertifikat“ mit „Inhaber im CA-Zertifikat“.
Ablaufschritt 2	Signaturprüfung
Beschreibung	Prüfung der mathematischen Korrektheit des Zertifikats (Ableitung vom ermittelten Ausstellerzertifikat)
Vorbedingung	vorliegendes Ausstellerzertifikat
Anmerkungen	Die Prüfung erfolgt über Verifikation der Signatur und Hashwert-Vergleich.
Ablaufschritt 3	Prüfung der zeitlichen Gültigkeit
Beschreibung	Prüfung, ob der Referenzzeitpunkt innerhalb des im Zertifikat definierten Gültigkeitszeitraums liegt
Vorbedingung	keine
Anmerkungen	Im Zertifikat ist immer ein Zeitraum (gültig von ... bis ...) angegeben

Ablaufschritt 4	Prüfung des Sperrstatus
Beschreibung	Prüfung, ob Zertifikat gesperrt ist durch Abfrage des OCSP-Responders, ggf. durch Auswertung von in Signatur eingebetteter OCSP-Response
Vorbedingung	TSL-Informationen in sicherem Speicher vorhanden
Anmerkungen	OCSP-Adresse wird aus der TSL ermittelt, mehrere Adressen möglich, die der Reihe nach geprüft werden bis Prüfung erfolgreich ist.
Ablaufschritt 5	Weitere Prüfungen und Auswertungen
Beschreibung	Weitere Schritte die gemäß relevanter Standards verpflichtend sind, sowie weitere TI-spezifische Auswertungen, s. Informationen in Abschnitt 6.5.3
Vorbedingung	

### 6.5.3 Weitere Prüfungen und Auswertungen

Neben den hier dargestellten grundsätzlichen Ablaufschritten gibt es weitere Prüfschritte, die gemäß den Standards [Common PKI] und [RFC5280] und [RFC6960] verpflichtend umzusetzen sind:

- Prüfung auf Korrektheit des Verwendungszwecks (vorgesehene Schlüsselverwendung (KeyUsage) und, wenn vorhanden, vorgesehene erweiterte Schlüsselverwendung (ExtendedKeyUsage))
- Prüfung auf akzeptierte Zertifikatsrichtlinie (Certificate Policy)

#### **TIP1-A\_2176-01 - Vorgaben zur Zertifikatsprüfung gemäß internationaler Standards**

Die TI-Plattform MUSS bei der Prüfung von Zertifikaten Vorgaben hinsichtlich Prüftiefe und Prüfungsumfang gemäß den Standards [Common PKI], [RFC2560] und [RFC6960] definieren. [≤]

Darüber hinaus gibt es Auswertungen der Zertifikate, die TI-spezifisch sind:

**Rollenermittlung:** Im Endnutzertifikat müssen Informationen bzgl. der Rolle des durch das Zertifikat bestätigten Akteurs hinterlegt werden. Je nach Zertifikatstyp repräsentieren diese Rollen entweder Berufsgruppen (Bsp. „Arzt“) oder technische Gerätegruppen (Bsp. „Kartenterminal“). Die Definition zu Repräsentationsart und Speicherort der Rolle innerhalb des Zertifikats wird in den jeweiligen Zertifikatsprofilen spezifiziert.

**TIP1-A\_2177 - Ermittlung von Rolleninformationen bei der Zertifikatsprüfung**

Die TI-Plattform MUSS bei der Prüfung von Zertifikaten die Rolleninformation aus dem Zertifikat ermitteln und an die aufrufende Anwendung zurückgeben.

[<=]

Die weitere Verwendung der ermittelten Rolle (eine oder mehrere) sowie deren Prüfung gegen eine im Zertifikat erwartete Rolle liegt im Verantwortungsbereich der aufrufenden Anwendung.

**Zertifikatstypermittlung:** Als Vorbereitung für weitere Prüfschritte kann es notwendig sein, zu ermitteln, um welchen Typ von Zertifikat es sich handelt, bspw. eGK-AUT-Zertifikat oder HBA-ENC-Zertifikat. Dazu muss dieser sog. Zertifikatstyp im Zertifikat selbst hinterlegt sein. Die genaue Definition zur Darstellung und Speicherort des Zertifikatstyps innerhalb des Zertifikats erfolgt in den Spezifikationen der jeweiligen Zertifikatsprofile. Im Rahmen der Zertifikatsprüfung muss es möglich sein, den Zertifikatstyp aus dem Zertifikat zu ermitteln.

**TIP1-A\_4499 - Ermittlung des Zertifikatstyps bei der Zertifikatsprüfung**

Die TI-Plattform MUSS bei der Prüfung von Zertifikaten den Zertifikatstyp aus dem Zertifikat ermitteln und an die aufrufende Anwendung zurückgeben.

[<=]

Innerhalb des Prozesses zur Zulassung eines TSP-X.509 zur Aufnahme in die TSL können Informationen erfasst werden, für welche Zertifikatstypen dieser TSP mit der jeweiligen CA erstellungsberechtigt ist, z. B. nur für Komponentenzertifikate, oder nur für eGK-Zertifikate. Diese Informationen – hinterlegt im Element „ServiceInformationExtensions“ in der TSL (siehe TAB\_PKI\_113) – ergeben sich anhand der Beauftragungen durch die für den jeweiligen Kartentyp verantwortlichen Kartenherausgeber.

**Tabelle 8: TAB\_PKI\_113 Zuordnung der (zugelassenen) X.509-Sub-CAs zu Zertifikatstypen**

Spezifischer CA-Einsatzbereich	CN (<usage> im Feld DN)	OID-Referenz in anderen Dokumenten	Name des Zertifikatstyp	Referenz/Anmerkung
Elektronische Gesundheitskarte	<TSP>.eGK-CA<n> *) z.B. ATOS.EGK-CA201	oid_egk_enc	C.CH.ENC	[gemSpec_PKI#5.1.3;5.11] [gemSpec_OID#Tab_PKI_405]
		oid_egk_encv	C.CH.ENCV	[gemSpec_PKI#5.1.3;5.11] [gemSpec_OID#Tab_PKI_405]
		oid_egk_aut	C.CH.AUT	[gemSpec_PKI#5.1.3;5.11] [gemSpec_OID#Tab_PKI_405]

		oid_egk_autn	C.CH.AUTN	[gemSpec_PKI#5.1.3;5.11] [gemSpec_OID# Tab_PKI_405]
	<TSP>.eGK-ALVI-CA<n> *)	oid_egk_aut_al t	C.CH.AUT_A LT	[gemSpec_PKI#5.1.3;5.11] [gemSpec_OID# Tab_PKI_405]
Heilberufsausweis	<TSP>.HBA-qCA<n> *) D-Trust.HBA-qCA1	oid_hba_qes	C.HP.QES	[gemSpec_PKI#5.11;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_hba_enc	C.HP.ENC	[gemSpec_PKI#5.11;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_hba_aut	C.HP.AUT	[gemSpec_PKI#5.11;5.11] [gemSpec_OID# Tab_PKI_405]
Institutionskarten	<TSP>.SMCB-CA<n> *) z.B. D-Trust.SMCB-CA1	oid_smc_b_enc	C.HCI.ENC	[gemSpec_PKI#5.3.4;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_smc_b_aut	C.HCI.AUT	[gemSpec_PKI#5.3.4;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_smc_b_osig	C.HCI.OSIG	[gemSpec_PKI#5.3.4;5.11] [gemSpec_OID# Tab_PKI_405]
Komponenten-PKI	<TSP>.KOMP-CA<n> *) z.B. GEM.KOMP-CA1	oid_fd_tls_s	C.FD.TLS-S	[gemSpec_PKI#5.9.3;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_zd_tls_s	C.ZD.TLS-S	[gemSpec_PKI#5.8.3;5.11] [gemSpec_OID# Tab_PKI_405]



		oid_smkt_aut	C.SMKT.AUT	[gemSpec_PKI#5.5.2;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_nk_vpn	C.NK.VPN	[gemSpec_PKI#5.6.4;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_sak_aut	C.SAK.AUT	[gemSpec_PKI#5.6.4;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_ak_aut	C.AK.AUT	[gemSpec_PKI#5.6.4;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_cm_tls_c	C.CM.TLS-CS	[gemSpec_PKI#5.10.3;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_fd_tls_c	C.FD.TLS-C	[gemSpec_PKI#5.9.3;.11] [gemSpec_OID# Tab_PKI_405]
		oid_fd_aut	C.FD.AUT	[gemSpec_OID# Tab_PKI_405]
		oid_zd_tls_c	C.ZD.TLS-C	[gemSpec_OID# Tab_PKI_405] (derzeit nicht verwendet)
		oid_zd_aut	C.ZD.AUT	[gemSpec_OID# Tab_PKI_405] (derzeit nicht verwendet)
		oid_fd_sig	C.FD.SIG	[gemSpec_OID# Tab_PKI_405]
		oid_fd_enc	C.FD.ENC	[gemSpec_OID# Tab_PKI_405]
		oid_sgd_hsm_aut	C.SGD-HSM.AUT	[gemSpec_OID# Tab_PKI_405]

VPN-Zugangsdienst	<TSP>.VPN K-CA<n> *) z.B. GEM.VPNK- CA1	oid_vpnk_vpn	C.VPNK.VPN	[gemSpec_PKI#5.7.3;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_vpnk_vpn_sis	C.VPNK.VPN-SIS	[gemSpec_PKI#5.7.3;5.11] [gemSpec_OID# Tab_PKI_405]

\*) Für CA-Zertifikate der zentralen PKI wird für <ts> die Bezeichnung "GEM" und für <tsName> "gematik GmbH" eingesetzt; für von TSPs betriebene Sub-CAs wird das jeweilige TSP-Kürzel sowie der vollständige TSP-Name eingefügt. Bei laufenden beispielhaften SubCA-Nummern können Abweichungen auftreten.

## 6.6 QES-Zertifikatsprüfung

### 6.6.1 Konzeptionelle Festlegungen zur QES-Zertifikatsprüfung

Bei der Prüfung qualifizierter Zertifikate gibt es eine Reihe grundlegender Aspekte, die sich von der Prüfung nicht-qualifizierter Zertifikate unterscheiden. Die Prüfung erfolgt im Rahmen der Vorgaben aus [eIDAS].

Als Gültigkeitsmodelle lässt [eIDAS] Schalen- und Kettenmodell zu. In der TI wird das Kettenmodell als verbindlich festgelegt.

Die Gültigkeitsprüfung bezieht sich grundsätzlich auf den Signaturerstellungszeitpunkt als Referenzzeitpunkt, nicht auf den Zeitpunkt der Prüfung (Systemzeit).

Die OCSP-Prüfung eines QES-Zertifikates kann entfallen, wenn dies vom Benutzer explizit gewünscht oder eine Online-Verbindung nicht möglich ist. In diesem Fall muss der Benutzer aber explizit auf den Offline-Fall hingewiesen werden

Die Gültigkeitsprüfung von CA-Zertifikaten der QES-VDAs erfolgt durch die Prüfung auf sein Vorhandensein in der BNetzA-VL und seines Servicestatus in der BNetzA-VL.

Generelle Prüfschritte gemäß [Common PKI eIDAS] und [nach technischen Festlegungen aus den Standards ([RFC5280], [RFC6960]), wie die Prüfung der zeitlichen Gültigkeit, Verwendungszeit (keyUsage), OCSP-Prüfung, sind auch bei der QES-Prüfung obligatorisch. Sie sind in der folgenden Übersicht zwecks Vereinfachung und Übersichtlichkeit nicht aufgeführt.

### 6.6.2 Ablaufschritte der QES-Zertifikatsprüfung

#### TIP1-A\_2178 - Ablaufschritte der QES-Zertifikatsprüfung

Die TI-Plattform MUSS die Prüfung von Zertifikaten entsprechend der in Tab\_PKI\_106 definierten Ablaufschritte umsetzen.

[<=]

2621 Tabelle 9: Tab\_PKI\_106 Ablaufschritte der QES-Zertifikatsprüfung

<b>Ablaufschritte der QES-Zertifikatsprüfung</b> <b>Anmerkung:</b> Die Sequenz der Ablaufschritte ist funktional hergeleitet, kann jedoch auch anders gestaltet werden, sofern das Ergebnis der Prüfung qualitativ äquivalent ist.	
Ablaufschritt 1	Prüfung ob „qualifiziert“
Beschreibung	Prüfung, ob das QES-Zertifikat das spezifische QES-Attribut („QCStatement“) als Merkmal enthält
Vorbedingung	keine
Ablaufschritt 2	Prüfung des QES-CA-Zertifikates gegen die BNetzA-VL
Beschreibung	Das QES-CA-Zertifikat wird gegen die BNetzA-VL zum Referenzzeitpunkt geprüft (Prüfung auf Vorhandensein und gültigen Servicestatus des QES-CA-Zertifikates)
Vorbedingungen	BnetzA-VL
Anmerkungen	Gültiger Servicestatus des QES-CA-Zertifikates gemäß [ETSI TS 119 612#Annex J] zum Referenzzeitpunkt
Ablaufschritt 3	Validierung der Zertifikatssignatur
Beschreibung	Prüfung der mathematischen Korrektheit des QES-Zertifikats (Ableitung vom ermittelten QES-CA-Zertifikat )
Vorbedingungen	QES- und QES-CA-Zertifikat vorhanden
Anmerkungen	Die Prüfung erfolgt über Verifikation der Signatur
Ablaufschritt 4	Prüfung des Sperrstatus
Beschreibung	Prüfung, ob Zertifikat gesperrt ist durch Abfrage des OCSP-Responders, ggf. durch Auswertung von in Signatur eingebetteter OCSP-Response. Dabei sind die Sonderfälle für die Ermittlung der OCSP-Responder-Adresse (aus End-Entity-Zertifikat bzw. TSL, s. Kap. 4.4.2) und die Prüfung des OCSP-Signer-Zertifikats (s. Kap. 4.5) zu beachten.
Vorbedingung	QES-Zertifikat vorhanden
Anmerkungen	OCSP-Dienste für QES-Zertifikate müssen den Vorgaben von [eIDAS] genügen. Die Ableitung des OCSP-Signer-Zertifikates erfolgt normalerweise gemäß [RFC6960] (zu Abweichungen davon vgl. Kap. 4.5)

## 6.7 Festlegungen zur Durchführung

### 6.7.1 Durchführung von Zertifikatsprüfungen

Kryptographische Identitäten werden zur Erreichung folgender Schutzziele eingesetzt:

- Authentizität -> technische Umsetzung mittels zertifikatsbasierter Identitäten -> Notwendigkeit der Zertifikatsprüfung bei Authentisierung von Akteuren
- Vertraulichkeit -> technische Umsetzung mittels Verschlüsselung -> Notwendigkeit der Zertifikatsprüfung bei der Verschlüsselung von Daten
- Integrität -> technische Umsetzung mittels Datensignatur -> Notwendigkeit der Zertifikatsprüfung bei der Signaturprüfung

#### TIP1-A\_2179 - Anwendungskontext für Zertifikatsprüfungen

Die TI-Plattform MUSS die Zertifikatsprüfung durchführen im Kontext der

(a) Authentisierung von Akteuren und Komponenten,

(b) Verschlüsselung von Daten und der

(c) Signaturprüfung inkl. QES-Signaturprüfung.

[<=]

### 6.7.2 Spezialfälle der Zertifikatsprüfung

#### Offline-Prüfung

Die Unterscheidung, ob offline oder online geprüft wird, wirkt sich auf Ablaufschritt 4 „Prüfung des Sperrstatus“ der Zertifikatsprüfung aus.

Prinzipiell wird die Offline-Prüfung erfolgen:

- falls aus technischen Gründen der OCSP-Responder nicht erreichbar ist
- falls sonstige technische Gründe eine gültige Antwort verhindern.

Falls im Online-Fall technische Gründe verhindern, dass eine Statusüberprüfung erfolgreich durchgeführt werden kann, ist damit die Zertifikatsprüfung als Ganzes unvollständig. Es kann nicht garantiert werden, dass das Zertifikat, das für eine Authentisierung, Verschlüsselung oder Signaturprüfung zugrunde liegt, noch gültig ist und nicht zwischenzeitlich gesperrt wurde.

Eine Backup-Lösung in Form von Zertifikatssperrlisten ist im Kontext der Zertifikatsprüfung nicht vorgesehen. Es liegt im Ermessen des Prüfenden, ob er dem unvollständigen Prüfergebnis vertraut oder er das Risiko als so groß einstuft, dass er die gesamte Zertifikatsprüfung verwirft und das Zertifikat als „nicht gültig“ bewertet. So könnte bspw. Mittels eines Übergabeparameters eine Offline-Prüfung von vornherein toleriert (aber nicht erzwungen!) werden, die in dem Fall (OCSP-Auskunft konnte nicht eingeholt werden) zu einem „gültig“ Resultat führen würde.

#### TIP1-A\_2180 - Warnmeldung bei Offline-Fall der Zertifikatsprüfung

Die TI-Plattform MUSS die Zertifikatsprüfung so gestalten, dass auf besondere Anforderung der aufrufenden Funktion ein Sperrstatus als gültig bewertet wird, auch wenn eine Online-Prüfung nicht erfolgreich abgeschlossen werden konnte. Es MUSS dabei eine Warnmeldung zurückgegeben werden mit einem Hinweis, dass nur offline geprüft wurde. Dabei MUSS sichergestellt werden, dass eine technisch mögliche Online-Prüfung nicht verhindert wird.

[<=]

#### Caching-Modus

2665 Sperrinformationen müssen nicht aktuell beim OCSP-Responder abgefragt werden,  
2666 sondern können von einer zertifikatsprüfenden Komponente auch gespeichert werden.

2667 Sperrinformationen werden für eine bestimmte Zeitdauer als gültig bewertet, abhängig  
2668 vom Anwendungsfall (z. B. dem jeweiligen Schutzbedarf). Daraus lassen sich Caching-  
2669 Mechanismen ableiten, um die Anzahl von Abfragen zu reduzieren und damit die  
2670 Lastanforderungen an OCSP-Responder zu senken. Erforderlich ist die Festlegung eines  
2671 Zeitraums, für den eine OCSP-Response maximal als gültig angesehen werden darf. Dazu  
2672 kann per Konfiguration festgelegt werden, wie lange dieser Zeitraum ist bzw. ob  
2673 überhaupt ein Caching genutzt werden soll.

#### 2674 **TIP1-A\_2181 - Default-Lebensdauer einer Statusantwort**

2675 Die TI-Plattform MUSS die Zertifikatsprüfung so gestalten, dass eine Default-  
2676 Lebensdauer einer Statusantwort über die gesamte TI festgelegt und dynamisch nach  
2677 Vorgaben der TI-Plattform verändert werden kann.  
2678 [ $\leq$ ]

#### 2679 **TIP1-A\_2182 - Lebensdauer einer Statusantwort**

2680 Die TI-Plattform MUSS bei der Zertifikatsprüfung die akzeptierte Lebensdauer einer  
2681 Statusantwort wählbar gestalten.  
2682 [ $\leq$ ]

#### 2683 **Nutzung eingebetteter OCSP-Responses**

2684 Sperrinformationen können für den Fall von Signaturen auch in die Datenstruktur der  
2685 Signatur eingebettet sein, wenn bei der Erstellung der Signatur gleich die OCSP-  
2686 Response über den Status des Signaturzertifikats eingeholt wird. Bei der  
2687 Zertifikatsprüfung kann dann diese eingebettete, bereits vorliegende OCSP-Response  
2688 genutzt werden, eine Abfrage beim OCSP-Responder ist damit nicht notwendig.

2689 Mit diesem Vorgehen lassen sich die Lastanforderungen an die OCSP-Responder senken.  
2690 Die Zertifikatsprüfung ist so zu gestalten, dass vor Abfrage des OCSP-Responders auf  
2691 Vorhandensein dieser eingebetteten OCSP-Response geprüft wird.

### 2692 **6.7.3 Bedingungen für eine erfolgreiche Zertifikatsprüfung**

#### 2693 **TIP1-A\_2184 - Bedingungen für Zertifikatsprüfung**

2694 Die TI-Plattform DARF als Prüfergebnis einer Zertifikatsprüfung NICHT das Zertifikat als  
2695 gültig bewerten, wenn nicht alle definierten Ablaufschritte der Zertifikatsprüfung  
2696 erfolgreich durchlaufen sind. Als Ausnahmen bei Ablaufschritt 4 „Prüfung des  
2697 Sperrstatus“ sind erlaubt: Prüfung mit tolerierter Nichterreichbarkeit des OCSP-  
2698 Responders.

2699 [ $\leq$ ]

2700 Es ist zu unterscheiden zwischen dem Prüfvorgang, ob dieser erfolgreich durchgeführt  
2701 wurde, und dem eigentlichen Prüfergebnis der Zertifikatsprüfung.

2702 Der Prüfvorgang kann folgende Status haben:

- 2703
- 2704 • Prüfvorgang komplett durchgeführt
  - 2705 • Prüfvorgang durchgeführt mit Einschränkungen (einzelne Prüfschritte konnten  
2706 nicht durchgeführt werden)
  - 2707 • Prüfvorgang fehlgeschlagen (kritische Prüfschritte konnten nicht durchgeführt  
2708 werden)

2708 Als Prüfergebnis („VerificationResult“) einer durchgeführten Prüfung sind möglich:

- 2709
- Zertifikat ist gültig

2710 • Zertifikat ist gültig mit Einschränkung (Online-Prüfung des Gültigkeitsstatus  
2711 konnte nicht durchgeführt werden, TSL ist abgelaufen); die Einschränkung wird in  
2712 Form einer Warnung mit ausgegeben

2713 • Zertifikat ist gesperrt seit <Sperrdatum>

2714 Bei qualifizierten Zertifikaten muss das Prüfergebnis in Bezug zum Referenzzeitpunkt  
2715 (Zeitpunkt der Erstellung der Signatur) gesetzt werden. D. h. bei einer Sperrung des  
2716 Zertifikats nach Erstellung der Signatur, ist das Zertifikat zum Referenzzeitpunkt der  
2717 Erstellung der Signatur als gültig zu betrachten.  
2718

### 2719 **TIP1-A\_2185 - Prüfung und Interpretation der TSL-Graceperiod**

2720 Die Produkttypen der TI-Plattform, die Zertifikate prüfen, MÜSSEN im Falle einer  
2721 abgelaufenen TSL auch auf die zeitliche Überschreitung der TSL-Graceperiod prüfen:  
2722 (a) TSL-Graceperiod nicht überschritten: es müssen die Einträge in der TSL als „gültig“  
2723 gewertet werden und die prüfende Einheit muss einen Warnhinweis an die aufrufende  
2724 Funktion/Anwendung zurückmelden.

2725 (b) TSL-Graceperiod überschritten: die prüfende Einheit muss eine Fehlermeldung an die  
2726 aufrufende Funktion/Anwendung zurückgeben, da keine valide Prüfbasis vorliegt. Eine  
2727 Aussage über die Gültigkeit des angefragten Aussteller-CA-Zertifikates wird in diesem  
2728 Falle nicht gegeben.

2729 [ $\leq$ ]

2730

## 7 Betriebliche Aspekte der PKI

### 2731 7.1 Einführung

2732 Innerhalb der PKI der TI-Plattform müssen neben der rein technischen Sicht auf  
2733 Zertifikats- und CA-Strukturen auch aus der Betriebsperspektive die für die Umsetzung  
2734 notwendigen Dienste betrachtet werden. Dazu müssen zugehörige Rollen identifiziert und  
2735 Schnittstellen beschrieben werden.

2736 Die beim jeweiligen TSP für die Umsetzung der Dienste notwendigen internen Rollen sind  
2737 nicht Gegenstand der Betrachtung. Weitere betriebliche Rollen (gemäß ITIL und weiteren  
2738 best-practise Modellen), werden hier ebenfalls nicht betrachtet.

2739 Die hier dargestellte Sicht konzentriert sich auf zwei Aspekte:

- 2740 • Verfahren im Rahmen der Aufnahme eines TSP-X.509 in den Vertrauensraum der  
2741 TI; siehe Kap. 7.2.
- 2742 • Dienste, die der TSP-X.509 im Rahmen des Lebenszyklus der X.509-Zertifikate  
2743 von der Erstellung bis zur Sperrung implementieren muss; siehe Kap. 7.3 (für die  
2744 CV-Zertifikate sind die Ausführungen zu Sperr- und Validierungsdienst nicht  
2745 anwendbar).

#### 2746 7.1.1 Rollen

2747 Im Zertifikatslebenszyklus sind folgende Rollen relevant:

2748 **Antragsberechtigter:** ist berechtigt, Zertifikate beim TSP zu beantragen und wird im  
2749 Folgenden auch als „Antragsteller“ oder „Zertifikatsantragsteller“ bezeichnet.

2750 **Sperrberechtigter:** ist berechtigt, Zertifikate beim TSP-X.509 zu sperren.

2751 Zur Verwaltung dieser Rollen gegenüber dem TSP muss eine **Berechtigungsprüfende**  
2752 **Stelle** existieren.

2753 Spätere Änderungen bei der personellen Besetzung der Rollen sind möglich. Sie müssen  
2754 der berechtigungsprüfenden Stelle mitgeteilt werden. Der Datenaustausch zwischen der  
2755 berechtigungsprüfenden Stelle und dem TSP muss über etablierte Schnittstellen erfolgen.  
2756 In welcher Form und über welche Schnittstellen dies geschieht, wird im vorliegenden  
2757 Konzept noch nicht betrachtet.

2758 Im Kontext der unterschiedlichen Verantwortlichkeiten für die Zertifikate der  
2759 Versicherten, der Leistungserbringer und Institutionen sowie der Komponentenzertifikate  
2760 ergeben sich unterschiedliche Besetzungen der Rollen und der jeweils  
2761 berechtigungsprüfenden Stelle.

#### 2762 7.1.2 Authentisierung der Rolleninhaber

2763 Bei der Bearbeitung eines Antrags zur Erstellung oder Sperrung eines Zertifikats muss  
2764 durch den TSP sichergestellt werden, dass die jeweilige Person in ihrer Rolle sicher und  
2765 eindeutig identifiziert und authentifiziert, und ihre Berechtigung anhand der von der  
2766 berechtigungsprüfenden Stelle mitgeteilten Daten überprüft wird.



**TIP1-A\_2186 - Sichere Authentifizierung von PKI-Prozess-Rolleninhabern**

Die TI-Plattform MUSS sicherstellen, dass die Rolleninhaber der PKI-Prozesse sicher authentifiziert werden.

[<=]

**7.2 Zulassung von TSP in den Vertrauensraum der TI**

Um im Vertrauensraum der X.509 Zertifikate der TI als berechtigter TSP tätig zu werden, muss der TSP in die TSL als technische Umsetzung des Vertrauensraums aufgenommen werden und dazu ein Zulassungsverfahren durchlaufen.

Im Bereich der CV-Zertifikate wird der Vertrauensraum durch einen zentralen Vertrauensanker in Form einer CVC-Root-CA umgesetzt. Um als Zertifikatsherausgeber tätig zu werden, muss ein Anbieter seine CVC-Sub-CA von der übergeordneten CVC-Root-CA zertifizieren lassen und dabei ein ähnlich gelagertes Registrierungsverfahren durchlaufen. Erst dann ist er berechtigt, CV-Zertifikate auszustellen und nur dann lassen sich diese auf die gemeinsame CVC-Root-CA zurückführen und erfolgreich validieren.

CVC-Sub-CAs werden auch als CVC-CAs der zweiten Ebene bezeichnet.

Im Folgenden sind Eckpunkte und Rollen für diese beiden Zulassungsverfahren für ein einführendes Verständnis grob skizziert.

**7.2.1 Zulassung von TSP-X.509 zur Aufnahme in die TSL**

Die Zulassung von TSP für X.509-Zertifikate dient der Zugangsberechtigung dieser TSP zum Vertrauensraum der X.509-PKI der TI-Plattform und zur Erstellung von X.509-Personen-, Organisations-, Komponenten- und Dienstzertifikaten.

Zu berücksichtigende Eckpunkte sind:

- Die gematik trägt die Gesamtverantwortung für die Sicherheit von X.509-Zertifikaten und definiert somit die Sicherheitsvorgaben für die TSP und auch für den Anbieter des TSL-Dienstes. Daraus leitet sich auch die Verantwortung für die Prüfung der Sicherheitseignung der TSP ab, die in einem entsprechenden Verfahren durchgeführt und bestätigt werden muss.
- Der TSL-Dienst erzeugt die TSL und nimmt auf Anweisung der gematik TSP-X.509 in die TSL auf.

Hieraus werden folgende Rollen abgeleitet:

**Tabelle 10: Übersicht der Rollen und deren Aufgaben bei der TSP-Zulassung**

Rolle	Aufgabe/Funktion
Anbieter TSL-Dienst	erzeugt die TSL zyklisch und ad-hoc auf besondere Anforderung der gematik
TSP-X.509	beantragt die Aufnahme in die TSL
gematik	Gesamtverantwortung für den TI-Betrieb und Zulassung der TSP

2799

## 2800 7.2.2 Zulassung von CVC-CAs der zweiten Ebene

2801 Die gematik-Zulassung eines TSP-CVC als CVC-Sub-CA-Anbieter berechtigt diesen:

- 2802 • zum Betrieb einer von der gematik CV-Root-CA abgeleiteten CV-Sub-CA
- 2803 • zur Erstellung von CV-Zertifikaten für Kartenherausgeber zur Einbringung in
- 2804 Chipkarten bzw. Sicherheitsmodule.

2805 Zu berücksichtigende Eckpunkte sind:

- 2806 • Die gematik trägt die Gesamtverantwortung für die Sicherheit von CV-Zertifikaten
- 2807 und definiert somit die Sicherheitsvorgaben für die Anbieter der CVC-Sub-CA und
- 2808 auch der CVC-Root-CA. Daraus leitet sich auch die Verantwortung für die Prüfung
- 2809 der Sicherheitseignung der Anbieter ab, die in einem entsprechenden Verfahren
- 2810 durchgeführt und bestätigt werden muss.
- 2811 • Nur die CVC-Root-CA als Besitzer des übergeordneten Root-Schlüsselpaars kann
- 2812 die Ausstellung der CV-CA-Zertifikate vornehmen.
- 2813 • Die CV-Zertifikate enthalten Rollenattribute, über die Zugriffsprofile umgesetzt
- 2814 werden. Die Bestätigung, dass in ein CV-Zertifikat ein bestimmtes Zugriffsprofil
- 2815 eingebracht werden darf, muss durch eine zuständige Qualifizierende
- 2816 Stelle gemäß [gemSpec\_PKI#Tab\_PKI\_254] erfolgen, bspw. Ärztekammer für das
- 2817 Arztattribut, vgl. dazu auch Kap 2.7.9.2.

2818 Hieraus werden folgende Rollen abgeleitet:

2819

2820 **Tabelle 11: Übersicht der Rollen und deren Aufgaben bei der Zulassung von CVC-CAs**

Rolle	Aufgabe/Funktion
TSP-CVC-Root	stellt die CV-CA-Zertifikate für die CVC-Sub-CA-Anbieter aus
TSP-CVC-CA (Anbieter der CVC-Sub-CA)	beantragt CV-CA-Zertifikat und nutzt dieses nach Erhalt zur Produktion von CV-Zertifikaten
gematik	Gesamtverantwortung für den TI-Betrieb und Zulassung der TSP

## 2821 7.3 TSP-Dienste im Rahmen des X.509-Zertifikatslebenszyklus

### 2822 7.3.1 Registrierungsdienst

2823 Der Registrierungsdienst nimmt die Zertifikatsanträge eines Antragsberechtigten

2824 entgegen und leitet diese nach erfolgreicher Authentifizierung und Autorisierung an den

2825 Erstellungsdienst weiter. Nach Erstellung wird das Zertifikat an den Antragsteller

2826 ausgeliefert.

2827 Zu berücksichtigende Eckpunkte sind:

- Um sicherzustellen, dass ein TSP-X.509 nicht für Unberechtigte Zertifikate erstellt, muss eine berechtigungsprüfende Stelle übergreifend festlegen, wer welche Zertifikate (Komponenten, etc.) beim TSP-X.509 beantragen darf.
- Der TSP-X.509 muss vor Zertifikatserstellung die Berechtigung des Antragsstellers prüfen.

Basierend auf diesen Eckpunkten ergeben sich folgende Rollen:

**Tabelle 12: Übersicht der Rollen und deren Aufgaben beim Registrierungsdienst**

Rolle	Aufgabe/Funktion
TSP-X.509	nimmt Anfragen entgegen und liefert Zertifikate nach Erstellung aus
Antragsberechtigter	beantragt Zertifikat und setzt dieses nach Auslieferung ein
Berechtigungsprüfende Stelle	verwaltet wer die Berechtigung besitzt, einen bestimmten Zertifikatstyp zu beantragen und teilt diese Berechtigungen dem TSP-X.509 mit

Spezifische Ausprägungen des Registrierungsdienstes im Kontext TSP-X.509 für Komponentenzertifikate:

- Berechtigungsprüfende Stelle ist die gematik.
- Schlüsselerzeugung erfolgt beim Antragsteller, die Zertifikatsbeantragung erfolgt über eine technische Schnittstelle.
- Zertifikatsausgabe erfolgt über eine technische Schnittstelle.

Im Kontext der weiteren Angebote des TSP-X.509 sowie der direkt von den LEOs zugelassenen und den Kostenträger beauftragten TSP-X.509 (Zertifikate für Organisationen, Leistungserbringer und Versicherte) ergeben sich Abweichungen zu den eben beschriebenen Ausprägungen, die im Folgenden beschrieben sind:

Spezifische Ausprägungen des Registrierungsdienstes im Kontext Leistungserbringer- und Organisationszertifikate:

- Berechtigungsprüfende Stelle ist die zuständige LEO bzw. KTR-Organisation.
- Schlüsselerzeugung erfolgt beim jeweiligen TSP-X.509, die Zertifikatsbeantragung erfolgt über eine technische Schnittstelle.
- Zertifikatsausgabe erfolgt nach Einbringung der Zertifikate in den HBA bzw. die SMC-B, der Antragsteller erhält die Karte inkl. der Zertifikate vom jeweiligen TSP-X.509.

Spezifische Ausprägungen des Registrierungsdienstes im Kontext TSP-X.509 der Kostenträger (Versichertenzertifikate):

- Antragsberechtigter ist nicht der Versicherte selbst, sondern der für ihn zuständige Kostenträger.
- Berechtigungsprüfende Stelle ist der Kostenträger selbst.

- Schlüsselerzeugung erfolgt beim jeweiligen TSP-X.509 oder alternativ beim Antragsteller, die Zertifikatsbeantragung erfolgt über eine technische Schnittstelle.  
Für die AUT\_ALT-Identität erfolgt die Schlüsselerzeugung beim Signaturdienst (s. gemKPT\_Arch\_TIP#5.4.17).
- Zertifikatsausgabe erfolgt nach Einbringung der Zertifikate in die eGK, der Versicherte erhält die eGK inkl. der Zertifikate.  
Für die alternativen Versichertenidentitäten erfolgt die Zertifikatsausgabe an den Signaturdienst (AUT\_ALT-Identität)

**TIP1-A\_2193 - Implementierung der Schnittstellen des Registrierungsdienstes**

Der TSP-X.509 MUSS in der Umsetzung des Registrierungsdienstes der PKI die geforderten technischen und organisatorischen Schnittstellen implementieren.  
[<=]

**7.3.2 Erstellungsdienst**

Der Erstellungsdienst dient der Erstellung der Endnutzerzertifikate.

Zu berücksichtigende Eckpunkte sind:

- Der TSP-X.509 ist bei der Erstellung der jeweiligen Zertifikate zur Umsetzung der von der TI-Plattform definierten Zertifikatsprofile verpflichtet.
- Um die Nachprüfbarkeit der erzeugten Zertifikate zu ermöglichen, müssen diese einem Statusprüfdienst zur Prüfbarkeit per OCSP zugeführt werden.

Basierend auf diesen Eckpunkten ergeben sich folgende Rollen:

**Tabelle 13: Übersicht der Rollen und deren Aufgaben beim Erstellungsdienst**

Rolle	Aufgabe/Funktion
TSP-X.509	nimmt Zertifikatsrequests entgegen, erzeugt die Zertifikate und liefert Zertifikate nach Erstellung an den Registrierungsdienst zurück

**TIP1-A\_2194 - Implementierung der Schnittstellen des Erstellungsdienstes**

Der TSP-X.509 MUSS in der Umsetzung des Erstellungsdienstes der PKI die geforderten technischen und organisatorischen Schnittstellen implementieren.  
[<=]

**7.3.3 Statusprüfdienst**

Der Statusprüfdienst stellt Zertifikatsstatusinformationen für eine automatisierte Gültigkeitsüberprüfung zur Verfügung.

Zu berücksichtigende Eckpunkte sind:

- Im Rahmen der Nutzung von Zertifikaten besteht die Notwendigkeit zur Zertifikatsprüfung inkl. Prüfung des Sperrstatus.
- Der TSP-X.509, der ein Zertifikat erzeugt hat, muss eine Statusauskunft dazu bereitstellen.

- Der TSP-X.509, der ein Zertifikat erzeugt hat, dessen Status zusätzlich auch im Internet prüfbar sein muss, muss die zugehörigen Statusinformationen zeitgleich in der TI und im Internet zur Verfügung stellen.

Basierend auf diesen Eckpunkten ergeben sich folgende Rollen:

**Tabelle 14: Übersicht der Rollen und deren Aufgaben beim Statusprüfdienst**

Rolle	Aufgabe/Funktion
TSP-X.509	nimmt Statusanfragen entgegen und liefert die Statusinformation zu dem angefragten Zertifikat
Zertifikatsnutzer	stellt über ein technisches System eine Statusanfrage (OCSP-Request) an den für das angefragte Zertifikat relevanten OCSP-Responder

#### **TIP1-A\_2195 - Implementierung der Schnittstellen des Statusprüfdienstes**

Der TSP-X.509 MUSS in der Umsetzung des Statusprüfdienstes der PKI die geforderten technischen und organisatorischen Schnittstellen implementieren.

[<=]

### **7.3.4 Sperrdienst**

Der Sperrdienst nimmt Sperraufträge von berechtigten Personen entgegen und leitet die Änderung des Zertifikatsstatus an den Statusprüfdienst weiter. Daraufhin ergibt die Abfrage der Zertifikatsgültigkeit ein negatives Ergebnis.

Zu berücksichtigende Eckpunkte sind:

- Im Rahmen der Nutzung von Zertifikaten besteht die Notwendigkeit zu deren Sperrung, bspw. Nach Verlust der zugehörigen Karte oder des Gerätes.
- Der TSP-X.509, der ein Zertifikat erzeugt hat, muss eine Sperrmöglichkeit bereitstellen.
- Der TSP-X.509 muss das zu sperrende Zertifikat eindeutig identifizieren.
- Der Nachweis der Sperrberechtigung muss erbracht werden, dazu muss der TSP-X.509 den Anfragenden sicher authentifizieren.
- Der Sperrberechtigte muss nach erfolgreicher Sperrung eine Rückinformation erhalten.

Basierend auf diesen Eckpunkten ergeben sich folgende Rollen:

**Tabelle 15: Übersicht der Rollen und deren Aufgaben beim Sperrdienst**

Rolle	Aufgabe/Funktion
TSP-X.509	nimmt Sperranfragen entgegen, prüft diese auf Authentizität und Autorisierung und sperrt ggf. das angefragte Zertifikat
Sperrberechtigter	stellt über eine technische oder organisatorische Schnittstelle einen Sperrauftrag an den TSP-X.509

2924 **TIP1-A\_2196 - Implementierung der Schnittstellen des Sperrdienstes**  
2925 Der TSP-X.509 MUSS in der Umsetzung des Sperrdienstes der PKI die geforderten  
2926 technischen und organisatorischen Schnittstellen implementieren.  
2927 [ $\leq$ ]

## 2928 **7.4 Verzeichnisdienst der TI**

2929 Der Verzeichnisdienst im Sinne dieses Kapitels ist das TI-eigene Verzeichnis („das  
2930 Telefonbuch“) für Einträge von Leistungserbringern und Institutionen.

2931 NICHT Gegenstand dieses Kapitels sind die Verzeichnisdienste zur  
2932 Zertifikatsstatusprüfung (mittels OCSP) sowie die ggf. im Internet bereitgestellten  
2933 Verzeichnisdienste (X.500/LDAP/OCSP) der TSPs. Hierzu siehe Kap. 4.4.

### 2934 **7.4.1 Geltungsbereich**

2935 Verzeichniseinträge müssen einer bereits bestehenden elektronischen Identität  
2936 zuordenbar sein. Dabei handelt es sich um:

- 2937 • Natürliche Personen, denen aufgrund ihrer bestätigten Berufszugehörigkeit als  
2938 Leistungserbringer des deutschen Gesundheitswesens ein HBA/BA (oder HBA-  
2939 Vorläuferkarte) ausgestellt wurde.
- 2940 • Juristische Personen (Organisationen/Institutionen) des deutschen  
2941 Gesundheitswesens denen eine SMC-B ausgestellt wurde.

2942 Die Teilnahme am Verzeichnisdienst ist freiwillig.

#### 2943 **TIP1-A\_5455 - Teilnehmer des Verzeichnisdienstes**

2944 Die TI-Plattform MUSS einen Verzeichnisdienst für Einträge von Leistungserbringern und  
2945 medizinischen Institutionen realisieren.

2946 [ $\leq$ ]

#### 2947 **TIP1-A\_5456 - Freiwillige Teilnahme am Verzeichnisdienst**

2948 Die gematik MUSS sicherstellen, dass die Teilnahme am Verzeichnisdienst auf freiwilliger  
2949 Basis erfolgt.

2950 [ $\leq$ ]

### 2951 **7.4.2 Datenmodell**

#### 2952 **TIP1-A\_5457 - Datenmodell Verzeichnisdienst**

2953 Die TI-Plattform MUSS für den Verzeichnisdienst ein Datenmodell mit folgenden logischen  
2954 Elementen eines Eintrags definieren:

- 2955 1) Basisdaten (zertifikatsbasiert)
- 2956 2) Fachanwendungsdaten (optional)

2957 [ $\leq$ ]

#### 2958 **7.4.2.1 Basisdaten (zertifikatsbasiert)**

2959 Die bei der Registrierung des Teilnehmers aus dem Zertifikat übernommenen Basisdaten  
2960 enthalten u.a. die Telematik-ID als eindeutigen Identifikator des Teilnehmers im  
2961 Verzeichnisdienst. Dieser wird aus Datenschutzgründen nicht als öffentliches Attribut  
2962 genutzt.

2963 Ein weiterer wesentlicher Bestandteil eines Basisdatensatzes ist das (oder sind die)  
2964 Verschlüsselungszertifikat(e) eines Teilnehmers. Für eine sichere Ende-zu-Ende-  
2965 Kommunikation zwischen den Teilnehmern ist es unabdingbar, dass der Sender einer  
2966 Nachricht Zugriff auf das Verschlüsselungszertifikat des Empfängers hat. Der  
2967 Verzeichnisdienst dient dazu, diesen Zugriff zu gewährleisten.

2968 (Hinweis: Ein Teilnehmer kann im Besitz mehrerer gültiger Verschlüsselungszertifikate  
2969 sein. Z.B. entsteht bei der Neuausstellung einer Karte eine Überlappung zwischen der  
2970 Gültigkeitsdauer der Zertifikate der alten und der neuen Karte. Der Verzeichnisdienst gibt  
2971 dem Akteur die Möglichkeit, alle gültigen Verschlüsselungszertifikate zu veröffentlichen.)

2972 Die Basisdaten sind zwingender Bestandteil eines Eintrages. Werden die  
2973 unveränderlichen Basisdaten gelöscht, zieht dies auch die Löschung der zugehörigen  
2974 Fachanwendungsdaten nach sich. (Vgl. folgende Kapitel.)

#### 2975 **7.4.2.2 Fachanwendungsdaten (optional)**

2976 Der Verzeichnisdienst dient auch den Fachdiensten als Medium, um identitätsspezifische,  
2977 also auf einen eingetragenen Teilnehmer bezogene Daten der Fachanwendung direkt im  
2978 Verzeichnisdienst ablegen und bedarfsweise publizieren zu können.

2979 Anlage und Pflege dieser fachanwendungsspezifischen Ergänzungsdaten erfolgen über  
2980 den Fachdienst. Dafür werden Schreib- und Löschrecht für diese Ergänzungen im  
2981 Verzeichniseintrag vom Teilnehmer an den Fachdienst, bzw. an einen Fachdienst-anbieter  
2982 erteilt. Dieser Anbieter trägt somit die Verantwortung für die Richtigkeit der von ihm  
2983 gepflegten Daten. Die Rechte sind eingeschränkt auf diejenigen Daten, die über den  
2984 Fachdienst selbst verwaltet werden.

#### 2985 **7.4.3 Lifecyclemanagement für Verzeichniseinträge**

##### 2986 **TIP1-A\_5458 - Kartenbasierte Registrierung**

2987 Der Verzeichnisdienst MUSS eine Teilnehmer- und eine Zertifikats-Eintragung,  
2988 Aktualisierung und Austragung ermöglichen, welche neben den Karten eines HBA oder  
2989 einer SMC-B keine weiteren Identifikations- und Registrierungsprozesse fordert.

2990 [ $\leq$ ]

2991 Die gegenseitige Authentisierung zwischen Fachdienst und Verzeichnisdienst erfolgt  
2992 zertifikatsbasiert über TLS. Die Zertifikate werden dabei von der zentralen Dienste- und  
2993 Komponenten-CA ausgestellt.

#### 2994 **7.4.4 Aufbau und Außensicht**

2995 Die in Kapitel 7.4.2 angesprochene Partitionierung der Daten zieht auch unterschiedliche  
2996 Zuständigkeiten bzw. Hoheiten über diese Daten nach sich. Diese müssen auch auf  
2997 Ebene Autorisierung berücksichtigt werden.

2998 Die Datenbestände aus verschiedenen Quellen müssen aber unter einer für den Benutzer  
2999 einheitlichen logischen Sicht genutzt und verwaltet werden können.

##### 3000 **7.4.4.1 Autorisierung**

3001 Die technischen Zuständigkeiten für Datenbestände, die einer bestimmten Identität  
3002 zugeordnet sind, können bei verschiedenen Akteuren und Anbietern liegen:

3003 Die Basisdaten des Teilnehmers werden aus dessen Zertifikaten übernommen und  
3004 können durch den Teilnehmer selbst nicht modifiziert werden. Er kann nur über die



Publizierung des Datensatzes als Ganzes oder in Teilen (Name, Vorname optional) entscheiden. Fachanwendungsspezifische Ergänzungsdaten werden durch den jeweiligen FA-Anbieter verwaltet.

#### **TIP1-A\_5459 - Autorisierung**

Der Verzeichnisdienst MUSS seine Administrationsschnittstellen so zur Verfügung stellen, dass zu einem Verzeichniseintrag Datenstrukturen verschiedener Art und von verschiedenen Verantwortlichen gepflegt werden können:

- 1) Zertifikatsdaten dürfen nur durch die Übernahme aus Zertifikaten erstellt werden.
- 2) Fachanwendungsdaten dürfen nur vom jeweiligen FA-Anbieter gepflegt werden.

[<=]

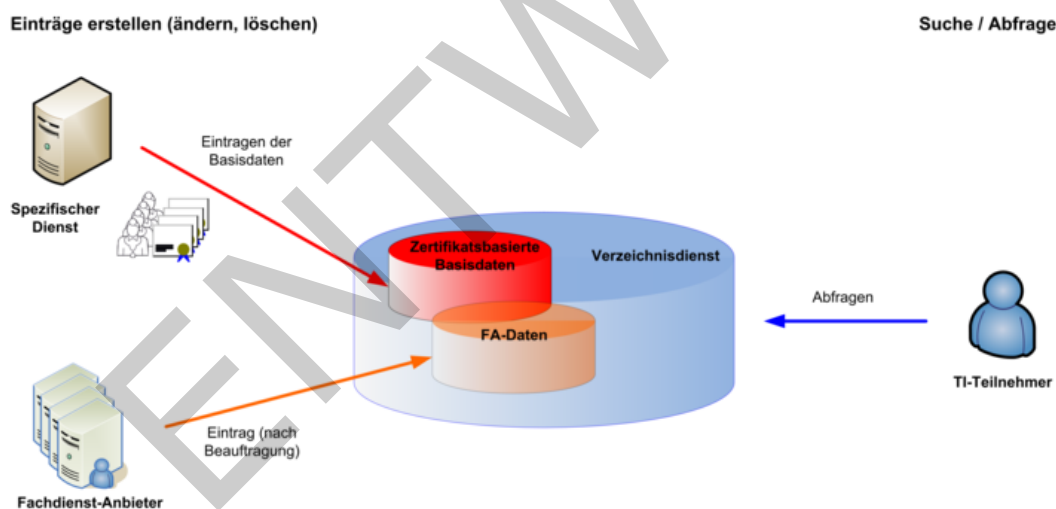
#### **7.4.4.2 Sichtbarkeit in der TI**

Der Verzeichnisdienst ist ein zentraler Dienst in der TI. Er erlaubt die Abfrage der Daten eines eingetragenen Teilnehmers unter einer einheitlichen Schnittstelle. Die architektonische Partitionierung, welche sich aus den verschiedenen Datentypen und Zuständigkeiten ergibt, bleibt einem abfragenden Client gegenüber verborgen.

#### **TIP1-A\_5460 - Eine logische Sicht auf das Verzeichnis**

Der Verzeichnisdienst MUSS für Fachdienste und dezentrale Systeme eine logische Sicht auf das Verzeichnis für Identitäten von Leistungserbringern und Institutionen bereitstellen.

[<=]



**Abbildung 8: Außenschnittstellen des Verzeichnisdienstes**

3029

## 8 Anhang A – Verzeichnisse

3030

### 8.1 Abkürzungen

Kürzel	Erläuterung
AES	Advanced Encryption Standard
AK	Anwendungskonnektor
AN	alphanumerisch
AUT	Authentisierung (Authentication)
AUT_ALT	Authentisierung mit alternativer Identität
AUTN	Technisches Authentisierungszertifikat für Nachrichten
AVS	Apothekenverwaltungssystem (Primärsystem der Apotheker)
BAEK	Bundesärztekammer
BAK	Bundesapothekerkammer
BMG	Bundesministerium für Gesundheit
BnetzA	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

CH	Card Holder
CHA	Certificate Holder Authorisation
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
DES	Data Encryption Standard
DIMDI	Deutsches Institut für Medizinische Dokumentation und Information
DN	Distinguished Name
DNS	Domain Name Service
ECC	Elliptic Curve Cryptography (Kryptographie auf Basis elliptischer Kurven)
EE	End Entity
eGBR	Elektronisches Gesundheitsberuferegister
eGK	Elektronische Gesundheitskarte
ENC	Verschlüsselung (Encryption)
ENCV	Technisches Verschlüsselungszertifikat für Verordnungen
ETSI	Europäisches Institut für Telekommunikationsnormen
EU-LOTL	List of Trusted Lists der Europäischen Kommission

FIPS-140 2	Federal Information Processing Standard 140 2
FQDN	Fully Qualified Domain Name
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
KOM-LE	Kommunikation für Leistungserbringer
KSR	Konfigurationsdienst
KT	Kartenterminal
KTR	Kostenträger
KV	Kassenärztliche Vereinigung
KVNR	Krankenversichertennummer
KZBV	Kassenzahnärztliche Bundesvereinigung
LAK	Landesapothekerkammer

LÄK	Landesärztekammer
LDAP	Lightweight Directory Access Protocol
LEI	Leistungserbringerinstitution
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
ORG	Gesellschafterorganisation
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
QES	Qualifizierte elektronische Signatur
RA	Registration Authority
RCA	Root-CA
RFC	Request For Comment
RSA	Rivest Shamir Adleman (Verfahren)
SAK	Signaturanwendungskomponente

SGB	Sozialgesetzbuch
SHA	Secure Hash Algorithm
SIG	Elektronische Signatur
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen
SigV	Signaturverordnung
SIS	Secure Internet Service
SLA	Service Level Agreement
SM	Security Module
SMC-B	Sicherheitsmodul vom Typ B
SMC	Security Module Card
gSMC-K	Security Module Card Konnektor als <holder>
gSMC-KT	Security Module Kartenterminal als <holder>
SubjectDN	Subject Distinguished Name
TCL	Trusted Component List
TI	Telematikinfrastruktur
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

## 3031 8.2 Glossar

3032 Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung  
3033 gestellt.

## 3034 8.3 Abbildungsverzeichnis

3035	Abbildung 1: TSL-Modell .....	17
3036	Abbildung 2: Zertifikathierarchien und deren Abbildung in der TSL .....	18
3037	Abbildung 3: Aufbau der TSL .....	18
3038	Abbildung 4: Gültigkeitszeiträume TSL .....	20
3039	Abbildung 5: Hierarchie der CVC-PKI (je Kartengeneration) .....	28
3040	Abbildung 6: Zuordnung der Verantwortlichkeiten für die Zertifikate .....	32
3041	Abbildung 7: OCSP-Responder Proxy .....	66
3042	Abbildung 8: Außenschnittstellen des Verzeichnisdienstes .....	93
3043	Abbildung 1: TSL-Modell .....	17
3044	Abbildung 2: Zertifikathierarchien und deren Abbildung in der TSL .....	18
3045	Abbildung 3: Aufbau der TSL .....	18
3046	Abbildung 4: Gültigkeitszeiträume TSL .....	20
3047	Abbildung 5: Hierarchie der CVC-PKI (je Kartengeneration) .....	28
3048	Abbildung 6: Zuordnung der Verantwortlichkeiten für die Zertifikate .....	32
3049	Abbildung 7: OCSP-Responder Proxy .....	66
3050	Abbildung 8: Außenschnittstellen des Verzeichnisdienstes .....	93
3051		

## 3052 8.4 Tabellenverzeichnis

3053	Tabelle 1: Tab_PKI_107 Übersicht der PKI-spezifischen Sperrgründe .....	35
3054	Tabelle 2: Verantwortlichkeiten in Bezug auf ein Zertifikat .....	45
3055	Tabelle 3: Übersicht Identitätselemente und Verantwortungsdomänen .....	49
3056	Tabelle 4: Tab_PKI_108 Informationen für ein CV-Zertifikat G2 .....	69
3057	Tabelle 5: Übersicht Felder eines CV-Zertifikats .....	69
3058	Tabelle 6: Tab_PKI_104 Ablaufschritte der Vertrauensraumprüfung .....	73
3059	Tabelle 7: Tab_PKI_105 Ablaufschritte der Zertifikatsprüfung .....	75
3060	Tabelle 8: TAB_PKI_113 Zuordnung der (zugelassenen) X.509-Sub-CAs zu	
3061	Zertifikatstypen .....	77
3062	Tabelle 9: Tab_PKI_106 Ablaufschritte der QES-Zertifikatsprüfung .....	81
3063	Tabelle 10: Übersicht der Rollen und deren Aufgaben bei der TSP-Zulassung .....	86



Tabelle 11: Übersicht der Rollen und deren Aufgaben bei der Zulassung von CVC-CAs..	87
Tabelle 12: Übersicht der Rollen und deren Aufgaben beim Registrierungsdienst .....	88
Tabelle 13: Übersicht der Rollen und deren Aufgaben beim Erstellungsdienst .....	89
Tabelle 14: Übersicht der Rollen und deren Aufgaben beim Statusprüfdienst.....	90
Tabelle 15: Übersicht der Rollen und deren Aufgaben beim Sperrdienst.....	90
Tabelle 1: Tab_PKI_107 Übersicht der PKI-spezifischen Sperrgründe .....	35
Tabelle 2: Verantwortlichkeiten in Bezug auf ein Zertifikat.....	45
Tabelle 3: Übersicht Identitätselemente und Verantwortungsdomänen .....	49
Tabelle 4: Tab_PKI_108 Informationen für ein CV-Zertifikat G2 .....	69
Tabelle 5: Übersicht Felder eines CV-Zertifikats .....	69
Tabelle 6: Tab_PKI_104 Ablaufschritte der Vertrauensraumprüfung .....	73
Tabelle 7: Tab_PKI_105 Ablaufschritte der Zertifikatsprüfung .....	75
Tabelle 8: TAB_PKI_113 Zuordnung der (zugelassenen) X.509-Sub-CAs zu Zertifikatstypen .....	77
Tabelle 9: Tab_PKI_106 Ablaufschritte der QES-Zertifikatsprüfung .....	81
Tabelle 10: Übersicht der Rollen und deren Aufgaben bei der TSP-Zulassung .....	86
Tabelle 11: Übersicht der Rollen und deren Aufgaben bei der Zulassung von CVC-CAs..	87
Tabelle 12: Übersicht der Rollen und deren Aufgaben beim Registrierungsdienst .....	88
Tabelle 13: Übersicht der Rollen und deren Aufgaben beim Erstellungsdienst .....	89
Tabelle 14: Übersicht der Rollen und deren Aufgaben beim Statusprüfdienst.....	90
Tabelle 15: Übersicht der Rollen und deren Aufgaben beim Sperrdienst.....	90

## 8.5 Referenzierte Dokumente

### 8.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemSpec_PK_eGK]	Spezifikation für Prüfkarten eGK der Generation 2.1

[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_Arch_TIP]	gematik: Architektur der TI-Plattform
[gemRL_Betr_TI]	gematik: Übergreifende Richtlinien zum Betrieb der TI
[gemRL_TSL_SP_CP]	gematik: Certificate Policy – Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation, Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_DS_Anbieter]	gematik: Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter

## 3097 8.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[Ärzte-ZV]	Zulassungsverordnung für Vertragsärzte (Ärzte-ZV) Zulassungsverordnung für Vertragsärzte auf der Grundlage des Artikel 9 des Gesetzes zur Verbesserung der Versorgungsstrukturen in der gesetzlichen Krankenversicherung (GKV-Versorgungsstrukturgesetz – GKV-VStG) vom 28.12.2011 (BGBl. I S. 3016)
[Common-PKI]	T7 & TeleTrust (20.01.2009): Common PKI Spezifikation, Version 2.0; Aktuelle Quelle <a href="http://www.t7ev.org/themen/entwickler/common-pki-v20-spezifikation.html">http://www.t7ev.org/themen/entwickler/common-pki-v20-spezifikation.html</a>
[CP-HPC]	Bundesapothekerkammer, Bundesärztekammer et al (08.06.2009, Bundespsychotherapeutenkammer, Bundeszahnärztekammer (24.09.2018): Gemeinsame Policy für die Ausgabe der HPC Heilberufsausweise – Zertifikatsrichtlinie HPC Heilberufsausweis (Version 12.0.0) <a href="http://www.bundesaerztekammer.de/downloads/CP_HPC_v1.0.0_19062009.pdf">http://www.bundesaerztekammer.de/downloads/CP_HPC_v1.0.0_19062009.pdf</a> <a href="https://www.abda.de/fileadmin/user_upload/assets/Telematik/CP_HPC_v2.0.0.pdf">https://www.abda.de/fileadmin/user_upload/assets/Telematik/CP_HPC_v2.0.0.pdf</a>
[baekV alidity Model]	Bundesärztekammer (29.05.2009) Gültigkeitsmodell der elektronischen Arztausweise und Laufzeit der Zertifikate (Version 2.3.1)
[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

[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 <del>V2.1.1</del> 'Electronic Signatures and Infrastructures (ESI); Trusted Lists', Version 2.1.1
[EU_L OTL]	<a href="https://ec.europa.eu/information_society/policy/esignature/trusted-list/">https://ec.europa.eu/information_society/policy/esignature/trusted-list/</a>
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, <a href="http://www.ietf.org/rfc/rfc2119.txt">http://www.ietf.org/rfc/rfc2119.txt</a>
[RFC2560]	<del>RFC 2560 (Juni 1999): X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP</del> <a href="http://www.ietf.org/rfc/rfc2560.txt">http://www.ietf.org/rfc/rfc2560.txt</a>
[RFC5280]	RFC 5280 (Mai 2008): Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile <a href="http://www.ietf.org/rfc/rfc3280.txt">http://www.ietf.org/rfc/rfc3280.txt</a>
[RFC6960]	RFC 6960 (Juni 2013): X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP <a href="https://tools.ietf.org/html/rfc6960">https://tools.ietf.org/html/rfc6960</a>
[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
[BSI-TR-03110 Part3Part 3]	BSI (2012): Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3 – Common Specifications, Version 2.10 <a href="https://www.bsi.bund.de/ContentBSI/EN/Publications/Techguidelines/TR03110/BSITR03110.html">https://www.bsi.bund.de/ContentBSI/EN/Publications/Techguidelines/TR03110/BSITR03110.html</a>
[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 <a href="https://www.gesetze-im-internet.de/vdg/BJNR274510017.html">https://www.gesetze-im-internet.de/vdg/BJNR274510017.html</a>