Elektronische Gesundheitskarte und Telematikinfrastruktur

Übergreifende Spezifikation
Spezifikation PKI

Version:	2.9.0
Revision:	241931
Stand:	30.06.2020
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_PKI

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Datum	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
2.0.0	05.10.17		freigegeben	gematik
			Einarbeitung der abgestimmten Änderungen, Einarbeitung der Errata 1.6.4-1, 1.6.4-2 und 1.6.4-3	gematik
2.1.0	18.12.17		Einarbeitung der Änderungen zu OPB1 R1.6.4-0, der abgestimmten Änderungen, Einarbeitung der Errata und die Entfernung von LE-AdV	gematik
2.2.0	14.05.18		Einarbeitung der Änderungen gemäß der Änderungsliste P15.2. und P15.4	gematik
2.3.0	26.10.18		Einarbeitung der Änderungen gemäß der Änderungsliste P15.9	
2.3.1			Einarbeitung P15.11	
2.4.0	18.12.18		Einarbeitung P17.1/ePA	
	21.12.18		redaktionelle Anpassung "Tab_PKI_109 Werte für das Präfix <TSP-ID>"	gematik
	09.01.19		Redaktionelle Korrektur der Anpassung P17.1/ePA in Kap. 5.9.3.3 und 5.9.3.4	gematik
2.5.0	15.05.19		Einarbeitung P18.1	gematik
2.6.0	28.06.19		Einarbeitung P19.1	gematik
2.7.0	02.10.19		Einarbeitung P20.1 und P16.1/2	gematik
2.8.0	02.03.20		Einarbeitung P21.1	gematik

2.8.1	26.05.20		Einarbeitung P21.3	gematik
2.9.0	30.06.20		Anpassungen gemäß Änderungsliste P22.1 und Scope-Themen aus Systemdesign R4.0.0	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes 11
1.1 Zielsetzung 11
1.2 Zielgruppe 11
1.3 Geltungsbereich 11
1.4 Abgrenzungen 11
1.5 Methodik 12
1.5.1 Hinweis auf offene Punkte 12
2 Notation kryptographischer Objekte 13
2.1 Basis-Bezeichner 13
2.2 Optionale Bezeichnung der technischen Ausprägung 13
2.3 Optionales Unterscheidungsmerkmal bei gleicher technischer Ausprägung 13
2.4 Allgemeine Notationsvorschrift 14
2.5 Type (Objekttyp) 14
2.6 Holder (Objektbesitzer) 15
2.7 Usage (Objektverwendung) 17
2.8 n (lfd. Nummer) 18
2.9 Instance (Ausprägung) 19
2.10 Beispiele zur Umsetzung 20
2.10.1 Beispiele für asymmetrische Objekte 20
2.10.2 Beispiele für symmetrische Objekte 21
3 CA-Strukturen 22
3.1 Übergreifende Festlegung für CA der TI 22
3.1.1 Übersicht der Identitäten/Zertifikate 22
3.1.2 Laufzeiten der CA 22
3.1.3 Unterstützung verschiedener Schlüsselgenerationen 22
3.2 TI-Betriebsumgebungen 23
3.2.1 PKI-Sicht auf die Produktivumgebung 24
3.2.2 PKI-Sicht auf Test- u. Referenzumgebung (PKI-TeRe) 24
3.2.3 Pseudo-QES PKI in Test- u. Referenzumgebung 25
3.3 Zentrale Aussteller-CAs in der TI für nonQES-Zertifikate 25
3.4 Spezifische Aussteller-CA in der TI 26
4 Kodierung von X.509-Identitäten 28
4.1 Namensregeln und -formate 28
4.1.1 Verarbeitung von Sonderzeichen 28
4.1.2 Definition der Subject-DNs für Personen und Komponenten 28

4.1.3 SubjectDN von CA-Zertifikaten und von OCSP-Responder-Zertifikaten 28
4.2 Schlüssel der Versichertenidentität (eGK) 29
4.3 Pseudonym der Versichertenidentität (eGK) 29
4.3.1 Versicherten-Pseudonym in X.509-Zertifikaten der eGK 29
4.3.2 Eindeutigkeit des Pseudonym 30
4.3.3 Pseudonym-Erstellungsregel 30
4.3.4 Hs-ZW – Herausgeberspezifischer Zufallswert (hs-ZW) 31
4.3.5 Kodierung des Pseudonyms 32
4.4 Berufsgruppen-ID der Leistungserbringer 33
4.4.1 Berufsgruppe des Heilberuflers 33
4.5 ID der Organisation/Einrichtung des Gesundheitswesens 34
4.5.1 Typ und Exemplar der Organisation/Einrichtung des Gesundheitswesens 34
4.6 Technische Rolle von Komponenten und Diensten 34
4.6.1 Technische Rolle im Komponentenzertifikat 34
4.7 Telematik-ID 35
4.7.1 Abbildung der Telematik-ID im X.509-Zertifikat 35
4.7.2 Aufbau der Telematik-ID 36
4.7.2.1 Sektoraler Präfix 36
4.7.2.2 Separator 37
4.7.2.3 Fortsatz der Telematik-ID 37
4.8 Kodierung der Zertifikate 38
4.8.1 Kodierung der Attribute 38
4.8.2 Stringlänge der Attribute 39
4.8.3 Struktur 39
4.8.3.1 serialNumber 39
4.8.3.2 Admission 40
4.8.3.3 CertificatePolicies 42
4.8.3.4 CRLDistributionPoints 44
4.8.3.5 SubjectAltNames 44
4.9 Erläuterungen zu Zertifikatsprofilen 45
4.9.1 Allgemeine Erläuterungen 46
4.9.2 Berufs-/Rollenattribute und Sperrbarkeit 46
4.9.3 Benennung der Zertifikatsprofile 46
4.9.4 Distinguished Name 47
4.10 Kodierung der Betriebsumgebungen in Zertifikaten 48
4.11 Kartenverlust und Deaktivierung von Chipkarten 50
5 X.509-Zertifikate 51
5.1 eGK – Versichertenkarte 51
5.1.1 Definition der Versichertenidentität 51
5.1.2 Belegung der Felder im SubjectDN 52
5.1.3 X.509-Zertifikatsprofile der eGK 53
5.1.3.1 C.CH.AUT und C.CH.AUT_ALT – Authentisierung eGK 53
5.1.3.2 C.CH.ENC – Verschlüsselung eGK 55
5.1.3.3 C.CH.QES – Qualifizierte Signatur eGK (optional) 57
5.1.3.4 C.CH.AUTN - Technische Authentisierung eGK 58
5.1.3.5 C.CH.ENCV - Technische Verschlüsselung eGK 60

5.2 HBA – Heilberufsausweis 61
5.2.1 X.509 Zertifikatsprofile des HBA 61
5.2.1.1 C.HP.AUT – Authentisierung HBA 61
5.2.1.2 C.HP.ENC – Verschlüsselung HBA 63
5.2.1.3 C.HP.QES – Qualifizierte Signatur HBA 65

5.3 SMC-B – Ausweis einer Organisation/Einrichtung des Gesundheitswesens 69
5.3.1 Definition der Organisationsidentität 69
5.3.2 Aufbau Anschriftzone nach [DIN5008] 70
5.3.3 Umgang mit überlangen Attributen im SubjectDN 71
5.3.4 X.509 Zertifikatsprofile der SMC-B 71
5.3.4.1 C.HCI.AUT – Authentisierung SMC- B 71
5.3.4.2 C.HCI.ENC – Verschlüsselung SMC-B 73
5.3.4.3 C.HCI.OSIG – Signatur SMC-B 75

5.4 HSM-B – Ausweis einer Organisation/Einrichtung des Gesundheitswesens 76

5.5 gSMC-KT – eHealth-Kartenterminal 77
5.5.1 Definition der Kartenterminalidentität 77
5.5.2 X.509 Zertifikatsprofile der gSMC-KT 77
5.5.2.1 C.SMKT.AUT – Identität der gSMC-KT 77

5.6 gSMC-K – Konnektor 79
5.6.1 Definition und Zuweisung der Konnektoridentität 79
5.6.2 Aufbau des SubjectDN 79
5.6.3 Statusprüfung von Konnektorzertifikaten 80
5.6.4 X.509 Zertifikatsprofile des Konnektors 80
5.6.4.1 C.NK.VPN – VPN-Authentisierung Netzkonnektor 80
5.6.4.2 C.AK.AUT - Authentisierung Anwendungskonnektor 82
5.6.4.3 C.SAK.AUT - Authentisierung Signaturdienst 84

5.7 VPN-Zugangsdienst 85
5.7.1 Definition und Zuweisung der Zugangsdienstidentitäten 86
5.7.2 Aufbau des SubjectDN 86
5.7.3 X.509-Zertifikatsprofile des Zugangsdienstes 86
5.7.3.1 C.VPNK.VPN - VPN-Authentisierung Zugangsdienst TI 86
5.7.3.2 C.VPNK.VPN-SIS - VPN-Authentisierung Zugangsdienst Sicherer Internetzugang 87

5.8 ZD – Zentrale Dienste 89
5.8.1 Definition der Identität der Zentralen Dienste 89
5.8.2 Aufbau des SubjectDN 89
5.8.3 X.509 Zertifikatsprofile der Zentralen Dienste 89
5.8.3.1 C.ZD.TLS-S Server-Authentisierung (ehemals C.SF.SSL-S) 89

5.9 FD – Fachanwendungsspezifische Dienste 91
5.9.1 Definition der Identität der Fachanwendungsspezifischen Dienste 91
5.9.2 Aufbau des SubjectDN 91
5.9.3 X.509 Zertifikatsprofile der Fachanwendungsspezifischen Dienste 92
5.9.3.1 C.FD.TLS-C Client-Authentisierung (ehemals C.SF.SSL-C) 92
5.9.3.2 C.FD.TLS-S Server-Authentisierung (ehemals C.SF.SSL-S) 93
5.9.3.3 C.FD.SIG Signatur Fachdienst 95
5.9.3.4 C.FD.AUT Authentisierung Fachdienst 97
5.9.3.5 C.FD.ENC Verschlüsselung Fachdienst 98

5.10 CM – Clientmodul 100

5.10.1 Definition der Identität eines Clientmoduls 100
5.10.2 Aufbau des SubjectDN 100
5.10.3 X.509 Zertifikatsprofil des Clientmoduls 100
5.10.3.1 C.CM.TLS-CS Clientmodul-Authentisierung 100

5.11 SGD-HSM – Schlüsselgenerierungsdienst-HSM 102
5.11.1 Beschreibung der Identität 102
5.11.2 X.509 Zertifikatsprofil der SGD-HSM 102

5.12 CA - Zertifikatsprofile 104
5.12.1 GEM.RCA<n> - Zentrale Root-CA_nonQES 104
5.12.2 <tsp>.<usage>-CA<n> - Aussteller-CA_nonQES 106
5.12.3 <tsp>.HBA-qCA<n> - Aussteller-CA_QES 108

5.13 OCSP – Statusauskunftsdienst 109
5.13.1 Definition der OCSP-Signer-Identität 109
5.13.2 Aufbau des SubjectDN 110
5.13.3 X.509-Profil des OCSP-Signer-Zertifikates 110
5.13.3.1 C.GEM.OCSP OCSP-Signer-Zertifikat 110

5.14 CRL – Statusauskunftsdienst 111
5.14.1 Definition der CRL-Signer-Identität 112
5.14.2 Aufbau des SubjectDN 112
5.14.3 X.509 Profil des CRL-Signer-Zertifikates 112
5.14.3.1 C.GEM.CRL CRL-Signaturzertifikat 112

5.15 TSL - Zertifikatsprofile 114
5.15.1 Definition der TSL-Signer-Identität 114
5.15.2 Aufbau des SubjectDN 114
5.15.3 X.509 Zertifikatsprofil der TSL-Signer-CA 114
5.15.4 TSL-Signer- Zertifikat 115
5.15.5 TSL-OCSP-Responder-Zertifikat 116

6 CV-Zertifikate 118

6.1 Festlegungen zur Abgrenzung 118

6.2 Namensregeln und -formate 118

6.3 Rollen und Profile 119
6.3.1 Rollenauthentisierung 119
6.3.2 Authentisierung einer Funktionseinheit 128

6.4 CV-Zertifikatsprofile der Generation 2 129
6.4.1 Berechtigung einer CVC-CA zur Zertifikatserstellung 129
6.4.2 Aufbau und Bestandteile der CV-Zertifikate der Generation 2 130
6.4.3 Zertifikatsprofil eines CV-Zertifikates für ELC-Schlüssel 131
6.4.3.1 Certificate Profile Identifier (CPI) 131
6.4.3.2 Certification Authority Reference (CAR) 131
6.4.3.3 Öffentlicher Schlüssel 132
6.4.3.4 Certificate Holder Reference (CHR) 133
6.4.3.5 Certificate Holder Authorization Template (CHAT) 135
6.4.3.6 Certificate Effective Date (CED) 136
6.4.3.7 Certificate Expiration Date (CXD) 136
6.4.3.8 Zu signierende Nachricht M eines CV-Zertifikates der Generation 2 136
6.4.4 Struktur und Inhalt eines CV-Zertifikates für ELC-Schlüssel der Generation 2 137

6.4.5 Struktur und Inhalt eines CV-Zertifikates für ELC-Schlüssel der Generation 2 138
6.4.5.1 Struktur und Inhalt von CA CV-Zertifikaten für ELC-Schlüssel 138
6.4.5.2 Struktur und Inhalt von Cross-CV-Zertifikaten für ELC-Schlüssel 140
6.4.5.3 Struktur und Inhalt von Endnutzer-CV-Zertifikaten für ELC-Schlüssel 141
6.4.6 Flagliste mit Berechtigungen in CV-Zertifikaten für ELC-Schlüssel 143

7 Festlegung von OIDs 149

8 Prüfung von Zertifikaten 150

8.1 Vertrauensraum der TI 152
8.1.1 TSL im Kontext der ECC-Migration 154
8.1.2 Initialisierung TI-Vertrauensraum 154
8.1.2.1 TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum" 158
8.1.3 Geplanter Wechsel TI-Vertrauensanker 164
8.1.3.1 TUC_PKI_013 „Import TI-Vertrauensanker aus TSL" 164
8.1.3.2 TSL-Einträge für die Bereitstellung neuer TI-Vertrauensanker 167
8.1.3.3 Prüfung der TSL nach Wechsel des TI-Vertrauensanker 169
8.1.4 Ungeplanter Wechsel des TI-Vertrauensanker 170

8.2 TSL-Prüfung 170
8.2.1 Erreichbarkeit und Download der TSL 170
8.2.1.1 TUC_PKI_017 „Lokalisierung TSL Download-Adressen" 170
8.2.1.2 TUC_PKI_016 „Download der TSL-Datei" 172
8.2.2 Vertrauensstatus und Authentifizieren der TSL 175
8.2.2.1 TUC_PKI_019 „Prüfung der Aktualität der TSL" 175
8.2.2.2 TUC_PKI_020 „XML-Dokument validieren" 183
8.2.2.3 TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates" 184
8.2.2.4 TUC_PKI_012 „XML-Signatur-Prüfung" 187
8.2.3 TSL-Sicherheitsaspekte 188
8.2.4 TSL-Zeitparameter 189
8.2.5 ServiceTypeIdentifier "unspecified" 189

8.3 Zertifikatsprüfung X.509 nonQES 190
8.3.1 Zertifikatsprüfung in der TI 191
8.3.1.1 TUC_PKI_018 „Zertifikatsprüfung in der TI" 191
8.3.1.2 TUC_PKI_002 „Gültigkeitsprüfung des Zertifikats" 198
8.3.1.3 TUC_PKI_003 „CA-Zertifikat in TSL-Informationen finden" 200
8.3.1.4 TUC_PKI_004 „Mathematische Prüfung der Zertifikatssignatur" 203
8.3.2 Statusprüfung 206
8.3.2.1 TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln" 206
8.3.2.2 TUC_PKI_006 „OCSP-Abfrage" 208
8.3.2.3 TUC_PKI_021 „CRL-Prüfung" 215
8.3.2.4 Szenarien für Offline und Timeout von OCSP 220
8.3.2.5 Statusprüfung von eGK-Zertifikaten 220
8.3.3 Ermittlung von Autorisierungsinformationen 220
8.3.3.1 Bestätigte Zertifikatsinformationen 220
8.3.3.2 TUC_PKI_009 „Rollenermittlung" 220
8.3.3.3 TUC_PKI_007 „Prüfung Zertifikatstyp" 223
8.3.4 Weitere Prüfungen 228
8.3.4.1 Umgang mit kritischen Extensions 228

8.4 Überprüfung der Zertifikate auf Netzwerk- und Transportebene 228
8.4.1 TLS-Verbindungsaufbau 228

8.4.2 IPsec-Verbindungsaufbau 229
8.5 Zertifikatsprüfung X.509 QES 229
8.5.1 TUC_PKI_030 „QES-Zertifikatsprüfung“ 230
8.5.2 TUC_PKI_036 „BNetzA-VL Aktualisierung“ 237
8.6 Fehlercodes bei TSL- und Zertifikatsprüfung X.509 241
8.7 Zertifikatsprüfung CV-Zertifikate der 2. Generation 250
9 OCSP-Statusinformation 252
9.1 Statusprüfung 252
9.1.1 Schnittstelle I_OCSP_Status_Information 252
9.1.1.1 Schnittstellendefinition 253
9.1.1.1.1 OCSP-Request 253
9.1.1.1.2 OCSP-Response 254
9.1.1.2 Umsetzung 255
9.1.1.3 Nutzung 256
9.1.2 Artefakte 256
9.1.2.1 OCSP-Response – Response Status 256
9.1.2.2 OCSP-Response - Zeiten 257
9.1.2.3 OCSP-Response - CertStatus 258
9.1.2.4 OCSP-Response - CertID 259
9.1.2.5 OCSP-Response – Sperrzeitpunkt und Sperrgrund 259
9.1.2.6 OCSP-Response – CertHash 259
9.1.2.7 OCSP-Response – Responder-Zertifikate 260
9.1.3 Testunterstützung 260
9.1.4 Hardwaremerkmale 260
10 Anhang A – Sektorspezifische Ausprägungen der SMC-B-Zertifikate 261
10.1 KZBV 261
10.2 KBV 263
10.3 DKG 265
10.4 GKV-Spitzenverband 267
10.5 Apothekerschaft 269
10.6 AdV-Umgebung im Auftrag der Kostenträger 271
10.7 SMC-B-ORG 272
10.8 Weitere Leistungserbringerinsitutionen 275
10.9 Weitere Ärztliche Institutionen 277
11 Anhang B – Verzeichnisse 280
11.1 Abkürzungen 280
11.2 Glossar 285
11.3 Abbildungsverzeichnis 285
11.4 Tabellenverzeichnis 286

11.5 Referenzierte Dokumente 290
11.5.1 Dokumente der gematik 290
11.5.2 Weitere Dokumente 291

12 Anhang C – Sektorspezifische Ausprägungen der HBA Zertifikate 296

12.1 BÄK 296

12.2 BZÄK 298

12.3 BPtK 299

12.4 Apothekerschaft 301

12.5 Weitere Leistungserbringer 303

1 Einordnung des Dokumentes

1.1 Zielsetzung

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

1.2 Zielgruppe

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

1.3 Geltungsbereich

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

Schutzrechts-/Patentrechtshinweis

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

1.4 Abgrenzungen

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

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

1.5 Methodik

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

Sie werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=]

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

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

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

1.5.1 Hinweis auf offene Punkte

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

Beispiel für einen offenen Punkt.

2 Notation kryptographischer Objekte

2.1 Basis-Bezeichner

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

<Objekttyp>.<Objektbesitzer>.<Objektverwendung>

Im weiteren Dokument werden dafür die kürzeren englischen Begriffe verwendet:

<type>.<holder>.<usage>

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

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

2.2 Optionale Bezeichnung der technischen Ausprägung

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

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

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

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

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

2.3 Optionales Unterscheidungsmerkmal bei gleicher technischer Ausprägung

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

Beispiel:
PrK.CH.ENCn.R2048, wobei n mit 1 beginnt und fortlaufend nummeriert wird

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

2.4 Allgemeine Notationsvorschrift

Die Benennung kryptographischer Objekte erfolgt gemäß der Notationsvorschrift in Tab_PKI_201.

Tabelle 1: Tab_PKI_201 Allgemeine Notationsvorschrift für kryptographische Objekte

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

2.5 Type (Objekttyp)

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

Tabelle 2: Tab_PKI_202: Notationsvorgaben für Objekttyp

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

Wertebereich von <key>

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

Wertebereich von <certificate>

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

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

Wertebereich von <ID>

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

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

2.6 Holder (Objektbesitzer)

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

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

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

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

Tabelle 3: Tab_PKI_203 Notationsvorgaben für Objektbesitzer

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

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

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

Wertebereich von <holder X.509 | SK>

<root certification authority> ::= RCA

<health professional> ::= HP

<card holder> ::= CH (Versicherte)

<Clientmodul> ::= CM

<health care institution> ::= HCI

<security module Kartenterminal> ::= SMKT

<Anwendungskonnektor> ::= AK

<Netzkonnektor> ::= NK

<VPN Zugangsdienst> ::= VPNK

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

<Signatur Anwendungs Komponente>::= SAK

<TLS> ::= TLS

<Fachdienst VSD> ::= VSD

<Zentraler Dienst> ::= ZD

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

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

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

Wertebereich von <holder CVC>

<root certification authority> ::= RCA

<certification authority> ::= CA

<certification authority eGK> ::= CA_eGK

<certification authority HPC> ::= CA_HPC

<certification authority SMC> ::= CA_SMC

<certification authority SAK> ::= CA_SAK

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

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

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

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

<health professional card> ::= HPC

<health professional card role> ::= HPC_Role

<health professional card device> ::= HPC_Device

<electronic health card> ::= eGK (elektronische Gesundheitskarte)

<security module card> ::= SMC

<security module card role> ::= SMC_role

<security module card device> ::= SMC_device

<Signatur Anwendungs Komponente>::= SAK

<Komfort-Merkmal> ::= KM (RFID-Token)

<Kostenträger AdV> ::= KTRADV

2.7 Usage (Objektverwendung)

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

Tabelle 4: Tab_PKI_204 Notationsvorgaben für Objektverwendung

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

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

Wertebereich von <usage X.509 | SK>

<qualified electronic signature> ::= QES

<electronic signature> ::= SIG

<electronic signature of an organization>::= OSIG

<encipherment> ::= ENC

<encipherment prescription> ::= ENCV
<authentication X509> ::= AUT
<authentication X509 organisation> ::= AUTO (opt.)
<authentication message X509> ::= AUTN
<authentication X509 alternative-id> ::= AUT_ALT
<certsign X509> ::= CA
<VPN-Tunnel> ::= VPN
<VPN-Tunnel secure internet service>::= VPN-SIS
<TLS> ::= TLS
<TLS-Client> ::= TLS-C
<TLS-Server> ::= TLS-S
<TLS-Clientmodul> ::= TLS-CS
<OCSP> ::= OCSP
<calculation message auth. code> ::= MAC
<key generation> ::= KG
<CRL> ::= CRL
<certification authority component> ::= KOMP
<certification authority VPNservice> ::= VPNK
<certification authority SMC-B> ::= SMCB
<certification authority HBA> ::= HBA

Wertebereich von <usage CVC>

<certsign CVC> ::= CS
<authentication CVC> ::= AUT_CVC
<authentication role CVC> ::= AUTR_CVC
<authentication device CVC> ::= AUTD_CVC
<authentication device CVC AKS> ::= AUTD_AKS_CVC (Auslösung Komfortsignatur)
<authentication device CVC RPE> ::= AUTD_RPE_CVC (Remote-PIN-Empfänger)
<authentication device CVC RPS> ::= AUTD_RPS_CVC (Remote-PIN-Sender)
<authentication device CVC SUK> ::= AUTD_SUK_CVC (Stapel- und komfortfähige SSEE)

2.8 n (lfd. Nummer)

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

Wertebereich von <lfd. Nummer>

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

2.9 Instance (Ausprägung)

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

Tabelle 5: Tab_PKI_205-01 Notationsvorgaben für Ausprägung

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

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

Wertebereich von <instance X.509>

<X.509 RSA 2048 > ::= R2048

<X.509 RSA 3072 > ::= R3072

<X.509 ECC 256 > ::= E256

<X.509 ECC 384 > ::= E384

<X.509 ECC 512 > ::= E512

Wertebereich von <instance CVC>

<CVC ECC 256 > ::= E256

<CVC ECC 384 > ::= E384

<CVC ECC 512 > ::= E512

Wertebereich von <instance SYM>

<2KeyTripleDES> ::= 2DES

<3KeyTripleDES> ::= 3DES

<AES mit 128 Bit> ::= AES128

<AES mit 256 Bit> ::= AES256

2.10 Beispiele zur Umsetzung

2.10.1 Beispiele für asymmetrische Objekte

Tabelle 6: Tab_PKI_206-01 Beispiele für asymmetrische Objekte

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

s-dienst	des VPN-Zugangsdienstes			
Fachan w. spez. Dienst allgem.	X.509-Zertifikat/Schlüssel eines Fachanwendungs-spez. Dienstes als Server für TLS-Verbindung	C.FD.TLS-S	PrK.FD.TLS-S	PuK.FD.TLS-S.R2048
Fach-dienst VSD	X.509-Zertifikat/Schlüssel des VSD-Fachdienstes zum Signieren einer Nachricht	C.VSD.AUT	PrK.VSD.AUT	PuK.VSD.AUT R2048

2.10.2 Beispiele für symmetrische Objekte

Tabelle 7: Tab_PKI_207 Beispiele für symmetrische Objekte

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

3 CA-Strukturen

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

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

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

3.1 Übergreifende Festlegung für CA der TI

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

GS-A_4257 - Hauptsitz und Betriebsstätte
Die gematik Root-CA, ein TSP-X.509 nonQES, ein TSP-X.509 QES, ein TSP-CVC die CVC-Root und der TSL-Dienst MÜSSEN ihren Hauptsitz und die Betriebsstätten für den tatsächlichen Betrieb in einem Land der Europäischen Union haben.
[<=]

3.1.1 Übersicht der Identitäten/Zertifikate

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

3.1.2 Laufzeiten der CA

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

3.1.3 Unterstützung verschiedener Schlüsselgenerationen

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

GS-A_5511 - Unterstützung der Schlüsselgeneration RSA durch TSP-X.509 nonQES
Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN die Schlüsselgeneration RSA (gemäß [gemSpec_Krypt#GS-A_4357]) unterstützen.
[<=]

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

GS-A_5528 - Unterstützung der Schlüsselgeneration ECDSA durch TSP-X.509 nonQES
Die gematik Root-CA und ein TSP-X.509 nonQES, der Zertifikate für die Kartengeneration G2.1 erstellt oder verwendet, MÜSSEN die Schlüsselgeneration ECDSA (gemäß [gemSpec_Krypt#GS-A_4357]) unterstützen.
[<=]

GS-A_5512 - Unterstützung der Schlüsselgeneration RSA durch TSP-X.509 QES
Ein TSP-X.509 QES MUSS die Schlüsselgeneration RSA gemäß [gemSpec_Krypt#GS-A_4358] unterstützen.
[<=]

GS-A_5529 - Unterstützung der Schlüsselgeneration ECDSA durch TSP-X.509 QES
Ein TSP-X.509 QES, der Zertifikate für die Kartengeneration G2.1 erstellt oder verwendet, MUSS die Schlüsselgeneration ECDSA gemäß [gemSpec_Krypt#GS-A_4358] unterstützen.
[<=]

GS-A_5513 - Wahl des Signaturalgorithmus für Zertifikate
Die gematik Root-CA, die TSP-X.509 QES und die TSP-X.509 nonQES MÜSSEN Zertifikate mit dem Signaturalgorithmus der Schlüsselgeneration des Zertifikats signieren. Ausgenommen davon sind die Crosszertifikate der gematik Root-CA.
[<=]

3.2 TI-Betriebsumgebungen

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

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

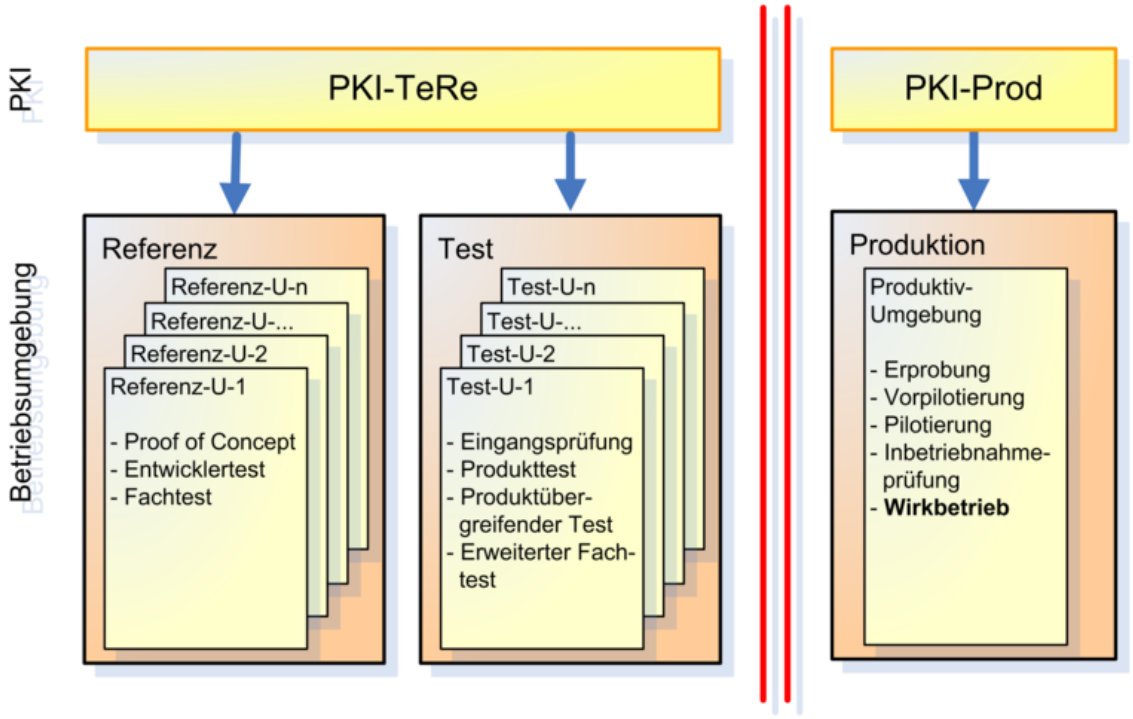


Abbildung 1: Betriebsumgebungen aus Sicht der PKI

3.2.1 PKI-Sicht auf die Produktivumgebung

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

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

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

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

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

GS-A_4695 - Zentrale Root-CA für Test- und Referenzumgebung
Der Anbieter der gematik Root-CA MUSS in der Test- und Referenzumgebung eine zentrale TeRe-Root-CA bereitstellen und hieraus TeRe-CAs der zweiten Ebene zertifizieren.
[<=]

GS-A_4696 - OCSP-Responder für gematik TeRe-Root-CA im Internet
Der Anbieter der gematik Root-CA MUSS einen OCSP-Responder für die CA-Zertifikate der TeRe-Root-CA im Internet bereitstellen.
[<=]

GS-A_4697 - PKI für Test- und Referenzumgebung
Der TSP-X.509 nonQES MUSS für jede von ihm betriebene CA der Produktivumgebung eine korrespondierende CA für die Test- und Referenzumgebung implementieren.
[<=]

Die CA-Struktur entspricht insgesamt derjenigen der Produktivumgebung.

3.2.3 Pseudo-QES PKI in Test- u. Referenzumgebung

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

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

GS-A_4698 - Pseudo-QES PKI für PKI-TeRe
Der TSP-X.509 QES SOLL für jede von ihm betriebene QES-CA der Produktivumgebung eine funktional äquivalente CA in der PKI-TeRe implementieren.
[<=]

GS-A_5483 - Aufnahme der Pseudo-QES CA in die Pseudo-BNetzA-VL
Der TSP-X.509 QES MUSS jede von ihm in der PKI-TeRe betriebene CA in die Pseudo-BNetzA-VL aufnehmen lassen.
[<=]

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

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

GS-A_4702 - Zentrale Aussteller-CA für nonQES-Zertifikate
Der TSP-X.509 nonQES, der eine zentrale Aussteller-CA in der TI für die Ausgabe von nonQES-X.509-Zertifikaten für Komponenten oder Dienste bereitstellt, MUSS (1) die Zertifikatsstruktur gemäß Tab_PKI_212 und (2) im **`commonName die <usage>`** = KOMP, sowie (3) im **`organizationalUnitName den <usageName>`** = 'Komponenten' umsetzen.
[<=]

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

GS-A_5212 - Zentrale Aussteller-CA für VPN-Zugangsdienst-Zertifikate
Der TSP-X.509 nonQES, der eine zentrale Aussteller-CA in der TI für die Ausgabe von nonQES-X.509-Zertifikaten für VPN-Zugangsdienste bereitstellt, MUSS (1) die Zertifikatsstruktur gemäß Tab_PKI_212 und (2) im **`commonName`** die <usage> = VPNK,

sowie (3) im **organizationalUnitName** den <usageName> = 'VPN-Zugangsdienst' umsetzen.
[<=]

3.4 Spezifische Aussteller-CA in der TI

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

GS-A_4703 - CA-Zertifikatsprofil für nonQES-Zertifikate
Ein TSP-X.509 nonQES und der Anbieter des TSL-Dienstes MÜSSEN für die Beantragung einer Aussteller-CA unterhalb der zentralen gematik-Root-CA die Zertifikatsstruktur gemäß Tab_PKI_212 und einem CA-Namen entsprechend der Tabelle Tab_PKI_213 umsetzen.
[<=]

GS-A_4704 - Nutzung von CA mit spezifischem Verwendungszweck
Ein TSP-X.509 nonQES, TSP-X.509 QES und der Anbieter des TSL-Dienstes DÜRFEN aus einer Aussteller-CA mit einem spezifischen Verwendungszweck NICHT weitere EE-Zertifikate für andere Zwecke ausgeben.
[<=]

GS-A_4828 - Vorgaben zur Bildung von nonQES-CA-Namen
Ein TSP-X.509 nonQES MUSS für eine Aussteller-CA unterhalb der zentralen gematik-Root-CA (1) die Zertifikatsstruktur gemäß Tab_PKI_212 umsetzen und (2) für die Bildung des subjectDN im Feld subject.commonName die Einträge aus der Spalte <usage> sowie (3) im Feld organizationalUnitName die korrespondierenden Einträge aus der Spalte <usageName> aus der Tabelle Tab_PKI_213 umsetzen.
[<=]

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

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

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

4 Kodierung von X.509-Identitäten

4.1 Namensregeln und -formate

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

4.1.1 Verarbeitung von Sonderzeichen

GS-A_4705-01 - Verarbeitung von Sonderzeichen in PKI-Komponenten
gematik-Root-CA, TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN sicherstellen, dass von ihnen eingesetzte Komponenten in der Lage sind, Sonderzeichen wie ä, ü, ö, ß etc. anhand eines Zeichensatzes gemäß Tab_PKI_229-01 in den einzelnen Namenselementen zu verarbeiten und darzustellen.
[<=]

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

Distinguished Names können daher generell mit diesen Sonderzeichen gebildet werden. Bei Kommunikationspartnern außerhalb Deutschlands kann die Verwendung von Umlauten zu Problemen führen, z. B. bei der Darstellung von Distinguished Names. Die zuständigen Instanzen für die Namensgebung müssen diese Problematik berücksichtigen.

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

4.1.2 Definition der Subject-DNs für Personen und Komponenten

- Definition der Versichertenidentität in Kap 5.1.15.11
- Definition der Organisationsidentität in Kap 5.3.1
- Definition der Identitäten von Konnektor und SMKT in Kap. 5.5.1 bzw. 5.6.1
- Definition der Identitäten der Zentralen Dienste und Fachanwendungsspezifischen Dienste in Kap. 5.8.1 und 5.9.1

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

GS-A_4706 - Vorgaben zu SubjectDN von CA- und OCSP-Zertifikaten
gematik-Root-CA, TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN bzgl. Aufbau des SubjectDN in CA-Zertifikaten und OCSP-Responder-Zertifikaten folgende Vorgaben umsetzen: (a) Der subjectDN einer CA bzw. eines OCSP-Responders muss diese eindeutig innerhalb der TI identifizieren. (b) Das Attribut commonName muss enthalten sein und den relevanten Namen der CA bzw. des OCSP-Responders enthalten. (c) Das Attribut organizationName muss enthalten sein und den Namen des TSP enthalten. (d) Das Attribut countryName muss enthalten sein und das Herkunftsland des TSP (Land der

Anschrift des TSP) enthalten. (e) Die Attribute serialNumber und organizationalUnitName können enthalten sein, sollen jedoch nur dann verwendet werden, falls sie für die Eindeutigkeit des subjectDN notwendig sind. (f) Das Attribut organizationIdentifier kann enthalten sein. (g) Darüber hinaus sollen keine weiteren Attribute enthalten sein.
[<=]

4.2 Schlüssel der Versichertenidentität (eGK)

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

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

- OU = unveränderbarer Teil der KV-Nummer
- OU = Institutionskennzeichen

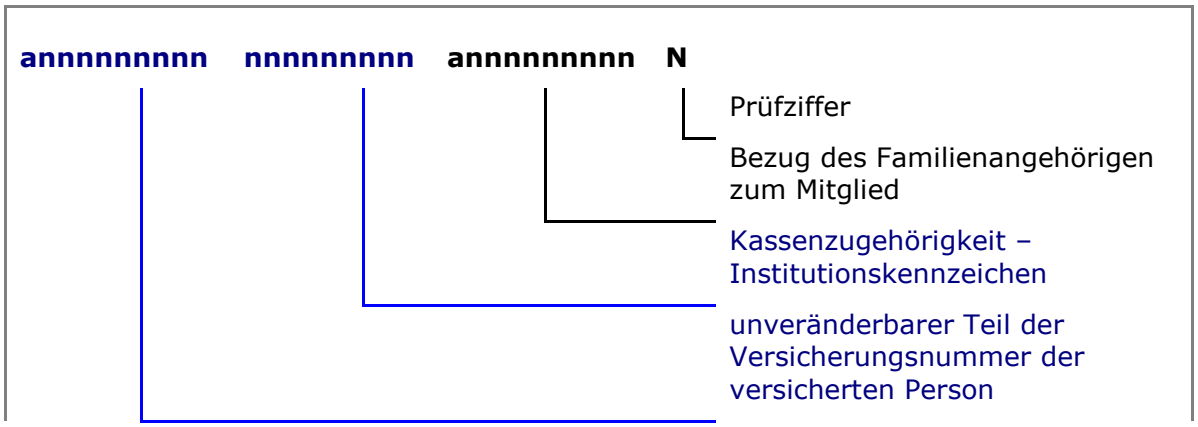


Abbildung 2: Aufbau der Krankenversichertennummer

4.3 Pseudonym der Versichertenidentität (eGK)

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

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

GS-A_4572 - Abbildung Pseudonym in X.509-Zertifikaten der eGK
Der TSP-X.509 nonQES (eGK) MUSS im Feld **`commonName`** der Zertifikatstypen C.CH.AUTN bzw. C.CH.ENCV das Pseudonym des Versicherten aufnehmen.
[<=]

4.3.2 Eindeutigkeit des Pseudonym

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

GS-A_4573 - Eindeutigkeit des Pseudonyms innerhalb Herausgeber-Domäne
Der TSP-X.509 nonQES (eGK) MUSS das im AUTN- und ENCV-Zertifikat des Versicherten gespeicherte Pseudonym innerhalb der Herausgeber-Domäne (IssuerDomain) eindeutig gestalten.
[<=]

4.3.3 Pseudonym-Erstellungsregel

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

GS-A_4574 - Pseudonym-Erstellungsregel
Der TSP-X.509 nonQES (eGK) MUSS das Pseudonym des Versicherten nach folgender Regel bilden: SHA-256 Hashwert über die Konkatenierung der Datenfelder (1) Nachname des Versicherten, (2) unveränderbarer Teil der KVNR des Versicherten und (3) einer vom Herausgeber (Kostenträger) verwendeten Zusatzinformation (herausgeberspezifischer Zufallswert).

[<=]

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

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

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

Beispiel:

Nachname =
„**Mustername1**“

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

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

Konkatenation =
„**Musternamelm331784849A32C93C6946314A9**“

SHA-256- Hashwert =
“**E3F3555165491A7FBE3F355516549E3F3555165902BFAF254518C469E584A793**”

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

commonName =
“**E3F3555165491A7FBE3F**”

GS-A_4575 - Prüfung auf Eindeutigkeit des Pseudonyms
Der TSP-X.509 nonQES (eGK) MUSS nach Erzeugung des Pseudonyms prüfen, ob dieses Pseudonym vom Kartenherausgeber bereits vergeben wurde. Ist dies der Fall, MUSS das Pseudonym mit inkrementiertem hs-ZW neu generiert und erneut auf Eindeutigkeit geprüft werden.
[<=]

GS-A_4576 - Pseudonym auf eGK-Ersatzkarten
Der TSP-X.509 nonQES (eGK) MUSS bei Ausstellung eines eGK-Ersatzausweises innerhalb der definierten Verwendungsperiode des herstellerspezifischen Zufallswertes (hs-ZW) dasselbe Pseudonym verwenden wie auf der vorgängigen Karte.
[<=]

GS-A_4577 - Pseudonym auf eGK-Folgekarten
Der TSP-X.509 nonQES (eGK) MUSS bei Ausstellung eines eGK-Ersatzausweises nach Ablauf der definierten Verwendungsperiode des hs-ZW oder bei Ausstellung einer Folgekarte nach Ablauf des Gültigkeitszeitraums der vorgängigen Karte ein neues Pseudonym auf Grundlage des geänderten hs-ZW vergeben.
[<=]

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

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

GS-A_4578 - eGK hs-ZW Bildungsregel
Der eGK-Herausgeber MUSS einen individuellen herausgeberspezifischen Zufallswert (hs-ZW) aus mindestens 16 Hexadezimal-Ziffern (64 Bit) festlegen, der jeweils kollisionsfrei zu allen vorherigen hs-ZW dieses eGK-Herausgebers ist.
[<=]

GS-A_4579 - eGK hs-ZW Verwendung/Wechsel
Der eGK-Herausgeber MUSS den aktuellen hs-ZW für alle Versichertenzertifikate für eine bestimmte Verwendungsperiode verwenden und mindestens einmal jährlich wechseln.
[<=]

GS-A_4580 - eGK hs-ZW Archivierung
Der eGK-Herausgeber MUSS alle nicht mehr verwendeten hs-ZW für Zwecke der Rekonstruktion von Pseudonymen für mindestens 10 Jahre sicher speichern und berechtigten Teilnehmern der TI verfügbar machen.
[<=]

4.3.5 Kodierung des Pseudonyms

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

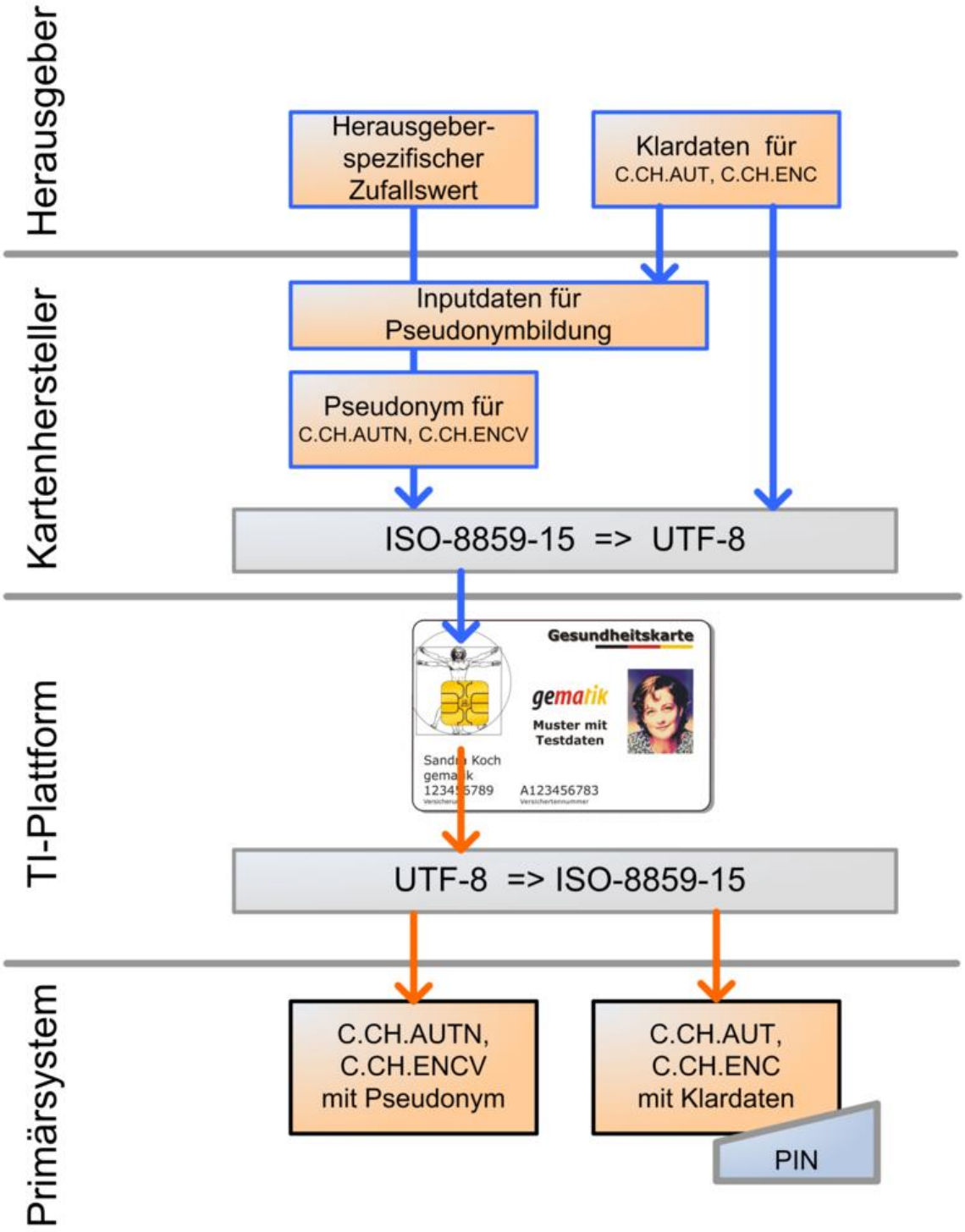


Abbildung 3: Pseudonym Kodierung in X.509-Versichertenzertifikaten

GS-A_4582 - Pseudonym-Personalisierung im X.509-SubjectDN
Der eGK-Herausgeber MUSS das Pseudonym im UTF-8-Zeichensatz codiert in das Zertifikat der eGK einbringen.
[<=]

4.4 Berufsgruppen-ID der Leistungserbringer

4.4.1 Berufsgruppe des Heilberuflers

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

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

GS-A_4583 - Berufsgruppenkennzeichen für HBA
Der HBA-Herausgeber MUSS die Berufsgruppe(n) des Heilberuflers in Form einer textuellen Bezeichnung und einer OID gemäß Tab_PKI_221 in jedes Zertifikat eines HBA gleichlautend einbringen und dabei die Werte aus [gemSpec_OID#GS-A_4442] verwenden.
[<=]

GS-A_4584 - Verwendung von Berufsgruppenkennzeichen
TSP-X.509 nonQES und TSP-X.509 QES DÜRFEN NICHT Berufsgruppenkennzeichen, für deren Verwendung sie nicht zugelassen und beauftragt sind, in HBA-Zertifikate einbringen.
[<=]

Tabelle 9: Tab_PKI_221 Berufsgruppenkennzeichnung

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

4.5 ID der Organisation/Einrichtung des Gesundheitswesens

4.5.1 Typ und Exemplar der Organisation/Einrichtung des Gesundheitswesens

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

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

GS-A_4585 - Typ der Organisation/Einrichtung des Gesundheitswesens für SMC-B
Der SMC-B-Herausgeber MUSS den Typ der Organisation/Einrichtung des Gesundheitswesens in Form einer textuellen Bezeichnung und einer OID gemäß Tab_PKI_222 in jedes Zertifikat einer SMC-B gleichlautend einbringen und dabei die Werte aus [gemSpec_OID#GS-A_4443] verwenden.
[<=]

GS-A_4586 - Verwendung von Institutionskennzeichen
TSP-X.509 nonQES DÜRFEN Institutskennzeichen, für deren Verwendung sie nicht zugelassen und beauftragt sind, NICHT in SMC-B-Zertifikate einbringen.
[<=]

Tabelle 10: Tab_PKI_222 Institutionstypkennzeichnung

Art der ID	Ort	X.509 Feldname	Format	Inhalt	Beispiel
Institutionstyp	Admission	`ProfessionItem`	Text	<Institutionstyp>	Zahnarztpraxis
		`ProfessionOID`	OID	oid_<institutionstyp>	1.2.276.0.76.4.51
Einzelne Institution	Admission	`RegistrationNumber`	AN	<Telematik-ID>	2- 2a25sd-d529

4.6 Technische Rolle von Komponenten und Diensten

4.6.1 Technische Rolle im Komponentenzertifikat

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

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

GS-A_4707 - Kennzeichen für Technische Rolle für Komponenten und Dienste
Der Kartenherausgeber MUSS die technische Rolle einer Komponente bzw. eines Dienstes in Form einer textuellen Bezeichnung und einer OID gemäß Tab_PKI_230 in jedes Zertifikat der Komponente bzw. des Dienstes gleichlautend einbringen und dabei die Werte aus [gemSpec_OID#GS-A_4446] verwenden.
[<=]

GS-A_4708 - Verwendung von Kennzeichen für Technische Rolle
TSP-X.509 nonQES für gSMC MÜSSEN ausschließlich solche Kennzeichen für technische Rollen in Komponentenzertifikate einbringen, für die der Antragsteller nachweislich berechtigt ist.
[<=]

Tabelle 11: Tab_PKI_230 Kennzeichnung Technische Rolle

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

4.7 Telematik-ID

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

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

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

GS-A_4958 - Neue Telematik-ID bei Folgekarten
Der Kartenherausgeber MUSS bei der Ausgabe von Folgekarten dem Antragsteller die Möglichkeit bieten, eine neue Telematik-ID zu beziehen.
[<=]

GS-A_4960 - System für Sektorkennzeichen
Der Gesamtbetriebsverantwortliche der TI MUSS zur Sicherstellung der Eindeutigkeit der Telematik-ID über die verschiedenen Sektoren des Gesundheitswesens hinweg ein System für Sektorkennzeichen als Bestandteil (Präfix) der Telematik-ID etablieren und verwalten.
[<=]

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

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

GS-A_4709 - Abbildung der Telematik-ID in Admission-Struktur
TSP-X.509 nonQES MÜSSEN zur Abbildung der Telematik-ID in HBA- sowie SMC-B-Zertifikaten eine Admission Extension aufnehmen, die eine oder mehrere Struktur(en) „ProfessionInfo" und darin im Feld „registrationNumber" die Telematik-ID enthalten

muss.
[<=]

GS-A_4901 - Einheitliche Admission in Zertifikaten einer Karte
TSP-X.509 QES und TSP-X.509 nonQES SOLLEN die Admission Extension in allen X.509-Zertifikaten einer Karte identisch einbringen. In den Herausgabe-Policies können Ausnahmen hiervon definiert sein.
[<=]

Tabelle 12: Tab_PKI_224 Telematik-ID-Kennzeichnung

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

4.7.2 Aufbau der Telematik-ID

GS-A_4587 - Gesamtlänge der Telematik-ID
Herausgeber von HBA und SMC-B MÜSSEN sicherstellen, dass die Gesamtlänge der Telematik-ID (Präfix, Separator und Fortsatz) 128 Zeichen nicht überschreitet.
[<=]

Tabelle 13: Tab_PKI_223 Aufbau der Telematik-ID

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

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

4.7.2.1 Sektoraler Präfix

GS-A_4710 - Präfix der Telematik-ID
Herausgeber von HBA und SMC-B MÜSSEN die in Tab_PKI_101 festgelegten Präfixe der Telematik-ID verwenden.
[<=]

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

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

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

Die gematik teilt den von ihr herausgegebenen Identitäten bzw. Karten SMC-B ORG das Präfix "9" zu, auch wenn die berechtigten Organisationen den in Tab_PKI_101-01 gelisteten Sektoren mit den Präfixen "1-8" zuzurechnen sind. Darüber hinaus sind für eine Übergangszeit, voraussichtlich bis 2025, im Bereich der Kassenzahnärztlichen Vereinigungen noch Karten SMC-B ORG im produktiven Einsatz, die das Präfix "2" tragen.

Der Nummernraum des Präfixes wird durch die gematik GmbH verwaltet.

4.7.2.2 Separator

GS-A_4711 - Separator der Telematik-ID
Herausgeber von HBA und SMC-B MÜSSEN sicherstellen, dass bei der Abbildung der Telematik-ID das Präfix vom Rest der Telematik-ID durch einen Separator getrennt wird und als Separator das Minuszeichen „-" mit ASCII-Wert 45 dezimal beziehungsweise 0x2D hexadezimal verwendet wird.

[<=]

4.7.2.3 Fortsatz der Telematik-ID

GS-A_4712 - Definition und Eindeutigkeit der Telematik-ID
Kartenherausgeber von HBA und SMC-B in den jeweiligen Sektoren MÜSSEN Syntax, Semantik und Vergabe des Fortsatzes der Telematik-ID so definieren, dass die

Eindeutigkeit des sektorspezifischen Anteils der Telematik-ID gewährleistet ist.
[<=]

Beispiele für die weiterführende Unterteilung für den Bereich der Ärzteschaft:

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

GS-A_4713 - Zeichensatz für den Fortsatz der Telematik-ID
TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN den vom jeweiligen Sektor vorgegebenen Zeichensatz für den Fortsatz der Telematik-ID verwenden.
[<=]

4.8 Kodierung der Zertifikate

4.8.1 Kodierung der Attribute

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

GS-A_4714-01 - Kodierung der Attribute in X.509-Zertifikaten
TSP-X.509 und der Anbieter des TSL-Dienstes MÜSSEN bei der Kodierung der Attribute in X.509-Zertifikaten die Vorgaben aus Tab_PKI_229-01 umsetzen. Die Vorgaben sind unabhängig davon, ob das jeweilige Attribut innerhalb eines issuer (Typ Name)-, subject (Typ Name)- oder eines extension (Typ Extension)-Elementes im Zertifikat verwendet wird

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

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

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

[<=]

4.8.2 Stringlänge der Attribute

GS-A_4715-01 - Maximale Stringlänge der Attribute im SubjectDN
TSP-X.509 und der Anbieter des TSL-Dienstes MÜSSEN bzgl. der maximalen Stringlänge der Attribute in X.509-Zertifikaten die Vorgaben aus Tab_PKI_229-01 umsetzen. Die Vorgaben sind unabhängig davon, ob das jeweilige Attribut innerhalb eines issuer (Typ Name)-, subject (Typ Name)- oder eines extension (Typ Extension)-Elementes im Zertifikat verwendet wird.**[<=]**

GS-A_4716 - Umgang mit überlangen Organisationsnamen im SubjectDN
Der TSP-X.509 nonQES für Komponenten, die gematik Root-CA und der Anbieter des TSL-Dienstes MÜSSEN für den Fall, dass der Wert des Attributs organizationName {id-at 10} in X.509-Zertifikaten eine String-Länge größer als 64 Zeichen hat, sicherstellen, dass die Angabe im subject auf 64 Zeichen abgekürzt wird und die Extension SubjectAltNames {2 5 29 17} mit der ungekürzten Angabe in das Zertifikat eingefügt wird.
[<=]

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

4.8.3 Struktur

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

4.8.3.1 serialNumber

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

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

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

Der Nummernraum des Präfixes wird durch die gematik GmbH verwaltet.

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

GS-A_4725 - Eindeutiger SubjectDN durch serialNumber
Ein TSP-X.509 nonQES KANN die Eindeutigkeit des SubjectDN in einem X.509-Zertifikat für Zentrale Dienste und Fachanwendungsspezifischen Dienste durch die Verwendung des Attributes serialNumber {id-at-serialNumber} gewährleisten.
[<=]

GS-A_4726 - Verwendung von serialNumber zur Schaffung eindeutiger SubjectDNs
TSP-X.509 nonQES MÜSSEN bei Verwendung des Attributs serialNumber in X.509-Zertifikaten für Zentrale Dienste und Fachanwendungsspezifische Dienste den Inhalt entsprechend dem folgenden Format aufbauen: Instanz (fünfstellige Dezimalzahl) + "-" + Unterscheidung Zertifikat (alphanumerischer Wert).
[<=]

4.8.3.2 Admission

Die Extension Admission enthält Angaben zur Registrierung und zu der beruflichen Zulassung (und somit auch zu daraus ableitbaren Autorisierungsinformationen) sowohl als Text als auch in Form einer maschinenlesbaren OID.
Für die verschiedenen Zertifikatstypen sind dies jeweils:

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

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

GS-A_4717-01 - TI-spezifische Vorgabe zur Nutzung der Extension Admission
TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN bei Verwendung der Extension Admission {1 3 36 8 3 3} die Struktur in X.509-Zertifikaten entsprechend Tab_PKI_226-01 erstellen

Tabelle 17: Tab_PKI_226-01 Struktur Admission

#	ASN.1 definition	TI-spezifische Vorgaben
1	**id-isismtt-at-admission** OBJECT IDENTIFIER ::= {1 3 36 8 3 3}	Identifizierung des Objekts über die OID
2	**id-isismtt-at-namingAuthorities** OBJECT IDENTIFIER ::= {1 3 36 8 3 11}	Identifizierung des Objekts über die OID
3	**AdmissionSyntax ::=** SEQUENCE {	
4	admissionAuthority GeneralName OPTIONAL,	Angabe (optional) der admissionAuthority auf der obersten Ebene der Extension in Form eines Distinguished Name (directoryName). In den jeweiligen Zertifikatsprofilen und -ausprägungen wird dieser Distinguished Name in Textform gemäß [RFC4514] dargestellt.
5	contentsOfAdmissions SEQUENCE OF Admissions }	Diese Sequenz MUSS genau ein Element vom Typ Admissions enthalten.
6	**Admissions** ::= SEQUENCE {	
7	admissionAuthority [0] EXPLICIT GeneralName OPTIONAL,	
8	namingAuthority [1] EXPLICIT NamingAuthority OPTIONAL,	
9	professionInfos SEQUENCE OF ProfessionInfo }	Diese Sequenz MUSS ein Element vom Typ ProfessionInfo enthalten.
-		
14	**ProfessionInfo** ::= SEQUENCE {	
15	namingAuthority [0] EXPLICIT NamingAuthority OPTIONAL,	
16	professionItems SEQUENCE OF DirectoryString (SIZE(1..128)),	professionItems enthält ein Element von Typ DirectoryString Für DirectoryString MUSS die Kodierung UTF8String verwendet werden.

17	professionOIDs SEQUENCE OF OBJECT IDENTIFIER OPTIONAL,	Dieses Element MUSS eine OID enthalten.
18	registrationNumber PrintableString(SIZE(1..128)) OPTIONAL,	Wenn dieses optionale Feld enthalten ist, enthält es die Telematik-ID. In QES-HBA-Zertifikaten für Ärzte wird das Feld registrationNumber nicht gesetzt.
19	addProfessionInfo OCTET STRING OPTIONAL }	

[<=]

4.8.3.3 CertificatePolicies

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

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

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

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

[<=]

Tabelle 18: Tab_PKI_227 Struktur CertificatePolicies

#	Asn.1 Definition	TI-spezifische Vorgaben
1	CertificatePolicies ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation	In allen End-Entity-Zertifikaten MUSS genau ein Element dieser Sequenz enthalten.
2	PolicyInformation ::= SEQUENCE {	
3	policyIdentifier CertPolicyId,	Dieses Element MUSS mindestens zweimal enthalten sein: 1 – Policy-OID (einmal oder mehrfach) 2 – Zertifikatstyp-OID (genau einmal bei EE-Zertifikaten, nicht bei Signer-EE-Zertifikaten)

4	policyQualifiers SEQUENCE SIZE(1..MAX) OF PolicyQualifierInfo OPTIONAL }	Enthält das Element PolicyIdentifier die Zertifikatstyp-OID, DARF das Element policyQualifiers NICHT verwendet werden
5	CertPolicyId ::= OBJECT IDENTIFIER	
6	PolicyQualifierInfo ::= SEQUENCE {	
7	policyQualifierId PolicyQualifierId,	
8	qualifier ANY DEFINED BY policyQualifierId }	
9	id-qt OBJECT IDENTIFIER ::= {id-pkix 2}	
10	id-qt-cps OBJECT IDENTIFIER ::= {id-qt 1}	
11	id-qt-unotice OBJECT IDENTIFIER ::= {id-qt 2}	
12	PolicyQualifierId ::= OBJECT IDENTIFIER {id-qt-cps | id-qt-unotice }	
13	CPSUri ::= IA5String	
14	UserNotice ::= SEQUENCE {	
15	noticeRef NoticeReference OPTIONAL,	
16	explicitText DisplayText OPTIONAL }	
17	NoticeReference ::= SEQUENCE {	
18	organization DisplayText,	
19	noticeNumber SEQUENCE OF INTEGER }	
20	DisplayText ::= CHOICE {	
20a	ia5String IA5String (SIZE (1..200)),	
21	visibleString VisibleString (SIZE (1..200)),	

22	bmpString BMPString (SIZE (1..200)),	
23	utf8String UTF8String (SIZE (1..200)) }	

4.8.3.4 CRLDistributionPoints

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

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

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

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

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

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

4.8.3.5 SubjectAltNames

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

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

Tabelle 19: Tab_PKI_228 Struktur SubjectAltName

#	Asn.1 Definition	TI-spezifische Vorgaben
1	SubjectAltNames ::= GeneralNames	Ein GeneralNames-Feld enthält eine Sequenz von GeneralName-Elementen. Die Typ-Ausprägungen in den folgenden Zeilen sind für GeneralName zulässig.
2	rfc822Name [1] IMPLICIT IA5String,	E-Mail-Adresse in der Form rfc822Name
3	dNSName [2] IMPLICIT IA5String,	"Domain Name Label" wie in [RFC5280], Kap. 4.2.1.6. beschrieben

4	otherName [0] IMPLICIT OtherName,
	
	OtherName ::= SEQUENCE
	{
	type-id OBJECT IDENTIFIER
	value [0] EXPLICIT ANY DEFINED BY type-id
	}
		‚type-id' ist gleich dem OID eines Attributes im SubjectDN.
		Als ‚value' ist ein UTF8-String enthalten. Dieser String enthält
		• den im Attribut enthaltenen Namen in voller Länge, wenn er aufgrund der Längenbeschränkung im SubjectDN gekürzt werden musste
		• oder bei Bedarf einen Alternativnamen oder eine Ergänzung zu diesem Attribut.

Erläuterung:

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

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

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

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

- commonName {id-at 3}
- organizationalUnitName {id-at 11}
- organizationName {id-at 10}

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

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

4.9 Erläuterungen zu Zertifikatsprofilen

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

4.9.1 Allgemeine Erläuterungen

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

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

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

Die normative Festlegung der Werte der Felder **`professionItems`** und **`professionOIDS`** erfolgt in den Tabellen Tab_PKI_402, Tab_PKI_403 und Tab_PKI_406 in [gemSpec_OID#3.5].

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

4.9.2 Berufs-/Rollenattribute und Sperrbarkeit

GS-A_4721 - Beantragung Rollenattribute im X.509-Zertifikatsrequest
Der TSP-X.509 nonQES der Komponenten-PKI MUSS bei der Erstellung von X.509-Zertifikate für Dienste sicherstellen, dass ein Diensteanbieter nur Zertifikate für die Rollen beantragen kann, für die dieser Diensteanbieter in der TI von der gematik zugelassen ist.
[<=]

GS-A_4961 - Verwendung zugewiesener Berufs- und Rollenattribute
Die Kartenherausgeber MÜSSEN genau die Berufs- und Rollenattribute verwenden, die den zertifizierten Identitäten entweder auf gesetzlicher Grundlage oder durch Zuweisung einer gesetzlich autorisierten Standesvertretung zugewiesen wurden. Für die codierte Form dieser Attribute MÜSSEN die von der TI-Plattform verwalteten Berufs- und Rollencodes verwendet werden.
[<=]

GS-A_4722 - Belegung der Felder professionInfos
Der TSP-X.509 nonQES MUSS bei der Erstellung von X.509-Zertifikaten sicherstellen, dass die Werte **`professionItems`** und **`professionOIDS`** den Festlegungen für den Typ des beantragten Zertifikats entsprechen.
[<=]

GS-A_4724 - Komplettsperrung aller Zertifikate einer Karte
TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN sicherstellen, dass alle Zertifikate auf einem Kartenexemplar durch einen Sperrauftrag gesperrt werden können (sofern für die jeweiligen Zertifikatstypen die Statusinformationsbereitstellungen gefordert sind).
[<=]

4.9.3 Benennung der Zertifikatsprofile

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

4.9.4 Distinguished Name

Die Bezeichnung von Entitäten in X.509-Zertifikaten (in den Feldern „Subject", „Issuer" oder „admissionAuthority") erfolgt über eine Datenstruktur, welche „Distinguished Name" genannt wird. Beispiel:
"CN=John Smith,OU=Sales,O=ACME Limited,L=Moab,ST=Utah,C=US"

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

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

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

Distinguished Names können auch tabellarisch dargestellt werden. Dabei wird das hierarchisch höchste Element zuunterst aufgeführt. Die Reihenfolge in den Subject-Feldern in den Zertifikatsprofilen in Kapitel 5 folgt auch der tabellarischen Darstellung. Das hierarchisch tiefste Element (commonName bzw. CN) wird jeweils zuoberst notiert, „C=DE" ganz unten in der Tabelle.

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

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

A_15676 - Reihenfolge der Elemente im SubjectDN von X.509-Zertifikaten
Der TSP-X.509 und der TSL-Dienst SOLLEN die Reihenfolge der Elemente im SubjectDN von erstellten X.509-Zertifikaten gemäß der Zertifikatsprofiltabellen in [gemSpec_PKI] umsetzen. Dabei sind die Elemente in den Zertifikatsprofiltabellen in aufsteigender Hierarchie angeordnet. In den X.509-Zertifikaten sind die Elemente in der Reihenfolge der entsprechenden absteigenden Hierarchie zu realisieren.
[<=]

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

SubjectDN (String)

```
C=DE, O=2-29999999999 NOT-VALID, serialNumber=12.80276002791200027011,
CN=Zahnarztpraxis Prof. Dr. Dr. Dr. med. rer. nat. Dip:PN TEST-ONLY
```

SubjectDN (ASN.1-Codierung)

```
SEQUENCE {
  SET {
    SEQUENCE {
      OBJECT IDENTIFIER countryName (2 5 4 6)
      PrintableString 'DE'
      }
    }
  SET {
    SEQUENCE {
      OBJECT IDENTIFIER organizationName (2 5 4 10)
      UTF8String '2-29999999999 NOT-VALID'
      }
    }
 SET {
   SEQUENCE {
     OBJECT IDENTIFIER serialNumber (2 5 4 5)
     PrintableString '12.80276002791200027011'
     }
   }
 SET {
   SEQUENCE {
     OBJECT IDENTIFIER commonName (2 5 4 3)
     UTF8String
       'Zahnarztpraxis Prof. Dr. Dr. Dr. med. rer. nat. '
       'Dip:PN TEST-ONLY'
     }
   }
}
```

4.10 Kodierung der Betriebsumgebungen in Zertifikaten

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

GS-A_4727 - PKI-Separierung von Test- und Produktivumgebung in der TI
Der TSP-X.509 und der Anbieter des TSL-Dienstes DÜRFEN für die Generierung von EE-Zertifikaten der Produktivumgebung NICHT eine CA der Testumgebung verwenden. Umgekehrt DÜRFEN der TSP-X.509 und der Anbieter des TSL-Dienstes für die Generierung von EE-Zertifikaten der Testumgebung NICHT eine CA der Produktivumgebung verwenden.
[<=]

GS-A_4588 - CA-Namen für Test-PKI der TI
Der TSP-X.509 und der Anbieter des TSL-Dienstes MÜSSEN die Namen (CN: und O:) sämtlicher CAs in der Test-PKI entsprechend den korrespondierenden CAs der Produktivumgebung vergeben und diese um den String „TEST-ONLY" im CN-Feld sowie „NOT-VALID" im O-Feld ergänzen.
[<=]

GS-A_4589 - EE-Namen für Test-PKI der TI
TSP-X.509 nonQES (außer eGK) und TSP-X.509 QES MÜSSEN die Namen (CN: und O:) der EE-Zertifikate in der Test-PKI entsprechend den korrespondierenden Zertifikatsprofilen der Produktivumgebung verwenden und ergänzen:

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

[<=]

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

Die folgende Tabelle dient der Detaillierung dieses Sachverhaltes:

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

Zertifikatstyp	Halter / Art	CN Test-PKI gleich CN Produktiv-PKI?
C.HCI.AUT	Organisation/Institution	Nein
C.HCI.ENC	Organisation/Institution	Nein
C.HCI.OSIG	Organisation/Institution	Nein
C.HP.AUT	Person	Nein
C.HP.ENC	Person	Nein
C.HP.QES	Person	Nein
C.GEM.OCSP	Signer	Nein
C.GEM.CRL	Signer	Nein
C.TSL.SIG	Signer	Nein
C.SMKT.AUT	Gerät	Ja
C.NK.VPN	Gerät	Ja
C.AK.AUT	Gerät	Ja
C.SAK.AUT	Gerät	Ja
C.VPNK.VPN	Dienst	Ja
C.VPNK.VPN-SIS	Dienst	Ja
C.ZD.TLS-C	Dienst	Ja
C.ZD.TLS-S	Dienst	Ja
C.FD.TLS-C	Dienst	Ja
C.FD.TLS-S	Dienst	Ja
C.FD.SIG	Dienst	Ja
C.FD.AUT	Dienst	Ja
C.FD.ENC	Dienst	Ja

C.CM.TLS-CS	Dienst	Ja
C.SGD-HSM.AUT	Dienst	Ja

GS-A_4590 - Zertifikatsprofile für Test-PKI
Der TSP-X.509 und der Anbieter des TSL-Dienstes SOLLEN die Feldattribute (außer CN: und O:) für sämtliche Zertifikate in der Test-PKI gemäß den korrespondierenden Profilen der Produktivumgebung setzen.
[<=]

4.11 Kartenverlust und Deaktivierung von Chipkarten

GS-A_4962 - Verhalten bei Kartenverlust und Änderung persönlicher Daten
Der Kartenherausgeber MUSS den Zertifikatsnehmer verpflichten, Sperrungen seiner Karte bzw. seines Sicherheitsmoduls bei dem Kartenherausgeber oder bei einer von ihm benannten Stelle durchführen zu lassen. Sperrgründe können beispielweise der Verlust der Karte bzw. des Sicherheitsmoduls sowie Änderungen zu registrierungsrelevanten persönlichen Daten sein (z. B. Änderung der Zugehörigkeit zu einer Berufsgruppe).
[<=]

GS-A_4963 - Deaktivierung von Chipkarten nach Gültigkeitsende
Der Kartenherausgeber MUSS Vorgaben definieren, wie eine Chipkarte sowie die enthaltenen kryptographischen Schlüssel nach Ablauf ihrer definierten Gültigkeitsdauer dauerhaft unbrauchbar gemacht werden.
[<=]

5 X.509-Zertifikate

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

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

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

GS-A_4965 - Keine Suspendierung von X.509-Zertifikaten (außer für eGK)
Ein TSP-X.509 DARF für X.509-Zertifikate – außer denen der eGK – eine Suspendierung NICHT implementieren.
[<=]

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

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

GS-A_5337 - Größenbeschränkung von X.509 Zertifikaten auf Karten
Ein TSP X.509 (außer ein TSP X.509 für eGK) MUSS sicherstellen, dass die von ihm erzeugten Zertifikate, die für die Speicherung auf Karten vorgesehen sind, die Maximalgröße der dafür vorgesehenen Kartenobjekte - gemäß der relevanten Objektsystemspezifikationen - nicht überschreiten. Wenn zu lange Eingangsdaten vorliegen sind diese in Abstimmung mit dem Antragsteller/Kartenherausgeber zu ändern.
[<=]

5.1 eGK – Versichertenkarte

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

5.1.1 Definition der Versichertenidentität

Folgende Datenfelder bilden die Namensidentität des Versicherten

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

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

- **commonName**
- **title**
- **givenName**
- **surname**

GS-A_4966 - Nutzung bestehender Versichertendatensätze für eGK-Zertifikate
Für die Erstellung von Versichertenzertifikaten SOLL der Kartenherausgeber bestehende Versichertendatensätze für die Registrierung von Zertifikatsnehmern verwenden.
[<=]

5.1.2 Belegung der Felder im SubjectDN

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

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

Titel Vorname Namenszusatz Vorsatzwort Familienname

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

GS-A_4968 - Erzeugung und Einbringung der KVNR
Der eGK-Kartenherausgeber MUSS als eindeutigen Identifier des Versicherten die KVNR gemäß gesetzlicher Vorgaben erzeugen und Festlegungen treffen, welche Anteile der KVNR in die Versichertenzertifikate einzubringen sind.
[<=]

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

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

GS-A_4594 - Bildung des title im SubjectDN eGK-Zertifikat
Der Kartenherausgeber MUSS für das Feld `title` im SubjectDN der eGK-Zertifikate das Attribut *Titel* verwenden. Kürzungen können bei Überschreitung der maximal zulässigen Länge vorgenommen werden; Kürzungsregeln sind nicht definiert.
[<=]

Beispielsatz der Feldinhalte

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

Im Zertifikat wären folgende Attribute zu verwenden:

Tabelle 21: Tab_PKI_231 Personennamen im subjectDN

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

5.1.3 X.509-Zertifikatsprofile der eGK

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

GS-A_4969 - Suspendierung von eGK-Zertifikaten (nonQES)
Ein Kartenherausgeber SOLL für die X.509-Zertifikate der eGK eine Suspendierung und Desuspendierung von nonQES-Zertifikaten NICHT implementieren. Für das optional auf der eGK befindliche QES-Zertifikat und die AUT_ALT-Zertifikate ist eine Suspendierung/Desuspendierung nicht möglich.
[<=]

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

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

GS-A_4595 - Umsetzung Zertifikatsprofil C.CH.AUT
Der TSP-X.509 nonQES (eGK) MUSS C.CH.AUT gemäß Tab_PKI_232 umsetzen.
[<=]

A_17989 - Umsetzung Zertifikatsprofil C.CH.AUT_ALT
Der TSP-X.509 nonQES (eGK) MUSS C.CH.AUT_ALT gemäß Tab_PKI_232 umsetzen.
[<=]

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

Element	Inhalt	Kar.	
certificate	C.CH.AUT, C.CH.AUT_ALT		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
issuer	DN der ausstellenden CA		
validity	Gültigkeit des Zertifikats (von - bis)		
subject			
CommonName	CN = Aufgedruckte Namenszeilen der Karte	1	
title	Titel des Versicherten	0-1	
givenName	Vorname des Versicherten	1	
surname	Nachname des Versicherten	1	
organizationalUnitName	OU = unveränderbarer Teil der KV-Nummer	1	
organizationalUnitName	OU = Institutionskennzeichen	1	
organizationName	O = Herausgeber	1	
countryName	C = DE	1	
subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers	1	
extensions			critical
SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Versicherten	1	FALSE
KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	 1 0-1 1	**TRUE**
SubjectAltNames {2 5 29 17}	rfc822Name	0-1	FALSE
BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) *Für Zertifikate der eGK:* policyIdentifier = <oid_egk_aut>	1 0-1 1	FALSE

				Für Zertifikate der alternativen Versichertenidentitäten: policyIdentifier = <oid_egk_aut_alt>	1	
			CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
			AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
			Admission {1 3 36 8 3 3}	professionItem = Beschreibung zu <oid_versicherter> gemäß [gemSpec_OID#GS-A_4442] professionOID = OID <oid_versicherter> gemäß gemSpec_OID#GS-A_4442	1 1	FALSE
			ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth	0-1	FALSE
			andere Erweiterungen		0	
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	signature			Wert der Signatur		

5.1.3.2 C.CH.ENC – Verschlüsselung eGK

GS-A_4596 - Umsetzung Zertifikatsprofil C.CH.ENC

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

Tabelle 23: Tab_PKI_233 C.CH.ENC Verschlüsselung eGK

Element			Inhalt	Kar.	
certificate			C.CH.ENC		
	tbsCertificate				
		version	2 (v3)		
		serialNumber	gemäß [RFC5280#4.1.2.2.]		
		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt# GS-A_4362]		
		issuer	DN der ausstellenden CA		
		validity	Gültigkeit des Zertifikats (von - bis)		
		subject			
		CommonName	CN = Aufgedruckte Namenszeilen der Karte	1	
		title	Titel des Versicherten	0-1	
		givenName	Vorname des Versicherten	1	
		surname	Nachname des Versicherten	1	

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

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

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

Element	Inhalt	Kar.	
certificate	C.CH.QES		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt# GS-A_4358]		
issuer	DN der ausstellenden CA		
validity	Gültigkeit des Zertifikats (von - bis)		
subject			
CommonName	CN = Aufgedruckte Namenszeilen der Karte	1	
title	Titel des Versicherten	0-1	
givenName	Vorname des Versicherten	1	
surname	Nachname des Versicherten	1	
organizationalUnitName	OU = unveränderbarer Teil der KV-Nummer	1	
organizationalUnitName	OU = Institutionskennzeichen	1	
organizationName	O = Herausgeber	1	
countryName	C = DE	1	
subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4358] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers	1	
extensions	Erweiterungen		critical
SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Versicherten	1	FALSE
KeyUsage {2 5 29 15}	nonRepudiation	1	**TRUE**
BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_egk_qes>	1 0-1 1	FALSE
CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE

			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
			SubjectDirectoryAttributes (2.5.29.9)	Angaben, die den Zertifikatsinhaber zusätzlich zu den Angaben unter 'subject' eindeutig identifizieren: Titel (optional), Geburtstag (optional), Geburtsort (optional), Geburtsname (optional)	0-1	FALSE
			AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
			Admission {1 3 36 8 3 3}	professionItem = Beschreibung zu <oid_versicherter> gemäß [gemSpec_OID#GS-A_4442] professionOID = OID <oid_versicherter> gemäß gemSpec_OID#GS-A_4442	1 1	FALSE
			QCStatements (1.3.6.1.5.5.7.1.3)	id-qcs-pkixQCSyntax-v1(1.3.6.1.5.5.7.11.1) Konformität zu Syntax und Semantik nach [RFC3739] (optional) id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) Ausgabe des Zertifikats erfolgte konform zur Europäischen Richtlinie 1999/93/EG und nach dem Recht des Landes, nach dem die CA arbeitet. (obligatorisch)	1 1	FALSE
			ExtendedKeyUsage {2 5 29 37}		0	
			andere Erweiterungen		0	
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt# GS-A_4358]		
	signature			Wert der Signatur		

5.1.3.4 C.CH.AUTN - Technische Authentisierung eGK

GS-A_4598 - Umsetzung Zertifikatsprofil C.CH.AUTN

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

[<=]

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

Element			Inhalt	Kar.	
certificate			C.CH.AUTN		
	tbsCertificate				
		version	2 (v3)		
		serialNumber	gemäß [RFC5280#4.1.2.2.]		

		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
		issuer	DN der ausstellenden CA		
		validity	Gültigkeit des Zertifikats (von - bis)		
		subject			
		CommonName	CN = Pseudonym der Versichertenidentität	1	
		organizationalUnitName	OU = Institutionskennzeichen	1	
		organizationName	O = Herausgeber	1	
		countryName	C = DE	1	
		subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers	1	
		extensions	Erweiterungen		critical
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Versicherten	1	FALSE
		KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	1 0-1 1	**TRUE**
		SubjectAltNames {2 5 29 17}	rfc822Name	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_egk_autn>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = Beschreibung zu <oid_versicherter> gemäß [gemSpec_OID#GS-A_4442] professionOID = OID <oid_versicherter> gemäß gemSpec_OID#GS-A_4442	1 1	FALSE
		ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth	1	FALSE

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

5.1.3.5 C.CH.ENCV - Technische Verschlüsselung eGK

GS-A_4599 - Umsetzung Zertifikatsprofil C.CH.ENCV

Der TSP-X.509 nonQES (eGK) MUSS C.CH.ENCV gemäß Tab_PKI_236 umsetzen.
[<=]

Tabelle 26: Tab_PKI_236 C.CH.ENCV Technische Verschlüsselung eGK

Element			Inhalt	Kar.	
certificate			C.CH.ENCV		
	tbsCertificate				
		version	2 (v3)		
		serialNumber	gemäß [RFC5280#4.1.2.2.]		
		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4362]		
		issuer	DN der ausstellenden CA)		
		validity	Gültigkeit des Zertifikats (von – bis)		
		subject			
		CommonName	CN = Pseudonym der Versichertenidentität	1	
		organizationalUnitName	OU = Institutionskennzeichen	1	
		organizationName	O = Herausgeber	1	
		countryName	C = DE	1	
		subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt# GS-A_4362] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers	1	
		extensions	Erweiterungen		critical
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Versicherten	1	FALSE
		KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* keyEncipherment dataEncipherment *Für Schlüsselgeneration ECDSA:* keyAgreement	 1 1 1	**TRUE**
		SubjectAltNames {2 5 29 17}	rfc822Name	0-1	FALSE

			BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
			CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_egk_encv>	1 0-1 1	FALSE
			CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
			AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
			Admission {1 3 36 8 3 3}	professionItem = Beschreibung zu <oid_versicherter> gemäß [gemSpec_OID#GS-A_4442] professionOID = OID <oid_versicherter> gemäß gemSpec_OID#GS-A_4442	1 1	FALSE
			ExtendedKeyUsage {2 5 29 37}		0	
			andere Erweiterungen		0	
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4362]		
	signature			Wert der Signatur		

5.2 HBA – Heilberufsausweis

GS-A_5042 - Kodierung der X.509-Zertifikate für HBA und SMC-B
TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN bei der Herausgabe von Zertifikaten für HBA und SMC-B die übergreifenden Kodierungsvorschriften aus [gemSpec_PKI#4] umsetzen.

[<=]

5.2.1 X.509 Zertifikatsprofile des HBA

5.2.1.1 C.HP.AUT – Authentisierung HBA

GS-A_5531-01 - Umsetzung Zertifikatsprofil C.HP.AUT
Der TSP-X.509 nonQES MUSS C.HP.AUT gemäß Tab_PKI_268_1 umsetzen.**[<=]**

Tabelle 27: Tab_PKI_268_1 C.HP.AUT Authentisierung HBA

Element	Inhalt *)	Kar.	
certificate	C.HP.AUT		
tbsCertificate			

		version	2 (v3)		
		serialNumber	gemäß [RFC5280#4.1.2.2.]		
		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
		issuer	Distinguished Name (DN) der Aussteller-CA gemäß [gemSpec_PKI# GS-A_4737]		
		validity	Gültigkeit des Zertifikats (von – bis)		
		subject			
		commonName **)	Vor- und Nachname des Inhabers (bei Kürzung ev. Suffix :PN)	1	
		title **)	nicht gesetzt	0	
		givenName **)	Vornamen des Inhabers	1	
		surName **)	Nachname des Inhabers	1	
		serialNumber **)	Eindeutige Identifikationsnummer (dieselbe wie in ENC und QES)	1	
		organizationalUnitName	nicht gesetzt	0	
		organizationName	nicht gesetzt	0	
		countryName	DE	1	
		andere Attribute		0	
		subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
		extensions			critical
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Inhabers	1	FALSE
		KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature keyAgreement	 1 1 1 1	**TRUE**
		SubjectAltNames {2 5 29 17}	rfc822Name = E-Mail-Adresse	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = <URL zur Publikation der Zertifikatsrichtlinie(n)> policyIdentifier = <oid_hba_aut> gemäß [gemSpec_OID#GS-A_4445] policyIdentifier =<OID der TSP-spezifischen	1 0-1 1 0-1	FALSE

				Policy> policyQualifierInfo = URL der TSP-spezifischen Zertifikatsrichtlinie ggf. weitere sektorspezifische policyIdentifier und policyQualifierInfo	0-1 0-1	
			CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
			AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
			Admission {1 3 36 8 3 3}	admissionAuthority = {O=< zuständige Registrierungsstelle gemäß sektorspezifischer Ausprägung*>,C=DE} professionItem = gemäß [gemSpec_OID#GS-A_4442] professionOID = gemäß [gemSpec_OID#GS-A_4442] registrationNumber = Telematik-ID des Inhabers	1 1 1 1	FALSE
			ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth keyPurposeId = id-kp- emailProtection	1 1	FALSE
			ValidityModel {1 3 6 1 4 1 8301 3 5}	nicht gesetzt	0	FALSE
			QCStatements {1 3 6 1 5 5 7 1 3}	nicht gesetzt	0	FALSE
			additionalInformation {1 3 36 8 3 15}	nicht gesetzt	0	FALSE
			Restriction {1 3 36 8 3 8}	nicht gesetzt	0	FALSE
			andere Erweiterungen		0	
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
	signature			Wert der Signatur		

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

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

5.2.1.2 C.HP.ENC – Verschlüsselung HBA

GS-A_5532-01 - Umsetzung Zertifikatsprofil C.HP.ENC
Der TSP-X.509 nonQES MUSS C.HP.ENC gemäß Tab_PKI_269_1 umsetzen.**[<=]**

Tabelle 281: Tab_PKI_269_1 C.HP.ENC Verschlüsselung HBA

Element	Inhalt *)	Kar.	
certificate	C.HP.ENC		

tbsCertificate				
	version	2 (v3)		
	serialNumber	gemäß [RFC5280#4.1.2.2.]		
	signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
	issuer	Distinguished Name (DN) der Aussteller-CA gemäß [gemSpec_PKI# GS-A_4737]		
	validity	Gültigkeit des Zertifikats (von - bis)		
	subject			
	commonName **)	Vor- und Nachname des Inhabers (bei Kürzung ev. Suffix :PN)	1	
	title **)	nicht gesetzt	0	
	givenName **)	Vornamen des Inhabers	1	
	surName **)	Nachname des Inhabers	1	
	serialNumber **)	Eindeutige Identifikationsnummer (dieselbe wie in AUT und QES)	1	
	organizationalUnitName	nicht gesetzt	0	
	organizationName	nicht gesetzt	0	
	countryName	DE	1	
	andere Attribute		0	
	subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4362] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
	extensions			critical
	SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Inhabers	1	FALSE
	KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* keyEncipherment dataEncipherment *Für Schlüsselgeneration ECDSA:* keyAgreement	 1 1 1	**TRUE**
	SubjectAltNames {2 5 29 17}	rfc822Name = E-Mail-Adresse	0-1	FALSE
	BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
	CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = <URL zur Publikation der Zertifikatsrichtlinie(n)> policyIdentifier = <oid_hba_enc> gemäß [gemSpec_OID#GS-A_4445] policyIdentifier =<OID der TSP-spezifischen	1 0-1 1 0-1	FALSE

				Policy> policyQualifierInfo = URL der TSP-spezifischen Zertifikatsrichtlinie ggf. weitere sektorspezifische policyIdentifier und policyQualifierInfo	0-1 0-1	
			CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
			AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
			Admission {1 3 36 8 3 3}	admissionAuthority = {O=< zuständige Registrierungsstelle gemäß sektorspezifischer Ausprägung*>,C=DE} professionItem = gemäß [gemSpec_OID#GS-A_4442] professionOID = gemäß [gemSpec_OID#GS-A_4442] registrationNumber = Telematik-ID des Inhabers	1 1 1 1	FALSE
			ExtendedKeyUsage {2 5 29 37}	nicht gesetzt	0	FALSE
			ValidityModel {1 3 6 1 4 1 8301 3 5}	nicht gesetzt	0	FALSE
			QCStatements {1 3 6 1 5 5 7 1 3}	nicht gesetzt	0	FALSE
			additionalInformation {1 3 36 8 3 15}	nicht gesetzt	0	FALSE
			Restriction {1 3 36 8 3 8}	nicht gesetzt	0	FALSE
			andere Erweiterungen		0	
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
	signature			Wert der Signatur		

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

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

5.2.1.3 C.HP.QES – Qualifizierte Signatur HBA

GS-A_5533-01 - Umsetzung Zertifikatsprofil C.HP.QES
Der TSP-X.509 QES MUSS C.HP.QES gemäß Tab_PKI_270_1 umsetzen.**[<=]**

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

Element	Inhalt *)	Kar.	
certificate	C.HP.QES		

tbsCertificate				
	version	2 (v3)		
	serialNumber	gemäß [RFC5280#4.1.2.2.]		
	signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4358]		
	issuer	Distinguished Name (DN) der Aussteller-CA gemäß [gemSpec_PKI# GS-A_4948]		
	validity	Gültigkeit des Zertifikats (von – bis)		
	subject			
	commonName **)	Vor- und Nachname des Inhabers (bei Kürzung ev. Suffix :PN)	1	
	title **)	nicht gesetzt	0	
	givenName **)	Vorname des Inhabers	1	
	surName **)	Nachname des Inhabers	1	
	serialNumber **)	Eindeutige Identifikationsnummer (dieselbe wie in AUT und ENC)	1	
	organizationalUnitName	nicht gesetzt	0	
	organizationName	nicht gesetzt	0	
	countryName	DE	1	
	andere Attribute		0	
	subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4358] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
	extensions			critical
	SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Inhabers	1	FALSE
	KeyUsage {2 5 29 15}	nonRepudiation (laut RFC5280 alternative Bezeichnung „contentCommitment“)	1	**TRUE**
	SubjectAltNames {2 5 29 17}	nicht gesetzt	0	FALSE
	BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
	CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = <URL zur Publikation der Zertifikatsrichtlinie(n)> policyIdentifier = <oid_hba_qes> gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <id-etsi-qcp-natural-qscd> {0.4.0.194112.1.2} policyIdentifier =<OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP-	1 0-1 1 1 0-1 0-1 0-1	FALSE

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

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

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

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

Zusatzinformationen zu einzelnen Feldern:

- **SubjectDN**

  Bildungsregel-Vorschlag gemäß Informationen aus bisherigen Sektor-Spezifikationen:

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

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

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

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

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

- **SubjectSerialNumber**

  Zusätzliche Hinweise gemäß Informationen aus bisherigen Sektor-Spezifikationen:

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

  Bildungs-Vorschlag für subjectSerialNumber:

  subjectSerialNumber = <TSP-ID>.<ICCSN>

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

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

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

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

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

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

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

5.3.1 Definition der Organisationsidentität

Der eindeutige Identitätsname der Organisation wird durch folgende Felder gebildet:

- **`commonName`**
- **`organizationName`**
- **`countryName`**

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

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

GS-A_4971 - Zuordnung von SMC-B zur Institution
Die Kartenherausgeber MÜSSEN die eindeutige Zuordnung von SMC-B zur berechtigten Institution sicherstellen.
[<=]

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

A_15190 - HBA als Grundlage zur Nutzung von medizinischen Anwendungen
Die Kartenherausgeber von SMC-B, welche Leistungserbringern den Zugriff auf Daten von Anwendungen der elektronischen Gesundheitskarte gemäß §291a SGB V ermöglicht, MÜSSEN mittels organisatorischer oder technischer Maßnahmen sicherstellen, dass der

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

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

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

5.3.2 Aufbau Anschriftzone nach [DIN5008]

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

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



Abbildung 4: Das Anschriftenfeld nach DIN5008

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

5.3.3 Umgang mit überlangen Attributen im SubjectDN

Siehe Kapitel 4.8.3.5 „SubjectAltNames".

5.3.4 X.509 Zertifikatsprofile der SMC-B

5.3.4.1 C.HCI.AUT – Authentisierung SMC- B

GS-A_4600 - Umsetzung Zertifikatsprofil C.HCI.AUT
Der TSP-X.509 nonQES MUSS C.HCI.AUT gemäßTab_PKI_238 umsetzen.
[<=]

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

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

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

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

5.3.4.2 C.HCI.ENC – Verschlüsselung SMC-B

GS-A_4601 - Umsetzung Zertifikatsprofil C.HCI.ENC
Der TSP-X.509 nonQES MUSS C.HCI.ENC gemäß Tab Tab_PKI_239 umsetzen.
[<=]

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

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

		extensions			critical
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels der Organisation/Einrichtung des Gesundheitswesens	1	FALSE
		KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* keyEncipherment dataEncipherment *Für Schlüsselgeneration ECDSA:* keyAgreement	 1 1 1	**TRUE**
		SubjectAltNames {2 5 29 17}	rfc822Name ggf. überlange Institutionsnamen, Alternativnamen oder Ergänzungen	0-1 0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_smc_b_enc> policyIdentifier = <OID d. TSP-spezifischen Policy>	1 0-1 1 0-1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	admissionAuthority = {O=<zuständige Registrierungsstelle gemäß sektorspezifischer Ausprägung*)>,C=DE} professionItem = Beschreibung der Institution gemäß [gemSpec_OID#GS-A_4443] professionOID = OID der Institution gemäß [gemSpec_OID#GS-A_4443] registrationNumber = Telematik-ID der Institution	0-1 1 1 1	FALSE
		ExtendedKeyUsage {2 5 29 37}		0	
		andere Erweiterungen		0	
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4362]		
	signature		Wert der Signatur		

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

5.3.4.3 C.HCI.OSIG – Signatur SMC-B

GS-A_4602 - Umsetzung Zertifikatsprofil C.HCI.OSIG
Der TSP-X.509 nonQES MUSS C.HCI.OSIG gemäß Tab_PKI_240 umsetzen.
[<=]

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

Element	Inhalt *)	Kar.	
certificate	C.HCI.OSIG		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
issuer	Distinguished Name (DN) der Aussteller-CA		
validity	Gültigkeit des Zertifikats (von – bis)		
subject			
commonName	Erste zwei Zeilen des Anschriftenfeldes	1	
title	Titel des Verantwortlichen/Inhabers	0-1	
givenName	Vorname des Verantwortlichen/Inhabers	0-1	
surName	Nachname des Verantwortlichen/Inhabers	0-1	
serialNumber	Ti-weit eindeutige Identifikationsnummer	0-1	
organizationalUnitName	Organisationseinheit der Organisation/Einrichtung des Gesundheitswesens	0-1	
organizationName	Name der Organisation/Einrichtung des Gesundheitswesens	0-1	
streetAddress	Strasse, Hausnummer	0-1	
postalCode	Postleitzahl	0-1	
localityName	Stadt	0-1	
stateOrProvinceName	Bundesland	0-1	
countryName	DE	1	
andere Attribute		0	
subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4357] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
extensions			critical

			SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels der Organisation/Einrichtung des Gesundheitswesens	1	FALSE
			KeyUsage {2 5 29 15}	nonRepudiation	1	**TRUE**
			SubjectAltNames {2 5 29 17}	rfc822Name ggf. überlange Institutionsnamen, Alternativnamen oder Ergänzungen	0-1 0-1	FALSE
			BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
			CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_smc_b_osig> policyIdentifier = <OID d. TSP-spezifischen Policy>	1 0-1 1 0-1	FALSE
			CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
			AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
			Admission {1 3 36 8 3 3}	admissionAuthority = {O=<zuständige Registrierungsstelle gemäß sektorspezifischer Ausprägung*)>,C=DE} professionItem = Beschreibung der Institution gemäß [gemSpec_OID#GS-A_4443] professionOID = OID der Institution gemäß [gemSpec_OID#GS-A_4443] registrationNumber = Telematik-ID der Institution	0-1 1 1 1	FALSE
			ExtendedKeyUsage {2 5 29 37}		0	
			andere Erweiterungen		0	
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
	signature			Wert der Signatur		

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

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

Bestehen höhere Performance-Anforderungen an eine SMC-B (z. B. in Krankenhäusern), kann als funktionales Äquivalent eine HSM-basierte Lösung eingesetzt werden. Gemäß

Anforderung [gemKPT_PKI_TIP#TIP1-A_2084] sind die X.509-Zertifikate eines HSM-B entsprechend den Festlegungen der X.509-Zertifikate für SMC-B auszuführen.

5.5 gSMC-KT – eHealth-Kartenterminal

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

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

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

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

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

5.5.1 Definition der Kartenterminalidentität

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

- **`commonName = [ICCSN des gSMC-KT]`**
- **`organizationName = [Name des Kartenterminal-Herstellers],`**
- **`countryName = [Herkunftsland des Kartenterminal-Herstellers]`**

5.5.2 X.509 Zertifikatsprofile der gSMC-KT

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

GS-A_4604 - Umsetzung Zertifikatsprofil C.SMKT.AUT
Der TSP-X.509 nonQES MUSS C.SMKT.AUT gemäß Tab_PKI_241 umsetzen.
[<=]

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

Element	Inhalt	Kar.	
certificate	C.SMKT.AUT		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		

		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
		issuer	DN der ausstellenden CA		
		validity	Gültigkeit des Zertifikats (von – bis)		
		subject			
		commonName	ICCSN der gSMC-KT	1	
		organizationalUnitName	Relevante Einheit des Kartenterminal-Herstellers	0-1	
		organizationName	Name des Kartenterminal-Herstellers	1	
		countryName	Herkunftsland des Kartenterminal-Herstellers	1	
		andere Attribute		0	
		subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
		extensions			**critical**
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Kartenterminals	1	FALSE
		KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	 1 1 1	**TRUE**
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Kartenterminal-Herstellers	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_smkt_aut>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}		0	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}		0	FALSE

			AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
			Admission {1 3 36 8 3 3}	professionItem = Beschreibung zu <oid_kt> gemäß [gemSpec_OID#GS-A_4446] professionOID = OID <oid_kt> gemäß [gemSpec_OID#GS-A_4446]	1 1	FALSE
			ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-serverAuth	1	FALSE
			andere Erweiterungen		0	
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	signature			Wert der Signatur		

5.6 gSMC-K – Konnektor

5.6.1 Definition und Zuweisung der Konnektoridentität

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

GS-A_4605 - Verwendung registrierter Daten für gSMC-K-Zertifikatsbeantragung
Der Konnektor-Hersteller MUSS sicherstellen, dass bei der Beantragung von X.509-Zertifikaten für Konnektoren für die Felder **`SubjectDN`** nur die Werte verwendet werden, die im Rahmen seiner Zulassung registriert sind.
[<=]

GS-A_4606 - Identischer ICCSN in allen Zertifikaten einer gSMC-K
Der Konnektor-Hersteller MUSS sicherstellen, dass bei der Beantragung der X.509-Zertifikate für die zu einer gSMC-K gehörenden Zertifikate der Wert ICCSN für das Feld **`commonName`** in allen drei zu einer gSMC-K gehörenden Zertifikaten identisch angeben wird.
[<=]

GS-A_4607 - Zuordnung Konnektorinstanz zu verbauter gSMC-K
Der Konnektorhersteller MUSS den Zusammenhang zwischen Konnektorinstanz sowie der darin verbauten gSMC-K dokumentieren und hierüber gegenüber der gematik jederzeit Auskunft geben können.
[<=]

5.6.2 Aufbau des SubjectDN

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

- **`commonName = [ICCSN der gSMC-K] + "-" + [ Kartenausgabedatum in der Form JJJJMMTT]`**

- `organizationName = [Name des Konnektor-Herstellers],`
- `countryName = [Herkunftsland des Konnektor-Herstellers]`

5.6.3 Statusprüfung von Konnektorzertifikaten

GS-A_4608 - Statusprüfung von Konnektorzertifikaten
Der TSP-X.509 nonQES MUSS für die von ihm ausgestellten X.509-Zertifikate des Konnektors eine Statusprüfung per OCSP gemäß Tabelle Tab_PKI_237 sowohl in der TI als auch im Internet vorsehen.**[**<=**]**

Tabelle 34: Tab_PKI_237 Statusprüfung von Konnektorzertifikaten

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

5.6.4 X.509 Zertifikatsprofile des Konnektors

5.6.4.1 C.NK.VPN – VPN-Authentisierung Netzkonnektor

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

GS-A_4609 - Umsetzung Zertifikatsprofil C.NK.VPN
Der TSP-X.509 nonQES MUSS C.NK.VPN gemäß Tab_PKI_242 umsetzen.
[<=**]**

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

Element			Inhalt	Kar.	
certificate			C.NK.VPN		
	tbsCertificate				
		version	2 (v3)		
		serialNumber	gemäß [RFC5280#4.1.2.2.]		
		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4360]		
		issuer	DN der ausstellenden CA		
		validity	Gültigkeit des Zertifikats (von – bis)		
		subject			

		commonName	<ICCSN der gSMC-K>-<Kartenausgabedatum in der Form JJJJMMTT >	1	
		organizationalUnitName	Relevante Einheit des Konnektor-Herstellers	0-1	
		organizationName	Name des Konnektor-Herstellers	1	
		streetAddress	Anschrift des Konnektor-Herstellers	0-1	
		postalCode	Postleitzahl der Anschrift des Konnektor-Herstellers	0-1	
		localityName	Stadt der Anschrift des Konnektor-Herstellers	0-1	
		stateOrProvinceName	Bundesland der Anschrift des Konnektor-Herstellers	0-1	
		countryName	Herkunftsland des Konnektor-Herstellers	1	
		andere Attribute		0	
	subjectPublicKeyInfo		Algorithmus gemäß [gemSpec_Krypt# GS-A_4360] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
	extensions				**critical**
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Konnektors	1	FALSE
		KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	 1 1 1	**TRUE**
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Konnektor-Herstellers	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_nk_vpn>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE

			Admission {1 3 36 8 3 3}	professionItem = Beschreibung zu <oid_nk> gemäß [gemSpec_OID#GS-A_4446] professionOID = OID <oid_nk> gemäß [gemSpec_OID#GS-A_4446]	1 1	FALSE
			ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth keyPurposeId = id-kp-serverAuth	1 1	FALSE
			andere Erweiterungen		0	
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4360]		
	signature			Wert der Signatur		

5.6.4.2 C.AK.AUT - Authentisierung Anwendungskonnektor

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

GS-A_4610 - Umsetzung Zertifikatsprofil C.AK.AUT
Der TSP-X.509 nonQES MUSS C.AK.AUT gemäß Tab_PKI_243 umsetzen.
[<=]

Tabelle 36: Tab_PKI_243 Zertifikatsprofil C.AK.AUT Authentisierung Anwendungskonnektor

Element				Inhalt	Kar.	
certificate				C.AK.AUT		
	tbsCertificate					
		version		2 (v3)		
		serialNumber		gemäß [RFC5280#4.1.2.2.]		
		signature		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
		issuer		DN der ausstellenden CA		
		validity		Gültigkeit des Zertifikats (von – bis)		
		subject				
			commonName	<ICCSN der gSMC-K>-< Kartenausgabedatum in der Form JJJJMMTT >	1	
			organizationalUnitName	Relevante Einheit des Konnektor-Herstellers	0-1	
			organizationName	Name des Konnektor-Herstellers	1	
			streetAddress	Anschrift des Konnektor-Herstellers	0-1	
			postalCode	Postleitzahl der Anschrift des Konnektor-Herstellers	0-1	

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

	signature	Wert der Signatur		

5.6.4.3 C.SAK.AUT - Authentisierung Signaturdienst

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

GS-A_4611 - Umsetzung Zertifikatsprofil C.SAK.AUT
Der TSP-X.509 nonQES MUSS C.SAK.AUT gemäß Tab_PKI_244 umsetzen.
[<=]

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

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

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

5.7 VPN-Zugangsdienst

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

5.7.1 Definition und Zuweisung der Zugangsdienstidentitäten

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

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

5.7.2 Aufbau des SubjectDN

Siehe Tab_PKI_245.

5.7.3 X.509-Zertifikatsprofile des Zugangsdienstes

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

GS-A_4613 - Umsetzung Zertifikatsprofil C.VPNK.VPN
Der TSP-X.509 nonQES MUSS C.VPNK.VPN gemäß Tab_PKI_245 umsetzen.
[<=]

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

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

		extensions			**critical**
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Konzentrators	1	FALSE
		KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	 1 1 1	**TRUE**
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Zugangsdienstanbieters dNSName = FQDN des Dienstes gemäß Zuweisung (Hinweis: siehe CommonName oben)	0-1 1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_vpnk_vpn>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}	URL für CRL-Statusdienst DN d. CRL-Ausstellers (f. indirekte CRL, s. RFC5280#4.2.1.13) reasons	1 1 0	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = Beschreibung zu <oid_vpnz_ti> gemäß [gemSpec_OID#GS-A_4446] professionOID = OID <oid_vpnz_ti> gemäß [gemSpec_OID#GS-A_4446]	1 1	FALSE
		ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth keyPurposeId = id-kp-serverAuth	1 1	FALSE
		andere Erweiterungen		0	
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4360]		
	signature		Wert der Signatur		

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

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

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

[<=]

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

Element	Inhalt	Kar.	
certificate	C.VPNK.VPN-SIS		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4360]		
issuer	DN der ausstellenden CA		
validity	Gültigkeit des Zertifikats (von – bis)		
subject			
commonName	FQDN des Zugangsdienstes gemäß Festlegung aus Dienstezulassung	1	
serialNumber	Zur Unterscheidung gleichartiger Instanzen	0-1	
organizationName	Name des Zugangsdienstanbieters	1	
countryName	Land der Anschrift des Zugangsdienstanbieters	1	
andere Attribute		0	
subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4360] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
extensions			**critical**
SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Konzentrators	1	FALSE
KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	 1 1 1	**TRUE**
SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Zugangsdienstanbieters dNSName = FQDN des Dienstes gemäß Zuweisung (Hinweis: siehe CommonName oben)	0-1 1	FALSE
BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo =	1 0-1	FALSE

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

5.8 ZD – Zentrale Dienste

5.8.1 Definition der Identität der Zentralen Dienste

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

5.8.2 Aufbau des SubjectDN

Siehe Tab_PKI_247.

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

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

5.8.3 X.509 Zertifikatsprofile der Zentralen Dienste

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

GS-A_4615 - Umsetzung Zertifikatsprofil C.ZD.TLS-S
Der TSP-X.509 nonQES MUSS C.ZD.TLS-S gemäß Tab_PKI_247 umsetzen.
[<=]

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

Element	Inhalt	Kar.	
certificate	C.ZD.TLS-S		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
issuer	DN der ausstellenden CA		
validity	Gültigkeit des Zertifikats (von – bis)		
subject			
commonName	FQDN des Dienstes gemäß Zuweisung	1	
serialNumber	bei Bedarf zur Unterscheidung gleichartiger Instanzen	0-1	
organizationName	Name des verantwortlichen Anbieters	1	
countryName	Land der Anschrift des verantwortlichen Anbieters	1	
andere Attribute		0	
subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
extensions			**critical**
SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Zentralen Dienstes	1	FALSE
KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	 1 1 1	**TRUE**
SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters dNSName = FQDN des Dienstes gemäß Zuweisung (Hinweis: siehe CommonName oben)	0-1 1	FALSE
BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo =	1 0-1	FALSE

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

5.9 FD – Fachanwendungsspezifische Dienste

5.9.1 Definition der Identität der Fachanwendungsspezifischen Dienste

Gemäß übergreifender Definition beinhaltet der Begriff „Fachanwendungsspezifischer Dienst" die Fachdienste und Intermediäre.

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

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

GS-A_4720 - Verwendung registrierter Werte für subjectDN
Anbieter von zentralen und fachanwendungsspezifischen Diensten in der TI MÜSSEN bei der Beantragung von X.509-Zertifikaten für den FQDN im **`SubjectDN`** ausschließlich einen FQDN aus dem zugehörigen Namensraum der TI unter Beachtung des zugewiesenen Domainnamen verwenden. Dabei MUSS der verwendete FQDN mit dem FQDN der zugewiesenen Komponente übereinstimmen.
[<=]

5.9.2 Aufbau des SubjectDN

Siehe Tab_PKI_249 oder Tab_PKI_250.

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

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

5.9.3 X.509 Zertifikatsprofile der Fachanwendungsspezifischen Dienste

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

GS-A_4617 - Umsetzung Zertifikatsprofil C.FD.TLS-C
Der TSP-X.509 nonQES MUSS C.FD.TLS-C gemäß Tab_PKI_249 umsetzen.
[<=]

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

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

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

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

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

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

[<=]

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

Element	Inhalt	Kar.	
certificate	C.FD.TLS-S		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
issuer	DN der ausstellenden CA		
validity	Gültigkeit des Zertifikats (von – bis)		
subject			
commonName	FQDN des Dienstes gemäß Zuweisung	1	
serialNumber	bei Bedarf zur Unterscheidung gleichartiger Instanzen	0-1	
organizationName	Name des verantwortlichen Anbieters	1	
countryName	Land der Anschrift des verantwortlichen Anbieters	1	
andere Attribute		0	
subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
extensions			**critical**
SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Fachanwendungsspezifischen Dienstes	1	FALSE
KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	 1 1 1	**TRUE**
SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters dNSName = FQDN des Dienstes gemäß Zuweisung (Hinweis: siehe CommonName oben)	0-1 1	FALSE
BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**

			CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_fd_tls_s>	1 0-1 1	FALSE
			CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
			AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
			Admission {1 3 36 8 3 3}	professionItem = Beschreibung der technischen Rolle gemäß [gemSpec_OID#GS-A_4446] professionOID = OID der technischen Rolle gemäß [gemSpec_OID#GS-A_4446]	1 1	FALSE
			ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-serverAuth	1	FALSE
			andere Erweiterungen		0	
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	signature			Wert der Signatur		

5.9.3.3 C.FD.SIG Signatur Fachdienst

A_15172 - Umsetzung Zertifikatsprofil C.FD.SIG

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

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

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

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

5.9.3.4 C.FD.AUT Authentisierung Fachdienst

A_15591 - Umsetzung Zertifikatsprofil C.FD.AUT
Der TSP-X.509 nonQES MUSS C.FD.AUT gemäß Tab_PKI_275 umsetzen.**[<=]**

Tabelle 44: Tab_PKI_275 C.FD.AUT Authentisierung fachanwendungsspezifische Dienste

Element	Inhalt	Kar.	
certificate	C.FD.AUT		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
issuer	DN der ausstellenden CA		
validity	Gültigkeit des Zertifikats (von – bis)		
subject			
commonName	Name des Dienstes gemäß Festlegung aus Dienstezulassung	1	
serialNumber	bei Bedarf zur Unterscheidung gleichartiger Instanzen	0-1	
organizationName	Name des verantwortlichen Anbieters	1	
countryName	Land der Anschrift des verantwortlichen Anbieters	1	
andere Attribute		0	
subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
extensions			**critical**
SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Fachanwendungsspezifischen Dienstes	1	FALSE
KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	 1 1 1	**TRUE**
SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	FALSE
BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**

			CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_fd_aut>	1 0-1 1	FALSE
			CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
			AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
			Admission {1 3 36 8 3 3}	professionItem = Beschreibung der technischen Rolle gemäß [gemSpec_OID#GS-A_4446] professionOID = OID der technischen Rolle gemäß [gemSpec_OID#GS-A_4446]	1 1	FALSE
			ExtendedKeyUsage {2 5 29 37}		0	FALSE
			andere Erweiterungen		0	
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	signature			Wert der Signatur		

5.9.3.5 C.FD.ENC Verschlüsselung Fachdienst

A_16213 - Umsetzung Zertifikatsprofil C.FD.ENC

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

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

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

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

	signature	Wert der Signatur		

5.10 CM – Clientmodul

5.10.1 Definition der Identität eines Clientmoduls

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

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

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

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

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

5.10.2 Aufbau des SubjectDN

Siehe Tab_PKI_267.

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

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

5.10.3 X.509 Zertifikatsprofil des Clientmoduls

5.10.3.1 C.CM.TLS-CS Clientmodul-Authentisierung

GS-A_5280 - Umsetzung Zertifikatsprofil C.CM.TLS-CS
Der TSP-X.509 nonQES MUSS C.CM.TLS-CS gemäß Tab_PKI_267 umsetzen.
[<=]

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

Element	Inhalt	Kar.	
certificate	C.CM.TLS-CS		
tbsCertificate			
version	2 (v3)		

		serialNumber	gemäß [RFC5280#4.1.2.2.]		
		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
		issuer	DN der ausstellenden CA		
		validity	Gültigkeit des Zertifikats (von – bis)		
		subject			
		commonName	keine Festlegung	1	
		serialNumber	bei Bedarf zur Unterscheidung gleichartiger Instanzen (z.B. Release-Nr.)	0-1	
		organizationName	Name des verantwortlichen Anbieters	1	
		countryName	Land der Anschrift des verantwortlichen Anbieters	1	
		andere Attribute		0	
		subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
		extensions			**critical**
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Clientmoduls	1	FALSE
		KeyUsage {2 5 29 15}	*Für Schlüsselgeneration RSA:* digitalSignature keyEncipherment *Für Schlüsselgeneration ECDSA:* digitalSignature	 1 1 1	**TRUE**
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_cm_tls_c>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	keine Festlegung	0-1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = Beschreibung der technischen Rolle gemäß [gemSpec_OID#GS-A_4446]	1 1	FALSE

				professionOID = OID der technischen Rolle gemäß [gemSpec_OID#GS-A_4446]		
			ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth keyPurposeId = id-kp-serverAuth	1 1	FALSE
			andere Erweiterungen		0	
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	signature			Wert der Signatur		

5.11 SGD-HSM – Schlüsselgenerierungsdienst-HSM

5.11.1 Beschreibung der Identität

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

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

5.11.2 X.509 Zertifikatsprofil der SGD-HSM

A_17844 - Umsetzung Zertifikatsprofil C.SGD-HSM.AUT
Der TSP-X.509 nonQES MUSS das Zertifikatsprofil C.SGD-HSM.AUT nach Tab_PKI_296 umsetzen.

[<=]

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

Element			Inhalt	Kar.	
certificate			C.SGD-HSM.AUT		
	tbsCertificate				
		version	2 (v3)		
		serialNumber	gemäß [RFC5280#4.1.2.2.]		

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

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

5.12 CA - Zertifikatsprofile

GS-A_4730 - Eindeutige Identifizierung der CA-Zertifikate
Der TSP-X.509 nonQES und TSP-X.509 QES MUSS bei der Beantragung von X.509-CA-Zertifikaten sicherstellen, dass der subjectDN die CA eindeutig innerhalb der TI identifiziert.
[<=]

GS-A_4731 - Attribute der CA-Zertifikate
Der TSP-X.509 nonQES und TSP-X.509 QES SOLL bei der Beantragung von X.509-CA-Zertifikaten nur die Attribute mit der Kardinalität 1 verwenden.
[<=]

GS-A_4732 - Extension der CA-Zertifikate
Der TSP-X.509 nonQES (eGK) und die gematik Root-CA SOLLEN bei der Erstellung eines Root- bzw. self-signed CA-Zertifikats die Extension AuthorityKeyIdentifier entfallen lassen.
[<=]

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

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

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

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

GS-A_4735 - Namenskonvention für CA-Zertifikate
Der TSP-X.509 nonQES und TSP-X.509 QES MUSS für jede von ihm betriebene CA die Namenskonventionen gemäß [GS-A_4588], [GS-A_4590] umsetzen sowie die Namensbildung im Feld commonName nach dem Schema <holder>.<usage>-CA<n> vornehmen.
[<=]

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

GS-A_4736 - Umsetzung Zentrale nonQES-Root-CA-Zertifikat
Die gematik-Root-CA MUSS die Namenskonvention und Attributsbelegung der Felder für folgende CA-Zertifikate umsetzen gemäß:
a) Tab_PKI_211 für gematik-Root-CA,

b) Tab_PKI_212 für i) Zentrale Aussteller-CA_nonQES, ii) Aussteller-CA_nonQES, iii) TSL-Signer-CA.**[<=]**

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

Element	**Inhalt**	**Kar.**	
certificate	C.GEM.RCA<n>		
tbsCertificate			
version	2 (v3)		
CertificateSerialNumber	gemäß [RFC5280#4.1.2.2]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
issuer	derselbe DN wie unter "subject" aufgeführt		
validity	Gültigkeit des Zertifikats (von - bis)		
subject			
commonName	GEM.RCA<n>	1	
serialNumber	Zur Unterscheidung gleichartiger Instanzen	0-1	
organizationalUnitName	Zentrale Root-CA der Telematikinfrastruktur	1	
organizationName	gematik GmbH	1	
countryName	DE	1	
andere Attribute		0	
subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4357] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
extensions			**critical**
SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels der Zentralen gematik Root-CA, für die dieses Zertifikat ausgestellt wird.	1	FALSE
KeyUsage {2 5 29 15}	keyCertSign crlSign	1 0-1	**TRUE**
SubjectAltNames {2 5 29 17}		0	FALSE
BasicConstraints {2 5 29 19}	ca = TRUE pathLength	1 0	**TRUE**
CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie)	1 1	FALSE
CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE

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

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

GS-A_4737 - Umsetzung nonQES-CA-Zertifikate
Der TSP-X.509 nonQES MUSS für die von ihm betriebenen CAs die Attributsbelegung der Felder gemäß Tab_PKI_212 und die Namenskonvention gemäß Tab_PKI_213 umsetzen.
[<=]

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

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

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

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

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

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

GS-A_4948 - Umsetzung QES-CA-Zertifikate
Der TSP-X.509 QES MUSS für die Zertifikate der von ihm betriebenen CAs die Attributsbelegung der Felder gemäß Tab_PKI_215 umsetzen.
[<=]

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

Element	Inhalt	Kar.	
certificate	C.<tsp>.HBA-qCA<n>		
tbsCertificate			
version	2 (v3)		
CertificateSerialNumber	gemäß [RFC5280#4.1.2.2]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4358]		
issuer	DN der ausstellenden CA		
validity	Gültigkeit des Zertifikats (von - bis)		
subject			
commonName	<tsp>.HBA-qCA <n> *)	1	
organizationalUnitName	Qualifizierter VDA der Telematikinfrastruktur	0-1	
organizationIdentifier	Vom VDA verwendeter organizationIdentifier gemäß [ETSI EN 319 412-2] und [X.520]	0-1	
organizationName	Name des VDA für QES	1	
countryName	DE	1	
andere Attribute		0	
subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4358] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
extensions			**critical**
SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels der CA, für die dieses Zertifikat ausgestellt wird	1	FALSE
KeyUsage {2 5 29 15}	keyCertSign crlSign	1 0-1	**TRUE**
SubjectAltNames {2 5 29 17}		0	FALSE
BasicConstraints {2 5 29 19}	ca = TRUE pathLength = 0	1 1	**TRUE**

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

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

5.13 OCSP – Statusauskunftsdienst

5.13.1 Definition der OCSP-Signer-Identität

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

GS-A_4738 - Eindeutige Identifizierung der OCSP-Signer-Zertifikate
Der TSP-X.509 nonQES und der Anbieter des TSL-Dienstes MÜSSEN bei der Beantragung von X.509-OCSP-Signer-Zertifikaten sicherstellen, dass der subjectDN das OCSP-Signer-Zertifikat eindeutig innerhalb der TI identifiziert.
[<=]

GS-A_4739 - Attribute der OCSP-Signer-Zertifikate
Der TSP-X.509 nonQES und der Anbieter des TSL-Dienstes SOLLEN bei der Beantragung von X.509-OCSP-Signer-Zertifikaten nur die Attribute mit der Kardinalität 1 verwenden.
[<=]

GS-A_5514 - Verwendung separater OCSP-Signer-Zertifikate
Ein TSP-X.509 nonQES, die gematik Root-CA und der Anbieter des TSL-Dienstes MÜSSEN für jede unterstützte Schlüsselgeneration (gemäß [gemSpec_Krypt#GS-A_4357]) jeweils ein separates OCSP-Signer-Zertifikat verwenden.
[<=]

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

5.13.2 Aufbau des SubjectDN

Siehe Tab_PKI_253.

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

5.13.3.1 C.GEM.OCSP OCSP-Signer-Zertifikat

GS-A_4741 - Umsetzung Zertifikatsprofil C.GEM.OCSP
Der TSP-X.509 nonQES, die gematik-Root-CA und der TSL-Dienst MÜSSEN C.GEM.OCSP gemäß Tab_PKI_253 umsetzen.
[<=]

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

Element	Inhalt	Kar.	
certificate	C.GEM.OCSP		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
issuer	DN der ausstellenden CA		
validity	Gültigkeit des Zertifikats (von – bis)		
subject			
commonName	Name des OCSP-Responders	1	
serialNumber	Zur Unterscheidung gleichartiger Instanzen	0-1	
organizationalUnitName	Name der Abteilung für den Betrieb des OCSP	0-1	

			organizationName	Name des OCSP-Dienstanbieters	1	
			countryName	Land der Anschrift des OCSP-Dienstanbieters	1	
			andere Attribute		0	
		subjectPublicKeyInfo		Algorithmus gemäß [gemSpec_Krypt#GS-A_4357] und individueller Wert des öffentlichen Schlüssels des Zertifikatsbesitzers		
		extensions				**critical**
			SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des OCSP-Signers	1	FALSE
			KeyUsage {2 5 29 15}	nonRepudiation	1	**TRUE**
			SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	FALSE
			BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
			CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie)	1 0-1	FALSE
			CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	0-1	FALSE
			AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
			ExtendedKeyUsage {2 5 29 37}	KeyPurposeId = id-kp-OCSPSigning	1	FALSE
			id-pkix-ocsp-nocheck {1.3.6.1.5.5.7.48.1.5}	OCSP-Nocheck = NULL	0-1	FALSE
			andere Erweiterungen		0	
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
	signature			Wert der Signatur		

5.14 CRL – Statusauskunftsdienst

GS-A_5066-01 - Indirekte CRL gemäß Standards
Der TSP-X.509 nonQES für Komponenten MUSS CRLs für X.509-Zertifikate als indirekte CRLs gemäß [RFC5280] und [X.509] unter Verwendung eines dedizierten CRL-Signers erzeugen.
[<=]

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

5.14.1 Definition der CRL-Signer-Identität

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

GS-A_4935 - Eindeutige Identifizierung der CRL-Signer-Zertifikate
Der TSP-X.509 nonQES MUSS bei der Beantragung von X.509-CRL-Signer-Zertifikaten sicherstellen, dass der subjectDN das CRL-Signer-Zertifikat eindeutig innerhalb der TI identifiziert.
[<=]

GS-A_4936 - Attribute der CRL-Signer-Zertifikate
Der TSP-X.509 nonQES SOLL bei der Beantragung von X.509-CRL-Signer-Zertifikaten nur die Attribute mit der Kardinalität 1 verwenden.
[<=]

GS-A_4937 - Ableitung des CRL-Signer-Zertifikates
Ein TSP-X.509 nonQES MUSS das CRL-Signer-Zertifikat der jeweiligen Schlüsselgeneration für die von ihm be-triebenen CRL-Dienste aus der VPNK-CA derselben Schlüsselgeneration beziehen.
[<=]

GS-A_5515 - Bezug separater CRL-Signer-Zertifikate
Ein TSP-X.509 nonQES, der CRL-Dienste betreibt, MUSS für jede unterstützte Schlüsselgeneration (gemäß [gemSpec_Krypt#GS-A_4357]) jeweils ein separates CRL-Signer-Zertifikat beziehen.
[<=]

5.14.2 Aufbau des SubjectDN

Siehe Tab_PKI_214.

5.14.3 X.509 Profil des CRL-Signer-Zertifikates

5.14.3.1 C.GEM.CRL CRL-Signaturzertifikat

GS-A_4939 - Umsetzung Zertifikatsprofil C.GEM.CRL
Der TSP-X.509 nonQES MUSS C.GEM.CRL gemäß Tab_PKI_214 umsetzen.
[<=]

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

Element	Inhalt	Kar.	
certificate	C.GEM.CRL		
tbsCertificate			
version	2 (v3)		

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

	signature	Wert der Signatur		

5.15 TSL - Zertifikatsprofile

5.15.1 Definition der TSL-Signer-Identität

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

GS-A_4742 - Eindeutige Identifizierung der TSL-Signer-Zertifikate
Der Anbieter des TSL-Dienstes MUSS bei der Beantragung von X.509-TSL-Signer-Zertifikaten sicherstellen, dass der subjectDN das TSL-Signer-Zertifikat eindeutig innerhalb der TI identifiziert.
[<=]

GS-A_4743 - Attribute der TSL-Signer-Zertifikate
Der Anbieter des TSL-Dienstes SOLL bei der Beantragung von X.509-TSL-Signer-Zertifikaten nur die Attribute mit der Kardinalität 1 verwenden.
[<=]

5.15.2 Aufbau des SubjectDN

Siehe Tab_PKI_252_01.

5.15.3 X.509 Zertifikatsprofil der TSL-Signer-CA

GS-A_4744 - Zentrale TSL-Signer-CA-Zertifikate
Der Anbieter des TSL-Dienstes MUSS für die von ihm betriebenen TSL-Signer-CAs die Attributsbelegung der Felder gemäß Tab_PKI_212 und die Namenskonvention für den TSL-Dienst gemäß Tab_PKI_213 umsetzen.
[<=]

A_17686 - TSL-Signer-CA Cross-Zertifikate (ECC-Migration)
Der TSL-Dienst MUSS für die TSL-Signer-CA der Schlüsselgeneration ECDSA beidseitige Cross-Zertifikate zu der aktiven TSL-Signer-CA der Schlüsselgeneration RSA bereitstellen und dabei die folgenden Punkte berücksichtigen:

- das bereits existierende Schlüsselmaterial (PublicKey) der TSL-Signer-CA (ECDSA) wird durch die TSL-Signer-CA (RSA) mit deren PrivateKey signiert und damit das Cross-Zertifikat mit dem Namen C.GEM.TSL-CA<Index der ECDSA-CA>-CROSS<Index der RSA-CA> erzeugt
- das bereits existierende Schlüsselmaterial (PublicKey) der TSL-Signer-CA (RSA) wird durch die TSL-Signer-CA (ESCDA) mit deren PrivateKey signiert und damit das Cross-Zertifikat mit dem Namen C.GEM.TSL-CA<Index der RSA-CA>-CROSS<Index der ECDSA-CA> erzeugt

[<=]

A_17687 - TSL-Signer-CA Cross-Zertifikate – Attributsbelegung (ECC-Migration)
Der TSL-Dienst MUSS für die zu erstellenden Cross-Zertifikate die Attributsbelegung der Felder gemäß Tab_PKI_212 umsetzen, wobei Abweichungen bei folgenden Elementen vorzunehmen sind:

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

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

[<=]

Beispiele für TSL-Signer-CA Cross-Zertifikate:

- C.GEM.TSL-CA1-CROSS3

  Erklärung: Das Cross-Zertifikat ist für TSL-Signer-CA1 (RSA Public Key) ausgestellt und von TSL-Signer-CA3 (ECDSA) signiert.
- C.GEM.TSL-CA3-CROSS1

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

5.15.4 TSL-Signer- Zertifikat

GS-A_4745-01 - Umsetzung Zertifikatsprofil C.TSL.SIG für TSL-Dienst
Der TSL-Dienst MUSS das TSL-Signer-Zertifikat C.TSL.SIG gemäß Tab_PKI_252_01 umsetzen.
[<=]

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

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

			organizationalUnitName	Name der Abteilung für den Betrieb des TSL-Dienstes	0-1	
			organizationName	gematik GmbH	1	
			countryName	DE	1	
			andere Attribute		0	
		subjectPublicKeyInfo		Algorithmus gemäß [gemSpec_Krypt#GS-A_4357] und individueller Wert des öffentlichen Schlüssels des Zertifikatsbesitzers		
		extensions				**critical**
			SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des TSL-Signers	1	FALSE
			KeyUsage {2 5 29 15}	nonRepudiation	1	**TRUE**
			SubjectAltNames {2 5 29 17}		0	FALSE
			BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
			CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_tsl_signer>	1	FALSE
			CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
			AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
			ExtendedKeyUsage {2 5 29 37}	KeyPurposeId = id-tsl-kptslSigning gemäß [ETSI_TS_102_231_v3.1.2#6.2]	1	FALSE
			andere Erweiterungen		0	
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
	signature			Wert der Signatur		

5.15.5 TSL-OCSP-Responder-Zertifikat

GS-A_4747 - Umsetzung Zertifikatsprofil C.GEM.OCSP für TSL-Dienst
Der TSL-Dienst MUSS für die OCSP-Prüfung des TSL-Signer-Zertifikats ein OCSP-Signer-Zertifikat C.GEM.OCSP gemäß Tab_PKI_253 umsetzen.

[<=]

GS-A_4918 - Ableitung des OCSP-Signer-Zertifikates für TSL-Dienst
Der TSL-Dienst MUSS das OCSP-Signer-Zertifikat der jeweiligen Schlüsselgeneration gemäß [RFC6960] von der TSL-Signer-CA derselben Schlüsselgeneration beziehen.**[<=]**

6 CV-Zertifikate

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

GS-A_4972 - Bezug des CV-Zertifikat
Ein Kartenherausgeber KANN das nicht-personenbezogene CV-Zertifikat nach entsprechender Registrierung vom TSP-CVC-CA beziehen.
[<=]

GS-A_4973 - Ausstellung aller CV-Zertifikate einer Karte durch gleiche CVC-Sub-CA
Der Kartenherausgeber MUSS sicherstellen, dass alle zu einer Chipkarte gehörenden CV-Zertifikate durch dieselbe CA der zweiten Ebene erzeugt werden.
[<=]

6.1 Festlegungen zur Abgrenzung

Grundsätzlich sind CV-Zertifikatsprofile zu unterscheiden für

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

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

GS-A_4974 - CV-Ausstattung von Smartcards der TI
Ein Kartenherausgeber, der Smartcards für Einsatzbereiche der TI herausgeben will, MUSS sicherstellen, dass die Karten über folgende CV-Ausstattung verfügen: (a) 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 (b) das CV-CA-Zertifikat der zweiten Ebene sowie (c) der öffentliche Schlüssel der CV-Root.
[<=]

6.2 Namensregeln und -formate

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

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

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

6.3 Rollen- und gerätebasierte Zugriffsprofile

6.3 Rollen und Profile

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

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

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

-

6.3.1 Rollenauthentisierung

GS-A_4620 - Zugriffsprofil einer eGK
Der Kartenherausgeber MUSS sicherstellen, dass das CV-Rollen-Zertifikat einer eGK als Zugriffsprofil CHAT.0 den Wert ´00 0000 0000 0000´ hat.

[<=]

GS-A_4621 - Zugriffsprofil von HBA und SM-B (SMC-B, HSM-B)
Der Kartenherausgeber MUSS sicherstellen, dass bei einem HBA bzw. einer SM-B das Zugriffsprofil in einem CV-Zertifikat der Rolle des Karteninhabers bzw. der Organisation gemäß Tabelle Tab_PKI_254 entspricht.
Eine Ausnahme hiervon ist die SM-B für Gesellschafterorganisationen, da sie keine CV-Rollenzertifikate erhält.
[<=]

A_16179 - Zugriffsprofil einer KTR-AdV
Der Kartenheraugeber für SM-B KTR-AdV MUSS sicherstellen, dass die CV-Rollen-Zertifkate für eine KTR-AdV jeweils das Zugriffsprofil CHAT.1 bzw. CHAT.0 gemäß [gemSpec_PKI#Tab_PKI_254] besitzen.
[<=]

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

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

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

Tabelle 53: Tab_PKI_254 Zugriffsprofile für eine Rollenauthentisierung

Profile / Akteure / Rollen und OID aus gemSpec_PKI					X.509 Admission Extension	
Zugriffs-profil	**Kartentyp**	**Beschreibung fachlicher Akteur**	**Fachliche Rolle**	**Qualifizierende Stelle**	**professionItem**	**OID-Referenz**
0						
CHAT.0	eGK	Versicherter	Versicherter	keine Qualifizierung	Versicherte/-r	oid_versicherter
CHAT.0	KTR-AdV	KTR-AdV	Versicherter	gesetzliche Krankenkasse	AdV-Umgebung bei Kostenträger	oid_adv_ktr
1						
CHAT.1	KTR-AdV	KTR-AdV	Versicherter	gesetzliche Krankenkasse	AdV-Umgebung bei Kostenträger	oid_adv_ktr
2						
CHAT.2A	HBA – Arzt	Arzt in einer Institution (z. B. eigene Praxis, Gemeinschaftspraxis, Krankenhaus). Auch der ärztliche Psychotherapeut fällt unter diese Kategorie.	Arzt	BAEK	Ärztin/Arzt	oid_arzt
CHAT.2ZA	HBA – Zahnarzt	Zahnarzt in einer Institution	Zahnarzt	BZÄK	Zahnärztin/Zahnarzt	oid_zahnarzt

CHAT .2A	(H)BA für Mitarb eiter-(innen) in Arztpr axis, oder Kranke n-haus	Mitarbeiter medizinische Institution (z. B. in Arztpraxis, Krankenhaus). Der „Mitarbeiter medizinische Institution" verkörpert gegenüber der TI die Institution des Arztes	Nicht definier t	Nicht definiert	Nicht definiert	Nicht definiert
CHAT .2ZA	(H)BA für Mitarb eiter-(innen) in Zahna rzt-praxis	Mitarbeiter medizinische Institution (z. B. in Zahnarztprax is). Der „Mitarbeiter medizinische Institution" verkörpert gegenüber der TI die Institution des Zahnarztes	Nicht definier t	Nicht definiert	Nicht definiert	Nicht definiert
CHAT .2A	SMC-B	Mitarbeiter medizinische Institution Arztpraxis (inkl. Praxis ärztlicher Psychotherap eut) mit Autorisierung und Protokollieru ng gemäß § 291a Abs. 5 Satz 4 SGB V. Der „Mitarbeiter medizinische Institution" verkörpert gegenüber	Mitarbe iter Arzt	KV	Betriebsstätte Arzt	oid_praxis_arzt

		der TI die Institution des Arztes.				
CHAT .2A	SMC-B	Behörden des Öffentlichen Gesundheitsdienstes sowie Institutionen der Fachärzte für Arbeitsmedizin, Betriebsärzte und Institutionen der Vorsorge- oder Rehabilitation nach SGB V § 107 Absatz 2 oder der medizinischen Rehabilitation nach SGB VI oder der Heilbehandlung einschließlich medizinischer Rehabilitation nach SGB VII	Mitarbeiter weitere Ärztliche Institution	Nicht definiert	Betriebsstätte Arbeitsmedizin Betriebsstätte Öffentlicher Gesundheitsdienst Betriebsstätte Vorsorge- und Rehabilitation	oid_arbeitsmedizin oid_gesundheitsdienst oid_vorsorge_reha
CHAT .2ZA	SMC-B	Mitarbeiter medizinische Institution Zahnarztpraxis mit Autorisierung und Protokollierung gemäß § 291a Abs. 5 Satz 4 SGB V. Der „Mitarbeiter medizinische Institution" verkörpert gegenüber der TI die Institution des Zahnarztes.	Mitarbeiter Zahnarzt	KZBV	Zahnarztpraxis	oid_zahnarztpraxis

CHAT .2A	SMC-B	Mitarbeiter medizinische Institution Krankenhaus mit Autorisierung und Protokollierung gemäß § 291a Abs. 5 Satz 4 SGB V. Der „Mitarbeiter medizinische Institution" verkörpert gegenüber der TI die Institution des Arztes.	Mitarbeiter Krankenhaus	DKTIG	Krankenhaus	oid_krankenhaus
3						
CHAT .3	HBA – Apotheker	Apotheker in einer öffentlichen Apotheke oder einer Krankenhaus apotheke, jeweils mit Sitz in Deutschland.	Apotheker	BAK	Apotheker/in	oid_apotheker
CHAT .3	(H)BA für Mitarbeiter (-innen) der Apotheke	Mitarbeiter Apotheke als berufsmäßiger Gehilfe oder Person, die zur Vorbereitung auf den Beruf tätig ist, gemäß § 291a Abs. 4 [SGB V]. Der „Mitarbeiter Apotheke" verkörpert gegenüber der TI die Institution des	Apotheker	BAK	Apotheker-assistent/in Pharmazie-ingenieur/in Apotheken-assistent/-in	oid_apotheker assisten oid_pharmazie ingenieur oid_apotheken assistent

		Apothekers.				
CHAT .3	SMC–B	Mitarbeiter Apotheke mit Autorisierung und Protokollierung gemäß § 291a Abs.5 Satz 4 SGB V. Der „Mitarbeiter Apotheke" verkörpert gegenüber der TI die Institution des Apothekers.	Mitarbeiter Apotheke	Für den jeweiligen Betriebs-erlaubnis-inhaber zuständige Apotheker-kammer	Öffentliche Apotheke	oid_öffentliche_apotheke
4						
CHAT .4	HBA – Psycho the-rapeut	Psychotherapeut, Psychologischer Psychotherapeut, Kinder- und Jugendlichen-psychotherapeut	Psychothe-rapeut	BPTK	Psychothe-rapeut/ in Psycholo-gische/r Psychothe-rapeut/ in Kinder- und Jugendlichen-psychothe-rapeut/-in	oid_psychotherapeut oid_ps_psychothe rapeut oid_kuj_psychothe rapeut
CHAT .4	SMC–B	Institutionskarte eines Psychotherapeuten. Der mit der Karte mögliche Zugriff auf die medizinischen Anwendungen der eGK ist ausschließlich dem psychologischen Psychotherap	Mitarbeiter Psychothe-rapeut	KV	Betriebsstätte Psychothe-rapeut	oid_praxis_psychothe rapeut

		euten und dem Kinder- und Jugendlichen-psychotherapeuten selbst gestattet und nicht seinen berufsmäßigen Gehilfen.				
5						
CHAT.5	(H)BA sonstige Leistungs-erbringer	Weitere Heilberufler mit BA	Sonstige Leistungs-erbringer	Nicht definiert	Altenpfleger/-in Pflegefachfrauen und Pflegefachmänner Hebamme Physiotherapeut/-in Augenoptiker/-in und Optometrist/-in Hörakustiker/-in Orthopädieschuhmacher/-in Betriebsstätte Orthopädietechniker Zahntechniker/-in Gesundheits- und Krankenpfleger/-in, Gesundheits- und Kinderkrankenpfleger/-in	oid_altenpfleger oid_pflegefachkraft oid_hebamme oid_physiotherapeut oid_augenoptiker oid_hoerakustiker oid_orthopaedieschuhmacher oid_orthopaediestechniker oid_zahntechniker oid_pfleger
CHAT.5	SMC-B sonstige Leistu	Institution eines weiteren Heilberuflers	Institution Sonstige	Nicht definiert	Betriebsstätte Gesundheits-, Kranken- und Altenpflege	oid_institution_pflege

	ngs-erbringer	mit BA	Leistungs-erbringer		Betriebsstätte Geburtshilfe Betriebsstätte Physiotherapie Betriebsstätte Augenoptiker Betriebsstätte Hörakustiker Betriebsstätte Orthopädieschuhmacher Betriebsstätte Orthopädietechniker Betriebsstätte Zahntechniker Rettungsleitstelle Betriebsstätte Sanitätsdienst Bundeswehr Betriebsstätte Öffentlicher Gesundheitsdienst Betriebsstätte Arbeitsmedizin Betriebsstätte Vorsorge- und Rehabilitation	oid_geburtshilfe oid_praxis_physiotherapeut oid_institution_augenoptiker oid_institution_hoerakustiker oid_institution_orthopaedieschuhmacher oid_institution_orthopaedietechniker oid_institution_zahntechniker oid_rettungsleitstellen oid_sanitaetsdienst_bundeswehr oid_gesundheitsdien oid_arbeitsmedizin oid_vorsorge_reha
6						
CHA.6	SMC	Kein fachlicher Akteur - wird nicht verwendet	Nicht definiert	Nicht definiert	Nicht definiert	Nicht definiert
7						

CHAT .7	(H)BA	Rettungsassistent Bei den Akteuren handelt es sich um „Angehörige eines anderen Heilberufs, die für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung“ (§ 291a Abs. 4 Satz 1 Nr. 2e) absolviert haben.	Anderer Heilberuf	Nicht definiert	Rettungs-assistent/-in Notfall-sanitäter/-in	oid_rettungsassistent oid_notfallsanitaeter
CHAT .7	SMC-B	Mobile Einrichtung Rettungsdienst	Nicht definiert	Nicht definiert	Betriebsstätte Mobile Einrichtung Rettungsdienst	oid_mobile_einrichtung_rettungsdienst
8						
CHAT .8	SMC-B (ohne Zugriff auf med. Daten)	Mitarbeiter von Gesundheits-einrichtungen ohne eigenen HBA oder BA	Mitarbeiter Medizinische Institution	Nicht definiert	Nicht definiert	Nicht definiert
CHAT .8		Mitarbeiter von Krankenkassen	Mitarbeiter Kostenträger	GKV-SV	Betriebsstätte Kostenträger	oid_kostentraeger
CHAT .8		Verifikationskarten Kostenträger	Mitarbeiter Kostenträger	GKV-SV	n.a. (Karte enthält keine X.509)	n.a. (Karte enthält keine X.509)
9						

CHAT .9	SMC-B (mit Zugriff auf med. Daten)	a) Mitarbeiter von Gesundheits-einrichtungen ohne eigenen HBA oder BA	a) Mitarbeiter Medizinische Institution	Nicht definiert	Nicht definiert	Nicht definiert
CHAT .9		b) ohne zugeordneten Akteur, sichere Einsatzumgebung für Versicherten	b) Versicherter	Nicht definiert	Nicht definiert	Nicht definiert

6.3.2 Authentisierung einer Funktionseinheit

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

Tabelle 54: Tab_PKI_255 Zugriffsprofile G2 für eine Authentisierung einer Funktionseinheit

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

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

GS-A_4622 - Zugriffsprofil einer gSMC-K
Der Kartenherausgeber MUSS sicherstellen, dass das CV-Gerätezertifikat einer gSMC-K als Flagliste den Wert ’0000 0000 0001’ hat (Zugriffsprofil 51 für G2 gemäß Tab_PKI_918).
[<=]

GS-A_5126 - Zugriffsprofil einer gSMC-KT
Der Kartenherausgeber MUSS sicherstellen, dass das CV-Gerätezertifikat einer gSMC-KT als Flagliste den Wert ’00 0000 0000 0002’ hat (Zugriffsprofil 54 für G2 gemäß Tab_PKI_918).
[<=]

GS-A_4623 - Zugriffsprofil eines HBA
Der Kartenherausgeber MUSS sicherstellen, dass das CV-Gerätezertifikat eines HBA als Flagliste den Wert ’00 0000 0000 000C’ hat (Zugriffsprofil 53 für G2 gemäß Tab_PKI_918).
[<=]

GS-A_4624 - Zugriffsprofil einer SM-B
Der Kartenherausgeber MUSS sicherstellen, dass das CV-Gerätezertifikat einer SM-B als Flagliste den Wert ’00 0000 0000 0004’ hat (Zugriffsprofil 55 für G2 gemäß Tab_PKI_918).
[<=]

GS-A_5335 - Zugriffsprofil einer gSMC-K für Administrationszwecke
Der Kartenherausgeber MUSS sicherstellen, dass die Flagliste des CV-Zertifikats für die Authentisierung einer gSMC-K gegenüber einem Aktualisierungssystem den Wert ’00 0000 0000 0000’ hat (Zugriffsprofil 0 für G2 gemäß Tab_PKI_918).
[<=]

6.4 CV-Zertifikatsprofile der Generation 2

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

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

6.4.1 Berechtigung einer CVC-CA zur Zertifikatserstellung

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

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

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

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

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

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

GS-A_5213 - CA-Flaglist für CVC-CA eines Profiltyps
Die CVC-Root-CA MUSS bei der Generierung eines CA-Zertifikates
(a) für eine CVC-CA, welche ausschließlich zur Ausstellung von EE-Zertifikaten eines bestimmten Zugriffsprofils (oder eines spezifischen Tupels aus Geräte- und Rollen-Zugriffsprofilen) aus Tab_PKI_919, genau die zugeordnete Flaglist aus der Spalte Sub-CA in das CA-Zertifikat einbringen.
(b) Für eine CVC-CA mit kombinierten Zugriffsprofilen ist die Veroderung der zugehörigen Flaglisten aus Tab_PKI_919 zulässig für die Zugriffsprofile
(b.1) aller HBA- und SMC-B sowie
(b.2) aller gSMC-K und gSMC-KT.
[<=**]**

6.4.2 Aufbau und Bestandteile der CV-Zertifikate der Generation 2

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

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

Berechtigungssteuerung über die Flagliste im Feld CHAT

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

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

6.4.3 Zertifikatsprofil eines CV-Zertifikates für ELC-Schlüssel

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

6.4.3.1 Certificate Profile Identifier (CPI)

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

GS-A_4986 - Datenobjekt für das Feld Card Profile Identifier in G2
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS den Wert für den CPI in das Datenobjekt ´5F29´ einstellen.
[<=]

GS-A_4987 - Wert des Card Profile Identifier in G2
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS als Wert für den CPI ´70´ eintragen.
[<=]

6.4.3.2 Certification Authority Reference (CAR)

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

Tabelle 55: Tab_PKI_266 Aufbau CAR für Karten der Generation 2

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

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

GS-A_4988 - Datenobjekt für das Feld Certificate Authority Reference in G2
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS den Wert für die CAR in das Datenobjekt ´42´ einstellen
[<=]

GS-A_4989 - Länge der Certificate Authority Reference in G2

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

GS-A_4990 - Verwendung des Feldes Certificate Authority Reference in G2
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS das Feld CAR weiter unterteilen in die Konkatenation der Datenelemente CA Name, Service-Indikator, CA-spezifische Information, Algorithmenreferenz und Datum sowie dabei die Festlegungen bzgl. Länge und zugelassener Werte gemäß Tab_PKI_266 berücksichtigen.
[<=]

GS-A_4991 - Zuordnung von CAR zu Schlüsselpaar des Herausgebers für G2
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS sicherstellen, dass die Zuordnung zwischen Certificate Authority Reference (CAR) und Schlüsselpaar eindeutig ist.
[<=]

6.4.3.3 Öffentlicher Schlüssel

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

GS-A_4992 - Datenobjekt für den öffentlichen Schlüssel
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS den öffentlichen Schlüssel in das Datenobjekt ´7F49´ einstellen.
[<=]

GS-A_4993 - Aufbau eines öffentlichen Schlüssel
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS in das Wertfeld des Datenobjekt ´7F49´ des öffentlichen Schlüssels genau zwei Datenobjekte eintragen. Dabei MÜSSEN das erste Datenobjekt ein Objektidentifier OIDPuK gemäß Tabelle Tab_PKI_901 und das zweite Datenobjekt ein Datenobjekt DO´86´ mit dem öffentlichen Punkt Q, dessen Wertfeld sich aus Tabelle Tab_PKI_902 ergibt, sein.
[<=]

Tabelle 56: Tab_PKI_901 Objektidentifier des öffentlichen Schlüssels eines CV-Zertifikats der Generation 2

Verwendungszweck des CV-Zertifikats	Domain-parameter	Objektidentifier
Transport des öffentlichen Signaturprüfschlüssels einer CA	brainpoolP256r1	OID_{PuK} = ´06-L_{06}-ecdsa-with-SHA256´ OID_{Hex} = ´06 08 2A8648CE3D040302´ OID_{Dez} = ´1.2.840.10045.4.3.2´
	brainpoolP384r1	OID_{PuK} = ´06-L_{06}-ecdsa-with-SHA384´ OID_{Hex} = ´06 08 2A8648CE3D040303´ OID_{Dez} = ´1.2.840.10045.4.3.3´
	brainpoolP512r1	OID_{PuK} = ´06-L_{06}-ecdsa-with-SHA512´ OID_{Hex} = ´06 08 2A8648CE3D040304´ OID_{Dez} = ´1.2.840.10045.4.3.4´

Transport eines öffentlichen Authentisierungsschlüssels	brainpoolP256r1	OID_{PuK} = ´06-L_{06}-authS_gemSpec-COS-G2_ecc-with-sha256´ OID_{Hex} = ´06 06 2B2403050301´ OID_{Dez} = ´1.3.36.3.5.3.1´
	brainpoolP384r1	OID_{PuK} = ´06-L_{06}-authS_gemSpec-COS-G2_ecc-with-sha384´ OID_{Hex} = ´06 06 2B2403050302´ OID_{Dez} = ´1.3.36.3.5.3.2´
	brainpoolP512r1	OID_{PuK} = ´06-L_{06}-authS_gemSpec-COS-G2_ecc-with-sha512´ OID_{Hex} = ´06 06 2B2403050303´ OID_{Dez} = ´1.3.36.3.5.3.3´

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

Domainparameter	Codierung eines öffentlichen Punktes *Q* in DO´86´
brainpoolP256r1	DO´86´= ´86 – 41 – P2OS(*Q*)´
brainpoolP384r1	DO´86´= ´86 – 61 – P2OS(*Q*)´
brainpoolP512r1	DO´86´= ´86 – 8181 – P2OS(*Q*)´

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

6.4.3.4 Certificate Holder Reference (CHR)

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

GS-A_4994 - Datenobjekt für die Certificate Holder Reference
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS die Certificate Holder Reference in das Datenobjekt ´5F20´ einstellen.
[<=]

GS-A_4995 - Wertfeld der Certificate Holder Reference
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS in das Wertfeld der Certificate Holder Reference eine Schlüsselreferenz zum öffentlichen Schlüssel gemäß [GS-A_4629], bei Ausgabe des CV-Zertifikats durch die CVC-Root-CA, bzw. gemäß [GS-A_4630], bei Ausgabe des CV-Zertifikats durch die CVC-CA, in das CV-Zertifikat der Generation 2 einstellen.
[<=]

GS-A_4629 - CHR des CV-Zertifikats einer CVC-CA
Die CVC-Root-CA MUSS als Wert für die CHR gemäß Tab_PKI_258 die CAR der CVC-CA zu dem Schlüsselpaar eintragen, für den das CV-Zertifikat erzeugt wird.
[<=]

GS-A_4630 - CHR des CV-Zertifikats einer Chipkarte
Der TSP-CVC MUSS als Wert für die CHR gemäß Tab_PKI_258 ein Datum eintragen, das aus der Konkatenation einer zwei Byte langen, innerhalb der Chipkarte eindeutigen Schlüsselidentifikation und der 10 Byte langen ICCSN als weltweit eindeutigen Identifier

der Chipkarte besteht.
[<=]

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

Tabelle 58: Tab_PKI_258 Aufbau CHR

CV-Zertifikat für	Länge CHR	Inhalt	
CVC-CA	8 Bytes siehe Kap. 6.4.3.2	CAR zu dem Schlüsselpaar siehe Kap. 6.4.3.2	
Chipkarte	12 Bytes	'xx xx' || ICCSN der Chipkarte	
	Zertifikat	CHR	Anforderung für CHR
eGK	C.eGK.AUT_CVC.E256	'00 09' || ICCSN	Card-G2-A_2363
HBA	C.HPC.AUTR_CVC.E256	'00 06' || ICCSN	Card-G2-A_3386
	C.HPC.AUTD_SUK_CVC.E256	'00 09' || ICCSN	Card-G2-A_3387
SMC-B	C.SMC.AUTR_CVC.E256	'00 06' || ICCSN	Card-G2-A_3389
	C.SMC.AUTD__RPE_CVC.E256	'00 09' || ICCSN	Card-G2-A_3390
	C.SMC.AUT_CVC.E256	'00 05' || ICCSN	Card-G2-A_3328
gSMC-K	C.SMC.AUT_CVC.E384	'00 06' || ICCSN	Card-G2-A_3331
	C.SAK.AUTD_CVC.E256	'00 0A' || ICCSN	Card-G2-A_2638
	C.SAK.AUTD_CVC.E384	'00 0F' || ICCSN	Card-G2-A_2640

	C.SMC.AUTD_RPS_CVC.E256	'00 0A' || ICCSN	Card-G2-A_2500
gSMC-KT	C:SMS.AUTD_RPS_CVC.E384	'00 0F' || ICCSN	Card-G2-A_2502
	C.KTRADV.AUTR_CVC.E256	'00 05' || ICCSN	-
KTR-AdV			

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

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

6.4.3.5 Certificate Holder Authorization Template (CHAT)

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

GS-A_4996 - Wertfeld des Certificate Holder Authorization Templates
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS das Certificate Holder Authorization Template in das Datenobjekt ´7F4C´ einstellen.
[<=]

GS-A_4997 - Aufbau der Certificate Holder Authorization Templates
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS in das Wertfeld des Datenobjekt ´7F4C´ genau zwei Datenobjekte eintragen. Dabei MUSS das zweite Datenobjekt ein Datenobjekt DO´53´ gemäß Tabelle Tab_PKI_910 (bei Anwendung von oid_cvc_fl_ti) oder Tab_PKI_911 (bei Anwendung von oid_cvc_fl_cms) sein und das erste Datenobjekt einen Objektidentifier OIDflags gemäß Tabelle Tab_PKI_904 enthalten, der angibt, wie die Flags im zweiten Datenobjekt zu interpretieren sind. Die Umsetzung eines bestimmten Berechtigungsprofils MUSS durch die Kombination der Einzelflags gemäß TAB_PKI_918 erfolgen.
[<=]

Tabelle 59: Tab_PKI_904 Mögliche Objektidentifier OID_{flags} in Certificate Holder Authorization Templates

OID_{flags}
OID_{flags} = ´06-L_{06}-oid_cvc_fl_ti
OID_{flags} = ´06-L_{06}- oid_cvc_fl_cms

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

6.4.3.6 Certificate Effective Date (CED)

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

GS-A_4998 - Datenobjekt des Certificate Effective Date
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS das Certificate Effective Date in das Datenobjekt ´5F25´ einstellen.
[<=]

GS-A_4999 - Länge des Certificate Effective Date
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS für das Certificate Effective Date ein Wertfeld der Länge sechs Oktett einstellen.
[<=]

GS-A_5000 - Format des Certificate Effective Date
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS ein Datum in der Form YYMMDD in unkomprimierter BCD Form in das Wertfeld des Certificate Effective Date eintragen.
[<=]

6.4.3.7 Certificate Expiration Date (CXD)

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

GS-A_5001 - Datenobjekt des Certificate Expiration Date
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS das Certificate Expiration Date in das Datenobjekt ´5F24´ einstellen.
[<=]

GS-A_5002 - Länge des Certificate Expiration Date
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS für das Certificate Expiration Date ein Wertfeld der Länge sechs Oktett einstellen.
[<=]

GS-A_5003 - Format des Certificate Expiration Date
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS ein Datum in der Form YYMMDD in unkomprimierter BCD Form in das Wertfeld des Certificate Expiration Date eintragen.
[<=]

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

GS-A_5004 - Tag der zu signierenden Nachricht M eines CV-Zertifikates
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS die zu signierende Nachricht des CV-Zertifikats in das Datenobjekt ´7F4E´ einstellen.
[<=]

GS-A_5005 - Datenstruktur der zu signierenden Nachricht M eines CV-Zertifikates
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS die zu signierende Nachricht M des CV-Zertifikats gemäß Tabelle Tab_PKI_905 bilden.
[<=]

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

M = DO´7F4E´
DO´7F4E´ = ´7F4E´-L7F4E-(DO´5F29´ || DO´42´ || DO´7F49´ || DO´5F20´ || DO´7F4C´ || DO´5F25´ || DO´5F24´)

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

GS-A_5006 - Signatur des Zertifikatsdatenobjekts
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS die Signatur der Nachricht *M* des CV-Zertifikates in Abhängigkeit vom Domainparameter des privaten Signaturschlüssels *PrK* des Herausgebers gemäß Tabelle Tab_PKI_906 erzeugen.
[<=]

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

Domainparameter des privaten Schlüssels *PrK*	**Signaturformat**
brainpoolP256r1	(*R, S*) = ECDSA(*PrK*, SHA_256(*M*)) im Format ecdsa-plain-SHA256 gemäß BSI-TR-03111#5.2.1.1
brainpoolP384r1	(*R, S*) = ECDSA(*PrK*, SHA_384(*M*)) im Format ecdsa-plain-SHA384 gemäß BSI-TR-03111#5.2.1.1
brainpoolP512r1	(*R, S*) = ECDSA(*PrK*, SHA_512(*M*)) im Format ecdsa-plain-SHA512 gemäß BSI-TR-03111#5.2.1.1

GS-A_5007 - Tag eines Zertifikatsdatenobjekts
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS die Inhalte des Zertifikatsdatenobjekts in das Datenobjekt ´7F21´ einstellen.
[<=]

GS-A_5008 - Aufbau eines Zertifikatsdatenobjekts
Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS das CV-Zertifikat als zusammengesetztes Datenobjekt gemäß Tabelle Tab_PKI_907 erzeugen. Er MUSS dabei sicherstellen, dass das zusammengesetzte Datenelement genau die beiden primitiven Datenobjekte in der dargestellten Reihenfolge enthält.
[<=]

Tabelle 62: Tab_PKI_907 Struktur und Inhalt eines CV-Zertifikat

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

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

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

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

Tabelle 63: Tab_PKI_912 CA CV-Zertifikate für 256 bit ELC-Schlüssel, insgesamt 220 Oktett

Tag	L	Wert					
´7F21´	´81D8´	CV–Zertifikat					
		Tag	L	Wert			
		´7F4E´	´8191´	Nachricht *M*			
				Tag	L	Wert	
				´5F29´	´01´	CPI = ´70´	
				´42´	´08´	CAR	
				´7F49´	´4D´	öffentlicher Schlüssel	
						Tag	L	Wert
						´06	´08´	´2A8648CE3D040302´
						´86´	´41´	P2OS(Q, 32)
				´5F20´	´08´	CHR	
				´7F4C´	´13´	CHAT	
						Tag	L	Wert
						´06´	´08´	OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}
						´53´	´07´	´XX...XX´, Flagliste

			´5F25´	´06´	CED
			´5F24´	´06´	CXD
	´5F37´	´40´	Signatur = *R* || *S*		

Tabelle 64: Tab_PKI_913 CA CV-Zertifikate für 384 bit ELC-Schlüssel, insgesamt 285 Oktett

Tag	L	Wert						
´7F21´	´820118´	CV–Zertifikat						
		Tag	**L**	**Wert**				
		´7F4E´	´81B1´	Nachricht *M*				
				Tag	**L**	**Wert**		
				´5F29´	´01´	CPI = ´70´		
				´42´	´08´	CAR		
				´7F49´	´6D´	öffentlicher Schlüssel		
						Tag	**L**	**Wert**
						´06	´08´	´2A8648CE3D040303´
						´86´	´61´	P2OS(Q, 48)
				´5F20´	´08´	CHR		
				´7F4C´	´13´	CHAT		
						Tag	**L**	**Wert**
						´06´	´08´	OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}
						´53´	´07´	´XX...XX´, Flagliste
				´5F25´	´06´	CED		
				´5F24´	´06´	CXD		
		´5F37´	´60´	Signatur = *R* || *S*				

Tabelle 65: Tab_PKI_914 CA CV-Zertifikate für 512 bit ELC-Schlüssel, insgesamt 352 Oktett

Tag	L	Wert		
´7F21´	´82015B´	CV–Zertifikat		
		Tag	**L**	**Wert**
		´7F4E´	´81D3´	Nachricht *M*
			Tag	**L**	**Wert**

		´5F29´	´01´	CPI = ´70´			
		´42´	´08´	CAR			
		´7F49´	´818E´	öffentlicher Schlüssel			
				Tag	**L**	**Wert**	
				´06´	´08´	´2A8648CE3D040304´	
				´86´	´8181´	P2OS(Q, 64)	
		´5F20´	´08´	CHR			
		´7F4C´	´13´	CHAT			
				Tag	**L**	**Wert**	
				´06´	´08´	OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}	
				´53´	´07´	´XX...XX´, Flagliste	
		´5F25´	´06´	CED			
		´5F24´	´06´	CXD			
	´5F37´	´8180´	Signatur = *R* || *S*				

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

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

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

Tag	**L**	**Wert**				
´7F21´	*	CV–Zertifikat				
		Tag	**L**	**Wert**		
		´7F4E´	*	Nachricht *M*		
				Tag	**L**	**Wert**
				´5F29´	´01´	CPI = ´70´
				´42´	´08´	CAR
				´7F49´	*	öffentlicher Schlüssel
					Tag	**L**	**Wert**

				´06	´08´	*
				´86´	*	*
			´5F20´	´08´	CHR	
			´7F4C´	´13´	CHAT	
				Tag	**L**	**Wert**
				´06´	´08´	OID = oid_cvc_fl_ti
				´53´	´07´	´FF FFFF FFFF FFFF´
			´5F25´	´06´	CED	
			´5F24´	´06´	CXD	
		´5F37´	*	Signatur = *R* || *S*		

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

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

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

Tag	**L**	**Wert**				
´7F21´	´81DA´	CV–Zertifikat				
		Tag	**L**	**Wert**		
		´7F4E´	´8193´	Nachricht *M*		
				Tag	**L**	**Wert**
				´5F29´	´01´	CPI = ´70´
				´42´	´08´	CAR
				´7F49´	´4B´	öffentlicher Schlüssel
					Tag	**L**	**Wert**
					´06	´06´	´2B2403050301´
					´86´	´41´	P2OS(Q, 32)
				´5F20´	´0C´	CHR	
				´7F4C´	´13´	CHAT	
					Tag	**L**	**Wert**
					´06´	´08´	OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}
					´53´	´07´	´XX...XX´, Flagliste
				´5F25´	´06´	CED	
				´5F24´	´06´	CXD	
		´5F37´	´40´	Signatur = *R* || *S*		

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

Tag	L	Wert						
´7F21´	´82011A´	CV–Zertifikat						
		Tag	**L**	**Wert**				
		´7F4E´	´81B3´	Nachricht *M*				
				Tag	**L**	**Wert**		
				´5F29´	´01´	CPI = ´70´		
				´42´	´08´	CAR		
				´7F49´	´6B´	öffentlicher Schlüssel		
						Tag	**L**	**Wert**
						´06	´06´	´2B2403050302´
						´86´	´61´	P2OS(Q, 48)
				´5F20´	´0C´	CHR		
				´7F4C´	´13´	CHAT		
						Tag	**L**	**Wert**
						´06´	´08´	OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}
						´53´	´07´	´XX...XX´, Flagliste
				´5F25´	´06´	CED		
				´5F24´	´06´	CXD		
		´5F37´	´60´	Signatur = *R* || *S*				

Tabelle 69: Tab_PKI_917 Endnutzer-CV-Zertifikate für 512 bit ELC-Schlüssel, insgesamt 354 Oktett

Tag	L	Wert			
´7F21´	´82015D´	CV–Zertifikat			
		Tag	**L**	**Wert**	
		´7F4E´	´81D5´	Nachricht *M*	
			Tag	**L**	**Wert**
			´5F29´	´01´	CPI = ´70´
			´42´	´08´	CAR
			´7F49´	´818C´	öffentlicher Schlüssel

					Tag	**L**	**Wert**
					´06	´06´	´2B2403050303´
					´86´	´8181´	P2OS(Q, 64)
			´5F20´	´0C´	CHR		
			´7F4C´	´13´	CHAT		
					Tag	**L**	**Wert**
					´06´	´08´	OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}
					´53´	´07´	´XX...XX´, Flagliste
			´5F25´	´06´	CED		
			´5F24´	´06´	CXD		
	´5F37´	´8180´	Signatur = *R* || *S*				

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

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

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

Tabelle 70: Tab_PKI_910 TI-PKI, Bedeutung der Bits innerhalb der Flagliste eines CHAT

Bitnummer	**Bedeutung**
Rollenkennzeichnung in den Bits b0 und b1	
b0 b1 = 11_2	Rolle = Root-CA-Schlüssel (in [BSI-TR-03110-3] als CVCA bezeichnet)
b0 b1 = 10_2	Rolle = CA unterhalb der Root-CA
b0 b1 = 00_2	Rolle = CVC enthält öffentlichen Authentisierungsschlüssel
Flaglist mit Funktionen, die nach einer erfolgreichen Authentisierung freigeschaltet werden	
b02	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b03	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen

b04	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b05	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b06	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b07	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b08	eGK: Verwendung der ESIGN-AUTN-Funktionalität mit PIN.CH
b09	eGK: Verwendung der ESIGN-AUTN Funktionalität ohne PIN
b10	eGK: Verwendung der ESIGN-ENCV Funktionalität mit PIN.CH
b11	eGK: Verwendung der ESIGN-ENCV Funktionalität ohne PIN
b12	eGK: Verwendung der ESIGN-AUT Funktionalität
b13	eGK: Verwendung der ESIGN-ENC Funktionalität
b14	eGK: Notfalldatensatz verbergen und sichtbar machen
b15	eGK: Notfalldatensatz schreiben, löschen (hier „erase", nicht „delete") mit PIN.NFD
b16	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b17	eGK: Notfalldatensatz lesen mit MRPIN.NFD
b18	eGK: Notfalldatensatz lesen ohne PIN
b19	eGK: Persönliche Erklärungen (DPE) verbergen und sichtbar machen
b20	eGK: DPE schreiben, löschen (hier „erase", nicht „delete") mit MRPIN.DPE
b21	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b22	eGK: DPE lesen mit MRPIN.DPE_READ
b23	eGK: DPE lesen ohne PIN
b24	eGK: Einwilligungen und Verweise im DF.HCA verbergen und sichtbar machen
b25	eGK: Einwilligungen im DF.HCA lesen und löschen (hier „erase", nicht „delete")
b26	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b27	eGK: Einwilligungen im DF.HCA schreiben
b28	eGK: Verweise im DF.HCA lesen und schreiben
b29	eGK: Geschützte Versichertendaten lesen mit PIN.CH
b30	eGK: Geschützte Versichertendaten lesen ohne PIN
b31	eGK: Loggingdaten schreiben mit PIN.CH
b32	eGK: Loggingdaten schreiben ohne PIN
b33	eGK: Zugriff in den AdV-Umgebungen (vormals: Loggingdaten lesen)
b34	eGK: Prüfungsnachweis lesen und schreiben

b35	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b36	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b37	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b38	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b39	eGK: Gesundheitsdatendienste verbergen und sichtbar machen
b40	eGK: Gesundheitsdatendienste lesen, schreiben und löschen (hier „erase")
b41	eGK: Organspendedatensatz lesen mit MRPIN.OSE
b42	eGK: Organspendedatensatz lesen ohne PIN
b43	eGK: Organspendedatensatz schreiben, löschen (hier „erase", nicht „delete") mit MRPIN.OSE
b44	eGK: Organspendedatensatz aktivieren/deaktivieren mit MRPIN.OSE
b45	eGK: AMTS-Datensatz verbergen und sichtbar machen
b46	eGK: AMTS-Datensatz lesen
b47	eGK: AMTS-Datensatz schreiben, löschen (hier „erase", nicht „delete")
b48	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b49	Fingerprint des COS erstellen
b50	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b51	Auslöser Komfortsignatur
b52	Sichere Signaturerstellungseinheit (SSEE)
b53	Remote-PIN Empfänger
b54	Remote-PIN Sender
b55	SAK für Stapel- oder Komfortsignatur

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

Tabelle 71: Tab_PKI_918 Abbildung von Rollenberechtigungen Zugriffsprofilen auf äquivalente Flaglisten

Zugriffsprofil		**CHAT-Wert / Flagliste (G2)**
Rolle	CHAT.0	´00 0000 0000 0000´

(AUTR_CVC)	CHAT.1	´00 AE1A CDC1 DC00´
	CHAT.2A Ärztin/Arzt Fachliche Institution des Arztes Krankenhaus	´00 5D29 DAA0 BB00´
	CHAT.2ZA Zahnärztin/Zahnarzt Fachliche Institution des Zahnarztes	´00 5D20 DAA0 8300´
	CHAT.3	´00 5C40 DAA0 8300´
	CHAT.4	´00 4C40 DAA0 8200´
	CHAT.5	´00 5C00 02A0 0000´
	CHAT.6	wird nicht verwendet
	CHAT.7	´00 0020 0480 0000´
	CHAT.8	´00 4000 02A0 0000´
	CHAT.9	´00 6800 0AA0 0000´
Gerät (AUTD_CVC)	CHAT.51	´00 0000 0000 0001´
	CHAT.53	´00 0000 0000 000C´
	CHAT.54	´00 0000 0000 0002´
	CHAT.55	´00 0000 0000 0004´
Administration (AUT_CVC)	CHAT.0	´00 0000 0000 0000´

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

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

Die Flagliste für das Profil CHAT.2ZA des Rollen-Zertifikates lautet ´00 5D20 DAA0 8300´.
Die Flagliste für das Profil CHAT.53 des Geräte-Zertifikates lautet ´00 0000 0000 000C´.
Die Kombination, bzw. Veroderung der beiden Flaglisten ergibt ´00 5D20 DAA0 830C´.
Die Flagliste einer Sub-CA beginnt mit der Bit-Folge ´10´ (vgl. Tab_PKI_910). Der Wert für die Flagliste des CA-Zertifikates des TSP-CVC in Tab_PKI_919 lautet ´80 5D20

DAA0 830C´.

Tabelle 72: Tab_PKI_919 Sub-CA-Flaglisten nach Kartentyp (G2) und Zugriffsprofilen

Kartentyp / Geräte-Zugriffsprofil	Rollen-Zugriffsprofil	Sub-CA
CHAT-Wert / Flagliste für ein bestimmtes Zugriffsprofil		
eGK	CHAT.0	´80000000000000´
KTR-AdV	CHAT.1 & CHAT.0	´80AE1ACDC1DC04´
gSMC-K / CHAT.51	-	´80000000000001´
gSMC-KT / CHAT.54	-	´80000000000002´
HBA / CHAT.53	CHAT.2A	´805D29DAA0BB0C´
HBA / CHAT.53	CHAT.2ZA	´805D20DAA0830C´
HBA / CHAT.53	CHAT.3	´805C40DAA0830C´
HBA / CHAT.53	CHAT.4	´804C40DAA0820C´
HBA / CHAT.53	CHAT.5	´805C0002A0000C´
HBA / CHAT.53	CHAT.7	´8000200480000C´
SMC-B / CHAT.55	CHAT.1	´80AE1ACDC1DC04´
SMC-B / CHAT.55	CHAT.2A	´805D29DAA0BB04´
SMC-B / CHAT.55	CHAT.2ZA	´805D20DAA08304´
SMC-B / CHAT.55	CHAT.3	´805C40DAA08304´
SMC-B / CHAT.55	CHAT.4	´804C40DAA08204´
SMC-B / CHAT.55	CHAT.8	´80400002A00004´
SMC-B / CHAT.55	CHAT.9	´8068000AA00004´
CHAT-Wert / Flagliste für kombinierte Zugriffsprofile		
eGK	CHAT.0	–
gSMC-K und gSMC-KT / CHAT.51 & 54	-	´80000000000003´

HBA und SMC-B / CHAT.53 & 55	CHAT.1 - 5 & 7-9	´80FF7BDFE1FF0C´

Tabelle 73: Tab_PKI_911 CMS-PKI, Bedeutung der Bits innerhalb der Flagliste eines CHAT

Bitnummer	Bedeutung
Rollenkennzeichnung in den Bits b0 und b1	
b0 b1 = 11_2	Rolle = Root-CA-Schlüssel (in [BSI-TR-03110-3] als CVCA bezeichnet)
b0 b1 = 10_2	Rolle = CA unterhalb der Root-CA
b0 b1 = 00_2	Rolle = CVC enthält öffentlichen Authentisierungsschlüssel
Flagliste mit Funktionen, die nach einer erfolgreichen Authentisierung freigeschaltet werden	
b02 … b07	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b08	Administrative Tätigkeiten CMS
b09	Administrative Tätigkeiten VSD
b10	Administrative Tätigkeiten zum Schreiben von CV-Zertifikaten
b11	Administrative Tätigkeiten eines TSP zur Laufzeitverlängerung der QES-Anwendung
b12 … b55	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen

7 Festlegung von OIDs

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

8 Prüfung von Zertifikaten

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

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

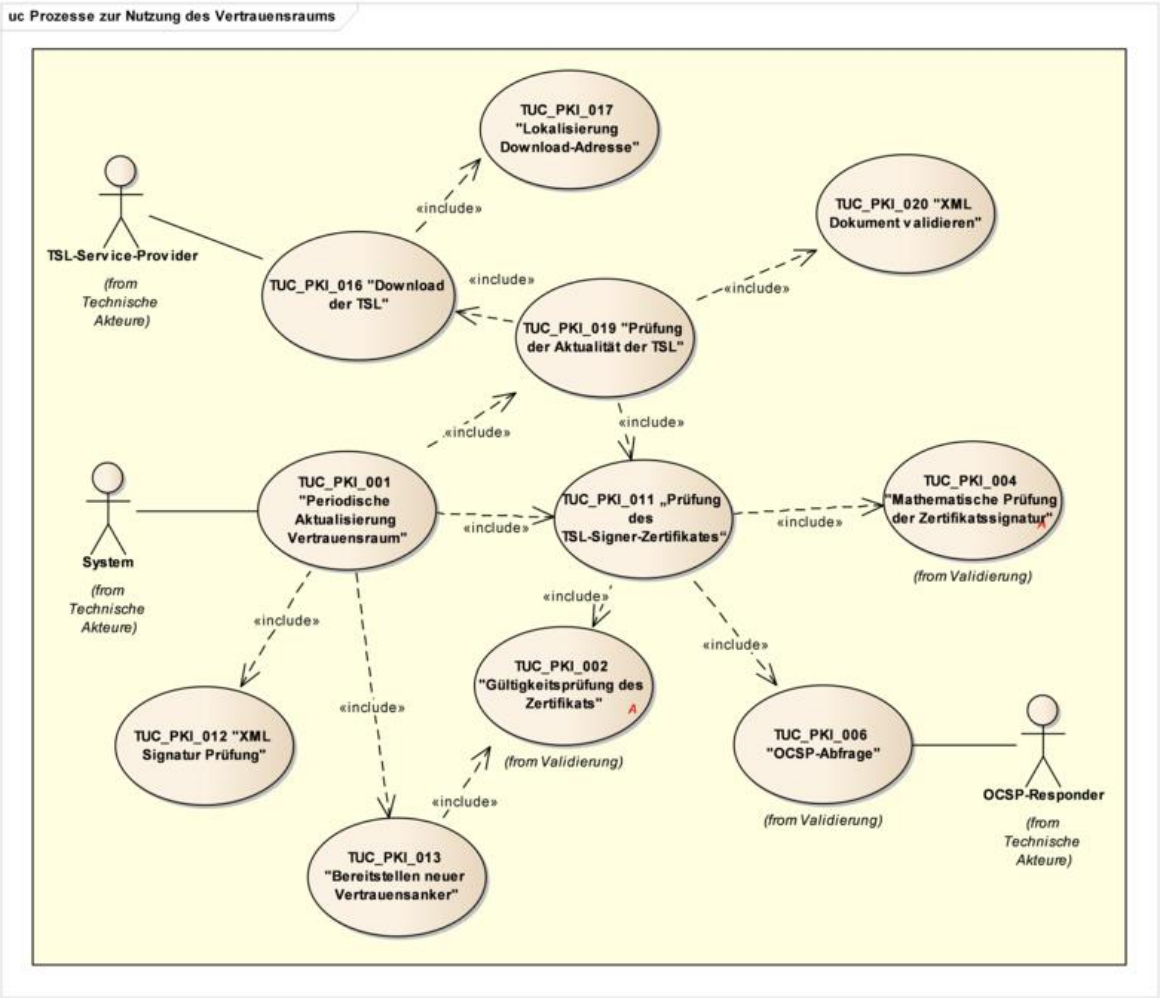


Abbildung 5: Use Case Diagramm „Prozesse zur Nutzung des TI-Vertrauensraums"

Die Funktionalitäten der zertifikatsprüfenden Komponenten werden nachfolgend in „Technischen Use Cases" (TUCs) beschrieben und spezifiziert. Dabei können in jedem der beschriebenen Schritte eines TUC Fehler auftreten. Übergreifend gilt dazu:

GS-A_4637 - TUCs, Durchführung Fehlerüberprüfung
Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN bei der Ausführung eines TUC auf Verarbeitungsfehler prüfen und eine definierte Fehlerbehandlung einleiten**.**
[<=]

GS-A_4829 - TUCs, Fehlerbehandlung
Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN bei der Fehlerbehandlung von TUCs Systemmeldungen ausgeben und der Prozess muss beendet werden, sofern der TUC keine spezifische Fehlerbehandlung beschreibt.
[<=]

Bei der Beschreibung der TUCs sind folgende Punkte zu beachten:

- Die unter „Vorbedingungen" beschriebenen Bedingungen sind nicht Bestandteil des TUC und werden im Ablauf des TUC nicht explizit geprüft. Stattdessen muss der Kontext aus dem heraus der TUC aufgerufen wird sicherstellen, dass bei einer

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

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

Zur Zertifkatsprüfung werden die Vorgaben aus [gemKPT_PKI_TIP] Kap. 6.5 „Zertifikatsprüfung nonQES" berücksichtigt.

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

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

GS-A_5043 - Auflösung von OCSP-Adressen im Internet
TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN für Zertifikatstypen, die zusätzlich zur TI auch im Internet statusgeprüft werden, sicherstellen, dass die im Zertifikat eingetragene OCSP-Responderadresse im Internet aufgelöst und eine Statusabfrage erfolgreich durchgeführt werden kann.
[<=]

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

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

8.1 Vertrauensraum der TI

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

Der Vertrauensraum der TI besteht also aus der Menge der CAs (bzw. deren Zertifikate), die in der TI zugelassen, also als vertrauenswürdig anerkannt sind. Außerdem enthält er

die Einsatzzwecke, für welche die CAs End-Entity-Zertifikate ausgeben dürfen. Dieser TI-Vertrauensraum wird in der TSL abgebildet.

Die TSL enthält Informationen gemäß [ETSI_TS_102_231#5]. Sie beinhalten neben den CA-Zertifikaten im TI-Vertrauensraum zusätzliche Angaben, wie z. B. die Sequenznummer oder die Adressen und Zertifikate der zuständigen OCSP-Responder.

Die TSL spielt also in zertifikatsprüfenden Komponenten die zentrale Rolle.

Konkret bereitgestellt wird die TSL als TSL-Datei in Form einer signierten XML-Datei gemäß [ETSI_TS_102_231#B].

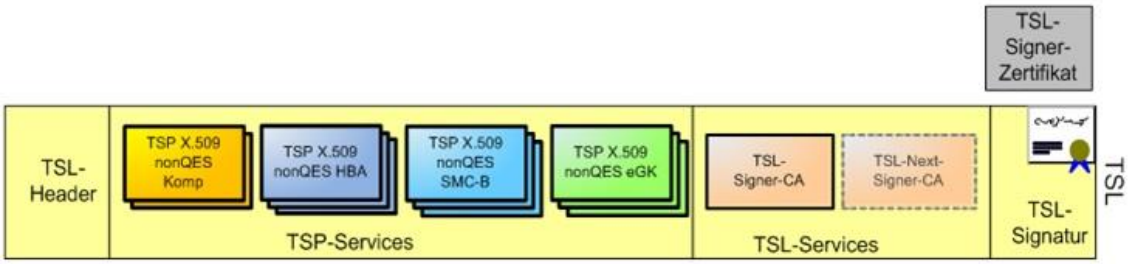


Abbildung 6 : Aufbau der TSL

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

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

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

- Initialisierung / Aktualisierung des TI-Vertrauensraumes
- Lokalisieren der TSL-Datei
- Download der TSL-Datei (ggf. nach vorheriger Aktualitätsprüfung mittels Hashwert-Vergleichsverfahren)
- Validierung der TSL-Datei
- Prüfung der Integrität und Authentizität der TSL-Datei durch die Prüfung ihrer Signatur

Die bereits im Internet etablierten PKIs der 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 Statusinformationen der zugehörigen EE-Zertifikate durch Nachnutzung des OCSP-Responder Proxy zur Verfügung gestellt werden (s. Beschreibung in [gemKPT_Arch_TIP#5.4.13].

8.1.1 TSL im Kontext der ECC-Migration

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

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

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

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

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

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

8.1.2 Initialisierung TI-Vertrauensraum

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

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

Dies gilt für die Anwendungsfälle

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

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

GS-A_4640 - Identifizierung/Validierung des TI-Vertrauensankers bei der initialen Einbringung
Hersteller von Produkttypen der TI, die Zertifikate prüfen, MÜSSEN bei der initialen Einbringung das aktuell gültige TSL-Signer-CA-Zertifikat eindeutig identifizieren und mittels Fingerprint validieren, bevor dieses Zertifikat als TI-Vertrauensanker in die Komponente eingebracht werden darf.
[<=]

GS-A_4641 - Initiale Einbringung TI-Vertrauensanker
Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN die initiale Einbringung des aktuell gültigen TSL-Signer-CA-Zertifikat als TI-Vertrauensanker in die Komponente nachweislich sicher vor Manipulation vornehmen.
[<=]

WA-A_2111 - Initiale Einbringung TI-Vertrauensanker in andere Anwendungen
Der Anbieter einer aAdG oder aAdG-NetG-TI MUSS sicherstellen, dass die initiale Einbringung des aktuell gültigen TSL-Signer-CA-Zertifikats als TI-Vertrauensanker in Dienste der aAdG oder der aAdG-NetG-TI nachweislich sicher vor Manipulation vorgenommen wird.**[<=]**

GS-A_4748 - Initiale Einbringung TSL-Datei
Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN die initiale Einbringung der TSL-Datei in die Komponente nachweislich sicher vor Manipulation vornehmen.
[<=]

WA-A_2112 - Initiale Einbringung TSL-Datei
Der Anbieter einer aAdG oder aAdG-NetG-TI MUSS sicherstellen, dass die initiale Einbringung der TSL-Datei in Dienste der aAdG oder der aAdG-NetG-TI nachweislich sicher vor Manipulation vorgenommen wird.**[<=]**

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

A_17688 - Nutzung des ECC-RSA-Vertrauensraumes (ECC-Migration)
Die Produkttypen der TI, die ECC-Zertifikate validieren müssen, MÜSSEN das TSL-Signer-CA-Zertifikat (ECDSA) als TI-Vertrauensanker und die TSL(ECC-RSA) verwenden.

[<=]

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

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

A_17689 - Nutzung von Cross-Zertifikaten für Vertrauensraum-Wechsel nach ECC-RSA (ECC-Migration)
Die Produkttypen der TI, die einen Vertrauensanker (ECC-RSA) zur Etablierung des Vertrauensraumes (ECC-RSA) initialisieren, KÖNNEN Cross-Zertifikate verwenden, um auf Basis ihres bereits etablierten Vertrauensankers (RSA) in den Vertrauensraum (ECC-RSA) zu wechseln.

[<=]

A_17820 - Nutzung von Cross-Zertifikaten für Vertrauensraum-Wechsel nach RSA (ECC-Migration)
Die Produkttypen der TI, die einen Vertrauensanker (RSA) zur Etablierung des Vertrauensraumes (RSA) initialisieren, KÖNNEN Cross-Zertifikate verwenden, um auf Basis ihres bereits etablierten Vertrauensankers (ECC-RSA) in den Vertrauensraum (RSA) zu wechseln.
[<=]

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

A_17821 - Wechsel des Vertrauensraumes mittels Cross-Zertifikaten (ECC-Migration)
Die Produkttypen der TI, die den Vertrauensraum mittels Cross-Zertifikates wechseln (siehe A_17689 und A_17820) MÜSSEN die folgenden Schritte erfolgreich durchlaufen, um auf den Vertrauensanker des neuen Vertrauensraumes zu wechseln.
Vorbedingung: Das System besitzt zum aktuell etablierten Vertrauensraum den aktuell aktiven Vertrauensanker (der zu dem benutzten Cross-Zertifikat passend ist).

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

Wenn einer der Schritte fehlschlägt, MUSS der Vertrauensraum-Wechsel-Prozess abgebrochen werden und der alte Vertrauensanker (TSL-Signer-CA<Y>) im System verbleiben.
Nach erfolgreichem Durchlaufen aller Schritte, MUSS der Vertrauensanker (TSL-Signer-CA<X>) im System etabliert sein.
Erklärungen zu den verwendeten Begriffen:

- Vertrauensanker im System vor dem Vertrauensraum-Wechsel: TSL-Signer-CA<Y>
- Vertrauensanker des neuen Vertrauensraumes: TSL-Signer-CA<X>
- Verwendetes Cross-Zertifikat: C.GEM-TSL-CA<X>-CROSS<Y>
- TSLSequenceNumber – Nummernkreis RSA: 0..9999

- TSLSequenceNumber – Nummernkreis ECC-RSA: ab 10000

[<=]

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

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

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

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

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

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

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

	Anchor BNetzA-VL-Signer Unspecified ServiceType	
http://uri.etsi.org/TrstSvc/Svcstatus/revoked	X.509-CA	Die Zulassung des Dienstes wurde wegen eines nicht-sicherheitskritischen Incidents widerrufen und die CA stellt keine End-Entity-Zertifikate mehr aus. Bis zum Widerrufsdatum (im Element StatusStartingTime) ausgegebene End-Entity-Zertifikate müssen aber normal (also als gültig, falls nicht widerrufen) behandelt werden.
http://uri.etsi.org/TrstSvc/Svcstatus/expired	X.509-CA	Der Dienst war für die TI zugelassen und war bis zum angegebenen Datum (im Element StatusStartingTime) in Betrieb und im TI-Vertrauensraum.

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

8.1.2.1 TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum"

GS-A_4642 - TUC_PKI_001: Periodische Aktualisierung TI-Vertrauensraum
Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_001 zur periodischen Aktualisierung des TI-Vertrauensraums umsetzen.
[<=]

Tabelle 75: TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum"

Element	Beschreibung
Name	TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum"

Beschreibung	Dieser Use Case beschreibt den gesamten Ablauf zur periodischen Aktualisierung des TI-Vertrauensraumes mittels einer TSL-Datei. Dabei verwendet er weitere TUCs, die im Laufe des Kapitels detailliert spezifiziert werden Ein Offline-Modus ist zu berücksichtigen für a) das Mobile-Kartenterminal b) Konnektor ohne Anbindung an die TI Beide verfügen nicht über die automatischen Online-Möglichkeiten zum Bezug von Statusinformationen oder TSL-Aktualisierungen aus der TI.
Anwendungsumfeld	System, das die TSL auswertet
Vorbedingungen	Gültige TSL im System (optional mit Hashwert)
Auslöser	Produkttypspezifischer Trigger Zeitpunkt MUSS durch Facharchitekturen vorgegeben werden. (Standardmäßig ist eine tägliche Prüfung der Aktualität vorzusehen.)
Eingangsdaten	• Neu eingebrachte TSL-Datei (optional) • OCSP-Graceperiod (legt bei der Verwendung von gecachten OCSP-Antworten den maximal zulässigen Zeitraum fest, den die Systemzeit der prüfenden Komponente noch nach dem Zeitpunkt der OCSP-Antwort liegen darf) • Flag für Offline-Modus (Im Offline-Fall kann keine Sperrstatusprüfung des TSL-Signer-Zertifikates durchgeführt werden.)
Komponenten	System, TSL-Download-Punkt, OCSP-Responder
Ausgangsdaten	Status der Initialisierung
Referenzen	[ETSI_TS_102_231]
Standardablauf	1. [System:] System startet die Initialisierung des TI-Vertrauensraums. 2. [System:] Die TSL im System wird auf Aktualität geprüft (TUC_PKI_019 „Prüfung der Aktualität der TSL"). Diese Prüfung erfolgt gegen die neu eingebrachte TSL-Datei als Eingangsparameter oder optional bei Vorhandensein eines TSL-Hashwertes im System über einen Vergleich mit der TSL-Hashwert-Datei am Downloadpunkt. (Ansonsten wird die aktuelle TSL-Datei bei diesem Schritt heruntergeladen.) Die Prüfung ergibt, dass die im System abgelegten TSL-Informationen erneuert werden müssen. 3.

	[System:] Das verwendete TSL-Signer-Zertifikat wird aus der TSL-Datei extrahiert. 4. [System:] OCSP-Abfrage für das extrahierte TSL-Signer-Zertifikat durch das System (TUC_PKI_006 "OCSP-Abfrage"). Wenn der zuständige OCSP-Responder die Statusinformation des Zertifikats mit einem Wert „revoked" oder „unknown" gemäß GS-A_4690 zurückgibt oder die certHash-Erweiterung fehlt (CERTHASH_EXTENSION_MISSING) bzw. falsch ist (CERTHASH_MISMATCH), darf es nicht zu einer Aktualisierung des TI-Vertrauensraums kommen. (Sämtliche anderen Schritte einer Prüfung des Zertifikates und der XML-Signatur sind im TUC_PKI_019 „Prüfung der Aktualität der TSL" referenziert, vgl. im Schritt 2.) 5. [System:] Es wird ermittelt, ob in der neuen TSL ein neuer TI-Vertrauensanker vorliegt (TUC_PKI_013 „Import TI-Vertrauensanker aus TSL"). 6. [System:] Aus den CA-Zertifikaten aus der neuen TSL wird der neue TI-Vertrauensraum gebildet. Dazu werden sie aus der TSL-Datei extrahiert, z. B. in einen System-eigenen Truststore gespeichert und dem System bereitgestellt. Bei der Extraktion der Zertifikate aus der TSL darf keine inhaltliche Überprüfung der Datenfelder oder eine Signaturprüfung des Zertifikats erfolgen. Falls ein solcher Truststore nur den Vertrauensraum der TI enthält, wird er vor der Neubefüllung geleert, so dass anschließend nur die Zertifikate aus der aktuellen TSL dem System zur Verfügung stehen. Falls der Truststore auch für die sichere Speicherung von Zertifikaten benutzt wird, die nicht in der TSL stehen, muss keine komplette Leerung des Truststores erfolgen. Das System muss aber sicherstellen, dass im Truststore nur diejenigen Zertifikate der TI enthalten sind, die den aktuellen Vertrauensraum der TI aufspannen bzw. in der aktuellen TSL-Datei enthalten sind. Die Form des Truststore wird nicht näher spezifiziert, dieser muss nur den gestellten Anforderungen (z. B. bezüglich Sicherheit oder Performance) genügen. Das System muss den TI-Vertrauensraum mit den in der TSL als vertrauenswürdig bezeichneten und für den Produkttyp relevanten CA-Zertifikaten gemäß Tab_PKI_271 „Erlaubte Inhalte des TSL-Elements ServiceStatus" befüllen. 7. [System:] Der Truststore wird für Zertifikatsprüfung (wieder) bereitgestellt. 8. [System:] Ende des Use Case

Varianten/Alternativen	Der Standardablauf stellt die Prüfungen dar, die vollzogen werden müssen. Eine Trennung in zwei Prozesse oder eine Umstrukturierung, bei der alle notwendigen Prüfungen erfolgen, ist zulässig. Im Falle einer aktuellen TSL im System endet der Ablauf nach Schritt 2: 2a. [System:] TSL aus Download ist gleich TSL im System; und TSL ist noch gültig. 2a.1 [System:] Ende des Use Case 3a. [System:] Wenn das Offline-Flag gesetzt ist (offline==true), dann wird mit Schritt 5 fortgesetzt. (Im Offline-Fall kann keine OCSP-Abfrage stattfinden.)
Fehlerfälle/Warnung	2b. [System:] Der TUC_PKI_019 wirft eine VALIDITY_WARNING_2. VALIDITY_WARNING_2 wird als Fehlermeldung ausgegeben. Die weitere Fehlerbehandlung erfolgt unter Beachtung von [GS-A_5336]. 3b. [System:] Das TSL-Signer-Zertifikat lässt sich nicht aus der TSL-Datei extrahieren (TSL_CERT_EXTRACTION_ERROR). Weitere Fehlerfälle sind in den jeweiligen referenzierten TUCs beschrieben.
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	Die Angaben zur Prüfung einer neuen TSL-Datei müssen als vertrauenswürdige Informationen im System schon vorhanden sein. Deshalb muss die OCSP-Adresse zur Prüfung des Signers der neuen TSL-Datei aus der TSL im System ausgelesen werden. Für die Prüfung der ersten TSL-Datei nach einem Vertrauensankerwechsel (entsprechend TUC_PKI_013 „Import TI-Vertrauensanker aus TSL“ und angekündigt mit ServiceTypeIdentifier „http://uri.etsi.org/TrstSvc/Svctype/TSLServiceCertChange“) bedeutet dies, dass die OCSP-Adresse aus dem „TSLServiceCertChange“ Eintrag aus der TSL im System genommen werden muss. Bei der OCSP-Abfrage für das extrahierte TSL-Signer-Zertifikat gemäß TUC_PKI_006 "OCSP-Abfrage" ist es nicht zulässig, im Schritt „Ermittlung der OCSP-Adresse“ (TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln") bereits Daten aus der zu importierenden TSL zu verwenden. Hinweis zur Robustheit der TSL-Verarbeitung: Nach

	erfolgreichen Schema- und Signatur-Prüfungen darf es bei der Verarbeitung der TSL-Elemente nicht mehr zum Abbruch des TUC kommen.
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_001 "Periodische Aktualisierung TI-Vertrauensraum". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

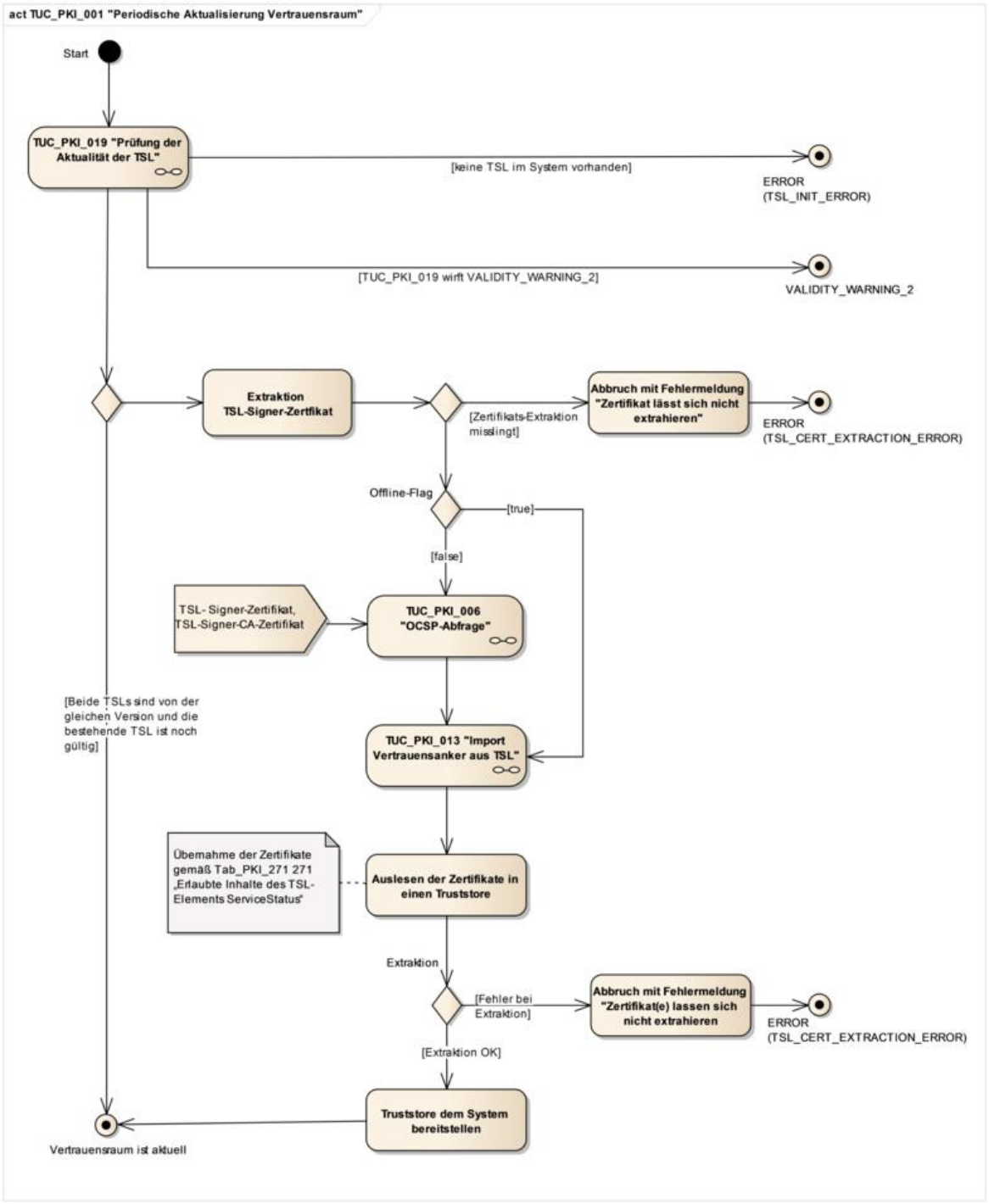


Abbildung 7: Aktivitätsdiagramm TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum"

8.1.3 Geplanter Wechsel TI-Vertrauensanker

Im Folgenden werden der Prozess und die Vorgaben zum TI-Vertrauensankerwechsel beschrieben, die sich beim Wechsel innerhalb einer Schlüsselgeneration (RSA bzw. ECDSA) ergeben.

Wird ein Vertrauensankerwechsel im Rahmen der ECC-Migration vorgenommen, so gelten die Hinweise zur ECC-Migration in Kapitel 8.1.

8.1.3.1 TUC_PKI_013 „Import TI-Vertrauensanker aus TSL"

GS-A_4643 - TUC_PKI_013: Import TI-Vertrauensanker aus TSL
Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_013 zum Import neuer TI-Vertrauensanker umsetzen.
[<=]

Tabelle 76: TUC_PKI_013 „Import neuer TI-Vertrauensanker"

Element	Beschreibung
Name	TUC_PKI_013 „Import neuer TI-Vertrauensanker"
Beschreibung	Als TI-Vertrauensanker gilt das aktuell gültige TSL-Signer-CA-Zertifikat. Das neue TSL-Signer-CA-Zertifikat wird rechtzeitig vor dem geplanten Aktivierungsdatum in die TSL integriert und als zukünftiger TI-Vertrauensanker markiert. Über diesen Weg wird es an Komponenten und Systeme ausgeliefert. Die Integrität des neuen Schlüssels wird somit durch den gültigen alten gesichert.
Anwendungsumfeld	System, das die TSL verwendet
Vorbedingungen	TSL mit gültiger Signatur
Auslöser	TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum"
Eingangsdaten	Neue TSL-Datei (TSL aus dem Download oder manuellen Import)
Komponenten	System
Ausgangsdaten	Status des Prozesses, im Erfolgsfall eine Erweiterung des sicheren Speichers des Systems um den neuen TI-Vertrauensanker und dessen Aktivierungsdatum.

Referenzen	[ETSI_TS_102_231]
Standardablauf	1. [System:] Das System sucht in der TSL nach den Einträgen für den neuen TI-Vertrauensanker. Die Identifikation erfolgt über den in GS-A_4644 bezeichneten ServiceTypeIdentifier-URI. Zusätzlich kann auch der in GS-A_4644 angegebene OID in der ServiceInformationExtension auf korrekte Belegung geprüft werden. Siehe Kapitel 8.1.3.2. Es wird immer das CA-Zertifikat bereitgestellt. Alle anderen Zustände (z. B. wenn nur der unzertifizierte Schlüssel bereitgestellt wird) müssen als Fehler behandelt werden. Parameter: heruntergeladene TSL 2. [System:] Aus dem gefundenen Eintrag wird das Zertifikat extrahiert. Ergebnis: zukünftiges TSL-Signer-CA-Zertifikat 3. [System:] Aus dem Eintrag des zukünftigen TSL-Signer-CA-Zertifikats wird die „StatusStartingTime" extrahiert. Ergebnis: StatusStartingTime 4. [System:] Für das zukünftige TSL-Signer-CA-Zertifikat wird TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats" durchlaufen. Parameter: zukünftiges TSL-CA-Zertifikat, StatusStartingTime. 5. [System:] Der zukünftige TI-Vertrauensanker wird parallel zum aktiven TI-Vertrauensanker abgelegt. Parameter: zukünftiges TSL-Signer-CA-Zertifikat 6. [System:] Der zukünftige TI-Vertrauensanker darf nicht vor dem Zeitpunkt „StatusStartingTime" aktiviert werden. Der zukünftige TI-Vertrauensanker muss spätestens dann aktiviert werden, wenn nach Erreichen der „StatusStartingTime" ein Update der TSL durchgeführt wird. Bei Aktivierung des zukünftigen TI-Vertrauensankers wird der alte TI-

	Vertrauensanker deaktiviert. Parameter: StatusStartingTime
Varianten/Alternativen	1a. [System:] Es wird kein als neuer TI-Vertrauensanker markiertes CA-Zertifikat gefunden und der Use Case wird beendet.
Fehlerfälle	Ein Abbruch des TUC führt nur dazu, dass kein neuer TI-Vertrauensanker abgelegt wird. Er hat keinen Einfluss auf die Gültigkeit des bestehenden TI-Vertrauensankers oder auf die anderen Schritte der TSL-Aktualisierung. Das System muss dies jedoch protokollieren. 1b. [System:] Es wird mehr als ein markiertes CA-Zertifikat gefunden. (MULTIPLE_TRUST_ANCHOR) 2b. [System:] Das TSL-Signer-CA-Zertifikat lässt sich nicht aus der TSL extrahieren. (TSL_SIG_CERT_EXTRACTION_ERROR)
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	Der Prozess wird unhabhängig davon durchlaufen, ob schon ein zukünftiger TI-Vertrauensanker vorliegt oder nicht. Es ist immer nur der zuletzt angekündigte zukünftige TI-Vertrauensanker gültig. Ältere Ankündigungen müssen überschrieben werden. Die Gestaltung des sicheren Speichers des Systems ist durch den Betreiber/Implementierer des Systems zu definieren.
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_013 "Import neuer TI-Vertrauensanker". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

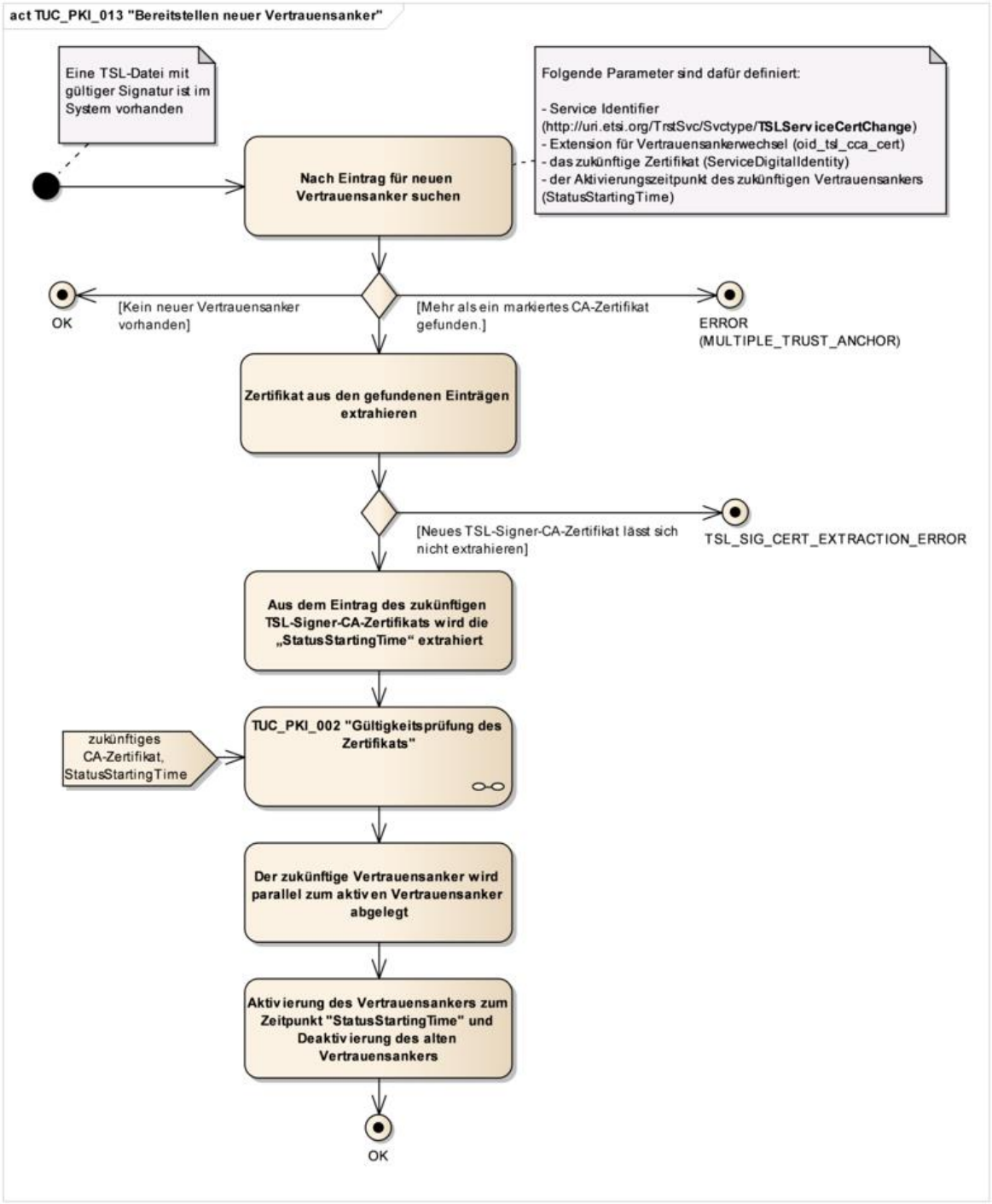


Abbildung 8: Aktivitätsdiagramm TUC_PKI_013 „Import neuer TI-Vertrauensanker"

8.1.3.2 TSL-Einträge für die Bereitstellung neuer TI-Vertrauensanker

Für den Wechsel auf ein neues TSL-Signer-CA-Zertifikat wird dieses in der TSL aufgenommen unter Berücksichtigung folgender Rahmenbedingungen:

Die Aufnahme des Zertifikates erfolgt rechtzeitig, also erstmals zu einem Datum, welches eine definierte Zeitspanne vor dem geplanten Aktivierungsdatum liegt. Diese Aufnahme

erfolgt in Abstimmung mit der gematik und unter Einhaltung der üblichen Prozesse der Eintragsverwaltung für Zertifikate in der TSL (s. auch [gemSpec_TSL#6.1.2]). Ab diesem Datum wird das Zertifikat auch in den folgenden TSL-Dateien bis zum Erreichen des Aktivierungszeitpunkts als nächster TI-Vertrauensanker geführt.

Dies wird so gehandhabt, um temporär offline befindliche Komponenten eine als zumutbar angenommene Zeitspanne zur Migration zu gewähren.

Die Integrität des neuen Schlüssels wird durch den alten gesichert. Dazu erzeugt der gematik TSL-Dienst einen TSP-Dienst-Eintrag in der TSL-Datei mit folgenden Eigenschaften (Update-Parameter):

- Service Type Identifier (http://uri.etsi.org/TrstSvc/Svctype/TSLServiceCertChange) signalisiert den Verwendungszweck des Eintrags,
  `<xsd:element name="ServiceTypeIdentifier" type="tsl:NonEmptyURIType"/>`
- das neue TSL-Signer-CA-Zertifikat (ServiceDigitalIdentity),
  `<xsd:element name="X509Certificate" type="xsd:base64Binary"/>`
- der Aktivierungszeitpunkt des neuen TSL-Signer-CA-Zertifikats (StatusStartingTime)
  `<xsd:element name="StatusStartingTime" type="xsd:dateTime"/>`
- die Extension für den TI-Vertrauensanker-Wechsel gemäß [gemSpec_OID#3.6] (in ServiceInformationExtension).
  `<xsd:element name="ServiceInformationExtensions" type="tsl:ExtensionsListType" minOccurs="0"/>`

Ergänzend dazu gelten die allgemeinen Vorgaben für das Element TSPService wie in [gemSpec_TSL#7.3.2] beschrieben, siehe z. B. TIP1-A_4104 hinsichtlich Eintrag des X.509-Zertifikats oder TIP1-A_4106 bezüglich der Adresse der OCSP-Responder-Adresse.

Als TI-Vertrauensanker wird das TSL-Signer-CA-Zertifikat angesehen. Bei jedem Wechsel wird der vollständige TI-Vertrauensanker in der TSL veröffentlicht.

GS-A_4644 - TSL-Vertrauensankerwechsel
Der TSL-Dienst MUSS für einen TI-Vertrauensankerwechsel die folgenden Einträge aufnehmen:
(a) Innerhalb Element ServiceTypeIdentifier:
URI http://uri.etsi.org/TrstSvc/Svctype/TSLServiceCertChange
(b) das Zertifikat des neuen TI-Vertrauensankers in ServiceDigitalIdentity
(c) Einen durch die gematik vorgegebenen Aktivierungszeitpunkt im Element StatusStartingTime
(d) Adresse des OCSP-Responders zur Prüfung von ausgestellten Zertifikaten (TSL-Signer) in ServiceSupplyPoint(s) (e) die Extension für den TI-Vertrauensankerwechsel {oid_tsl_cca_cert} gemäß [gemSpec_OID#GS-A_4447] (in ServiceInformationExtension)
[<=]

Hinweis: Der TSL-Dienst führt das Zertifikat des nächsten TI-Vertrauensankers ab dem erstmaligen Eintrag zusammen mit den anderen Einträgen (a) – (e) in allen folgenden TSL-Dateien bis zu seiner Aktivierung.

Das vorliegende Dokument trifft keine Festlegungen zu den konkret einzutragenden OID-Werten, sondern verwendet stattdessen eine OID-Referenz, die in der Spalte "Inhalt" der Tabelle 82 genannt ist. Die normative Festlegung der OIDs trifft das Dokument [gemSpec_OID], dort ist die Zuordnung zur OID-Referenz ersichtlich.

Tabelle 77: Gültige Werte für den TI-Vertrauensankerwechsel

Beschreibung	Ort	Bezeichnung	Format	Inhalt
Eintragsdaten für den Wechsel des TSL-Signer-CA-Zertifikats des TSL-Vertrauensankers	TSL	Change of TSL Signer-CA Certificate	OID	oid_tsl_cca_cert

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

Tabelle 78: Beispiel für den TSL-Eintrag zum Wechsel des TSL-Signer-CA-Zertifikats

```
<TSPService>
    <ServiceInformation>
    <ServiceTypeIdentifier>
http://uri.etsi.org/TrstSvc/Svctype/TSLServiceCertChange
</ ServiceTypeIdentifier>
<ServiceName>
        <Name xml:lang="DE">{Name des neuen TSL-Vertrauensankers}</Name>
</ServiceName>
    <ServiceDigitalIdentity>
        <DigitalId>
    <X509Certificate>{Base64-codiertes X.509-Zertifikat}</X509Certificate>
        </DigitalId>
    </ServiceDigitalIdentity>
    <ServiceStatus>http://uri.etsi.org/TrstSvc/Svcstatus/inaccord
</ServiceStatus>
    <StatusStartingTime>2008-04-01T09:30:47Z</StatusStartingTime>
    <ServiceSupplyPoints>
    <ServiceSupplyPoint>http://pki01ocsp02.gematik.net
</ServiceSupplyPoint>
    </ServiceSupplyPoints>
    <ServiceInformationExtensions>
        <Extension Critical="false">
            <ExtensionOID>{oid_tsl_cca_cert}</ExtensionOID>
            <ExtensionValue>oid_tsl_cca_cert</ExtensionValue>
        </Extension>
    </ServiceInformationExtensions>
    </ServiceInformation>
</TSPService>
```

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

8.1.3.3 Prüfung der TSL nach Wechsel des TI-Vertrauensanker

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

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

GS-A_4645 - TSL-Signatur ab Aktivierungsdatum neuer TI-Vertrauensanker
Der TSL-Dienst MUSS ab dem Aktivierungsdatum eines über die TSL publizierten TI-Vertrauensankers (TSL-Signer-CA-Zertifikat) die TSL mit einem TSL-Signer-Zertifikat

signieren, das von dieser TSL-Signer-CA ausgestellt wurde.
[<=]

8.1.4 Ungeplanter Wechsel des TI-Vertrauensanker

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

8.2 TSL-Prüfung

8.2.1 Erreichbarkeit und Download der TSL

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

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

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

Die Lokalisierung der Adresse ist in Abschnitt 8.2.1.1 detailliert beschrieben.

8.2.1.1 TUC_PKI_017 „Lokalisierung TSL Download-Adressen"

GS-A_4646 - TUC_PKI_017: Lokalisierung TSL Download-Adressen
Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_017 zur Lokalisierung der Download-Adressen der TSL umsetzen.
[<=]

Tabelle 79: TUC_PKI_017 „Lokalisierung Download-Adressen"

Element	Beschreibung
Name	TUC_PKI_017 „Lokalisierung Download-Adressen"
Beschreibung	Die TSL enthält im Element „PointersToOtherTSL" die Zugriffsadresse für die jeweilige Liste. Zusätzlich ist ein Eintrag für eine Backup-Zugriffsadresse vorhanden. Dieser Use Case beschreibt, wie diese Adressen lokalisiert werden.
Anwendungsumfeld	System, das die TSL verwendet

Vorbedingungen	TSL mit gültiger Signatur
Auslöser	TUC_PKI_016 „Download der TSL”
Eingangsdaten	TSL
Komponenten	System
Ausgangsdaten	PointersToOtherTSL[Primär-Zugriffsadresse, Backup-Zugriffsadresse]
Referenzen	[ETSI_TS_102_231] Annex H und B.2.13
Standardablauf	1. [System:] System startet die Lokalisierung der Adressen 2. [System:] Das Element „PointersToOtherTSL“ wird ausgewählt. 3. [System:] Übergabe des Elements 4. [System:] Ende des Use Cases mit Rückgabe des Adressen-Elements
Fehlerfälle	2a. [System:] Das Element ist nicht vorhanden und der Vorgang wird mit Fehlermeldung abgebrochen. (TSL_DOWNLOAD_ADDRESS_ERROR)
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	Die Kennzeichnung der Adressen in der TSL als primär oder als Backup erfolgt gemäß Tab_PKI_272
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_017 "Lokalisierung Download-Adresse". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

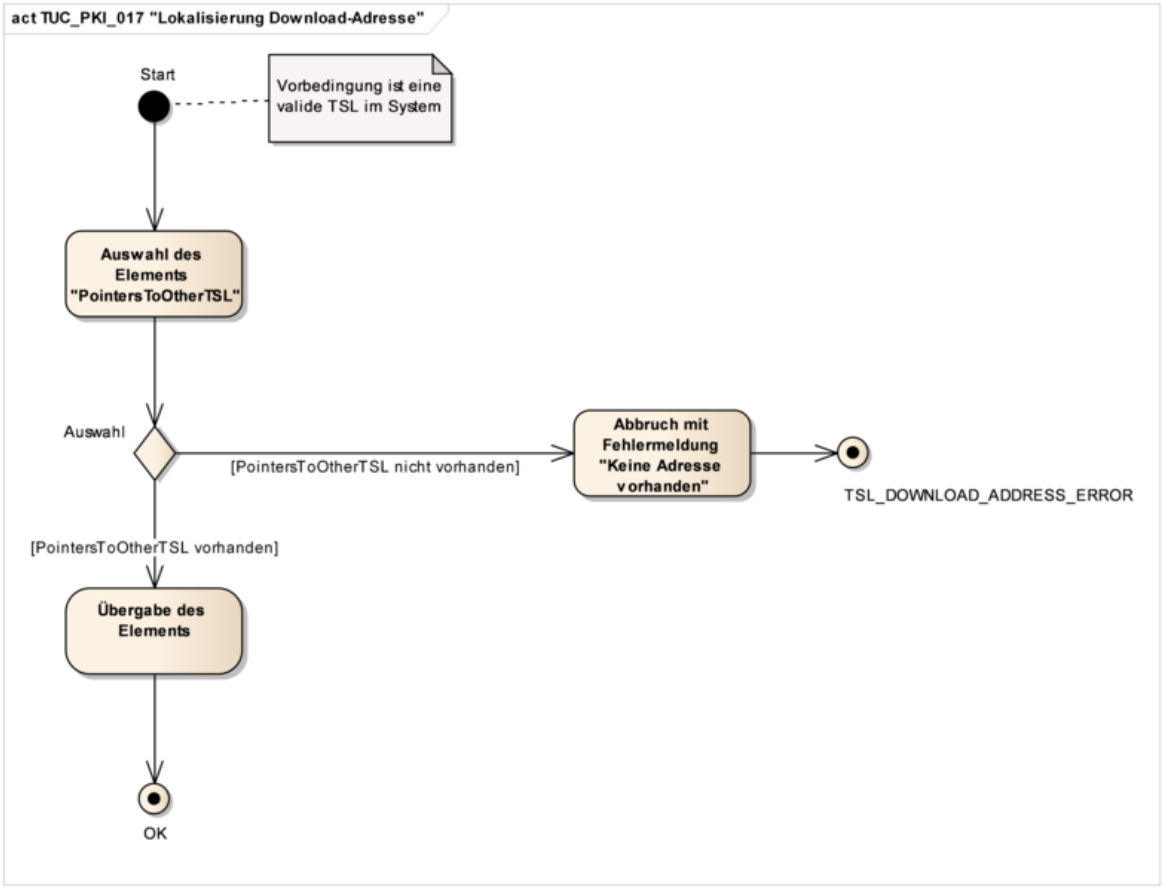


Abbildung 9: Aktivitätsdiagramm TUC_PKI_017 „Lokalisierung Download-Adresse“

Tabelle 80: Tab_PKI_272 Gültige Werte zur Download-Adresse

Beschreibung	Ort	Bezeichnung	Format	Inhalt
Bezeichner der Eintragsdaten für die Primär-Adresse der TSL	TSL	Primär-Adresse	OID	oid_tsl_p_loc
Bezeichner der Eintragsdaten für die Backup-Adresse der TSL	TSL	Backup-Adresse	OID	oid_tsl_b_loc

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

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

8.2.1.2 TUC_PKI_016 „Download der TSL-Datei“

GS-A_4647 - TUC_PKI_016: Download der TSL-Datei
Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_016 zum Download der TSL-Datei umsetzen.
[<=]

Tabelle 81: TUC_PKI_016 „Download der TSL-Datei"

Element	Beschreibung
Name	TUC_PKI_016 „Download der TSL-Datei"
Beschreibung	Es wird der Download-Prozess der TSL-Datei und das Verhalten des Systems bei Fehlerfällen, wie nicht erfolgreicher Download bzw. Netzwerkproblemen beschrieben.
Anwendungsumfeld	System, das die TSL verwendet
Vorbedingungen	Lokalisierung der Download-Adresse
Auslöser	TUC_PKI_019 „Prüfung der Aktualität der TSL"
Eingangsdaten	TSL
Komponenten	System, TSL-Download-Punkt
Ausgangsdaten	Status des Prozesses
Referenzen	[ETSI_TS_102_231]
Standardablauf	1. [System:] Das System startet den Prozess zum Download der TSL-Datei. 2. [System:] Lokalisierung der Download-Adresse (TUC_PKI_017 „Lokalisierung TSL Download-Adressen") 3. [System:] Auswahl der Primär-Adresse gemäß Tab_PKI_272 aus dem Element „PointersToOtherTSL" und Download der TSL-Datei.Ist der TSL-Download anhand der Primär-Adresse nicht erfolgreich, wird die Backup-Adresse für den Download verwendet. 4. [System:] Ende des Use Case mit entsprechender Rückmeldung.

Varianten/Alternativen	3a. [System:] Bei Fehlern wird ein einfaches Fehlerhandling angestoßen: Der TSL-Download anhand der Primär-Adresse wird dreimal wiederholt. Bei Wiederholung des TSL-Downloads anhand der Backup-Adresse ist analog zu verfahren.
Fehlerfälle	4a. [System:] Sollte der wiederholte Download über keine der Download-Adressen erfolgreich sein, meldet das System einen Fehler und es werden für den Moment keine weiteren Download-Versuche mehr unternommen. (TSL_DOWNLOAD_ERROR)
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_016 "Download der TSL-Datei". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

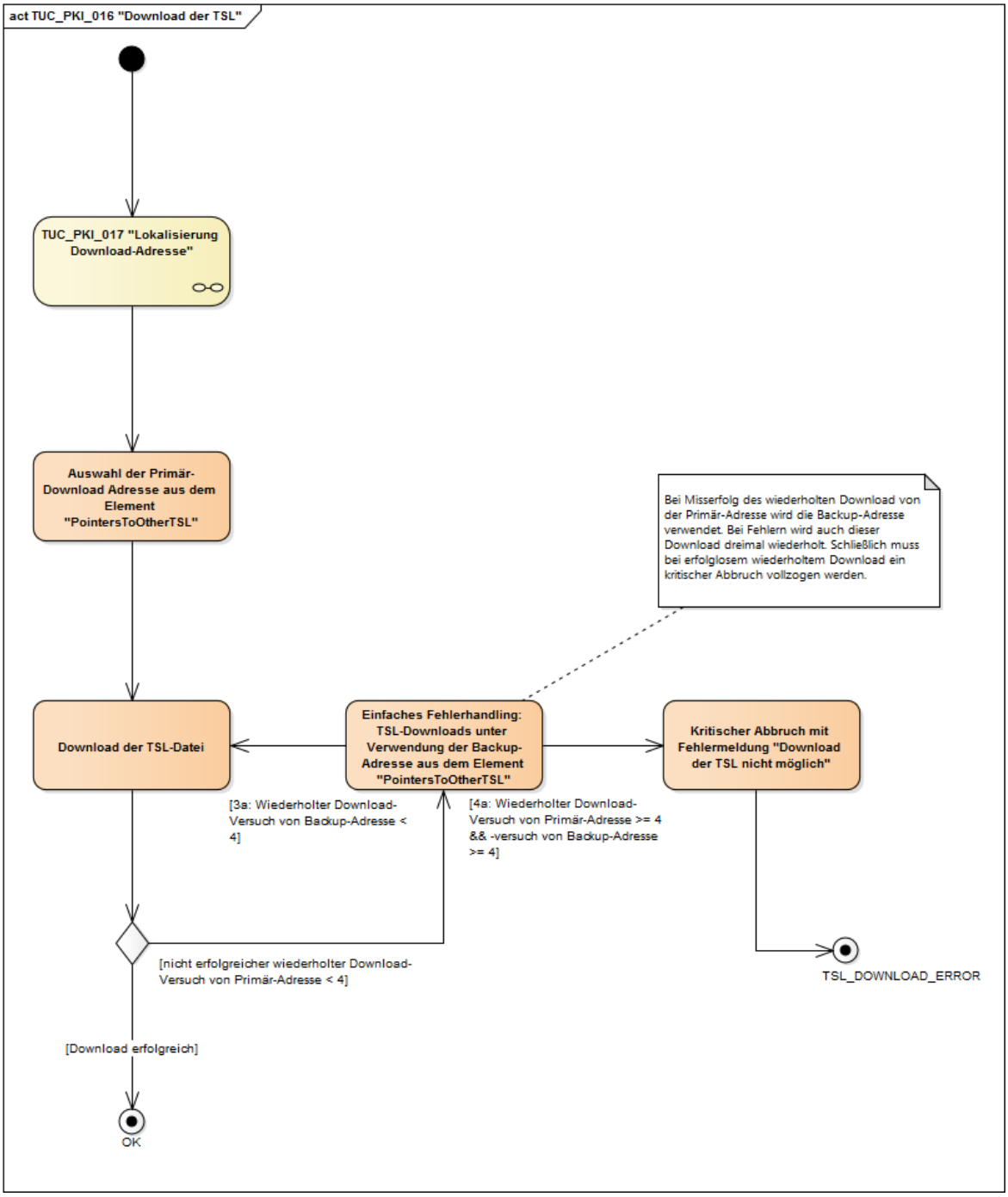


Abbildung 10: Aktivitätsdiagramm TUC_PKI_016 „Download der TSL-Datei"

8.2.2 Vertrauensstatus und Authentifizieren der TSL

8.2.2.1 TUC_PKI_019 „Prüfung der Aktualität der TSL"

Eine TSL-prüfende Komponente oder Anwendung kann den übergreifend festgelegten maximalen Wert der TSL-Graceperiod (30 Tage) mit dem Eingangsparameter TSL-Grace-Period überschreiben. Je nach Kritikalität der prüfenden Anwendung kann die TSL-Grace-Period damit zwischen 0 .. 30 Tagen gewählt werden.

Wird der TUC mit dem Wert „0" aufgerufen, kann die Bedingung für Validity-Warning-1 nicht erfüllt werden, so dass die TSL mit Überschreitung des „nextUpdate" auf jeden Fall als „ungültig" mit der Rückmeldung „VALIDITY_WARNING_2" reklamiert wird. Damit gilt:

1. OK: nextUpdate > aktuelles Datum
2. VALIDITY_WARNING_1: nextUpdate < aktuelles Datum < (nextUpdate + TSL-Grace-Period)
3. VALIDITY_WARNING_2: nextUpdate < aktuelles Datum > (nextUpdate + TSL-Grace-Period)

Wird VALIDITY_WARNING_2 geworfen, ist der gültige Vertrauensraum der TI nicht verfügbar, d. h. die TSL-Informationen im System sind nicht mehr vertrauenswürdig.

Der Vertrauensraum muss deaktiviert werden und bis zu dessen Re-Etablierung (Import einer gültigen TSL-Datei) darf keine Zertifikatsprüfung „gültig" ergeben.

Dies kann z. B. durch Leeren des Truststores (Löschen der Zertifikate) erfolgen.

GS-A_5336 - Zertifikatsprüfung nach Ablauf TSL-Graceperiod
Die Produkttypen der TI-Plattform, die Zertifikate prüfen, MÜSSEN nach zeitlichem Ablauf der TSL-Graceperiod oder spätestens ab dem Zeitpunkt der darauf folgenden Prüfung der Aktualität der TSL (TUC_PKI_019) die TSL selbst als nicht mehr gültig bewerten (das TSL-Update-Prüfintervall wird in Tab_PKI_294 festgelegt).
Es steht somit keine valide Basis zur Prüfung von Zertifikaten zur Verfügung.
Die Produkttypen der TI-Plattform, die Zertifikate prüfen, MÜSSEN sicherstellen, dass nach zeitlichem Ablauf der TSL-Graceperiod die Zertifikatsprüfung in der TI (TUC_PKI_018) nicht als positiv bewertet wird. Dies gilt unabhängig vom letzten bekannten Status des (ausstellenden) CA-Zertifikats.

[<=]

Um den regelmäßigen Download der TSL effizient zu gestalten, wird neben der eigentlichen Bereitstellung der TSL-Datei auch jeweils ein SHA256-Hash der TSL-Datei bereitgestellt. Damit kann von TSL-auswertenden Komponenten auf den täglichen Download der TSL verzichtet werden, wenn anhand des zuvor geprüften Hashes festgestellt wird, dass die am Download-Punkt verfügbare TSL identisch mit der zuvor schon eingelesenen und verwendeten TSL ist.

A_17690 - Nutzung der Hash-Datei für TSL (ECC-Migration)
Die Produkttypen der TI, die Zertifikate validieren, und dafür die TSL verwenden, KÖNNEN vorab die Hash-Datei der TSL herunterladen, um zu prüfen, ob die am TSL-Downloadpunkt verfügbare TSL eine andere ist, als die schon zuvor heruntergeladene und bereits ausgewertete TSL. Entspricht der Hash-Wert am Download-Punkt (vgl. [gemSpec_TSL]#6.3.1.2) der bereits heruntergeladenen und ausgewerteten TSL, KANN auf den Download verzichtet werden.
[<=]

GS-A_4648 - TUC_PKI_019: Prüfung der Aktualität der TSL
Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_019 zur Prüfung der Aktualität der TSL umsetzen.
[<=]

Tabelle 82: TUC_PKI_019 „Prüfung der Aktualität der TSL“

Element	Beschreibung
Name	TUC_PKI_019 „Prüfung der Aktualität der TSL“
Beschreibung	Das System überprüft (standardmäßig täglich) die Aktualität der TSL. Dies geschieht bei Vorhandensein eines TSL-Hashwertes zunächst anhand eines Vergleichs der TSL-Hashwerte im System und auf dem TSL-Downloadpunkt. Nachfolgend erfolgt ein Vergleich der TSL aus dem System und der TSL aus dem Download: Die jeweilige ID und die jeweilige Sequenznummer der beiden TSL werden dabei verglichen.
Anwendungsumfeld	System, das die TSL auswertet
Vorbedingungen	Eine geprüfte TSL im System
Auslöser	TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“
Eingangsdaten	TSL im System, Hashwert-Datei der TSL im System (optional), neue (nicht über TSL-Download) eingebrachte TSL-Datei (optional), TSL-Grace-Period
Komponenten	System
Ausgangsdaten	Status der Prüfung
Referenzen	[ETSI_TS_102_231]

Standardablauf	1. [System:] System lädt die aktuelle TSL-Datei herunter (TUC_PKI_016 "Download der TSL-Datei"). Im Folgenden wird diese als neue TSL-Datei bezeichnet. 2. [System:] Neue TSL-Datei wird validiert (TUC_PKI_020 „XML-Dokument validieren“) Das entsprechende von der gematik benannte Schema muss verwendet werden. 3. [System:] Das TSL-Signer-Zertifikat der neuen TSL-Datei wird geprüft. (TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“). 4. [System:] Die Signatur der neuen TSL-Datei muss geprüft werden (TUC_PKI_012 „XML-Signatur-Prüfung“) 5. [System:] Aus der TSL im System und der neuen TSL-Datei werden die jeweilige ID und das jeweilige TSLSequenceNumber-Element selektiert. 6. [System:] System prüft die ID-Attribute und das TSLSequenceNumber-Element aus Schritt 5 auf Gleichheit. Sind sie identisch, muss keine Aktualisierung erfolgen. 7. [System:] Prüfung, ob die TSL im System noch aktuell ist. Dies geschieht anhand des aktuellen Datums und des Elements „NextUpdate“ aus der TSL. Eine TSL wird als aktuell bezeichnet, wenn ihr NextUpdate in der Zukunft liegt. 8. [System:] TSL im System ist gültig. Ende des Use Case mit entsprechender Rückmeldung

Varianten/Alternativen	1a. [System:] Wenn eine TSL-Datei als Eingangsparameter eingebracht wurde, dann wird diese TSL-Datei verwendet, und es erfolgt kein Download. Im Folgenden wird diese neu eingebrachte TSL als neue TSL-Datei bezeichnet. 1b. [System:] Wenn ein TSL-Hashwert als Eingangsparameter im System vorhanden ist, wird die aktuelle Hashwert-Datei der TSL vom TSL Downloadpunkt heruntergeladen. Dazu wird der TSL-Downloadpunkt ermittelt (TUC_PKI_017 „Lokalisierung TSL Download-Adressen“) und von der emittelten URI statt der Datei mit Endung „*.xml“ die Datei mit Endung „*.sha2“ heruntergeladen. 1b1. [System:] Ist der heruntergeladene TSL-Hashwert mit dem Hashwert der aktuell im System gespeicherten TSL identisch, dann wird die im System vorhandene TSL–Datei weiter verwendet und es erfolgt kein TSL-Download. Es wird mit Schritt 7 fortgefahren. 1b2. [System:] Falls die Hashwerte verschieden sind oder im System noch kein TSL-Hashwert vorhanden ist, muss eine neue TSL-Datei heruntergeladen werden. Es wird die neue TSL-Hashwert-Datei im System gespeichert und mit Schritt 1 fortgefahren. Variante 1a kann hier nicht wiederholt werden. 6a. [System:] Die ID-Attribute aus Schritt 5 sind nicht gleich und das TSLSequenceNumber-Element der TSL im System ist kleiner als die der neuen TSL. Somit ist die TSL im System älter als die die neue TSL. 6a1. [System:] Rückmeldung an den aufrufenden Use Case (TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“)

Fehlerfälle	6b. [System:] Keine der beschriebenen Varianten des Vergleichs der ID und SequenceNumber tritt ein. Ende des Use Case mit Fehlermeldung (TSL_ID_INCORRECT) 7a. [System:] Die Aktualitäts-Prüfung ergibt, dass die TSL im System abgelaufen ist (nextUpdate < aktuelles Datum). Das aktuelle Datum liegt aber innerhalb der TSL-Grace-Period (aktuelles Datum < nextUpdate + TSL-Grace-Period). Warnung (VALIDITY_WARNING_1) mit der entsprechenden Meldung. (Die TSL ist nicht mehr aktuell.) Rückmeldung des Warnhinweises. 7a1. [System:] Die Aktualitäts-Prüfung ergibt, dass die TSL-Grace-Period überschritten ist (aktuelles Datum > nextUpdate + TSL-Grace-Period). Warnung (VALIDITY_WARNING_2) mit der entsprechenden Meldung, (Ablauf der TSL-Grace-Period, die TSL im System ist nicht mehr vertrauenswürdig und darf nicht als valide Prüfbasis verwendet werden, s. [GS-A_5336]). Rückmeldung des Warnhinweises. Weitere Fehlerfälle sind in den referenzierten Use Cases beschrieben.
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.

Anmerkungen	Die ID der TSL-Datei befindet sich als Attribut im Root-Tag des XML-Dokuments.
	`<xsd:attribute name="Id" type="xsd:ID" use="optional"/>`
	Das Attribut Id wird vom TSL-Service-Provider immer gefüllt.
	`Das Element TSLSequenceNumber beschreibt die Folgenummer der TSL. Sein erstmaliger Inhalt der TSL(RSA) ist gleich 1 und wird jeweils um 1 hoch gezählt. Der erstmalige Wert der TSL(ECC-RSA) ist 10000.`

Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_019 "Prüfung der Aktualität der TSL". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

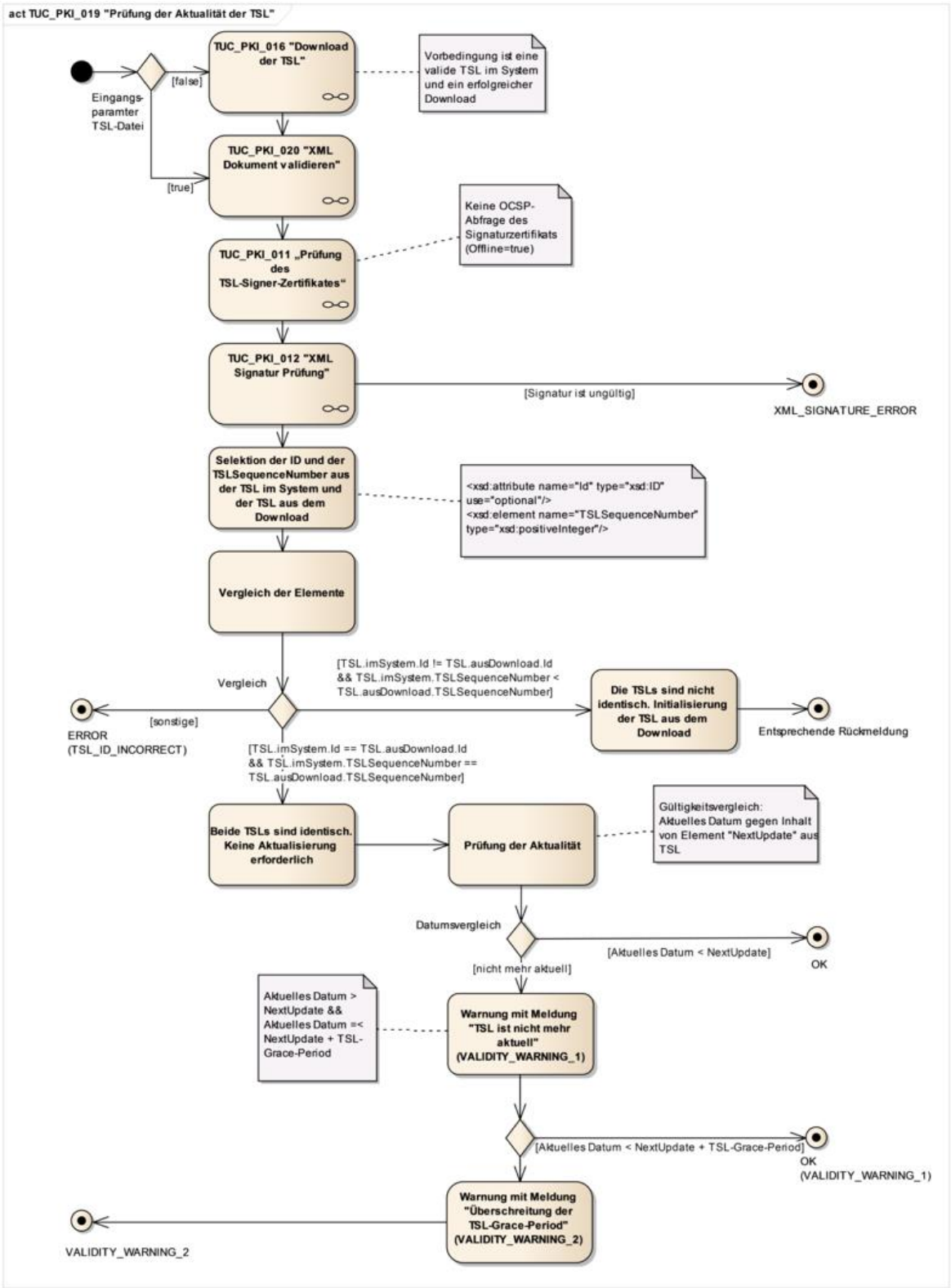


Abbildung 11: Aktivitätsdiagramm TUC_PKI_019 „Prüfung der Aktualität der TSL“

8.2.2.2 TUC_PKI_020 „XML-Dokument validieren"

GS-A_4649 - TUC_PKI_020: XML-Dokument validieren
Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_020 zur Validierung eines XML-Dokumentes umsetzen.
[<=]

Tabelle 83: TUC_PKI_020 „XML-Dokument validieren"

Element	Beschreibung
Name	TUC_PKI_020 „XML-Dokument validieren"
Beschreibung	Ein XML-Dokument wird gegen ein XML-Schema validiert.
Anwendungsumfeld	Dieser Use Case wird verwendet, um XML-Dokumente zu validieren. In diesem Dokument betrifft das die Validierung der TSL.
Vorbedingungen	Eine vollständig vorliegende TSL-Datei im XML-Format
Auslöser	TUC_PKI_019 „Prüfung der Aktualität der TSL"
Eingangsdaten	TSL-Datei und TSL-XML-Schema (und alle in ihm referenzierten Schemata). Das System muss sicherstellen, dass zur Validierung nur das von der gematik spezifizierte bzw. benannte Schema benutzt wird.
Komponenten	System
Ausgangsdaten	Entsprechendes Ergebnis der Validierung (Erfolg | Misserfolg)
Referenzen	[XML]
Standardablauf	Das System prüft die Wohlgeformtheit des Dokumentes und validiert es gegen das Schema. 1. [System:] System startet Prüfung der TSL-Datei. 2. [System:] System prüft Wohlgeformtheit der TSL-Datei. 3. [System:] System validiert die TSL-Datei gegen die Schemata. 4.

	[System:] Ende des Use Case mit positivem Ergebnis
Fehlerfälle	Die übergebenen Schemata könnten selbst invalide oder unvollständig sein. 2a. [System:] Ende des Use Case mit Fehlermeldung (TSL_NOT_WELLFORMED) 3a. [System:] Ende des Use Case mit Fehlermeldung (TSL_SCHEMA_NOT_VALID)

8.2.2.3 TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates"

GS-A_4650 - TUC_PKI_011: Prüfung des TSL-Signer-Zertifikates
Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_011 zur Prüfung des TSL-Signer-Zertifikats umsetzen.
[<=]

Tabelle 84: TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates"

Element	Beschreibung
Name	TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates"
Beschreibung	Es wird der Prozess zur Prüfung des TSL-Signer-Zertifikates gegen ein sicher verwahrtes TSL-Signer-CA-Zertifikat spezifiziert. Der Prozess verläuft analog demjenigen für Zertifikatsprüfung im Allgemeinen (TUC_PKI_018 "Zertifikatsprüfung in der TI "), berücksichtigt aber die Besonderheiten des TSL-Signer-Zertifikates. Außerdem erfolgt hier keine Statusprüfung des TSL-Signer-Zertifikates. (Der Aufruf von TUC_PKI_006 „OCSP-Abfrage" erfolgt in TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum".)
Anwendungsumfeld	System, das die TSL verwendet
Vorbedingungen	TSL-Signer-CA-Zertifikat in einem sicheren Speicher des Systems
Auslöser	TUC_PKI_019 „Prüfung der Aktualität der TSL"

Eingangsdaten	• TSL-Datei • Referenzzeitpunkt (Datum optional; bei Nichtangabe Verwendung der aktuellen Systemzeit)
Komponenten	System
Ausgangsdaten	Status der Prüfung
Referenzen	[ETSI_TS_102_231], [XMLSig]
Standardablauf	1. [System:] Das verwendete TSL-Signer-Zertifikat wird aus der TSL-Datei extrahiert. 2. [System] Der Use Case TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats" wird durchlaufen. 3. [System:] Prüfung der Extension KeyUsage auf vorhanden sein. Zudem wird die KeyUsage auf die richtige Belegung (nonRepudiation) geprüft. Weiter wird die ExtendedKeyUsage auf die richtige Belegung mit {id-tsl-kp-tslSigning} geprüft (vgl. Kap. 5.13.1 TSL-Signer-Zertifikat). 4. [System:] Das TSL-Signer-CA-Zertifikat aus dem sicheren Speicher des Systems wird geladen. 5. [System:] Anhand dieses CA-Zertifikates wird die mathematische Prüfung der Signatur des TSL-Signer-Zertifikats durchgeführt (TUC_PKI_004 "Mathematische Prüfung der Zertifikatssignatur"). (Jedes System muss Initial dieses CA-Zertifikat als TI-Vertrauensanker auf sicherem Wege integrieren.) 6. [System:] Ende des Use Case mit Status Rückmeldung
Varianten/Alternativen	

Fehlerfälle	1a. [System:] Das TSL-Signer-Zertifikat lässt sich nicht aus der TSL-Datei extrahieren (TSL_CERT_EXTRACTION_ERROR). 3a. [System:] KeyUsage ist nicht vorhanden bzw. entspricht nicht der vorgesehenen KeyUsage (WRONG_KEYUSAGE). 3a1. [System:] ExtendedKeyUsage entspricht nicht der vorgesehenen ExtendedKeyUsage (WRONG_EXTENDEDKEYUSAGE). 4a. [System:] Das TSL-Signer-CA-Zertifikat kann nicht aus dem sicheren Speicher des Systems geladen werden (TSL_CA_NOT_LOADED). Fehlerfälle sind in den referenzierten Use Cases beschrieben.
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	Die Gestaltung des sicheren Speichers des Systems ist durch den Betreiber des Systems auszuarbeiten. TUC_PKI_018 "Zertifikatsprüfung in der TI "fordert zusätzlich die Ermittlung von Autorisierungsinformationen. Dies wird im vorliegenden Use Case nicht benötigt und kann entfallen. Der Aufruf von TUC_PKI_006 "OCSP-Abfrage erfolgt nicht hier, sondern in TUC_PKI_001 "Periodische Aktualisierung TI-Vertrauensraum".
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_011 "Prüfung des TSL-Signer-Zertifikates". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

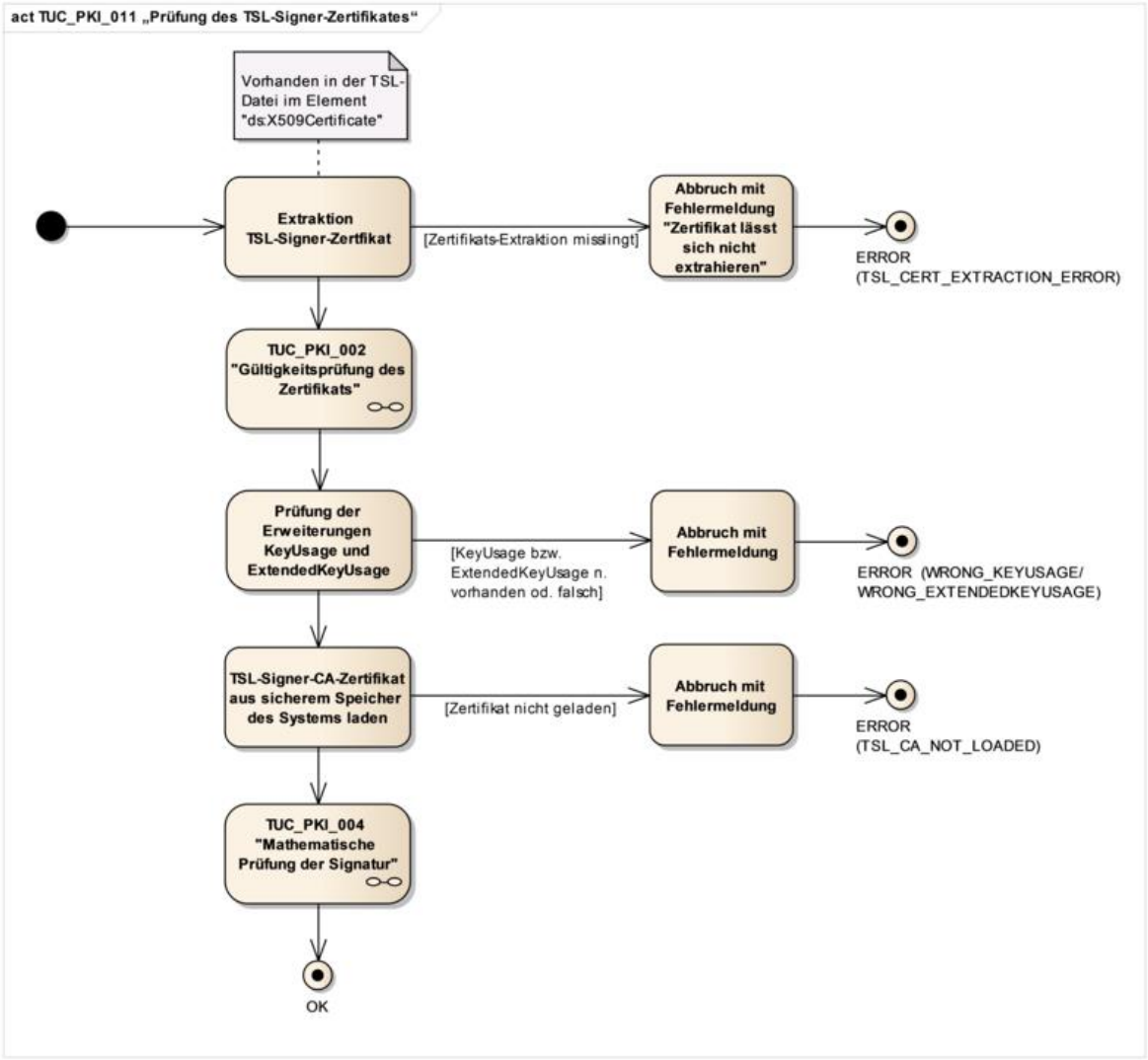


Abbildung 12: Aktivitätsdiagramm TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“

8.2.2.4 TUC_PKI_012 „XML-Signatur-Prüfung“

GS-A_4651 - TUC_PKI_012: XML-Signatur-Prüfung

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

[<=]

Tabelle 85: TUC_PKI_012 „XML-Signatur- Prüfung“

Element	Beschreibung
Name	TUC_PKI_012 „XML-Signatur-Prüfung“

Beschreibung	In diesem Use Case wird die Prüfung der XML-Signatur der TSL beschrieben. Die Prüfung wird nicht näher spezifiziert, sondern richtet sich nach den Vorgaben und Standards von W3C.
Anwendungsumfeld	Dieser Use Case umfasst die Prüfung der XML-Signatur und wird durch jedes System verwendet, das eine XML-Signatur prüfen muss.
Vorbedingungen	(Valide) TSL-Datei mit Signatur: Die TSL-Datei wurde Schema-validiert (TUC_PKI_020) Das Signaturzertifikat dieser TSL-Datei muss erfolgreich geprüft worden sein. (TUC_PKI_011).
Auslöser	TUC_PKI_019 „Prüfung der Aktualität der TSL"
Eingangsdaten	signierte XML-Datei und Signaturzertifikat
Komponenten	System
Ausgangsdaten	Status der Prüfung
Referenzen	[XMLSig]
Standardablauf	Der Ablauf richtet sich nach den Vorgaben von W3C.
Fehlerfälle	[System:] Die Signatur ist nicht gültig. Ende des Use Case. Abbruch mit Fehlermeldung (XML_SIGNATURE_ERROR)
Anmerkungen	Vorgaben für die verwendeten Algorithmen und Schlüssellängen der Signatur werden hier nicht getroffen. Siehe dazu [gemSpec_Krypt#GS-A_4371].

8.2.3 TSL-Sicherheitsaspekte

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

8.2.4 TSL-Zeitparameter

GS-A_4897 - Gültigkeitsdauer einer TSL
Der TSL-Dienst MUSS die Gültigkeitsdauer der TSL gemäß Tab_PKI_294 umsetzen.
Der TSL-Dienst MUSS den Zeitpunkt des resultierenden Gültigkeitsendes der TSL innerhalb des Elementes NextUpdate in der TSL-Datei eintragen.
[<=]

GS-A_4898 - TSL-Grace-Period einer TSL
Produkttypen der TI, die die TSL zur Validierung des TI-Vertrauensraums einsetzen, MÜSSEN die TSL-Grace-Period gemäß Tab_PKI_294 umsetzen.
[<=]

GS-A_4899 - TSL Update-Prüfintervall
Produkttypen der TI, die die TSL zur Validierung des TI-Vertrauensraums einsetzen, MÜSSEN gemäß den in Tab_PKI_294 festgelegten TSL-Update Intervall prüfen, ob eine aktuellere als die vom System verwendete TSL bereitgestellt wurde.
[<=]

GS-A_5214 - TSL Neuausstellung
Der TSL-Dienst MUSS mindestens 7 Tage vor Ablauf der Gültigkeit der TSL eine neue Version der TSL erstellen.
[<=]

Tabelle 86: Tab_PKI_294 TSL Zeitparameter

Beschreibung	Zeitparameter
Gültigkeitsdauer einer TSL	Ausstellungsdatum + 30 Tage
TSL-Grace-Period für zentrale Dienste und fachanwendungsspezifische Dienste mit Anschluss an das zentrale Netz	0 Tage
TSL-Grace-Period für sonstige Dienste und Komponenten	0-30 Tage
TSL Update-Prüfintervall	24 Stunden

8.2.5 ServiceTypeIdentifier "unspecified"

Die Auswertung der TSL in der TI basiert auf [ETSI_TS_102_231_v3.1.2]. Dort wird der ServiceTypeIdentifier " http://uri.etsi.org/TrstSvc/Svctype/unspecified" definiert. Eine Komponente oder ein Dienst der TI muss also mit solch einem Identifier umgehen können. Um diesen Punkt jedoch noch deutlicher sichtbar zu machen wird er mit einer Anforderung in den Vordergrund gestellt.

A_17700 - TSL-Auswertung ServiceTypeIdentifier "unspecified"
Alle Produkttypen der TI, die die TSL auswerten, MÜSSEN TSPService-Einträge verarbeiten können mit dem ServiceTypeIdentifier " http://uri.etsi.org/TrstSvc/Svctype/unspecified". Die Auswertung der TSL darf also nicht fehlschlagen wenn ein solcher ServiceTypeIdentifier in der TI vorgefunden wird.

[<=]

8.3 Zertifikatsprüfung X.509 nonQES

Für die Prüfung der X.509-Zertifikate gelten folgende Vorbedingungen (s. Kapitel 8.1 und 8.2):

- aktuelle TSL liegt vor
- TSL-Datei wurde geprüft
- Der TI-Vertrauensraum wurde initialisiert, der Truststore kann benutzt werden.

Die folgende Use Case Übersicht verdeutlicht die Aktionen des Systems.

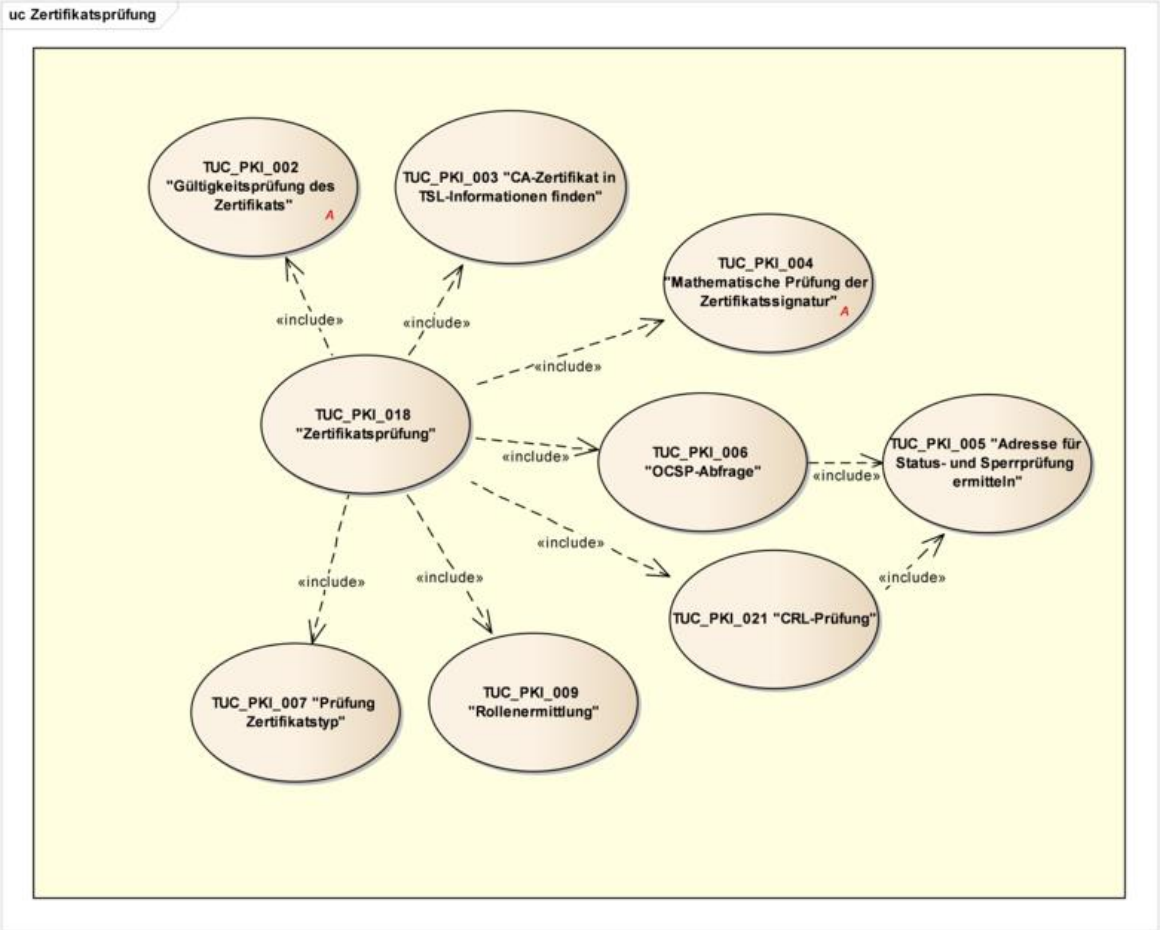


Abbildung 13: Use Case Diagramm „Zertifikatsprüfung"

Die folgenden Schritte sind für eine nonQES-Zertifikatsprüfung durchzuführen:

- Prüfung der Gültigkeit (TUC_PKI_002)
- Prüfung der Identität des Zertifikatsherausgebers (TUC_PKI_003)
- Prüfung der mathematischen Korrektheit des Zertifikats (Signaturprüfung) (TUC_PKI_004)

- Abfrage des Sperrstatus des zu prüfenden Zertifikats gegen den im „ServiceSupplyPoint" der TSL eingetragenen OCSP-Responder (TUC_PKI_006) und Prüfung der OCSP-Antwort (Responder-Zertifikat, Sperrstatus)
- Rollenermittlung (TUC_PKI_009)
- Prüfung Zertifikatstyp (TUC_PKI_007)

Bei jeder dieser Prüfungen muss nicht nur die mathematisch-kryptographische Korrektheit der jeweiligen Mechanismen, sondern auch deren Zulässigkeit mit in die Prüfung einbezogen werden. Zum Beispiel darf ein Zertifikat, welches nicht mit einem zugelassenen Hash-Algorithmus signiert ist, nie als gültig eingestuft werden. Für die TI gültige Hash-Algorithmen siehe [gemSpec_Krypt].

Die Verwendung von Informationen aus Zertifikaten kann nur dann erfolgen, wenn das zugehörige Zertifikat validiert wurde. Somit MUSS eine Zertifikatsprüfung der Ermittlung bestätigter Zertifikatsinformationen vorangehen.

In dem Dokument wird der Begriff „gültiger Zeitraum" verwendet. Dieser bedeutet, dass sich der aktuelle Zeitpunkt innerhalb des Gültigkeitszeitraums des Objektes befindet.

Die Fachdokumente müssen die entsprechenden Eingangsparameter der Use Cases berücksichtigen. Die Festlegungen aus den Standards [RFC6960], [RFC5280], [RFC5019] und [RFC3370/5754] sowie TI-spezifische Vorgaben der gematik sind für die Zertifikatsprüfung verbindlich.

8.3.1 Zertifikatsprüfung in der TI

8.3.1.1 TUC_PKI_018 „Zertifikatsprüfung in der TI"

GS-A_4652-01 - TUC_PKI_018: Zertifikatsprüfung in der TI
Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_018 zur Zertifikatsprüfung umsetzen

Tabelle 87: TUC_PKI_018 „Zertifikatsprüfung in der TI"

Element	Beschreibung
Name	TUC_PKI_018 „Zertifikatsprüfung"
Beschreibung	Dieser Use Case beschreibt die Prüfung nicht-qualifizierter Zertifikate und umfasst die Offline- wie Online-Prüfung.
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	Eine zeitlich nicht abgelaufene TSL (innerhalb der TSL-Graceperiod) steht als valide Basis zur Prüfung von Zertifikaten zur Verfügung
Auslöser	Zertifikats-Check

Eingangsdaten	• Das zu prüfende Zertifikat • Referenzzeitpunkt: Zeitpunkt, für den das Zertifikat geprüft werden soll (optional; bei Nichtangabe Verwendung der aktuellen Systemzeit): Zeitpunkt, für den das Zertifikat geprüft werden soll, s. a. Glossar aus Kap. 11.2 • PolicyList Liste der im aktuellen Aufruf zulässigen Zertifikatstyp-OIDs. Die Liste muss mindestens eine OID enthalten. • Vorgesehene KeyUsage (intendedKeyUsage, mehrere Werte möglich) • Vorgesehene ExtendedKeyUsage (intendedExtendedKeyUsage, mehrere Werte möglich) • OCSP-Graceperiod (legt bei der Verwendung von (gecachten) OCSP-Antworten den maximal zulässige Zeitraum fest, den die Systemzeit der prüfenden Komponente noch nach dem Zeitpunkt der OCSP-Antwort liegen darf (Default: 10 min) • Offline-Modus (ja/nein) • Beigefügte OCSP-Response zum angefragten Zertifikat (optional; z. B. in der Signatur eingebettet) • Timeout-Parameter (Default: 10s) • TOLERATE_OCSP_FAILURE (true/false, Default: false) - Der Parameter definiert das Verhalten für den Fall, dass die OCSP-Prüfung nicht durchgeführt werden konnte, weil der OCSP-Responder beispielsweise technisch nicht erreichbar ist. • Prüfmodus (OCSP, CRL)
Komponenten	System, OCSP-Responder
Ausgangsdaten	Status der Prüfung, OCSP-Response, im Zertifikat enthaltene Rollen-OIDs

Referenzen	[RFC5280] Kap. 6.1, [X.509] Referenzierte Standards in den aufzurufenden TUCs
Standardablauf	Die Zertifikatsprüfung setzt sich aus folgenden Schritten zusammen: 1. [System] Die Gültigkeit des Zertifikats wird geprüft (TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats") . 2. [System] Prüfung der Extension KeyUsage auf Vorhandensein. Zudem wird die KeyUsage und ExtendedKeyUsage (falls vorhanden) auf die richtige Belegung entsprechend der vorgesehenen (intendedKeyUsage bzw. intendedExtendedKeyUsage) KeyUsage geprüft. Die intendedKeyUsage sowie die intendedExtendedKeyUsage können aus einer Liste mehrerer erlaubter Werte bestehen. Es wird geprüft, dass die im Parameter intendedKeyUsage bzw. intendedExtendedKeyUsage übergebenen Werte eine Teilmenge der Werte in der jeweiligen Extension KeyUsage bzw. ExtendedKeyUsage des Zertifikats sind. Da die übergebenen Parameter die Verwendung des Zertifikats im Aufrufkontext widerspiegeln, ist es dabei nicht notwendig, dass diese zu den Werten in der Zertifikatsextension komplett identisch sind. Enthält ein übergebener Parameter keine Werte, so bedeutet dies, dass der Inhalt der Zertifikatsextension nicht relevant ist. 3. [System] Das passende CA-Zertifikat wird in den TSL-Informationen gesucht (TUC_PKI_003 "CA-Zertifikat in TSL-Informationen finden") 4. [System] Mathematische Prüfung der Signatur des Zertifikats (TUC_PKI_004 "Mathematische Prüfung der Zertifikatssignatur"). 5. [System] Der ServiceStatus (vgl. Tab_PKI_271) des CA-Zertifikats wird geprüft. Im Fall von „revoked“ wird der Zeitpunkt des Gültigkeitsbeginns (Feld "notBefore" gemäß [RFC5280]#4.1.2.5) des End-Entity-Zertifikats mit dem Datum

	des Statuswechsels (StatusStartingTime) verglichen. Der Zeitpunkt des Gültigkeitsbeginns des End-Entity-Zertifikats liegt vor dem Zeitpunkt des Statuswechsels. 6. [System, Prüfmodus Offline] Falls JA, weiter mit Schritt 8, sonst mit 7. 7. [System, Prüfmodus OCSP] Statusinformation zum Zertifikat durch Abfrage des zugeordneten OCSP-Dienstes ermitteln (TUC_PKI_006 "OCSP-Abfrage"). TUC_PKI_006 wird für TLS-Zertifikate der Störungsampel (C.ZD.TLS-S mit technischer Rolle oid_stamp) und nonQES-Zertifikate einer eGK mit dem Parameter ENFORCE_CERTHASH_CHECK=false aufgerufen. Für alle anderen Zertifikate wird TUC_PKI_006 mit dem Defaultwert ENFORCE_CERTHASH_CHECK=true aufgerufen. Wenn der zuständige OCSP-Responder die Statusinformation des Zertifikats mit einem Wert „revoked" oder „unknown" gemäß GS-A_4690 zurückgibt – Meldungskürzel (CERT_REVOKED) bzw. (CERT_UNKNOWN) gemäß Tab_PKI_274 oder eine wegen ENFORCE_CERTHASH_CHECK=true erforderliche certHash-Erweiterung fehlt (CERTHASH_EXTENSION_MISSING) bzw. falsch ist (CERTHASH_MISMATCH), darf das Zertifikat nicht als gültig bewertet werden. 8. [System:] Ermittlung (TUC_PKI_009 "Rollenermittlung") der Rolle 9. [System:] Prüfung, ob eine der übergebenen Zertifikatstyp-OIDs (aus der Parameter PolicyList) im Zertifikat enthalten ist (TUC_PKI_007 "Prüfung Zertifikatstyp"). Zur Prüfung muss die Liste (PolicyList s.o.) mindestens eine OID enthalten. 10. [System:] Ende des Use Cases mit Rückgabe des/der im Zertifikat enthaltenen Rollen-OID(s).

Varianten/Alternativen	6a. [System:] Der Offline-Modus ist aktiviert. Es werden keine Statusinformationen zum Zertifikat eingeholt. 7a. [System, Prüfmodus CRL] Prüfung der Sperrinformation des Zertifikates mittels CRL (TUC_PKI_021 "CRL-Prüfung"). Wenn das Zertifikat in der Sperrliste (CRL) enthalten ist – Meldungskürzel (CERT_REVOKED) gemäß Tab_PKI_274, darf das Zertifikat nicht als gültig bewertet werden. 7b [System] Eine OCSP-Response zu dem zu prüfenden Zertifikat wurde im Aufruf mit übergeben. Falls diese zum Referenzzeitpunkt gültig ist, wird nicht der TUC_PKI_006 aufgerufen, sondern die beigefügte OCSP-Response zur weiteren Prüfung verwendet.
Fehlerfälle	2a. [System:] KeyUsage ist nicht vorhanden bzw. nicht alle Werte der intendedKeyUsage in der KeyUsage enthalten (WRONG_KEYUSAGE). 2a1. [System:] intendedExtendedKeyUsage enthält Werte und nicht alle davon sind in der ExtendedKeyUsage enthalten (WRONG_EXTENDEDKEYUSAGE). 5a. [System:] Das Ausgabedatum des End-Entity-Zertifikats liegt nach dem Datum des Statuswechsels. Abbruch mit Fehlermeldung (CA_CERTIFICATE_REVOKED_IN_TSL) 7c. [System] Eine OCSP-Response zu dem zu prüfenden Zertifikat wurde im Aufruf mit übergeben, ergab bei den weiteren Prüfschritten jedoch kein gültiges Ergebnis (Überprüfung und Auswertung der Gültigkeit der OCSP-Response in TUC_PKI_006 schlägt fehl). Eine erneute Prüfung wird in diesem Fall durch Aufruf des TUC_PKI_006 durchgeführt, als wäre keine OCSP-Response beigefügt. In den Rückgabewerten dieses TUC wird die Warnmeldung

	(PROVIDED_OCSP_RESPONSE_NOT_VALID) an die aufrufende Funktion übergeben.
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	Gültige Status zu Schritt 5 sind gemäß Tab_PKI_271 inaccord, revoked und expired. Schritt 5 stellt eine Sperrprüfung des CA-Zertifikats (für nonQES-HBA- und SMC-B-Zertifikate) gemäß Ketten- bzw. Kompromissmodell dar. Vgl. Kap. 8.1.1 Initialisierung TI-Vertrauensraum. Eine Zertifikatsprüfung in der TI gemäß TUC_PKI_018 darf nach Ablauf der TSL-Graceperiod nicht positiv ausfallen (vgl. GS-A_5336).
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_018 "Zertifikatsprüfung". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

[<=]

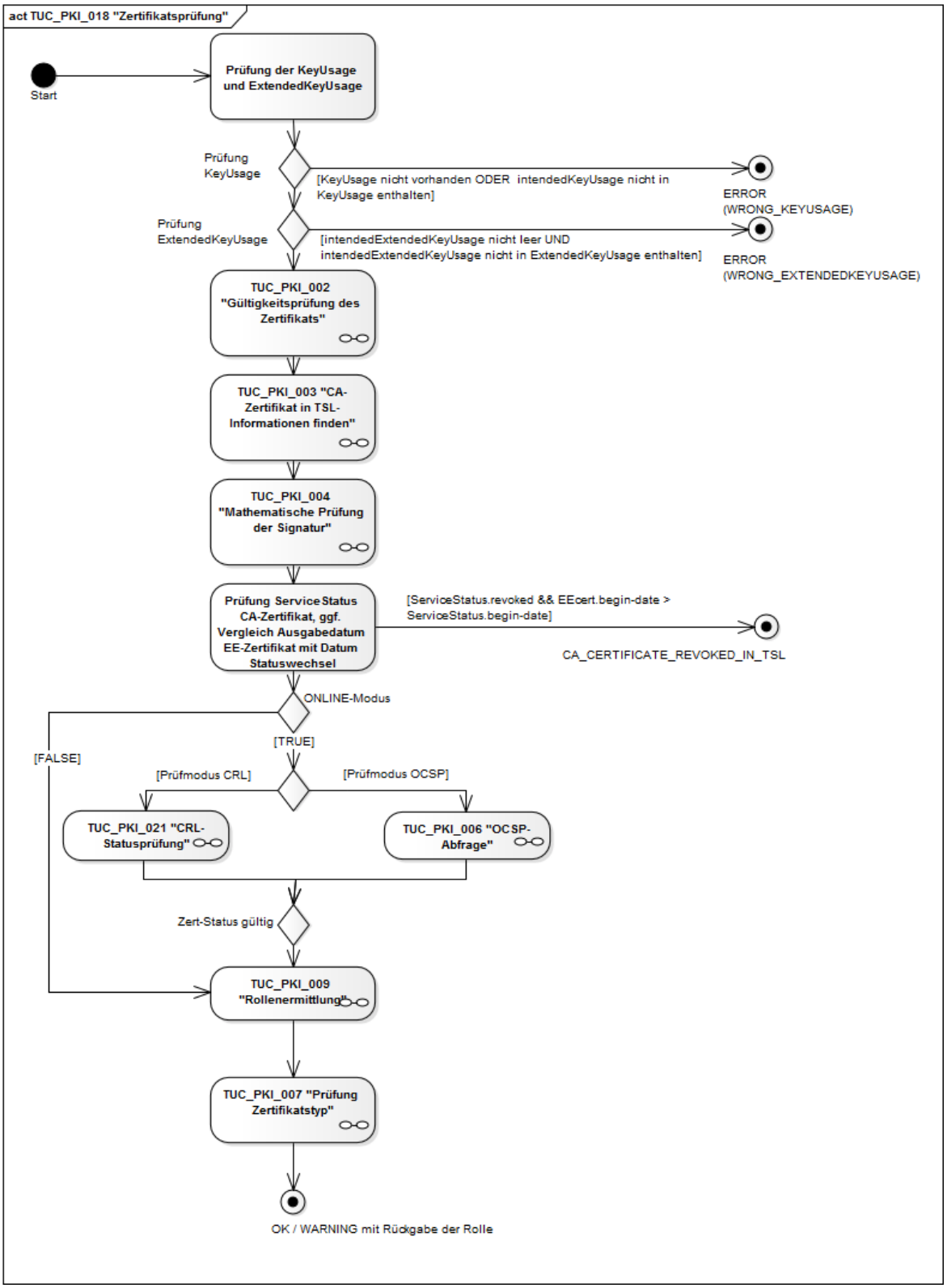


Abbildung 14: Aktivitätsdiagramm TUC_PKI_018 „Zertifikatsprüfung“

8.3.1.2 TUC_PKI_002 „Gültigkeitsprüfung des Zertifikats"

GS-A_4653-01 - TUC_PKI_002: Gültigkeitsprüfung des Zertifikats
Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_002 zur Gültigkeitsprüfung des Zertifikates umsetzen

Tabelle 88: TUC_PKI_002 „Gültigkeitsprüfung des Zertifikats"

Element	Beschreibung
Name	TUC_PKI_002 „Gültigkeitsprüfung des Zertifikats"
Beschreibung	Dieser Use Case beschreibt die Prüfung des Zertifikats auf seine aktuelle zeitliche Gültigkeit. Damit ist der Zeitraum gemeint, der im Feld *validity* steht. Die Prüfung richtet sich nach referenzierten Standards.
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	Zertifikat vorhanden
Auslöser	Zertifikatsprüfung in der TI, TUC_PKI_013 „Import TI-Vertrauensanker aus TSL", TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates", TUC_PKI_018 "Zertifikatsprüfung in der TI " TUC_PKI_030 "QES-Zertifikatsprüfung"
Eingangsdaten	• Das zu prüfende Zertifikat • Referenzzeitpunkt (optional; bei Nichtangabe Verwendung der aktuellen Systemzeit): Zeitpunkt, für den das Zertifikat geprüft werden soll, s. a. Glossar aus Kap. 11.2
Komponenten	System
Ausgangsdaten	Status der Prüfung
Referenzen	[eIDAS], [ETSI EN 319 412-5], [RFC5280]

Standardablauf	1. [System:] Zertifikat lesen 2. [System:] Aus dem Zertifikat das Feld Validity ermitteln und auslesen. 3. [System:] Anhand der ermittelten Daten wird die Gültigkeit geprüft. Dabei kommt folgender Algorithmus zu tragen: notBefore =< Referenzzeitpunkt && notAfter >= Referenzzeitpunkt entspricht einem zeitlich gültigen Zertifikat. Details siehe [RFC5280] Kap. 4.1.2.5 und 6.1.3 4. [System:] Rückmeldung des Status
Fehlerfälle	1a. [System:] Zertifikat ist nicht lesbar (CERT_READ_ERROR). 3a. [System:] Prüfzeitpunkt nicht innerhalb der Gültigkeitsdauer des Zertifikats (CERTIFICATE_NOT_VALID_TIME).
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	Der Aufbau der Gültigkeit: wird nicht näher spezifiziert, sondern richtet sich nach referenzierten Standards. Die (zeitliche) Gültigkeitsprüfung ist nach [eIDAS] Artikel 28 Satz (1) auch für die QES-Zertifikatsprüfung gemäß TUC_PKI_030 verpflichtend.
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_002 Gültigkeitsprüfung des Zertifikats. Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

[<=]

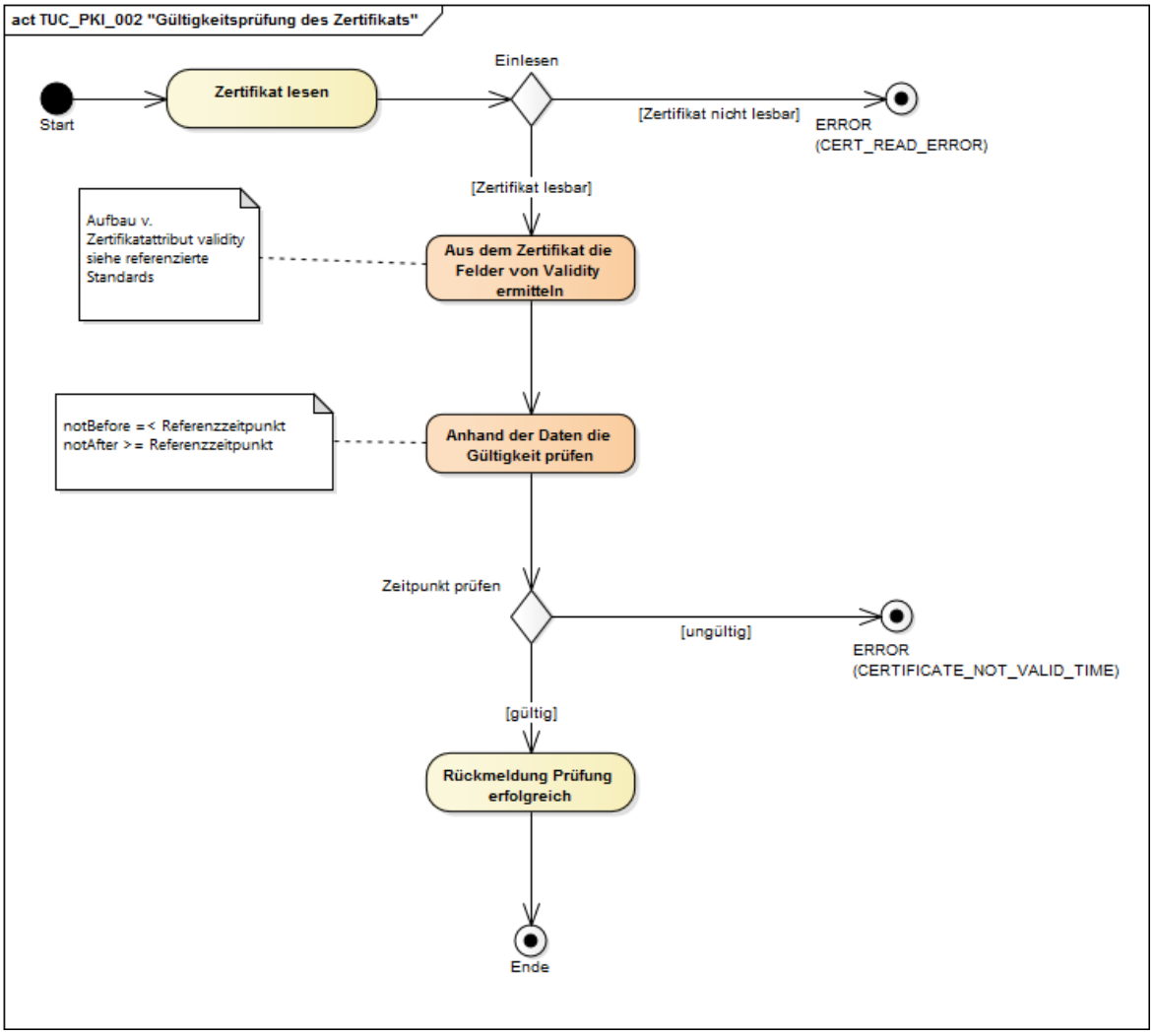


Abbildung 15: Aktivitätsdiagramm TUC_PKI_002 Gültigkeitsprüfung des Zertifikats

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

GS-A_4654-01 - TUC_PKI_003: CA-Zertifikat finden
Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_003 zur Ermittlung des CA-Zertifikats aus den TSL-Informationen umsetzen

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

Element	Beschreibung
Name	TUC_PKI_003 „CA-Zertifikat in TSL-Informationen finden“
Beschreibung	Anhand der Daten aus dem Zertifikat wird versucht das CA-Zertifikat in der TSL zu finden.

Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	Zertifikat innerhalb des definierten Gültigkeitszeitraums Eine TSL mit gültiger Signatur
Auslöser	TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln", TUC_PKI_018 "Zertifikatsprüfung in der TI "
Eingangsdaten	End-Entity-Zertifikatsdaten, TSL-Informationen
Komponenten	System
Ausgangsdaten	Status der Prüfung, (Referenz auf) CA-Zertifikat
Referenzen	[ETSI TS 102 231]
Standardablauf	1. [System:] Anhand der End-Entity-Zertifikatsdaten werden die TSL-Informationen durchsucht, um das passende CA-Zertifikat zu finden. Details siehe [ETSI TS 102 231] Kap. 5.5.1 und D.2. 2. [System:] Vergleich 1: IssuerDN des End-Entity-Zertifikats mit dem subjectDN des CA-Zertifikats 3. [System:] Vergleich 2: AuthorityKeyIdentifier des End-Entity-Zertifikats mit SubjectKeyIdentifier des CA-Zertifikats 4. [System:] Selektion (Referenz auf) CA-Zertifikat und Rückgabe
Varianten/Alternativen	2a. [System:] Keine Übereinstimmung. Der Vorgang wird mit einem anderen CA-Zertifikat wiederholt (Iteration)

Fehlerfälle	2b. [System:] Ende der Liste erreicht UND keine Übereinstimmung im DN gefunden. Abbruch des TUC mit Fehlermeldung (CA_CERT_MISSING) 3a. [System:] CA mit passendem DN gefunden, aber Ausstellerschlüssel (SubjectKeyIdentifier) und die Referenz (AuthorityKeyIdentifier) stimmen nicht überein. Abbruch des TUC mit Fehlermeldung (AUTHORITYKEYID_DIFFERENT)
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_003 CA-Zertifikat in TSL-Informationen finden. Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

[<=]

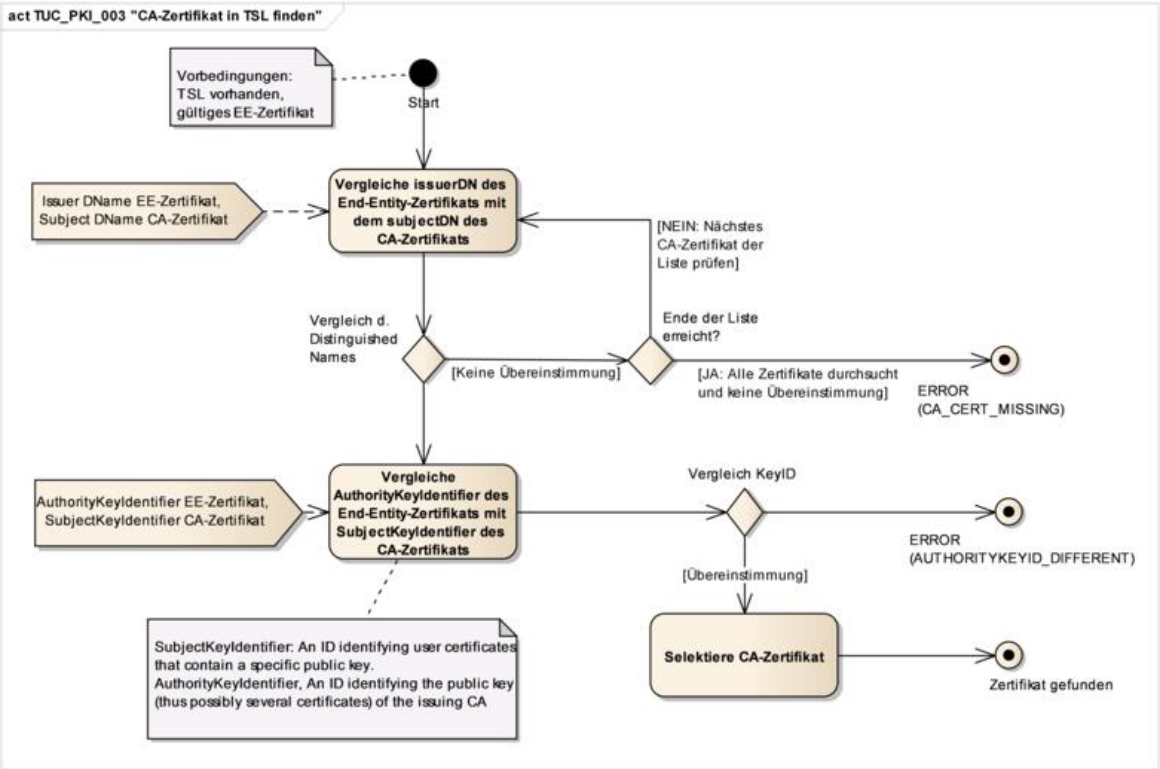


Abbildung 16: Aktivitätsdiagramm TUC_PKI_003 CA-Zertifikat in TSL-Informationen finden

8.3.1.4 TUC_PKI_004 „Mathematische Prüfung der Zertifikatssignatur"

GS-A_4655-01 - TUC_PKI_004: Mathematische Prüfung der Zertifikatssignatur
Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_004 zur mathematischen Prüfung der Zertifikatssignatur umsetzen

Tabelle 90: TUC_PKI_004 „Mathematische Prüfung der Zertifikatssignatur"

Element	Beschreibung
Name	TUC_PKI_004 „Mathematische Prüfung der Zertifikatssignatur"
Beschreibung	Dieser Use Case beschreibt die mathematische Prüfung der Signatur des End-Entity-Zertifikats mit Hilfe des CA-Zertifikats.
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	Gültiges CA-Zertifikat und passendes End-Entity-Zertifikat innerhalb des definierten Gültigkeitszeitraums

Auslöser	TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“, TUC_PKI_013 „Import TI-Vertrauensanker aus TSL“, TUC_PKI_018 "Zertifikatsprüfung in der TI "
Eingangsdaten	End-Entity-Zertifikat, CA-Zertifikat
Komponenten	System
Ausgangsdaten	Status der Prüfung
Referenzen	[RFC5280]
Standardablauf	1. [System:] Auswahl des öffentlichen Schlüssels des CA-Zertifikats 2. [System:] Die Signatur und der verwendete Algorithmus werden aus dem End-Entity-Zertifikat ausgelesen 3. [System:] Verifikation der Signatur und Hashwert-Vergleich (Verfahren siehe [RFC5280] Kap. 6.1) 4. [System:] Rückmeldung an das System
Fehlerfälle	3a. [System:] Die Zertifikats-Signatur ist nicht gültig. Ende des Use Case. Abbruch mit Fehlermeldung (CERTIFICATE_NOT_VALID_MATH)
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	signatureAlgorithm AlgorithmIdentifier: Stellt den verwendeten Signatur-Algorithmus dar, den die CA benutzt hat, um das Zertifikat zu signieren. signature BIT STRING: Die Signatur des Zertifikats.
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_004 Mathematische Prüfung der Zertifikatssignatur. Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

[<=]

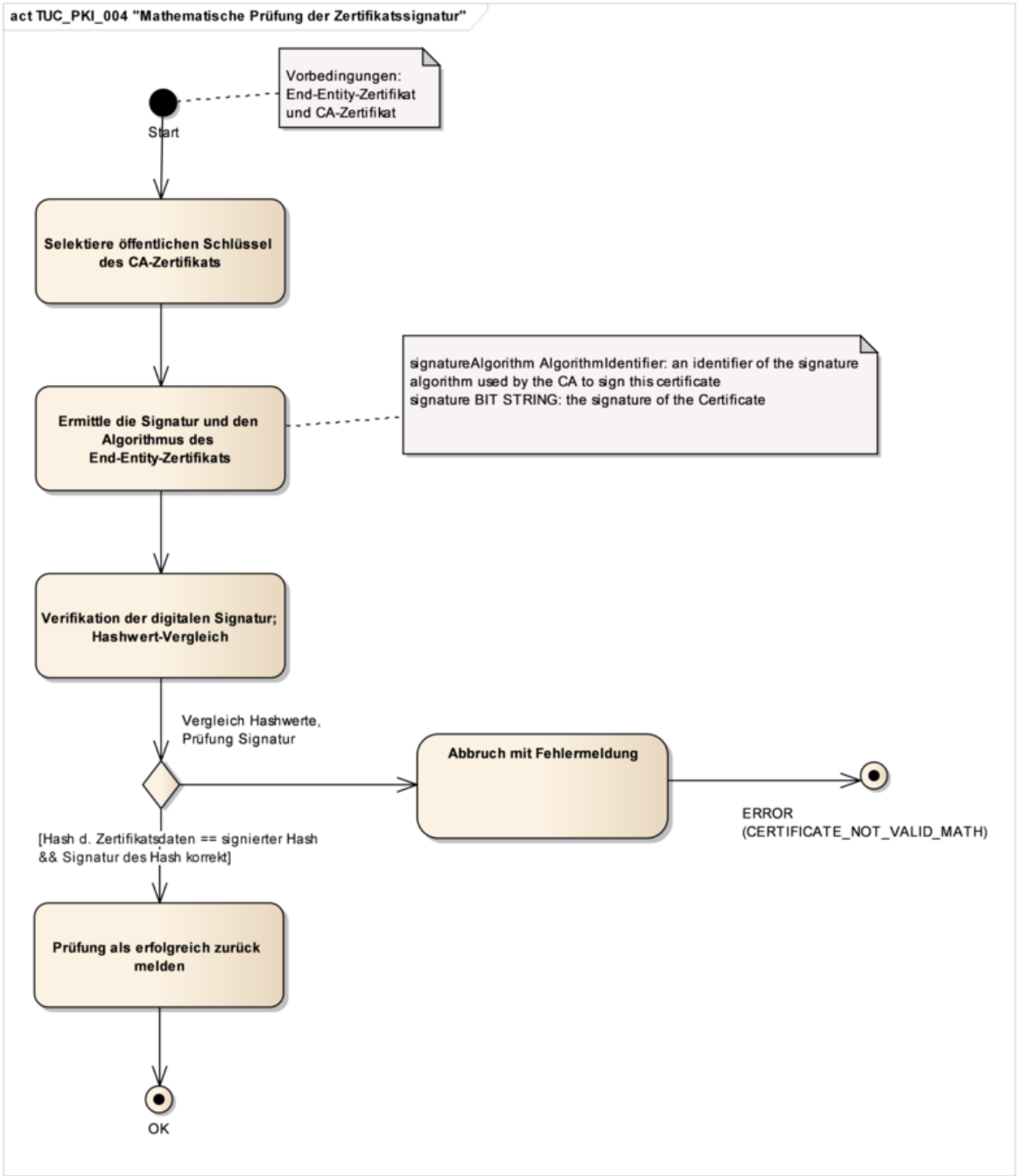


Abbildung 17: Aktivitätsdiagramm TUC_PKI_004 Mathematische Prüfung der Zertifikatssignatur

8.3.2 Statusprüfung

8.3.2.1 TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln"

GS-A_4656 - TUC_PKI_005: Adresse für Status- und Sperrprüfung ermitteln
Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_005 zur Ermittlung der Adresse für Status- und Sperrprüfung umsetzen.
[<=]

Tabelle 91: TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln"

Element	Beschreibung
Name	TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln"
Beschreibung	In diesem Use Case wird die Ermittlung der Adresse für Status- und Sperrprüfung beschrieben. Default-mäßig handelt es sich dabei um die Adresse des OCSP-Responders, alternativ um diejenige des CRL-Downloadpunktes. Hierbei wird auf die TSL-Informationen zurückgegriffen. Die Adresse ist im CA-Eintrag der TSL hinterlegt. Für das Verhalten in spezifizierten Offline-Szenarien gilt [GS-A_4658].
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	Eine TSL mit gültiger Signatur
Auslöser	TUC_PKI_006 "OCSP-Abfrage" oder TUC_PKI_021 "CRL-Prüfung"
Eingangsdaten	• End-Entity-Zertifikatsdaten • TSL-Informationen
Komponenten	System
Ausgangsdaten	OCSP-Adresse oder Adresse des CRL-Downloadpunktes
Standardablauf	1. [System:] (Referenz auf) CA-Zertifikat in TSL-Informationen finden (TUC_PKI_003 "CA-Zertifikat in TSL-Informationen finden") 2. [System:] Das Element "ServiceSupplyPoint" (bzw. via referenziertes CA-Zertifikat die Referenz auf den bezeichneten Statusprüfdienst- oder CRL Downloadpunkt) auswählen und URI selektieren.

	3. [System:] Adresse zurückmelden
Fehlerfälle	1a. [System:] CA kann nicht in den TSL-Informationen ermittelt werden (CA_CERT_MISSING). 2a. [System:] Das Element „ServiceSupplyPoint" konnte nicht gefunden werden (SERVICESUPPLYPOINT_MISSING). Weitere Fehlerfälle werden in den jeweiligen referenzierten TUCs beschrieben.
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	Die Adresse des Statusprüfdienstes oder des CRL-Downloadpunktes muss nicht zwingend in der TSL-Datei vorgehalten werden, sondern kann z. B. im Truststore des Systems gespeichert und aufgerufen werden.
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln ". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

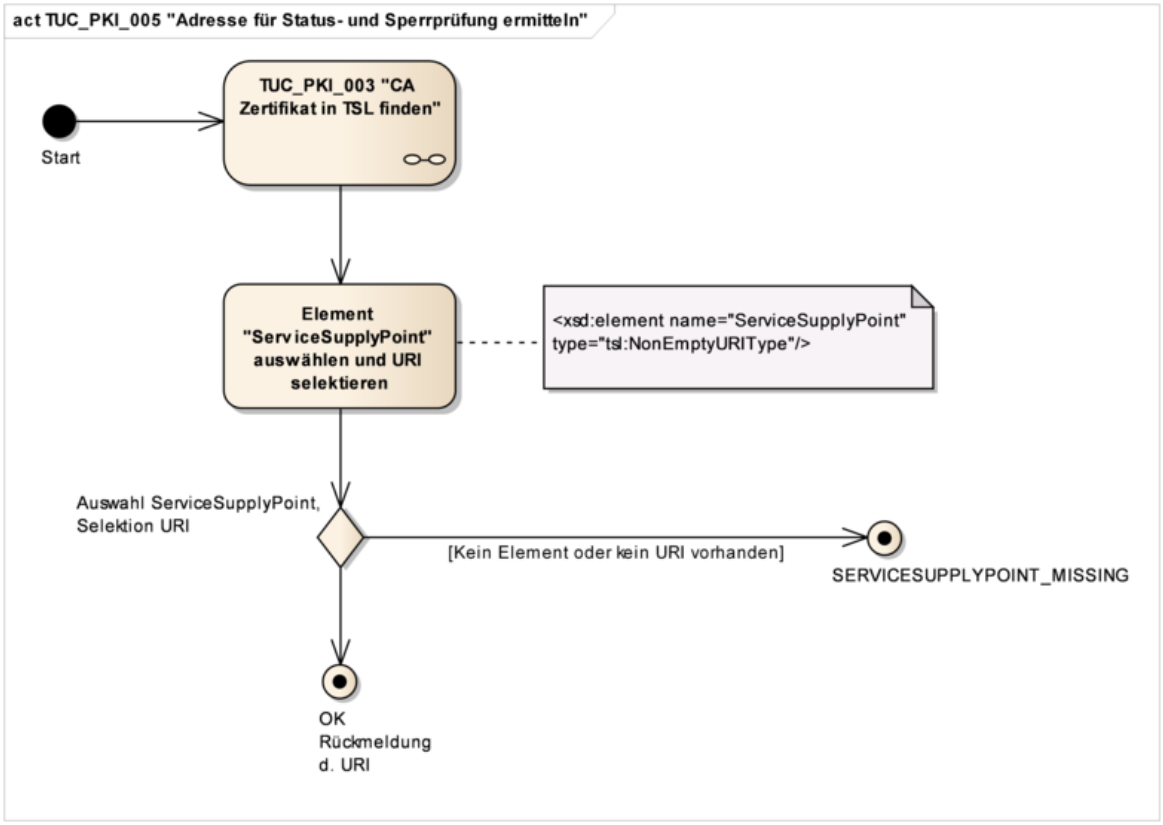


Abbildung 18: Aktivitätsdiagramm TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln"

8.3.2.2 TUC_PKI_006 „OCSP-Abfrage"

GS-A_4657-03 - TUC_PKI_006: OCSP-Abfrage
Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_006 zur OCSP-Abfrage umsetzen.

Tabelle 92: TUC_PKI_006 „OCSP-Abfrage"

Element	Beschreibung
Name	TUC_PKI_006 „OCSP-Abfrage"
Beschreibung	Dieser Use Case beschreibt den Prozess zur OCSP-Prüfung eines Zertifikats. Für das Verhalten in spezifizierten Offline-Szenarien gilt [GS-A_4658]. Der Use Case richtet sich nach den Anforderungen aus den referenzierten Standards und den spezifischen Eigenschaften der TI.
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	Zeitlich gültiges End-Entity- und CA-Zertifikat. TSL-Informationen sind vorhanden.

Auslöser	Zertifikats-Check
Eingangsdaten	• End-Entity-Zertifikatsdaten • CA-Zertifikatsdaten • TSL-Informationen • Referenzzeitpunkt (optional; bei Nichtangabe Verwendung der aktuellen Systemzeit, vgl. Glossar aus Kapitel 11.2): Zeitpunkt, für den das Zertifikat geprüft werden soll • OCSP-Graceperiod (Default: 10min) • Timeout-Parameter (Default: 10s) • TOLERATE_OCSP_FAILURE (true/false, Default: false) • ENFORCE_CERTHASH_CHECK (true/false, Default: f true)
Komponenten	System, OCSP-Responder
Ausgangsdaten	Status der Prüfung OCSP-Response
Referenzen	[RFC6960], [RFC5019],[RFC3370], [RFC5754]
Standardablauf	1. [System:] Prüfung, ob (zum Referenzzeitpunkt unter Berücksichtigung der OCSP-Graceperiod) gültige Statusinformationen bereits vorliegen (z. B. im lokalen Cache bereitgestellt). 2. [System:] Ermittlung der OCSP-Adresse (TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln") 3. [System:] Aufbau des OCSP-Request anhand der passenden Zertifikatsdaten 4. [System:] Absenden des Request an die ermittelte Adresse Der Timeout-Parameter definiert hier, zu welchem Zeitpunkt das System ein Timeout bei Nichterreichbarkeit des Dienstes meldet. 5. [System, OCSP-Responder:] Überprüfung der OCSP-Response (Signatur) auf Integrität. Das dazu benötigte OCSP-Responder-Zertifikat in den TSL-Informationen ermitteln. Die OCSP-Responder-Zertifikate sind alle in den TSL-Informationen enthalten. Somit kann direkt nach dem Zertifikat gesucht werden. (OCSP-Responder sind in der TSL-Datei mit dem

	„ServiceTypeIdentifier“ "http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP" markiert.) 6. [System:] Auswertung der OCSP-Response. Dies umfasst die Prüfung von • Statuscode („OCSPResponseStatus“) auf Belegung mit ‚0‘ (für „successful“), • Zertifikatsidentifizierungs-Informationen („CertID“) auf Identiät mit derjenigen aus dem Request und • Konformität/Plausibilität der Zeitangaben („producedAt“, „thisUpdate“ und (sofern vorhanden) „nextUpdate“). Details siehe • [RFC2560]/[RFC6960] Kap. 4.1, 4.2 und 4.4 • [RFC5019], Kap. 4, • [gemSpec_PKI] Kap. 9.1.2 (insb. [GS-A_5215]). 7. [System:] Wenn ENFORCE_CERTHASH_CHECK auf ´true´ gesetzt ist, wird das End-Entity-Zertifikat mit dem in der certHash-Erweiterung bezeichneten Algorithmus gehasht (vgl. [gemSpec_Krypt#GS-A_4393]). Das Resultat stimmt mit dem gelieferten certificateHash überein. 8. [System:] Überprüfung der Gültigkeit anhand des Referenzzeitpunkts. Der CertStatus "good“ wird gemeldet. 9. [System:] Rückmeldung, dass das Zertifikat gültig ist und Rückgabe der OCSP-Response. 10. [System:] Ende des UseCase

Varianten/Alternativen	1a. [System:] Prüfung der Gültigkeit des Zertifikats gegen vorliegende Informationen. 1a1. [System:] Zertifikat ist gesperrt. Weiter mit Schritt 5, falls die entsprechenden Prüfungen nicht bereits erfolgt sind. Ansonsten Rückmeldung analog 8. 1a2. Die Statusinformationen sind zu alt (Zertifikat nicht gesperrt && (Referenzzeit - Statusinfo.producedAt) > OCSP-Graceperiod)). Neue Informationen müssen eingeholt werden. Es geht weiter mit Schritt 2 (Standardablauf). 1a3. [System:] Zertifikat ist nicht gesperrt und Statusinformationen sind noch gültig Referenzzeit - Statusinfo.producedAt) <= OCSP-Graceperiod. Rückmeldung: Zertifikat ist gültig. 7a. [System:] ENFORCE_CERTHASH_CHECK ist auf ´false´ gesetzt. Weiter mit nächstem Schritt. Damit wird eine etwaig vorhandene Erweiterung ‚certHash' ignoriert. 8a. [System:] Das Zertifikat ist für den Referenzzeitpunkt gültig, obwohl der CertStatus "revoked" gemeldet wird, da "revocationTime" > Referenzzeitpunkt. Rückmeldung Zertifikat ist für den Referenzzeitpunkt gültig und Rückgabe der OCSP-Response. 8b. [System:] Zertifikat ist gesperrt und die Referenzzeit liegt nach dem Sperrzeitpunkt (CertStatus revoked UND revocationTime <= des Referenzzeitpunkts). Rückmeldung Zertifikat ist gesperrt und Rückgabe der OCSP-Response. (CERT_REVOKED) 8c. [System:] Zertifikat ist unbekannt (Status unknown) Rückmeldung, dass das Zertifikat ungültig ist und Rückgabe der OCSP-Response. (CERT_UNKNOWN)

Fehlerfälle/Warnungen	4a. [System:] Die OCSP-Prüfung konnte nicht durchgeführt werden: Im Falle von TOLERATE_OCSP_FAILURE=true wird als Ergebnis eine Warnung generiert (OCSP_CHECK_REVOCATION_FAILED). 4b. [System:] Die OCSP-Prüfung konnte nicht durchgeführt werden: Im Falle von TOLERATE_OCSP_FAILURE=false wird mit einer Fehlermeldung abgebrochen. (OCSP_CHECK_REVOCATION_ERROR) 4c. [System:] Der OCSP-Responder ist (unabhängig v. TOLERATE_OCSP_FAILURE) nicht verfügbar. (OCSP_NOT_AVAILABLE) 5a. [System:] OCSP-Zertifikat nicht in TSL-Informationen enthalten. Abbruch mit Fehlermeldung. (OCSP_CERT_MISSING) 5a1. [System:] Signatur der Response ist nicht gültig. Abbruch mit Fehlermeldung (OCSP_SIGNATURE_ERROR) 6a. [System:] Die Response enthält einen Statuscode („OCSPResponseStatus"), der ungleich 0 (für „successful") ist. (Damit zeigt der OCSP-Responder eine Exception an. Z. B. kann der Wert für den Status auf 3 für „tryLater" gesetzt sein.) Abbruch mit Fehlermeldung (OCSP_STATUS_ERROR) 6b. [System:] Die Response enthält einen Statuscode („OCSPResponseStatus"), der gleich 0 („successful") ist. Die ausgewertete OCSP-Response passt aber nicht zum OCSP-Request (z.B. CertID in OCSP-Request und -Response stimmt nicht überein). Abbruch mit Fehlermeldung (OCSP_CHECK_REVOCATION_ERROR) 7b. ENFORCE_CERTHASH_CHECK ist auf ´true´ gesetzt und die OCSP-Response enthält keine certHash-Erweiterung. (CERTHASH_EXTENSION_MISSING) 7c. Der errechnete Zertifikats-Hash stimmt nicht mit demjenigen aus der in der Erweiterung certHash überein. (CERTHASH_MISMATCH)
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.

Anmerkungen	Der genaue Aufbau des OCSP-Requests und der OCSP-Response ist in Kapitel 9 spezifiziert. Zur Abfrage beim OCSP-Responder MUSS ein Timeout-Parameter konfiguriert werden können. Dieser definiert, zu welchem Zeitpunkt das System ein Timeout bei Nichterreichbarkeit des Dienstes meldet. Die OCSP-Graceperiod dient der Performance-Steigerung. Die OCSP-Graceperiod legt bei der Verwendung von OCSP-Antworten (im Cache) deren maximal zulässiges Alter fest (gemessen an der Systemzeit). Ein Zwang, OCSP-Responses über die gesamte Dauer der OCSP-Graceperiod zu cachen, existiert nicht. Anmerkung zu 6b: Die OCSP-Response muss gemäß [RFC6960] Kap. 4.2 verarbeitet werden, unabhängig davon, ob das Feld "parameters" der Sequenz AlgorithmIdentifier innerhalb der CertID mit NULL belegt oder nicht gesetzt ist, Details siehe Tab_PKI_290. Der in [RFC5754] Kap. 2 empfohlene SHA2 als Hash-Algorithmus für die Bildung von certID wird nicht von allen OCSP-Responder-Produkten unterstützt. Hinweis zum Referenzzeitpunkt (s. auch Glossar aus Kapitel 11.2): Bei der Prüfung von nonQES-Zertifikaten handelt es sich beim jeweiligen Referenzzeitpunkt um die aktuelle Systemzeit. Dadurch vereinfacht sich der Ablauf des TUC: Die Variante 8a ist unter diesen Umständen nicht möglich, sie muss also nicht berücksichtigt werden.
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_006 "OCSP-Abfrage". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

[<=]

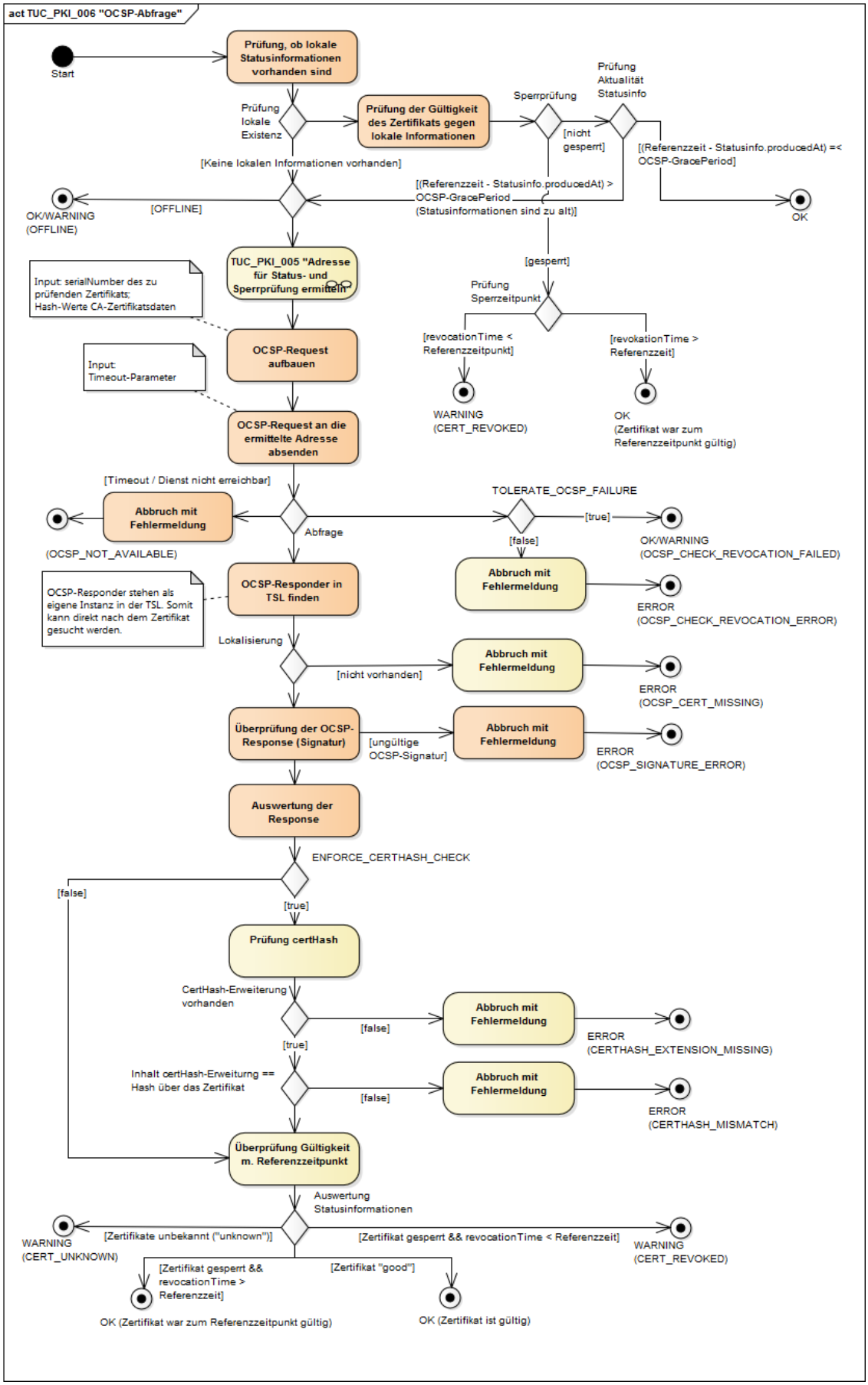

act TUC_PKI_006 "OCSP-Abfrage"
Start
Prüfung, ob lokale Statusinformationen vorhanden sind
Prüfung lokale Existenz
Prüfung der Gültigkeit des Zertifikats gegen lokale Informationen
Sperrprüfung
Prüfung Aktualität Statusinfo
[nicht gesperrt]
[(Referenzzeit - Statusinfo.producedAt) =< OCSP-GracePeriod]
OK
[Keine lokalen Informationen vorhanden]
[(Referenzzeit - Statusinfo.producedAt) > OCSP-GracePeriod (Statusinformationen sind zu alt)]
[OFFLINE]
OK/WARNING (OFFLINE)
[gesperrt]
Prüfung Sperrzeitpunkt
[revocationTime < Referenzzeitpunkt]
[revokationTime > Referenzzeit]
WARNING (CERT_REVOKED)
OK (Zertifikat war zum Referenzzeitpunkt gültig)
TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln"
Input: serialNumber des zu prüfenden Zertifikats; Hash-Werte CA-Zertifikatsdaten
OCSP-Request aufbauen
Input: Timeout-Parameter
OCSP-Request an die ermittelte Adresse absenden
[Timeout / Dienst nicht erreichbar]
Abbruch mit Fehlermeldung
(OCSP_NOT_AVAILABLE)
Abfrage
TOLERATE_OCSP_FAILURE
[true]
OK/WARNING (OCSP_CHECK_REVOCATION_FAILED)
[false]
Abbruch mit Fehlermeldung
ERROR (OCSP_CHECK_REVOCATION_ERROR)
OCSP-Responder in TSL finden
OCSP-Responder stehen als eigene Instanz in der TSL. Somit kann direkt nach dem Zertifikat gesucht werden.
Lokalisierung
[nicht vorhanden]
Abbruch mit Fehlermeldung
ERROR (OCSP_CERT_MISSING)
Überprüfung der OCSP-Response (Signatur)
[ungültige OCSP-Signatur]
Abbruch mit Fehlermeldung
ERROR (OCSP_SIGNATURE_ERROR)
Auswertung der Response
ENFORCE_CERTHASH_CHECK
[false]
[true]
Prüfung certHash
CertHash-Erweiterung vorhanden
[false]
Abbruch mit Fehlermeldung
ERROR (CERTHASH_EXTENSION_MISSING)
[true]
Inhalt certHash-Erweiturng == Hash über das Zertifikat
[false]
Abbruch mit Fehlermeldung
ERROR (CERTHASH_MISMATCH)
Überprüfung Gültigkeit m. Referenzzeitpunkt
Auswertung Statusinformationen
WARNING (CERT_UNKNOWN)
[Zertifikate unbekannt ("unknown")]
[Zertifikat gesperrt && revocationTime < Referenzzeit]
WARNING (CERT_REVOKED)
[Zertifikat gesperrt && revocationTime > Referenzzeit]
[Zertifikat "good"]
OK (Zertifikat war zum Referenzzeitpunkt gültig)
OK (Zertifikat ist gültig)

Abbildung 19: Aktivitätsdiagramm TUC_PKI_006 „OCSP-Abfrage“

8.3.2.3 TUC_PKI_021 „CRL-Prüfung“

GS-A_4900-01 - TUC_PKI_021 “CRL-Prüfung”
Der Konnektor MUSS den TUC_PKI_021 zur Prüfung der Widerrufsinformationen (Statusprüfung) mittels Zertifikatssperrliste (CRL) umsetzen

Tabelle 93: TUC_PKI_021 „CRL-Prüfung“

Element	Beschreibung
Name	TUC_PKI_021 „CRL-Prüfung“
Beschreibung	Dieser Use Case beschreibt den Prozess zur Validierung einer CRL (Certificate Revocation List) sowie den Prozess zur Ermittlung der Sperrinformationen zu einem End-Entity-Zertifikat mittels einer CRL. Die Festlegungen aus [RFC5280], [X.509] und den spezifischen Eigenschaften der TI sind verbindlich.
Anwendungsumfeld	Use Case für den Anwendungsfall zur Prüfung der Sperrinformationen eines End-Entity-Zertifikats.
Vorbedingungen	Ein End-Entity-Zertifikat (mathematisch und zeitlich gültig) Eine CRL ist vorhanden oder kann heruntergeladen werden.
Auslöser	TUC_PKI_018 "Zertifikatsprüfung in der TI "
Eingangsdaten	CRL End-Entity-Zertifikatsdaten (Zertifikats-Seriennummer, CertificateIssuer) Timeout-Parameter (alternativ zu CRL) CRL-Downloadpunkt-Adresse (optional, alternativ zu CRL)
Komponenten	System (nur Konnektor)
Ausgangsdaten	Status der Prüfung
Referenzen	[[RFC5280] [X.509]

Standardablauf	1. [System:] Selektion der CRL 2. [System:] Prüfen der zeitlichen Gültigkeit der CRL (Systemzeit < crl.NextUpdate), s. [RFC5280] Kap. 5.1.2.5. 3. [System:] Auswertung der Art der CRL. Es wird anhand der IssuingDistributionPoint-Erweiterung in der Sperrliste (CRL) geprüft, ob es sich um eine indirekte CRL handelt (indirectCRL-bit), s. [RFC5280] Kap. 5.2.5, [X.509] Kap. 7.12.. 4. [System:] Das zugehörige CRL-Signer-Zertifikat wird in den TSL-Informationen ermittelt. In der TSL-Datei ist der CRL-Signer mit „http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL" im Element ServiceTypeIdentifier gekennzeichnet, s. [ETSI_TS_102_231_V3.1.2] D.2 ETSI Common Domain URIs. 5. [System:] Prüfung der Signatur der CRL, s. [RFC5280] Kap. 6.3.3. 6. [System:] Auswertung der CRL-Einträge. Es wird nach der Zertifikatsseriennummer des zu überprüfenden End-Entity-Zertifikats in der CRL gesucht, s. [RFC5280] Kap. 6.3.3. 7. [System:] Falls einer oder mehrere Einträge gefunden wurden, wird die CRL-Entry-Erweiterung „CertificateIssuer" ausgelesen und deren Inhalt mit dem Issuer-DistinguishedName des End-Entity-Zertifikats verglichen. Nur wenn der Inhalt der CertificateIssuer-Erweiterung mit diesem DistinguishedName übereinstimmt, ist das Zertifikat gesperrt, s. [RFC5280] Kap. 6.3.3. 8. [System:] Rückmeldung, dass das Zertifikat nicht in der Sperrliste enthalten ist. 9. [System:] Ende des Use Case

Varianten/Alternativen	1a. Die CRL ist nicht im System vorhanden und der CRL-Downloadpunkt unbekannt. 1a1. [System:] Ermittlung des TSL-Eintrags der CA, welche das End-Entity-Zertifikat herausgegeben hat. (TUC_PKI_003 „CA Zertifikat in TSL finden“) 1a2. [System:] Ermittlung des CRL-Downloadpunktes aus dem „Service-SupplyPoint“ des TSL-Service Eintrags (TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln"). 1a3. [System:] Herunterladen der CRL aus der ermittelten Adresse. Der Timeout-Parameter definiert hier, zu welchem Zeitpunkt das System ein Timeout bei Nichterreichbarkeit des Dienstes meldet. 1b. Die CRL ist nicht im System vorhanden, der CRL-Downloadpunkt ist aber schon bekannt. 1b1. [System:] Weiter mit 1a3. 7a. [System:] Zertifikat ist gesperrt. Rückmeldung an das System. (CERT_REVOKED)
Fehlerfälle	1a3a. [System:] Die CRL kann nicht heruntergeladen werden. (CRL_DOWNLOAD_ERROR) 2a. [System:] Die Prüfung der zeitlichen Gültigkeit der CRL ergibt, dass die CRL abgelaufen ist (Systemzeit > crl.NextUpdate) (CRL_OUTDATED_ERROR) 3 b. [System:] CRL-Signer-Zertifikat nicht in TSL-Informationen enthalten. Abbruch mit Fehlermeldung. (CRL_SIGNER_CERT_MISSING) 4a. [System:] Signatur der CRL ist nicht gültig. (CRL_SIGNATURE_ERROR) 5a. [System:] Die CRL ist fehlerhaft aufgebaut und kann nicht geprüft werden. (CRL_CHECK_ERROR) 6a. [System:] Die CRL ist fehlerhaft aufgebaut und ihre Einträge können nicht ausgewertet werden. (CRL_CHECK_ERROR) 7b. [System:] Die CRL-Einträge sind fehlerhaft aufgebaut und können nicht weiter geprüft werden. (CRL_CHECK_ERROR)

Anmerkungen, Bemerkungen	Dieser TUC kommt z.B. bei der Konzentrator-Zertifikatsprüfung zur Anwendung. Der Downloadpunkt der CRL ist aus dem Internet erreichbar. Als Übertragungsprotokoll für den allfälligen Download ist „HTTP" zu verwenden. Die Schritte 1-5 beinhalten die Validierung der CRL. Diese können vorgängig durchgeführt werden und müssen also nicht bei jeder einzelnen CRL-Prüfung eines End-Entity-Zertifikats durchlaufen werden, solange gewährleistet ist, dass die CRL zeitlich gültig ist. Die Zertifikats-Extension crlDistributionPoint wird bei der Zertifikatsprüfung von TI-Zertifikaten gemäß TUC_PKI_018/TUC_PKI_021 nicht ausgewertet (vgl. Tab_PKI_245/Tab_PKI_265).
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_021 "CRL-Prüfung". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

[<=]

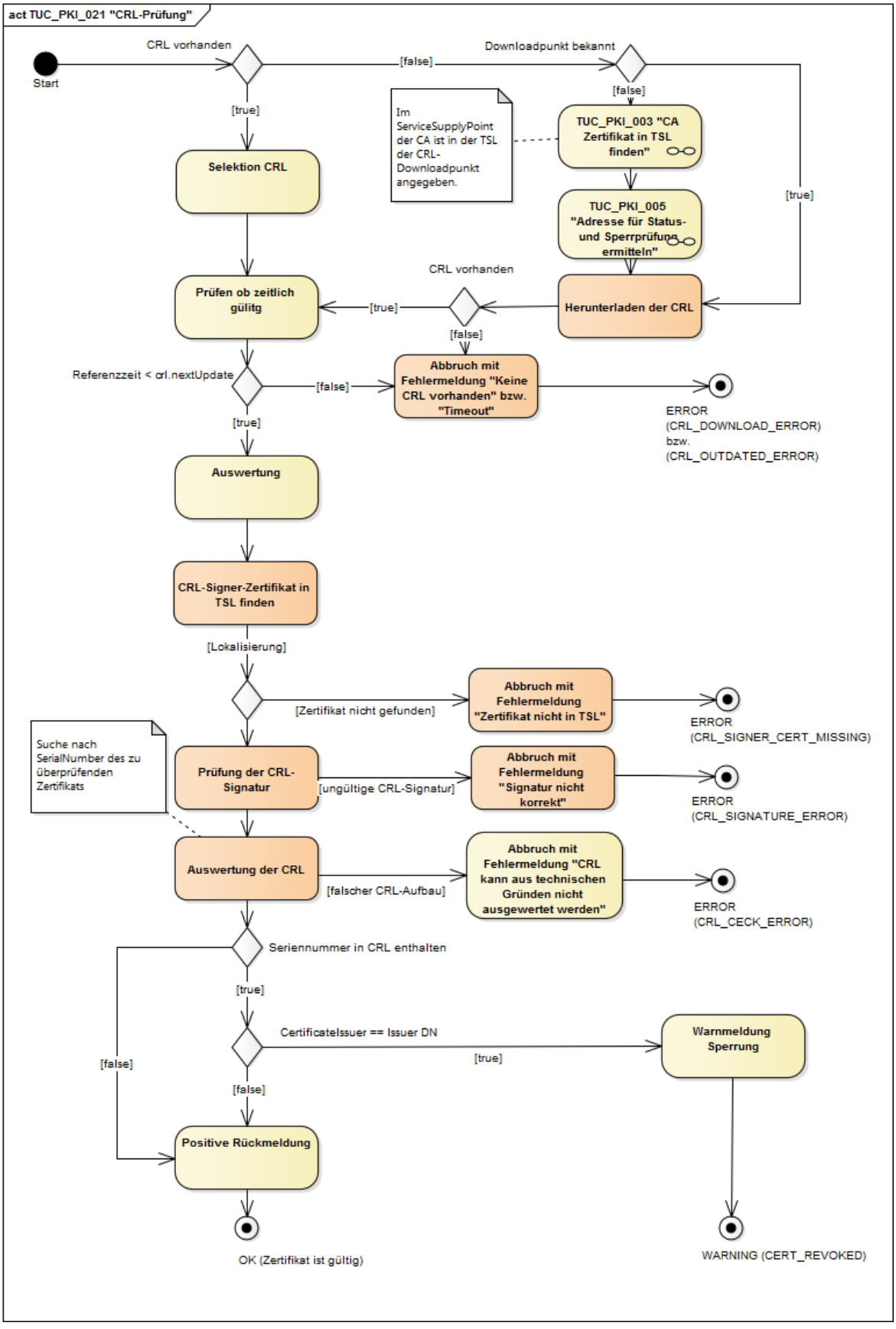

act TUC_PKI_021 "CRL-Prüfung"
Start
CRL vorhanden
[false]
[true]
Downloadpunkt bekannt
[false]
[true]
Im ServiceSupplyPoint der CA ist in der TSL der CRL-Downloadpunkt angegeben.
TUC_PKI_003 "CA Zertifikat in TSL finden"
TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln"
Herunterladen der CRL
Selektion CRL
CRL vorhanden
[true]
[false]
Prüfen ob zeitlich gültig
Referenzzeit < crl.nextUpdate
[false]
[true]
Abbruch mit Fehlermeldung "Keine CRL vorhanden" bzw. "Timeout"
ERROR (CRL_DOWNLOAD_ERROR) bzw. (CRL_OUTDATED_ERROR)
Auswertung
CRL-Signer-Zertifikat in TSL finden
[Lokalisierung]
[Zertifikat nicht gefunden]
Abbruch mit Fehlermeldung "Zertifikat nicht in TSL"
ERROR (CRL_SIGNER_CERT_MISSING)
Suche nach SerialNumber des zu überprüfenden Zertifikats
Prüfung der CRL-Signatur
[ungültige CRL-Signatur]
Abbruch mit Fehlermeldung "Signatur nicht korrekt"
ERROR (CRL_SIGNATURE_ERROR)
Auswertung der CRL
[falscher CRL-Aufbau]
Abbruch mit Fehlermeldung "CRL kann aus technischen Gründen nicht ausgewertet werden"
ERROR (CRL_CECK_ERROR)
Seriennummer in CRL enthalten
[true]
CertificateIssuer == Issuer DN
[true]
Warnmeldung Sperrung
[false]
[false]
Positive Rückmeldung
OK (Zertifikat ist gültig)
WARNING (CERT_REVOKED)

Abbildung 20: Aktivitätsdiagramm TUC_PKI_021 „CRL-Prüfung"

8.3.2.4 Szenarien für Offline und Timeout von OCSP

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

GS-A_4658 - Zertifikatsprüfung in spezifizierten Offline-Szenarien
Die Produkttypen der TI, die Zertifikate prüfen und per Spezifikation ihre Funktionen zeitweise oder ständig offline von der TI erbringen, MÜSSEN für die explizit spezifizierten Offline-Szenarien bei der Zertifikatsprüfung die TUCs *TUC_PKI_005 OCSP-Adresse ermitteln* und *TUC_PKI_006 OCSP-Abfrage* auslassen.
[<=]

8.3.2.5 Statusprüfung von eGK-Zertifikaten

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

GS-A_4943 - Alter der OCSP-Responses für eGK-Zertifikate
Die Produkttypen der TI, die Zertifikate der elektronischen Gesundheitskarte (eGK) prüfen, DÜRFEN NICHT OCSP-Responses für die Statusprüfung verwenden, deren Alter die OCSP-Graceperiod (maximale Caching-Dauer) übersteigt. Dies beinhaltet auch OCSP-Responses, die den Status „revoked" enthalten.
[<=]

8.3.3 Ermittlung von Autorisierungsinformationen

8.3.3.1 Bestätigte Zertifikatsinformationen

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

- Zertifikatstypen
- Die Rolle der Zertifikatsidentität

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

8.3.3.2 TUC_PKI_009 „Rollenermittlung"

GS-A_4660-01 - TUC_PKI_009: Rollenermittlung
Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_009 zur Ermittlung der Rolle der Identität umsetzen

Tabelle 94: TUC_PKI_009 „Rollenermittlung“

Element	Beschreibung
Name	TUC_PKI_009 „Rollenermittlung“
Beschreibung	Die Rolle einer Identität steht im jeweiligen Zertifikat. Dieser Use Case beschreibt die Ermittlung dieser Rolle aus dem Zertifikat. Jede Rolle wird in der Struktur `professionInfo` als OID gespeichert (siehe Kap 4.4, 4.5, 4.6). In allen Zertifikaten, die eine Rolle besitzen, steht diese in der Extension Admission, aus welcher der OID ausgelesen wird.
Anwendungsumfeld	System, das spezifische Inhalte von Zertifikaten verwendet
Vorbedingungen	Gültiges End-Entity-Zertifikat
Auslöser	Zertifikatsprüfung in der TI, TUC_PKI_018 "Zertifikatsprüfung in der TI ", TUC_PKI_030 "QES-Zertifikatsprüfung"
Eingangsdaten	End-Entity-Zertifikatsdaten
Komponenten	System
Ausgangsdaten	OID der Rolle
Referenzen	[Common-PKI#Part1#3.1]
Standardablauf	1. [System:] Prozess zur Ermittlung der Rolle beginnt 2. [System:] Extension Admission aus dem Zertifikat auslesen. 3. [System] Admission ist vorhanden und die Rolle aus dem Feld `professionOIDs` ermittelt. Sind weitere Einträge `professionInfo` enthalten, wird dieser Schritt so oft durchlaufen, bis alle `professionOIDs` ermittelt sind. 4. [System:] Mindestens eine OID ist vorhanden und wird zurück geliefert. Bei mehreren OID wird die Liste der OID als

	Rückgabewert geliefert. Ende des Use Case mit vorhandener Rolle
Varianten/Alternativen	3a. [System:] Extension Admission ist nicht vorhanden. 3a1. [System:] Meldung des Systems, dass keine Rolle vorhanden ist. 3a2. [System:] Ende des Use Case ohne Rolle 4a. [System:] OID nicht vorhanden 4a1. [System:] Meldung des Systems, dass keine Rolle vorhanden ist. 4a2. [System:] Ende des Use Case ohne Rolle
Fehlerfälle	Es werden keine spezifischen Fehlerfälle beschrieben.
Anmerkungen	Die Rolle in der Extension Admission befindet sich im Feld professionOIDs und ist als OID abgelegt. Die genaue Festlegung der OID wird im Dokument [gemSpec_OID] spezifiziert. Syntax der Extension Admission siehe IT-spezifische Festlegungen, insbesondere Tab_PKI_226-01. Die Auswertung der Rolle und wie im Fehlerfall zu verfahren ist, wird in der jeweiligen Produktspezifikation beschrieben.
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_009 „Rollenermittlung“. Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

[<=]

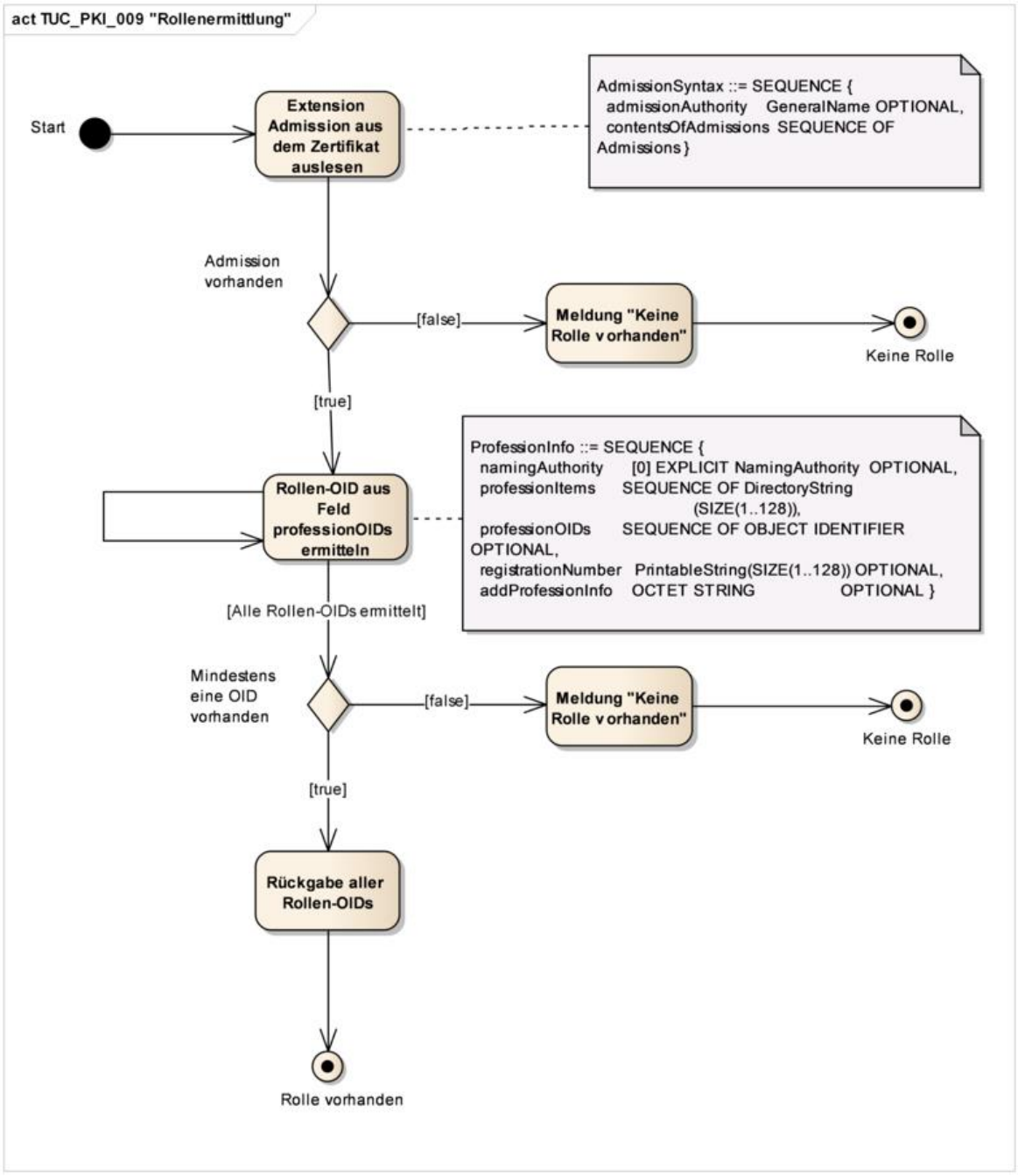


Abbildung 21: Aktivitätsdiagramm TUC_PKI_009 „Rollenermittlung"

8.3.3.3 TUC_PKI_007 „Prüfung Zertifikatstyp"

GS-A_4749-01 - TUC_PKI_007: Prüfung Zertifikatstyp

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

Tabelle 95 : TUC_PKI_007 „Prüfung Zertifikatstyp“

Element	Beschreibung
Name	TUC_PKI_007 „Prüfung Zertifikatstyp“
Beschreibung	In diesem Use Case wird der Soll-/Ist-Vergleich des Zertifikatstyps im Zuge einer Zertifikatsprüfung beschrieben. Verglichen wird die im Zertifikat hinterlegte Zertifikatstyp-OID (abgelegt in einem Element PolicyIdentifier der X.509-Extension CertificatePolicies) mit der als Eingangsparameter dieses TUC übergebenen Liste der erwarteten Zertifikatstyp-OIDs. Zusätzlich wird die Zertifikatstyp-OID aus dem Zertifikat jeweils mit den in der TSL (TSL-Extension "ServiceInformationExtensions") enthaltenen ExtensionOIDs der CA verglichen, die das Zertifikat ausgestellt hat.
Anwendungsumfeld	System, das spezifische Inhalte von Zertifikaten verwendet
Vorbedingungen	Gültiges End-Entity-Zertifikat Aktuelle TSL-Informationen im System.
Auslöser	TUC_PKI_018 "Zertifikatsprüfung in der TI "
Eingangsdaten	• Das zu prüfende Zertifikat • PolicyList
Komponenten	System
Ausgangsdaten	• Status der Prüfung • OID des Zertifikatstyps
Referenzen	[RFC5280], [gemSpec_TSL]

Standardablauf	1. [System:] Start des Prozesses zur Ermittlung des Zertifikatstyps. 2. [System:] Zertifikat laden 3. [System:] Auswahl der CertificatePolicies aus dem Zertifikat 4. [System:] Auswahl des Elements PolicyInformation. Es können mehrere Elemente vorkommen, da es eine SEQUENCE ist. In jedem Schritt wird ein Element aus der SEQUENCE entnommen. 5. [System:] Selektion der CertPolicyId aus dem Element PolicyInformation 6. [System:] Prüfung der Zertifikatstyp-OID (nicht jedoch der Policy-OID)aus dem Zertifikat gegen Liste der Zertifikatstyp-OIDs aus dem Parameter PolicyList der Eingangsdaten. 7. [System:] Die Zertifikatstyp-OID ist in PolicyList enthalten. Aus den TSL-Informationen wird der TSL-Eintrag der passenden CA ermittelt, welche das Zertifikat herausgegeben hat. (TUC_PKI_003 "CA Zertifikat in TSL finden"), s. [gemSpec_TSL#7.3.2.1]. 8. [System:] Prüfung der Zertifikatstyp-OID aus dem Zertifikat gegen die im TSL-Eintrag in der TSL-Extension "ServiceInformationExtensions" enthaltenen OIDs. 9. [System:] Die Zertifikatstyp-OID stimmt mit einer ExtensionOID überein. Ende des Use Case mit der Rückgabe der Zertifikatstyp-OID. Mit dem ersten OID-Match wird der Use Case beendet und die gesamte Prüfung als erfolgreich gewertet.
Varianten/Alternativen	6a. [System:] Keine Übereinstimmung, nächstes Element PolicyInformation des Zertifikates wird analysiert. Wiederholung des Vorgangs ab Schritt 4. 7a. Wird die Prüfung der ExtensionOID ausgelassen, endet der Use Case mit der Rückmeldung „Prüfung Zertifikatstyp erfolgreich“ und der Rückgabe der OID des Zertifikatstyps.

Fehlerfälle/Warnungen	4a. [System:] Abbruch und Rückmeldung. Kein Element PolicyIdentifier vorhanden. (CERT_TYPE_INFO_MISSING) 7. [System:] Abbruch und Fehlermeldung. Ende der SEQUENCE ist erreicht und es wurde keine Übereinstimmung festgestellt. (CERT_TYPE_MISMATCH) 9a. [System:] Es wurde keine Übereinstimmung mit den ExtensionOIDs im Element ServiceInformationExtensions festgestellt. Abbruch mit der Fehlermeldung CERT_TYPE_CA_NOT_AUTHORIZED.
Anmerkungen	Zusätzlich zu [RFC5280] Kap. 4.2.1.4 ist der Aufbau der Extension CertificatePolicies in Kapitel 4.8.3.3 TI-spezifisch (Zertifikatstyp-OID) beschrieben. Für die Speicherung des Zertifikatstyps enthält das Element PolicyInformation kein Unterelement policy-Qualifier.
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_007 "Prüfung Zertifikatstyp". Das Diagramm dient nur der Veranschaulichung und ist nicht normativ. Gegebenenfalls enthält es nicht alle Prüfschritte und Meldungen im Detail.

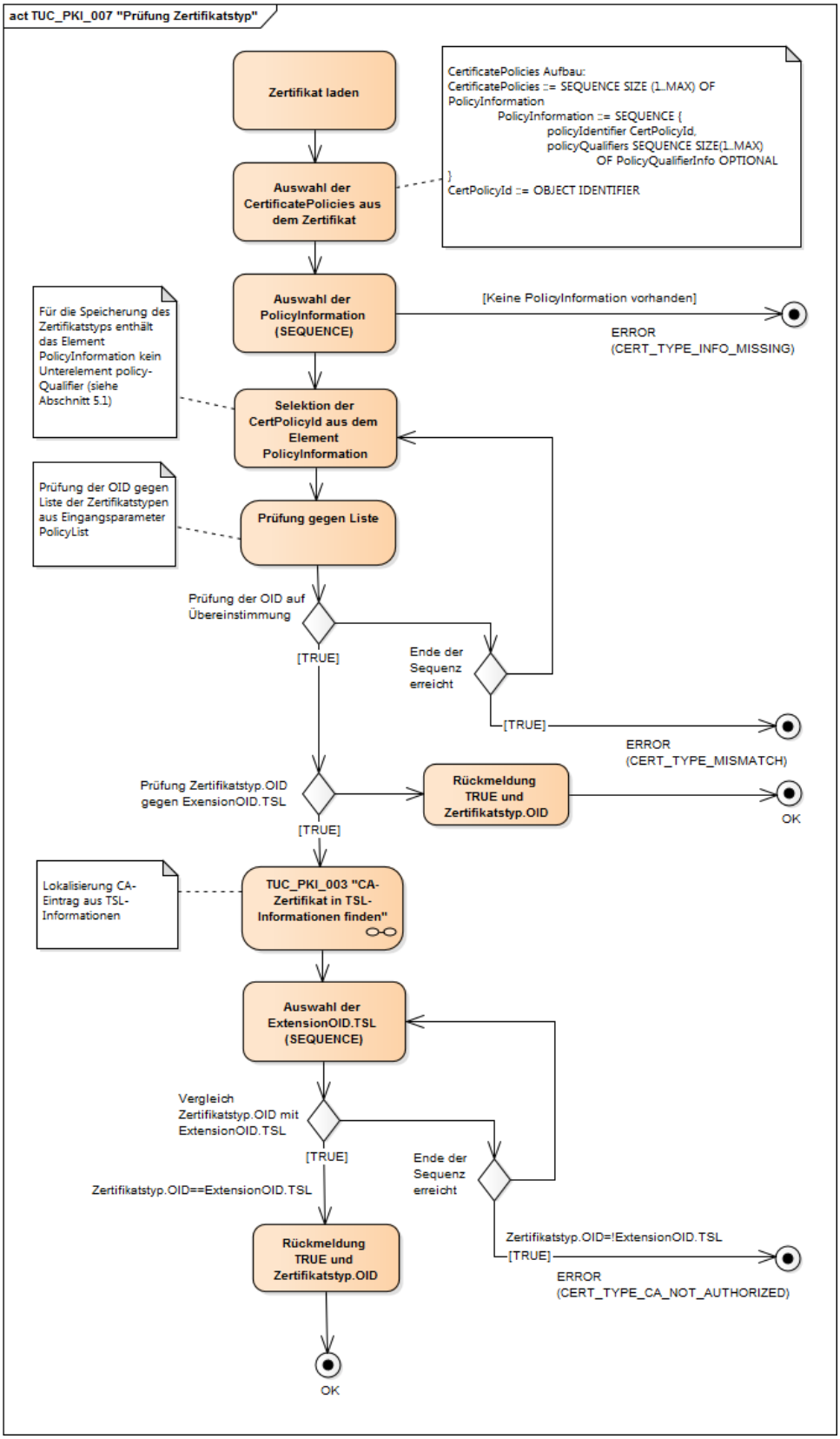


Abbildung 22 : Aktivitätsdiagramm TUC_PKI_007 „Prüfung Zertifikatstyp“

[<=]

8.3.4 Weitere Prüfungen

8.3.4.1 Umgang mit kritischen Extensions

GS-A_4661-01 - kritische Erweiterungen in Zertifikaten
Zertifikatsprüfenden Komponenten MÜSSEN kritische Zertifikatserweiterungen gemäß [RFC5280] Kapitel 4.2 verarbeiten.
[<=]

8.4 Überprüfung der Zertifikate auf Netzwerk- und Transportebene

8.4.1 TLS-Verbindungsaufbau

GS-A_4662 - Bedingungen für TLS-Handshake
Produkttypen der TI, die TLS nutzen, MÜSSEN sicherstellen, dass TLS-Applikationsdaten (d. h. TLS-Nutzdaten, wie z. B. die Protokollschicht HTTP, LDAP, SMTP, IMAP oder POP3) nur ausgetauscht werden, wenn im Falle von einseitiger Authentisierung das Serverzertifikat aktuell gültig ist oder im Falle von gegenseitiger Authentisierung beide Zertifikate aktuell gültig sind und zusätzlich in beiden Fällen der TLS-Handshake erfolgreich absolviert wurde.
[<=]

GS-A_4663 - Zertifikats-Prüfparameter für den TLS-Handshake
Produkttypen der TI, die TLS nutzen, MÜSSEN sicherstellen, dass für den TLS-Verbindungsaufbau die in Tab_PKI_273 beschriebene Nutzung der Eingangsdaten-Parameter von TUC_PKI_018 „Zertifikatsprüfung" für diese Zertifikatsprüfungen verwendet werden.
[<=]

Tabelle 96: Tab_PKI_273 Prüfparameter für TLS-Aufbau

TUC_PKI_018 Eingangsdaten	Beschreibung
Zertifikat	das zu prüfende Zertifikat vom Kommunikationspartner
Referenzzeitpunkt	Aktuelle Systemzeit
Prüfmodus	OCSP
PolicyList	Für den Verwendungszweck TLS zulässige Zertifikatstyp-OID gemäß [gemSpec_OID#Tab_PKI_405]
Vorgesehene KeyUsage	Der Wert MUSS konfigurierbar sein. Die zu konfigurierenden Werte sind in den Zertifikatsprofilen der TLS-nutzenden Komponenten enthalten.

Vorgesehene ExtendedKeyUsage	Der Wert MUSS konfigurierbar sein. Die zu konfigurierenden Werte sind in den Zertifikatsprofilen der TLS-nutzenden Komponenten enthalten.
OCSP-Graceperiod	Der Wert muss konfigurierbar sein.
Offline-Modus	Nein, mit Ausnahme der Komponenten und Dienste, bei denen ein Offline-Modus explizit spezifiziert ist.

GS-A_5077 - FQDN-Prüfung beim TLS-Handshake
Produkttypen der TI, die beim TLS-Handshake das TLS-Serverzertifikat prüfen, MÜSSEN sicherstellen, dass für den Verbindungsaufbau der FQDN im Zertifikat C.ZD.TLS-S bzw. C.FD.TLS-S mit dem der Komponente zugeordneten FQDN übereinstimmt.
[<=]

8.4.2 IPsec-Verbindungsaufbau

GS-A_5078 - FQDN-Prüfung beim IPsec-Aufbau
Produkttypen der TI die beim Aufbau einer IPsec-Verbindung das IPsec-Serverzertifikat prüfen, MÜSSEN sicherstellen, dass der FQDN im Zertifikatattribut *SubjectDN* oder in der Erweiterung *SubjectAltNames* des Zertifikats C.VPNK.VPN bzw. C.VPNK.VPN-SIS mit dem der Komponente zugeordneten FQDN übereinstimmt.

[<=]

8.5 Zertifikatsprüfung X.509 QES

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

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

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

Die folgenden Use Cases verdeutlichen die Aktionen des Systems.

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

8.5.1 TUC_PKI_030 „QES-Zertifikatsprüfung"

GS-A_4750-01 - TUC_PKI_030 „QES-Zertifikatsprüfung"
Alle Produkttypen, die QES-Zertifikate prüfen, MÜSSEN TUC_PKI_030 zur Prüfung der QES-Zertifikate umsetzen.

Tabelle 97: TUC_PKI_030 „QES-Zertifikatsprüfung"

Element	Beschreibung
Name	TUC_PKI_030 „QES-Zertifikatsprüfung"
Beschreibung	In diesem Use Case wird die Prüfung von Zertifikaten mit qualifizierter Signatur beschrieben. Die Prüfung von QES-Zertifikaten und die Sperrprüfung per OCSP entsprechen den gesetztlichen Vorgaben und relevanten Standards. Die zugrundeliegende Prüfung des Zertifikatspfads (Validation Certificate Path) basiert auf dem Kettenmodell (chain model), siehe Anmerkung [1]. Zusätzlich werden folgende Schritte in diesem Technical Use Case (TUC) durchgeführt.
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	aktuelle TSL-Informationen im Truststore (inkl. OCSP-Adressen in der TI für die zugelassenen VDAs), eine aktuell gültige BNetzA-VL.
Auslöser	Zertifikats-Check
Eingangsdaten	• QES-Zertifikat • Referenzzeitpunkt (optional; bei Nichtangabe Verwendung der aktuellen Systemzeit): Zeitpunkt, für den das Zertifikat geprüft werden soll, Details siehe Anmerkung [2] • Offline-Modus (ja/nein) • Beigefügte OCSP-Response, die zur Prüfung des angefragten QES-Zertifikates erforderlich ist (optional; z. B. in Signatur eingebettet)

	• Nonce (optional; Wert ausschließlich zur Verwendung bei der OCSP-Prüfung des zu prüfenden QES-Zertifikates) • Timeout-Parameter für OCSP-Abfragen (Default: 10s)
Komponenten	System
Ausgangsdaten	• Status der Prüfung • OCSP-Response zum angefragten QES-Zertifikat • im Zertifikat enthaltene Rollen-OIDs • im Zertifikat enthaltene QCStatements-Einträge
Referenzen	[eIDAS], [VDG] [ETSI TS 119 612], [ETSI EN 319 412-5], [ETSI EN 319 412-2], [ETSI EN 319 102-1], [ETSI TS 119 172-4] [RFC5280], [RFC6960], [RFC5019]
Standardablauf	1. [System:] Auslesen und Ausgabe aller gesetzten Elemente der Extension QCStatements des Zertifikates, Details siehe Anmerkung [3]. 2. [System:] Prüfung der (zeitlichen) Gültigkeit des Zertifikats mittels TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats", Details siehe Anmerkung [4]. 3. [System:] Prüfung der Extension KeyUsage auf Vorhandensein und die richtige Belegung entsprechend [ETSI EN 319 412-2], Details siehe Anmerkung [5]. 4. [System:] Anhand der End-Entity-Zertifikate wird die BNetzA-VL durchsucht, um das passende QES-CA-Zertifikat zu finden. 5. [System:] Prüfung, ob das ausstellende QES-CA-Zertifikat für die QES-Prüfung zum Zeitpunkt der Erstellung des End-Entity-Zertifikats in der BNetzA-VL gemäß [eIDAS] und [ETSI TS 119 612 qualifiziert und als gültig gekennzeichnet ist, Details siehe Anmerkung [7]. 6. [System:] Prüfung der mathematischen Signaturkorrektheit des Signaturzertifikats zum übergebenen Referenzzeitpunkt gegen das CA-Zertifikat aus Schritt 5 nach dem Kettenmodell, Details siehe Anmerkungen [1], [9]. 7. [System:] Ermittlung der OCSP-Adresse aus dem AIA-Feld des QES-EE-Zertifikates. Dabei handelt es sich um eine öffentlich aufrufbare URL im Internet. Wird für die ermittelte OCSP-URL in der TSL derselbe Wert im InformationValue-Element von AdditionalServiceInformation von BNetzA-VL-Service (mit ServiceTypeIdentifier

	http://uri.telematik/TrstSvc/Svctype/TrustedList/schemerules/DE) gefunden, so wird die dahinter folgende (nach Leerzeichen) URL als Adresse für die OCSP-Anfrage verwendet. Andernfalls wird die zuvor ermittelte OCSP-Adresse aus dem AIA-Feld für die OCSP-Anfrage verwendet, Details siehe Anmerkung [10]. 8. [System:] Die abzufragenden Statusinformationen zu QES-Zertifikaten werden per OCSP-Requests unter Verwendung der aus der TSL ermittelten OCSP-Adresse aus Schritt 7 eingeholt. 9. Prüfung der OCSP-Response auf Integrität [System, OCSP-Responder:] Das dazu benötigte OCSP-Responder-Zertifikat (OCSP-Signer-Zertifikat) wird aus dem URI (markiert mit dem ServiceTypeIdentifier http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP oder http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC) in der BNetzA-VL ermittelt. Die Signatur der OCSP-Response wird zum Referenzzeitpunkt mittels des ermittelten OCSP-Signer-Zertifikats geprüft. Falls keiner der URIs vorhanden ist, wird weiter mit Schritt 10 verfahren, siehe Anmerkung [12]. 10. [System, OCSP-Responder:] Das OCSP-Signer-Zertifikat aus dem Feld „certs" in der OCSP-Response ermitteln. Die Signatur des OCSP-Signer-Zertifikats wird entsprechend mittels des im Schritt 6 validierten QES-CA-Zertifikats geprüft. Die Signatur der OCSP-Response wird anschließend mittels des ermittelten OCSP-Signer-Zertifikats geprüft, siehe Anmerkungen [12]. 11. [System] Auswertung der OCSP-Respone. Dies umfasst die Prüfung gemäß Standards (Details siehe Anmerkung [11]) • Statuscode („OCSPResponseStatus") auf Belegung mit ‚0' (für „successful"), • Zertifikatsidentifizierungs-Informationen („CertID") auf Identität mit derjenigen aus dem Request und • Konformität/Plausibilität der Zeitangaben („producedAt", „thisUpdate" und (sofern vorhanden) „nextUpdate"). 12. [System:] Überprüfung der Gültigkeit der Statusinformation anhand des übergegebenen Referenzzeitpunkts. Der certStatus „good" wird gemeldet. Rückmeldung „Das Zertifikat ist gültig" und Rückgabe der OCSP-Response. 13. [System:] Ermittlung der Rolle (TUC_PKI_009 "Rollenermittlung") 14. [System:] Ende des Use Case mit Rückgabe des/der im Zertifikat enthaltenen Rollen-OID(s)

Varianten/Alternativen	Der Standardablauf stellt die üblichen Schritte dar, die durchgeführt werden müssen. Eine Trennung in zwei Prozesse oder eine Umstrukturierung, bei der alle notwendigen Schritte erfolgen, ist zulässig. 7a. [System:] Der Offline-Modus ist aktiviert. Es werden keine Statusinformationen eingeholt. (Schritte 8, 9, 10, 11 und 12 entfallen) 8a. [System:] Wird im optionalen Parameter Nonce ein Wert übergeben, dann muss für QES-Zertifikate dieser Wert als OCSP-Parameter in den OCSP-Request integriert und im Response geprüft werden. 8b. [System:] Eine OCSP-Response zu dem zu prüfenden Zertifikat wurde im Aufruf mit übergeben. Falls dieses zum Referenzzeitpunkt gültig ist, werden keine OCSP-Requests erzeugt, sondern die beigefügte OCSP-Response zur weiteren Prüfung verwendet.
Fehlerfälle/Warnung	In jedem der beschriebenen Schritte können Fehler auftreten. Diese sind durch das System zu melden und der Prozess muss beendet werden. 1a. Ist die Extension QCStatements nicht auslesbar, leer oder enthält keine auslesbaren Elemente, bricht der TUC mit dem Fehler QC_STATEMENT_ERROR ab. 3a. [System:] KeyUsage ist nicht vorhanden bzw. entspricht nicht der vorgesehenen keyUsage (WRONG_KEYUSAGE) 5a. Ist das QES-CA-Zertifikat in der BNetzA-VL nicht vorhanden oder zum Referenzzeitpunkt nicht mit einem gültigen Status gekennzeichnet, muss der TUC mit einer Fehlermeldung CA_CERTIFICATE_NOT_QES_QUALIFIED abbrechen. 5b. [System:] QES-CA-Zertifikat des QES-Zertifikates ist in der BNetzA-VL als revoked gekennzeichnet und QES-Zertifikat ist nach Sperrzeitpunkt erstellt worden. Abbruch mit Fehlermeldung (CA_CERTIFICATE_REVOKED_IN_BNETZA-VL). 6a. [System] Die Zertifikats-Signatur ist nicht gültig. Ende des Use Case. Abbruch mit Fehlermeldung (CERTIFICATE_NOT_VALID_MATH) 7b. [System:] Warnmeldung, dass keine Online-Statusprüfung durchgeführt wurde (NO_OCSP_CHECK). 8c. [System:]. Der zuständige OCSP-Responder ist nicht erreichbar. Abbruch mit Fehlermeldung (OCSP_NOT_AVAILABLE). 8d. [System:] OCSP-Responses zu dem zu prüfenden Zertifikat

	wurden im Aufruf mit übergeben, ergaben bei den weiteren Prüfschritten jedoch kein gültiges Ergebnis. Eine erneute Prüfung wird in diesem Fall durchgeführt, als wären keine OCSP-Responses beigefügt. In den Rückgabewerten dieses TUC wird die Warnmeldung (PROVIDED_OCSP_RESPONSE_NOT_VALID) an die aufrufende Funktion übergeben. 8e. Wenn die in einer OCSP-Response zurückgelieferte Nonce nicht mit der Nonce des OCSP-Requests für ein QES-Zertifikat übereinstimmt, wird die Prüfung abgebrochen mit der Fehlermeldung OCSP_NONCE_MISMATCH. 8f. [System] Nach zeitlichem Ablauf der TSL-Graceperiod ist die aus der TSL zu ermittelnde OCSP-Adresse nicht mehr vertrauenswürdig. Abbruch mit Fehlermeldung (OCSP_CHECK_REVOCATION_ERROR). 9a/10a. [System:] OCSP-Signer-Zertifikat nicht in der OCSP-Response enthalten. Abbruch mit Fehlermeldung. (OCSP_CERT_MISSING). 9a1/10a1. [System] Signatur der OCSP-Response ist nicht gültig. Abbruch mit Fehlermeldung (OCSP_SIGNATURE_ERROR) 11a. [System] Die Response enthält einen Statuscode („OCSPResponseStatus"), der ungleich 0 (für „successful") ist. (Damit zeigt der OCSP-Responder eine Exception an. Beispielsweise kann der Wert für den Status auf 3 für „tryLater" gesetzt sein.) Abbruch mit Fehlermeldung (OCSP_STATUS_ERROR) 11b. [System] Die Response enthält einen Statuscode („OCSPResponseStatus"), der gleich 0 („successful") ist. Die ausgewertete OCSP-Response passt aber nicht zum OCSP-Request (z.B. CertID in OCSP-Request und -Response stimmt nicht überein, s. a. Anmerkung [13]). Abbruch mit Fehlermeldung (OCSP_CHECK_REVOCATION_ERROR) 12a. [System:] Das Zertifikat ist für den Referenzzeitpunkt gültig, obwohl der CertStatus "revoked" gemeldet wird, da "revocationTime" > Referenzzeitpunkt. Rückmeldung Zertifikat ist für den Referenzzeitpunkt gültig und Rückgabe der OCSP-Response, siehe Anmerkung [14]. 12b. [System:] Zertifikat ist gesperrt und die Referenzzeit liegt nach dem Sperrzeitpunkt (CertStatus revoked UND revocationTime <= Referenzzeitpunkts). Rückmeldung Zertifikat ist gesperrt und Rückgabe der OCSP-Response. (CERT_REVOKED) 12c. [System:] Zertifikat ist unbekannt (Status unknown) Rückmeldung, dass das Zertifikat ungültig ist und Rückgabe

	der OCSP-Response. (CERT_UNKNOWN) Weitere Fehlerfälle werden in den jeweiligen referenzierten Use Cases beschrieben.
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an die Produkttypen der TI, die QES-Zertifikate prüfen, siehe auch [RFC6960] Kap. 5.
Anmerkungen	Folgende Hinweise sollen als Hilfestellung für eine Umsetzung des TUC dienen: [1] Kettenmodell (chain model) für die Validierung von QES-X.509-Zertifikatketten: Alle CA-Zertifikate müssen zum Zeitpunkt der Ausstellung eines QES-EE-Zertifikats gültig sein und das Zertifikat war beim Erstellen der qualifizierten Signatur gültig und nicht von der CA gesperrt, s. Artikel 32, Absatz (1), Satz (b) [eIDAS], Definition Kettenmodell s. [ETSI TR 119 001], Verwendung v. Prüfmodellen s. [ETSI EN 319 102-1] Kap. 5.2.6.4. [2]Weiterführende Informationen siehe Glossar aus Kap. 11.2 und Definition der Zeitparameter aus [gemSpec_Kon] Kap. 4.1.8.1.3. [3] Schritt 1: Im Signaturzertifikat muss mindestens ein QCStatement mit dem OID id-etsi-qcs-QcCompliance. (0.4.0.1862.1.1) enthalten sein. Die QC-Statement-Typen werden in ETSI EN 319 412-5, insbesondere Kap. 5 – Table 2 für QES-Zertifikate, bezüglich der Extension QCStatements des Zertifikates beschrieben. [4] Schritt 2: Die (zeitliche) Gültigkeitsprüfung ist nach [eIDAS] Artikel 28 Satz (1) ANHANG I Buchstabe e) auch für die QES-Zertifikatsprüfung gemäß TUC_PKI_030 verpflichtend, s. a. [ETSI EN 319 412-5] Annex A.1 Buchstabe (e). [5] Schritt 3: Die Prüfung der KeyUsage lehnt sich an [RFC5280] Kap. 4.2.1.3 und [ETSI EN 319 412-2] Kap. 4.3.2 – Table 1 (KeyUsage v. Type A) sowie Tab_PKI_270. [6] Schritt 4: Das Verfahren zum Finden des QES-CA-Zertifikates in BNetzA-VL verläuft analog zum Finden des nonQES-CA-Zertifikates in der TSL mittels TUC_PKI_003. [7] Schritt 5: Gültigkeitsstatus einer QES-CA wird gemäß [ETSI TS 119 612] Kap. 5.5.4 und Annex J durch den Servicestatus granted und withdrawn in der BNetzA-VL gekennzeichnet. Pre-eIDAS-relevante Servicestatus (undersupervision, supervisionincessation oder accredited) werden in granted bzw. (supervisionceased oder supervisionrevoked") in withdrawn überführt. Historien zum Servicestatus v. VDAs, hinterlegt im Element <ServiceHistory> in der BNetzA-VL, sind bei der Prüfung der CA zu berücksichtigen. [8] Die Einträge der QES-CA-Zertifikate in der BNetzA-VL besitzen gemäß [ETSI TS 119 612] Kap. 5.5.9.4 die Extension additionalServiceInformation http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatu

	res. [9] Schritt 6: Die Prüfung der Korrektheit der digitalen Signatur des Signaturzertifikats ist z.B. gemäß FDP_DAU.2/QES aus [BSI-CC-PP-0098] ein Bestandteil der QES-Prüfung, welcher sich nicht aus TUC_PKI_004 ableiten lässt. [10] Schritt 7: • Details zu den TSL-Einträgen für URLs für OCSP-Responder in der TI unter gemSpec_TSL#TIP1-A_7219. Das Verfahren zur Weiterleitung der OCSP-Anfrage an die zuvor ermittelte OCSP-Adresse aus dem AIA-Feld ist analog zur Weiterleitung von OCSP-Anfragen für QES-Zertifikate der Vorläuferkarten (HBAqSig/ZOD2). • Die Bereitstellung von Statusprüfdiensten durch die VDAs richtet sich nach den Vorgaben gemäß [eIDAS] Artikel 24, Abs. (2) Buchstabe k), Abs. (3) und (4). Die technische Umsetzung des Statusprüfdienstes per OCSP basiert auf [RFC6960]. [11] Schritt 11: Die Response enthält einen Statuscode („OCSPResponseStatus"), der gleich 0 („successful") ist: • Die Prüfung der certHash-Erweiterung richtet sich nach GS-A_4693 und [gemSpec_Krypt#GS-A_4393] • Die Auswertung der OCSP-Responses (Signatur der OCSP-Responses) gemäß [RFC6960] Kap. 4.1, 4.2 und 4.4 und Kap. 9.1.2 aus [gemSpec_PKI] [12] Schritt 9, 10: Zur Prüfung der OCSP-Response auf Integrität (Signatur): 1. Die gematik trifft hierzu keine Vorgabe zum Prüfmodell für die Validierung der Signatur von im TUC verwendeten OCSP-Signer-Zertifikaten. 2. Schritt 9: Das OCSP-Signer-Zertifikat kann gemäß [RFC6960] von der ausstellenden QES-CA selbst signiert sein oder von einer beliebigen aktuell qualifizierten CA (vgl. gemKPT_PKI_TIP#4.5). In Bezug auf die Anmerkung aus [ETSI TS 119 612] Kap. 5.5.1.1 (a) NOTE - können OCSP-Signer-Zertifikate aufgrund der Komplexitätsreduzierung nicht direkt als Statusprüfdienst in die BNetzA-VL eingetragen sein (s. URIs in Schritt 9), siehe Schritt 10. 3. Schritt 10: Falls keiner der URIs in der BNetzA-VL vorhanden ist, muss die Prüfung der Signatur der Response technisch gemäß [RFC6960] mittels des OCSP-Signer-Zertifikats erfolgen, welches von der ausstellenden QES-CA selbst signiert und im Feld „certs" der „BasicOCSPResponse" hinterlegt ist (Festlegung dazu siehe Vorgabe aus Kapitel 9.1.2.7).

	Der Vertrauensstatus des OCSP-Signer-Zertifikats muss somit über die BNetzA-VL prüfbar sein [13] Schritt 11b: Die OCSP-Response muss gemäß [RFC6960] Kap. 4.2 verarbeitet werden, unabhängig davon, ob das Feld "parameters" der Sequenz AlgorithmIdentifier innerhalb der CertID mit NULL belegt oder nicht gesetzt ist, siehe Tab_PKI_290. Der in [RFC5754] Kap. 2 empfohlene SHA2 als HashAlgorithmus für die Bildung von certID wird nicht von allen OCSP-Responder-Produkten unterstützt. [14] Schritt 12a: Falls die Referenzzeit nicht übergeben wird, wird die aktuelle Systemzeit verwendet. Die Variante 12a. ist unter diesen Umständen nicht möglich; sie wird also nicht berücksichtigt.
Zugehörige Diagramme/Tabelle	

[<=]

8.5.2 TUC_PKI_036 „BNetzA-VL Aktualisierung"

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

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

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

GS-A_5484 - TUC_PKI_036 „BNetzA-VL-Aktualisierung"
Alle Produkttypen, die die BNetzA-VL verwenden, MÜSSEN TUC_PKI_036 zur Aktualisierung umsetzen.

Tabelle 98: TUC_PKI_036 „BNetzA-VL Aktualisierung"

Element	Beschreibung
Name	TUC_PKI_036 „BNetzA-VL Aktualisierung"
Beschreibung	Dieser Use Case beschreibt die Aktualisierung der im System gespeicherten BNetzA-VL.
Anwendungsumfeld	System, das die BNetzA-VL verwendet
Vorbedingungen	Eine aktuell gültige TSL im System
Auslöser	Produkttypspezifischer Trigger
Eingangsdaten	• optional: neu eingebrachte BNetzA-VL-Datei
Komponenten	System

Ausgangsdaten	Status des Prozesses
Referenzen	[ETSI_TS_119_612] [XML] [XMLSig]
Standardablauf	Der Standardablauf stellt die Prüfungen dar, die vollzogen werden müssen. Die Reihenfolge der Schritte ist aber nicht normativ. Eine Trennung in zwei Prozesse oder eine Umstrukturierung, bei der alle notwendigen Prüfungen erfolgen, ist zulässig. 1. [System:] System startet die Aktualisierung der BNetzA-VL 2. [System:] Primäre BNetzA-VL Hash Download-Adresse aus der TSL extrahieren (s. [gemSpec_TSL#7.5]). 3. [System:] Von der im vorherigen Schritt ermittelten Downloadadresse den aktuellen BNetzA-VL Hashwert vom TSL-Dienst herunterladen. 4. [System:] Heruntergeladenen BNetzA-VL Hashwert mit dem Hashwert der aktuell im System gespeicherten BNetzA-VL (falls vorhanden) vergleichen. Falls die Hashwerte verschieden sind oder im System noch keine BNetzA-VL vorhanden ist muss die BNetzA-VL im System aktualisiert werden. 5. [System:] Primäre BNetzA-VL Download-Adresse aus der TSL extrahieren (s. [gemSpec_TSL#7.5]). 6. [System:] Von der ermittelten Downloadadresse die aktuelle BNetzA-VL vom TSL-Dienst herunterladen. 7. [System:] Die Wohlgeformtheit der BNetzA-VL-Datei prüfen. 8. [System:] Die BNetzA-VL-Datei gegen das XML-Schema gem. [ETSI_TS_119_612#Annex C.2] validieren. 9. [System:] Die Aktualität der BNetzA-VL prüfen. Dies geschieht anhand des aktuellen Datums und des Elements „NextUpdate" aus der BNetzA-VL. Die BNetzA-VL wird als aktuell bezeichnet, wenn ihr NextUpdate nicht in der Vergangenheit liegt. 10. [System:] Das verwendete BNetzA-VL-Signer-Zertifikat aus der BNetzA-VL-Datei extrahieren. 11. [System:] Prüfen ob das BNetzA-VL-Signerzertifikat in der TSL enthalten ist. Die Identifizierung des Zertifikats erfolgt durch

	• Suche nach einem TSPService mit ServiceTypeIdentifier für „BNetzA-VL" gem. [gemSpec_TSL#7.3.2] und • Vergleich des Elements X509Certificate in zugehöriger DigitalId mit dem BNetzA-VL-Signer-Zertifikat aus Schritt 10 12. [System:] Die XML-Signatur der BNetzA-VL-Datei mittels in der TSL gefundenem BNetzA-VL-Signerzertifikat gem. [XAdES] prüfen. 13. [System:] Die aktualisierte BNetzA-VL und deren Hashwert (falls vorhanden) sicher im System speichern. Ende des Use Cases.
Varianten/Alternativen	1a. System:] Wenn eine BNetzA-VL-Datei als Eingangsparameter eingebracht wurde, dann wird diese Datei validiert und geprüft. Weiter mit Schritt 7. 2a. [System:] Das Element ist nicht vorhanden. Weiter mit Schritt 3a.2 3a. [System:] Das Herunterladen von der primären Downloadadresse schlägt fehl. 3a.1 [System:] Das Herunterladen wird bis zu drei Mal wiederholt versucht (insgesamt wird der Vorgang also maximal vier Mal ausgeführt). Falls erfolgreich, weiter mit Schritt 4. 3a.2 [System:] Backup BNetzA-VL Hash Download-Adresse aus der TSL extrahieren (s. [gemSpec_TSL#7.5]). Falls nicht erfolgreich, weiter mit Schritt 5. 3a.3 [System:] Das Herunterladen wird von der Backup Downloadadresse ausgeführt. Falls erfolgreich, weiter mit Schritt 4. 3a.4 [System:] Das Herunterladen von der Backup Downloadadresse wird bis zu drei Mal wiederholt versucht (insgesamt wird der Vorgang also maximal vier Mal ausgeführt). Falls erfolgreich, weiter mit Schritt 4. Falls nicht erfolgreich, weiter mit Schritt 5. 4a. [System:] Die verglichenen Hashwerte sind identisch. In diesem Fall ist die im System gespeicherte BNetzA-VL aktuell. Ende des Use Cases ohne Fehler. 5b. [System:] Das Element ist nicht vorhanden. Weiter mit Schritt 6a.2 6a. [System:] Das Herunterladen von der primären

	Downloadadresse schlägt fehl. 6a.1 [System:] Das Herunterladen wird bis zu drei Mal wiederholt versucht (insgesamt wird der Vorgang also maximal vier Mal ausgeführt). Falls erfolgreich, weiter mit Schritt 7. 6a.2 [System:] Backup BNetzA-VL Download-Adresse aus der TSL extrahieren (s. [gemSpec_TSL#7.5]). 6a.3 [System:] Das Herunterladen wird von der Backup Downloadadresse ausgeführt. Falls erfolgreich, weiter mit Schritt 7. 6a.4 [System:] Das Herunterladen von der Backup Downloadadresse wird bis zu drei Mal wiederholt versucht (insgesamt wird der Vorgang also maximal vier Mal ausgeführt). Falls erfolgreich, weiter mit Schritt 7.
Fehlerfälle	Ein Abbruch des TUC führt nur dazu, dass keine neue BNetzA-VL gespeichert wird. Er hat keinen Einfluss auf die Gültigkeit der bestehenden BNetzA-VL. Das System muss dies jedoch protokollieren. 6a.2a [System:] Das Element ist nicht vorhanden. Ende des Use Case mit der Fehlermeldung VL_UPDATE_ERROR. 6a.4a [System:] Das Herunterladen der BNetzA-VL ist fehlgeschlagen. Ende des Use Cases mit der Fehlermeldung VL_UPDATE_ERROR. 7a. [System:] Die XML-Datei ist nicht wohlgeformt. Ende des Use Cases mit der Fehlermeldung VL_UPDATE_ERROR. 8a. [System:] Die XML-Schema-Validierung liefert einen Fehler. Ende des Use Cases mit der Fehlermeldung VL_UPDATE_ERROR. 9a. [System:] Die Aktualitäts-Prüfung ergibt, dass die BNetzA-VL abgelaufen ist (nextUpdate < aktuelles Datum). Ende des Use Cases mit der Fehlermeldung VL_UPDATE_ERROR. 10a. [System:] Das BNetzA-VL-Signer-Zertifikat lässt sich nicht aus der BNetzA-VL-Datei extrahieren. Ende des Use Cases mit der Fehlermeldung VL_UPDATE_ERROR. 11a. BNetzA-VL-Signerzertifikat ist nicht in der TSL enthalten. Ende des Use Case mit der Fehlermeldung VL_UPDATE_ERROR. 12a. [System:] Die Signatur ist nicht gültig. Ende des Use Cases mit der Fehlermeldung XML_SIGNATURE_ERROR.

Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	Das BNetzA-VL-Signer-Zertifikat wird vor Aufnahme in die TSL geprüft (s. [gemSpec_TSL#6.3]). Diese Prüfschritte werden darum nach dem Download innerhalb der TI nicht wiederholt.
Zugehörige Diagramme	

[<=]

8.6 Fehlercodes bei TSL- und Zertifikatsprüfung X.509

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

GS-A_4751 - Fehlercodes bei TSL- und Zertifikatsprüfung
Die Produkttypen der TI, die Zertifikate prüfen und die TSL auswerten MÜSSEN die Fehlercodes gemäß Tab_PKI_274 nutzen. Das Element CompType MUSS belegt werden mit „[Produkttyp]:PKI", wobei [Produkttyp] zu ersetzen ist durch den konkreten Produkttyp in der umzusetzenden Anforderung
[<=]

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

Code	Severity	ErrorType	ErrorText	Detail	Meldungskürzel
1001	Error	Technical	Es liegt keine gültige TSL vor		TSL_INIT_ERROR
1002	Error	Technical	Zertifikate lassen sich nicht extrahieren		TSL_CERT_EXTRACTION_ERROR
1003	Error	Security	Mehr als ein markierter V-Anker gefunden		MULTIPLE_TRUST_ANCHOR
1004	Error	Technical	TSL-Signer-		TSL_SIG_CERT_EXTRACTION_ERROR

			CA lässt sich nicht extrahieren		
1005	Error	Technical	Element „PointersTo OtherTSL" nicht vorhanden		TSL_DOWNLOAD_ADDRESS_ERROR
1006	Error	Technical	TSL-Download-adressen wiederholt nicht erreichbar		TSL_DOWNLOAD_ERROR
1007	Error	Security	Vergleich der ID und Sequence-Number entspricht nicht der Vergleichs-variante 6a		TSL_ID_INCORRECT
1008	Warning	Security	Die TSL ist nicht mehr aktuell		VALIDITY_WARNING_1
1009	Warning	Security	Über-schreitung des Elements NextUpdate um TSL-Grace-Period		VALIDITY_WARNING_2
1010	Warning	Security	*Veraltet: Diese Warn-meldung ist redundant zu VALIDITY_WARNING_1 (Code*		TSL_ NEXTUPDATE_EXPIRED

			1008). Sie soll deshalb nicht mehr verwendet werden.		
1011	Error	Technical	TSL-Datei nicht wellformed		TSL_NOT_WELLFORMED
1012	Error	Technical	Schemata der TSL-Datei nicht korrekt		TSL_SCHEMA_NOT_VALID
1013	Error	Security	Signatur ist nicht gültig		XML_SIGNATURE_ERROR
1016	Error	Security	KeyUsage ist nicht vorhanden bzw. entspricht nicht der vor-gesehenen KeyUsage		WRONG_KEYUSAGE
1017	Error	Security	Extended-KeyUsage entspricht nicht der vor-gesehenen Extended-KeyUsage		WRONG _EXTENDEDKEYUSAGE
1018	Error	Security	Zertifikats-typ-OID stimmt nicht überein		CERT_TYPE_MISMATCH
1019	Error	Technical	Zertifikat nicht lesbar		CERT_READ_ERROR
1021	Error	Security	Zertifikat ist zeitlich nicht gültig		CERTIFICATE_NOT_VALID_TIME
1023	Error	Security	Authority-Key-Identifier		AUTHORITYKEYID_DIFFERENT

			des End-Entity-Zertifikats von Subject-Key-Identifier des CA-Zertifikats unterschiedlich		
1024	Error	Security	Zertifikats-Signatur ist mathematisch nicht gültig.		CERTIFICATE_NOT_VALID_MATH
1026	Error	Technical	Das Element „Service-Supply Point" konnte nicht gefunden werden.		SERVICESUPPLYPOINT_MISSING
1027	Error	Technical	CA kann nicht in den TSL-Informationen ermittelt werden.	Keine Adresse hinterlegt.	CA_CERT_MISSING
1028	Warning	Technical	Die OCSP-Prüfung konnte nicht durchgeführt werden (1)	TOLERATE_OCSP_FAILURE=true	OCSP_CHECK_REVOCATION_FAILED
1029	Error	Technical	Die OCSP-Prüfung konnte nicht durchgeführt werden (2)	TOLERATE_OCSP_FAILURE=false	OCSP_CHECK_REVOCATION_ERROR
1030	Error	Security	OCSP-Zertifikat nicht		OCSP_CERT_MISSING

			in TSL-Infor-mationen enthalten		
1031	Error	Security	Signatur der Response ist nicht gültig.		OCSP_SIGNATURE_ERROR
1032	Error	Technical	OCSP-Responder nicht verfügbar		OCSP_NOT_AVAILABLE
1033	Error	Security	Kein Element Policy-Information vorhanden		CERT_TYPE_INFO_MISSING
1034	Error	Technical	*Veraltet: Diese Fehler-meldung wird nicht mehr verwendet. Stattdessen ist der Fehlercode 1032 zu verwenden.*		OCSP_PROXY_NOT_AVAILABLE
1036	Error	Security	Das Zertifikat ist ungültig. Es wurde nach der Sperrung der aus-gebenden CA ausgestellt.		CA_CERTIFICATE_ REVOKED_IN_TSL
1039	Warning	Security	Warnung, dass Offline-Modus aktiviert ist und		NO_OCSP_CHECK

			keine OCSP-Status-abfrage durch-geführt wurde		
1040	Error	Security	Bei der Online-status-prüfung ist ENFORCE_CERTHASH_CHECK auf ´true´ gesetzt, die OCSP-Response enthält jedoch keine certHash-Erweiterung		CERTHASH_EXTENSION_MISSING
1041	Error	Security	Der certHash in der OCSP-Response stimmt nicht mit dem certHash des vorliegenden Zertifikats überein.		CERTHASH_MISMATCH
1042	Error	Technical	Das TSL-SignerCA-Zertifikat kann nicht aus dem sicheren Speicher des Systems geladen werden.		TSL_CA_NOT_LOADED

1043	Error	Technical	CRL kann aus technischen Gründen nicht ausgewertet werden.		CRL_CHECK_ERROR
1044	Warning	Technical	Warnung, dass zum angefragten Zertifikat keine Statusinformationen verfügbar sind.		CERT_UNKNOWN
1047	Warning	Security	Das Zertifikat wurde vor oder zum Referenzzeitpunkt widerrufen.		CERT_REVOKED
1048	Error	Technical	Es ist ein Fehler bei der Prüfung des QC-Statements aufgetreten (z. B. nicht vorhanden, obwohl gefordert).		QC_STATEMENT_ERROR
1050	Warning	Technical	Die einem TUC zur Zertifikatsprüfung beigefügte OCSP-Response zu dem zu prüfenden		PROVIDED_OCSP_RESPONSE_NOT_VALID

			Zertifikat kann nicht erfolgreich gegen das Zertifikat validiert werden.		
1051	Error	Security	Die in einem OCSP-Response zurück-gelieferte Nonce stimmt nicht mit der Nonce des OCSP-Requests überein.		OCSP_NONCE_MISMATCH
1052	Error	Security	Attribut-Zertifikat kann dem über-gebenen Basis-Zertifikat nicht zu-geordnet werden.		ATTR_CERT_MISMATCH
1053	Error	Technical	Die CRL kann nicht herunter-geladen werden.		CRL_DOWNLOAD_ERROR
1054	Error	Technical	Eine verwendete CRL ist zum aktuellen Zeitpunkt nicht mehr gültig.		CRL_OUTDATED_ERROR
1055	Error	Security	CRL-Signer-Zertifikat nicht		CRL_SIGNER_CERT_MISSING

			in TSL-Informationen enthalten		
1057	Error	Security	Signatur der CRL ist nicht gültig.		CRL_SIGNATURE_ERROR
1058	Error	Technical	Die OCSP-Response enthält eine Exception-Meldung.		OCSP_STATUS_ERROR
1059	Error	Security	CA-Zertifikat für QES-Zertifikatsprüfung nicht qualifiziert		CA_CERTIFICATE_NOT_QES_QUALIFIED
1060	Error	Technical	Die VL kann nicht aktualisiert werden.		VL_UPDATE_ERROR
1061	Error	Security	CA (laut TSL) nicht autorisiert für die Herausgabe dieses Zertifikatstyps.		CERT_TYPE_CA_NOT_AUTHORIZED
1062	Error	Security	Das QES-EE-Zertifikat ist ungültig. Es wurde nach der Sperrung der ausgebenden QES-CA ausgestellt.		CA_CERTIFICATE_REVOKED_IN_BNETZA_VL

8.7 Zertifikatsprüfung CV-Zertifikate der 2. Generation

Die Prüfung von CV-Zertifikaten der Generation 2 beschränkt sich nicht nur auf die Prüfung der Vertrauenskette und die Signaturprüfung. Zusätzlich werden einige der verwendeten Schlüsselattribute des CV-Zertifikats und der weiteren CV-Zertifikate in der Vertrauenskette geprüft bzw. ausgewertet, insbesondere das Certificate Effective Date (CED) und das Certificate Expiration Date (CXD). Die Prüfung der Signatur eines CV-Zertifikats erfolgt mittels eines öffentlichen Schlüssels, der vor der Zertifikatsprüfung ausgewählt wird. Die Prüfschritte erfolgen gemäß Schalenmodell komplett „intern" durch das Betriebssystem der prüfenden Chipkarte.

Handelt es sich bei dem Produkttyp der TI, der das CV-Zertifikat prüfen soll, um eine Chipkarte, dann wird dieser öffentliche Schlüssel durch ein MSE-Set-Kommando der Karte bekannt gegeben.

GS-A_5009 - Prüfung der mathematischen Korrektheit von CV-Zertifikate der Generation 2
Die Produkttypen der TI, die CV-Zertifikate prüfen, MÜSSEN bei der Prüfung von CV-Zertifikaten der Generation 2 die Prüfung der mathematischen Korrektheit vornehmen, d. h. ob die Signatur des CV-Zertifikats mit dem CV-Zertifikat der ausstellenden TSP-CVC und ob die Signatur des TSP-CVC -Zertifikats mit dem CV-Zertifikat der ausstellenden CVC-Root-CA erfolgreich geprüft werden kann.
[<=]

GS-A_5010 - Prüfung der Signatur eines CV-Zertifikats der Generation 2 mit Hilfe des CV-Zertifikats des Herausgebers
Die Produkttypen der TI, die CV-Zertifikate prüfen, MÜSSEN bei der Prüfung der mathematischen Korrektheit der Signatur eines CV-Zertifikates *C* die im CV-Zertifikat des öffentlichen Schlüssels des Herausgebers enthaltenen Schlüsselattribute dieses öffentlichen Schlüssels anwenden. Die Prüfung MUSS den Vorgaben aus Tabelle TAB_PKI_908 folgen.
[<=]

Tabelle 100: Tab_PKI_908 Prüfung der Signatur eines CV-Zertifikats der Generation 2 mit Hilfe des CV-Zertifikats des Herausgebers

Prüfung der Korrektheit der Signatur eines CV-Zertifikats *C*
Sei die Nachricht M die gemäß Tabelle Tab_PKI_905 zu signierende Nachricht M des CV-Zertifikates C. Sei Signatur = R || S gemäß Tabelle Tab_PKI_906 die Signatur der Nachricht M des CV-Zertifikats *C.* *Sei PuK* der im CV-Zertifikat des Herausgebers enthaltene öffentliche Signaturschlüssel des Herausgebers.
Bei der Prüfung der Signatur MUSS der domainParameter des Schlüssels *PuK* gemäß des CV-Zertifikats des Herausgebers genutzt werden (gemäß Tab_PKI_901). Falls das Wertfeld von DO´86´ im CV-Zertifikat des Herausgebers eine Länge von A. ´41´= 65 hat, gilt PuK.domainParameter = brainpoolP256r1. B. ´61´= 97 hat, gilt PuK.domainParameter = brainpoolP384r1. C. ´81´= 129 hat, gilt PuK.domainParameter = brainpoolP512r1.
Bei der Prüfung der Signatur MUSS das Hashverfahren gemäß dem domainParameter genutzt werden (gemäß Tab_PKI_906).

Falls CAR und CHAT aus CV-Zertifikat *C* und CV-Zertifikat des Herausgebers nicht miteinander korrespondieren sind, dann ist das CV-Zertifikat *C* nicht korrekt.

GS-A_5011 - Prüfung der Gültigkeit von CV-Zertifikaten der Generation G2
Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN bei der Prüfung von CV-Zertifikaten der Generation 2 die Prüfung der Gültigkeit vornehmen, d. h. die Gültigkeit des CV-Zertifikats gemäß Tabelle TAB_PKI_909 prüfen.
[<=]

Tabelle 101: Tab_PKI_909 Gültigkeit eines CV-Zertifikats der Generation 2

Gültigkeit eines CV-Zertifikats *C*
Ein CV-Zertifikat einer CVC-Root-CA ist gültig, wenn • das CV-Zertifikat mathematisch korrekt gebildet ist und • das Certificate Expiration Date (CXD) des CV-Zertifikats noch nicht überschritten ist.
Ein CV-Zertifikat *C*, das von einem Herausgeber der Generation 2 (TSP-CVC oder CVC-Root-CA) erzeugt wurde, ist gültig, wenn • das CV-Zertifikat für den öffentlichen Schlüssels des Herausgebers gültig und • das CV-Zertifikat mathematisch korrekt gebildet ist und • das Certificate Expiration Date (CXD) des CV-Zertifikats *C* nicht überschritten ist.
In allen anderen Fällen ist das CV-Zertifikat ungültig.

GS-A_5012 - Prüfung von CV-Zertifikaten der Generation 2
Die Produkttypen der TI, die CV-Zertifikate prüfen, MÜSSEN bei der Prüfung von CV-Zertifikaten der Generation 2 die Prüfung der mathematischen Korrektheit und die Prüfung der Gültigkeit des CV-Zertifikats gemäß Schalenmodell vornehmen.

[<=]

9 OCSP-Statusinformation

Dieses Kapitel enthält die Festlegung von Schnittstellen, die durch mehrere Produkttypen der PKI bereitgestellt werden müssen. Diese Schnittstellen werden in der vorliegenden Spezifikation beschrieben. Eine wiederholte Darstellung dieser Schnittstellen in den Spezifikationen der Produkttypen erfolgt nicht, vielmehr wird in diesen Dokumenten auf die folgenden Beschreibungen verwiesen.

9.1 Statusprüfung

Gemäß [gemKPT_Arch_TIP] ist zur Statusprüfung die Schnittstelle I_OCSP_Status_Information durch die Produkttypen

- TSL-Dienst,
- gematik Root-CA
- TSP-X.509 nonQES,
- TSP-X.509 QES und
- OCSP-Responder Proxy

anzubieten. Darüber können Nutzer, wie z. B. Konnektor und VPN-Zugangsdienst, Statusinformationen zu X.509-Zertifikaten von OCSP-Respondern erhalten. Die Schnittstelle implementiert die logische Operation check_Revocation_Status mit der der Sperrstatus eines X.509-Zertifikats ermittelt werden kann (vgl. auch [gemKPT_PKI_TIP]).

GS-A_4669 - Umsetzung Statusprüfdienst
Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES, TSP-X.509 QES und OCSP-Responder Proxy MÜSSEN die Schnittstelle I_OCSP_Status_Information implementieren.
[<=]

Die Algorithmen und Parameter für die Erstellung der Signaturen über die OCSP-Responses des OCSP werden in [gemSpec_Krypt] festgelegt. Die Statusprüfung von QES-CA-Zertifikaten erfolgt durch die Prüfung des Vorkommens des Zertifikats der QES-CA in der BNetzA-VL und des Dienststatus (Servicestatus) der QES-CA in der TSL und BNetzA_VL (s. Kap. 8.5). Anhand der gemäß TIP1-A_7219 aus der TSL ermittelten OCSP-Adressen werden Statusinformationen angefragter QES-Zertifikate eingeholt.

9.1.1 Schnittstelle I_OCSP_Status_Information

GS-A_4670 - Statusprüfdienst über Gültigkeitszeitraum des X.509-Zertifikats
Die Produkttypen TSL-Dienst, gematik Root-CA und TSP-X.509 nonQES MÜSSEN den Statusprüfdienst über den gesamten Gültigkeitszeitraum des zu prüfenden Zertifikats sicherstellen. Darüber hinausgehende Anforderungen an die Verfügbarkeit von Statusinformationen MÜSSEN in der Policy des Zertifikatsherausgebers definiert sein.
[<=]

Die gematik Root-CA sowie TSP-X.509 nonQES können Dritte mit der Bereitstellung des Statusprüfdienstes beauftragen.

GS-A_4672-01 - Statusprüfdienst QES gemäß den Vorgaben von eIDAS und Standards
Der TSP-X.509 QES MUSS für den Statusprüfdienst die Vorgaben gemäß [eIDAS] und [VDG§16] sowie den technischen Anforderungen nach [RFC6960] erfüllen.
[<=]

Abweichungen von [RFC6960] werden detailliert in [gemKPT_PKI_TIP#4.5] beschrieben.

GS-A_5050 - gematik-Root-CA Statusprüfdienst im Internet
Die gematik Root-CA MUSS im Internet einen OCSP-Dienst für die Statusauskünfte der CAs zur Verfügung stellen, die Zertifikate zur Verwendung in HBA und SMC-B und eGK bzw. alternative Versichertenidentitäten herausgeben.

[<=]

GS-A_5052 - gematik Root-CA Zertifikatsstatus
Die gematik Root-CA MUSS sicherstellen, dass die Zertifikatsstatusinformation zu einem X.509-CA-Zertifikat im Internet identisch ist zum Status dieses CA-Zertifikates in der TSL.
[<=]

GS-A_5053 - TI-Zertifikatstypen im Internet
Der TSP-X.509 nonQES für HBA, eGK oder SMC-B MUSS Zertifikatsstatusinformationen zu den ausgestellten X.509-Zertifikaten im Internet bereitstellen.
[<=]

Hinweis: Für einen TSP-X.509 nonQES eGK ist es in Abstimmung mit der gematik bis maximal 06/2020 zulässig, noch keine Zertifikatsstatusinformationen im Internet bereitzustellen.

GS-A_5051 - TSP-X.509 nonQES Zertifikatsstatus
Der TSP-X.509 nonQES für HBA oder SMC-B MUSS sicherstellen, dass die Zertifikatsstatusinformation zu einem X.509-Zertifikat in der TI und im Internet identisch ist.
[<=]

9.1.1.1 Schnittstellendefinition

Gemäß [gemKPT_PKI_TIP#TIP1-A_2140] muss die Schnittstelle zur Statusprüfung von nonQES-Zertifikaten der eGK und der alternativen Versichertenidentitäten technisch nach [RFC6960] implementiert werden. Bei allen anderen X.509-Zertifikaten, in denen die CertHash-Erweiterung (Positive Statement) obligatorisch verwendet wird, erfolgt die Statusprüfung zusätzlich gemäß GS-A_4693.

9.1.1.1.1 OCSP-Request

Der OCSP-Request und Erweiterungen sind komplett in [RFC6960] beschrieben. Die certHash-Erweiterung (außer nonQES-Zertifikaten einer eGK) wird gemäß GS-A_4693 umgesetzt.

Wesentliches Merkmal zur Identifizierung des Zertifikats ist dessen Seriennummer. Der Herausgeber des Zertifikats wird über Hashwerte seines öffentlichen Schlüssels und

seines Namens identifiziert. OCSP-Requests können gemäß den Standards signiert sein, dies wird (s. a. Abschnitt 9.1.2.1) in der TI allerdings nicht gefordert und deshalb diese Signaturen auch nicht geprüft.

GS-A_4674-01 - OCSP-Requests gemäß Standards
Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN OCSP-Requests gemäß [RFC6960] unter obligatorischer Verwendung der CertHash-Erweiterung verarbeiten können. Der Parameter certID MUSS gemäß Tab_PKI_290 gebildet werden.
[<=]

Tabelle 102: Tab_PKI_290 Struktur certID in OCSP-Request/Response

#	Asn.1 Definition	TI-spezifische Vorgaben
1	`CertID ::= SEQUENCE {`	
2	`hashAlgorithm AlgorithmIdentifier OPTIONAL, {DIGEST-ALGORITHM, {...}}`	`hashAlgorithm` ist der zur Erzeugung der Hashwerte `issuerNameHash` und `issuerKeyHash` verwendete Hash-Algorithmus. Default SHA1 gemäß [RFC5019] Kap. 2.1.1 und [RFC3370] Kap. 2.1.1, optional SHA2 gemäß [RFC5754] Kap. 2. Das Setzen `AlgorithmIdentifier` mit oder ohne `NULL` ist optional.
3	`issuerNameHash OCTET STRING,`	`Hash of issuer's DN.`
4	`issuerKeyHash OCTET STRING,`	`Hash of issuer's public key`
5	`serialNumber CertificateSerialNumber`	`serialNumber is the serial number of the certificate`

GS-A_4957-01 - Beschränkungen OCSP-Request
Komponenten (Produkttypen der TI, aAdG und aAdG-NetG-TI), die Zertifikate prüfen, DÜRFEN (abweichend von [RFC6960]) je OCSP-Request NICHT mehr als den Status für genau ein Zertifikat abfragen. Ist hierbei die Verwendung der OCSP-Extension „Nonce" zulässig, DARF diese die Länge von 256 Bit NICHT überschreiten.**[<=]**

WA-A_2033 - Nutzung der OCSP-Responder der TI
Eine aAdG oder aAdG-NetG-TI MUSS die OCSP-Responder der TI nutzen.**[<=]**

9.1.1.1.2 OCSP-Response

Die OCSP-Response und ihre Extension sind komplett in [RFC6960] beschrieben. Die certHash-Erweiterung (außer nonQES-Zertifikaten einer eGK) wird gemäß GS-A_4693 umgesetzt.

Wesentlicher Inhalt ist der Status des angefragten Zertifikats, sowie zeitliches Aussagen zu dem gelieferten Status und dessen Aktualität. Die Antwort ist signiert. Weitere Details siehe Abschnitt 9.1.2.2 und folgende.

GS-A_4675-01 - OCSP-Responses zu eGK-Zertifikaten gemäß Standards
Der TSP-X.509 nonQES eGK MUSS für Statusauskünfte zu X.509-Zertifikaten OCSP-Responses gemäß [RFC6960] und [RFC5280] erzeugen.
[<=]

GS-A_4676-01 - OCSP-Responses gemäß Standards
Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES (außer eGK) und TSP-X.509 QES MÜSSEN für Statusauskünfte zu X.509-Zertifikaten OCSP-Responses gemäß [RFC6960] und [RFC5280] unter obligatorischer Verwendung der CertHash-Erweiterung erzeugen. Der Parameter certID MUSS gemäß Tab_PKI_290 gebildet werden.
[<=]

GS-A_5124-01 - OCSP-Responses mit Parameter Nonce gemäß [RFC6960]
Der TSP-X.509 QES MUSS für Statusauskünfte zu X.509-Zertifikaten den Parameter „Nonce" für OCSP-Responses gemäß Tab_PKI_289 unterstützen.

Tabelle 103 : Tab_PKI_289 Struktur Nonce

#	Asn.1 Definition		TI-spezifische Vorgaben
1	id-pkix-ocsp	OBJECT IDENTIFIER ::= {id-ad-ocsp}	Siehe [RFC6960#4.4.1, B.1 und B.2]
2	id-pkix-ocsp-nonce	OBJECT IDENTIFIER ::= {id-pkix-ocsp 2}	Referenzen siehe oben
3		Nonce ::= OCTET STRING	optional

[<=]

Ergänzend zu [RFC6960] kann der OCSP-Client anhand der Festlegung gemäß Tab_PKI_289 jeden Rückgabewert analysieren. Nicht alle Standard-OCSP-Responder unterstützen diese Nonce-Erweiterung.

9.1.1.2 Umsetzung

GS-A_4677 - Spezifikationskonforme OCSP-Responses
Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN sicherstellen, dass ihr OCSP-Responder spezifikationskonform antwortet, wenn der OCSP-Request „well formed" spezifikationskonform formuliert ist und der Responder für diesen Service konfiguriert ist.
[<=]

GS-A_4678 - Signierte OCSP-Responses
Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN sicherstellen, dass ihr OCSP-Responder alle Antworten (Responses) mit

Response-Status 'successful' (0) digital signiert.
[<=]

GS-A_4679 - Signatur zu Statusauskünften von nonQES-Zertifikaten
Die Produkttypen TSL-Dienst, gematik Root-CA, und TSP-X.509 nonQES MÜSSEN zur Erzeugung von Signaturen über OCSP-Responses mit Statusauskünften zu nicht-qualifizierten X.509-Zertifikaten ein Schlüsselpaar einsetzen, für das ein nicht-qualifiziertes X.509-Zertifikat ausgestellt wurde.
[<=]

GS-A_5517 - Schlüsselgenerationen der OCSP-Signer-Zertifikate
Die Produkttypen TSL-Dienst, gematik Root-CA und TSP-X.509 nonQES MÜSSEN sicherstellen, dass zum Signieren von OCSP-Responses für Zertifikate einer bestimmten Schlüsselgeneration, ausschließlich ein OCSP-Signer-Zertifikat derselben Schlüsselgeneration (gemäß [gemSpec_Krypt#GS-A_4357] bzw. [gemSpec_Krypt#GS-A_4358]) verwendet wird.

[<=]

GS-A_4684 - Auslassung der Signaturprüfung bei OCSP-Requests
Zur Gewährleistung der Performance MÜSSEN die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 QES und TSP-X.509 nonQES OCSP-Responder so konfigurieren, dass signierte Requests wie unsignierte Requests behandelt werden und die Signaturprüfung der Requests entfällt.
[<=]

GS-A_4685 - Statusprüfdienst - Steigerung der Performance
Die Produkttypen TSL-Dienst, gematik Root-CA und TSP-X.509 nonQES SOLLEN Methoden des Response-Caching anwenden, um die Performance des Statusprüfdienstes zu steigern.
[<=]

9.1.1.3 Nutzung

Gemäß [gemKPT_PKI_TIP] müssen anfragende Komponenten sicherstellen, dass je OCSP-Request nicht mehr als der Status für ein X.509-Zertifikat abgefragt wird (vgl. [gemKPT_PKI_TIP#TIP1-A_2144]).

Weiterhin müssen Produkttypen der TI, die OCSP-Responses auswerten, sicherstellen, dass für jede mögliche Ausprägung der zurückgegebenen Parameter eine geordnete Reaktion implementiert wird (vgl. [gemKPT_PKI_TIP#TIP1-A_2149]).

9.1.2 Artefakte

9.1.2.1 OCSP-Response – Response Status

GS-A_4686 - Statusprüfdienst – Response Status
Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN sicherstellen, dass für den Response Status die Werte „successful", „malformedRequest", „internalError", „tryLater" und „unauthorized" gemäß Tab_PKI_291 unterstützt werden.
[<=]

Tabelle 104: Tab_PKI_291 OCSP-Response Status Ergebnisse

Ergebnis Anfrage	Bedeutung
successful	Erfolgreiche Bearbeitung einer Anfrage
malformed Request	Wegen fehlerhaftem Anfrageformat konnte keine erfolgreiche Bearbeitung der Anfrage erfolgen.
internalError	Auftretung eines internen Fehlers beim OCSP-Server
tryLater	Nicht-Verfügbarkeit des OCSP-Servers (temporär)
unauthorized	Der Client ist nicht berechtigt

GS-A_4687 - Statusprüfdienst – Response Status sigRequired
Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN sicherstellen, dass für den Response Status der Wert „sigRequired" nicht verwendet wird.
[<=]

Mit dem Response Status „sigRequired" fordert der OCSP-Responder explizit, dass die Anfrage vom OCSP-Client signiert werden muss. Da keine signierten OCSP-Requests in der TI gefordert sind, darf der Exception Case „sigRequired" vom OCSP-Responder nicht verwendet werden.

9.1.2.2 OCSP-Response - Zeiten

GS-A_4688 - Statusprüfdienst – Angabe von Zeitpunkten
Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN sicherstellen, dass die Angabe zu den Zeitpunkten **`producedAt`**, **`thisUpdate`** und **`nextUpdate`** spezifikationskonform gemäß Tab_PKI_292 erfolgt.
[<=]

Tabelle 105: Tab_PKI_292 Zeiten in einer OCSP-Response

Zeiten	Bedeutung
thisUpdate	„**`thisUpdate`**" enthält den Zeitpunkt, für den die gemachte Aussage gültig ist. Es gibt den Zeitpunkt an zu der die Statusinformation als korrekt angesehen wurde.
nextUpdate	„**`nextUpdate`**" enthält die Zeit, wann neue Informationen über das angefragte Zertifikat verfügbar sein werden. OCSP-Antworten, die keinen „nextUpdate" Zeitpunkt enthalten, zeigen an, dass jederzeit neuere Statusinformationen zu Zertifikaten vorhanden sein können.
producedAt	Der Zeitpunkt der Signierung einer OCSP-Response.

Der Zeitpunkt **`nextUpdate`** ist nur für OCSP-Antworten sinnvoll, die auf CRLs basieren.

GS-A_4689 - Statusprüfdienst – Zeitquelle von producedAt
Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN sicherstellen, dass der Zeitpunkt **`producedAt`** auf einer in der TI verbindlichen

Zeitquelle beruht.
[<=]

GS-A_5215 - Festlegung der zeitlichen Toleranzen in einer OCSP-Response
Produkttypen der TI, die Zertifikate prüfen, MÜSSEN die Angaben zu den Zeitpunkten **`producedAt`**, **`thisUpdate`** und **`nextUpdate`** in der OCSP-Response mit einer Zeit-Toleranz bezüglich der lokalen Systemzeit interpretieren.
Produkttypen der TI, die Zertifikate prüfen, MÜSSEN die folgenden Fälle als gültig akzeptieren, wenn im Rahmen von TUC_PKI_006
eine Online-Abfrage durchgeführt wird:
(a) producedAt liegt weniger als (oder ist gleich wie) die Toleranz ‚t' gegenüber der Systemzeit bei Erhalt der Response in der Vergangenheit.
(b) producedAt liegt weniger als (oder ist gleich wie) die Toleranz ‚t' gegenüber der Systemzeit bei Erhalt der Response in der Zukunft.
(c) thisUpdate liegt weniger als (oder ist gleich wie) die Toleranz ‚t' gegenüber der Systemzeit bei Erhalt der Response in der Zukunft.
(d) nextUpdate liegt weniger als (oder ist gleich wie) die Toleranz ‚t' gegenüber der Systemzeit bei Erhalt der Response in der Vergangenheit.
Produkttypen der TI, die Zertifikate prüfen, MÜSSEN die Toleranz ‚t' auf genau 37,5 Sekunden ansetzen.
[<=]

Hinweis: Das in der Anforderung spezifizierte Verhalten weicht von den Empfehlungen von [RFC2560] / [RFC6960] Kap. 4.2.2.1 zur Prüfung von thisUpdate und nextUpdate ab.
Das Setzen von Zeittoleranzen (mindestens bezüglich nextUpdate) wird aber in [RFC5019], Kap. 4 besprochen: „[…] Clients MAY allow configuration of a small tolerance period for acceptance of responses after nextUpdate to handle minor clock differences relative to responders and caches. This tolerance period should be chosen based on the accuracy and precision of time synchronization technology available to the calling application environment. […]"

9.1.2.3 OCSP-Response - CertStatus

GS-A_4690 - Statusprüfdienst – Status des X.509-Zertifikats
Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN sicherstellen, dass ein OCSP-Responder den Status eines Zertifikats mit einem der drei Werte a) good, b) revoked, c) unknown gemäß Tab_PKI_293 zurückgibt.
[<=]

Tabelle 106: Tab_PKI_293 Status der OCSP Antworten

OCSP Antwort	Bedeutung
good	Der Zustand „good" sagt aus, dass zum Zeitpunkt thisUpdate das Zertifikat nicht gesperrt war. Good sagt aber nichts über die Gültigkeitsdauer und Existenz des Zertifikates aus.
revoked	Der Zustand „revoked" sagt aus, dass das Zertifikat von der zugehörigen Zertifizierungsstelle ausgestellt wurde, dem OCSP-Responder bekannt ist und temporär oder endgültig gesperrt ist.
unknown	Diese Antwort bedeutet, dass der OCSP-Responder das nachgefragte Zertifikat nicht kennt. Entweder ist dieser von der entsprechenden CA nicht

	für die Beantwortung von Statusabfragen autorisiert oder es können keine Informationen zu dem Zertifikat gefunden werden.

9.1.2.4 OCSP-Response - CertID

GS-A_4691 - Statusprüfdienst – X.509-Zertifikat mit Status „unknown"
Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN sicherstellen, dass im Falle eines `certStatus` mit Wert „unknown" im Feld `certID` der Struktur `SingleResponse` der Inhalt des `certID`-Feldes in der Struktur `Request` des OCSP-Requests wiederholt wird.
[<=]

9.1.2.5 OCSP-Response – Sperrzeitpunkt und Sperrgrund

GS-A_4692 - Statusprüfdienst – Angabe Sperrzeitpunkt
Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN sicherstellen, dass im Falle eines gesperrten X.509-Zertifikats die Angabe des Sperrzeitpunkts im Teilfeld **`revocationTime`** in einer OCSP-Response erfolgt.
[<=]

GS-A_5090 - Statusprüfdienst – Keine Angabe von Sperrgründen
Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES SOLLEN sicherstellen, dass kein Sperrgrund mit der OCSP-Response geliefert wird.
[<=]

9.1.2.6 OCSP-Response – CertHash

GS-A_4693-01 - Statusprüfdienst – Positive Statement
Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES (außer nonQES-Zertifikaten einer eGK) und TSP-X.509 QES MÜSSEN sicherstellen, dass die von ihnen betriebenen OCSP-Responder bei OCSP-Antworten immer die OCSP-Extension „certHash" gemäß Tab_PKI_288 in der OCSP-Response des zu prüfenden X.509-Zertifikats mitsenden

Tabelle 107 : Tab_PKI_288 Struktur certHash

#	Asn.1 Definition	TI-spezifische Vorgaben
1	id-commonpki-at-certHash OBJECT IDENTIFIER ::= {1 3 36 8 3 13}	
2	CertHash ::= SEQUENCE {	
3	hashAlgorithm AlgorithmIdentifier,	Algorithmus-Identifier zur Berechnung des Hash-Wertes, Details siehe [gemSpec_Krypt#GS-A_4393].
4	certificateHash OCTET STRING }	Hash-Wert über das DER-kodierte angefragte Zertifikat.

[<=]

9.1.2.7 OCSP-Response – Responder-Zertifikate

A_19500 - Statusprüfdienst – Hinterlegung OCSP-Signer-Zertifikat
Der TSP-X_509 QES MUSS für Statusauskünfte zu X.509-Zertifikaten das für die Überprüfung der OCSP-Response auf Integrität (mathematische Korrektheitsprüfung der Signatur) benötigte OCSP-Signer-Zertifikat im Feld „certs" der zu übermittelnden „BasisOCSPResponse" gemäß [RFC6960] hinterlegen.**[**<=**]**

9.1.3 Testunterstützung

Bei der PKI für X.509-Zertifikate wird zwischen einer Produktiv-PKI und einer Test-PKI unterschieden.

GS-A_4694 - Betrieb von OCSP-Responder für Test-PKI-CAs
Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN neben OCSP-Respondern für die produktive PKI ebenfalls OCSP-Responder für die Test-PKI betreiben.
[<=**]**

9.1.4 Hardwaremerkmale

Die Statusprüfung setzt keine besonderen Hardwaremerkmale voraus.

10 Anhang A – Sektorspezifische Ausprägungen der SMC-B-Zertifikate

Die nachfolgenden Profiltabellen der Sektoren referenzieren auf die Festlegungen aus Kap. 5.3.4 für alle sektorübergreifenden Attribute und ergänzen/ersetzen diese um sektorspezifische Ausprägungen.

Die Profiltabellen gelten einheitlich für die Zertifikate:

- C.HCI.AUT
- C.HCI.ENC
- C.HCI.OSIG

Hinweis: Während der Erprobungsphase ORS1 enthielten die Zertifikate im Feld ***CertificatePolicies*** *zusätzlich die Policy-OID der „Policy für SMC-B Zertifikate während Erprobung". Die während der Erprobungsphase ausgegebenen Zertifikate behalten ihre Gültigkeit bis zu ihrem zeitlichen Ablauf.*

10.1 KZBV

Tabelle 108: Tab_SMCB_KZBV_ZA SMC-B-Zertifikate für Zahnarzt (Sektor KZBV)

Element	Inhalt	Kar.	
certificate	C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
tbsCertificate			
version	siehe Kap 5.3.4		
serialNumber	siehe Kap 5.3.4		
signature	siehe Kap 5.3.4		
issuer	siehe Kap 5.3.4		
validity	siehe Kap 5.3.4		
subject			
commonName	**Gemäß Freigabedaten der zuständigen KZV**	**1**	
title	**nicht belegt**	**0**	
givenName	**nicht belegt**	**0**	
surName	**nicht belegt**	**0**	
serialNumber	**TI-weit eindeutiger Identifier der Karte in der Form: <TSP-ID>.<ICCSN> (<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)**	**1**	
organizationalUnitName	**nicht belegt**	**0**	
organizationName	**Telematik-ID gemäss Freigabedaten der zuständigen KZV**	**1**	

	streetAddress	**nicht belegt**	**0**	
	postalCode	**nicht belegt**	**0**	
	localityName	**nicht belegt**	**0**	
	stateOrProvinceName	**nicht belegt**	**0**	
	countryName	siehe Kap 5.3.4	1	
	andere Attribute		0	
subjectPublicKeyInfo		siehe Kap 5.3.4		
extensions				critical
	SubjectKeyIdentifier {2 5 29 14}	siehe Kap 5.3.4	1	FALSE
	KeyUsage {2 5 29 15}	siehe Kap 5.3.4	1	**TRUE**
	SubjectAltNames {2 5 29 17}	rfc822Name type-id= {2 5 4 3}; value= ggf. überlange Institutionsnamen, Alternativnamen oder Ergänzungen	0-1 0-1	FALSE
	BasicConstraints {2 5 29 19}	siehe Kap 5.3.4	1	**TRUE**
	CertificatePolicies {2 5 29 32}	siehe Kap 5.3.4 **zusätzlich: policyQualifierInfo**	1 **0**	FALSE
	CRLDistributionPoints {2 5 29 31}	**CDP des TSP für das betreffende Zertifikat**	**1**	**FALSE**
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap 5.3.4	1	FALSE
	AuthorityKeyIdentifier {2 5 29 35}	siehe Kap 5.3.4	1	FALSE
	Admission {1 3 36 8 3 3}	**admissionAuthority = {O=<von der KZBV benannte attributbestätigende Stelle – zuständige KZV>,C=DE}** **professionItem = Beschreibung zu <oid_zahnarztpraxis> gemäß [gemSpec_OID#GS-A_4443]** **professionOID = OID <oid_zahnarztpraxis> gemäß [gemSpec_OID#GS-A_4443]** **registrationNumber = <Telematik-ID gemäss Freigabedaten der zuständigen KZV>**	**1** **1** **1** **1**	**FALSE**
	ExtendedKeyUsage {2 5 29 37}	siehe Kap 5.3.4	*)	FALSE
	andere Erweiterungen		0	
signatureAlgorithm		siehe Kap 5.3.4		
signature		siehe Kap 5.3.4		

*) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und Tab_PKI_240 ist die Kardinalität gleich 0.

Hinweis: In einer früheren Version der vorliegenden Spezifikation war an dieser Stelle das SMC-B-ORG-Profil des Sektors KZBV zu finden in Form der Tabelle "Tab_SMCB_KZBV_KZV SMC-B-Zertifikate für KZV (Sektor KZBV)". Dieses Profil ist nun fachlich unverändert in Kapitel 10.7 mittels der Tabelle "Tab_SMCB_ORG_Gen - Generisches Zertifikatsprofil" beschrieben.

10.2 KBV

Die nachfolgende Profiltabelle der durch die KBV betreuten Sektoren gilt für die Sektoren:

- Niedergelassene Vertragsärzte (KV)
- Niedergelassene Psychologische Psychotherapeuten (KV)
- Niedergelassene Kinder- und Jugendlichenpsychotherapeuten (KV)

Tabelle 109: Tab_SMCB_KV-T SMC-B-Zertifikate für Sektoren der KBV

Element	Inhalt	Kar.	
certificate	C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
tbsCertificate			
version	siehe Kap 5.3.4		
serialNumber	siehe Kap 5.3.4		
signature	siehe Kap 5.3.4		
issuer	siehe Kap 5.3.4		
validity	siehe Kap 5.3.4		
subject			
commonName	**Erste zwei Zeilen der Anschriftenzone (DIN5008), somit „Kurzname" der Institution, so wie für das Anschriftenfeld definiert.**	**1**	
title	**Titel des Verantwortlichen/Inhabers**	**0-1**	
givenName	**Vorname des Verantwortlichen/Inhabers (mehrere Vornamen sind durch Blank oder Bindestrich getrennt)**	**0-1**	
surName	**Familienname des Verantwortlichen/Inhabers**	**0-1**	
serialNumber	**nicht belegt**	**0**	

			organizationalUnitName	**nicht belegt**	**0**	
			organizationName	**9-stellige Betriebsstättennummer (z.B. „121234512") der Praxis als eindeutige Nummer. Für privat abrechnende Ärzte wird hier eine 10-stellige Ersatznummer eingefügt.**	**1**	
			streetAddress	**Strassen-Anschrift der Institution (mehrere Wörter sind durch Blank getrennt)**	**0-1**	
			postalCode	**Postleitzahl des Ortes der Institution (Deutsche PLZ werden 5-stellig abgebildet)**	**0-1**	
			localityName	**Stadt des Institut-Standortes**	**0-1**	
			stateOrProvinceName	**Bundesland des Institut-Standortes**	**0-1**	
			countryName	siehe Kap 5.3.4	1	
			andere Attribute		0	
		subjectPublicKeyInfo		siehe Kap 5.3.4		
		extensions				critical
			SubjectKeyIdentifier {2 5 29 14}	siehe Kap 5.3.4	1	FALSE
			KeyUsage {2 5 29 15}	siehe Kap 5.3.4	1	**TRUE**
			SubjectAltNames {2 5 29 17}	siehe Kap 5.3.4	0-1	FALSE
			BasicConstraints {2 5 29 19}	siehe Kap 5.3.4	1	**TRUE**
			CertificatePolicies {2 5 29 32}	siehe Kap 5.3.4	1	FALSE
			CRLDistributionPoints {2 5 29 31}	**CDP des TSP für das betreffende Zertifikat**	**1**	**FALSE**
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap 5.3.4	1	FALSE
			AuthorityKeyIdentifier {2 5 29 35}	siehe Kap 5.3.4	1	FALSE
			Admission {1 3 36 8 3 3}	**admissionAuthority: nicht gesetzt professionItem = Beschreibung zu <oid_praxis_arzt> bzw. <oid_praxis_psychotherapeut> gemäss [gemSpec_OID#GS-A_4443] professionOID = OID <oid_praxis_arzt> bzw. <oid_praxis_psychotherapeut> gemäss [gemSpec_OID#GS-A_4443] registrationNumber <Telematik-ID gemäß Freigabedaten der KBV> (Es wird genau eine Admission-Struktur verwendet, mit je genau**	**0 1 1 1**	**FALSE**

			einem Element: professionInfo, professionItem, registrationNumber)		
		ExtendedKeyUsage {2 5 29 37}	siehe Kap 5.3.4	*)	FALSE
		andere Erweiterungen		0	
	signatureAlgorithm		siehe Kap 5.3.4		
	signature		siehe Kap 5.3.4		

**) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und Tab_PKI_240 ist die Kardinalität gleich 0.*

Hinweis: Ein weiteres Zertifikatsprofil im Verantwortungsbereich der KBV ist das Profil der SMC-B-ORG mit KBV-Ausprägung. Dieses ist mittels der Tabelle "Tab_SMCB_ORG_Gen - Generisches Zertifikatsprofil" in Kapitel 10.7 beschrieben.

10.3 DKG

Die nachfolgende Profiltabelle der DKTIG gilt für den Sektor:

- Krankenhäuser (DKTIG)

Tabelle 110: Tab_SMCB_DKTIG SMC-B-Zertifikate für Sektor der DKTIG

Element			Inhalt	Kar.	
certificate			C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
	tbsCertificate				
		version	siehe Kap 5.3.4		
		serialNumber	siehe Kap 5.3.4		
		signature	siehe Kap 5.3.4		
		issuer	siehe Kap 5.3.4		
		validity	siehe Kap 5.3.4		
		subject			
		commonName	**Gemäss Freigabedaten der DKTIG.**	**1**	
		title	**nicht belegt**	**0**	
		givenName	**nicht belegt**	**0**	
		surName	**nicht belegt**	**0**	
		serialNumber	**TI-weit eindeutiger Identifier der Karte in der Form: <TSP-ID>.<ICCSN> (<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)**	**1**	
		organizationalUnitName	**nicht belegt**	**0**	

			organizationName	**abgeleitet aus dem Institutionskennzeichen eines Krankenhauses**	**0-1**
			streetAddress	**Strassen-Anschrift der Institution (mehrere Wörter sind durch Blank getrennt)**	**1**
			postalCode	**Postleitzahl des Ortes der Institution (Deutsche PLZ werden 5-stellig abgebildet)**	**1**
			localityName	**Stadt des Institut-Standortes**	**1**
			stateOrProvinceName	**Bundesland des Institut-Standortes**	**1**
			countryName	siehe Kap 5.3.4	1
			andere Attribute		0
		subjectPublicKeyInfo		siehe Kap 5.3.4	
		extensions			critical
			SubjectKeyIdentifier {2 5 29 14}	siehe Kap 5.3.4	1 FALSE
			KeyUsage {2 5 29 15}	siehe Kap 5.3.4	1 **TRUE**
			SubjectAltNames {2 5 29 17}	siehe Kap 5.3.4	0-1 FALSE
			BasicConstraints {2 5 29 19}	siehe Kap 5.3.4	1 **TRUE**
			CertificatePolicies {2 5 29 32}	siehe Kap 5.3.4	1 FALSE
			CRLDistributionPoints {2 5 29 31}	siehe Kap 5.3.4	0-1 FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap 5.3.4	1 FALSE
			AuthorityKeyIdentifier {2 5 29 35}	siehe Kap 5.3.4	1 FALSE
			Admission {1 3 36 8 3 3}	**admissionAuthority = {O=<von der DKG benannte attributbestätigende Stelle>,C=DE}** **professionItem = Beschreibung zu <Krankenhaus> gemäss [gemSpec_OID#GS-A_4443]** **professionOID = OID <oid_krankenhaus> gemäss [gemSpec_OID#GS-A_4443]** **registrationNumber = siehe Tabelle Tab_SMCB_TID_DKTIG**	**1** **1** **1** **1** **FALSE**
			ExtendedKeyUsage {2 5 29 37}	siehe Kap 5.3.4	*) FALSE
			andere Erweiterungen		0
	signatureAlgorithm			siehe Kap 5.3.4	

	signature	siehe Kap 5.3.4		

**) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und Tab_PKI_240 ist die Kardinalität gleich 0.*

Tabelle 111: Tab_SMCB_TID_DKTIG Aufbau Telematik-ID in SMC-B-Zertifikaten der DKTIG

Präfix s. Kap 4.7.2.1	**Separator s. Kap 4.7.2.2**	**Fortsatz s. Kap 4.7.2.3**
Krankenhaus		SMC-B Kennzeichen + Institutsindividuelle Kennzeichnung
5	-	2 <gem. Freigabedaten der DKTIG>

10.4 GKV-Spitzenverband

Die nachfolgende Profiltabelle des GKV-Spitzenverbandes gilt für Betriebsstätten bzw. Geschäftsstellen der gesetzlichen Krankenkassen.

Tabelle 112: Tab_SMCB_KTR SMC-B-Zertifikate für Mitarbeiter Kostenträger

Element	**Inhalt**	**Kar.**	
certificate	C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
tbsCertificate			
version	*siehe Kap 5.3.4*		
serialNumber	*siehe Kap 5.3.4*		
signature	*siehe Kap 5.3.4*		
issuer	*siehe Kap 5.3.4*		
validity	*siehe Kap 5.3.4*		
subject			
commonName	Kurzbezeichnung der Krankenkasse gemäß Freigabedaten des GKV-SV	1	
title	nicht belegt	0	
givenName	nicht belegt	0	
surName	nicht belegt	0	
serialNumber	TI-weit eindeutiger Identifier der Karte in der Form: <TSP-ID>.<ICCSN> (<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)	1	
organizationalUnitName	nicht belegt	0	

			organizationName	8-stellige eindeutige Betriebsnummer (BBNR) der Krankenkassenhauptverwaltung gemäß Freigabedaten des GKV-SV	1	
			streetAddress	Straßenanschrift und Hausnummer des Krankenkassenhauptsitzes gemäß Freigabedaten des GKV-SV	1	
			postalCode	Postleitzahl des Krankenkassenhauptsitzes gemäß Freigabedaten des GKV-SV (Deutsche PLZ werden 5-stellig abgebildet)	1	
			localityName	Stadt des Krankenkassenhauptsitzes gemäß Freigabedaten des GKV-SV	1	
			stateOrProvinceName	nicht belegt	0	
			countryName	*siehe Kap 5.3.4*		
			andere Attribute	*siehe Kap 5.3.4*		
		subjectPublicKeyInfo		*siehe Kap 5.3.4*		
		extensions				critical
			SubjectKeyIdentifier {2 5 29 14}	*siehe Kap 5.3.4*		FALSE
			KeyUsage {2 5 29 15}	*siehe Kap 5.3.4*		**TRUE**
			SubjectAltNames {2 5 29 17}	otherName (s. Tab_PKI_228) type-id= {2 5 4 3}; value=ggf. überlange Bezeichnung der Krankenkasse oder Ergänzungen	0-1	FALSE
			BasicConstraints {2 5 29 19}	*siehe Kap 5.3.4*		**TRUE**
			CertificatePolicies {2 5 29 32}	*siehe Kap 5.3.4*		FALSE
			CRLDistributionPoints {2 5 29 31}	nicht belegt	0	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	*siehe Kap 5.3.4*		FALSE
			AuthorityKeyIdentifier {2 5 29 35}	*siehe Kap 5.3.4*		FALSE
			Admission {1 3 36 8 3 3}	admissionAuthority = {O=GKV-Spitzenverband,C=DE} professionItem = Beschreibung zu <oid_kostentraeger> gemäß [gemSpec_OID#GS-A_4443] professionOID = OID <oid_kostentraeger> gemäß [gemSpec_OID#GS-A_4443] registrationNumber = siehe Tabelle Tab_SMCB_TID_GKVSV	1 1 1 1	FALSE
			ExtendedKeyUsage {2 5 29 37}	*siehe Kap 5.3.4*	*)	FALSE
			andere Erweiterungen		0	

	signatureAlgorithm	*siehe Kap 5.3.4*		
	signature	*siehe Kap 5.3.4*		

**) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und Tab_PKI_240 ist die Kardinalität gleich 0.*

Tabelle 113: Tab_SMCB_TID_GKVSV Aufbau Telematik-ID in SMC-B-Zertifikaten des GKV-SV

Präfix s. Kap 4.7.2.1	**Separator s. Kap 4.7.2.2**	**Fortsatz s. Kap 4.7.2.3**
8 (Kostenträger)	-	8-stellige eindeutige Betriebsnummer (BBNR) des GKV-SV oder eine alternative ID gemäß Freigabedaten des GKV-SV

10.5 Apothekerschaft

Tabelle 114: Tab_SMCB_BAK SMC-B-Zertifikate für Apotheker

Element			**Inhalt**	**Kar.**	
certificate			C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
	tbsCertificate				
		version	*siehe Kap 5.3.4*		
		serialNumber	*siehe Kap 5.3.4*		
		signature	*siehe Kap 5.3.4*		
		issuer	*siehe Kap 5.3.4*		
		validity	*siehe Kap 5.3.4*		
		subject			
		commonName	Name der Apotheke	1	
		title	siehe Kap 5.3.4		
		givenName	Vorname des Verantwortlichen/Inhabers (mehrere Vornamen sind durch Blank oder Bindestrich getrennt) *Hinweis: bei mehreren Personen bleibt das Feld leer*	0-1	
		surName	Familienname des Verantwortlichen/Inhabers *Hinweis: bei mehreren Personen bleibt das Feld leer*	0-1	
		serialNumber	TI-weit eindeutiger Identifier der Karte in der Form: <TSP-ID>.<ICCSN>	0-1	

				(<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)		
			organizationalUnitName	nicht belegt	0	
			organizationName	Telematik-ID der Institution gemäß Freigabedaten der Apothekerkammer	1	
			streetAddress	Strassen-Anschrift der Institution (mehrere Wörter sind durch Blank getrennt)	1	
			postalCode	Postleitzahl des Ortes der Institution (Deutsche PLZ werden 5-stellig abgebildet)	1	
			localityName	Stadt des Apotheken-Standortes	1	
			stateOrProvinceName	Bundesland des Apotheken-Standortes	1	
			countryName	siehe Kap 5.3.4		
			andere Attribute	siehe Kap 5.3.4		
		subjectPublicKeyInfo		siehe Kap 5.3.4		
		extensions				critical
			SubjectKeyIdentifier {2 5 29 14}	siehe Kap 5.3.4		FALSE
			KeyUsage {2 5 29 15}	siehe Kap 5.3.4		**TRUE**
			SubjectAltNames {2 5 29 17}	ggf. überlange Institutionsnamen, Alternativnamen oder Ergänzungen	0-1	FALSE
			BasicConstraints {2 5 29 19}	siehe Kap 5.3.4		**TRUE**
			CertificatePolicies {2 5 29 32}	siehe Kap 5.3.4		FALSE
			CRLDistributionPoints {2 5 29 31}	nicht belegt	0	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap 5.3.4		FALSE
			AuthorityKeyIdentifier {2 5 29 35}	siehe Kap 5.3.4		FALSE
			Admission {1 3 36 8 3 3}	admissionAuthority = {O=<von der BAK benannte attributbestätigende Stelle *)>,C=DE} professionItem = Beschreibung zu <oid_oeffentliche_apotheke> gemäß [gemSpec_OID#GS-A_4443] professionOID = OID <oid_oeffentliche_apotheke> gemäß [gemSpec_OID#GS-A_4443] registrationNumber = <Telematik-ID der Institution gemäß Freigabedaten der Apothekerkammer>	0-1 1 1 1	FALSE
			ExtendedKeyUsage {2 5 29 37}	siehe Kap 5.3.4	*)	FALSE

			andere Erweiterungen	siehe Kap 5.3.4		
	signatureAlgorithm			siehe Kap 5.3.4		
	signature			siehe Kap 5.3.4		

**) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und Tab_PKI_240 ist die Kardinalität gleich 0.*

Tabelle 115: Tab_SMCB_TID_BAK Aufbau Telematik-ID in SMC-B-Zertifikaten der Apotheker

Präfix	Separator	Fortsatz	Weiterer Fortsatz
3 (Apothekerschaft)	-	2 (SMC)	gem. Freigabedaten der Apothekerkammer

10.6 AdV-Umgebung im Auftrag der Kostenträger

Tabelle 116: Tab_SMCB_ADV_KTR SMC-B-Zertifikate für die AdV-Umgebung im Auftrag der Kostenträger

Element			Inhalt *)	Kar.	
certificate			C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
	tbsCertificate				
		version	siehe Kap 5.3.4		
		serialNumber	siehe Kap 5.3.4		
		signature	siehe Kap 5.3.4		
		issuer	siehe Kap 5.3.4		
		validity	siehe Kap 5.3.4		
		subject			
			commonName	**Herausgebende Krankenkasse**	**1**
			title	**nicht belegt**	**0**
			givenName	**nicht belegt**	**0**
			surName	**nicht belegt**	**0**
			serialNumber	**nicht belegt**	**0**
			organizationalUnitName	**nicht belegt**	**0**
			organizationName	**siehe Kap 5.3.4**	**0-1**
			streetAddress	**siehe Kap 5.3.4**	**0-1**
			postalCode	**siehe Kap 5.3.4**	**0-1**
			localityName	**siehe Kap 5.3.4**	**0-1**

			stateOrProvinceName	**nicht belegt**	**0**	
			countryName	siehe Kap 5.3.4	1	
			andere Attribute		0	
		subjectPublicKeyInfo		siehe Kap 5.3.4		
		extensions				critical
			SubjectKeyIdentifier {2 5 29 14}	siehe Kap 5.3.4	1	FALSE
			KeyUsage {2 5 29 15}	siehe Kap 5.3.4	1	**TRUE**
			SubjectAltNames {2 5 29 17}	**siehe Kap 5.3.4**	**0-1**	FALSE
			BasicConstraints {2 5 29 19}	siehe Kap 5.3.4	1	**TRUE**
			CertificatePolicies {2 5 29 32}	siehe Kap 5.3.4	1	FALSE
			CRLDistributionPoints {2 5 29 31}	**nicht belegt**	**0**	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap 5.3.4	1	FALSE
			AuthorityKeyIdentifier {2 5 29 35}	siehe Kap 5.3.4	1	FALSE
			Admission {1 3 36 8 3 3}	**admissionAuthority : nicht gesetzt** **professionItem = Beschreibung zu <oid_adv_ktr> gemäss [gemSpec_OID#GS-A_4443]** **professionOID = OID < oid_adv_ktr> gemäss [gemSpec_OID#GS-A_4443]** **registrationNumber = Telematik-ID der Institution**	**0** **1** **1** **1**	FALSE
			ExtendedKeyUsage {2 5 29 37}	siehe Kap 5.3.4		FALSE
			andere Erweiterungen		0	
	signatureAlgorithm			siehe Kap 5.3.4		
	signature			siehe Kap 5.3.4		

10.7 SMC-B-ORG

Die nachfolgende Profiltabelle gilt für die Zertifikate der SMC-B-ORG und kann als generisches Zertifikatsprofil von verschiedenen Organisationen zur Herausgabe einer SMC-B-ORG verwendet werden.

Herausgeberspezifische Ausprägungen zu einzelnen Zertifikatsfeldern sind in der Tabelle Tab_SMCB_ORG_Herausgeber im Dokument [gemRL_SMC-B_ORG_BP] beschrieben.

Tabelle 117: Tab_SMCB_ORG_Gen - Generisches Zertifikatsprofil für die SMC-B-ORG

Element	Inhalt *)	Kar.	
certificate	C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
tbsCertificate			
version	*siehe Kap. 5.3.4*		
serialNumber	*siehe Kap. 5.3.4*		
signature	*siehe Kap. 5.3.4*		
issuer	*siehe Kap. 5.3.4*		
validity	*siehe Kap. 5.3.4*		
subject			
commonName	Kurzbezeichnung gemäß Freigabedaten der zuständigen Organisation (Herausgeberspezifische Ausprägung siehe [gemRL_SMC-B_ORG_BP#Tab_SMCB_ORG_Herausgeber])	1	
title	nicht belegt	0	
givenName	nicht belegt	0	
surName	nicht belegt	0	
serialNumber	TI-weit eindeutiger Identifier der Karte in der Form: <TSP-ID>.<ICCSN> (<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)	1	
organizationalUnitName	nicht belegt	0	
organizationName	*siehe Kap. 5.3.4* (Herausgeberspezifische Ausprägung siehe [gemRL_SMC-B_ORG_BP#Tab_SMCB_ORG_Herausgeber])	0-1	
streetAddress	nicht belegt	0	
postalCode	nicht belegt	0	
localityName	nicht belegt	0	
stateOrProvinceName	nicht belegt	0	
countryName	*siehe Kap. 5.3.4*	1	
andere Attribute		0	
subjectPublicKeyInfo	*siehe Kap. 5.3.4*		
extensions			critical
SubjectKeyIdentifier {2 5 29 14}	*siehe Kap. 5.3.4*	1	FALSE
KeyUsage {2 5 29 15}	*siehe Kap. 5.3.4*	1	**TRUE**

			SubjectAltNames {2 5 29 17}	Komplettangabe zur betreffenden Organisation (Herausgeberspezifische Ausprägung siehe [gemRL_SMC-B_ORG_BP#Tab_SMCB_ORG_Herausgeber])	0-1	FALSE
			BasicConstraints {2 5 29 19}	*siehe Kap. 5.3.4*	1	**TRUE**
			CertificatePolicies {2 5 29 32}	*siehe Kap. 5.3.4*	1	FALSE
			CRLDistributionPoints {2 5 29 31}	*siehe Kap. 5.3.4* (Herausgeberspezifische Ausprägung siehe gemRL_SMC-B_ORG_BP#Tab_SMCB_ORG_Herausgeber)	0-1	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	*siehe Kap. 5.3.4*	1	FALSE
			AuthorityKeyIdentifier {2 5 29 35}	*siehe Kap. 5.3.4*	1	FALSE
			Admission {1 3 36 8 3 3}	admissionAuthority = {O=<zuständige Registrierungsstelle>,C=DE} (Herausgeberspezifische Ausprägung siehe [gemRL_SMC-B_ORG_BP#Tab_SMCB_ORG_Herausgeber]) professionItem = Beschreibung der Institution gemäß [gemSpec_OID#GS-A_4443-01] (Herausgeberspezifische Ausprägung siehe [gemRL_SMC-B_ORG_BP#Tab_SMCB_ORG_Herausgeber]) professionOID = OID der Institution gemäß [gemSpec_OID#GS-A_4443-01] (Herausgeberspezifische Ausprägung siehe [gemRL_SMC-B_ORG_BP#Tab_SMCB_ORG_Herausgeber]) registrationNumber = Telematik-ID gemäßFreigabedaten der zuständigen Organisation (Herausgeberspezifische Ausprägung siehe [gemRL_SMC-B_ORG_BP#Tab_SMCB_ORG_Herausgeber])	1 1 1 1	FALSE
			ExtendedKeyUsage {2 5 29 37}	*siehe Kap. 5.3.4*	*)	FALSE
			andere Erweiterungen		0	
	signatureAlgorithm			*siehe Kap. 5.3.4*		
	signature			*siehe Kap. 5.3.4*		

**) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und Tab_PKI_240 ist die Kardinalität gleich 0.*

Die Verantwortung für die Herausgabe der SMC-B ORG als spezielle Form der SMC-B für Gesellschafterorganisationen ist im gesonderten Dokument [gemRL_SMC-B_ORG_BP] beschrieben.

Die in der Vergangenheit hier gepflegte Tabelle „Tab_SMCB_ORG_Herausgeber - Herausgeberspezifische Felder im SMC-B-ORG Profil“ finden Sie fortan im Dokument „gemRL_SMC-B_ORG_BP“ (Berechtigungs-Policy).

10.8 Weitere Leistungserbringerinsitutionen

Tabelle 118: Tab_PKI_286 Generisches Zertifikatsprofil für die SMC-B - Weitere Leistungserbringerinstitution

Element	Inhalt *)	Kar.	
certificate	C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
tbsCertificate			
version	*siehe Kap. 5.3.4*		
serialNumber	*siehe Kap. 5.3.4*		
signature	*siehe Kap. 5.3.4*		
issuer	*siehe Kap. 5.3.4*		
validity	*siehe Kap. 5.3.4*		
subject			
commonName	Kurzbezeichnung gemäß Freigabedaten der zuständigen Betriebsstätten und Leistungserbringerinstitution I	1	
title	nicht belegt	0	
givenName	nicht belegt	0	
surName	nicht belegt	0	
serialNumber	TI-weit eindeutiger Identifier der Karte in der Form: <TSP-ID>.<ICCSN> (<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)	1	
organizationalUnitName	nicht belegt	0	
organizationName	*siehe Kap. 5.3.4* (Herausgeberspezifische Ausprägung siehe [gemRL_SMC-B_Herausgabepolicy])	0-1	
streetAddress	siehe Kap. 5.3.4	0-1	
postalCode	siehe Kap. 5.3.4	0-1	
localityName	siehe Kap. 5.3.4	0-1	
stateOrProvinceName	siehe Kap. 5.3.4	0-1	
countryName	*siehe Kap. 5.3.4*	1	
andere Attribute		0	

		subjectPublicKeyInfo	*siehe Kap. 5.3.4*		
		extensions			critical
		SubjectKeyIdentifier {2 5 29 14}	*siehe Kap. 5.3.4*	1	FALSE
		KeyUsage {2 5 29 15}	*siehe Kap. 5.3.4*	1	**TRUE**
		SubjectAltNames {2 5 29 17}	Komplettangabe zur betreffenden Organisation	0-1	FALSE
		BasicConstraints {2 5 29 19}	*siehe Kap. 5.3.4*	1	**TRUE**
		CertificatePolicies {2 5 29 32}	*siehe Kap. 5.3.4*	1	FALSE
		CRLDistributionPoints {2 5 29 31}	siehe Kap. 5.3.4	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	*siehe Kap. 5.3.4*	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	*siehe Kap. 5.3.4*	1	FALSE
		Admission {1 3 36 8 3 3}	admissionAuthority = {O=<zuständige bestätigende Organisation>,C=DE} professionItem = Genau eine Beschreibung zu <oid_institution_pflege> bzw. <oid_geburtshilfe> bzw. <oid_institution_pflege> bzw. <oid_praxis_physiotherapeut> bzw. <oid_institution_augenoptiker> bzw. <oid_institution_hoerakustiker> bzw. <oid_institution_orthopaedieschuhmacher> bzw. <oid_institution_orthopaedietechniker> bzw. <oid_institution_zahntechniker> bzw. <oid_rettungsleitstellen> bzw. <oid_sanitaetsdienst_bundeswehr gemäß [gemSpec_OID#GS-A_4443-01] professionOID = Genau eine OID der Berufsgruppe <oid_institution_pflege> bzw. <oid_geburtshilfe> bzw. <oid_institution_pflege> bzw. <oid_praxis_physiotherapeut> bzw. <oid_institution_augenoptiker> bzw. <oid_institution_hoerakustiker> bzw. <oid_institution_orthopaedieschuhmacher> bzw.	1 1 1	FALSE

			<oid_institution_orthopaedietechniker> bzw. <oid_institution_zahntechniker> bzw. <oid_rettungsleitstellen> bzw. <oid_sanitaetsdienst_bundeswehr gemäß [gemSpec_OID#GS-A_4443-01] registrationNumber = Telematik-ID gemäß Freigabedaten der zuständigen bestätigenden Organisation gemäß Tab_PKI_101-01 (entsprechend dem Präfix 9, 10 oder 11)	1	
		ExtendedKeyUsage {2 5 29 37}	*siehe Kap. 5.3.4*	*)	FALSE
		andere Erweiterungen		0	
	signatureAlgorithm		*siehe Kap. 5.3.4*		
	signature		*siehe Kap. 5.3.4*		

**) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und Tab_PKI_240 ist die Kardinalität gleich 0.*

10.9 Weitere Ärztliche Institutionen

Tabelle 119: Tab_PKI_288 Generisches Zertifikatsprofil für die SMC-B - Weitere Ärztliche Institutionen

Element			Inhalt *)	Kar.	
certificate			C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
	tbsCertificate				
		version	*siehe Kap. 5.3.4*		
		serialNumber	*siehe Kap. 5.3.4*		
		signature	*siehe Kap. 5.3.4*		
		issuer	*siehe Kap. 5.3.4*		
		validity	*siehe Kap. 5.3.4*		
		subject			
		commonName	Kurzbezeichnung gemäß Freigabedaten der zuständigen Organisation	1	
		title	nicht belegt	0	
		givenName	nicht belegt	0	
		surName	nicht belegt	0	
		serialNumber	TI-weit eindeutiger Identifier der Karte in der Form: <TSP-ID>.<ICCSN>	1	

			(<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)		
		organizationalUnitName	nicht belegt	0	
		organizationName	siehe Kap. 5.3.4	0-1	
		streetAddress	siehe Kap. 5.3.4	0-1	
		postalCode	siehe Kap. 5.3.4	0-1	
		localityName	siehe Kap. 5.3.4	0-1	
		stateOrProvinceName	siehe Kap. 5.3.4	0-1	
		countryName	*siehe Kap. 5.3.4*	1	
		andere Attribute		0	
	subjectPublicKeyInfo		*siehe Kap. 5.3.4*		
	extensions				critical
		SubjectKeyIdentifier {2 5 29 14}	*siehe Kap. 5.3.4*	1	FALSE
		KeyUsage {2 5 29 15}	*siehe Kap. 5.3.4*	1	**TRUE**
		SubjectAltNames {2 5 29 17}	Komplettangabe zur betreffenden Organisation	0-1	FALSE
		BasicConstraints {2 5 29 19}	*siehe Kap. 5.3.4*	1	**TRUE**
		CertificatePolicies {2 5 29 32}	*siehe Kap. 5.3.4*	1	FALSE
		CRLDistributionPoints {2 5 29 31}	*siehe Kap. 5.3.4*	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	*siehe Kap. 5.3.4*	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	*siehe Kap. 5.3.4*	1	FALSE
		Admission {1 3 36 8 3 3}	admissionAuthority = {O=<zuständige bestätigende Organisation>,C=DE} professionItem = Genau eine Beschreibung zu <oid_gesundheitsdienst> <oid_arbeitsmedizin>	1 1	FALSE

				<oid_vorsorge_reha> gemäß [gemSpec_OID#GS-A_4443] professionOID = Genau eine OID der Berufsgruppe <oid_gesundheitsdienst> <oid_arbeitsmedizin> <oid_vorsorge_reha> gemäß [gemSpec_OID#GS-A_4443] registrationNumber = Telematik-ID gemäß Freigabedaten der zuständigen bestätigenden Organisation gemäß Tab_PKI_101-01 (entsprechend dem Präfix 9, 10 oder 11)	1 1	
			ExtendedKeyUsage {2 5 29 37}	*siehe Kap. 5.3.4*	*)	FALSE
			andere Erweiterungen		0	
	signatureAlgorithm			*siehe Kap. 5.3.4*		
	signature			*siehe Kap. 5.3.4*		

**) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und Tab_PKI_240 ist die Kardinalität gleich 0.*

11 Anhang B – Verzeichnisse

11.1 Abkürzungen

Kürzel	Erläuterung
aAdG	andere Anwendungen des Gesundheitswesens (mit Zugriff auf Dienste der TI)
aAdG-NetG	aAndere Anwendungen des Gesundheitswesens ohne Zugriff auf Dienste der TI in angeschlossenen Netzen des Gesundheitswesens
aAdG-NetG-TI	andere Anwendungen des Gesundheitswesens mit Zugriff auf Dienste der TI aus angeschlossenen Netzen des Gesundheitswesens
AES	Advanced Encryption Standard
AK	Anwendungskonnektor
AN	alphanumerisch
AUT	Authentisierung (Authentication)
AUTN	Technisches Authentisierungszertifikat für Nachrichten
AVS	Apothekenverwaltungssystem (Primärsystem der Apotheker)
BAEK/BÄK	Bundesärztekammer
BAK	Bundesapothekerkammer
BCD	Binary coded decimal
BMG	Bundesministerium für Gesundheit
BNetzA	Bundesnetzagentur
BNetzA-VL	Vertrauensliste (TSL) der Bundesnetzagentur
BPTK	Bundespsychotherapeutenkammer
BSI	Bundesamt für Sicherheit in der Informationstechnik
BZÄK	Bundeszahnärztekammer

C2C	card to card
CA	certification authority
CAMS	Card Application Management System
CAR	Certificate Authority Reference
CC	Common Criteria
CED	Certificate Effective Date
CH	Card Holder
CHA	Certificate Holder Authorisation
CHAT	Certificate Holder Authorization Template
CHR	Certificate Holder Reference
CMS	Karten Management System, Card Management System
CP	Certificate Policy
CPI	Certificate Profile Identifier
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CV	Card Verifiable
CVC	Card Verifiable Certificate
CVC-CA	CA für CV-Zertifikate
CV-Zertifikate	Card Verifiable-Zertifikate
CXD	Certificate Expiration Date
DES	Data Encryption Standard
DIMDI	Deutsches Institut für Medizinische Dokumentation und Information
DKG	Deutsche Krankenhausgesellschaft
DKTIG	Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH

DN	Distinguished Name
DNS	Domain Name Service
DNs	Distinguished Names
EE	End Entity
eGK	Elektronische Gesundheitskarte
ePA	Elektronische Patientenakte
ENC	Verschlüsselung (Encryption)
ENCV	Technisches Verschlüsselungszertifikat für Verordnungen
ETSI	Europäisches Institut für Telekommunikationsnormen
FdV	Frontend des Versicherten
FIPS-140 2	Federal Information Processing Standard 140 2
FQDN	Fully Qualified Domain Name
FM	Fachmodul
GBSM	Gerätebezogenes Sicherheitsmodul
GKV	Gesetzliche Krankenversicherung
gSMC	Gerätebezogene Security Module Card
HBA	Heilberufsausweis
HCI	Health Care Institution
HP	Health Professional
HPC	Health Professional Card
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ICCSN	ICC Serial Number
ID	Identität (Identity)

IK	Individual Key
IPSec	Internet Protocol Security
ISM	Information Security Management
ISO	International Standard Organization
KBV	Kassenärztliche Bundesvereinigung
KIS	Krankenhausinformationssystem (Primärsystem der Krankenhäuser)
KT	Kartenterminal
KTR	Kostenträger
KV	Kassenärztliche Vereinigung
KVK	Krankenversichertenkarte
KVNR	Krankenversichertennummer
KZBV	Kassenzahnärztliche Bundesvereinigung
LÄK	Landesärztekammer
LDAP	Lightweight Directory Access Protocol
LEO	Leistungserbringer-Organisation
LZÄK	Landeszahnärztekammer
MAC	Message Authentication Code
MON	Monitoring
NK	Netzkonnektor
OCSP	Online Certificate Status Protocol
OCSP-R	OCSP-Responder
OID	Object Identifier
OSIG	Organizational Signature
PIN	Personal Identification Number

PKI	Public Key Infrastructure
PKIX	PKI nach X.509 Standard der IETF
PrK	Private Key
PuK	Public Key
PVS	Praxisverwaltungssystem (Primärsystem des Arztes)
QES	Qualifizierte elektronische Signatur
RA	Registration Authority
RCA	Root-CA
RFC	Request For Comment
RSA	Rivest Shamir Adleman (Verfahren)
SAK	Signaturanwendungskomponente
SGB	Sozialgesetzbuch
SGD	Schlüsselgenerierungsdienst
SHA	Secure Hash Algorithm
SIG	Elektronische Signatur
SLA	Service Level Agreement
SM	Security Module
SMC-B	Sicherheitsmodul vom Typ B <medizinische Institution>
SMC	Security Module Card
gSMC-K	Security Module Card Konnektor als <holder>
SM-KT-Zertifikat	X.509-Komponentenzertifikat zu einem SM-KT
SubjectDN	Subject Distinguished Name
TCL	Trusted Component List
TI	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

11.2 Glossar

Begriff	Erläuterung
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.
Referenzzeitpunkt, Referenzzeit	Es handelt sich um den Zeitpunkt aus einem übergebenen Zeitparameter, für den das Zertifikat auf Gültigkeit geprüft wird und für den die Statusinformationen eingeholt werden. Dabei kann es sich um die aktuelle Systemzeit ‚current time' gemäß [RFC5280] Kap. 6.1.3 für nonQES nach dem Schalenmodell (PKIX shell model) handeln (z.B. bei TLS-Verbindungsaufbau). Der Referenzzeitpunkt kann auch in der Vergangenheit liegen: Der Signaturzeitpunkt für QES bezüglich des Ketten- für QES-Zertifikate für HBA bzw. Kompromissmodells für nonQES-Zertifikate für HBA und SMC-B (s. [gemKPT_PKI_TIP#2.4.2])

Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung gestellt.

11.3 Abbildungsverzeichnis

Abbildung 1: Betriebsumgebungen aus Sicht der PKI 24
Abbildung 2: Aufbau der Krankenversichertennummer 29
Abbildung 3: Pseudonym Kodierung in X.509-Versichertenzertifikaten.....32
Abbildung 4: Das Anschriftenfeld nach DIN5008 70
Abbildung 5: Use Case Diagramm „Prozesse zur Nutzung des TI-Vertrauensraums" 151
Abbildung 6 : Aufbau der TSL.....153

Abbildung 7: Aktivitätsdiagramm TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“ 163
Abbildung 8: Aktivitätsdiagramm TUC_PKI_013 „Import neuer TI-Vertrauensanker“ ... 167
Abbildung 9: Aktivitätsdiagramm TUC_PKI_017 „Lokalisierung Download-Adresse“ 172
Abbildung 10: Aktivitätsdiagramm TUC_PKI_016 „Download der TSL-Datei“ 175
Abbildung 11: Aktivitätsdiagramm TUC_PKI_019 „Prüfung der Aktualität der TSL“ 182
Abbildung 12: Aktivitätsdiagramm TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“ 187
Abbildung 13: Use Case Diagramm „Zertifikatsprüfung“ 190
Abbildung 14: Aktivitätsdiagramm TUC_PKI_018 „Zertifikatsprüfung“ 197
Abbildung 15: Aktivitätsdiagramm TUC_PKI_002 Gültigkeitsprüfung des Zertifikats 200
Abbildung 16: Aktivitätsdiagramm TUC_PKI_003 CA-Zertifikat in TSL-Informationen finden 203
Abbildung 17: Aktivitätsdiagramm TUC_PKI_004 Mathematische Prüfung der Zertifikatssignatur 205
Abbildung 18: Aktivitätsdiagramm TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln“ 208
Abbildung 19: Aktivitätsdiagramm TUC_PKI_006 „OCSP-Abfrage“ 215
Abbildung 20: Aktivitätsdiagramm TUC_PKI_021 „CRL-Prüfung“ 220
Abbildung 21: Aktivitätsdiagramm TUC_PKI_009 „Rollenermittlung“ 223
Abbildung 22 : Aktivitätsdiagramm TUC_PKI_007 „Prüfung Zertifikatstyp“ 227

11.4 Tabellenverzeichnis

Tabelle 1: Tab_PKI_201 Allgemeine Notationsvorschrift für kryptographische Objekte ... 14
Tabelle 2: Tab_PKI_202: Notationsvorgaben für Objekttyp 14
Tabelle 3: Tab_PKI_203 Notationsvorgaben für Objektbesitzer 15
Tabelle 4: Tab_PKI_204 Notationsvorgaben für Objektverwendung 17
Tabelle 5: Tab_PKI_205-01 Notationsvorgaben für Ausprägung 19
Tabelle 6: Tab_PKI_206-01 Beispiele für asymmetrische Objekte 20
Tabelle 7: Tab_PKI_207 Beispiele für symmetrische Objekte 21
Tabelle 8: Tab_PKI_213 Erlaubte Werte für <usage> und <usageName> 26
Tabelle 9: Tab_PKI_221 Berufsgruppenkennzeichnung 33
Tabelle 10: Tab_PKI_222 Institutionstypkennzeichnung 34
Tabelle 11: Tab_PKI_230 Kennzeichnung Technische Rolle 35
Tabelle 12: Tab_PKI_224 Telematik-ID-Kennzeichnung 36
Tabelle 13: Tab_PKI_223 Aufbau der Telematik-ID 36

Tabelle 14: Tab_PKI_101-01 Normative Festlegung für das Präfix der Telematik-ID.....37
Tabelle 15: Tab_PKI_229-01 Kodierung der Attribute in X.509-Zertifikaten.....38
Tabelle 16: Tab_PKI_109 Werte für das Präfix <TSP-ID> 40
Tabelle 17: Tab_PKI_226-01 Struktur Admission 41
Tabelle 18: Tab_PKI_227 Struktur CertificatePolicies 42
Tabelle 19: Tab_PKI_228 Struktur SubjectAltName 44
Tabelle 20: Common Name (CN) der End-Entity-Zertifikate Test-PKI 49
Tabelle 21: Tab_PKI_231 Personennamen im subjectDN 53
Tabelle 22: Tab_PKI_232 C.CH.AUT und C.CH.AUT_ALT Authentisierung eGK 54
Tabelle 23: Tab_PKI_233 C.CH.ENC Verschlüsselung eGK.....55
Tabelle 24: Tab_PKI_234 C.CH.QES Qualifizierte Signatur eGK 57
Tabelle 25: Tab_PKI_235 C.CH.AUTN Technische Authentisierung eGK.....58
Tabelle 26: Tab_PKI_236 C.CH.ENCV Technische Verschlüsselung eGK 60
Tabelle 27: Tab_PKI_268_1 C.HP.AUT Authentisierung HBA.....61
Tabelle 281: Tab_PKI_269_1 C.HP.ENC Verschlüsselung HBA 63
Tabelle 29: Tab_PKI_270_1 C.HP.QES Qualifizierte Signatur HBA 65
Tabelle 30: Tab_PKI_238 C.HCI.AUT Authentisierung SMC-B 71
Tabelle 31: Tab_PKI_239 C.HCI.ENC Verschlüsselung SMC-B.....73
Tabelle 32: Tab_PKI_240 C.HCI.OSIG Signatur SMC-B.....75
Tabelle 33: Tab_PKI_241 C.SMKT.AUT gSMC-KT 77
Tabelle 34: Tab_PKI_237 Statusprüfung von Konnektorzertifikaten 80
Tabelle 35: Tab_PKI_242 Zertifikatsprofil C.NK.VPN VPN-Authentisierung Netzkonnektor 80
Tabelle 36: Tab_PKI_243 Zertifikatsprofil C.AK.AUT Authentisierung Anwendungskonnektor 82
Tabelle 37: Tab_PKI_244 Zertifikatsprofil C.SAK.AUT Authentisierung SAK 84
Tabelle 38: Tab_PKI_245 Zertifikatsprofil C.VPNK.VPN VPN-Authentisierung Zugangsdienst TI 86
Tabelle 39: Tab_PKI_265 Zertifikatsprofil C.VPNK.VPN-SIS VPN-Authentisierung Zugangsdienst Sicherer Internetzugang 88
Tabelle 40: Tab_PKI_247 C.ZD.TLS-S Server-Authentisierung Zentrale Dienste 90
Tabelle 41: Tab_PKI_249 C.FD.TLS-C Client-Authentisierung Fachanwendungsspezifische Dienste 92
Tabelle 42: Tab_PKI_250 C.FD.TLS-S Server-Authentisierung Fachanwendungsspezifische Dienste 94
Tabelle 43: Tab_PKI_251 C.FD.SIG Signatur fachanwendungsspezifische Dienste.....95
Tabelle 44: Tab_PKI_275 C.FD.AUT Authentisierung fachanwendungsspezifische Dienste 97

Tabelle 45: Tab_PKI_276 C.FD.ENC Verschlüsselung fachanwendungsspezifische Dienste 98
Tabelle 46: Tab_PKI_267 C.CM.TLS-CS Clientmodul-Authentisierung 100
Tabelle 47: Tab_PKI_296 C.SGD-HSM.AUT Authentisierung SGD-HSM 102
Tabelle 48: Tab_PKI_211 GEM.R-CA<n> – Zentrale gematik Root-CA_nonQES der TI.105
Tabelle 49: Tab_PKI_212 <tsp>.<usage>-CA<n> –Aussteller- CA_nonQES der TI....106
Tabelle 50: Tab_PKI_253 C.GEM.OCSP Zertifikatsprofil OCSP-Signer 110
Tabelle 51: Tab_PKI_214 C.GEM.CRL Zertifikatsprofil CRL-Signer....112
Tabelle 52: Tab_PKI_252_01 C.TSL.SIG Zertifikatsprofil TSL-Signer 115
Tabelle 53: Tab_PKI_254 Zugriffsprofile für eine Rollenauthentisierung 120
Tabelle 54: Tab_PKI_255 Zugriffsprofile G2 für eine Authentisierung einer Funktionseinheit....128
Tabelle 55: Tab_PKI_266 Aufbau CAR für Karten der Generation 2 131
Tabelle 56: Tab_PKI_901 Objektidentifier des öffentlichen Schlüssels eines CV-Zertifikats der Generation 2 132
Tabelle 57: Tab_PKI_902 Punkt Q des öffentlichen Schlüssels eines CV-Zertifikats der Generation 2....133
Tabelle 58: Tab_PKI_258 Aufbau CHR....134
Tabelle 59: Tab_PKI_904 Mögliche Objektidentifier OID_{flags} in Certificate Holder Authorization Templates....135
Tabelle 60: Tab_PKI_905 Zu signierende Nachricht M eines CV-Zertifikates 137
Tabelle 61: Tab_PKI_906 Signatur der Nachricht M eines CV-Zertifikats 137
Tabelle 62: Tab_PKI_907 Struktur und Inhalt eines CV-Zertifikat 138
Tabelle 63: Tab_PKI_912 CA CV-Zertifikate für 256 bit ELC-Schlüssel, insgesamt 220 Oktett....138
Tabelle 64: Tab_PKI_913 CA CV-Zertifikate für 384 bit ELC-Schlüssel, insgesamt 285 Oktett....139
Tabelle 65: Tab_PKI_914 CA CV-Zertifikate für 512 bit ELC-Schlüssel, insgesamt 352 Oktett....139
Tabelle 66: Tab_PKI_937 Cross-CV-Zertifikat für ELC-Schlüssel 140
Tabelle 67: Tab_PKI_915 Endnutzer-CV-Zertifikate für 256 bit ELC-Schlüssel, insgesamt 222 Oktett....141
Tabelle 68: Tab_PKI_916 Endnutzer-CV-Zertifikate für 384 bit ELC-Schlüssel, insgesamt 287 Oktett....142
Tabelle 69: Tab_PKI_917 Endnutzer-CV-Zertifikate für 512 bit ELC-Schlüssel, insgesamt 354 Oktett....142
Tabelle 70: Tab_PKI_910 TI-PKI, Bedeutung der Bits innerhalb der Flagliste eines CHAT 143
Tabelle 71: Tab_PKI_918 Abbildung von Rollenberechtigungen Zugriffsprofilen auf äquivalente Flaglisten 145

Tabelle 72: Tab_PKI_919 Sub-CA-Flaglisten nach Kartentyp (G2) und Zugriffsprofilen 147
Tabelle 73: Tab_PKI_911 CMS-PKI, Bedeutung der Bits innerhalb der Flagliste eines CHAT 148
Tabelle 74: Tab_PKI_271 Erlaubte URIs als Inhalte des TSL-Elements ServiceStatus ..157
Tabelle 75: TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum" 158
Tabelle 76: TUC_PKI_013 „Import neuer TI-Vertrauensanker" 164
Tabelle 77: Gültige Werte für den TI-Vertrauensankerwechsel..... 169
Tabelle 78: Beispiel für den TSL-Eintrag zum Wechsel des TSL-Signer-CA-Zertifikats ..169
Tabelle 79: TUC_PKI_017 „Lokalisierung Download-Adressen" 170
Tabelle 80: Tab_PKI_272 Gültige Werte zur Download-Adresse 172
Tabelle 81: TUC_PKI_016 „Download der TSL-Datei" 173
Tabelle 82: TUC_PKI_019 „Prüfung der Aktualität der TSL" 177
Tabelle 83: TUC_PKI_020 „XML-Dokument validieren" 183
Tabelle 84: TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates" 184
Tabelle 85: TUC_PKI_012 „XML-Signatur- Prüfung" 187
Tabelle 86: Tab_PKI_294 TSL Zeitparameter 189
Tabelle 87: TUC_PKI_018 „Zertifikatsprüfung in der TI" 191
Tabelle 88: TUC_PKI_002 „Gültigkeitsprüfung des Zertifikats"..... 198
Tabelle 89: TUC_PKI_003 „CA-Zertifikat in TSL-Informationen finden" 200
Tabelle 90: TUC_PKI_004 „Mathematische Prüfung der Zertifikatssignatur" 203
Tabelle 91: TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln"..... 206
Tabelle 92: TUC_PKI_006 „OCSP-Abfrage"..... 208
Tabelle 93: TUC_PKI_021 „CRL-Prüfung"..... 215
Tabelle 94: TUC_PKI_009 „Rollenermittlung" 221
Tabelle 95 : TUC_PKI_007 „Prüfung Zertifikatstyp"..... 224
Tabelle 96: Tab_PKI_273 Prüfparameter für TLS-Aufbau 228
Tabelle 97: TUC_PKI_030 „QES-Zertifikatsprüfung" 230
Tabelle 98: TUC_PKI_036 „BNetzA-VL Aktualisierung"..... 237
Tabelle 99: Tab_PKI_274 Fehlercodes des SubCompTyps PKI bei TSL- und Zertifikatsprüfung..... 241
Tabelle 100: Tab_PKI_908 Prüfung der Signatur eines CV-Zertifikats der Generation 2 mit Hilfe des CV-Zertifikats des Herausgebers 250
Tabelle 101: Tab_PKI_909 Gültigkeit eines CV-Zertifikats der Generation 2 251
Tabelle 102: Tab_PKI_290 Struktur certID in OCSP-Request/Response 254
Tabelle 103 : Tab_PKI_289 Struktur Nonce 255
Tabelle 104: Tab_PKI_291 OCSP-Response Status Ergebnisse 257
Tabelle 105: Tab_PKI_292 Zeiten in einer OCSP-Response 257

Tabelle 106: Tab_PKI_293 Status der OCSP Antworten 258
Tabelle 107 : Tab_PKI_288 Struktur certHash 259
Tabelle 108: Tab_SMCB_KZBV_ZA SMC-B-Zertifikate für Zahnarzt (Sektor KZBV) 261
Tabelle 109: Tab_SMCB_KV-T SMC-B-Zertifikate für Sektoren der KBV 263
Tabelle 110: Tab_SMCB_DKTIG SMC-B-Zertifikate für Sektor der DKTIG 265
Tabelle 111: Tab_SMCB_TID_DKTIG Aufbau Telematik-ID in SMC-B-Zertifikaten der DKTIG 267
Tabelle 112: Tab_SMCB_KTR SMC-B-Zertifikate für Mitarbeiter Kostenträger 267
Tabelle 113: Tab_SMCB_TID_GKVSV Aufbau Telematik-ID in SMC-B-Zertifikaten des GKV-SV 269
Tabelle 114: Tab_SMCB_BAK SMC-B-Zertifikate für Apotheker 269
Tabelle 115: Tab_SMCB_TID_BAK Aufbau Telematik-ID in SMC-B-Zertifikaten der Apotheker 271
Tabelle 116: Tab_SMCB_ADV_KTR SMC-B-Zertifikate für die AdV-Umgebung im Auftrag der Kostenträger 271
Tabelle 117: Tab_SMCB_ORG_Gen - Generisches Zertifikatsprofil für die SMC-B-ORG 273
Tabelle 118: Tab_PKI_286 Generisches Zertifikatsprofil für die SMC-B - Weitere Leistungserbringerinstitution 275
Tabelle 119: Tab_PKI_288 Generisches Zertifikatsprofil für die SMC-B - Weitere Ärztliche Institutionen 277
Tabelle 120: Tab_HBA_BÄK HBA-Zertifikate (AUT, ENC, QES) für BÄK 296
Tabelle 121: Tab_HBA_BZÄK HBA-Zertifikate (AUT, ENC, QES) für BZÄK 298
Tabelle 122: Tab_HBA_BPtK HBA-Zertifikate (AUT, ENC, QES) für BPtK 299
Tabelle 123: Tab_HBA_BAK HBA-Zertifikate (AUT, ENC, QES) für Apotheker 301
Tabelle 124: Tab_PKI_285 Generisches Zertifikatsprofil (C.HP.AUT, C.HP.ENC, C.HP.QES) für BA - Weitere Leistungserbringer 303

11.5 Referenzierte Dokumente

11.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar
[gemKPT_Arch_TIP]	gematik: Architektur der TI-Plattform
[gemKPT_PKI_TIP]	gematik: Konzept PKI der TI-Plattform
[gemRL_TSL_SP_CP]	gematik: Certificate Policy - Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL
[gemSpec_COS]	gematik: Spezifikation des Card Operating System (COS), Elektrische Schnittstelle
[gemSpec_CVC_Root]	gematik: Spezifikation CVC-Root
[gemSpec_Krypt]	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_OID]	gematik: Spezifikation Festlegung von OIDs
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_TSL]	gematik: Spezifikation TSL-Dienst
[gemRL_SMC-B_ORG_BP]	gematik: Berechtigungsgrundlagen zur Beantragung und zum Erhalt der SMC-B ORG

11.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[SOG-IS]	SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms. Version 1.1, June 2018. https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.1.pdf
[BSI-TR-03110]	BSI, Advanced Security Mechanisms for Machine Readable Travel Documents, Version 2.10, 20.03.2012 https://www.bsi.bund.de/ContentBSI/Publikationen /TechnischeRichtlinien/tr03110/index_htm.html
[BSI-TR-03111]	BSI (2012): Elliptic Curve Cryptography, Version 2.0 https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtli

	nien /tr03111/index_htm.html
[BSI-CC-PP-0098]	BSI (03.07.2019): Common Criteria Schutzprofil (Protection Profile) Schutzprofil 2: Anforderungen an den Konnektor. Version 1.4
[CP-HPC]	Bundesapothekerkammer, Bundesärztekammer, Bundespsychotherapeutenkammer, Bundeszahnärztekammer (24.09.2018): Gemeinsame Policy für die Ausgabe der Heilberufsausweise – Zertifikatsrichtlinie Heilberufsausweis (Version 2.0.0) https://www.abda.de/fileadmin/user_upload/assets/Telematik/CP_HPC_v2.0.0.pdf
[DIN5008]	DIN 5008 (2005): Schreib- und Gestaltungsregeln für die Textverarbeitung
[eIDAS]	Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
[EN 14890-1]	EN 14890-1 (Draft: February 2007) Application Interface for smart cards used as secure signature Creation Devices - Part 1: Basic services
[ETSI EN 319 412-1]	ETSI (Februar 2016): ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Overview and common data structures, Version 1.1.1
[ETSI EN 319 412-2]	ETSI (Februar 2016): ETSI EN 319 412-2 'Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons', Version 2.1.1
[ETSI EN 319 412-5]	ETSI (2017-11): Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.
[ETSI_TS_102_231_v3.1.2]	ETSI (Dezember 2009): ETSI Technical Specification TS 102 231 ('Provision of harmonized Trust Service Provider (TSP) status information') Version 3.1.2
[ETSI_TS_119_612]	ETSI (July 2015): ETSI TS 119 612 'Electronic Signatures and Infrastructures (ESI); Trusted Lists', Version 2.1.1

[ETSI EN 119 001]	ETSI (2016-03): Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations, Version 1.2.1
[ETSI EN 319 102-1]	ETSI (2016-05): Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation, Version 1.1.1
[ETSI TS 119 172-4]	ETSI (2019-08-04): ETSI TS 119 172-4 Final draft for approval 'Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists', Version 0.0.7
[FIPS 180-4]	Federal Information Processing Standards Publication 180-4 Secure Hash Standard (SHS), March 2012 http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf
[ISO/IEC9594-2]	ISO/IEC 9594-2:2008-12 Information technology - Open Systems Interconnection - The Directory: Models
[ISO3166-1]	ISO/IEC 3166-1:1997 Codes for the representations of names of countries – Part 1: Country codes
[ISO8859-1]	ISO/IEC 8859-1 (1998): Information technology - 8-bit single-byte coded graphic character sets - Part 1: Latin alphabet No. 1
[ISO9796-2]	ISO9796-2: 2002 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://tools.ietf.org/html/rfc2109
[RFC3629]	RFC 3629 (November 2003): UTF-8, a transformation format of ISO 10646 http://tools.ietf.org/html/rfc3629
[RFC3739]	RFC 3739 (March 2004): Internet X.509 Public Key Infrastructure Qualified Certificates Profile http://tools.ietf.org/html/rfc3739

[RFC4514]	RFC 4514 (Juni 2006): Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names http://tools.ietf.org/html/rfc4514
[RFC5019]	RFC 5019 (September 2007): The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments http://tools.ietf.org/html/rfc5019
[RFC5280]	RFC 5280 (Mai 2008): Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile http://tools.ietf.org/html/rfc5280
[RFC6960]	RFC 6960 (Juni 2013): X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP https://tools.ietf.org/html/rfc6960
[RFC5754]	RFC5754 (Jan. 2010): Using SHA2 Algorithms with Cryptographic Message Syntax https://tools.ietf.org/html/rfc5754
[RFC3370]	RFC3370 (August 2002): Cryptographic Message Syntax (CMS) Algorithms https://tools.ietf.org/html/rfc3370
[SGB V]	BGBl. I S.2477 (20.12.1988): Sozialgesetzbuch, Fünftes Buch Zuletzt geändert durch Art. 4 G v. 14.4.2010 I 410 Gesetzliche Krankenversicherung
[VDG]	"Vertrauensdienstegesetz vom 18. Juli 2017 (BGBl. I S. 2745), das durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist" Stand: Geändert durch Art. 2 G v. 18.7.2017 I 2745 https://www.gesetze-im-internet.de/vdg/BJNR274510017.html
[X.509]	ITU-T X.509 (10/2019): SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY, Directory, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks http://www.itu.int/rec/T-REC-X.509/
[X.520]	ITU-T X.520 (10/2012): SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY, Directory, Information technology – Open Systems Interconnection – The Directory: Selected attribute types http://www.itu.int/rec/T-REC-X.520/

[X.521]	ITU-T X.521 (10/2012): SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY, Directory, Information technology – Open Systems Interconnection – The Directory: Selected object classes http://www.itu.int/rec/T-REC-X.521/
[XML]	World Wide Web Consortium (2006): Extensible Markup Language (XML) 1.0 http://www.w3.org/TR/REC-xml/
[XAdES]	ETSI (2010-12): ETSI TS 101 903 Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES), Version 1.4.2
[XMLSig]	W3C Recommendation: XML-Signature Syntax and Processing http://www.w3.org/TR/xmldsig-core/

12 Anhang C – Sektorspezifische Ausprägungen der HBA Zertifikate

Die nachfolgenden Profiltabellen der Sektoren referenzieren auf die Festlegungen aus Kap. 5.2.1 für alle sektorübergreifenden Attribute und ergänzen/ersetzen diese um sektorspezifische Ausprägungen.

Die Profiltabellen gelten einheitlich für die Zertifikate:

- C.HP.AUT
- C.HP.ENC
- C.HP.QES

12.1 BÄK

Tabelle 120: Tab_HBA_BÄK HBA-Zertifikate (AUT, ENC, QES) für BÄK

Element	Inhalt	Kar.	
certificate	C.HP.AUT, C.HP.ENC, C.HP.QES		
tbsCertificate			
version	*siehe Kap. 5.2.1*		
serialNumber	*siehe Kap. 5.2.1*		
signature	*siehe Kap. 5.2.1*		
issuer	*siehe Kap. 5.2.1*		
validity	*siehe Kap. 5.2.1*		
subject			
commonName	*siehe Kap. 5.2.1*		
title	*siehe Kap. 5.2.1*		
givenName	*siehe Kap. 5.2.1*		
surName	*siehe Kap. 5.2.1*		
serialNumber	*siehe Kap. 5.2.1*		
organizationalUnitName	*siehe Kap. 5.2.1*		
organizationName	*siehe Kap. 5.2.1*		
countryName	*siehe Kap. 5.2.1*		
andere Attribute	*siehe Kap. 5.2.1*		
subjectPublicKeyInfo	*siehe Kap. 5.2.1*		
extensions			critical
SubjectKeyIdentifier {2 5 29 14}	*siehe Kap. 5.2.1*		FALSE

			KeyUsage {2 5 29 15}	*siehe Kap. 5.2.1*		**TRUE**
			SubjectAltNames {2 5 29 17}	*siehe Kap. 5.2.1*		FALSE
			BasicConstraints {2 5 29 19}	*siehe Kap. 5.2.1*		**TRUE**
			CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = http://www.e-arztausweis.de/ policies/EE_policy.html policyIdentifier = Zertifikatstyp-OID gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <id-etsi-qcp-natural-qscd> {0.4.0.194112.1.2} (nur für QES) policyIdentifier = 1.3.6.1.4.1.42675.1.1: CPME European eID-Policy for Physicans policyIdentifier =<OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP-spezifischen Zertifikatsrichtlinie	1 0-1 1 (1) 1 0-1 0-1	FALSE
			CRLDistributionPoints {2 5 29 31}	*siehe Kap. 5.2.1*		FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	*siehe Kap. 5.2.1*		FALSE
			AuthorityKeyIdentifier {2 5 29 35}	*siehe Kap. 5.2.1*		FALSE
			Admission {1 3 36 8 3 3}	admissionAuthority = {O=<zuständige bestätigende Ärztekammer>,C=DE} professionItem = „Ärztin/Arzt“ (siehe [gemSpec_OID#GS-A_4442]) professionOID = <oid_arzt> (siehe [gemSpec_OID#GS-A_4442]) registrationNumber = Telematik-ID des Inhabers	1 1 1 1	FALSE
			ExtendedKeyUsage {2 5 29 37}	*siehe Kap. 5.2.1*		FALSE
			ValidityModel {1 3 6 1 4 1 8301 3 5}	*siehe Kap. 5.2.1*		FALSE
			QCStatements {1 3 6 1 5 5 7 1 3}	*siehe Kap. 5.2.1*		FALSE
			additionalInformation {1 3 36 8 3 15}	*siehe Kap. 5.2.1*		FALSE
			Restriction {1 3 36 8 3 8}	*siehe Kap. 5.2.1*		FALSE
			andere Erweiterungen	*siehe Kap. 5.2.1*		
		signatureAlgorithm		*siehe Kap. 5.2.1*		
		signature		*siehe Kap. 5.2.1*		

12.2 BZÄK

Tabelle 121: Tab_HBA_BZÄK HBA-Zertifikate (AUT, ENC, QES) für BZÄK

Element	Inhalt *)	Kar.	
certificate	C.HP.AUT, C.HP.ENC, C.HP.QES		
tbsCertificate			
version	*siehe Kap. 5.2.1*		
serialNumber	*siehe Kap. 5.2.1*		
signature	*siehe Kap. 5.2.1*		
issuer	*siehe Kap. 5.2.1*		
validity	*siehe Kap. 5.2.1*		
subject			
commonName	*siehe Kap. 5.2.1*		
title	*siehe Kap. 5.2.1*		
givenName	*siehe Kap. 5.2.1*		
surName	*siehe Kap. 5.2.1*		
serialNumber	*siehe Kap. 5.2.1*		
organizationalUnitName	*siehe Kap. 5.2.1*		
organizationName	*siehe Kap. 5.2.1*		
countryName	*siehe Kap. 5.2.1*		
andere Attribute	*siehe Kap. 5.2.1*		
subjectPublicKeyInfo	*siehe Kap. 5.2.1*		
extensions			critical
SubjectKeyIdentifier {2 5 29 14}	*siehe Kap. 5.2.1*		FALSE
KeyUsage {2 5 29 15}	*siehe Kap. 5.2.1*		**TRUE**
SubjectAltNames {2 5 29 17}	*siehe Kap. 5.2.1*		FALSE
BasicConstraints {2 5 29 19}	*siehe Kap. 5.2.1*		**TRUE**
CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = http://policies.bzaek.de policyIdentifier = Zertifikatstyp-OID gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <id-etsi-qcp-natural-	1 0-1 1	FALSE

				qscd> {0.4.0.194112.1.2} (nur für QES) policyIdentifier =<OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP-spezifischen Zertifikatsrichtlinie	(1) 0-1 0-1	
			CRLDistributionPoints {2 5 29 31}	CDP der ausstellenden CA … … für AUT und ENC zwingend, … für QES optional	 1 0-1	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	*siehe Kap. 5.2.1*		FALSE
			AuthorityKeyIdentifier {2 5 29 35}	*siehe Kap. 5.2.1*		FALSE
			Admission {1 3 36 8 3 3}	admissionAuthority = {O=< zuständige Landeszahnärztekammer>,C=DE} professionItem = „Zahnärztin/Zahnarzt“ (siehe [gemSpec_OID#GS-A_4442]) professionOID = <oid_zahnarzt> (siehe [gemSpec_OID#GS-A_4442]) registrationNumber = Telematik-ID des Inhabers	1 1 1 1	FALSE
			ExtendedKeyUsage {2 5 29 37}	*siehe Kap. 5.2.1*		FALSE
			ValidityModel {1 3 6 1 4 1 8301 3 5}	*siehe Kap. 5.2.1*		FALSE
			QCStatements {1 3 6 1 5 5 7 1 3}	*siehe Kap. 5.2.1*		FALSE
			additionalInformation {1 3 36 8 3 15}	*siehe Kap. 5.2.1*		FALSE
			Restriction {1 3 36 8 3 8}	*siehe Kap. 5.2.1*		FALSE
			andere Erweiterungen	*siehe Kap. 5.2.1*		
	signatureAlgorithm			*siehe Kap. 5.2.1*		
	signature			*siehe Kap. 5.2.1*		

12.3 BPtK

Tabelle 122: Tab_HBA_BPtK HBA-Zertifikate (AUT, ENC, QES) für BPtK

Element			Inhalt *)	Kar.	
certificate			C.HP.AUT, C.HP.ENC, C.HP.QES		
	tbsCertificate				
		version	*siehe Kap. 5.2.1*		
		serialNumber	*siehe Kap. 5.2.1*		
		signature	*siehe Kap. 5.2.1*		

		issuer	*siehe Kap. 5.2.1*		
		validity	*siehe Kap. 5.2.1*		
		subject			
		commonName	*siehe Kap. 5.2.1*		
		title	*siehe Kap. 5.2.1*		
		givenName	*siehe Kap. 5.2.1*		
		surName	*siehe Kap. 5.2.1*		
		serialNumber	*siehe Kap. 5.2.1*		
		organizationalUnitName	*siehe Kap. 5.2.1*		
		organizationName	*siehe Kap. 5.2.1*		
		countryName	*siehe Kap. 5.2.1*		
		andere Attribute	*siehe Kap. 5.2.1*		
		subjectPublicKeyInfo	*siehe Kap. 5.2.1*		
		extensions			critical
		SubjectKeyIdentifier {2 5 29 14}	*siehe Kap. 5.2.1*		FALSE
		KeyUsage {2 5 29 15}	*siehe Kap. 5.2.1*		**TRUE**
		SubjectAltNames {2 5 29 17}	*siehe Kap. 5.2.1*		FALSE
		BasicConstraints {2 5 29 19}	*siehe Kap. 5.2.1*		**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = http://www.e-psychotherapeutenausweis.de/policies/EE_policy.html policyIdentifier = Zertifikatstyp-OID gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <id-etsi-qcp-natural-qscd> {0.4.0.194112.1.2} (nur für QES) policyIdentifier =<OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP-spezifischen Zertifikatsrichtlinie	1 0-1 1 (1) 0-1 0-1	FALSE
		CRLDistributionPoints {2 5 29 31}	*siehe Kap. 5.2.1*		FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	*siehe Kap. 5.2.1*		FALSE
		AuthorityKeyIdentifier {2 5 29 35}	*siehe Kap. 5.2.1*		FALSE
		Admission {1 3 36 8 3 3}	admissionAuthority = {O=<zuständige Landespsychotherapeutenkammer>,C=DE} Eine oder zwei professionInfo-Elemente	1 1-2	FALSE

			bestehend aus: professionItem = „Psychotherapeut/-in" oder professionItem = „Psychologische/-r Psychotherapeut/-in“ und/oder professionItem = „Kinder- und Jugendlichenpsychotherapeut/-in“ professionOID = <oid_psychotherapeut> oder professionOID = <oid_ps_psychotherapeut> und/oder professionOID = <oid_kuj_psychotherapeut> (siehe gemSpec_OID#GS-A_4442) registrationNumber = Telematik-ID des Inhabers… … für AUT und ENC zwingend, … für QES optional (Diese muss dann in mindestens einem professionInfo-Element aufgeführt sein)	1 0-1	
		ExtendedKeyUsage {2 5 29 37}	*siehe Kap. 5.2.1*		FALSE
		ValidityModel {1 3 6 1 4 1 8301 3 5}	*siehe Kap. 5.2.1*		FALSE
		QCStatements {1 3 6 1 5 5 7 1 3}	*siehe Kap. 5.2.1*		FALSE
		additionalInformation {1 3 36 8 3 15}	*siehe Kap. 5.2.1*		FALSE
		Restriction {1 3 36 8 3 8}	*siehe Kap. 5.2.1*		FALSE
		andere Erweiterungen	*siehe Kap. 5.2.1*		
	signatureAlgorithm		*siehe Kap. 5.2.1*		
	signature		*siehe Kap. 5.2.1*		

12.4 Apothekerschaft

Tabelle 123: Tab_HBA_BAK HBA-Zertifikate (AUT, ENC, QES) für Apotheker

Element			Inhalt	Kar.	
certificate			C.HP.AUT, C.HP.ENC, C.HP.QES		
	tbsCertificate				
		version	*siehe Kap. 5.2.1*		
		serialNumber	*siehe Kap. 5.2.1*		
		signature	*siehe Kap. 5.2.1*		
		issuer	*siehe Kap. 5.2.1*		
		validity	*siehe Kap. 5.2.1*		
		subject			

			commonName	*siehe Kap. 5.2.1*		
			title	*siehe Kap. 5.2.1*		
			givenName	*siehe Kap. 5.2.1*		
			surName	*siehe Kap. 5.2.1*		
			serialNumber	*siehe Kap. 5.2.1*		
			organizationalUnitName	*siehe Kap. 5.2.1*		
			organizationName	*siehe Kap. 5.2.1*		
			countryName	*siehe Kap. 5.2.1*		
			andere Attribute	*siehe Kap. 5.2.1*		
		subjectPublicKeyInfo		*siehe Kap. 5.2.1*		
		extensions				critical
			SubjectKeyIdentifier {2 5 29 14}	*siehe Kap. 5.2.1*		FALSE
			KeyUsage {2 5 29 15}	*siehe Kap. 5.2.1*		**TRUE**
			SubjectAltNames {2 5 29 17}	*siehe Kap. 5.2.1*		FALSE
			BasicConstraints {2 5 29 19}	*siehe Kap. 5.2.1*		**TRUE**
			CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = https://www.abda.de/themen/positionen-und-initiativen/telematik/hba/ policyIdentifier = Zertifikatstyp-OID gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <id-etsi-qcp-natural-qscd> {0.4.0.194112.1.2} (nur für QES) policyIdentifier =<OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP-spezifischen Zertifikatsrichtlinie	1 0-1 1 (1) 0-1 0-1	FALSE
			CRLDistributionPoints {2 5 29 31}	*siehe Kap. 5.2.1*		FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	*siehe Kap. 5.2.1*		FALSE
			AuthorityKeyIdentifier {2 5 29 35}	*siehe Kap. 5.2.1*		FALSE
			Admission {1 3 36 8 3 3}	admissionAuthority = (O= <Apothekerkammer Bezeichnung>, C=DE) professionItem = Genau eine Beschreibung zu <oid_apotheker> bzw. <oid_apothekerassistent> bzw. <oid_pharmazieingenieur> bzw. <oid_apothekenassistent>.	1 1	FALSE

				gemäß [gemSpec_OID#GS-A_4442] professionOID = Genau eine OID der Berufsgruppe <oid_apotheker> bzw. <oid_apothekerassistent> bzw. <oid_pharmazieingenieur> bzw. <oid_apothekenassistent> gemäß [gemSpec_OID#GS-A_4442] registrationNumber = Telematik-ID des Inhabers … … für AUT und ENC zwingend, … für QES optional	1 1 0-1	
			ExtendedKeyUsage {2 5 29 37}	*siehe Kap. 5.2.1*		FALSE
			additionalInformation	*siehe Kap. 5.2.1*		FALSE
			Restriction	*siehe Kap. 5.2.1*		FALSE
			andere Erweiterungen	*siehe Kap. 5.2.1*		
	signatureAlgorithm			*siehe Kap. 5.2.1*		
	signature			*siehe Kap. 5.2.1*		

12.5 Weitere Leistungserbringer

Tabelle 124: Tab_PKI_285 Generisches Zertifikatsprofil (C.HP.AUT, C.HP.ENC, C.HP.QES) für BA - Weitere Leistungserbringer

Element			Inhalt	Kar.	
certificate			C.HP.AUT, C.HP.ENC, C.HP.QES		
	tbsCertificate				
		version	*siehe Kap. 5.2.1*		
		serialNumber	*siehe Kap. 5.2.1*		
		signature	*siehe Kap. 5.2.1*		
		issuer	*siehe Kap. 5.2.1*		
		validity	*siehe Kap. 5.2.1*		
		subject			
			commonName	*siehe Kap. 5.2.1*	
			title	*siehe Kap. 5.2.1*	
			givenName	*siehe Kap. 5.2.1*	
			surName	*siehe Kap. 5.2.1*	

			serialNumber	*siehe Kap. 5.2.1*		
			organizationalUnitName	*siehe Kap. 5.2.1*		
			organizationName	*siehe Kap. 5.2.1*		
			countryName	*siehe Kap. 5.2.1*		
			andere Attribute	*siehe Kap. 5.2.1*		
		subjectPublicKeyInfo		*siehe Kap. 5.2.1*		
		extensions				critical
			SubjectKeyIdentifier {2 5 29 14}	*siehe Kap. 5.2.1*		FALSE
			KeyUsage {2 5 29 15}	*siehe Kap. 5.2.1*		**TRUE**
			SubjectAltNames {2 5 29 17}	*siehe Kap. 5.2.1*		FALSE
			BasicConstraints {2 5 29 19}	*siehe Kap. 5.2.1*		**TRUE**
			CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = http://www.e-arztausweis.de/policies/EE_policy.html policyIdentifier = Zertifikatstyp-OID gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <id-etsi-qcp-natural-qscd> {0.4.0.194112.1.2} (nur für QES) policyIdentifier = 1.3.6.1.4.1.42675.1.1: CPME European eID-Policy for Physicans policyIdentifier =<OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP-spezifischen Zertifikatsrichtlinie	1 0-1 1 (1) 1 0-1 0-1	FALSE
			CRLDistributionPoints {2 5 29 31}	*siehe Kap. 5.2.1*		FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	*siehe Kap. 5.2.1*		FALSE
			AuthorityKeyIdentifier {2 5 29 35}	*siehe Kap. 5.2.1*		FALSE
			Admission {1 3 36 8 3 3}	admissionAuthority = {O=<zuständige bestätigende Organisation>, C=DE} professionItem = Genau eine Beschreibung zu <oid_altenpfleger> bzw. <oid_pflegefachkraft> bzw. <oid_pfleger> bzw. <oid_hebamme> bzw. <oid_physiotherapeut> bzw. <oid_augenoptiker> bzw. <oid_hoerakustiker> bzw. <oid_orthopaedieschuhmacher> bzw.	1 1	FALSE

				<oid_orthopaedietechniker> bzw. <oid_zahntechniker> gemäß [gemSpec_OID#GS-A_4442-01] professionOID = Genau eine OID der Berufsgruppe: <oid_altenpfleger> bzw. <oid_pflegefachkraft> bzw. <oid_pfleger> bzw. <oid_hebamme> bzw. <oid_physiotherapeut> bzw. <oid_augenoptiker> bzw. <oid_hoerakustiker> bzw. <oid_orthopaedieschuhmacher> bzw. <oid_orthopaedietechniker> bzw. <oid_zahntechniker> gemäß [gemSpec_OID#GS-A_4442-01] registrationNumber = Telematik-ID des Inhabers gemäß Tab_PKI_101-01 (entsprechend dem Präfix 9, 10 oder 11)	1	
			ExtendedKeyUsage {2 5 29 37}	*siehe Kap. 5.2.1*		FALSE
			ValidityModel {1 3 6 1 4 1 8301 3 5}	*siehe Kap. 5.2.1*		FALSE
			QCStatements {1 3 6 1 5 5 7 1 3}	*siehe Kap. 5.2.1*		FALSE
			additionalInformation {1 3 36 8 3 15}	*siehe Kap. 5.2.1*		FALSE
			Restriction {1 3 36 8 3 8}	*siehe Kap. 5.2.1*		FALSE
			andere Erweiterungen	*siehe Kap. 5.2.1*		
	signatureAlgorithm			*siehe Kap. 5.2.1*		
	signature			*siehe Kap. 5.2.1*		