

Einführung der Gesundheitskarte

Übergreifende Spezifikation

Spezifikation PKI

Version: 2.1.0
Revision: \main\rel_online\rel_ors1\rel_opb1\rel_ors2\42
Stand: 18.12.2017
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: [gemSpec_PKI]

Dokumentinformationen

Änderungen zur Vorversion

Die Änderungen zu OPB1 R1.6.4-0 sind **gelb** markiert.

Die Einarbeitung der abgestimmten Änderungen und die Entfernung LE-AdV sind **grün** markiert. Die Einarbeitung der Errata ist **pink** markiert.

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		freigegeben	gematik

Inhaltsverzeichnis

Dokumentinformationen	2
Inhaltsverzeichnis	3
1 Einordnung des Dokumentes	10
1.1 Zielsetzung	10
1.2 Zielgruppe	10
1.3 Geltungsbereich	10
1.4 Abgrenzungen	11
1.5 Methodik.....	11
2 Notation kryptographischer Objekte.....	12
2.1 Basis-Bezeichner	12
2.2 Optionale Bezeichnung der technischen Ausprägung	12
2.3 Optionales Unterscheidungsmerkmal bei gleicher technischer Ausprägung 12	
2.4 Allgemeine Notationsvorschrift.....	13
2.5 Type (Objekttyp)	13
2.6 Holder (Objektbesitzer)	14
2.7 Usage (Objektverwendung)	16
2.8 n (lfd. Nummer)	18
2.9 Instance (Ausprägung).....	18
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
3.5	Sperrungen von QES-CAs	27
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.....	30
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 Heilberufers	33
4.5	ID der Organisation/Einrichtung des Gesundheitswesens.....	33
4.5.1	Typ und Exemplar der Organisation/Einrichtung des Gesundheitswesens	33
4.6	Technische Rolle von Komponenten und Diensten	34
4.6.1	Technische Rolle im Komponentenzertifikat	34
4.7	Telematik-ID	34
4.7.1	Abbildung der Telematik-ID im X.509-Zertifikat.....	35
4.7.2	Aufbau der Telematik-ID.....	35
4.7.2.1	Sektoraler Präfix	36
4.7.2.2	Separator.....	36
4.7.2.3	Fortsatz der Telematik-ID	37
4.8	Kodierung der Zertifikate	37
4.8.1	Kodierung der Attribute.....	37
4.8.2	Stringlänge der Attribute	38
4.8.3	Struktur.....	38
4.8.3.1	serialNumber	39
4.8.3.2	Admission.....	39
4.8.3.3	CertificatePolicies.....	41
4.8.3.4	CRLDistributionPoints.....	42
4.8.3.5	SubjectAltNames	42
4.9	Erläuterungen zu Zertifikatsprofilen.....	43
4.9.1	Allgemeine Erläuterungen.....	44
4.9.2	Berufs-/Rollenattribute und Sperrbarkeit	44
4.9.3	Benennung der Zertifikatsprofile	45
4.9.4	Distinguished Name.....	45
4.10	Kodierung der Betriebsumgebungen in Zertifikaten.....	45
4.11	Kartenverlust und Deaktivierung von Chipkarten	47

5	X.509-Zertifikate	48
5.1	eGK - Versichertenkarte	48
5.1.1	Definition der Versichertenidentität	48
5.1.2	Belegung der Felder im SubjectDN	49
5.1.3	X.509-Zertifikatsprofile der eGK	50
5.1.3.1	C.CH.AUT – Authentisierung eGK	50
5.1.3.2	C.CH.ENC – Verschlüsselung eGK	52
5.1.3.3	C.CH.QES – Qualifizierte Signatur eGK (optional)	53
5.1.3.4	C.CH.AUTN - Technische Authentisierung eGK	54
5.1.3.5	C.CH.ENCV - Technische Verschlüsselung eGK	56
5.2	HBA – Heilberufsausweis	57
5.2.1	X.509 Zertifikatsprofile des HBA	57
5.2.1.1	C.HP.AUT – Authentisierung HBA	57
5.2.1.2	C.HP.ENC – Verschlüsselung HBA	59
5.2.1.3	C.HP.QES – Qualifizierte Signatur HBA	61
5.3	SMC-B – Ausweis einer Organisation/Einrichtung des Gesundheitswesens	64
5.3.1	Definition der Organisationsidentität	64
5.3.2	Aufbau Anschriftzone nach [DIN5008]	64
5.3.3	Umgang mit überlangen Attributen im SubjectDN	65
5.3.4	X.509 Zertifikatsprofile der SMC-B	65
5.3.4.1	C.HCI.AUT – Authentisierung SMC- B	65
5.3.4.2	C.HCI.ENC – Verschlüsselung SMC-B	67
5.3.4.3	C.HCI.OSIG – Signatur SMC-B	69
5.4	HSM-B – Ausweis einer Organisation/Einrichtung des Gesundheitswesens	70
5.5	gSMC-KT – eHealth-Kartenterminal	70
5.5.1	Definition der Kartenterminalidentität	71
5.5.2	X.509 Zertifikatsprofile der gSMC-KT	71
5.5.2.1	C.SMKT.AUT – Identität der gSMC-KT	71
5.6	gSMC-K – Konnektor	73
5.6.1	Definition und Zuweisung der Konnektoridentität	73
5.6.2	Aufbau des SubjectDN	73
5.6.3	Statusprüfung von Konnektorzertifikaten	73
5.6.4	X.509 Zertifikatsprofile des Konnektors	74
5.6.4.1	C.NK.VPN – VPN-Authentisierung Netzkonnektor	74
5.6.4.2	C.AK.AUT - Authentisierung Anwendungskonnektor	75
5.6.4.3	C.SAK.AUT - Authentisierung SAK	77
5.7	VPN-Zugangsdienst	78
5.7.1	Definition und Zuweisung der Zugangsdienstidentitäten	78
5.7.2	Aufbau des SubjectDN	78
5.7.3	X.509-Zertifikatsprofile des Zugangsdienstes	79
5.7.3.1	C.VPNK.VPN - VPN-Authentisierung Zugangsdienst TI	79
5.7.3.2	C.VPNK.VPN-SIS - VPN-Authentisierung Zugangsdienst Sicherer Internetzugang	80
5.7.3.3	VPN-Zugangsdienst – Verwendung mehrerer Schlüsselpaare	81
5.8	ZD - Zentrale Dienste	82

5.8.1	Definition der Identität der Zentralen Dienste	82
5.8.2	Aufbau des SubjectDN	82
5.8.3	X.509 Zertifikatsprofile der Zentralen Dienste	82
5.8.3.1	C.ZD.TLS-S Server-Authentisierung (ehemals C.SF.SSL-S)	82
5.9	FD – Fachanwendungsspezifische Dienste	84
5.9.1	Definition der Identität der Fachanwendungsspezifischen Dienste	84
5.9.2	Aufbau des SubjectDN	84
5.9.3	X.509 Zertifikatsprofile der Fachanwendungsspezifischen Dienste	84
5.9.3.1	C.FD.TLS-C Client-Authentisierung (ehemals C.SF.SSL-C)	84
5.9.3.2	C.FD.TLS-S Server-Authentisierung (ehemals C.SF.SSL-S)	86
5.10	CM – Clientmodul	87
5.10.1	Definition der Identität eines Clientmoduls	87
5.10.2	Aufbau des SubjectDN	87
5.10.3	X.509 Zertifikatsprofil des Clientmoduls	88
5.10.3.1	C.CM.TLS-CS Clientmodul-Authentisierung	88
5.11	CA - Zertifikatsprofile	89
5.11.1	GEM.RCA<n> - Zentrale Root-CA_nonQES	90
5.11.2	<tsp>.<usage>-CA<n> - Aussteller-CA_nonQES	91
5.11.3	<tsp>.HBA-qCA<n> - Aussteller-CA_QES	92
5.12	OCSP – Statusauskunftsdienst	94
5.12.1	Definition der OCSP-Signer-Identität	94
5.12.2	Aufbau des SubjectDN	94
5.12.3	X.509 Zertifikatsprofil der OCSP-Signer-CA	94
5.12.4	X.509 Profil des OCSP-Signer-Zertifikates	95
5.12.4.1	C.GEM.OCSP OCSP-Signer-Zertifikat	95
5.13	CRL – Statusauskunftsdienst	96
5.13.1	Definition der CRL-Signer-Identität	96
5.13.2	Aufbau des SubjectDN	96
5.13.3	X.509 Zertifikatsprofil der CRL-Signer-CA	97
5.13.4	X.509 Profil des CRL-Signer-Zertifikates	97
5.13.4.1	C.GEM.CRL CRL-Signaturzertifikat	97
5.14	TSL - Zertifikatsprofile	98
5.14.1	Definition der TSL-Signer-Identität	98
5.14.2	Aufbau des SubjectDN	98
5.14.3	X.509 Zertifikatsprofil der TSL-Signer-CA	98
5.14.4	TSL-Signer- Zertifikat	99
5.14.5	TSL-OCSP-Responder-Zertifikat	100
6	CV-Zertifikate	101
6.1	Festlegungen zur Abgrenzung	101
6.2	Namensregeln und -formate	101
6.3	Rollen und Profile	102
6.3.1	Rollenauthentisierung	102
6.3.2	Authentisierung einer Funktionseinheit	107
6.4	Aufbau und Bestandteile eines CV-Zertifikats der Generation 1	108
6.4.1	Bestandteile eines CV-Zertifikats	108

6.4.1.1	Certificate Profile Identifier (CPI)	108
6.4.1.2	Certification Authority Reference (CAR).....	108
6.4.1.3	Certificate Holder Reference (CHR).....	109
6.4.1.4	Certificate Holder Authorisation (CHA)	110
6.4.1.5	Object Identifier (OID).....	110
6.4.1.6	Öffentlicher Schlüssel.....	111
6.4.2	Aufbau eines CV-Zertifikats	111
6.5	Gesamtübersicht CV-Zertifikatsprofil einer CVC-CA der Generation 1.....	112
6.6	Gesamtübersicht CV-Zertifikatsprofil einer Chipkarte der Generation 1 ..	113
6.7	CV-Zertifikatsprofile der Generation 2	115
6.7.1	Berechtigung einer CVC-CA zur Zertifikatserstellung.....	115
6.7.2	Aufbau und Bestandteile der CV-Zertifikate der Generation 2.....	116
6.7.3	Zertifikatsprofil eines CV-Zertifikates für ELC-Schlüssel	117
6.7.3.1	Certificate Profile Identifier (CPI)	117
6.7.3.2	Certification Authority Reference (CAR).....	117
6.7.3.3	Öffentlicher Schlüssel.....	118
6.7.3.4	Certificate Holder Reference (CHR).....	119
6.7.3.5	Certificate Holder Authorization Template (CHAT).....	120
6.7.3.6	Certificate Effective Date (CED)	120
6.7.3.7	Certificate Expiration Date (CXD)	121
6.7.3.8	Zu signierende Nachricht M eines CV-Zertifikates der Generation 2.	121
6.7.4	Struktur und Inhalt eines CV-Zertifikates für ELC-Schlüssel der Generation 2	122
6.7.5	Struktur und Inhalt eines CV-Zertifikates für ELC-Schlüssel der Generation 2	123
6.7.5.1	Struktur und Inhalt von CA CV-Zertifikaten für ELC-Schlüssel.....	123
6.7.5.2	Struktur und Inhalt von Cross-CV-Zertifikaten für ELC-Schlüssel.....	125
6.7.5.3	Struktur und Inhalt von Endnutzer-CV-Zertifikaten für ELC-Schlüssel	126
6.7.6	Flagliste mit Berechtigungen in CV-Zertifikaten für ELC-Schlüssel	127
7	Festlegung von OIDs	132
8	Prüfung von Zertifikaten	133
8.1	Vertrauensraum der TI.....	135
8.1.1	Initialisierung TI-Vertrauensraum	137
8.1.1.1	TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“.....	139
8.1.2	Geplanter Wechsel TI-Vertrauensanker.....	143
8.1.2.1	TUC_PKI_013 „Import TI-Vertrauensanker aus TSL“.....	143
8.1.2.2	TSL-Einträge für die Bereitstellung neuer TI-Vertrauensanker.....	145
8.1.2.3	Prüfung der TSL nach Wechsel des TI-Vertrauensanker	147
8.1.3	Ungeplanter Wechsel des TI-Vertrauensanker	148
8.2	TSL-Prüfung.....	148
8.2.1	Erreichbarkeit und Download der TSL	148
8.2.1.1	TUC_PKI_017 „Lokalisierung TSL Download-Adressen“.....	148
8.2.1.2	TUC_PKI_016 „Download der TSL-Datei“	150
8.2.2	Vertrauensstatus und Authentifizieren der TSL.....	152
8.2.2.1	TUC_PKI_019 „Prüfung der Aktualität der TSL“	152

8.2.2.2	TUC_PKI_020 „XML-Dokument validieren“	157
8.2.2.3	TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“	157
8.2.2.4	TUC_PKI_012 „XML-Signatur-Prüfung“	160
8.2.3	TSL-Sicherheitsaspekte	160
8.2.4	TSL-Zeitparameter	161
8.3	Zertifikatsprüfung X.509 nonQES	161
8.3.1	Zertifikatsprüfung in der TI	163
8.3.1.1	TUC_PKI_018 „Zertifikatsprüfung in der TI“	163
8.3.1.2	TUC_PKI_002 „Gültigkeitsprüfung des Zertifikats“	167
8.3.1.3	TUC_PKI_003 „CA-Zertifikat in TSL-Informationen finden“	168
8.3.1.4	TUC_PKI_004 „Mathematische Prüfung der Zertifikatssignatur“	170
8.3.2	Statusprüfung	172
8.3.2.1	TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln“	172
8.3.2.2	TUC_PKI_006 „OCSP-Abfrage“	174
8.3.2.3	TUC_PKI_021 „CRL-Prüfung“	179
8.3.2.4	Szenarien für Offline und Timeout von OCSP	183
8.3.2.5	Statusprüfung von eGK-Zertifikaten	183
8.3.3	Ermittlung von Autorisierungsinformationen	183
8.3.3.1	Bestätigte Zertifikatsinformationen	183
8.3.3.2	TUC_PKI_009 „Rollenermittlung“	183
8.3.3.3	TUC_PKI_007 „Prüfung Zertifikatstyp“	185
8.3.4	Weitere Prüfungen	188
8.3.4.1	Umgang mit kritischen Extensions	188
8.4	Überprüfung der Zertifikate auf Netzwerk- und Transportebene	188
8.4.1	TLS-Verbindungsaufbau	188
8.4.2	IPsec-Verbindungsaufbau	189
8.5	Zertifikatsprüfung X.509 QES	189
8.5.1	TUC_PKI_030 „QES-Zertifikatsprüfung“	190
8.5.2	TUC_PKI_036 „BNetzA-VL Aktualisierung“	192
8.6	Fehlercodes bei TSL- und Zertifikatsprüfung X.509	196
8.7	Zertifikatsprüfung CVC	201
8.8	Zertifikatsprüfung CV-Zertifikate der 2. Generation	201
9	OCSP-Statusinformation	204
9.1	Statusprüfung	204
9.1.1	Schnittstelle I_OCSP_Status_Information	204
9.1.1.1	Schnittstellendefinition	205
9.1.1.1.1	OCSP-Request	205
9.1.1.1.2	OCSP-Response	206
9.1.1.2	Umsetzung	206
9.1.1.3	Nutzung	207
9.1.2	Artefakte	207
9.1.2.1	OCSP-Response – Response Status	207
9.1.2.2	OCSP-Response - Zeiten	208
9.1.2.3	OCSP-Response - CertStatus	209
9.1.2.4	OCSP-Response - CertID	210
9.1.2.5	OCSP-Response – Sperrzeitpunkt und Sperrgrund	210

9.1.2.6	OCSP-Response – CertHash	210
9.1.3	Testunterstützung	210
9.1.4	Hardwaremerkmale	211
Anhang A – Sektorspezifische Ausprägungen der SMC-B Zertifikate.....		212
A1	– KZBV	212
A2	– KBV	215
A3	– DKG	217
A4	– GKV-Spitzenverband	219
A5	– Apothekerschaft	221
A6	– AdV-Umgebung beim Leistungserbringer	223
A6.7	– AdV-Umgebung beim Kostenträger	224
Anhang B – Verzeichnisse.....		226
B1	– Abkürzungen	226
B2	– Glossar	229
B3	– Abbildungsverzeichnis	229
B4	– Tabellenverzeichnis	230
B5	– Referenzierte Dokumente	235
B5.1	– Dokumente der gematik	235
B5.2	– Weitere Dokumente	235
Anhang C – Sektorspezifische Ausprägungen der HBA Zertifikate		239
C1	– BÄK	239
C2	– BZÄK	241
C3	– BPtK	242
C4	– Apothekerschaft	244

1 Einordnung des Dokumentes

Nach Inkrafttreten der eIDAS-Verordnung wurde die Anforderungslage der gematik entsprechend angepasst. Signaturgesetz (SigG) und -verordnung (SigV) sind weiterhin gültig und finden dort Anwendung, wo sie der eIDAS-Verordnung nicht widersprechen. SigG und SigV sollen zukünftig durch das deutsche Vertrauensdienstegesetz (VDG) abgelöst werden. Mit Verabschiedung des Vertrauensdienstegesetzes kann es in diesem Dokument daher zu Anpassungen und Konkretisierungen entsprechend der geänderten Rechtslage kommen.

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.

Alle im Dokument enthaltenen Festlegungen im Zusammenhang mit Anwendungen des Versicherten in der Leistungserbringumgebung, mit dem LE-AdV-Terminal, mit Fachmodul AdV sowie mit Schnittstellen zu diesen sind als gegenständlich zu betrachten.

1.4 Abgrenzungen

Im vorliegenden Dokument werden Verfahren und Profile für digitale Zertifikate (X.509, CVC für die Generation G1 und 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:

☒ **GS-A_0000 <Titel der Afo>**

Text / Beschreibung☒

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken 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

2 Notation kryptographischer Objekte

2.1 Basis-Bezeichner

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

<Objekttyp>.<Objektbesitzer>.<Objektverwendung>

Im weiteren Dokument werden dafür die kürzeren englischen Begriffe verwendet:

<type>.<holder>.<usage>

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

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

2.2 Optionale Bezeichnung der technischen Ausprägung

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

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

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

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

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

2.3 Optionales Unterscheidungsmerkmal bei gleicher technischer Ausprägung

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

Beispiel:

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

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

2.4 Allgemeine Notationsvorschrift

Die Benennung kryptographischer Objekte erfolgt gemäß der Notationsvorschrift in Tab_PKI_201.

Tabelle 1: Tab_PKI_201 Allgemeine Notationsvorschrift für kryptographische Objekte

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

2.5 Type (Objekttyp)

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

Tabelle 2: Tab_PKI_202: Notationsvorgaben für Objekttyp

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

Wertebereich von <key>

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

Wertebereich von <certificate>

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

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

Wertebereich von <ID>

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

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)

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> <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
<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 Notationsvorgaben für Ausprägung

<instance> ::= <instance X.509> <instance CVC> <instance SYM>	
Asymmetrische Objekte	<instance X.509> ::= <X.509 RSA 2048 > <X.509 RSA 3072 > <X.509 ECC 256 > <X.509 ECC 384 > <X.509 ECC 512 >

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

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

Wertebereich von <instance X.509>

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

Wertebereich von <instance CVC>

<CVC RSA 2048 > ::= R2048
 <CVC ECC 256 > ::= E256
 <CVC ECC 384 > ::= E384
 <X.509CVC 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 Beispiele für asymmetrische Objekte

Komponente	Fachliche Beschreibung	Name des Zertifikats	Name des privaten Schlüssels	Name des öffentlichen Schlüssels mit einer konkreten technischen Ausprägung
eGK	X.509-Zertifikat/Schlüssel des Versicherten für die Verschlüsselung	C.CH.ENC	PrK.CH.ENC	PuK.CH.ENC2.R2048
	CV-Zertifikat der eGK zur C2C-Authentisierung	C.eGK.AUT_CVC	PrK.eGK.AUT_CVC	PuK.eGK.AUT_CVC.E256
HBA	X.509-Zertifikat/Schlüssel des Heilberufers für eine QES	C.HP.QES	PrK.HP.QES	PuK.HP.QES.R2048
	CV-Zertifikat des HBA zur C2C-Geräteauthentisierung	C.HPC.AUTD_SUK_CVC	PrK.HPC.AUTD_SUK_CVC	PuK.HPC.AUTD_SUK_CVC.R2048
SMC	X.509-Zertifikat/Schlüssel der Institution für eine elektronische Signatur	C.HCI.OSIG	PrK.HCI.OSIG	PuK.HCI.OSIG.E256
	CV-Zertifikat der SMC zur C2C-Rollenauthentisierung	C.SMC.AUTR_CVC	PrK.SMC.AUTR_CVC	PuK.SMC.AUTR_CVC.E256
VPN-Zugangsdienst	X.509-Zertifikat/Schlüssel des VPN-Zugangsdienstes	C.VPNK.VPN	PrK.VPNK.VPN	PuK.VPNK.VPN.R2048
Fachanw. spez. Dienst allgem.	X.509-Zertifikat/Schlüssel eines Fachanwendungsspez. Dienstes als Server für TLS-Verbindung	C.FD.TLS-S	PrK.FD.TLS-S	PuK.FD.TLS-S.R2048
Fachdienst VSD	X.509-Zertifikat/Schlüssel des VSD-Fachdienstes zum Signieren einer Nachricht	C.VSD.AUT	PrK.VSD.AUT	PuK.VSD.AUT R2048

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.

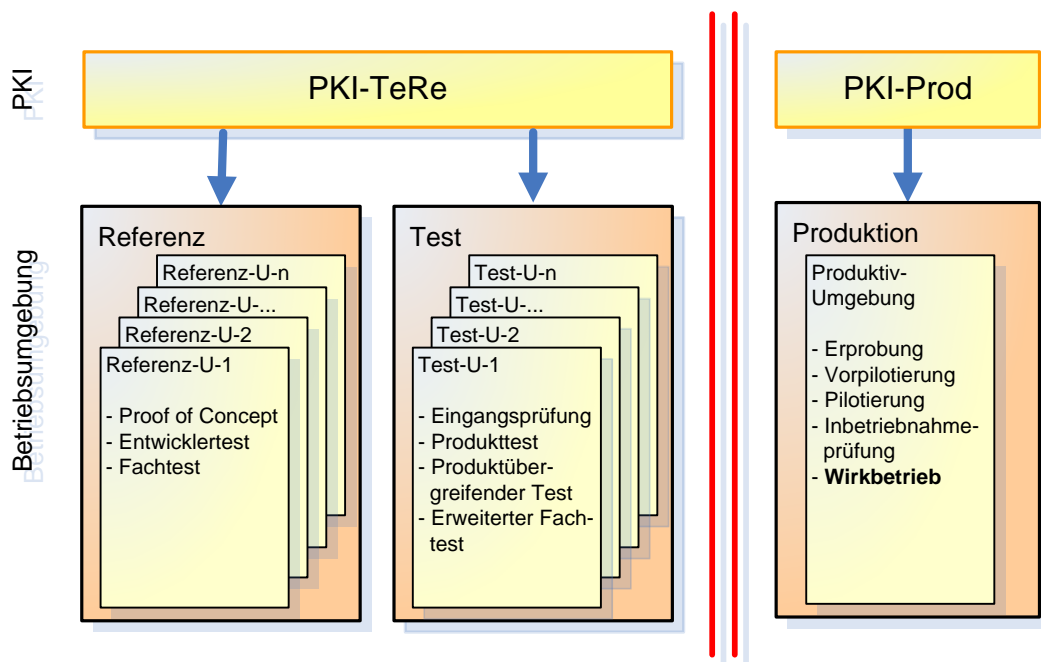


Abbildung 1: Betriebsumgebungen aus Sicht der PKI

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.

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	FachanwendungsspezifischerDienst
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
Komponenten (Geräte und Dienste)	KOMP	Komponenten

3.5 Sperrungen von QES-CAs

Im Falle von sicherheitskritischen Incidents bei QES-CA-Zertifikaten (s. Definition und Beschreibung in [gemKPT_PKI_TIP#2.3.3.5]) müssen innerhalb der TI besondere Maßnahmen ergriffen werden, wenn die betroffene QES-CA Zertifikate für die TI ausstellt und durch die BNetzA gesperrt wurde.

☒ **GS-A_5065 Sperrung einer QES-CA**

Der Gesamtbetriebsverantwortliche der TI MUSS im Falle der Sperrung einer QES-CA in Kooperation mit der BNetzA die erforderlichen Maßnahmen für die TI festlegen und den TSL-Dienst entsprechend anweisen. ☒

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 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., in den einzelnen Namens-elementen zu verarbeiten und darzustellen. Es MUSS dazu ein Zeichensatz gemäß [Common-PKI#Part1] unterstützt 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 gemäß [Common-PKI#Part 1] (s. o.) 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. 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 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

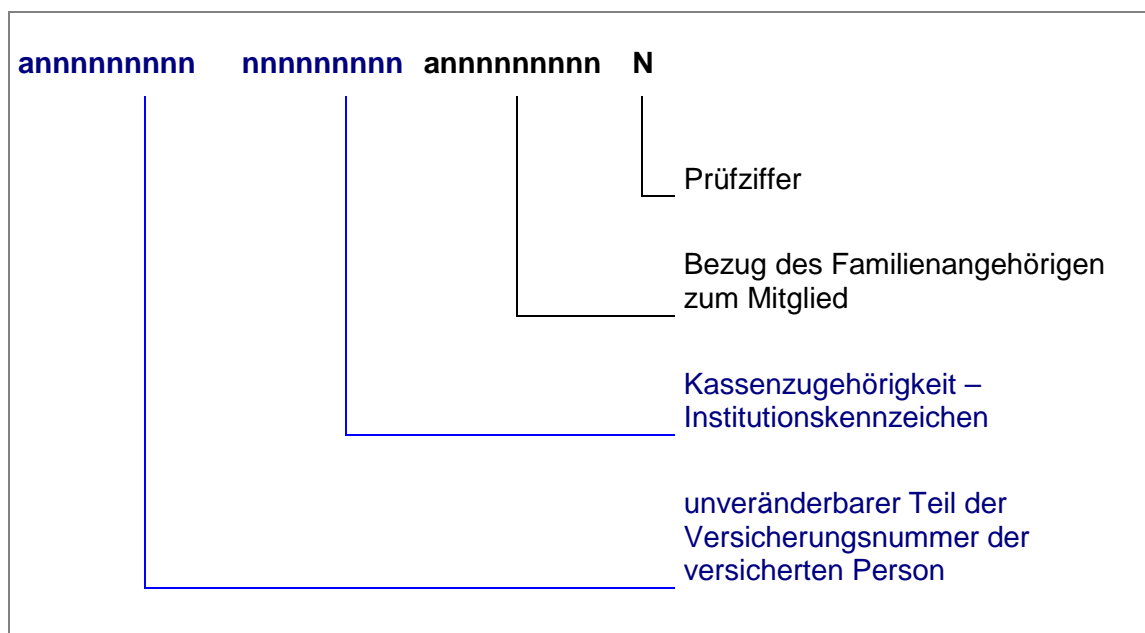


Abbildung 2: Aufbau der Krankenversichertennummer

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 Zertifikats-herausgeber 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 =
„Mustername1M331784849A32C93C6946314A9“

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 Versichertenkarten 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.

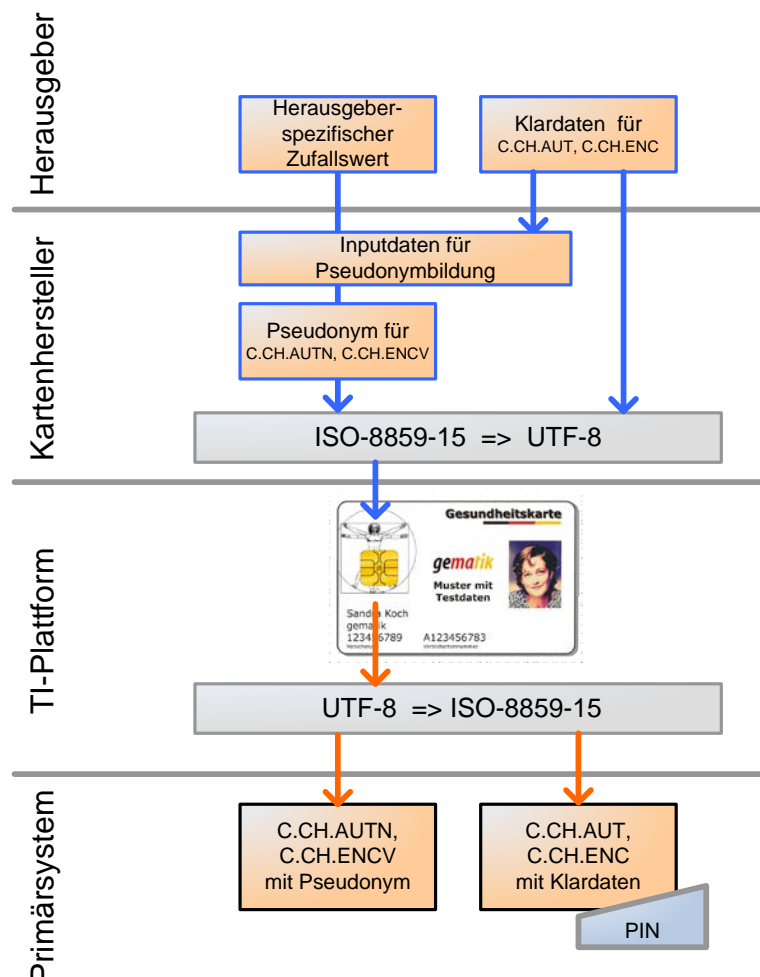


Abbildung 3: Pseudonym Kodierung in X.509-Versichertenkarten

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

Der eGK-Herausgeber MUSS das Pseudonym im UTF-8-Zeichensatz codiert in das Zertifikat der eGK einbringen. ☒

4.4 Berufsgruppen-ID der Leistungserbringer

4.4.1 Berufsgruppe des Heilberufers

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

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

☒ **GS-A_4583 Berufsgruppenkennzeichen für HBA**

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

☒ **GS-A_4584 Verwendung von Berufsgruppenkennzeichen**

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

Tabelle 9: Tab_PKI_221 Berufsgruppenkennzeichnung

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

4.5 ID der Organisation/Einrichtung des Gesundheitswesens

4.5.1 Typ und Exemplar der Organisation/Einrichtung des Gesundheitswesens

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

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

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

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

☒ **GS-A_4586 Verwendung von Institutionskennzeichen**

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

Tabelle 10: Tab_PKI_222 Institutionstypkennzeichnung

Art der ID	Ort	X.509 Feldname	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>	1-1a25sd-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 eindeutiges 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 eindeutig 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. Ein Suffix zum Hochzählen bei Folgekarten wird nicht verwendet.

☒ **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 Herausgabepolicies 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	<code>ProfessionItem</code>	Text	<Berufsgruppe>	Ärztin/Arzt
		<code>ProfessionOID</code>	OID	oid_<berufsgruppe>	1.2.276.0.76.4.30
Einzelne Person / Institution	Admission	<code>registrationNumber</code>	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 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	LE-Adv (Reserved for future use)	
7	KTR-Adv	
8	Kostenträger	GKV-SV

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

Der Nummernraum des Präfixes wird durch die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) verwaltet. Ein Präfix für weitere Sektoren kann unter der E-Mail-Adresse Industriepartnermanagement@gematik.de formlos beantragt werden.

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 ge-

trennt 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 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 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 Kodierung der Attribute in X.509-Zertifikaten

Attribut / Attribut-OID ([Common-PKI], [RFC 5280])	Kodierung	Max. Stringlänge (Zeichen)
commonName {id-at 3}	UTF8String [RFC3629] *)	64
surName {id-at 4}	UTF8String [RFC3629] *)	64
localityName {id-at 7}	UTF8String [RFC3629] *)	128
stateOrProvinceName {id-at 8}	UTF8String [RFC3629] *)	128
streetAdress {id-at 9}	UTF8String [RFC3629] *)	128

Attribut / Attribut-OID ([Common-PKI], [RFC 5280])	Kodierung	Max. Stringlänge (Zeichen)
organizationName {id-at 10}	UTF8String [RFC3629] *)	64
organizationalUnitName {id-at 11}	UTF8String [RFC3629] *)	64
title {id-at 12}	UTF8String [RFC3629] *)	64
postalCode {id-at 17}	UTF8String [RFC3629] *)	40
givenName {id-at 42}	UTF8String [RFC3629] *)	64
serialNumber {id-at 5}	PrintableString [RFC5280]	64
countryName {id-at 6}	PrintableString [RFC5280] gültiger "ISO 3166-1 alpha-2 country code" [ISO 3166-1]	2
organizationIdentifier {id-at 97}	UTF8String [X.520]	-
*) Einschränkung des erlaubten Zeichensatzes auf dedizierte ISO-Subsets gemäß Vorgaben der jeweiligen Kartenherausgeber		

4.8.2 Stringlänge der Attribute

☒ GS-A_4715 Maximale Stringlänge der Attribute im SubjectDN

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

☒ GS-A_4716 Umgang mit überlangen Organisationsnamen im SubjectDN

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

Hinweis:

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

4.8.3 Struktur

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

4.8.3.1 serialNumber

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

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

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

Der Nummernraum des Präfixes wird durch die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) 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),
- 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 TI-spezifische Vorgabe zur Nutzung der Extension Admission**

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

Tabelle 17: Tab_PKI_226 Struktur Admission

#	ASN.1 DEFINITION	TI-SPEZIFISCHE VORGABEN
1	id-isismtt-at-admission OBJECT IDENTIFIER ::= {id-isismtt-at 3}	
2	id-isismtt-at-namingAuthorities OBJECT IDENTIFIER ::= {id-isismtt-at 11}	
3	AdmissionSyntax ::= SEQUENCE {	
4	admissionAuthority GeneralName OPTIONAL,	Angabe (optional) der admissionAuthority auf der obersten Ebene der Extension in Form eines Distinguished Name (directoryName). In den jeweiligen Zertifikatsprofilen und -ausprägungen wird dieser Distinguished Name in Textform gemäß [RFC4514] dargestellt.
5	contentsOfAdmissions SEQUENCE OF Admissions }	Diese Sequenz MUSS genau ein Element vom Typ Admissions enthalten.
6	Admissions ::= SEQUENCE {	
7	admissionAuthority [0] EXPLICIT GeneralName OPTIONAL,	
8	namingAuthority [1] EXPLICIT NamingAuthority OPTIONAL,	
9	professionInfos SEQUENCE OF ProfessionInfo }	Diese Sequenz MUSS ein Element vom Typ ProfessionInfo enthalten.
...		
14	ProfessionInfo ::= SEQUENCE {	
15	namingAuthority [0] EXPLICIT NamingAuthority OPTIONAL,	
16	professionItems SEQUENCE OF DirectoryString (SIZE(1..128)),	professionItems enthält ein Element von Typ DirectoryString Für DirectoryString MUSS die Kodierung UTF8String verwendet werden.
17	professionOIDs SEQUENCE OF OBJECT IDENTIFIER OPTIONAL,	Dieses Element MUSS eine OID enthalten.
18	registrationNumber PrintableString(SIZE(1..128)) OPTIONAL,	Wenn dieses optionale Feld enthalten ist, enthält es die Telematik-ID. In QES-HBA-Zertifikaten für Ärzte wird das Feld registrationNumber nicht gesetzt.

19	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 werden im Internet mittels einer CRL auf ihren Sperrstatus geprüft.

☒ **GS-A_5074 Bereitstellung 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 diese Zertifikate eine CRL im Internet bereitstellen. ☒

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 Komplettspernung aller Zertifikate einer Karte**

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

4.9.3 Benennung der Zertifikatsprofile

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

4.9.4 Distinguished Name

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

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

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

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

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

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

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 und TSP-X.509 QES MÜSSEN die Namen (CN: und O:) der EE-Zertifikate (außer der eGK-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

Zertifikatstyp	Halter / Art	CN Test-PKI gleich CN Produktiv-PKI?
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.CM.TLS-CS	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 beispielsweise 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.

Die Schreibweise der Termini entspricht [Common-PKI].

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

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

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

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

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

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

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

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

5.1 eGK – Versichertenkarte

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 folgen-

de 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.

☒ **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 ist eine Suspendierung/Desuspendierung nicht möglich. ☒

5.1.3.1 C.CH.AUT – 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. ☒

Tabelle 22: Tab_PKI_232 C.CH.AUT Authentisierung eGK

Element	Inhalt	Kar	
certificate	C.CH.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	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) policyIdentifier = <oid_egk_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_versicherter> gemäß [gemSpec_OID#GS-A_4442] professionOID = OID <oid_versicherter> gemäß gemSpec_OID#GS-A_4442	1 1	FALSE

Element	Inhalt	Kar	
ExtendedKeyUsage {2 5 29 37}	keyPurposeld = 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

Element	Inhalt	Kar	
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]	1	

Element	Inhalt	Kar	
	und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
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
SubjectDirectory-Attributes (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}	keyPurposeld = 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-	1	FALSE

		A_4442]	professionOID = OID <oid_versicherter> gemäß gemSpec_OID#GS-A_4442	1	
		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 – Heilberufausweis

☒ 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 Umsetzung Zertifikatsprofil C.HP.AUT

Der TSP-X.509 nonQES MUSS C.HP.AUT gemäß Tab_PKI_268 umsetzen. ☒

Tabelle 27: Tab_PKI_268 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	

Element	Inhalt *)	Kar.	
	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
	KeyUsage {2 5 29 15}	Für Schlüsselgeneration RSA: digitalSignature keyEncipherment Für Schlüsselgeneration ECDSA: digitalSignature keyAgreement	1 1 1 1
	SubjectAltNames {2 5 29 17}	rfc822Name = E-Mail-Adresse	0-1
	BasicConstraints {2 5 29 19}	ca = FALSE	1
	CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = <URL zur Publikation der Zertifikatsrichtlinie(n)> policyIdentifier = <oid_hba_aut> gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP-spezifischen Zertifikatsrichtlinie ggf. weitere sektorspezifische policyIdentifier und policyQualifierInfo	1 0-1 1 0-1 0-1 0-1
	CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1
	AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1
	Admission {1 3 36 8 3 3}	admissionAuthority = {O=< zuständige Registrierungsstelle gemäß sektorspezifischer Ausprägung*>,C=DE} professionItem = gemäß [gemSpec_OID#GS-A_4442] professionOID = gemäß [gemSpec_OID#GS-A_4442] registrationNumber = Telematik-ID des Inhabers	1 1 1 1
	ExtendedKeyUsage {2 5 29 37}	keyPurposeld = id-kp-clientAuth keyPurposeld = id-kp- emailProtection	1 1
	ValidityModel {1 3 6 1 4 1 8301 3 5}	nicht gesetzt	0
	QCStatements {1 3 6 1 5 5 7 1 3}	nicht gesetzt	0
	additionalInformation {1 3 36 8 3 15}	nicht gesetzt	0
	Restriction {1 3 36 8 3 8}	nicht gesetzt	0

Element	Inhalt *)	Kar.	
 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 Umsetzung Zertifikatsprofil C.HP.ENC

Der TSP-X.509 nonQES MUSS C.HP.ENC gemäß Tab_PKI_269 umsetzen. ☒

Tabelle 28: Tab_PKI_269 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	1	TRUE

Element	Inhalt *)	Kar.	
	dataEncipherment	1	
	Für Schlüsselgeneration ECDSA: keyAgreement	1	
SubjectAltNames {2 5 29 17}	rfc822Name = E-Mail-Adresse	0-1	FALSE
BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = <URL zur Publikation der Zertifikatsrichtlinie(n)> policyIdentifier = <oid_hba_enc> gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP-spezifischen Zertifikatsrichtlinie ggf. weitere sektorspezifische policyIdentifier und policyQualifierInfo	1 0-1 1 0-1 0-1 0-1	FALSE
CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
Admission {1 3 36 8 3 3}	admissionAuthority = {O=< zuständige Registrierungsstelle gemäß sektorspezifischer Ausprägung*>,C=DE} professionItem = gemäß [gemSpec_OID#GS-A_4442] professionOID = gemäß [gemSpec_OID#GS-A_4442] registrationNumber = Telematik-ID des Inhabers	1 1 1 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 Umsetzung Zertifikatsprofil C.HP.QES

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

Tabelle 29: Tab_PKI_270 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>	1 0-1 1 1	FALSE

Element	Inhalt *)	Kar.	
	policyQualifierInfo = URL der TSP-spezifischen Zertifikatsrichtlinie ggf. weitere sektorspezifische policyIdentifier und policyQualifierInfo	0-1 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 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	0-1	FALSE
Restriction {1 3 36 8 3 8}	Falls das optionale esi4-qcStatement-2 gesetzt und/oder hier ein weiterer Freitext enthalten ist, muss diese Erweiterung mindestens die folgende Ergänzung enthalten: <i>Jegliche Beschränkungen gelten nicht für Anwendungen gemäß § 291a SGB V.</i>	0-1	FALSE
andere Erweiterungen		0	
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4358]		
signature	Wert der Signatur		

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

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

Zusatzinformationen zu einzelnen Feldern:

- **SubjectDN**

Bildungsregel-Vorschlag gemäß Informationen aus bisherigen Sektor-Spezifikationen:

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

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

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

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

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

- **SubjectSerialNumber**

Zusätzliche Hinweise gemäß Informationen aus bisherigen Sektor-Spezifikationen:

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

Bildungs-Vorschlag für subjectSerialNumber:

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

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

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**

Die Attribute serialNumber, givenName, surname, ggf. title und commonName werden in einem SET als ein einziges multivaluedRDN kodiert. Die entsprechenden Kodierungsregeln von X.690 (Reihenfolge im SET) müssen berücksichtigt werden.

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. 

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.

1.		
2.	Zusatz-undVermerkzone	elektronischeFreimachungsvermerke, Vorausverfügungen,Produkte
3.		
1.		
2.		
3.	Anschriftzone	Anschrift
4.		
5.		
6.		

Beispiel

1.	
2.	
3.	
1.	Kinderarzt
2.	Dr.med.KarlMustermann
3.	
4.	
5.	
6.	

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

Element	Inhalt *)	Kar.	
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}	keyPurposeld = 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	
organizationalUnitNam	Organisationseinheit der Organisation/Einrichtung	0-1	

Element	Inhalt *)	Kar.	
e	des Gesundheitswesens		
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]		

Element	Inhalt *)	Kar.	
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	0-1	FALSE

Element	Inhalt *)	Kar.	
	oder Ergänzungen	0-1	
BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_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, DE]

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	
streetAddress	Anschrift des Kartenterminal-Herstellers	0-1	

Element		Inhalt	Kar.	
	postalCode	Postleitzahl der Anschrift des Kartenterminal-Herstellers	0-1	
	localityName	Stadt der Anschrift des Kartenterminal-Herstellers	0-1	
	stateOrProvinceName	Bundesland der Anschrift des Kartenterminal-Herstellers	0-1	
	countryName	DE 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}	keyPurposeld = 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 angegeben wird. ☒

☒ **GS-A_4607 Zuordnung Konnektorinstanz zu verbauter gSMC-K**

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

5.6.2 Aufbau des SubjectDN

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

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

5.6.3 Statusprüfung von Konnektorzertifikaten

Nur für das Zertifikat des Netzkonnektors ist eine Statusprüfung per OCSP vorgesehen.

☒ **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 vorsehen. ☒

Tabelle 34: Tab_PKI_237 Statusprüfung von Konnektorzertifikaten

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

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	DE 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

Element	Inhalt	Kar.	
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}	keyPurposeld = id-kp-clientAuth keyPurposeld = 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		

Element	Inhalt	Kar.	
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	DE 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}	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 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}	keyPurposeld = id-kp-clientAuth keyPurposeld = id-kp-serverAuth	1 1	FALSE
andere Erweiterungen		0	
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus		

Element	Inhalt	Kar.	
	gemäß [gemSpec_Krypt#GS-A_4359]		
signature	Wert der Signatur		

5.6.4.3 C.SAK.AUT - Authentisierung SAK

Die Identität der SAK dient zur Authentisierung gegenüber den Kartenterminals und dem Extended Trusted Viewer. Darüber hinaus muss sich die Signaturanwendungskomponente (SAK) des Konnektors gegenüber dem Heilberufsausweis als solche ausweisen, um Stapelsignaturen durchführen zu können. Der SAK ist hierfür eine spezifische Rolle (Profil) zugeordnet.

☒ **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	DE 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:	1 1	TRUE

Element	Inhalt	Kar.	
	digitalSignature	1	
SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Konnektor-Herstellers	0-1	FALSE
BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_sak_aut>	1 0-1 1	FALSE
CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	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 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}	keyPurposeld = id-kp-clientAuth keyPurposeld = id-kp-serverAuth	1 1	FALSE
<i>andere Erweiterungen</i>		0	
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
signature	Wert der Signatur		

5.7 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 Zugangsdiensteanbieters	1	
countryName	DE Land der Anschrift des Zugangsdiensteanbieters	1	
andere Attribute		0	
subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4360] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
extensions			critical
SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Konzentrators	1	FALSE
KeyUsage {2 5 29 15}	Für Schlüsselgeneration RSA: digitalSignature keyEncipherment Für Schlüsselgeneration ECDSA: digitalSignature	1 1 1	TRUE
SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Zugangsdiensteanbieters	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_vpnk_vpn>	1 0-1 1	FALSE
CRLDistributionPoints {2 5 29 31}	URL für CRL-Statusdienst DN d. CRL-Ausstellers (f. indirekte CRL, s.	1 1	FALSE

Element	Inhalt	Kar.	
	RFC5280#4.2.1.13) reasons	0	
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 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}	keyPurposel = id-kp-clientAuth keyPurposel = 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 Zugangsdiensteanbieters	1	
countryName	DE Land der Anschrift des Zugangsdiensteanbieters	1	
andere Attribute		0	
subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4360] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
extensions			critical
SubjectKeyIdentifier	keyIdentifier = ID des öffentlichen Schlüssels des	1	FALSE

Element	Inhalt	Kar.	
{2 5 29 14}	Konzentrators		
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	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_vpnk_vpn_sis>	1 0-1 1	FALSE
CRLDistributionPoints {2 5 29 31}	URL für CRL-Statusdienst DN d. CRL-Ausstellers (f. indirekte CRL, s. RFC5280#4.2.1.13) reasons	1 1 0	FALSE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	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 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}	keyPurposeld = id-kp-clientAuth keyPurposeld = 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		

5.7.3.3 VPN-Zugangsdienst – Verwendung mehrerer Schlüsselpaare

Unabhängig von der Ausprägung mehrerer kryptographischer Identitäten für unterschiedliche Verwendungen (TI, Sicherer Internetzugang), können für einen Verwendungszweck als Vorbereitung neuer Krypto-Generationen auch zwei Schlüsselpaare verwendet werden.

☒ **GS-A_4728 Verwendung von zwei Schlüsselpaaren im VPN-Zugangsdienst**

Der Zugangsdienstanbieter KANN seinen VPN-Zugangsdienst mit je zwei Schlüsselpaaren und zugehörigen zwei X.509-Komponentenzertifikaten ausstatten, um auf neue Krypto-Generationen vorbereitet zu sein. ☒

Anmerkung: Die eindeutige Bezeichnung für solche Schlüssel und Zertifikate wird durch die Festlegungen in den Kapiteln 2.8 und 2.9 vorgegeben.

☒ **GS-A_4729 Vorgaben bei Verwendung von zwei Schlüsselpaaren im VPN-Zugangsdienst**

Der Zugangsdienstanbieter MUSS im Falle, dass sein VPN-Zugangsdienst mit zwei Schlüsselpaaren ausgestattet ist, sicherstellen, dass folgende Anforderungen erfüllt werden (a) die Vorgaben aus [gemSpec_Krypt#GS-A_4360] werden erfüllt und (b) die SubjectDN der beiden Zertifikate sind identisch. ☒

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 Telematikinfrastuktur 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	1	

Element		Inhalt	Kar	
		gemäß Zuweisung		
	serialNumber	bei Bedarf zur Unterscheidung gleichartiger Instanzen	0-1	
	organizationName	Name des verantwortlichen Anbieters	1	
	countryName	DE 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	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_zd_tls_s>	1 0-1 1	FALSE
	CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
	AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
	Admission {1 3 36 8 3 3}	professionItem = Beschreibung der technischen Rolle gemäß [gemSpec_OID#GS-A_4446] professionOID = OID der technischen Rolle gemäß [gemSpec_OID#GS-A_4446]	1 1	FALSE
	ExtendedKeyUsage {2 5 29 37}	keyPurposeld = 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 Werte aus dem im Rahmen ihrer Anbieterzulassung zugewiesenen Domainnamen aus dem Namensraum der TI verwenden. ☒

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]		

Element	Inhalt	Kar.	
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	DE 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_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	DE 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_tls_s>	1 0-1 1	FALSE
CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
AuthorityInfoAccess	URL für OCSP-Statusdienst	1	FALSE

Element	Inhalt	Kar.	
{1 3 6 1 5 5 7 1 1}			
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
<i>andere Erweiterungen</i>		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 43: 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	DE 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

Element	Inhalt	Kar.	
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	keine Festlegung	0-1	FALSE
AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
Admission {1 3 36 8 3 3}	professionItem = Beschreibung der technischen Rolle gemäß [gemSpec_OID#GS-A_4446] professionOID = OID der technischen Rolle gemäß [gemSpec_OID#GS-A_4446]	1 1	FALSE
ExtendedKeyUsage {2 5 29 37}	keyPurposel = id-kp-clientAuth keyPurposel = 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 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. ☒

5.11.1 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) OCSP-Signer-CA, iv) CRL-Signer-CA, v) TSL-Signer-CA. ☒

Tabelle 44: 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	1 0-1	FALSE

Element	Inhalt	Kar.	
	Publikation der Zertifikatsrichtlinie)		
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		

5.11.2 <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 Attributbelegung der Felder gemäß Tab_PKI_212 und die Namenskonvention gemäß Tab_PKI_213 umsetzen. ☒

Tabelle 45: 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

Element	Inhalt	Kar.	
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> davon abweichend: CAs für HBA-AUT/ENC- Zertifikate: policyIdentifier = <oid_policy_hba_cp> policyQualifierInfo = URL 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	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
<i>andere Erweiterungen</i>		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.

5.11.3 <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 46: 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		

Element	Inhalt	Kar.	
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.

5.12 OCSP – Statusauskunftsdienst

5.12.1 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. Bereits von der OCSP-Signer-CA der gematik bezogene OCSP-Signer-Zertifikate können weiter verwendet 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.)

5.12.2 Aufbau des SubjectDN

Siehe Tab_PKI_253.

5.12.3 X.509 Zertifikatsprofil der OCSP-Signer-CA

☒ **GS-A_4740 Zentrale OCSP-Signer-CA-Zertifikate**

Der TSP-X.509 nonQES MUSS für die von ihm betriebenen OCSP-Signer-CAs die Attributsbelegung der Felder gemäß Tab_PKI_212 und die Namenskonvention für den OCSP-Dienst gemäß Tab_PKI_213 umsetzen. ☒

5.12.4 X.509 Profil des OCSP-Signer-Zertifikates

5.12.4.1 C.GEM.OCSP OCSP-Signer-Zertifikat

☒ GS-A_4741 Umsetzung Zertifikatsprofil C.GEM.OCSP

Der TSP-X.509 nonQES MUSS C.GEM.OCSP gemäß Tab_PKI_253 umsetzen. ☒

Tabelle 47: 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

Element	Inhalt	Kar.	
ExtendedKeyUsage {2 5 29 37}	KeyPurposeld = 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		

5.13 CRL – Statusauskunftsdienst

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

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

5.13.1 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 für die von ihm betriebenen CRL-Dienste aus einer CRL-Signer-CA beziehen, die von der gematik Root-CA abgeleitet ist. ☒

☒ 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. ☒

5.13.2 Aufbau des SubjectDN

Siehe Tab_PKI_214.

5.13.3 X.509 Zertifikatsprofil der CRL-Signer-CA

☒ GS-A_4938 Zentrale CRL-Signer-CA-Zertifikate

Der TSP-X.509 nonQES MUSS für die von ihm betriebenen CRL-Signer-CAs die Attributsbelegung der Felder gemäß Tab_PKI_212 und die Namenskonvention für den CRL-Dienst gemäß Tab_PKI_213 umsetzen. ☒

5.13.4 X.509 Profil des CRL-Signer-Zertifikates

5.13.4.1 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 48: 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	policyIdentifier = <oid_policy_gem_or_cp>	1	FALSE

Element	Inhalt	Kar.	
{2 5 29 32}	policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie)	0-1	
CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	keine Festlegung	0-1	FALSE
AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
ExtendedKeyUsage {2 5 29 37}		0	FALSE
<i>andere Erweiterungen</i>		0	
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
signature	Wert der Signatur		

5.14 TSL - Zertifikatsprofile

5.14.1 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. ☒

5.14.2 Aufbau des SubjectDN

Siehe Tab_PKI_252.

5.14.3 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. ☒

5.14.4 TSL-Signer- Zertifikat

☒ GS-A_4745 Umsetzung Zertifikatsprofil C.TSL.SIG für TSL-Dienst

Der Anbieter des TSL-Dienstes MUSS das TSL-Signer-Zertifikat C.TSL.SIG gemäß Tab_PKI_252 umsetzen. ☒

Tabelle 49: Tab_PKI_252 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	Name des Anbieters TSL-Dienst	1	
countryName	Land der Anschrift des TSP	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
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	

Element	Inhalt	Kar.	
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
signature	Wert der Signatur		

☒ **GS-A_4746 Belegung organizationName im Zertifikatsprofil C.TSL.SIG für TSL-Dienst**

Der Anbieter des TSL-Dienstes SOLL den „organizationName“ im Subject des TSL-Signer-Zertifikats analog des Elements „Scheme operator name“ in der TSL umsetzen. ☒

5.14.5 TSL-OCSP-Responder-Zertifikat

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

Der Anbieter des TSL-Dienstes 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 Anbieter des TSL-Dienstes MUSS das OCSP-Signer-Zertifikat aus der zentral in der TI bereitgestellten OCSP-Signer-CA 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 6.4.1.2 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 6.4.1.3 beschrieben.

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 Profilen in CV-Zertifikaten erfolgt für Karten der Generation 1 anders als für Karten der Generation 2:

- Bei Karten der Generation 1 wird die Profilnummer direkt als Bestandteil der Kodierung im Feld CHA genutzt (siehe Kapitel 6.4).
- Bei Karten der Generation 2 wird die Profilnummer in eine Flagliste übersetzt, die die Berechtigungen steuert und im Feld CHAT gespeichert ist (siehe Kapitel 6.7).

6.3.1 Rollenauthentisierung

☒ **GS-A_4620 Zugriffsprofil einer eGK**

Der Kartenherausgeber MUSS sicherstellen, dass das CV-Rollen-Zertifikat einer eGK als Zugriffsprofil den Wert '00' (G1) bzw. '00 0000 0000 0000' (G2) 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. ☒

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 1 und der Generation 2.

Die Tabelle enthält auch, welche Organisation als sog. „Qualifizierende Stelle“ 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. Im Rahmen ihrer Zulassung bei der gematik müssen diese Betreiber den Nachweis der Qualifizierung erbringen. Für derzeit nicht verwendete Profile ist diese Zuordnung offen.

Es werden die Zugriffsprofile 0 – 919 für eine Rollenauthentisierung unterschieden:

Tabelle 50: 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						
CHA.0	eGK	Versicherter	Versichert er	keine Qualifizierung	Versicherte/-r	oid_versicherter
1						
CHA.1	SMC-B eKiosk KTR-AdV	eKiosk KTR-AdV	Versichert er	Nicht definiert GKV-SV	Nicht definiert AdV-Umgebung bei Kostenträger	Nicht definiert oid_adv_ktr
2						
CHA.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
CHA.2Z A	HBA – Zahnarzt	Zahnarzt in einer Institution	Zahnarzt	BZÄK	Zahnärztin/Zahnarzt	oid_zahnarzt
CHA.2A	(H)BA für Mitarbeiter(innen) in Arztpraxis, oder Krankenhaus	Mitarbeiter medizinische Institution (z. B. in Arztpraxis, Krankenhaus). Der „Mitarbeiter medizinische Institution“ verkörpert gegenüber der TI die Institution des Arztes	Nicht definiert	Nicht definiert	Nicht definiert	Nicht definiert
CHA.2Z A	(H)BA für Mitarbeiter(innen) in Zahnarztpraxis	Mitarbeiter medizinische Institution (z. B. in Zahnarztpraxis). Der „Mitarbeiter medizinische Institution“ verkörpert gegenüber der TI die Institution des Zahnarztes	Nicht definiert	Nicht definiert	Nicht definiert	Nicht definiert
CHA.2A	SMC-B	Mitarbeiter medizinische Institution Arztpraxis (inkl. Praxis ärztlicher Psychotherapeut) mit Autorisierung und Protokollierung gemäß § 291a Abs. 5 Satz 4 SGB V. Der „Mitarbeiter medizinische Institution“	Mitarbeiter Arzt	KV	Betriebsstätte Arzt	oid_praxis_arzt

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
		verkörpert gegenüber der TI die Institution des Arztes.				
CHA.2Z A	SMC-B	Mitarbeiter medizinische Institution Zahnarztpraxis mit Autorisierung und Protokollierung gemäß § 291a Abs. 5 Satz 4 SGB V. Der „Mitarbeiter medizinische Institution“ verkörpert gegenüber der TI die Institution des Zahnarztes.	Mitarbeiter Zahnarzt	KZBV	Zahnarztpraxis	oid_zahnarztpraxis
CHA.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						
CHA.3	HBA – Apotheker	Apotheker in einer öffentlichen Apotheke oder einer Krankenhausapotheke, jeweils mit Sitz in Deutschland.	Apotheker	BAK	Apotheker/in	oid_apotheker
CHA.3	(H)BA für Mitarbeiter(-innen) der Apotheke	Mitarbeiter Apotheke als berufsmäßiger Gehilfe oder Person, die zur Vorbereitung auf den Beruf tätig ist, gemäß § 291a Abs. 4 [SGB V]. Der „Mitarbeiter Apotheke“ verkörpert gegenüber der TI die Institution des Apothekers.	Apotheker	BAK	Apotheker-assistent/in Pharmazieingenieur/in Apotheken-assistent/-in	oid_apothekerassistenten oid_pharmazieingenieur oid_apothekenassistent
CHA.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 Betriebserlaubnisinhaber zuständige Apothekerkammer	Öffentliche Apotheke	oid_öffentliche_apotheke

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
4						
CHA.4	HBA – Psychotherapeut	Psychologischer Psychotherapeut, Kinder- und Jugendlichenpsychotherapeut	Psychotherapeut	BPTK	Psychotherapeut/ in Psychologische/r Psychotherapeut/ in Kinder- und Jugendlichenpsychotherapeut/-in	oid_psychotherapeut oid_ps_psychotherapeut oid_kuj_psychotherapeut
CHA.4	SMC-B	Institutionskarte eines Psychotherapeuten. Der mit der Karte mögliche Zugriff auf die medizinischen Anwendungen der eGK ist ausschließlich dem psychologischen Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten selbst gestattet und nicht seinen berufsmäßigen Gehilfen.	Nicht definiert Mitarbeiter Psychotherapeut	KV	Betriebsstätte Psychotherapeut	oid_praxis_psychotherapeut
5						
CHA.5	(H)BA sonstige Leistungserbringer	Heilmittelerbringer mit (H)BA Hilfsmittelerbringer mit BA	Sonstige Leistungserbringer	Nicht definiert	Nicht definiert	Nicht definiert
6						
CHA.6	SMC	Kein fachlicher Akteur - wird nicht verwendet	Nicht definiert	Nicht definiert	Nicht definiert	Nicht definiert
7						
CHA.7	(H)BA	Rettungsassistent Bei den Akteuren handelt es sich um „Angehörige eines anderen Heilberufs, die für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung“ (§ 291a Abs. 4 Satz 1 Nr. 2e) absolviert haben.	Anderer Heilberuf	Nicht definiert	Rettungsassistent/-in Notfallsanitäter/-in	oid_rettungsassistent oid_notfallsanitaeter

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
CHA.7	SMC-B	Mobile Einrichtung Rettungsdienst	Nicht definiert	Nicht definiert	Betriebsstätte Mobile Einrichtung Rettungsdienst	oid_mobile_einrichtung_rettungsdienst
8						
CHA.8	SMC-B (ohne Zugriff auf med. Daten)	Mitarbeiter von Gesundheitseinrichtungen ohne eigenen HBA oder BA	Mitarbeiter Medizinische Institution	Nicht definiert	Nicht definiert	Nicht definiert
CHA.8		Mitarbeiter von Krankenkassen	Mitarbeiter Kostenträger	GKV-SV	Betriebsstätte Kostenträger	oid_kostenträger
CHA.8		Verifikationskarten Kostenträger	Mitarbeiter Kostenträger	GKV-SV	n.a. (Karte enthält keine X.509)	n.a. (Karte enthält keine X.509)
9						
CHA.9	SMC-B (mit Zugriff auf med. Daten)	a) Mitarbeiter von Gesundheitseinrichtungen ohne eigenen HBA oder BA	a) Mitarbeiter Medizinische Institution	Nicht definiert	Nicht definiert	Nicht definiert
CHA.9		b) ohne zugeordneten Akteur, sichere Einsatzumgebung für Versicherten	b) Versicherter	Nicht definiert	Nicht definiert	Nicht definiert
10						
CHA.10	SMC-B UzWdRdV LE-AdV	Versicherter in der „Umgebung zur Wahrnehmung der Rechte des Versicherten“ UzWdRdV Leistungserbringers (LE-AdV) im Kontrollbereich eines Leistungserbringers	Versicherter	Nicht definiert (identisch zur qualifizierenden Stelle der SM-B des Instituts, in dem das AdV-Terminal aufgestellt wird)	Nicht definiert AdV Umgebung bei Leistungserbringer	Nicht definiert oid_adv_le

6.3.2 Authentisierung einer Funktionseinheit

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

Tabelle 51: Tab_PKI_255 Zugriffsprofile G2 für eine Authentisierung einer Funktionseinheit

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

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

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

☒ **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 Aufbau und Bestandteile eines CV-Zertifikats der Generation 1

In diesem Kapitel werden so genannte „nicht selbstbeschreibende“ CV-Zertifikate für G1-Karten betrachtet, welche eine Signatur mit „Message Recovery“ gemäß [ISO 9796-2], DS1 enthalten.

6.4.1 Bestandteile eines CV-Zertifikats

Alle im vorliegenden Kapitel betrachteten signierten Nachrichten *M* enthalten die in den folgenden Abschnitten beschriebenen Informationen.

6.4.1.1 Certificate Profile Identifier (CPI)

Der Certificate Profile Identifier (CPI) hat den Zweck, die genaue Struktur eines CV-Zertifikates anzuzeigen. Die folgenden Werte sind zu unterscheiden:

Tabelle 52: Tab_PKI_256 Mögliche Werte für CPI

CV-Zertifikat für	Wert für CPI
CVC-CA	'21'
Chipkarte	'22'

☒ GS-A_4625 CPI für CV-Zertifikate einer CVC-CA

Die CVC-Root-CA MUSS als Wert für den CPI '21' in das CV-Zertifikat einer CVC-CA der Generation 1 eintragen. ☒

☒ GS-A_4626 CPI für CV-Zertifikate einer Karte

Der TSP-CVC MUSS als Wert für den CPI '22' in das CV-Zertifikat einer Karte (eGK, HBA, SM-B, gSMC-K) der Generation 1 eintragen. ☒

6.4.1.2 Certification Authority Reference (CAR)

Die Certification Authority Reference (CAR) referenziert den Schlüssel der CVC-CA, welche das Zertifikat ausstellte. Das Feld CAR ist 8 Bytes lang und wie folgt weiter unterteilt:

Tabelle 53: Tab_PKI_257 Aufbau CAR für Karten der Generation 1

	CA Name	Service-Indikator	CA-spezifische Information	Algorithmenreferenz	Datum
Länge	5 Byte	1 BCD	1 BCD	2 BCD	2 BCD
zugelassene Werte	Anbieterkennung gemäß Registrierung bei Fraunhofer SIT	individuell belegbar	zur freien Verwendung durch den Anbieter; dient der	individuell belegbar zur Unterscheidung div. PuK-Algorithmen	letzte 2 Ziffern des Jahres der CA-Schlüssel-

	CA Name	Service-Indikator	CA-spezifische Information	Algorithmenreferenz	Datum
			Unterscheidung verschiedener CA-Schlüsselpaare		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_4627 Verwendung des Feldes Certificate Authority Reference**

Der Herausgeber eines CV-Zertifikats (CVC-Root-CA und CVC-CA) MUSS das Feld Certificate Authority Reference (CAR) weiter unterteilen in die Konkatenation der Datenelemente CA Name, Service-Indikator, CA-spezifische Information, Algorithmenreferenz und Datum und dabei die Festlegungen bzgl. Länge und zugelassener Werte gemäß Tab_PKI_257 berücksichtigen. ☒

Die Werte für die CA-spezifische Information kann der Herausgeber festlegen.

☒ **GS-A_4628 Zuordnung zwischen CAR und Schlüsselpaar des Herausgebers für Gen1**

Der Herausgeber eines CV-Zertifikats (CVC-Root-CA und CVC-CA) MUSS sicherstellen, dass die Zuordnung zwischen Certificate Authority Reference (CAR) und Schlüsselpaar eindeutig ist. ☒

6.4.1.3 Certificate Holder Reference (CHR)

Die Certificate Holder Reference (CHR) wird dazu verwendet, dem im Zertifikat enthaltenen öffentlichen Schlüssel einen eindeutigen Identifier zuzuordnen. 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 54: Tab_PKI_258 Aufbau CHR

CV-Zertifikat für	Länge CHR	Inhalt	
CVC-CA	8 Bytes	CAR zu dem Schlüsselpaar	
Chipkarte	12 Bytes	'xx xx' ICCSN der Chipkarte	
	Zertifikat	CHR	Anforderung für CHR
eGK	C.eGK.AUT_CVC.E256	'00 09' ICCSN	Card-G2-A_2363
HBA	C.HPC.AUTR_CVC.R2048	'00 10' ICCSN	Card-G2-A_3385
	C.HPC.AUTR_CVC.E256	'00 06' ICCSN	Card-G2-A_3386
	C.HPC.AUTD_SUK_CVC.E256	'00 09' ICCSN	Card-G2-A_3387
SMC-B	C.SMC.AUTR_CVC.R2048	'00 10' ICCSN	Card-G2-A_3388
	C.SMC.AUTR_CVC.E256	'00 06' ICCSN	Card-G2-A_3389
	C.SMC.AUTD__RPE_CVC.E256	'00 09' ICCSN	Card-G2-A_3390
gSMC-K	C.SMC.AUT_CVC.E256	'00 05' ICCSN	Card-G2-A_3328
	C.SMC.AUT_CVC.E384	'00 06' ICCSN	Card-G2-A_3331
	C.SAK.AUTD_CVC.E256	'00 0A' ICCSN	Card-G2-A_2638

	C.SAK.AUTD_CVC.E384	'00 0F' ICCSN	Card-G2-A_2640
gSMC-KT	C.SMC.AUTD_RPS_CVC.E256	'00 0A' ICCSN	Card-G2-A_2500
	C:SMS.AUTD_RPS_CVC.E384	'00 0F' ICCSN	Card-G2-A_2502

☒ **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. ☒

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.

6.4.1.4 Certificate Holder Authorisation (CHA)

Die Certificate Holder Authorisation (CHA) zeigt eine Rolle (Zugriffsprofil) des Zertifikatsinhabers an. Das Feld CHA existiert nur in CV-Rollen-Zertifikaten und CV-Gerätezertifikaten. Es ist wie folgt weiter unterteilt:

Tabelle 55: Tab_PKI_259 Aufbau CHA

AID Zugriffsprofil

☒ **GS-A_4631 CHA des CV-Zertifikats einer Karte**

Der TSP-CVC MUSS als Wert für die CHA ein Datum eintragen, das aus der Konkatenation der 6 Byte langen AID 'D2 76 00 00 40 00' der Gesundheitskartenanwendung und dem 1 Byte langen Zugriffsprofil gemäß Tab_PKI_254 für das zu zertifizierende Schlüsselpaar besteht. ☒

6.4.1.5 Object Identifier (OID)

Der Object Identifier (OID) in einem CV-Zertifikat beschreibt den Algorithmus, welcher dem Schlüssel im Zertifikat zugeordnet ist. Im Rahmen dieser Spezifikation werden verschiedene Algorithmen für verschiedene Verwendungszwecke genutzt, so dass implizit durch den Algorithmus-OID auch der Verwendungszweck des im Zertifikat enthaltenen öffentlichen Schlüssels festgelegt wird. OIDs sind weltweit eindeutig.

Es werden nur folgende OID-Werte verwendet:

Tabelle 56: Tab_PKI_260 Object Identifier der Registration Authority TeleTrust

CV-Zertifikat für	OID-Name	OID-Wert	OID-Codierung
CVC-CA	sigS_ISO9796-2Withrsa_sha256 signature scheme with RSA signature and DSI according to [ISO 9796-2] and SHA-256	{1 3 36 3 4 2 2 4}	2B24 0304 0202 04
Chipkarte	authS_ISO9796-2Withrsa_sha256_mutual authentication scheme with RSA signature and DSI according to [ISO 9796-2] and SHA-256 for mutual authentication with or without establishment of a Trusted Channel	{1 3 36 3 5 2 4}	2B24 0305 0204

Die Nutzung von SHA-256 ist in [FIPS 180-4#6.2] beschrieben.

☒ **GS-A_4632 OID für CV-Zertifikate einer CVC-CA**

Die CVC-Root-CA MUSS den Wert für den OID gemäß Tab_PKI_260 in das CV-Zertifikat einer CVC-CA der Generation 1 eintragen. ☒

☒ **GS-A_4633 OID für CV-Zertifikate einer Karte**

Der TSP-CVC MUSS den Wert für den OID gemäß Tab_PKI_260 in das CV-Zertifikat einer Karte (eGK, HBA, SM-B, gSMC-K) der Generation 1 eintragen. ☒

6.4.1.6 Öffentlicher Schlüssel

Der öffentliche RSA-Schlüssel besteht aus den Teilen Modulus und öffentlicher Exponent.

☒ **GS-A_4634 Öffentlicher Schlüssel eines CV-Zertifikats**

Der Herausgeber eines CV-Zertifikats (CVC-Root-CA und TSP-CVC) MUSS den zu zertifizierenden öffentlichen Schlüssel in das CV-Zertifikat eintragen. Der Herausgeber MUSS den Modulus hexadezimal, vorzeichenlos im Big-Endian-Format codiert und den öffentlichen Exponenten des öffentlichen Schlüssels hexadezimal, vorzeichenlos im Big-Endian-Format codiert im CV-Zertifikat angeben. ☒

6.4.2 Aufbau eines CV-Zertifikats

Ein CV-Zertifikat ist eine durch den Herausgeber signierte Datenstruktur, die in Form eines TLV-kodierten Datenobjekts vorliegt.

☒ **GS-A_4635 Aufbau eines CV-Zertifikats einer CVC-CA**

Die CVC-Root-CA als Herausgeber eines CV-Zertifikats MUSS das CV-Zertifikat einer CVC-CA als zusammengesetztes Datenobjekt gemäß Tabelle Tab_PKI_261 erzeugen. Sie MUSS dabei sicherstellen, dass das zusammengesetzte Datenelement genau die beiden primitiven Datenobjekte in der dargestellten Reihenfolge enthält. ☒

☒ GS-A_4636 Aufbau eines CV-Zertifikats zur Authentisierung

Der TSP-CVC als Herausgeber eines CV-Zertifikats MUSS das CV-Zertifikat zur Authentisierung als zusammengesetztes Datenobjekt gemäß Tabelle Tab_PKI_262 erzeugen. Er MUSS dabei sicherstellen, dass das zusammengesetzte Datenelement genau die beiden primitiven Datenobjekte in der dargestellten Reihenfolge enthält. ☒

Tabelle 57: Tab_PKI_261 CV-Zertifikat einer CVC-CA mit CPI = '21', SHA-256

Tag	L	Wert									
'7F21'	'820146'	CV-Zertifikat ('0146' = 326 Byte)									
		<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'5F37'</td><td>'820100'</td><td>Signatur SIG.CA ('0100' = 256 Byte)</td></tr> <tr> <td>'5F38'</td><td>'3E'</td><td>Non-Recoverable Part NRP ('003E' = 62 Byte)</td></tr> </table>	Tag	L	Wert	'5F37'	'820100'	Signatur SIG.CA ('0100' = 256 Byte)	'5F38'	'3E'	Non-Recoverable Part NRP ('003E' = 62 Byte)
Tag	L	Wert									
'5F37'	'820100'	Signatur SIG.CA ('0100' = 256 Byte)									
'5F38'	'3E'	Non-Recoverable Part NRP ('003E' = 62 Byte)									

Tabelle 58: Tab_PKI_262 CV-Zertifikat zur Authentisierung mit CPI = '22', SHA-256

Tag	L	Wert									
'7F21'	'820150'	CV-Zertifikat ('0150' = 336 Byte)									
		<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'5F37'</td><td>'820100'</td><td>Signatur SIG.CA ('0100' = 256 Byte)</td></tr> <tr> <td>'5F38'</td><td>'48'</td><td>Non-Recoverable Part NRP ('0048' = 72 Byte)</td></tr> </table>	Tag	L	Wert	'5F37'	'820100'	Signatur SIG.CA ('0100' = 256 Byte)	'5F38'	'48'	Non-Recoverable Part NRP ('0048' = 72 Byte)
Tag	L	Wert									
'5F37'	'820100'	Signatur SIG.CA ('0100' = 256 Byte)									
'5F38'	'48'	Non-Recoverable Part NRP ('0048' = 72 Byte)									

6.5 Gesamtübersicht CV-Zertifikatsprofil einer CVC-CA der Generation 1

Die folgende Tabelle fasst die zuvor beschriebenen Definitionen und Festlegungen zu den einzelnen Feldern der CV-Zertifikate einer CVC-CA übersichtlich zusammen, normativ sind jedoch nur die in Kapiteln 6.4.1 getroffenen Festlegungen:

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

Tabelle 59: Tab_PKI_263 Informationen für ein CV-Zertifikat einer CVC-CA

Element	Länge	Wert	Erläuterung
CPI	1 Byte	'21'	CPI eines CV-Zertifikats einer CVC-CA
Modulus	256 Byte		Modulus des öffentlichen Schlüssels. Die Länge des Modulus muss 28 Byte kleiner als die zu signierende Nachricht M sein.
Exponent	4 Byte		Exponent des öffentlichen Schlüssels
OID	7 Byte	'2B24 0304 0202 04'	Es wird lediglich der OID {1.3.36.3.4.2.2.4} verwendet

Element		Länge	Wert	Erläuterung
CHR		8 Byte		CAR der CVC-CA für die das CV-Zertifikat ausgestellt wird
	CA-Name	5 Byte	DEXXX	CA-Name gemäß Registrierung bei Fraunhofer SIT
	Service-Indikator	1 BCD	Individuell belegbar	
	CA-spez. Info	1 BCD	Nicht festgelegt	
	Algorithmen-Referenz	2 BCD	Individuell belegbar	Ggf. Unterscheidung diverser PuK-Algorithmen
	Datum	2 BCD	Letzte zwei Ziffern des Jahres der Schlüsselaktivierung	
CAR		8 Byte		CAR der CVC-CA, die das CV-Zertifikat ausstellt
	CA Name	5 Byte	DEXXX	Anbieterkennung gemäß Registrierung bei Fraunhofer SIT
	Service-Indikator	1 BCD	Individuell belegbar	
	CA-spez. Info	1 BCD	Nicht festgelegt	
	Algorithmen-Referenz	2 BCD	Individuell belegbar	Ggf. Unterscheidung diverser PuK-Algorithmen
	Datum	2 BCD	Letzte zwei Ziffern des Jahres der Schlüsselaktivierung	

6.6 Gesamtübersicht CV-Zertifikatsprofil einer Chipkarte der Generation 1

Die folgende Tabelle Tab_PKI_264 fasst die zuvor beschriebenen Definitionen und Festlegungen zu den einzelnen Feldern der CV-Zertifikate einer Karte der Generation 1 übersichtlich zusammen, normativ sind jedoch nur die in Kapiteln 6.4.1 getroffenen Festlegungen.

Tabelle 60: Tab_PKI_264 Informationen für ein CV-Zertifikat einer Karte

Datum	Länge	Wert	Erläuterung
CPI	1 Byte	'22'	CPI eines CV-Zertifikats einer Karte

Datum		Länge	Wert	Erläuterung
Modulus		256 Byte		Modulus des öffentlichen Schlüssels. Die Länge des Modulus muss 38 Byte kleiner als die zu signierende Nachricht M sein.
Exponent		4 Byte		Exponent des öffentlichen Schlüssels
OID		6 Byte	'2B24 0305 0204'	Es wird lediglich der OID {1.3.36.3.5.2.4} verwendet
CHA		7 Byte		Zertifikatsinhaber ist die Karte
	AID	6 Byte	'D27600004000'	AID der Gesundheitsanwendung
	Zugriffsprofil	1 Byte	'00'	Rollenprofil eGK
			'01'	Rollenprofil SM-B eKiosk
			'02'	Rollenprofil HBA/SM-B
			'03'	Rollenprofil HBA/SM-B
			'04'	Rollenprofil HBA/SM-B
			'05'	Rollenprofil (H)BA
			'06'	SMC
			'07'	Rollenprofil (H)BA
			'08'	Rollenprofil SM-B
			'09'	Rollenprofil SM-B
			'0A'	Rollenprofil SM-B.
			'33'	Geräteprofil gSMC-K
			'35'	Geräteprofil HBA
			'36'	Geräteprofil SM-B
			'37'	Geräteprofil SM-B
CHR		12 Byte		'xx xx' ICCSN der Karte
	Zuordnung Schlüsselpaar	2 Byte	'xx xx'	Zuordnung Schlüsselpaar zu CV-Zertifikat (Key Identifier)
	Major Industry Identifier	2 BCD	'80'	Gesundheitswesen
	Country Code	3 BCD	'276'	Germany
	Issuer Identifier	5 BCD		Kennung des Kartenherausgebers

Datum		Länge	Wert	Erläuterung
	Datum	10 BCD		Kartennummer
CAR		8 Byte		CAR der CVC-Root-CA, die das CV-Zertifikat ausstellt
	CA Name	5 Byte	DEXXX	Anbieterkennung gemäß Registrierung bei Fraunhofer SIT
	Service-Indikator	1 BCD	Individuell belegbar	
	CA-spez. Info	1 BCD	Nicht festgelegt	
	Algorithmen-Referenz	2 BCD	Individuell belegbar	Ggf. Unterscheidung diverser PuK-Algorithmen
	Datum	2 BCD	Letzte zwei Ziffern des Jahres der Schlüsselaktivierung	

6.7 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.

6.7.1 Berechtigung einer CVC-CA zur Zertifikatserstellung

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

- genau einen Kartentyp mit einem oder mehreren zugehörigen CV-Geräte-zertifikaten
- 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. ☒

6.7.2 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 6.7.3.1
- 2) Certification Authority Reference (CAR) gemäß 6.7.3.2
- 3) Öffentlicher Schlüssel: Die Abbildung des öffentlichen Schlüssels ändert sich gegenüber 6.4.1.6 aufgrund der Umstellung von RSA-basierten Schlüsseln (Darstellung von Modulus und öffentlichem Exponent) auf ELC-basierte 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 6.7.3.4
- 5) Certificate Holder Authorization Template (CHAT): Anders als bei Karten der Generation 1 wird die Rolle eines Zertifikatsinhabers nicht durch einen sieben Oktett langen String ausgedrückt, sondern gemäß [EN 14890-1#14.9.3.6] beschreibt eine Flagliste 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. (Objekt neu für G2)
- 7) Certificate Expiration Date (CXD): Dieses Datenobjekt enthält das Datum mit dem Gültigkeitsende des Zertifikates. (Objekt neu für G2)

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.

6.7.3 Zertifikatsprofil eines CV-Zertifikates für ELC-Schlüssel

Im Gegensatz zu 6.4.2 ist für ELC-Schlüssel 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.

6.7.3.1 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. ☒

6.7.3.2 Certification Authority Reference (CAR)

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

Tabelle 61: Tab_PKI_266 Aufbau CAR für Karten der Generation 2

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

6.7.3.3 Öffentlicher Schlüssel

Die hier folgenden Anforderungen sind 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 Objektidentifizier ODPuK 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 62: Tab_PKI_901 Objektidentifizier des öffentlichen Schlüssels eines CV-Zertifikats der Generation 2

Verwendungszweck des CV-Zertifikats	Domain-parameter	Objektidentifizier
Transport des öffentlichen	brainpoolP256r1	OID _{PuK} = '06-L ₀₆ -ecdsa-with-SHA256'

Signaturprüfsschlüssels einer CA		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 63: 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].

6.7.3.4 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. 

6.7.3.5 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 Objektidentifizier OIDflags gemäß Tabelle Tab_PKI_904 enthalten, der angibt, wie die Flags im zweiten Datenobjekt zu interpretieren sind. Die Umsetzung eines bestimmten Berechtigungsprofils MUSS durch die Kombination der Einzelflags gemäß TAB_PKI_918 erfolgen. 

Tabelle 64: Tab_PKI_904 Mögliche Objektidentifizier 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].


6.7.3.6 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. ☒

6.7.3.7 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. ☒

6.7.3.8 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 65: 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'
)

6.7.4 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 66: Tab_PKI_906 Signatur der Nachricht M eines CV-Zertifikats

Domainparameter des privaten Schlüssels PrK	Signaturformat
brainpoolP256r1	$(R, S) = \text{ECDSA}(PrK, \text{SHA_256}(M))$ im Format ecdsa-plain-SHA256 gemäß BSI-TR-03111#5.2.1.1
brainpoolP384r1	$(R, S) = \text{ECDSA}(PrK, \text{SHA_384}(M))$ im Format ecdsa-plain-SHA384 gemäß BSI-TR-03111#5.2.1.1
brainpoolP512r1	$(R, S) = \text{ECDSA}(PrK, \text{SHA_512}(M))$ 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 67: 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)

6.7.5 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.

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

Tabelle 68: Tab_PKI_912 CA CV-Zertifikate für 256 bit ELC-Schlüssel, insgesamt 220 Oktett

Tag	L	Wert																																																																		
'7F21'	'81D8'	CV-Zertifikat																																																																		
		<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'7F4E'</td><td>'8191'</td><td>Nachricht M</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'5F29'</td><td>'01'</td><td>CPI = '70'</td></tr> <tr> <td>'42'</td><td>'08'</td><td>CAR</td></tr> <tr> <td>'7F49'</td><td>'4D'</td><td>öffentlicher Schlüssel</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>'2A8648CE3D040302'</td></tr> <tr> <td>'86'</td><td>'41'</td><td>P2OS(Q, 32)</td></tr> </table> </td></tr> <tr> <td>'5F20'</td><td>'08'</td><td>CHR</td></tr> <tr> <td>'7F4C'</td><td>'13'</td><td>CHAT</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'xx...xx', Flagliste</td></tr> </table> </td></tr> <tr> <td>'5F25'</td><td>'06'</td><td>CED</td></tr> <tr> <td>'5F24'</td><td>'06'</td><td>CXD</td></tr> </table> </td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'5F37'</td><td>'40'</td><td>Signatur = R S</td></tr> </table> </td></tr> </table>	Tag	L	Wert	'7F4E'	'8191'	Nachricht M			<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'5F29'</td><td>'01'</td><td>CPI = '70'</td></tr> <tr> <td>'42'</td><td>'08'</td><td>CAR</td></tr> <tr> <td>'7F49'</td><td>'4D'</td><td>öffentlicher Schlüssel</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>'2A8648CE3D040302'</td></tr> <tr> <td>'86'</td><td>'41'</td><td>P2OS(Q, 32)</td></tr> </table> </td></tr> <tr> <td>'5F20'</td><td>'08'</td><td>CHR</td></tr> <tr> <td>'7F4C'</td><td>'13'</td><td>CHAT</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'xx...xx', Flagliste</td></tr> </table> </td></tr> <tr> <td>'5F25'</td><td>'06'</td><td>CED</td></tr> <tr> <td>'5F24'</td><td>'06'</td><td>CXD</td></tr> </table>	Tag	L	Wert	'5F29'	'01'	CPI = '70'	'42'	'08'	CAR	'7F49'	'4D'	öffentlicher Schlüssel			<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>'2A8648CE3D040302'</td></tr> <tr> <td>'86'</td><td>'41'</td><td>P2OS(Q, 32)</td></tr> </table>	Tag	L	Wert	'06'	'08'	'2A8648CE3D040302'	'86'	'41'	P2OS(Q, 32)	'5F20'	'08'	CHR	'7F4C'	'13'	CHAT			<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'xx...xx', Flagliste</td></tr> </table>	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			<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'5F37'</td><td>'40'</td><td>Signatur = R S</td></tr> </table>	Tag	L	Wert	'5F37'	'40'	Signatur = R S
Tag	L	Wert																																																																		
'7F4E'	'8191'	Nachricht M																																																																		
		<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'5F29'</td><td>'01'</td><td>CPI = '70'</td></tr> <tr> <td>'42'</td><td>'08'</td><td>CAR</td></tr> <tr> <td>'7F49'</td><td>'4D'</td><td>öffentlicher Schlüssel</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>'2A8648CE3D040302'</td></tr> <tr> <td>'86'</td><td>'41'</td><td>P2OS(Q, 32)</td></tr> </table> </td></tr> <tr> <td>'5F20'</td><td>'08'</td><td>CHR</td></tr> <tr> <td>'7F4C'</td><td>'13'</td><td>CHAT</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'xx...xx', Flagliste</td></tr> </table> </td></tr> <tr> <td>'5F25'</td><td>'06'</td><td>CED</td></tr> <tr> <td>'5F24'</td><td>'06'</td><td>CXD</td></tr> </table>	Tag	L	Wert	'5F29'	'01'	CPI = '70'	'42'	'08'	CAR	'7F49'	'4D'	öffentlicher Schlüssel			<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>'2A8648CE3D040302'</td></tr> <tr> <td>'86'</td><td>'41'</td><td>P2OS(Q, 32)</td></tr> </table>	Tag	L	Wert	'06'	'08'	'2A8648CE3D040302'	'86'	'41'	P2OS(Q, 32)	'5F20'	'08'	CHR	'7F4C'	'13'	CHAT			<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'xx...xx', Flagliste</td></tr> </table>	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																		
Tag	L	Wert																																																																		
'5F29'	'01'	CPI = '70'																																																																		
'42'	'08'	CAR																																																																		
'7F49'	'4D'	öffentlicher Schlüssel																																																																		
		<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>'2A8648CE3D040302'</td></tr> <tr> <td>'86'</td><td>'41'</td><td>P2OS(Q, 32)</td></tr> </table>	Tag	L	Wert	'06'	'08'	'2A8648CE3D040302'	'86'	'41'	P2OS(Q, 32)																																																									
Tag	L	Wert																																																																		
'06'	'08'	'2A8648CE3D040302'																																																																		
'86'	'41'	P2OS(Q, 32)																																																																		
'5F20'	'08'	CHR																																																																		
'7F4C'	'13'	CHAT																																																																		
		<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'xx...xx', Flagliste</td></tr> </table>	Tag	L	Wert	'06'	'08'	OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}	'53'	'07'	'xx...xx', Flagliste																																																									
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																																																																		
		<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'5F37'</td><td>'40'</td><td>Signatur = R S</td></tr> </table>	Tag	L	Wert	'5F37'	'40'	Signatur = R S																																																												
Tag	L	Wert																																																																		
'5F37'	'40'	Signatur = R S																																																																		

Tabelle 69: Tab_PKI_913 CA CV-Zertifikate für 384 bit ELC-Schlüssel, insgesamt 285 Oktett

Tag	L	Wert																																																												
'7F21'	'820118'	CV-Zertifikat																																																												
		<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'7F4E'</td><td>'81B1'</td><td>Nachricht <i>M</i></td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'5F29'</td><td>'01'</td><td>CPI = '70'</td></tr> <tr> <td>'42'</td><td>'08'</td><td>CAR</td></tr> <tr> <td>'7F49'</td><td>'6D'</td><td>öffentlicher Schlüssel</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>'2A8648CE3D040303'</td></tr> <tr> <td>'86'</td><td>'61'</td><td>P2OS(Q, 48)</td></tr> </table> </td></tr> <tr> <td>'5F20'</td><td>'08'</td><td>CHR</td></tr> <tr> <td>'7F4C'</td><td>'13'</td><td>CHAT</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'xx...xx', Flagliste</td></tr> <tr> <td>'5F25'</td><td>'06'</td><td>CED</td></tr> </table> </td></tr> <tr> <td>'5F24'</td><td>'06'</td><td>CXD</td></tr> <tr> <td>'5F37'</td><td>'60'</td><td>Signatur = <i>R</i> <i>S</i></td></tr> </table> </td></tr> </table>	Tag	L	Wert	'7F4E'	'81B1'	Nachricht <i>M</i>			<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'5F29'</td><td>'01'</td><td>CPI = '70'</td></tr> <tr> <td>'42'</td><td>'08'</td><td>CAR</td></tr> <tr> <td>'7F49'</td><td>'6D'</td><td>öffentlicher Schlüssel</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>'2A8648CE3D040303'</td></tr> <tr> <td>'86'</td><td>'61'</td><td>P2OS(Q, 48)</td></tr> </table> </td></tr> <tr> <td>'5F20'</td><td>'08'</td><td>CHR</td></tr> <tr> <td>'7F4C'</td><td>'13'</td><td>CHAT</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'xx...xx', Flagliste</td></tr> <tr> <td>'5F25'</td><td>'06'</td><td>CED</td></tr> </table> </td></tr> <tr> <td>'5F24'</td><td>'06'</td><td>CXD</td></tr> <tr> <td>'5F37'</td><td>'60'</td><td>Signatur = <i>R</i> <i>S</i></td></tr> </table>	Tag	L	Wert	'5F29'	'01'	CPI = '70'	'42'	'08'	CAR	'7F49'	'6D'	öffentlicher Schlüssel			<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>'2A8648CE3D040303'</td></tr> <tr> <td>'86'</td><td>'61'</td><td>P2OS(Q, 48)</td></tr> </table>	Tag	L	Wert	'06'	'08'	'2A8648CE3D040303'	'86'	'61'	P2OS(Q, 48)	'5F20'	'08'	CHR	'7F4C'	'13'	CHAT			<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'xx...xx', Flagliste</td></tr> <tr> <td>'5F25'</td><td>'06'</td><td>CED</td></tr> </table>	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 = <i>R</i> <i>S</i>
Tag	L	Wert																																																												
'7F4E'	'81B1'	Nachricht <i>M</i>																																																												
		<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'5F29'</td><td>'01'</td><td>CPI = '70'</td></tr> <tr> <td>'42'</td><td>'08'</td><td>CAR</td></tr> <tr> <td>'7F49'</td><td>'6D'</td><td>öffentlicher Schlüssel</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>'2A8648CE3D040303'</td></tr> <tr> <td>'86'</td><td>'61'</td><td>P2OS(Q, 48)</td></tr> </table> </td></tr> <tr> <td>'5F20'</td><td>'08'</td><td>CHR</td></tr> <tr> <td>'7F4C'</td><td>'13'</td><td>CHAT</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'xx...xx', Flagliste</td></tr> <tr> <td>'5F25'</td><td>'06'</td><td>CED</td></tr> </table> </td></tr> <tr> <td>'5F24'</td><td>'06'</td><td>CXD</td></tr> <tr> <td>'5F37'</td><td>'60'</td><td>Signatur = <i>R</i> <i>S</i></td></tr> </table>	Tag	L	Wert	'5F29'	'01'	CPI = '70'	'42'	'08'	CAR	'7F49'	'6D'	öffentlicher Schlüssel			<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>'2A8648CE3D040303'</td></tr> <tr> <td>'86'</td><td>'61'</td><td>P2OS(Q, 48)</td></tr> </table>	Tag	L	Wert	'06'	'08'	'2A8648CE3D040303'	'86'	'61'	P2OS(Q, 48)	'5F20'	'08'	CHR	'7F4C'	'13'	CHAT			<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'xx...xx', Flagliste</td></tr> <tr> <td>'5F25'</td><td>'06'</td><td>CED</td></tr> </table>	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 = <i>R</i> <i>S</i>									
Tag	L	Wert																																																												
'5F29'	'01'	CPI = '70'																																																												
'42'	'08'	CAR																																																												
'7F49'	'6D'	öffentlicher Schlüssel																																																												
		<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>'2A8648CE3D040303'</td></tr> <tr> <td>'86'</td><td>'61'</td><td>P2OS(Q, 48)</td></tr> </table>	Tag	L	Wert	'06'	'08'	'2A8648CE3D040303'	'86'	'61'	P2OS(Q, 48)																																																			
Tag	L	Wert																																																												
'06'	'08'	'2A8648CE3D040303'																																																												
'86'	'61'	P2OS(Q, 48)																																																												
'5F20'	'08'	CHR																																																												
'7F4C'	'13'	CHAT																																																												
		<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'xx...xx', Flagliste</td></tr> <tr> <td>'5F25'</td><td>'06'</td><td>CED</td></tr> </table>	Tag	L	Wert	'06'	'08'	OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}	'53'	'07'	'xx...xx', Flagliste	'5F25'	'06'	CED																																																
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 = <i>R</i> <i>S</i>																																																												

Tabelle 70: Tab_PKI_914 CA CV-Zertifikate für 512 bit ELC-Schlüssel, insgesamt 352 Oktett

Tag	L	Wert																																																												
'7F21'	'82015B'	CV-Zertifikat																																																												
		<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'7F4E'</td><td>'81D3'</td><td>Nachricht <i>M</i></td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'5F29'</td><td>'01'</td><td>CPI = '70'</td></tr> <tr> <td>'42'</td><td>'08'</td><td>CAR</td></tr> <tr> <td>'7F49'</td><td>'818E'</td><td>öffentlicher Schlüssel</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>'2A8648CE3D040304'</td></tr> <tr> <td>'86'</td><td>'8181'</td><td>P2OS(Q, 64)</td></tr> </table> </td></tr> <tr> <td>'5F20'</td><td>'08'</td><td>CHR</td></tr> <tr> <td>'7F4C'</td><td>'13'</td><td>CHAT</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'xx...xx', Flagliste</td></tr> <tr> <td>'5F25'</td><td>'06'</td><td>CED</td></tr> </table> </td></tr> <tr> <td>'5F24'</td><td>'06'</td><td>CXD</td></tr> <tr> <td>'5F37'</td><td>'8180'</td><td>Signatur = <i>R</i> <i>S</i></td></tr> </table> </td></tr> </table>	Tag	L	Wert	'7F4E'	'81D3'	Nachricht <i>M</i>			<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'5F29'</td><td>'01'</td><td>CPI = '70'</td></tr> <tr> <td>'42'</td><td>'08'</td><td>CAR</td></tr> <tr> <td>'7F49'</td><td>'818E'</td><td>öffentlicher Schlüssel</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>'2A8648CE3D040304'</td></tr> <tr> <td>'86'</td><td>'8181'</td><td>P2OS(Q, 64)</td></tr> </table> </td></tr> <tr> <td>'5F20'</td><td>'08'</td><td>CHR</td></tr> <tr> <td>'7F4C'</td><td>'13'</td><td>CHAT</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'xx...xx', Flagliste</td></tr> <tr> <td>'5F25'</td><td>'06'</td><td>CED</td></tr> </table> </td></tr> <tr> <td>'5F24'</td><td>'06'</td><td>CXD</td></tr> <tr> <td>'5F37'</td><td>'8180'</td><td>Signatur = <i>R</i> <i>S</i></td></tr> </table>	Tag	L	Wert	'5F29'	'01'	CPI = '70'	'42'	'08'	CAR	'7F49'	'818E'	öffentlicher Schlüssel			<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>'2A8648CE3D040304'</td></tr> <tr> <td>'86'</td><td>'8181'</td><td>P2OS(Q, 64)</td></tr> </table>	Tag	L	Wert	'06'	'08'	'2A8648CE3D040304'	'86'	'8181'	P2OS(Q, 64)	'5F20'	'08'	CHR	'7F4C'	'13'	CHAT			<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'xx...xx', Flagliste</td></tr> <tr> <td>'5F25'</td><td>'06'</td><td>CED</td></tr> </table>	Tag	L	Wert	'06'	'08'	OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}	'53'	'07'	'xx...xx', Flagliste	'5F25'	'06'	CED	'5F24'	'06'	CXD	'5F37'	'8180'	Signatur = <i>R</i> <i>S</i>
Tag	L	Wert																																																												
'7F4E'	'81D3'	Nachricht <i>M</i>																																																												
		<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'5F29'</td><td>'01'</td><td>CPI = '70'</td></tr> <tr> <td>'42'</td><td>'08'</td><td>CAR</td></tr> <tr> <td>'7F49'</td><td>'818E'</td><td>öffentlicher Schlüssel</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>'2A8648CE3D040304'</td></tr> <tr> <td>'86'</td><td>'8181'</td><td>P2OS(Q, 64)</td></tr> </table> </td></tr> <tr> <td>'5F20'</td><td>'08'</td><td>CHR</td></tr> <tr> <td>'7F4C'</td><td>'13'</td><td>CHAT</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'xx...xx', Flagliste</td></tr> <tr> <td>'5F25'</td><td>'06'</td><td>CED</td></tr> </table> </td></tr> <tr> <td>'5F24'</td><td>'06'</td><td>CXD</td></tr> <tr> <td>'5F37'</td><td>'8180'</td><td>Signatur = <i>R</i> <i>S</i></td></tr> </table>	Tag	L	Wert	'5F29'	'01'	CPI = '70'	'42'	'08'	CAR	'7F49'	'818E'	öffentlicher Schlüssel			<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>'2A8648CE3D040304'</td></tr> <tr> <td>'86'</td><td>'8181'</td><td>P2OS(Q, 64)</td></tr> </table>	Tag	L	Wert	'06'	'08'	'2A8648CE3D040304'	'86'	'8181'	P2OS(Q, 64)	'5F20'	'08'	CHR	'7F4C'	'13'	CHAT			<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'xx...xx', Flagliste</td></tr> <tr> <td>'5F25'</td><td>'06'</td><td>CED</td></tr> </table>	Tag	L	Wert	'06'	'08'	OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}	'53'	'07'	'xx...xx', Flagliste	'5F25'	'06'	CED	'5F24'	'06'	CXD	'5F37'	'8180'	Signatur = <i>R</i> <i>S</i>									
Tag	L	Wert																																																												
'5F29'	'01'	CPI = '70'																																																												
'42'	'08'	CAR																																																												
'7F49'	'818E'	öffentlicher Schlüssel																																																												
		<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>'2A8648CE3D040304'</td></tr> <tr> <td>'86'</td><td>'8181'</td><td>P2OS(Q, 64)</td></tr> </table>	Tag	L	Wert	'06'	'08'	'2A8648CE3D040304'	'86'	'8181'	P2OS(Q, 64)																																																			
Tag	L	Wert																																																												
'06'	'08'	'2A8648CE3D040304'																																																												
'86'	'8181'	P2OS(Q, 64)																																																												
'5F20'	'08'	CHR																																																												
'7F4C'	'13'	CHAT																																																												
		<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'xx...xx', Flagliste</td></tr> <tr> <td>'5F25'</td><td>'06'</td><td>CED</td></tr> </table>	Tag	L	Wert	'06'	'08'	OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}	'53'	'07'	'xx...xx', Flagliste	'5F25'	'06'	CED																																																
Tag	L	Wert																																																												
'06'	'08'	OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}																																																												
'53'	'07'	'xx...xx', Flagliste																																																												
'5F25'	'06'	CED																																																												
'5F24'	'06'	CXD																																																												
'5F37'	'8180'	Signatur = <i>R</i> <i>S</i>																																																												

6.7.5.2 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 71: Tab_PKI_937 Cross-CV-Zertifikat für ELC-Schlüssel

Tag	L	Wert																																																												
'7F21'	*	CV-Zertifikat																																																												
		<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'7F4E'</td><td>*</td><td>Nachricht <i>M</i></td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'5F29'</td><td>'01'</td><td>CPI = '70'</td></tr> <tr> <td>'42'</td><td>'08'</td><td>CAR</td></tr> <tr> <td>'7F49'</td><td>*</td><td>öffentlicher Schlüssel</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>*</td></tr> <tr> <td>'86'</td><td>*</td><td>*</td></tr> </table> </td></tr> <tr> <td>'5F20'</td><td>'08'</td><td>CHR</td></tr> <tr> <td>'7F4C'</td><td>'13'</td><td>CHAT</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID = oid_cvc_fl_ti</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'FF FFFF FFFF FFFF'</td></tr> </table> </td></tr> <tr> <td>'5F25'</td><td>'06'</td><td>CED</td></tr> <tr> <td>'5F24'</td><td>'06'</td><td>CXD</td></tr> <tr> <td>'5F37'</td><td>*</td><td>Signatur = <i>R</i> <i>S</i></td></tr> </table> </td></tr> </table>	Tag	L	Wert	'7F4E'	*	Nachricht <i>M</i>			<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'5F29'</td><td>'01'</td><td>CPI = '70'</td></tr> <tr> <td>'42'</td><td>'08'</td><td>CAR</td></tr> <tr> <td>'7F49'</td><td>*</td><td>öffentlicher Schlüssel</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>*</td></tr> <tr> <td>'86'</td><td>*</td><td>*</td></tr> </table> </td></tr> <tr> <td>'5F20'</td><td>'08'</td><td>CHR</td></tr> <tr> <td>'7F4C'</td><td>'13'</td><td>CHAT</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID = oid_cvc_fl_ti</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'FF FFFF FFFF FFFF'</td></tr> </table> </td></tr> <tr> <td>'5F25'</td><td>'06'</td><td>CED</td></tr> <tr> <td>'5F24'</td><td>'06'</td><td>CXD</td></tr> <tr> <td>'5F37'</td><td>*</td><td>Signatur = <i>R</i> <i>S</i></td></tr> </table>	Tag	L	Wert	'5F29'	'01'	CPI = '70'	'42'	'08'	CAR	'7F49'	*	öffentlicher Schlüssel			<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>*</td></tr> <tr> <td>'86'</td><td>*</td><td>*</td></tr> </table>	Tag	L	Wert	'06'	'08'	*	'86'	*	*	'5F20'	'08'	CHR	'7F4C'	'13'	CHAT			<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID = oid_cvc_fl_ti</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'FF FFFF FFFF FFFF'</td></tr> </table>	Tag	L	Wert	'06'	'08'	OID = oid_cvc_fl_ti	'53'	'07'	'FF FFFF FFFF FFFF'	'5F25'	'06'	CED	'5F24'	'06'	CXD	'5F37'	*	Signatur = <i>R</i> <i>S</i>
Tag	L	Wert																																																												
'7F4E'	*	Nachricht <i>M</i>																																																												
		<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'5F29'</td><td>'01'</td><td>CPI = '70'</td></tr> <tr> <td>'42'</td><td>'08'</td><td>CAR</td></tr> <tr> <td>'7F49'</td><td>*</td><td>öffentlicher Schlüssel</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>*</td></tr> <tr> <td>'86'</td><td>*</td><td>*</td></tr> </table> </td></tr> <tr> <td>'5F20'</td><td>'08'</td><td>CHR</td></tr> <tr> <td>'7F4C'</td><td>'13'</td><td>CHAT</td></tr> <tr> <td></td><td></td><td> <table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID = oid_cvc_fl_ti</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'FF FFFF FFFF FFFF'</td></tr> </table> </td></tr> <tr> <td>'5F25'</td><td>'06'</td><td>CED</td></tr> <tr> <td>'5F24'</td><td>'06'</td><td>CXD</td></tr> <tr> <td>'5F37'</td><td>*</td><td>Signatur = <i>R</i> <i>S</i></td></tr> </table>	Tag	L	Wert	'5F29'	'01'	CPI = '70'	'42'	'08'	CAR	'7F49'	*	öffentlicher Schlüssel			<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>*</td></tr> <tr> <td>'86'</td><td>*</td><td>*</td></tr> </table>	Tag	L	Wert	'06'	'08'	*	'86'	*	*	'5F20'	'08'	CHR	'7F4C'	'13'	CHAT			<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID = oid_cvc_fl_ti</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'FF FFFF FFFF FFFF'</td></tr> </table>	Tag	L	Wert	'06'	'08'	OID = oid_cvc_fl_ti	'53'	'07'	'FF FFFF FFFF FFFF'	'5F25'	'06'	CED	'5F24'	'06'	CXD	'5F37'	*	Signatur = <i>R</i> <i>S</i>									
Tag	L	Wert																																																												
'5F29'	'01'	CPI = '70'																																																												
'42'	'08'	CAR																																																												
'7F49'	*	öffentlicher Schlüssel																																																												
		<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>*</td></tr> <tr> <td>'86'</td><td>*</td><td>*</td></tr> </table>	Tag	L	Wert	'06'	'08'	*	'86'	*	*																																																			
Tag	L	Wert																																																												
'06'	'08'	*																																																												
'86'	*	*																																																												
'5F20'	'08'	CHR																																																												
'7F4C'	'13'	CHAT																																																												
		<table> <tr> <th>Tag</th><th>L</th><th>Wert</th></tr> <tr> <td>'06'</td><td>'08'</td><td>OID = oid_cvc_fl_ti</td></tr> <tr> <td>'53'</td><td>'07'</td><td>'FF FFFF FFFF FFFF'</td></tr> </table>	Tag	L	Wert	'06'	'08'	OID = oid_cvc_fl_ti	'53'	'07'	'FF FFFF FFFF FFFF'																																																			
Tag	L	Wert																																																												
'06'	'08'	OID = oid_cvc_fl_ti																																																												
'53'	'07'	'FF FFFF FFFF FFFF'																																																												
'5F25'	'06'	CED																																																												
'5F24'	'06'	CXD																																																												
'5F37'	*	Signatur = <i>R</i> <i>S</i>																																																												

Anmerkung: Die mit * gefüllten Feldinhalte müssen anhand der in 6.7.5.1 spezifizierten Zertifikatsprofile für 256/384/512 bit ELC-Schlüssel ermittelt bzw. berechnet werden.

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

Tabelle 72: Tab_PKI_915 Endnutzer-CV-Zertifikate für 256 bit ELC-Schlüssel, insgesamt 222 Oktett

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

Tabelle 73: Tab_PKI_916 Endnutzer-CV-Zertifikate für 384 bit ELC-Schlüssel, insgesamt 287 Oktett

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

Tabelle 74: 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 <i>M</i>
	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 = <i>R</i> <i>S</i>

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

6.7.6 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 gelöscht Bit an, dass auch nach einer erfolgreichen Authentisierung die zugehörige Aktion nicht freigeschaltet ist.

Tabelle 75: 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

Bitnummer	Bedeutung
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

Bitnummer	Bedeutung
b55	SAK für Stapel- oder Komfortsignatur

Hinweis: Die CV-Zertifikate der Generation 1 verwenden Rollenkennungen, während in der Generation 2 Flaglisten verwendet werden. Tabelle 71 zeigt korrespondierende Werte.

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 76: Tab_PKI_918 Abbildung von Rollenberechtigungen auf äquivalente Flaglisten

Zugriffsprofil	CHA-Wert (G1)	CHAT-Wert / Flagliste (G2)
Rolle (AUTR_CVC)	0	´D276 0000 4000 00´
	1	´D276 0000 4000 01´
	2A Ärztin/Arzt Fachliche Institution des Arztes Krankenhaus	´D276 0000 4000 02´
	2ZA Zahnärztin/Zahnarzt Fachliche Institution des Zahnarztes	´D276 0000 4000 02´
	3	´D276 0000 4000 03´
	4	´D276 0000 4000 04´
	5	´D276 0000 4000 05´
	6	wird nicht verwendet
	7	´D276 0000 4000 07´
	8	´D276 0000 4000 08´
	9	´D276 0000 4000 09´
	10	´D276 0000 4000 0A´
		´00 AE1A CDC1 DC00´
Gerät (AUTD_CVC)	51	wird nicht verwendet
	53	wird nicht verwendet
	54	wird nicht verwendet
	55	wird nicht verwendet
Administration (AUT_CVC)	0	wird nicht verwendet
		´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 CHA.2ZA des Rollen-Zertifikates lautet ´00 5D20 DAA0 8300´.
Die Flagliste für das Profil CHA.53 des Geräte-Zertifikates lautet ´00 0000 0000 000C´.
Die Kombination, bzw. Veroderung der beiden Flaglisten ergibt ´00 5D20 DAA0 8300-830C´.

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 77: 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	CHA.0	ˆ80000000000000ˆ
gSMC-K / CHA.51	-	ˆ800000000000001ˆ
gSMC-KT / CHA.54	-	ˆ800000000000002ˆ
HBA / CHA.53	CHA.2A	ˆ805D29DAA0BB0Cˆ
HBA / CHA.53	CHA.2ZA	ˆ805D20DAA0830Cˆ
HBA / CHA.53	CHA.3	ˆ805C40DAA0830Cˆ
HBA / CHA.53	CHA.4	ˆ804C40DAA0820Cˆ
HBA / CHA.53	CHA.5	ˆ805C0002A0000Cˆ
HBA / CHA.53	CHA.7	ˆ8000200480000Cˆ
SMC-B / CHA.55	CHA.1	ˆ80AE1ACDC1DC04ˆ
SMC-B / CHA.55	CHA.2A	ˆ805D29DAA0BB04ˆ
SMC-B / CHA.55	CHA.2ZA	ˆ805D20DAA08304ˆ
SMC-B / CHA.55	CHA.3	ˆ805C40DAA08304ˆ
SMC-B / CHA.55	CHA.4	ˆ804C40DAA08204ˆ
SMC-B / CHA.55	CHA.8	ˆ80400002A00004ˆ
SMC-B / CHA.55	CHA.9	ˆ8068000AA00004ˆ
SMC-B / CHA.55	CHA.10	ˆ80AF5ACDC1DF04ˆ
CHAT-Wert / Flagliste für kombinierte Zugriffsprofile		
eGK	CHA.0	-
gSMC-K und gSMC-KT / CHA.51 & 54	-	ˆ800000000000003ˆ
HBA und SMC-B / CHA.53 & 55	CHA.1 - 5 & 7- 940	ˆ80FF7BDFE1FF0Cˆ

Tabelle 78: 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 bildet den Vertrauensanker für die TI.
- Die TSL stellt (i. S. einer Whitelist) den Vertrauensraum für die in der TI zugelassenen Aussteller-CA.
- nonQES-Aussteller-CA-Zertifikate werden ausschließlich gegen die TSL geprüft
- QES-Aussteller-CA-Zertifikate werden
 - (a) hinsichtlich ihrer Zulassung in der TI gegen die TSL und
 - (b) hinsichtlich ihres VDA Qualifikationsstatus gemäß [eIDAS] gegen die BNetzA-VL geprüft.
- 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.

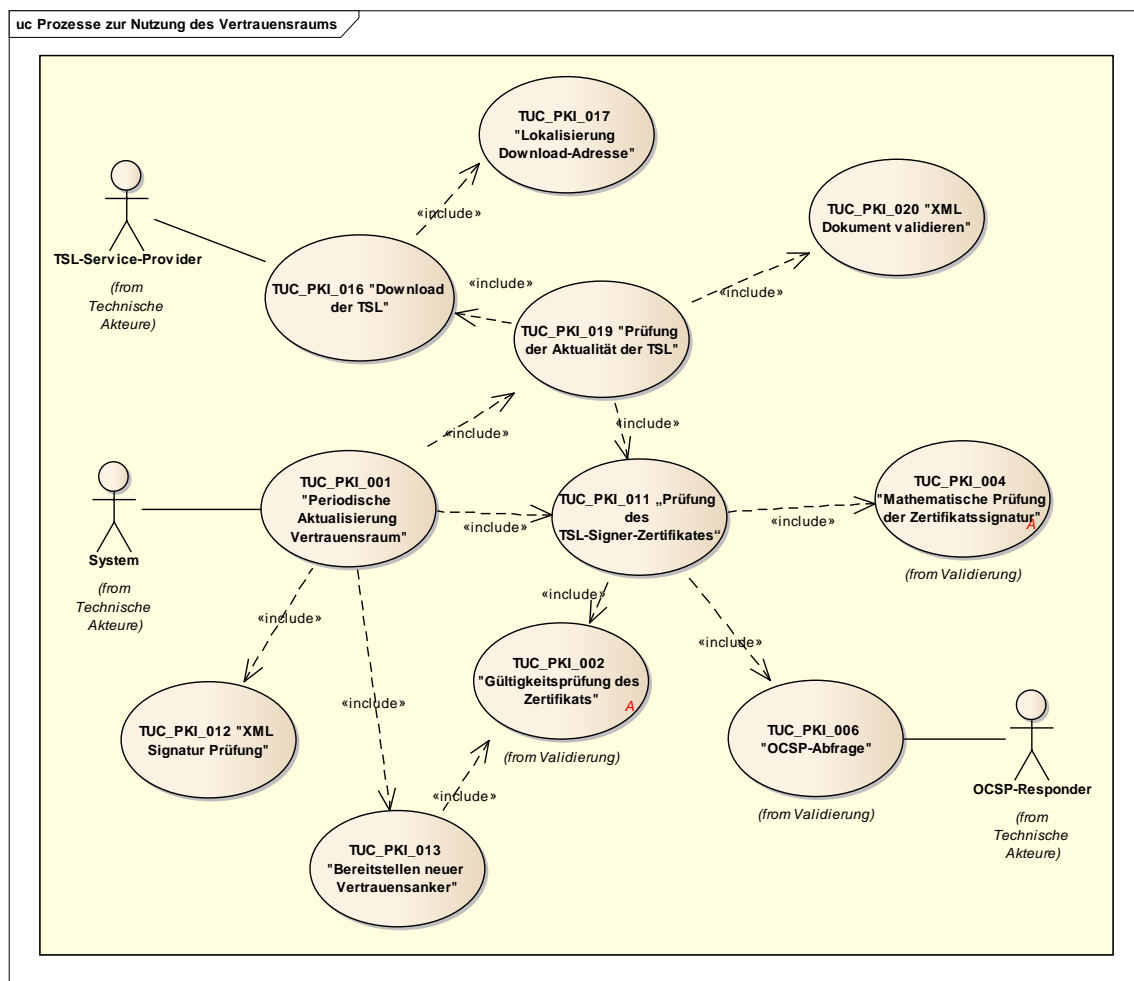


Abbildung 5: Use Case Diagramm „Prozesse zur Nutzung des TI-Vertrauensraums“

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 verletzen 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.

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

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].

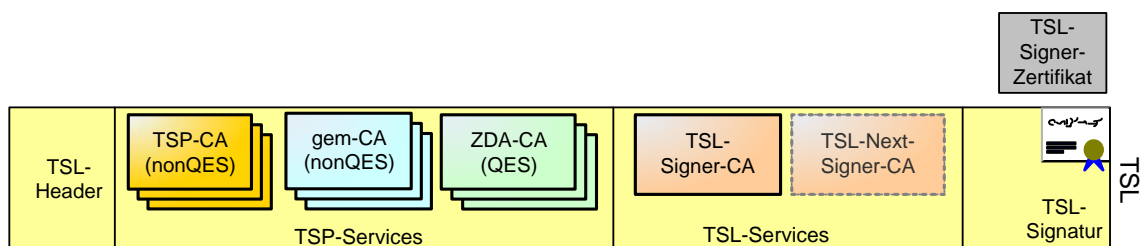


Abbildung 6: Aufbau der TSL

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
- 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 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.

☒ **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. ☒

☒ **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. ☒

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 „StatusStartTime“ an,

- seit wann ein Zertifikat dem aktuellen TI-X.509-Vertrauensraum angehört (mit „*inaccord*“ markiert), oder

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

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 79: 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 CVC-Root-CA DNSSEC-Trust-Anchor BNetzA-VL-Signer	Der Dienst ist für die TI zugelassen und ist in Betrieb.
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.

8.1.1.1 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 80: TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“

Element	Beschreibung
Name	TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“
Beschreibung	<p>Dieser Use Case beschreibt den gesamten Ablauf zur periodischen Aktualisierung des TI-Vertrauensraumes mittels einer TSL-Datei. Dabei verwendet er weitere TUCs, die im Laufe des Kapitels detailliert spezifiziert werden</p> <p>Ein Offline-Modus ist zu berücksichtigen für</p> <ul style="list-style-type: none"> a) das Mobile-Kartenterminal b) Konnektor ohne Anbindung an die TI <p>Beide verfügen nicht über die automatischen Online-Möglichkeiten zum Bezug von Statusinformationen oder TSL-Aktualisierungen aus der TI.</p>
Anwendungsumfeld	System, das die TSL auswertet
Auslöser	<p>Produkttypspezifischer Trigger</p> <p>Zeitpunkt MUSS durch Facharchitekturen vorgegeben werden. (Standardmäßig ist eine tägliche Prüfung der Aktualität vorzusehen.)</p>
Eingangsdaten	<ul style="list-style-type: none"> • TSL im System • Neu eingebrachte TSL-Datei (optional) • OCSP-Graceperiod (legt bei der Verwendung von gecachten OCSP-Antworten den maximal zulässigen Zeitraum fest, den die Systemzeit der prüfenden Komponente noch nach dem Zeitpunkt der OCSP-Antwort liegen darf) • Flag für Offline-Modus (Im Offline-Fall kann keine Sperrstatusprüfung des TSL-Signer-Zertifikates durchgeführt werden.)
Komponenten	System, TSL-Download-Punkt, OCSP-Responder
Ausgangsdaten	Status der Initialisierung
Referenzen	[ETSI_TS_102_231]
Standardablauf	<ol style="list-style-type: none"> 1. [System:] System startet die Initialisierung des TI-Vertrauensraums. 2. [System:] Die TSL im System wird auf Aktualität geprüft (TUC_PKI_019 „Prüfung der Aktualität der TSL“). Diese Prüfung erfolgt gegen die neu eingebrachte TSL-Datei als Eingangsparameter. (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") (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.

Element	Beschreibung
	<p>[System:] Es wird ermittelt, ob in der neuen TSL ein neuer TI-Vertrauensanker vorliegt (TUC_PKI_013 „Import TI-Vertrauensanker aus TSL“).</p> <p>6.</p> <p>[System:] Aus den CA-Zertifikaten aus der neuen TSL wird der neue TI-Vertrauensraum gebildet. Dazu werden sie aus der TSL-Datei extrahiert, z. B. in einen System-eigenen Truststore gespeichert und dem System bereitgestellt.</p> <p>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.</p> <p>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.</p> <p>Die Form des Truststore wird nicht näher spezifiziert, dieser muss nur den gestellten Anforderungen (z. B. bezüglich Sicherheit oder Performance) genügen.</p> <p>Das System muss den TI-Vertrauensraum mit den in der TSL als vertrauenswürdig bezeichneten CA-Zertifikaten gemäß Tab_PKI_271 „Erlaubte Inhalte des TSL-Elements ServiceStatus“ befüllen.</p> <p>7.</p> <p>[System:] Der Truststore wird für Zertifikatsprüfung (wieder) bereitgestellt.</p> <p>8.</p> <p>[System:] Ende des Use Case</p>
Varianten/Alternativen	<p>Der Standardablauf stellt die Prüfungen dar, die vollzogen werden müssen. Eine Trennung in zwei Prozesse oder eine Umstrukturierung, bei der alle notwendigen Prüfungen erfolgen, ist zulässig.</p> <p>Im Falle einer aktuellen TSL im System endet der Ablauf nach Schritt 2:</p> <p>2a.</p> <p>[System:] TSL aus Download ist gleich TSL im System; und TSL ist noch gültig.</p> <p>2a.1</p> <p>[System:] Ende des Use Case</p> <p>3a.</p> <p>[System:] Wenn das Offline-Flag gesetzt ist (offline==true), dann wird mit Schritt 5 weitergefahren. (Im Offline-Fall kann keine OCSP-Abfrage stattfinden.)</p>
Fehlerfälle/Warnung	<p>Ein Fehlerfall ist, dass dem System keine gültige TSL vorliegt :</p> <p>1a.</p> <p>[System:] Es ist keine TSL im System vorhanden. Abbruch mit Fehlermeldung (TSL_INIT_ERROR)</p> <p>2b.</p> <p>[System:] Der TUC_PKI_019 wirft eine VALIDITY_WARNING_2. VALIDITY_WARNING_2 wird als Fehlermeldung ausgegeben. Die weitere Fehlerbehandlung erfolgt unter Beachtung von [GS-A_5336].</p> <p>3b.</p> <p>[System:] Das TSL-Signer-Zertifikat lässt sich nicht aus der TSL-Datei extrahieren (TSL_CERT_EXTRACTION_ERROR).</p> <p>6a.</p> <p>[System:] Abbruch mit Fehlermeldung (TSL_CERT_EXTRACTION_ERROR)</p> <p>Weitere Fehlerfälle sind in den jeweiligen referenzierten TUCs</p>

Element	Beschreibung
	beschrieben.
Technische Fehlermeldung	Es ist keine TSL im System vorhanden. Zertifikat(e) lässt/lassen sich nicht extrahieren. Weitere technische Fehlermeldungen 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 ServiceTypenidentifizier „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.
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_001 "Periodische Aktualisierung TI-Vertrauensraum"

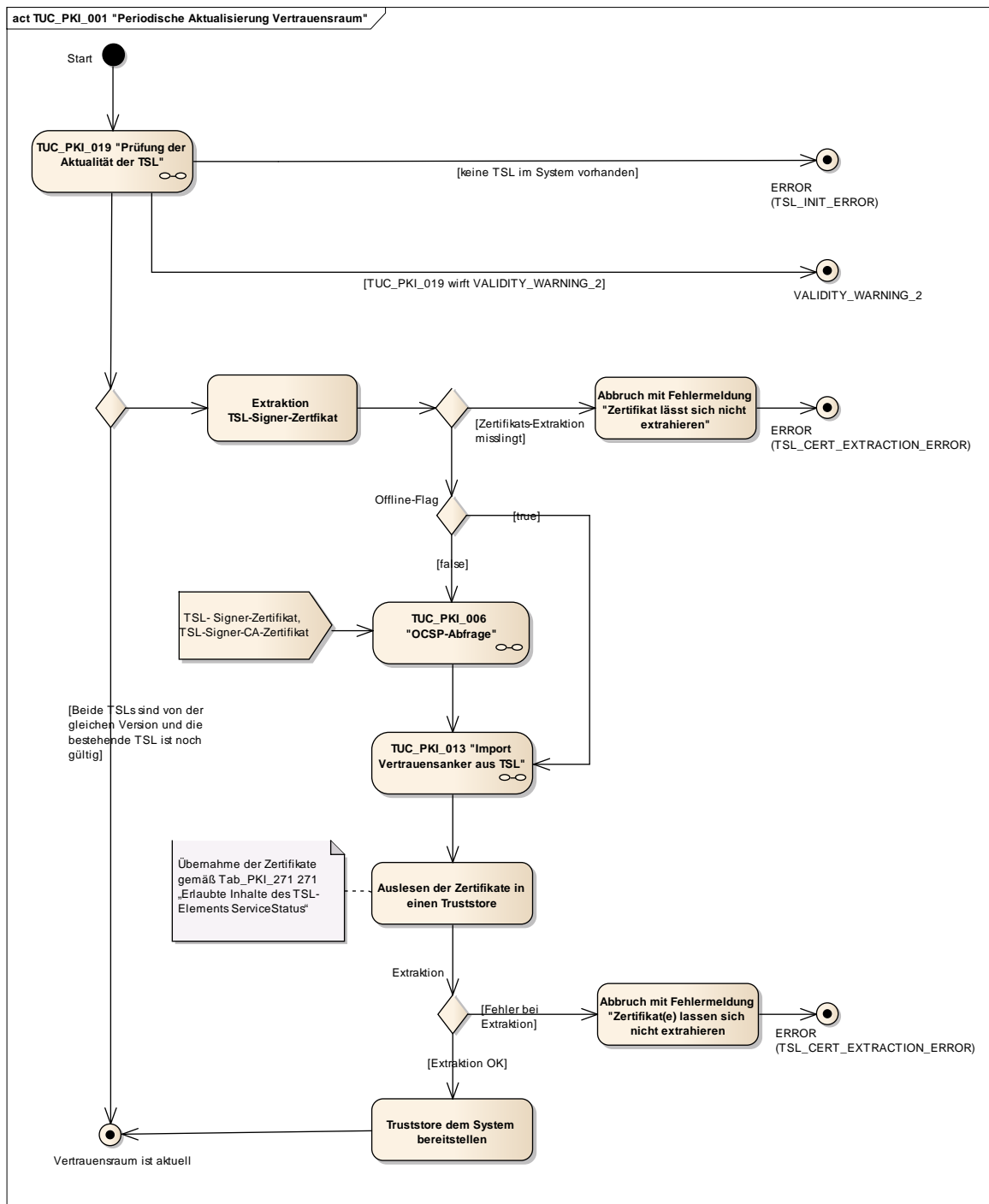


Abbildung 7: Aktivitätsdiagramm TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“

8.1.2 Geplanter Wechsel TI-Vertrauensanker

8.1.2.1 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 81: 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	<ol style="list-style-type: none"> 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 ServiceTypeldentifizier-URI. Zusätzlich kann auch der in GS-A_4644 angegebene OID in der ServiceInformationExtension auf korrekte Belegung geprüft werden. Siehe gemäß Kapitel 8.1.2.2. 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

Element	Beschreibung
	<p>„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</p>
Varianten/Alternativen	<p>1a. [System:] Es wird kein als neuer TI-Vertrauensanker markiertes CA-Zertifikat gefunden und der Use Case wird beendet.</p>
Fehlerfälle	<p>Ein Abbruch des TUC führt nur dazu, dass kein neuer TI-Vertrauensanker abgelegt wird. Er hat keinen Einfluss auf die Gültigkeit des bestehenden TI-Vertrauensankers oder auf die anderen Schritte der TSL-Aktualisierung. Das System muss dies jedoch protokollieren.</p> <p>1b. [System:] Es wird mehr als ein markiertes CA-Zertifikat gefunden. (MULTIPLE_TRUST_ANCHOR)</p> <p>2b. [System:] Das TSL-Signer-CA-Zertifikat lässt sich nicht aus der TSL extrahieren. (TSL_SIG_CERT_EXTRACTION_ERROR)</p>
Technische Fehlermeldung	<p>Zertifikat lässt sich nicht extrahieren. Das System meldet entsprechende Fehlercodes. Weitere technische Fehlermeldungen sind in den jeweiligen referenzierten TUCs beschrieben.</p>
Sicherheitsanforderungen	<p>Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.</p>
Anmerkungen	<p>Der Prozess wird unabhängig davon durchlaufen, ob schon ein zukünftiger TI-Vertrauensanker vorliegt oder nicht. Es ist immer nur der zuletzt angekündigte zukünftige TI-Vertrauensanker gültig. Ältere Ankündigungen müssen überschrieben werden. Die Gestaltung des sicheren Speichers des Systems ist durch den Betreiber/Implementierer des Systems zu definieren.</p>
Zugehörige Diagramme	<p>Aktivitätsdiagramm TUC_PKI_013 "Import neuer TI-Vertrauensanker"</p>

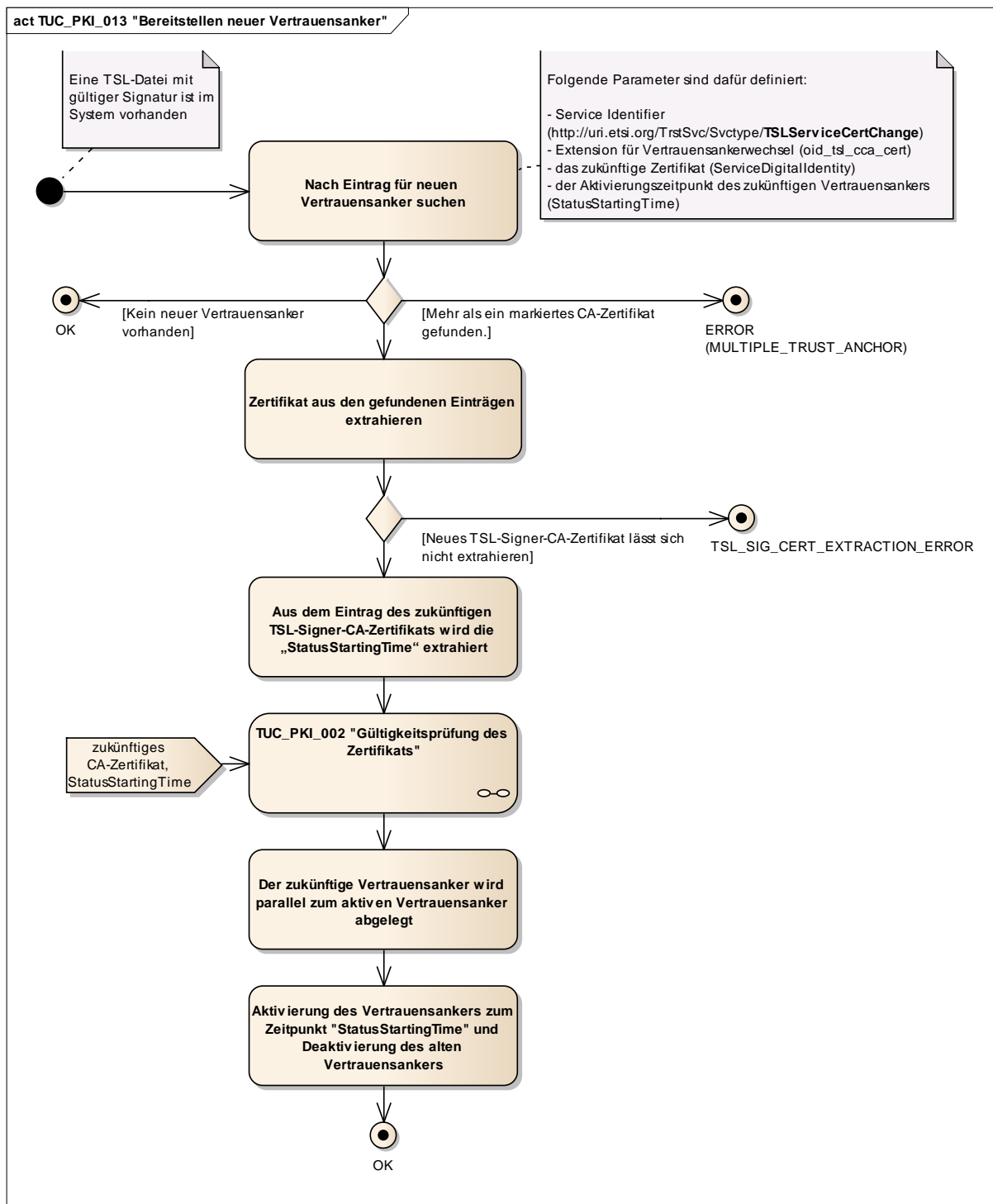


Abbildung 8: Aktivitätsdiagramm TUC_PKI_013 „Import neuer TI-Vertrauensanker“

8.1.2.2 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 82: 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 83: 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.

8.1.2.3 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. ☒

8.1.3 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 84: 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

Element	Beschreibung
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)
Technische Fehlermeldung	Download der TSL nicht möglich Das System meldet entsprechende Fehlercodes.
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"

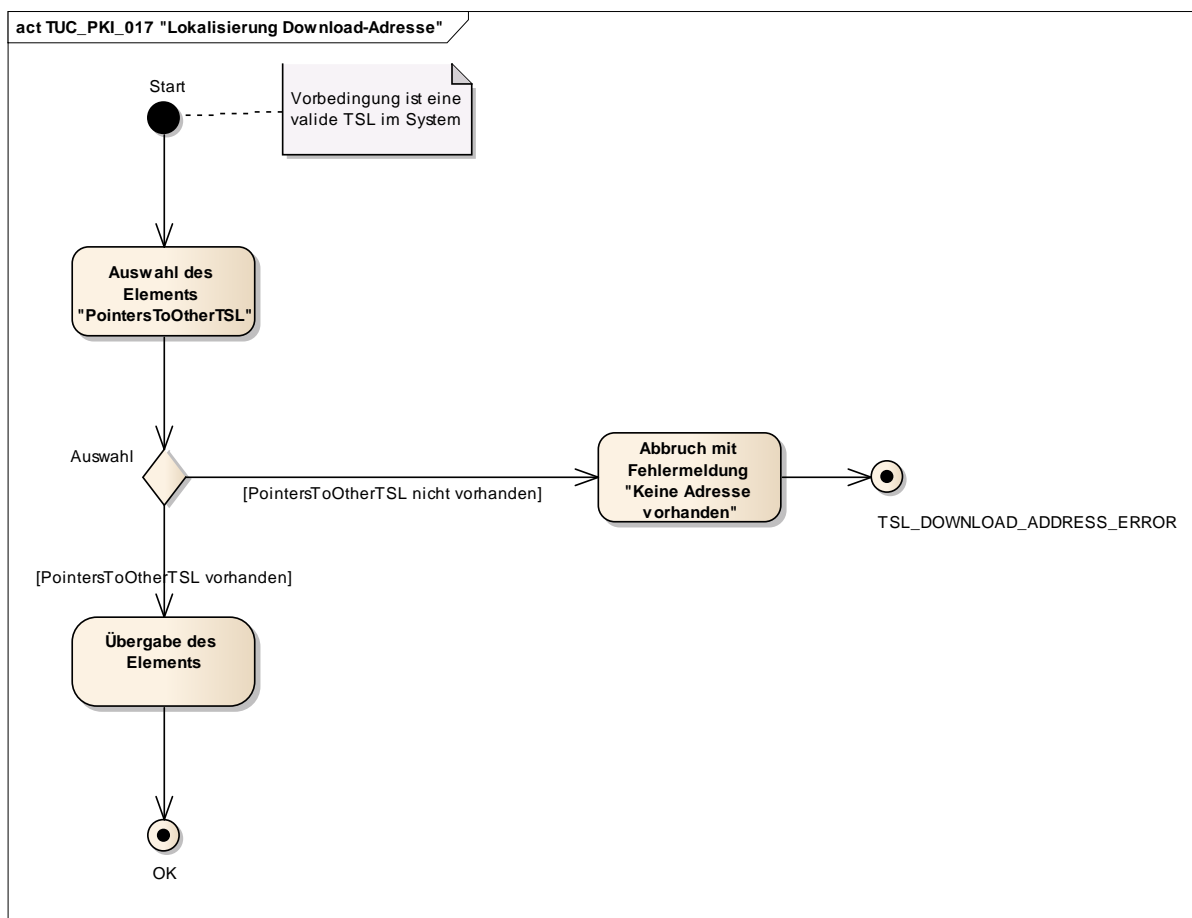


Abbildung 9: Aktivitätsdiagramm TUC_PKI_017 „Lokalisierung Download-Adresse“

Tabelle 85: 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.

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 86: 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.

Element	Beschreibung
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 Downloadadresse (TUC_PKI_017 „Lokalisierung TSL Download-Adressen“) 3. [System:] Auswahl der Primär-Download-Adresse gemäß Tab_PKI_272 aus dem Element „PointersToOtherTSL“ 4. [System:] Download der TSL-Datei. 5. [System:] Ende des Use Case mit entsprechender Rückmeldung
Varianten/Alternativen	4a. [System:] Bei Fehlern wird ein einfaches Fehlerhandling angestoßen. 4a.1 [System:] Wiederholung des Downloads. Der Download von der Primär-Download-Adresse wird dreimal wiederholt. Konnte die TSL dabei nicht erfolgreich geladen werden, erfolgt die Ausführung von 4a.2. 4a.2 [System:] Wechsel auf die Backup-Adresse gemäß Tab_PKI_272. Bei Fehlern wird auch dieser Download wiederholt. Die Wiederholung erfolgt dreimal.
Fehlerfälle	5a. [System:] Sollte der wiederholte Download über keine der Adressen erfolgreich sein, meldet das System einen Fehler und es werden für den Moment keine weiteren Download-Versuche mehr unternommen. (TSL_DOWNLOAD_ERROR)
Technische Fehlermeldung	Download der TSL nicht möglich Das System meldet entsprechende Fehlercodes Weitere technische Fehlermeldungen sind in den jeweiligen referenzierten TUCs beschrieben.
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_016 "Download der TSL-Datei"

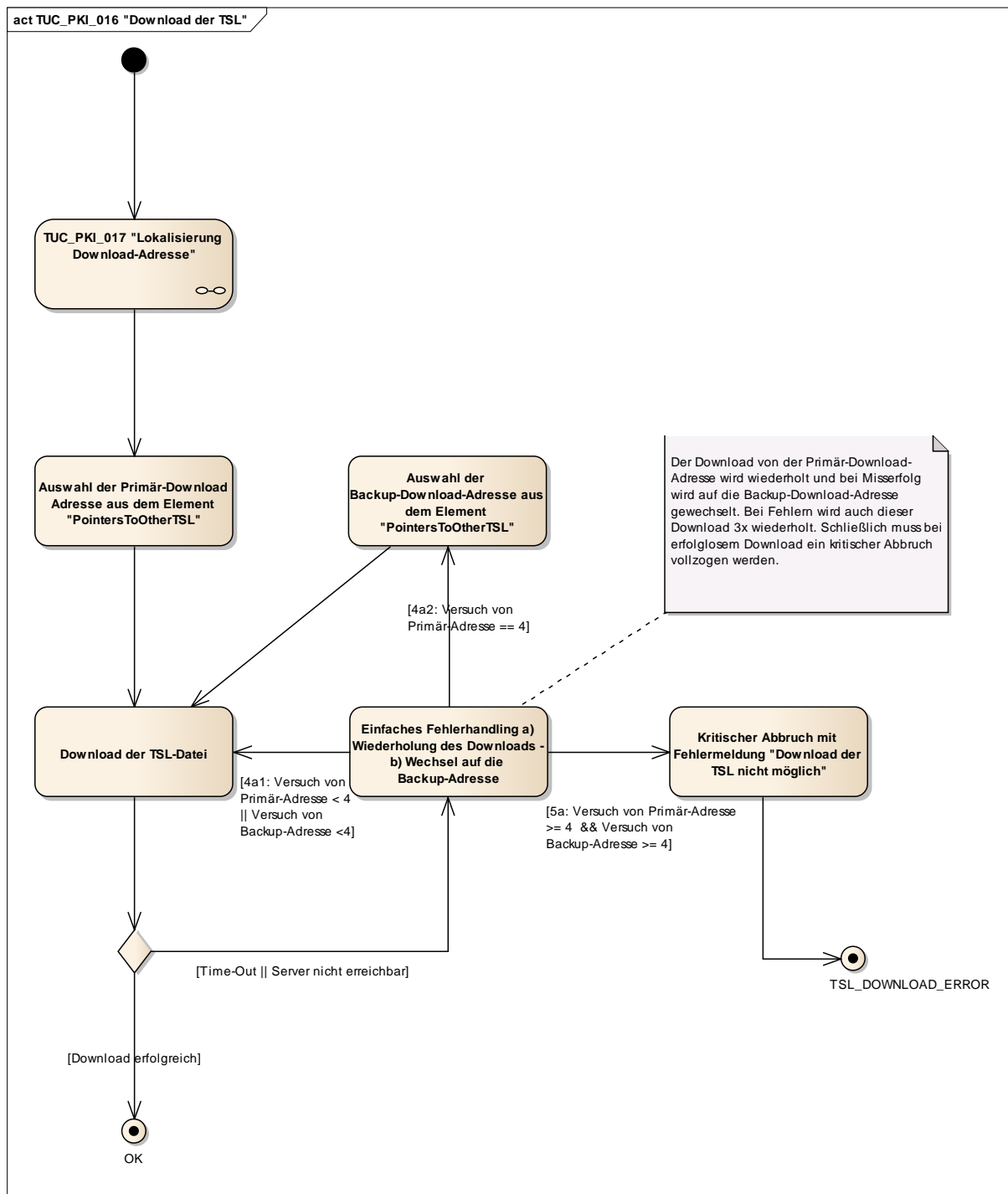


Abbildung 10: Aktivitätsdiagramm TUC_PKI_016 „Download der TSL-Datei“

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:

- a) OK: nextUpdate > aktuelles Datum
- b) VALIDITY_WARNING_1: nextUpdate < aktuelles Datum < (nextUpdate + TSL-Grace-Period)
- c) 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, d. h. es gibt keinen etablierten Vertrauensraum mehr.

Die Produkttypen der TI-Plattform, die Zertifikate prüfen, MÜSSEN sicherstellen, dass keine Zertifikatsprüfung als positiv bewertet wird, wenn kein etablierter Vertrauensraum besteht. Dies gilt unabhängig vom letzten bekannten Status des (ausstellenden) CA-Zertifikats. ☒

☒ **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 87: 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 anhand eines Vergleichs der TSL aus dem System und der TSL aus dem Download: Die jeweilige ID und die jeweilige Sequenznummer der beiden TSL werden verglichen.
Anwendungsumfeld	System, das die TSL auswertet
Vorbedingungen	Eine geprüfte TSL im System

Element	Beschreibung
Auslöser	TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“
Eingangsdaten	TSL im System, neu eingebrachte TSL-Datei (optional), TSL-Grace-Period
Komponenten	System
Ausgangsdaten	Status der Prüfung
Referenzen	[ETSI_TS_102_231]
Standardablauf	<ol style="list-style-type: none"> 1. [System:] System lädt die aktuelle TSL-Datei herunter (TUC_PKI_016 "Download der TSL-Datei"). 2. [System:] TSL-Datei aus dem Download 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 TSL-Datei aus dem Download oder aus den Eingangsdaten muss geprüft werden (TUC_PKI_012 „XML-Signatur-Prüfung“) 5. [System:] Aus der TSL im System und der TSL-Datei aus dem Download 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:] (Die IDs und TSLSequenceNumber-Elemente aus Schritt 5 sind identisch.) 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	<ol style="list-style-type: none"> 1a. [System:] Wenn eine TSL-Datei als Eingangsparameter eingebracht wurde, dann wird diese TSL-Datei verwendet, und es erfolgt kein Download. 6a. [System:] Die ID-Attribute aus Schritt 5 sind nicht gleich und das TSLSequenceNumber-Element der TSL im System ist kleiner als die aus dem Download. Somit ist die TSL im System älter als die aus dem Download. 6a1. [System:] Rückmeldung an den aufrufenden Use Case (TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“)
Fehlerfälle	<ol style="list-style-type: none"> 6b. [System:] Keine der beschriebenen Varianten des Vergleichs der ID und SequenceNumber tritt ein. Ende des Use Case mit Fehlermeldung

Element	Beschreibung
	<p>(TSL_ID_INCORRECT)</p> <p>7a.</p> <p>[System:] Die Aktualitäts-Prüfung ergibt, dass die TSL im System abgelaufen ist ($\text{nextUpdate} < \text{aktuelles Datum}$). Das aktuelle Datum liegt aber innerhalb der TSL-Grace-Period ($\text{aktuelles Datum} < \text{nextUpdate} + \text{TSL-Grace-Period}$).</p> <p>Warnung (VALIDITY_WARNING_1) mit der entsprechenden Meldung. (Die TSL ist nicht mehr aktuell.) Rückmeldung des Warnhinweises.</p> <p>7a1.</p> <p>[System:] Die Aktualitäts-Prüfung ergibt, dass die TSL-Grace-Period überschritten ist ($\text{aktuelles Datum} > \text{nextUpdate} + \text{TSL-Grace-Period}$).</p> <p>Warnung (VALIDITY_WARNING_2) mit der entsprechenden Meldung, (Ablauf der TSL-Grace-Period, die TSL ist nicht mehr vertrauenswürdig.) Rückmeldung des Warnhinweises.</p> <p>Weitere Fehlerfälle sind in den referenzierten Use Cases beschrieben.</p>
Technische Fehlermeldung	Weitere Fehlermeldungen finden sich in den jeweiligen referenzierten Use Cases.
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	<p>Die ID der TSL-Datei befindet sich als Attribut im Root-Tag des XML-Dokuments.</p> <pre><xsd:attribute name="Id" type="xsd:ID" use="optional"/></pre> <p>Das Attribut Id wird vom TSL-Service-Provider immer gefüllt. Das Element TSLSequenceNumber beschreibt die Folgenummer der TSL. Sein erstmaliger Inhalt ist gleich 1 und wird jeweils um 1 hoch gezählt.</p>
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_019 "Prüfung der Aktualität der TSL"

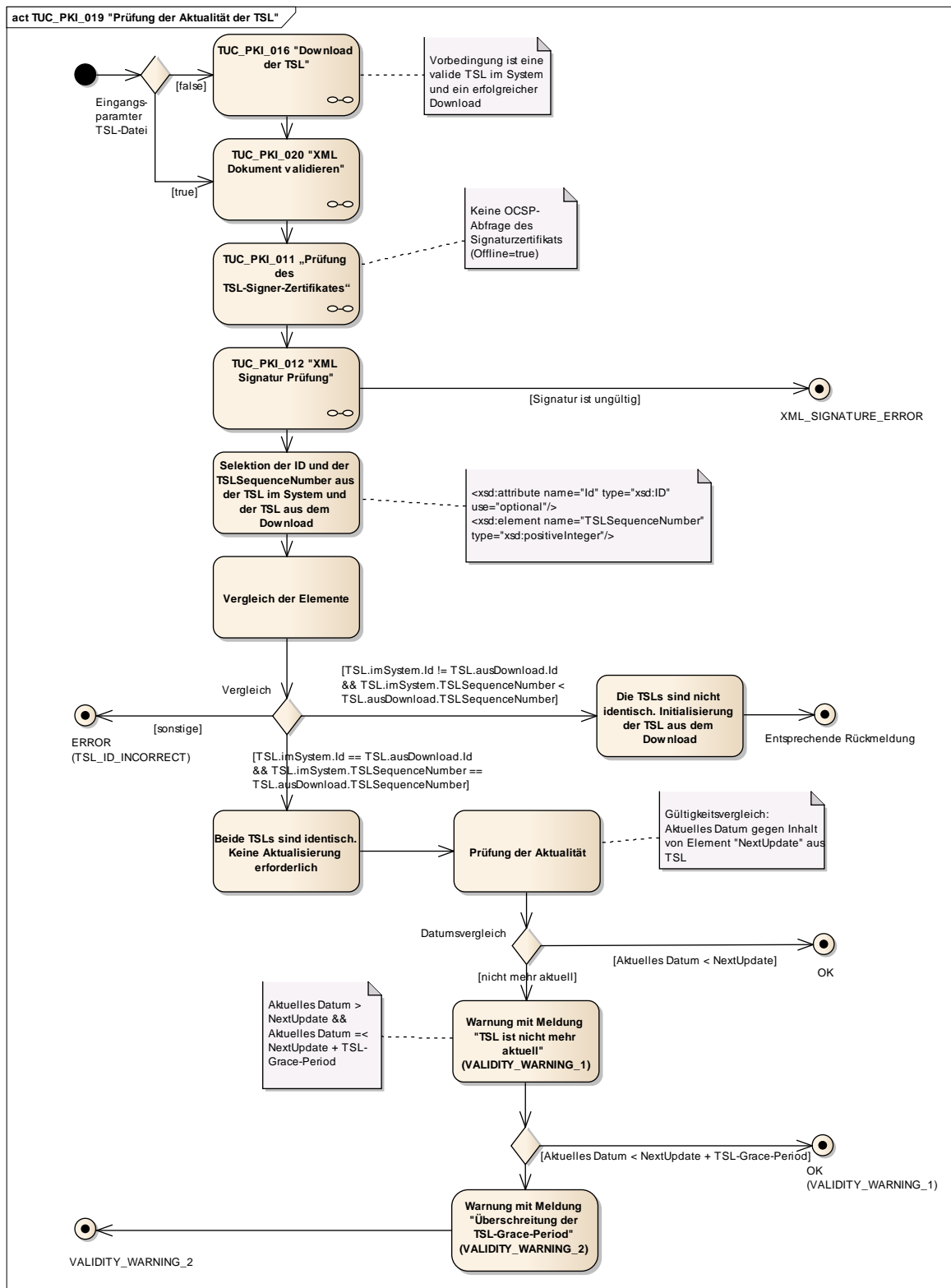


Abbildung 11: Aktivitätsdiagramm TUC_PKI_019 „Prüfung der Aktualität der TSL“

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 88: TUC_PKI_020 „XML-Dokument validieren“

Element	Beschreibung
Name	TUC_PKI_020 „XML-Dokument validieren“
Beschreibung	Ein XML-Dokument wird gegen ein XML-Schema validiert.
Anwendungsumfeld	Dieser Use Case wird verwendet, um XML-Dokumente zu validieren. In diesem Dokument betrifft das die Validierung der TSL.
Vorbedingungen	Eine vollständig vorliegende TSL-Datei im XML-Format
Auslöser	TUC_PKI_019 „Prüfung der Aktualität der TSL“
Eingangsdaten	TSL-Datei und TSL-XML-Schema (und alle in ihm referenzierten Schemata). Das System muss sicherstellen, dass zur Validierung nur das von der gematik spezifizierte bzw. benannte Schema benutzt wird.
Komponenten	System
Ausgangsdaten	Entsprechendes Ergebnis der Validierung (Erfolg Misserfolg)
Referenzen	[XML]
Standardablauf	<p>Das System prüft die Wohlgeformtheit des Dokumentes und validiert es gegen das Schema.</p> <ol style="list-style-type: none"> 1. [System:] System startet Prüfung der TSL-Datei. 2. [System:] System prüft Wohlgeformtheit der TSL-Datei. 3. [System:] System validiert die TSL-Datei gegen die Schemata. 4. [System:] Ende des Use Case mit positivem Ergebnis
Fehlerfälle	<p>Die übergebenen Schemata könnten selbst invalide oder unvollständig sein.</p> <ol style="list-style-type: none"> 2a. [System:] Ende des Use Case mit Fehlermeldung (TSL_NOT_WELLFORMED) 3a. [System:] Ende des Use Case mit Fehlermeldung (TSL_SCHEMA_NOT_VALID)
Technische Fehlermeldung	Das System meldet entsprechende Fehlercodes

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 89: TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“

Element	Beschreibung
Name	TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“
Beschreibung	Es wird der Prozess zur Prüfung des TSL-Signer-Zertifikates gegen ein sicher verwahrtes TSL-Signer-CA-Zertifikat spezifiziert. Der Prozess verläuft analog demjenigen für Zertifikatsprüfung im Allgemeinen (TUC_PKI_018 "Zertifikatsprüfung in der TI"), berücksichtigt aber die Besonderheiten des TSL-Signer-Zertifikates. Außerdem erfolgt hier keine Statusprüfung des TSL-Signer-Zertifikates. (Der Aufruf von TUC_PKI_006 „OCSP-Abfrage“ erfolgt in TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“.)
Anwendungsumfeld	System, das die TSL verwendet
Vorbedingungen	TSL-Signer-CA-Zertifikat in einem sicheren Speicher des Systems
Auslöser	TUC_PKI_019 „Prüfung der Aktualität der TSL“
Eingangsdaten	<ul style="list-style-type: none"> • TSL-Datei • Referenzzeitpunkt (aktuelles Datum)
Komponenten	System
Ausgangsdaten	Status der Prüfung
Referenzen	[ETSI_TS_102_231], [XMLSig]
Standardablauf	<ol style="list-style-type: none"> 1. [System:] Das verwendete TSL-Signer-Zertifikat wird aus der TSL-Datei extrahiert. 2. [System:] Der Use Case TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats" wird durchlaufen. 3. [System:] Prüfung der Extension KeyUsage auf vorhanden sein. Zudem wird die KeyUsage auf die richtige Belegung (nonRepudiation) geprüft. Weiter wird die ExtendedKeyUsage auf die richtige Belegung mit {id-tsl-kp-tslSigning} geprüft (vgl. Kap. 5.13.1 TSL-Signer-Zertifikat). 4. [System:] Das TSL-Signer-CA-Zertifikat aus dem sicheren Speicher des Systems wird geladen. 5. [System:] Anhand dieses CA-Zertifikates wird die mathematische Prüfung der Signatur des TSL-Signer-Zertifikats durchgeführt (TUC_PKI_004 "Mathematische Prüfung der Zertifikatssignatur"). (Jedes System muss Initial dieses CA-Zertifikat als TI-Vertrauensanker auf sicherem Wege integrieren.) 6. [System:] Ende des Use Case mit Status Rückmeldung
Varianten/Alternativen	
Fehlerfälle	<ol style="list-style-type: none"> 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

Element	Beschreibung
	Speicher des Systems geladen werden (TSL_CA_NOT_LOADED). Fehlerfälle sind in den referenzierten Use Cases beschrieben.
Technische Fehlermeldung	Das System meldet entsprechende Fehlercodes. Weitere technische Fehlermeldungen sind in den jeweiligen referenzierten TUCs 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	Abbildung 13 Aktivitätsdiagramm TUC_PKI_011 "Prüfung des TSL-Signer-Zertifikates"

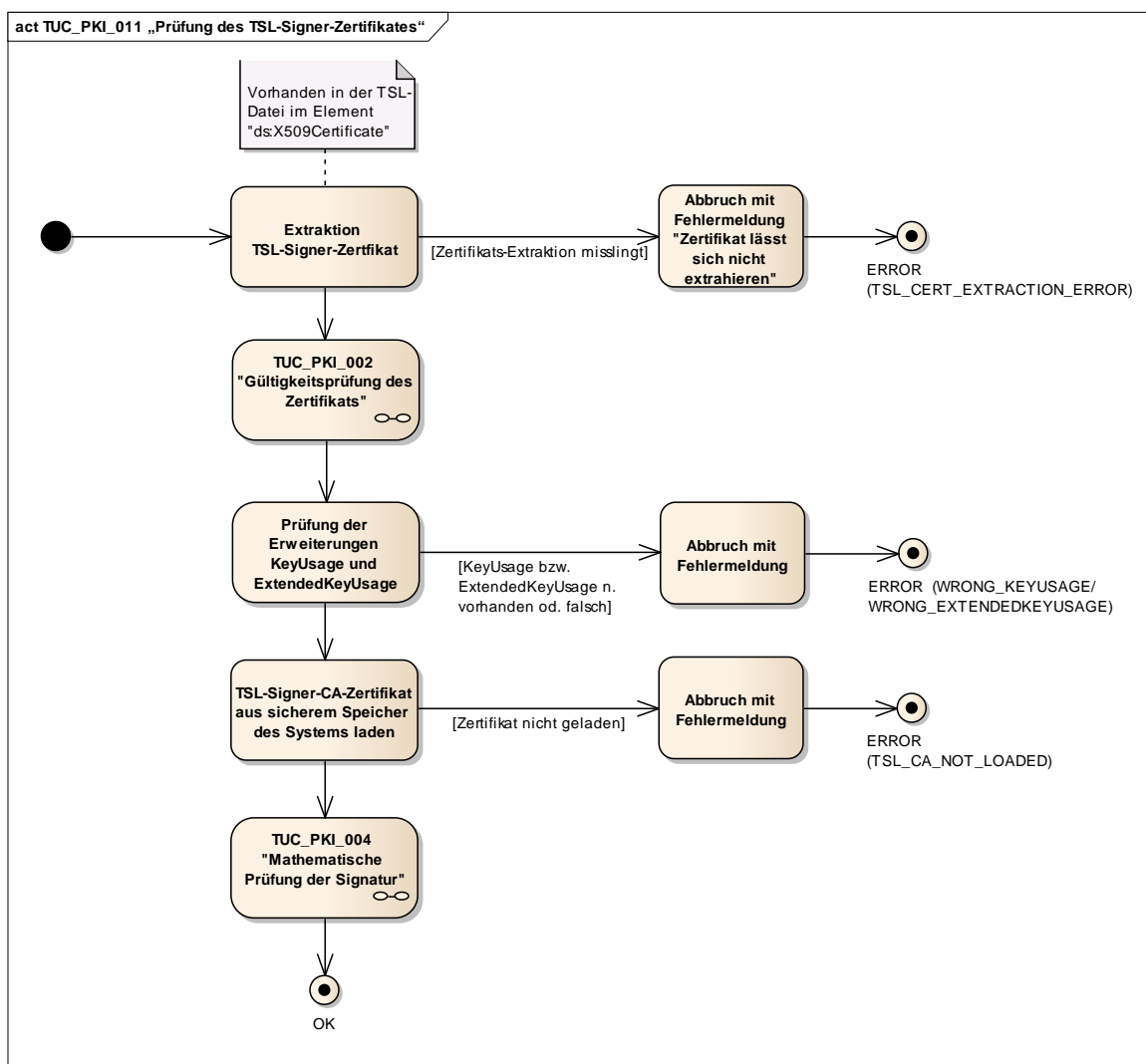


Abbildung 12: Aktivitätsdiagramm TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“

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 90: 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)
Technische Fehlermeldung	Das System meldet entsprechende Fehlercodes. Weitere Fehlermeldungen befinden sich in den referenzierten Spezifikationen.
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 91: Tab_PKI_294 TSL Zeitparameter

Beschreibung	Zeitparameter
Gültigkeitsdauer einer TSL	Ausstellungsdatum + 30 Tage
TSL-Grace-Period für zentrale 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

8.3 Zertifikatsprüfung X.509 nonQES

Für die Prüfung der X.509-Zertifikate gelten folgende Vorbedingungen (s. Kapitel 8.1 und 8.2):

- aktuelle TSL liegt vor
- TSL-Datei wurde geprüft
- Der TI-Vertrauensraum wurde initialisiert, der Truststore kann benutzt werden.

Die folgende Use Case Übersicht verdeutlicht die Aktionen des Systems.

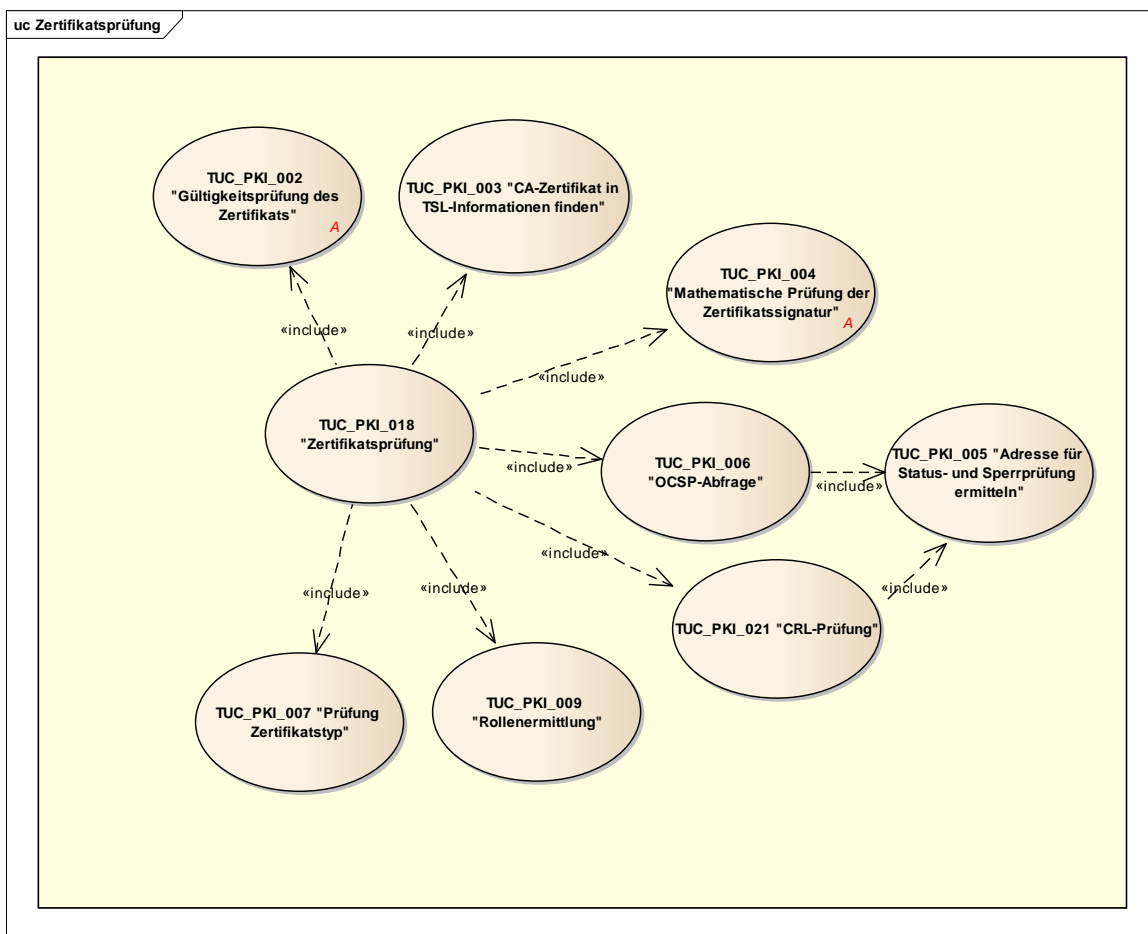


Abbildung 13: Use Case Diagramm „Zertifikatsprüfung“

Die folgenden Schritte sind für eine nonQES-Zertifikatsprüfung durchzuführen:

- Prüfung der Gültigkeit (TUC_PKI_002)
- Prüfung der Identität des Zertifikatsherausgebers (TUC_PKI_003)
- Prüfung der mathematischen Korrektheit des Zertifikats (Signaturprüfung) (TUC_PKI_004)
- Abfrage des Sperrstatus des zu prüfenden Zertifikats gegen den im „ServiceSupplyPoint“ der TSL eingetragenen OCSP-Responder (TUC_PKI_006) und Prüfung der OCSP-Antwort (Responder-Zertifikat, Sperrstatus)
- Rollenermittlung (TUC_PKI_009)
- Prüfung Zertifikatstyp (TUC_PKI_007)

Bei jeder dieser Prüfungen muss nicht nur die mathematisch-kryptographische Korrektheit der jeweiligen Mechanismen, sondern auch deren Zulässigkeit mit in die Prüfung einbezogen werden. Zum Beispiel darf ein Zertifikat, welches nicht mit einem zugelassenen Hash-Algorithmus signiert ist, nie als gültig eingestuft werden. Für die TI gültige Hash-Algorithmen siehe [gemSpec_Krypt].

Die Verwendung von Informationen aus Zertifikaten kann nur dann erfolgen, wenn das zugehörige Zertifikat validiert wurde. Somit MUSS eine Zertifikatsprüfung der Ermittlung bestätigter Zertifikatsinformationen vorangehen.

In dem Dokument wird der Begriff „gültiger Zeitraum“ verwendet. Dieser bedeutet, dass sich der aktuelle Zeitpunkt innerhalb des Gültigkeitszeitraums des Objektes befindet.

Die Fachdokumente müssen die entsprechenden Eingangsparameter der Use Cases berücksichtigen. Die Festlegungen aus den folgenden Dokumenten sind für die Zertifikatsprüfung verbindlich:

- [Common-PKI]: Specifications for Interoperable PKI Applications
- [RFC 2560]: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
- [RFC 5280]: Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile.

8.3.1 Zertifikatsprüfung in der TI

8.3.1.1 TUC_PKI_018 „Zertifikatsprüfung in der TI“

☒ **GS-A_4652 TUC_PKI_018: Zertifikatsprüfung in der TI**

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

Tabelle 92: 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	Etablierter Vertrauensraum der TI in der zertifikatsprüfenden Komponente (Die TSL-Informationen sind innerhalb der TSL-Graceperiod gültig bzw. vertrauenswürdig.)
Auslöser	Zertifikats-Check
Eingangsdaten	<ul style="list-style-type: none">• Das zu prüfende Zertifikat• Referenzzeitpunkt: Zeitpunkt, für den das Zertifikat geprüft werden soll (optional; bei Nichtangabe Verwendung der aktuellen Systemzeit)• PolicyList Liste der im aktuellen Aufruf zulässigen Zertifikatstyp-OIDs. Die Liste muss mindestens eine OID enthalten.• Vorgesehene KeyUsage (intendedKeyUsage, mehrere Werte möglich)• Vorgesehene ExtendedKeyUsage (intendedExtendedKeyUsage, mehrere Werte möglich)• OCSP-Graceperiod (legt bei der Verwendung von (gecachten) OCSP-Antworten den maximal zulässige Zeitraum fest, den die Systemzeit der prüfenden Komponente noch nach dem Zeitpunkt der OCSP-Antwort liegen darf)• Offline-Modus (ja/nein)

Element	Beschreibung
	<ul style="list-style-type: none"> Beigefügte OCSP-Response zum angefragten Zertifikat (optional; z. B. in der Signatur eingebettet) Timeout-Parameter (Default: 10s) TOLERATE_OCSP_FAILURE (true/false, Default: false) - Der Parameter definiert das Verhalten für den Fall, dass die OCSP-Prüfung nicht durchgeführt werden konnte, weil der OCSP-Responder beispielsweise technisch nicht erreichbar ist. Prüfmodus (OCSP, CRL)
Komponenten	System, OCSP-Responder
Ausgangsdaten	Status der Prüfung, OCSP-Response, im Zertifikat enthaltene Rollen-OIDs
Referenzen	[Common-PKI]
Standardablauf	<p>Die Zertifikatsprüfung setzt sich aus folgenden Schritten zusammen:</p> <ol style="list-style-type: none"> 1. [System] Die Gültigkeit des Zertifikats wird geprüft (TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats") . 2. [System] Prüfung der Extension KeyUsage auf Vorhandensein. Zudem wird die KeyUsage und ExtendedKeyUsage (falls vorhanden) auf die richtige Belegung entsprechend der vorgesehenen (intendedKeyUsage bzw. intendedExtendedKeyUsage) KeyUsage geprüft. Die intendedKeyUsage sowie die intendedExtendedKeyUsage können aus einer Liste mehrerer erlaubter Werte bestehen. 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 9, sonst mit 7. 7. [System, Prüfmodus OCSP] Statusinformation zum Zertifikat durch Abfrage des zugeordneten OCSP-Dienstes ermitteln (TUC_PKI_006 "OCSP-Abfrage") 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	<p>6a. [System:] Der Offline-Modus ist aktiviert. Es werden keine</p>

Element	Beschreibung
	<p>Statusinformationen zum Zertifikat eingeholt.</p> <p>7a. [System, Prüfmodus CRL] Prüfung der Sperrinformation des Zertifikates mittels CRL (TUC_PKI_021 "CRL-Prüfung")</p> <p>7b [System] Eine OCSP-Response zu dem zu prüfenden Zertifikat wurde im Aufruf mit übergeben. Falls diese zum Referenzzeitpunkt gültig ist, wird nicht der TUC_PKI_006 aufgerufen, sondern die beigelegte OCSP-Response zur weiteren Prüfung verwendet.</p>
Fehlerfälle	<p>2a. [System:] KeyUsage ist nicht vorhanden bzw. entspricht nicht der vorgesehenen KeyUsage (WRONG_KEYUSAGE).</p> <p>2a1. [System:] ExtendedKeyUsage entspricht nicht der vorgesehenen ExtendedKeyUsage (WRONG_EXTENDEDKEYUSAGE).</p> <p>5a. [System:] Das Ausgabedatum des End-Entity-Zertifikats liegt nach dem Datum des Statuswechsels. Abbruch mit Fehlermeldung (CA_CERTIFICATE_REVOKED_IN_TSL)</p> <p>7c. [System] Eine OCSP-Response zu dem zu prüfenden Zertifikat wurde im Aufruf mit übergeben, ergab bei den weiteren Prüfschritten jedoch kein gültiges Ergebnis (Überprüfung und Auswertung der Gültigkeit der OCSP-Response in TUC_PKI_006 schlägt fehl). Eine erneute Prüfung wird in diesem Fall durch Aufruf des TUC_PKI_006 durchgeführt, als wäre keine OCSP-Response beigelegt.</p> <p>In den Rückgabewerten dieses TUC wird die Warnmeldung (PROVIDED_OCSP_RESPONSE_NOT_VALID) an die aufrufende Funktion übergeben.</p>
Technische Fehlermeldung	<p>Das System meldet entsprechende Fehlercodes. Weitere technische Fehlermeldungen sind in den jeweiligen referenzierten TUCs beschrieben.</p>
Sicherheitsanforderungen	<p>Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.</p>
Anmerkungen	<p>Schritt 5 stellt eine Sperrprüfung des CA-Zertifikats (für nonQES-HBA- und SMC-B-Zertifikate) gemäß Ketten- bzw. Kompromissmodell dar. Vgl. Kap. 8.1.1 Initialisierung TI-Vertrauensraum.</p>
Zugehörige Diagramme	<p>Abbildung 15: Aktivitätsdiagramm TUC_PKI_018 "Zertifikatsprüfung"</p>

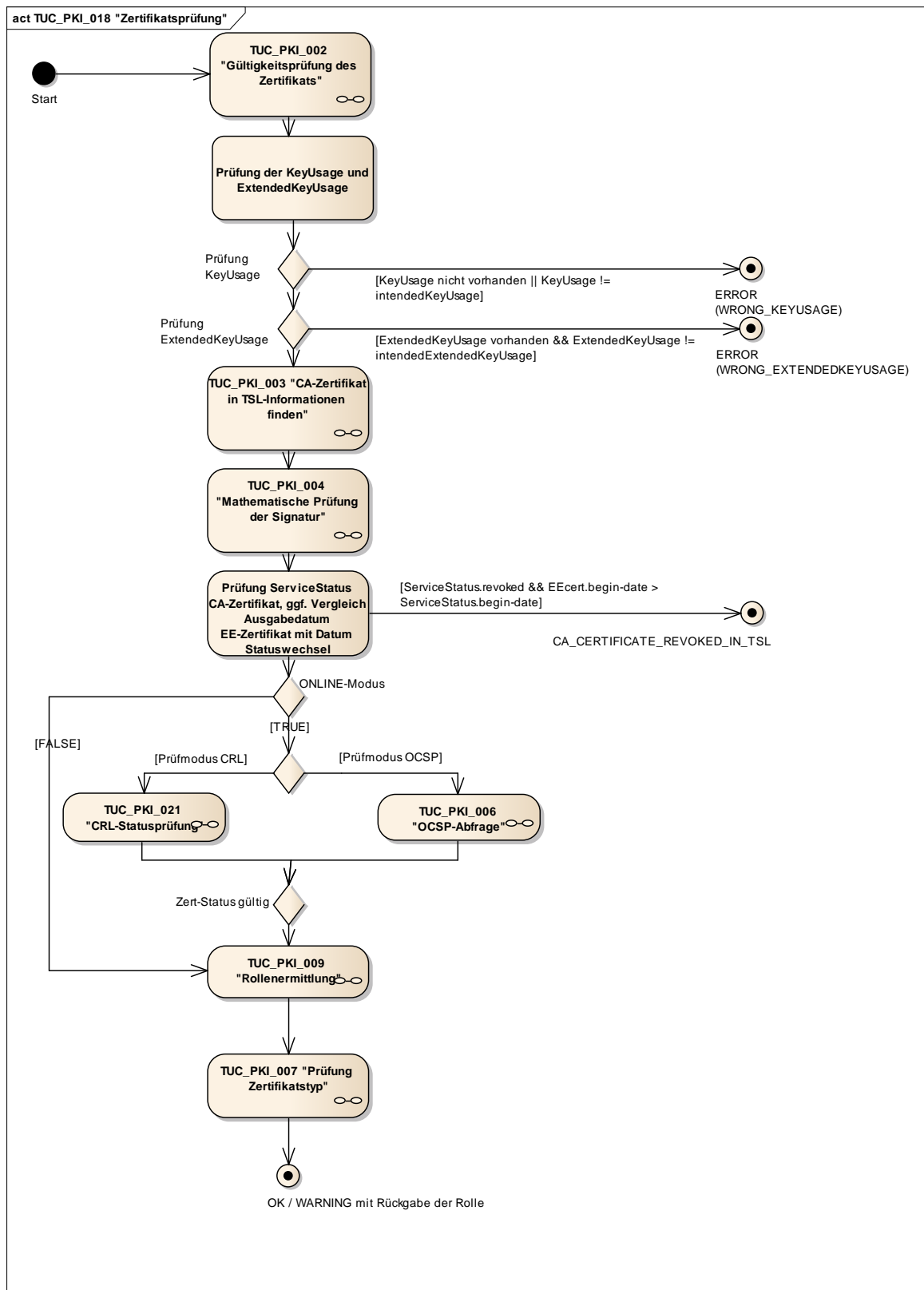


Abbildung 14: Aktivitätsdiagramm TUC_PKI_018 „Zertifikatsprüfung“

8.3.1.2 TUC_PKI_002 „Gültigkeitsprüfung des Zertifikats“

☒ GS-A_4653 TUC_PKI_002: Gültigkeitsprüfung des Zertifikats

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_002 zur Gültigkeitsprüfung des Zertifikates umsetzen. ☒

Tabelle 93: 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 Zertifikat steht.
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	Zertifikat vorhanden
Auslöser	TUC_PKI_013 „Import TI-Vertrauensanker aus TSL“, TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“, TUC_PKI_018 "Zertifikatsprüfung in der TI "
Eingangsdaten	<ul style="list-style-type: none"> Das zu prüfende Zertifikat Referenzzeitpunkt
Komponenten	System
Ausgangsdaten	Status der Prüfung
Referenzen	[Common-PKI]
Standardablauf	<ol style="list-style-type: none"> [System:] Zertifikat lesen [System:] Aus dem Zertifikat das Feld Validity ermitteln und auslesen. [System:] Anhand der ermittelten Daten wird die Gültigkeit geprüft. Dabei kommt folgender Algorithmus zu tragen: $\text{notBefore} < \text{Referenzzeitpunkt} \ \&\& \ \text{notAfter} > \text{Referenzzeitpunkt}$ entspricht einem zeitlich gültigem Zertifikat [System:] Rückmeldung des Status
Fehlerfälle	<ol style="list-style-type: none"> [System:] Zertifikat ist nicht lesbar (CERT_READ_ERROR). [System:] Prüfzeitpunkt nicht innerhalb der Gültigkeitsdauer des Zertifikats (CERTIFICATE_NOT_VALID_TIME).
Technische Fehlermeldung	<p>Das Zertifikat ist zum Referenzzeitpunkt nicht gültig (CERTIFICATE_NOT_VALID_TIME)</p> <p>Das System meldet entsprechende Fehlercodes.</p>
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	<p>Aufbau der Gültigkeit:</p> <pre>Validity ::= SEQUENCE { notBefore Time, notAfter Time }</pre>
Zugehörige Diagramme	Abbildung 16: Aktivitätsdiagramm TUC_PKI_002 Gültigkeitsprüfung des Zertifikats

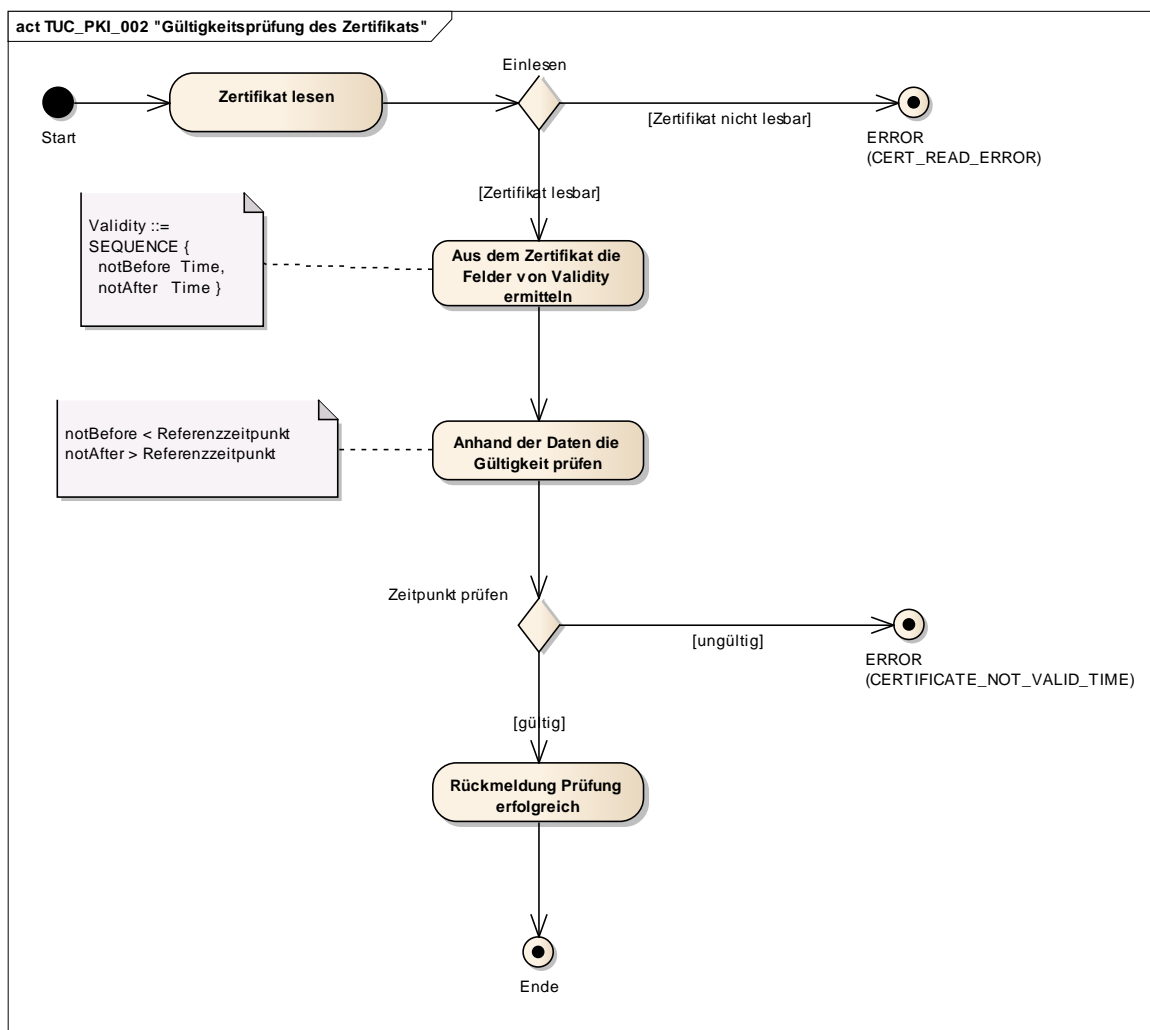


Abbildung 15: Aktivitätsdiagramm TUC_PKI_002 Gültigkeitsprüfung des Zertifikats

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

☒ GS-A_4654 TUC_PKI_003: CA-Zertifikat finden

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_003 zur Ermittlung des CA-Zertifikats aus den TSL-Informationen umsetzen. ☒

Tabelle 94: 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 "

Element	Beschreibung
Eingangsdaten	End-Entity-Zertifikatsdaten, TSL-Informationen
Komponenten	System
Ausgangsdaten	Status der Prüfung, (Referenz auf) CA-Zertifikat
Referenzen	[Common-PKI]
Standardablauf	<p>1. [System:] Anhand der End-Entity-Zertifikatsdaten werden die TSL-Informationen durchsucht, um das passende CA-Zertifikat zu finden.</p> <p>2. [System:] Vergleich 1: IssuerDN des End-Entity-Zertifikats mit dem subjectDN des CA-Zertifikats</p> <p>3. [System:] Vergleich 2: AuthorityKeyIdentifier des End-Entity-Zertifikats mit SubjectKeyIdentifier des CA-Zertifikats</p> <p>4. [System:] Selektion (Referenz auf) CA-Zertifikat und Rückgabe</p>
Varianten/Alternativen	<p>2a. [System:] Keine Übereinstimmung. Der Vorgang wird mit einem anderen CA-Zertifikat wiederholt (Iteration)</p>
Fehlerfälle	<p>2b. [System:] Ende der Liste erreicht UND keine Übereinstimmung im DN gefunden. Abbruch des TUC mit Fehlermeldung (CA_CERT_MISSING)</p> <p>3a. [System:] CA mit passendem DN gefunden, aber Ausstellerschlüssel (SubjectKeyIdentifier) und die Referenz (AuthorityKeyIdentifier) stimmen nicht überein. Abbruch des TUC mit Fehlermeldung (AUTHORITYKEYID_DIFFERENT)</p>
Technische Fehlermeldung	Das System meldet entsprechende Fehlercodes.
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	
Zugehörige Diagramme	Abbildung 17: Aktivitätsdiagramm TUC_PKI_003 CA-Zertifikat in TSL-Informationen finden

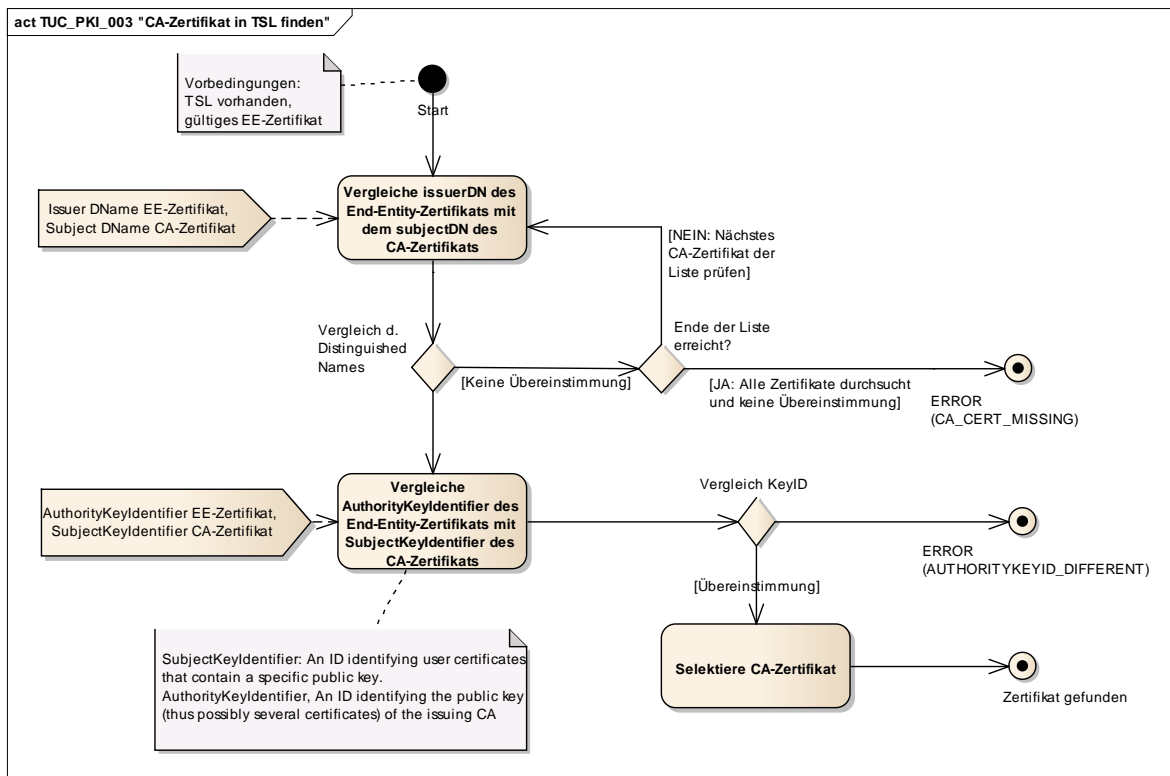


Abbildung 16: Aktivitätsdiagramm TUC_PKI_003 CA-Zertifikat in TSL-Informationen finden

8.3.1.4 TUC_PKI_004 „Mathematische Prüfung der Zertifikatssignatur“

☒ GS-A_4655 TUC_PKI_004: Mathematische Prüfung der Zertifikatssignatur

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

Tabelle 95: 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
Voraussetzungen	Gültiges CA-Zertifikat und passendes End-Entity-Zertifikat innerhalb des definierten Gültigkeitszeitraums
Auslöser	TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“, TUC_PKI_013 „Import TI-Vertrauensanker aus TSL“, TUC_PKI_018 "Zertifikatsprüfung in der TI "
Eingangsdaten	End-Entity-Zertifikat, CA-Zertifikat
Komponenten	System
Ausgangsdaten	Status der Prüfung
Referenzen	[Common-PKI]
Standardablauf	1. [System:] Auswahl des öffentlichen Schlüssels des CA-Zertifikats

Element	Beschreibung
	<p>2. [System:] Die Signatur und der verwendete Algorithmus werden aus dem End-Entity-Zertifikat ausgelesen</p> <p>3. [System:] Verifikation der Signatur und Hashwert-Vergleich (Verfahren siehe [RFC5280])</p> <p>4. [System:] Rückmeldung an das System</p>
Fehlerfälle	3a. [System:] Die Zertifikats-Signatur ist nicht gültig. Ende des Use Case. Abbruch mit Fehlermeldung (CERTIFICATE_NOT_VALID_MATH)
Technische Fehlermeldung	Die Zertifikats-Signatur ist nicht gültig (CERTIFICATE_NOT_VALID_MATH). Das System meldet entsprechende Fehlercodes.
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	<p>signatureAlgorithm AlgorithmIdentifizier: Stellt den verwendeten Signatur-Algorithmus dar, den die CA benutzt hat, um das Zertifikat zu signieren.</p> <p>signature BIT STRING: Die Signatur des Zertifikats.</p>
Zugehörige Diagramme	Abbildung 18: Aktivitätsdiagramm TUC_PKI_004 Mathematische Prüfung der Zertifikatssignatur

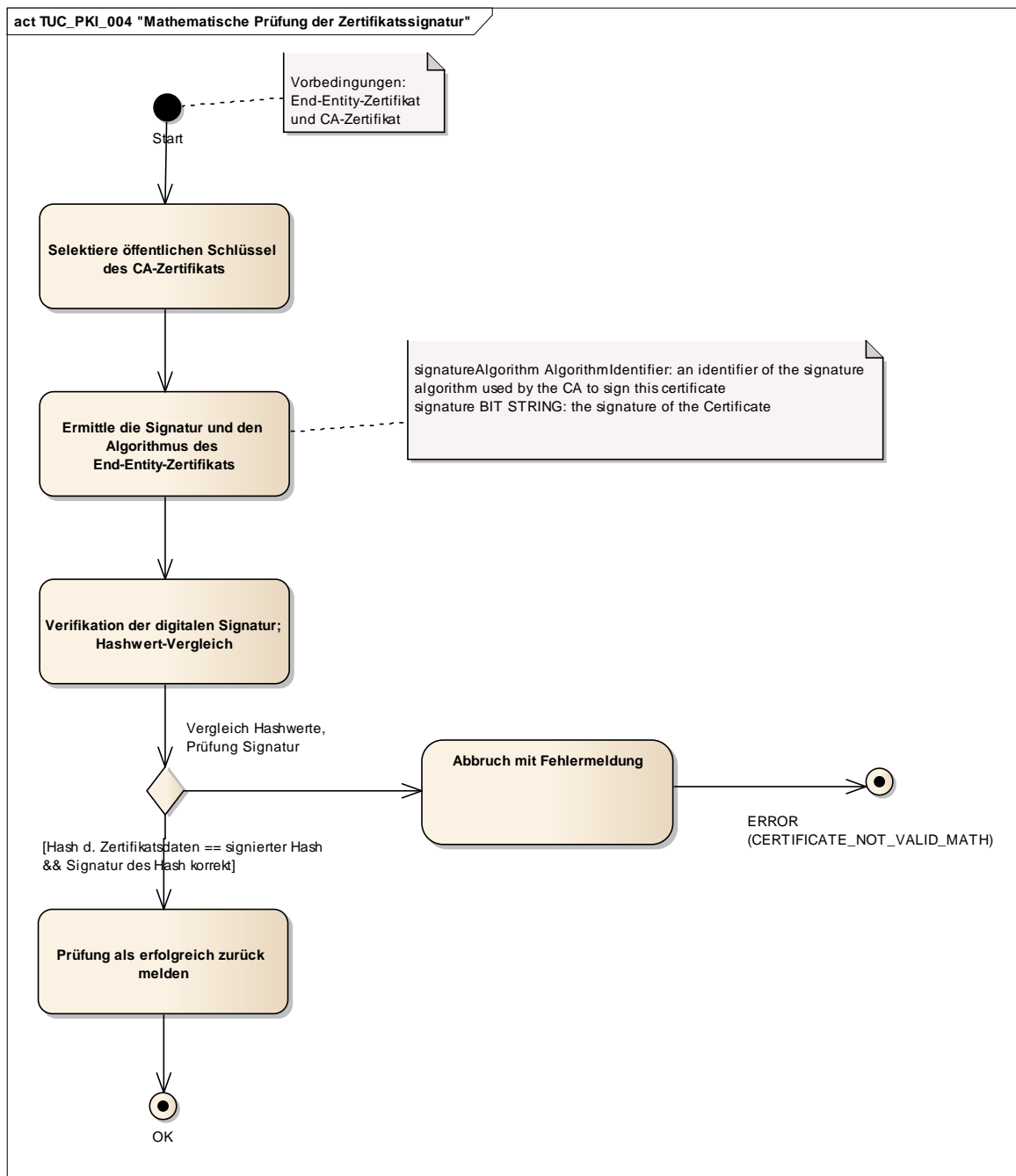


Abbildung 17: Aktivitätsdiagramm TUC_PKI_004 Mathematische Prüfung der Zertifikatssignatur

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 96: TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln“

Element	Beschreibung
Name	TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln“
Beschreibung	In diesem Use Case wird die Ermittlung der Adresse für Status- und Sperrprüfung beschrieben. Default-mäßig handelt es sich dabei um die Adresse des OCSP-Responders, alternativ um diejenige des CRL-Downloadpunktes. Hierbei wird auf die TSL-Informationen zurückgegriffen. Die Adresse ist im CA-Eintrag der TSL hinterlegt. Für das Verhalten in spezifizierten Offline-Szenarien gilt [GS-A_4658].
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	Eine TSL mit gültiger Signatur
Auslöser	TUC_PKI_006 "OCSP-Abfrage" oder TUC_PKI_021 "CRL-Prüfung"
Eingangsdaten	<ul style="list-style-type: none"> • End-Entity-Zertifikatsdaten • TSL-Informationen
Komponenten	System
Ausgangsdaten	OCSP-Adresse oder Adresse des CRL-Downloadpunktes
Standardablauf	<ol style="list-style-type: none"> 1. [System:] (Referenz auf) CA-Zertifikat in TSL-Informationen finden (TUC_PKI_003 "CA-Zertifikat in TSL-Informationen finden") 2. [System:] Das Element "ServiceSupplyPoint" (bzw. via referenziertes CA-Zertifikat die Referenz auf den bezeichneten Statusprüfdienst- oder CRL Downloadpunkt) auswählen und URI selektieren. 3. [System:] Adresse zurückmelden
Fehlerfälle	<ol style="list-style-type: none"> 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). <p>Weitere Fehlerfälle werden in den jeweiligen referenzierten TUCs beschrieben.</p>
Technische Fehlermeldung	Das System meldet entsprechende Fehlercodes.
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	Abbildung 19 Aktivitätsdiagramm TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln "

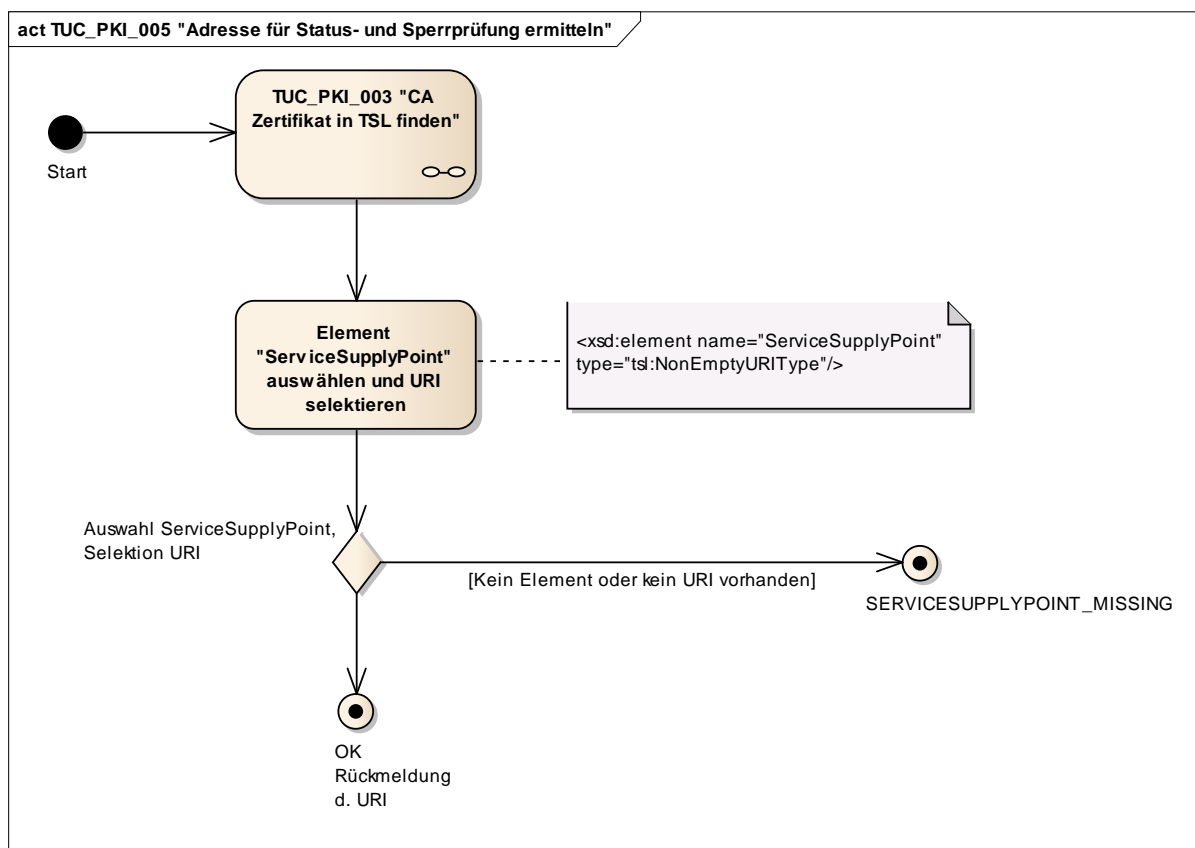


Abbildung 18: Aktivitätsdiagramm TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln“

8.3.2.2 TUC_PKI_006 „OCSP-Abfrage“

☒ GS-A_4657 TUC_PKI_006: OCSP-Abfrage

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_006 zur OCSP-Abfrage umsetzen. ☒

Tabelle 97: TUC_PKI_006 „OCSP-Abfrage“

Element	Beschreibung
Name	TUC_PKI_006 „OCSP-Abfrage“
Beschreibung	Dieser Use Case beschreibt den Prozess zur OCSP-Prüfung eines Zertifikats. Für das Verhalten in spezifizierten Offline-Szenarien gilt [GS-A_4658]. Der Use Case richtet sich nach den Anforderungen gemäß [Common-PKI#Part5#2.3] und nach den spezifischen Eigenschaften der TI. Für nicht-qualifizierte Zertifikate einer eGK wird der Schritt zur Prüfung der certHash-Erweiterung (gemäß [Common-PKI]) nicht abgearbeitet, d.h. der Parameter ENFORCE_CERTHASH_CHECK darf nicht auf „true“ gesetzt werden. (Vgl. [GS-A_4693].)
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	Zeitlich gültiges End-Entity- und CA-Zertifikat. TSL-Informationen sind vorhanden.

Element	Beschreibung
Auslöser	Zertifikats-Check
Eingangsdaten	<ul style="list-style-type: none"> • End-Entity-Zertifikatsdaten • CA-Zertifikatsdaten • TSL-Informationen • Referenzzeitpunkt (vgl. Glossar) • OCSP-Graceperiod (Default: 10min) • Timeout-Parameter (Default: 10s) • TOLERATE_OCSP_FAILURE (true/false, Default: false) • ENFORCE_CERTHASH_CHECK (true/false, Default: false)
Komponenten	System, OCSP-Responder
Ausgangsdaten	Status der Prüfung OCSP-Response
Referenzen	[Common-PKI] Part 4#3, [Common-PKI#Part5#2.3]
Standardablauf	<ol style="list-style-type: none"> 1. [System:] Prüfung, ob (zum Referenzzeitpunkt unter Berücksichtigung der OCSP-Graceperiod) gültige Statusinformationen bereits vorliegen (z. B. im lokalen Cache bereitgestellt). 2. [System:] Ermittlung der OCSP-Adresse (TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln") 3. [System:] Aufbau des OCSP-Request anhand der passenden Zertifikatsdaten 4. [System:] Absenden des Request an die ermittelte Adresse Der Timeout-Parameter definiert hier, zu welchem Zeitpunkt das System ein Timeout bei Nichterreichbarkeit des Dienstes meldet. 5. [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 „ServiceTypidentifizier“ "http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP" markiert.) 6. [System:] Auswertung der OCSP-Response. Details siehe [Common-PKI#Part4#3] 7. [System:] Wenn ENFORCE_CERTHASH_CHECK auf 'true' gesetzt ist, wird das End-Entity-Zertifikat mit dem in der certHash-Erweiterung bezeichneten Algorithmus gehasht (vgl. [gemSpec_Krypt#GS-A_4393]). Das Resultat stimmt mit dem gelieferten certificateHash überein. Details siehe [Common-PKI#Part4#3.1.2] und [Common-PKI#Part5#2.3]. 8. [System:] Überprüfung der Gültigkeit anhand des Referenzzeitpunkts. Der CertStatus "good" wird gemeldet. 9. [System:] Rückmeldung, dass das Zertifikat gültig ist und Rückgabe der OCSP-Response. 10. [System:] Ende des UseCase
Varianten/Alternati-	1a.

Element	Beschreibung
ven	<p>[System:] Prüfung der Gültigkeit des Zertifikats gegen vorliegende Informationen.</p> <p>1a1. [System:] Zertifikat ist gesperrt. Weiter mit Schritt 5, falls die entsprechenden Prüfungen nicht bereits erfolgt sind. Ansonsten Rückmeldung analog 8.</p> <p>1a2. Die Statusinformationen sind zu alt (Zertifikat nicht gesperrt && (Referenzzeit > Statusinfo.producedAt && (Systemzeit - Statusinfo.producedAt) > OCSP-Graceperiod)). Neue Informationen müssen eingeholt werden. Es geht weiter mit Schritt 2 (Standardablauf).</p> <p>1a3. [System:] Zertifikat ist nicht gesperrt und Referenzzeitpunkt <= Datum der Statusinformationen (producedAt) des Zertifikats oder (Systemzeit - Statusinfo.producedAt) <= OCSP-Graceperiod. Rückmeldung: Zertifikat ist gültig.</p> <p>7a. [System:] ENFORCE_CERTHASH_CHECK ist auf 'false' gesetzt. Weiter mit nächstem Schritt</p> <p>8a. [System:] Das Zertifikat ist für den Referenzzeitpunkt gültig, obwohl der CertStatus "revoked" gemeldet wird, da "revocationTime" > Referenzzeitpunkt. Rückmeldung Zertifikat ist für den Referenzzeitpunkt gültig und Rückgabe der OCSP-Response.</p> <p>8b. [System:] Zertifikat ist gesperrt und die Referenzzeit liegt nach dem Sperrzeitpunkt (CertStatus revoked UND revocationTime <= des Referenzzeitpunkts). Rückmeldung Zertifikat ist gesperrt und Rückgabe der OCSP-Response. (CERT_REVOKED)</p> <p>8c. [System:] Zertifikat ist unbekannt (Status unknown) Rückmeldung, dass das Zertifikat ungültig ist und Rückgabe der OCSP-Response. (CERT_UNKNOWN)</p>
Fehlerfälle/Warnungen	<p>4a. [System:] Die OCSP-Prüfung konnte nicht durchgeführt werden: Im Falle von TOLERATE_OCSP_FAILURE=true wird als Ergebnis eine Warnung generiert (OCSP_CHECK_REVOCATION_FAILED).</p> <p>4b. [System:] Die OCSP-Prüfung konnte nicht durchgeführt werden: Im Falle von TOLERATE_OCSP_FAILURE=false wird mit einer Fehlermeldung abgebrochen. (OCSP_CHECK_REVOCATION_ERROR)</p> <p>5a. [System:] OCSP-Zertifikat nicht in TSL-Informationen enthalten. Abbruch mit Fehlermeldung. (OCSP_CERT_MISSING)</p> <p>5a1. [System:] Signatur der Response ist nicht gültig. Abbruch mit Fehlermeldung (OCSP_SIGNATURE_ERROR)</p> <p>6a. [System:] Die Response enthält einen Statuscode („OCSPResponseStatus“), der ungleich 0 (für „successful“) ist. (Damit zeigt der OCSP-Responder eine Exception an. Z. B. kann der Wert für den Status auf 3 für „tryLater“ gesetzt sein.) Abbruch mit Fehlermeldung (OCSP_STATUS_ERROR)</p> <p>6b. [System:] Die Response enthält einen Statuscode („OCSPResponseStatus“), der gleich 0 („successful“) ist. Die ausgewertete OCSP-Response passt aber nicht zum OCSP-Request (z.B. CertID in</p>

Element	Beschreibung
	<p>OCSP-Request und –Response stimmt gemäß [Common-PKI#Part4#3] nicht überein). Abbruch mit Fehlermeldung (OCSP_CHECK_REVOCATION_ERROR)</p> <p>7b. ENFORCE_CERTHASH_CHECK ist auf 'true' gesetzt und die OCSP-Response enthält keine certHash-Erweiterung. (CERTHASH_EXTENSION_MISSING)</p> <p>7c. Der errechnete Zertifikats-Hash stimmt nicht mit demjenigen aus der in der Erweiterung certHash überein. (CERTHASH_MISMATCH)</p>
Technische Fehlermeldung	<p>Der OCSP-Responder ist nicht verfügbar. (OCSP_NOT_AVAILABLE)</p> <p>OCSP-Responder-Zertifikat steht nicht in der TSL. (OCSP_CERT_MISSING)</p> <p>Die OCSP-Response enthält eine Exception-Meldung. (OCSP_STATUS_ERROR)</p> <p>certHash-Erweiterung fehlt. (CERTHASH_EXTENSION_MISSING)</p> <p>Nicht übereinstimmende Zertifikats-Hashes (CERTHASH_MISMATCH)</p> <p>Das System meldet entsprechende Fehlercodes.</p> <p>Weitere technische Fehlermeldungen sind in den jeweiligen referenzierten TUCs beschrieben.</p>
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	<p>Der genaue Aufbau des OCSP-Requests und der OCSP-Response ist in Kapitel 9 spezifiziert.</p> <p>Zur Abfrage beim OCSP-Responder MUSS ein Timeout-Parameter konfiguriert werden können. Dieser definiert, zu welchem Zeitpunkt das System ein Timeout bei Nichterreichbarkeit des Dienstes meldet.</p> <p>Die OCSP-Graceperiod dient der Performance-Steigerung. Die OCSP-Graceperiod legt bei der Verwendung von OCSP-Antworten (im Cache) deren maximal zulässiges Alter fest (gemessen an der Systemzeit). Ein Zwang, OCSP-Responses über die gesamte Dauer der OCSP-Graceperiod zu cachen, existiert nicht.</p> <p>Anmerkung zu 6b: Die OCSP-Response muss gemäß [Common-PKI] Part 4#3 bzw. RFC3370#2.1 verarbeitet werden, unabhängig davon ob der Parameter AlgorithmIdentifier innerhalb der CertID mit NULL belegt oder nicht gesetzt ist.</p>
Zugehörige Diagramme	Abbildung 20: Aktivitätsdiagramm TUC_PKI_006 "OCSP-Abfrage"

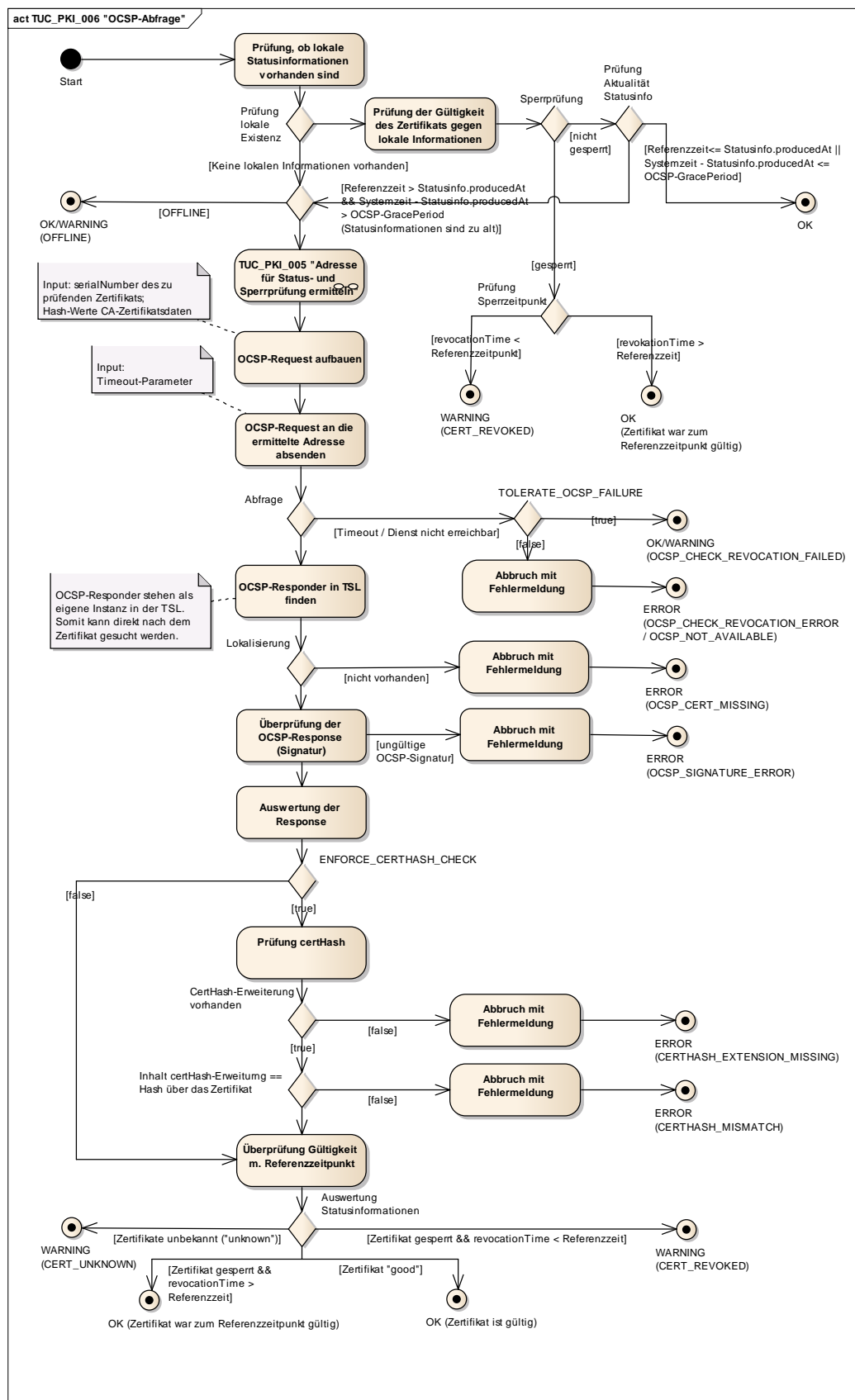


Abbildung 19: Aktivitätsdiagramm TUC_PKI_006 „OCSP-Abfrage“

8.3.2.3 TUC_PKI_021 „CRL-Prüfung“

☒ GS-A_4900 TUC_PKI_021 “CRL-Prüfung”

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

Tabelle 98: TUC_PKI_021 „CRL-Prüfung“

Element	Beschreibung
Name	TUC_PKI_021 „CRL-Prüfung“
Beschreibung	Dieser Use Case beschreibt den Prozess zur Validierung einer CRL (Certificate Revocation List) sowie den Prozess zur Ermittlung der Sperrinformationen zu einem End-Entity-Zertifikat mittels einer CRL.
Anwendungsumfeld	Use Case für den Anwendungsfall zur Prüfung der Sperrinformationen eines End-Entity-Zertifikats.
Vorbedingungen	Ein End-Entity-Zertifikat (mathematisch und zeitlich gültig) Eine CRL ist vorhanden oder kann heruntergeladen werden.
Auslöser	TUC_PKI_018 "Zertifikatsprüfung in der TI "
Eingangsdaten	CRL End-Entity-Zertifikatsdaten (Zertifikats-Seriennummer, CertificateIssuer) Timeout-Parameter (alternativ zu CRL) CRL-Downloadpunkt-Adresse (optional, alternativ zu CRL)
Komponenten	System (nur Konnektor)
Ausgangsdaten	Status der Prüfung
Referenzen	[COMMON-PKI#Part1#4], [COMMON-PKI#Part5#2.3], [RFC5280#5.2.5.], [RFC5280#5.3.3.]
Standardablauf	<ol style="list-style-type: none"> 1. [System:] Selektion der CRL 2. [System:] Prüfen der zeitlichen Gültigkeit der CRL (Systemzeit < crl.NextUpdate) 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). 4. [System:] Für eine indirekte CRL wird das zugehörige CRL-Signer-Zertifikat 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. 5. [System:] Prüfung der Signatur der CRL 6. [System:] Auswertung der CRL-Einträge. Es wird nach der Zertifikatsseriennummer des zu überprüfenden End-Entity-Zertifikats in der CRL gesucht. 7. [System:] Falls einer oder mehrere Einträge gefunden wurden, wird die CRL-Entry-Erweiterung „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. 8. [System:] Rückmeldung, dass das Zertifikat nicht in der Sperrliste

Element	Beschreibung
	<p>enthalten ist.</p> <p>9.</p> <p>[System:] Ende des Use Case</p>
Varianten/Alternativen	<p>1a. Die CRL ist nicht im System vorhanden und der CRL-Downloadpunkt unbekannt.</p> <p>1a1.</p> <p>[System:] Ermittlung des TSL-Eintrags der CA, welche das End-Entity-Zertifikat herausgegeben hat. (TUC_PKI_003 „CA Zertifikat in TSL finden“)</p> <p>1a2.</p> <p>[System:] Ermittlung des CRL-Downloadpunktes aus dem „Service-SupplyPoint“ des TSL-Service Eintrags (TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln").</p> <p>1a3.</p> <p>[System:] Herunterladen der CRL aus der ermittelten Adresse. Der Timeout-Parameter definiert hier, zu welchem Zeitpunkt das System ein Timeout bei Nichterreichbarkeit des Dienstes meldet.</p> <p>1b. Die CRL ist nicht im System vorhanden, der CRL-Downloadpunkt ist aber schon bekannt.</p> <p>1b1. [System:] Weiter mit 1a3.</p> <p>4a.</p> <p>[System:] Falls Schritt 3 ergeben hat, dass es sich um eine direkte CRL handelt, wird das Zertifikat der CA ermittelt, welches das End-EntityZertifikat ausgestellt hat.</p> <p>7a.</p> <p>[System:] Falls Schritt 3 ergeben hat, dass es sich um eine direkte CRL handelt, wird Schritt 7 übersprungen.</p> <p>8a.</p> <p>[System:] Zertifikat ist gesperrt. Rückmeldung an das System. (CERT_REVOKED)</p>
Fehlerfälle	<p>1a3a.</p> <p>[System:] Die CRL kann nicht heruntergeladen werden. (CRL_DOWNLOAD_ERROR)</p> <p>2a.</p> <p>[System:] Die Prüfung der zeitlichen Gültigkeit der CRL ergibt, dass die CRL abgelaufen ist (Systemzeit > crl.NextUpdate) (CRL_OUTDATED_ERROR)</p> <p>4b.</p> <p>[System:] CRL-Signer-Zertifikat nicht in TSL-Informationen enthalten. Abbruch mit Fehlermeldung. (CRL_SIGNER_CERT_MISSING)</p> <p>5a.</p> <p>[System:] Signatur der CRL ist nicht gültig. (CRL_SIGNATURE_ERROR)</p> <p>6a.</p> <p>[System:] Die CRL ist fehlerhaft aufgebaut und kann nicht geprüft werden.</p> <p>7a.</p> <p>[System:] Die CRL ist fehlerhaft aufgebaut und ihre Einträge können nicht ausgewertet werden.</p> <p>8b.</p> <p>[System:] Die CRL-Einträge sind fehlerhaft aufgebaut und können nicht weiter geprüft werden.</p>
Technische Fehlermeldung	<p>1a3a.</p> <p>[System:] Fehlermeldung CRL_DOWNLOAD_ERROR</p> <p>2a.</p> <p>[System:] Fehlermeldung CRL_OUTDATED_ERROR.</p> <p>4b.</p> <p>[System:] Fehlermeldung CRL_SIGNER_CERT_MISSING</p>

Element	Beschreibung
	<p>5a. [System:] Fehlermeldung CRL_SIGNATURE_ERROR</p> <p>6a. [System:] Fehlermeldung CRL_CHECK_ERROR</p> <p>7a. [System:] Fehlermeldung CRL_CHECK_ERROR</p> <p>8b. [System:] Fehlermeldung CRL_CHECK_ERROR</p>
Anmerkungen, Bemerkungen	<p>Dieser TUC kommt z.B. bei der Konzentration-Zertifikatsprüfung zur Anwendung.</p> <p>Der Downloadpunkt der CRL ist aus dem Internet erreichbar.</p> <p>Als Übertragungsprotokoll für den allfälligen Download ist „HTTP“ zu verwenden.</p> <p>Die Schritte 1-5 beinhalten die Validierung der CRL. Diese können vorgängig durchgeführt werden und müssen also nicht bei jeder einzelnen CRL-Prüfung eines End-Entity-Zertifikats durchlaufen werden, solange gewährleistet ist, dass die CRL zeitlich gültig ist.</p>
Zugehörige Diagramme	Abbildung 21: Aktivitätsdiagramm TUC_PKI_021 "CRL-Prüfung"

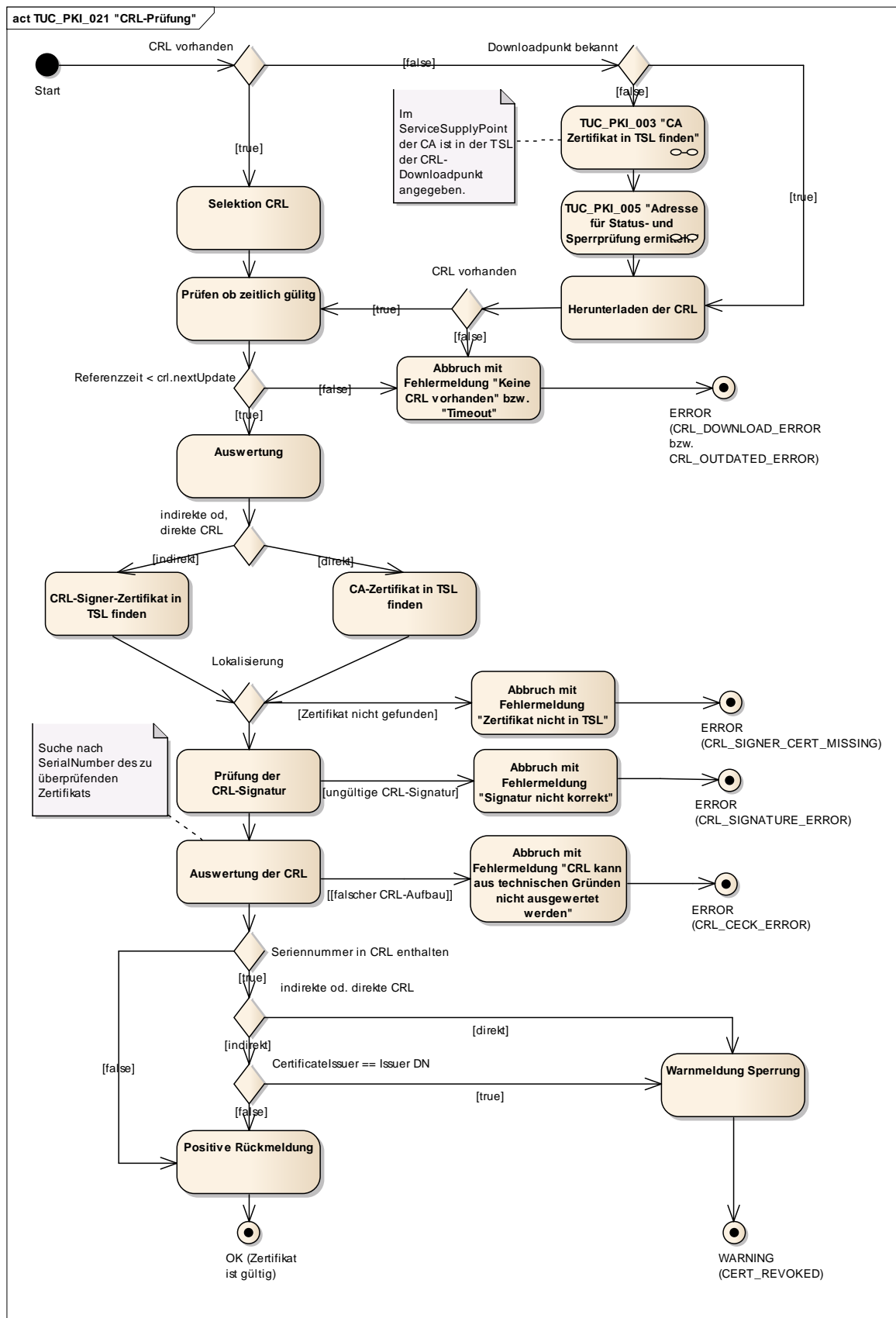


Abbildung 20: Aktivitätsdiagramm TUC_PKI_021 „CRL-Prüfung“

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 TUC_PKI_009: Rollenermittlung**

Die Produkttypen der TI, die Zertifikate prüfen, **MÜSSEN** TUC_PKI_009 zur Ermittlung der Rolle der Identität umsetzen. ☒

Tabelle 99: TUC_PKI_009 „Rollenermittlung“

Element	Beschreibung
---------	--------------

Element	Beschreibung
Name	TUC_PKI_009 „Rollenermittlung“
Beschreibung	Die Rolle einer Identität steht im jeweiligen Zertifikat. Dieser Use Case beschreibt die Ermittlung dieser Rolle aus dem Zertifikat. Jede Rolle wird in der Struktur <code>professionInfo</code> als OID gespeichert (siehe Kap 4.4, 4.5, 4.6). In allen Zertifikaten, die eine Rolle besitzen, steht diese in der Extension Admission, aus welcher der OID ausgelesen wird.
Anwendungsumfeld	System, das spezifische Inhalte von Zertifikaten verwendet
Vorbedingungen	Gültiges End-Entity-Zertifikat
Auslöser	Zertifikatsprüfung in der TI TUC_PKI_018 "Zertifikatsprüfung in der TI ", TUC_PKI_030 "QES-Zertifikatsprüfung"
Eingangsdaten	End-Entity-Zertifikatsdaten
Komponenten	System
Ausgangsdaten	OID der Rolle
Referenzen	[Common-PKI#Part1#3.1]
Standardablauf	<ol style="list-style-type: none"> 1. [System:] Prozess zur Ermittlung der Rolle beginnt 2. [System:] Extension Admission aus dem Zertifikat auslesen. 3. [System] Admission ist vorhanden und die Rolle aus dem Feld <code>professionOIDs</code> ermittelt. Sind weitere Einträge <code>professionInfo</code> enthalten, wird dieser Schritt so oft durchlaufen, bis alle <code>professionOIDs</code> ermittelt sind. 4. [System:] Mindestens eine OID ist vorhanden und wird zurück geliefert. Bei mehreren OID wird die Liste der OID als Rückgabewert geliefert. Ende des Use Case mit vorhandener Rolle
Varianten/Alternative n	<ol style="list-style-type: none"> 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.
Technische Fehlermeldung	Das System meldet entsprechende Fehlercodes.
Anmerkungen	Die Rolle in der Extension Admission befindet sich im Feld <code>professionOIDs</code> und ist als OID abgelegt. Die genaue Festlegung der OID wird im Dokument [gemSpec_OID] spezifiziert. Syntax der Extension Admission siehe [Common-PKI#Part1#3.1]
Zugehörige Diagramme	Abbildung 22 Aktivitätsdiagramm TUC_PKI_009 „Rollenermittlung“

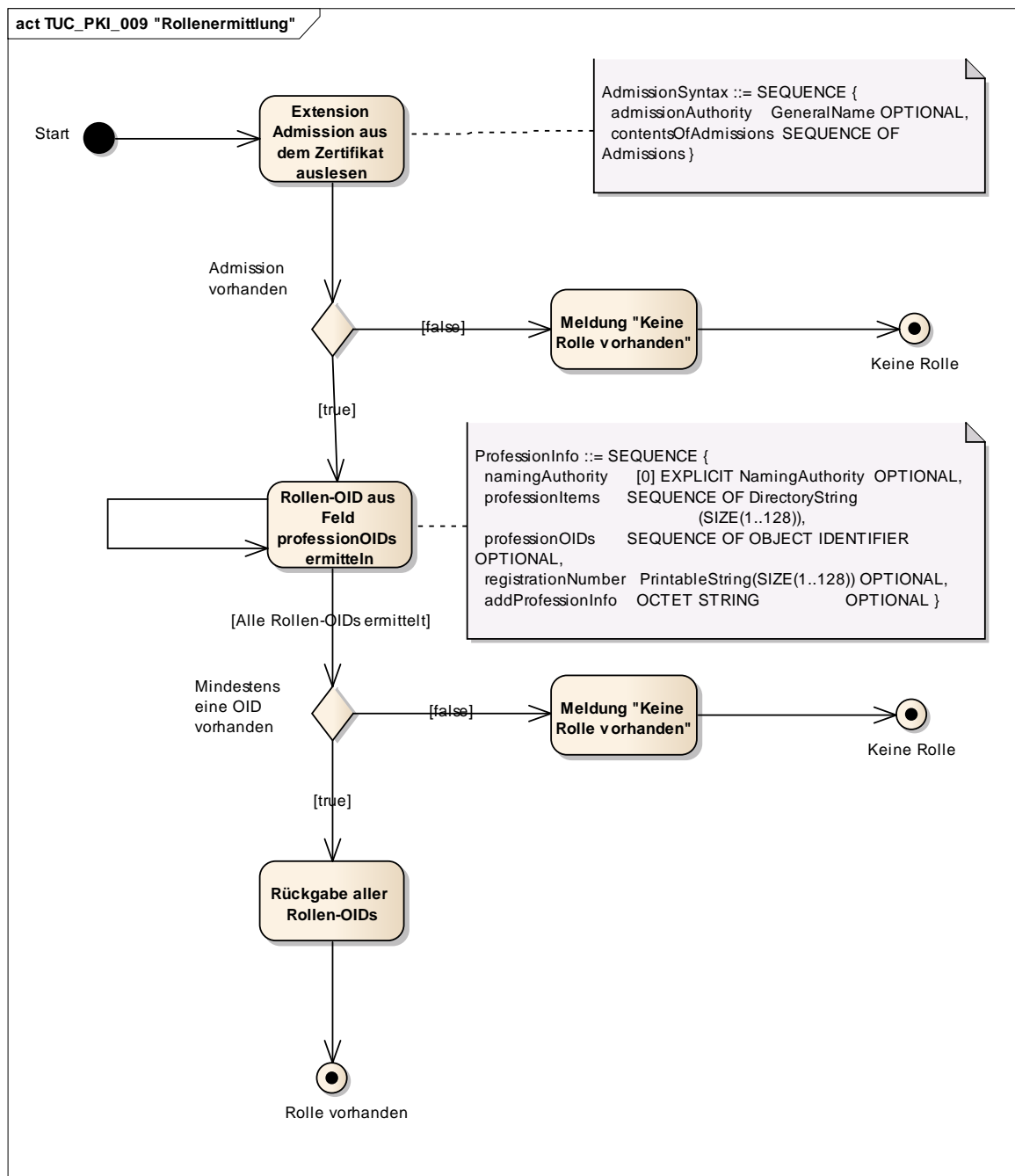


Abbildung 21: Aktivitätsdiagramm TUC_PKI_009 „Rollenermittlung“

8.3.3.3 TUC_PKI_007 „Prüfung Zertifikatstyp“

☒ GS-A_4749 TUC_PKI_007: Prüfung Zertifikatstyp

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

Tabelle 100: 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.
Anwendungsumfeld	System, das spezifische Inhalte von Zertifikaten verwendet
Vorbedingungen	Gültiges End-Entity-Zertifikat
Auslöser	TUC_PKI_018 "Zertifikatsprüfung in der TI "
Eingangsdaten	<ul style="list-style-type: none"> Das zu prüfende Zertifikat PolicyList
Komponenten	System
Ausgangsdaten	<ul style="list-style-type: none"> Status der Prüfung OID des Zertifikatstyps
Referenzen	<p>[RFC5280], [Common-PKI#2.2]</p> <p>Für weitere Erläuterungen zum Parameter „PolicyList“ siehe [Common-PKI#Part5], Kapitel 2.2 Validating the Certificate Path. In der TSL werden OIDs für Zertifikatstypen benutzt, um anzuzeigen, welche Typen von Zertifikaten unter einer CA ausgestellt werden dürfen. Diese OIDs werden jeweils im Element „ServiceInformationExtensions“ eingefügt, s. [gemSpec_TSL#7.3.2.1].</p>
Standardablauf	<ol style="list-style-type: none"> [System:] Start des Prozesses zur Ermittlung des Zertifikatstyps. [System:] Zertifikat laden [System:] Auswahl der CertificatePolicies aus dem Zertifikat [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. [System:] Selektion der CertPolicyId aus dem Element PolicyInformation [System:] Prüfung der OID aus dem Zertifikat gegen Liste der Zertifikatstyp-OIDs aus dem Parameter PolicyList der Eingangsdaten. [System:] Übereinstimmung der OIDs und Ende des Use Case mit Rückmeldung des logischen Wertes TRUE. Mit dem ersten OID-Match wird der TUC beendet und die geforderte Bedingung als erfüllt gewertet.
Varianten/Alternativen	<ol style="list-style-type: none"> 6a. [System:] Keine Übereinstimmung, nächstes Element PolicyInformation des Zertifikates wird analysiert. Wiederholung des Vorgangs ab Schritt 4.
Fehlerfälle/Warnungen	<ol style="list-style-type: none"> 4a. [System:] Abbruch und Rückmeldung. Kein Element PolicyIdentifier vorhanden. (CERT_TYPE_INFO_MISSING) 7a. [System:] Abbruch und Rückmeldung. Ende der SEQUENCE ist erreicht und es wurde keine Übereinstimmung festgestellt. (CERT_TYPE_MISMATCH)

Element	Beschreibung
Technische Fehlermeldung	Das System meldet entsprechende Fehlercodes.
Anmerkungen	Der Aufbau der Extension CertificatePolicies ist in Kapitel 4.8.3.3 beschrieben. Für die Speicherung des Zertifikatstyps enthält das Element PolicyInformation kein Unterelement policy-Qualifier.
Zugehörige Diagramme	Abbildung 23 Aktivitätsdiagramm TUC_PKI_007 "Prüfung Zertifikatstyp"

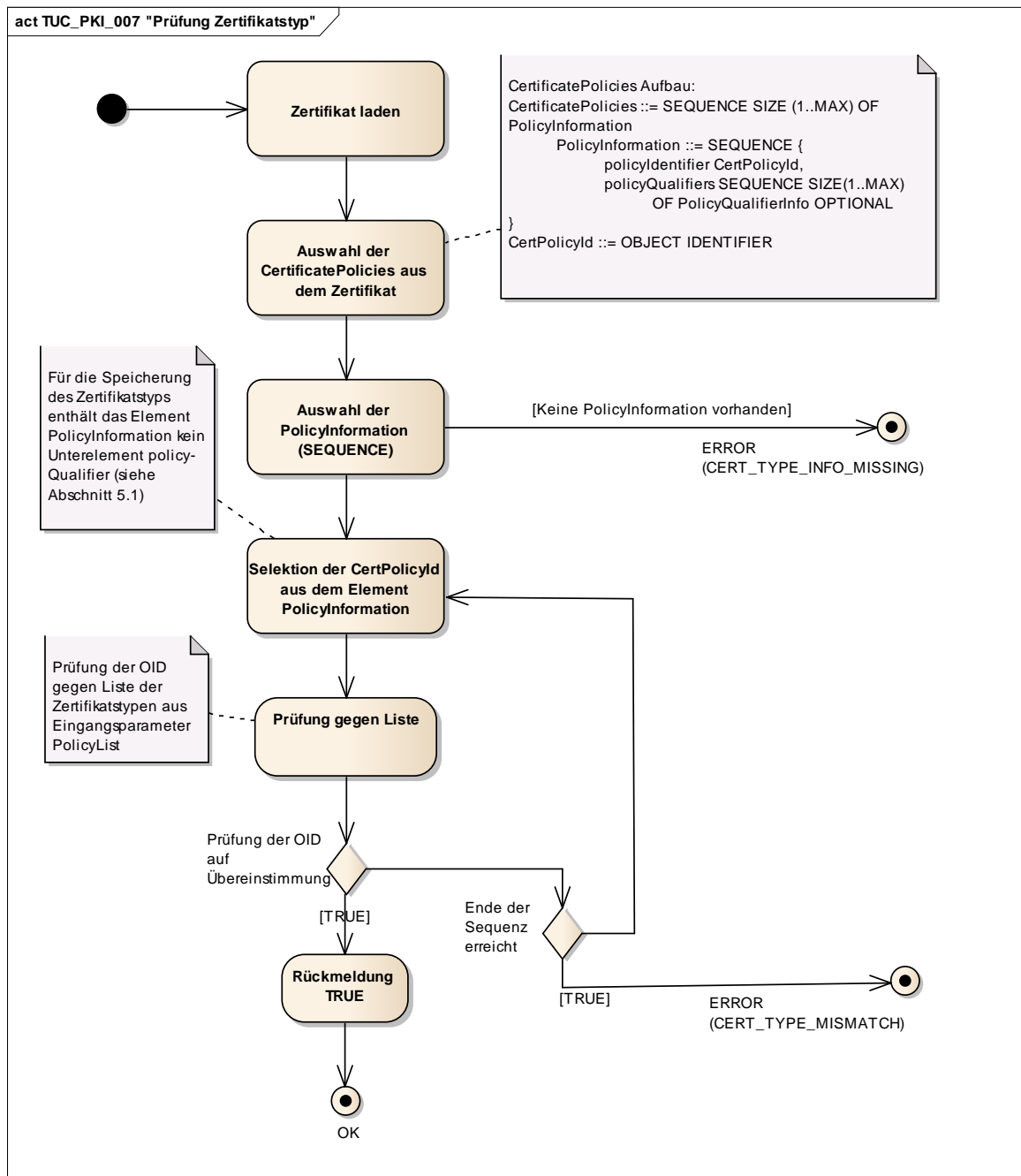


Abbildung 22: Aktivitätsdiagramm TUC_PKI_007 „Prüfung Zertifikatstyp“

8.3.4 Weitere Prüfungen

8.3.4.1 Umgang mit kritischen Extensions

☒ GS-A_4661 kritische Erweiterungen in Zertifikaten

Zertifikats-prüfenden Komponenten MÜSSEN kritische Zertifikatserweiterungen gemäß [RFC5280] und [Common-PKI] verarbeiten. ☒

8.4 Überprüfung der Zertifikate auf Netzwerk- und Transportebene

8.4.1 TLS-Verbindungsaufbau

☒ GS-A_4662 Bedingungen für TLS-Handshake

Produkttypen der TI, die TLS nutzen, MÜSSEN sicherstellen, dass TLS-Applikationsdaten (d. h. TLS-Nutzdaten, wie z. B. die Protokollschicht HTTP, LDAP, SMTP, IMAP oder POP3) nur ausgetauscht werden, wenn im Falle von einseitiger Authentisierung das Serverzertifikat aktuell gültig ist oder im Falle von gegenseitiger Authentisierung beide Zertifikate aktuell gültig sind und zusätzlich in beiden Fällen der TLS-Handshake erfolgreich absolviert wurde. ☒

☒ GS-A_4663 Zertifikats-Prüfparameter für den TLS-Handshake

Produkttypen der TI, die TLS nutzen, MÜSSEN sicherstellen, dass für den TLS-Verbindungsaufbau die in Tab_PKI_273 beschriebene Nutzung der Eingangsdaten-Parameter von TUC_PKI_018 „Zertifikatsprüfung“ für diese Zertifikatsprüfungen verwendet werden. ☒

Tabelle 101: 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 SubjectDN 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.

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

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

8.5.1 TUC_PKI_030 „QES-Zertifikatsprüfung“

Tabelle 102: 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.
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	aktuelle TSL-Informationen im Truststore, eine aktuell gültige BNetzA-VL.
Auslöser	Zertifikats-Check
Eingangsdaten	<ul style="list-style-type: none"> • QES-Zertifikat • Liste der korrespondierenden Attributzertifikate (optional, zum QES-Zertifikat als Basis-Zertifikat) • Referenzzeitpunkt (refTime): Zeitpunkt, für den das Zertifikat geprüft werden soll • PolicyList: Liste der im aktuellen Aufruf zulässigen Zertifikatstyp-OIDs. Die Liste muss mindestens eine OID enthalten. • 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) • TSL-Informationen (Adressen für OCSP-Abfragen) • Timeout-Parameter für OCSP-Abfragen (Default: 10s)
Komponenten	System
Ausgangsdaten	Status der Prüfung, OCSP-Response zum angefragten QES-Zertifikat, im Zertifikat enthaltene Rollen-OIDs
Standardablauf	<p>0. Die QES-Zertifikatsprüfung setzt sich aus den in [Common-PKI#Part5] und [Common-PKI#9] beschriebenen Schritten zusammen. Die Prüfungen der korrespondierenden Attributzertifikate müssen die Vorgaben gemäß [baekAttr], [RFC5755] und [Recommendation ITU-T X.509 ISO/IEC 9594-8] berücksichtigen. (Zusätzlich zu den in [Common-PKI] beschriebenen Schritten werden folgende Schritte durchgeführt:</p> <ol style="list-style-type: none"> 1. [System:] Prüfung, ob das CA-Zertifikat für die QES-Prüfung zum Referenzzeitpunkt in der BNetzA-VL gemäß [eIDAS] und [ETSI TS 119 612#5.5.4 und #Annex J] qualifiziert ist. 2. [System:] Prüfung, ob das ausstellende QES-CA-Zertifikat des QES-Zertifikates in der TSL enthalten ist (TUC_PKI_003 "CA-Zertifikat in TSL-Informationen finden").

Element	Beschreibung
	<p>3. [System:] Prüfung, ob das QES-CA-Zertifikat (zum Referenzzeitpunkt) in der TSL als gültig gekennzeichnet ist.</p> <p>4. [System:] Ermittlung der OCSP-Adresse aus der TSL (TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln")</p> <p>5. [System:] Die abzufragenden Statusinformationen zu QES-Zertifikaten werden unter Verwendung der extrahierten OCSP-Adressen eingeholt.</p> <p>6. [System:] Ermittlung der Rolle (TUC_PKI_009 "Rollenermittlung")</p> <p>7. [System:] Prüfung, ob eine der übergebenen Zertifikatstyp-OIDs (aus der Parameter PolicyList) im Zertifikat enthalten ist (TUC_PKI_007 "Prüfung Zertifikatstyp"). Zur Prüfung muss die Liste (PolicyList s.o.) mindestens eine OID enthalten.</p> <p>8. 7. [System:] Ende des Use Case mit Rückgabe des/der im Zertifikat enthaltenen Rollen-OID(s)</p>
Varianten/Alternativen	<p>Der Standardablauf stellt die üblichen Schritte dar, die durchgeführt werden müssen. Eine Trennung in zwei Prozesse oder eine Umstrukturierung, bei der alle notwendigen Schritte erfolgen, ist zulässig.</p> <p>0a. [System:] Wird im optionalen Parameter Nonce ein Wert übergeben, dann muss für QES-Zertifikate dieser Wert als OCSP-Parameter in den OCSP-Request integriert und im Response geprüft werden.</p> <p>4a . [System:] Der Offline-Modus ist aktiviert. Es werden keine Statusinformationen eingeholt. (Schritte 4 und 5 entfallen.)</p> <p>5a . [System:] Eine OCSP-Response zu dem zu prüfenden Zertifikat wurde im Aufruf mit übergeben. Falls dieses zum Referenzzeitpunkt gültig ist, werden keine OCSP-Requests erzeugt, sondern die beigefügte OCSP-Response zur weiteren Prüfung verwendet.</p>
Fehlerfälle	<p>In jedem der beschriebenen Schritte können Fehler auftreten. Diese sind durch das System zu melden und der Prozess muss beendet werden.</p> <p>0b. In [Common-PKI#Part5] und [Common-PKI#9] sind Fehlerfälle für die QES-Zertifikatsprüfung und die Prüfung von Attributzertifikaten beschrieben. Diese beinhalten:</p> <ul style="list-style-type: none"> - Prüfung von QCStatements: QC_STATEMENT_ERROR - Prüfung von QES-Basiszertifikat assoziierten Attributzertifikaten: ATTR_CERT_MISMATCH. <p>0c. Wenn die in einer OCSP-Response zurückgelieferte Nonce nicht mit der Nonce des OCSP-Requests für ein QES-Zertifikat übereinstimmt, wird die Prüfung abgebrochen mit der Fehlermeldung OCSP_NONCE_MISMATCH.</p> <p>1a. Ist das QES-CA-Zertifikat in der BNetzA-VL nicht vorhanden oder zum Referenzzeitpunkt nicht mit einem gültigen Status gekennzeichnet, muss der TUC mit einer Fehlermeldung CA_CERTIFICATE_NOT_QES_QUALIFIED abbrechen.</p> <p>3a. [System:] QES-CA-Zertifikat des QES-Zertifikates ist in der TSL als revoked gekennzeichnet und QES-Zertifikat ist nach Sperrzeitpunkt erstellt worden. Abbruch mit Fehlermeldung (CA_CERTIFICATE_REVOKED_IN_TSL).</p>

Element	Beschreibung
	<p>5b. [System:]. Der zuständige OCSP-Responder ist nicht erreichbar. Abbruch mit Fehlermeldung (OCSP_NOT_AVAILABLE).</p> <p>5c. [System:] OCSP-Responses zu dem zu prüfenden Zertifikat wurden im Aufruf mit übergeben, ergaben bei den weiteren Prüfschritten jedoch kein gültiges Ergebnis. Eine erneute Prüfung wird in diesem Fall durchgeführt, als wären keine OCSP-Responses beigefügt. In den Rückgabewerten dieses TUC wird die Warnmeldung (PROVIDED_OCSP_RESPONSE_NOT_VALID) an die aufrufende Funktion übergeben.</p> <p>5d. System:] Warnmeldung, dass keine Online-Statusprüfung durchgeführt wurde (NO_OCSP_CHECK).</p>
Technische Fehlermeldung	Das System meldet entsprechende Fehlercodes.
Sicherheitsanforderungen	
Anmerkungen	<p>Gültige Status zu Schritt 1 sind gemäß [ETSI TS 119 612#5.5.4 und #Annex J] <i>granted, accredited, undersupervision, supervisionincession</i></p> <p>Die Einträge der QES-CA-Zertifikate in der BNetzA-VL besitzen gemäß [ETSI TS 119 612#5.5.1.1] die Extension AdditionalServiceInformation http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures.</p> <p>Die Einträge der QES-CA-Zertifikate in der TSL und der BNetzA-VL besitzen den ServiceTypeldentifizier http://uri.etsi.org/TrstSvc/Svctype/CA/QC.</p> <p>Schritt 2 stellt eine TI-spezifische Sperrprüfung des QES-CA-Zertifikats gemäß Kettenmodell dar. Vgl. Kap. 8.1.1 Initialisierung TI-Vertrauensraum.</p> <p>Schritt 5 enthält die QES-spezifischen Statusprüfungen.</p>
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 103: 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	<ul style="list-style-type: none"> optional: neu eingebrachte BNetzA-VL-Datei
Komponenten	System
Ausgangsdaten	Status des Prozesses
Referenzen	[ETSI_TS_119_612] [XML] [XMLSig]
Standardablauf	<p>Der Standardablauf stellt die Prüfungen dar, die vollzogen werden müssen. Die Reihenfolge der Schritte ist aber nicht normativ. Eine Trennung in zwei Prozesse oder eine Umstrukturierung, bei der alle notwendigen Prüfungen erfolgen, ist zulässig.</p> <ol style="list-style-type: none"> 1. [System:] System startet die Aktualisierung der BNetzA-VL 2. [System:] Primäre BNetzA-VL Hash Download-Adresse aus der TSL extrahieren (s. [gemSpec_TSL#7.5]). 3. [System:] Von der im vorherigen Schritt ermittelten Downloadadresse den aktuellen BNetzA-VL Hashwert vom TSL-Dienst herunterladen. 4. [System:] Heruntergeladenen BNetzA-VL Hashwert mit dem Hashwert der aktuell im System gespeicherten BNetzA-VL (falls vorhanden) vergleichen. Falls die Hashwerte verschieden sind oder im System noch keine BNetzA-VL vorhanden ist muss die BNetzA-VL im System aktualisiert werden. 5. [System:] Primäre BNetzA-VL Download-Adresse aus der TSL extrahieren (s. [gemSpec_TSL#7.5]). 6. [System:] Von der ermittelten Downloadadresse die 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

Element	Beschreibung
	<p>ist. Die Identifizierung des Zertifikats erfolgt durch</p> <ul style="list-style-type: none"> Suche nach einem TSPService mit ServiceTypIdentifier für „BNetzA-VL“ gem. [gemSpec_TSL#7.3.2] und Vergleich des Elements X509Certificate in zugehöriger Digitalld mit dem BNetzA-VL-Signer-Zertifikat aus Schritt 10 <p>12. [System:] Die XML-Signatur der BNetzA-VL-Datei mittels in der TSL gefundenem BNetzA-VL-Signerzertifikat gem. [XAdES] prüfen.</p> <p>13. [System:] Die aktualisierte BNetzA-VL und deren Hashwert (falls vorhanden) sicher im System speichern. Ende des Use Cases.</p>
Varianten/Alternativen	<p>1a. [System:] Wenn eine BNetzA-VL-Datei als Eingangsparameter eingebracht wurde, dann wird diese Datei validiert und geprüft. Weiter mit Schritt 7.</p> <p>2a. [System:] Das Element ist nicht vorhanden. Weiter mit Schritt 3a.2</p> <p>3a. [System:] Das Herunterladen von der primären Downloadadresse schlägt fehl.</p> <p>3a.1 [System:] Das Herunterladen wird bis zu drei Mal wiederholt versucht (insgesamt wird der Vorgang also maximal vier Mal ausgeführt). Falls erfolgreich, weiter mit Schritt 4.</p> <p>3a.2 [System:] Backup BNetzA-VL Hash Download-Adresse aus der TSL extrahieren (s. [gemSpec_TSL#7.5]). Falls nicht erfolgreich, weiter mit Schritt 5.</p> <p>3a.3 [System:] Das Herunterladen wird von der Backup Downloadadresse ausgeführt. Falls erfolgreich, weiter mit Schritt 4.</p> <p>3a.4 [System:] Das Herunterladen von der Backup Downloadadresse wird bis zu drei Mal wiederholt versucht (insgesamt wird der Vorgang also maximal vier Mal ausgeführt). Falls erfolgreich, weiter mit Schritt 4. Falls nicht erfolgreich, weiter mit Schritt 5.</p> <p>4a. [System:] Die verglichenen Hashwerte sind identisch. In diesem Fall ist die im System gespeicherte BNetzA-VL aktuell. Ende des Use Cases ohne Fehler.</p> <p>5b. [System:] Das Element ist nicht vorhanden. Weiter mit Schritt 6a.2</p> <p>6a. [System:] Das Herunterladen von der primären Downloadadresse schlägt fehl.</p> <p>6a.1 [System:] Das Herunterladen wird bis zu drei Mal wiederholt versucht (insgesamt wird der Vorgang also maximal vier Mal ausgeführt). Falls erfolgreich, weiter mit Schritt 7.</p> <p>6a.2 [System:] Backup BNetzA-VL Download-Adresse aus der TSL extrahieren</p>

Element	Beschreibung
	<p>(s. [gemSpec_TSL#7.5]).</p> <p>6a.3 [System:] Das Herunterladen wird von der Backup Downloadadresse ausgeführt. Falls erfolgreich, weiter mit Schritt 7.</p> <p>6a.4 [System:] Das Herunterladen von der Backup Downloadadresse wird bis zu drei Mal wiederholt versucht (insgesamt wird der Vorgang also maximal vier Mal ausgeführt). Falls erfolgreich, weiter mit Schritt 7.</p>
Fehlerfälle	<p>Ein Abbruch des TUC führt nur dazu, dass keine neue BNetzA-VL gespeichert wird. Er hat keinen Einfluss auf die Gültigkeit der bestehenden BNetzA-VL. Das System muss dies jedoch protokollieren.</p> <p>6a.2a [System:] Das Element ist nicht vorhanden. Ende des Use Case mit der Fehlermeldung VL_UPDATE_ERROR.</p> <p>6a.4a [System:] Das Herunterladen der BNetzA-VL ist fehlgeschlagen. Ende des Use Cases mit der Fehlermeldung VL_UPDATE_ERROR.</p> <p>7a. [System:] Die XML-Datei ist nicht wohlgeformt. Ende des Use Cases mit der Fehlermeldung VL_UPDATE_ERROR.</p> <p>8a. [System:] Die XML-Schema-Validierung liefert einen Fehler. Ende des Use Cases mit der Fehlermeldung VL_UPDATE_ERROR.</p> <p>9a. [System:] Die Aktualitäts-Prüfung ergibt, dass die BNetzA-VL abgelaufen ist (nextUpdate < aktuelles Datum). Ende des Use Cases mit der Fehlermeldung VL_UPDATE_ERROR.</p> <p>10a. [System:] Das BNetzA-VL-Signer-Zertifikat lässt sich nicht aus der BNetzA-VL-Datei extrahieren. Ende des Use Cases mit der Fehlermeldung VL_UPDATE_ERROR.</p> <p>11a. BNetzA-VL-Signerzertifikat ist nicht in der TSL enthalten. Ende des Use Case mit der Fehlermeldung VL_UPDATE_ERROR.</p> <p>12a. [System:] Die Signatur ist nicht gültig. Ende des Use Cases mit der Fehlermeldung XML_SIGNATURE_ERROR.</p>
Technische Fehlermeldung	<p>Aktualisierung der BNetzA-VL nicht möglich. Das System meldet entsprechende Fehlercodes.</p>
Sicherheitsanforderungen	<p>Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.</p>
Anmerkungen	<p>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.</p>
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 einen 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 104: 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-CA lässt sich nicht extrahieren		TSL_SIG_CERT_EXTRACTION_ERROR
1005	Error	Technical	Element „PointersToOtherTSL“ nicht vorhanden		TSL_DOWNLOAD_ADDRESS_ERROR
1006	Error	Technical	TSL-Downloadadressen wiederholt nicht erreichbar		TSL_DOWNLOAD_ERROR
1007	Error	Security	Vergleich der ID und SequenceNumber entspricht nicht der Vergleichsvariante 6a		TSL_ID_INCORRECT
1008	Warning	Security	Die TSL ist nicht mehr aktuell		VALIDITY_WARNING_1
1009	Warning	Security	Überschreitung des Elements NextUpdate um TSL-Grace-Period		VALIDITY_WARNING_2
1010	Warning	Security	<i>Veraltet: Diese Warnmeldung ist redundant zu VALIDITY_WARNING_1 (Code 1008). Sie soll deshalb nicht mehr verwendet werden.</i>		TSL_NEXTUPDATE_EXPIRED
1011	Error	Technical	TSL-Datei nicht wellformed		TSL_NOT_WELLFORMED
1012	Error	Technical	Schemata der TSL-Datei nicht korrekt		TSL_SCHEMA_NOT_VALID
1013	Error	Security	Signatur ist nicht gültig		XML_SIGNATURE_ERROR
1016	Error	Security	KeyUsage ist nicht vorhanden bzw. entspricht nicht der vorgesehenen KeyUsage		WRONG_KEYUSAGE

Code	Severity	ErrorType	ErrorText	Detail	Meldungskürzel
1017	Error	Security	ExtendedKeyUsage entspricht nicht der vorgesehenen ExtendedKeyUsage		WRONG_EXTENDEDKEYUSAGE
1018	Error	Security	Zertifikatstyp-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	AuthorityKeyIdentifier des End-Entity-Zertifikats von SubjectKeyIdentifier des CA-Zertifikats unterschiedlich		AUTHORITYKEYID_DIFFERENT
1024	Error	Security	Zertifikats-Signatur ist mathematisch nicht gültig.		CERTIFICATE_NOT_VALID_MATH
1026	Error	Technical	Das Element „ServiceSupplyPoint“ 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_FAIL URE=true	OCSP_CHECK_REVOCATION_FAILED
1029	Error	Technical	Die OCSP-Prüfung konnte nicht durchgeführt werden (2)	TOLERATE_OCSP_FAIL URE=false	OCSP_CHECK_REVOCATION_ERROR
1030	Error	Security	OCSP-Zertifikat nicht in TSL-Informationen enthalten		OCSP_CERT_MISSING
1031	Error	Security	Signatur der Response ist nicht gültig.		OCSP_SIGNATURE_ERROR
1032	Error	Technical	OCSP-Responder nicht verfügbar		OCSP_NOT_AVAILABLE
1033	Error	Security	Kein Element PolicyInformation vorhanden		CERT_TYPE_INFO_MISSING
1034	Error	Technical	<i>Veraltet: Diese Fehlermeldung wird nicht mehr verwendet. Stattdessen ist der Fehlercode 1032 zu verwenden.</i>		OCSP_PROXY_NOT_AVAILABLE

Code	Severity	ErrorType	ErrorText	Detail	Meldungskürzel
1036	Error	Security	Das Zertifikat ist ungültig. Es wurde nach der Sperrung der ausgebenden CA ausgestellt.		CA_CERTIFICATE_REVOKED_IN_TSL
1039	Warning	Security	Warnung, dass Offline-Modus aktiviert ist und keine OCSP-Statusabfrage durchgeführt wurde		NO_OCSP_CHECK
1040	Error	Security	Bei der Onlinestatusprüfung 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-Signer-CA-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 QCStatements aufgetreten (z. B. nicht vorhanden, obwohl gefordert).		QC_STATEMENT_ERROR
1050	Warning	Technical	Die einem TUC zur Zertifikatsprüfung beigefügte OCSP-Response zu dem zu prüfenden Zertifikat kann nicht erfolgreich gegen das Zertifikat validiert werden.		PROVIDED_OCSP_RESPONSE_NOT_VALID

Code	Severity	ErrorType	ErrorText	Detail	Meldungskürzel
1051	Error	Security	Die in einem OCSP-Response zurückgelieferte Nonce stimmt nicht mit der Nonce des OCSP-Requests überein.		OCSP_NONCE_MISMATCH
1052	Error	Security	Attribut-Zertifikat kann dem übergebenen Basis-Zertifikat nicht zugeordnet werden.		ATTR_CERT_MISMATCH
1053	Error	Technical	Die CRL kann nicht heruntergeladen werden.		CRL_DOWNLOAD_ERROR
1054	Error	Technical	Eine verwendete CRL ist zum aktuellen Zeitpunkt nicht mehr gültig.		CRL_OUTDATED_ERROR
1055	Error	Security	CRL-Signer-Zertifikat nicht in TSL-Informationen enthalten		CRL_SIGNER_CERT_MISSING
1057	Error	Security	Signatur der CRL ist nicht gültig.		CRL_SIGNATURE_ERROR
1058	Error	Technical	Die OCSP-Response enthält eine 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

8.7 Zertifikatsprüfung CVC

Die Zertifikatsprüfung von CV-Zertifikaten der Generation 1 (G1) ist stark vereinfacht gegenüber der Prüfung von X.509-Zertifikaten.

CV-Zertifikate sind für einen offline-Einsatz konzipiert, somit entfallen eine Sperrmöglichkeit und dadurch auch die Notwendigkeit der Sperrstatusprüfung. Eine zeitliche Gültigkeit wird im CV-Zertifikat nicht hinterlegt und kann demzufolge auch nicht abgeprüft werden.

Somit beschränkt sich die Prüfung auf die Prüfung der Vertrauenskette und die Signaturprüfung. Die Prüfschritte erfolgen komplett „intern“ durch das Betriebssystem der prüfenden Chipkarte.

☒ **GS-A_4668 Prüfung der mathematischen Korrektheit bei CV-Zertifikaten der Generation G1**

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN bei der Prüfung von CV-Zertifikaten der Generation 1 die Prüfung der mathematischen Korrektheit vornehmen, d. h. ob die Signatur des CV-Zertifikats mit dem öffentlichen Schlüssel der ausstellenden CVC-CA und ob die Signatur des CVC-CA-Zertifikats mit dem öffentlichen Root-Schlüssel der ausstellenden CVC-Root-CA erfolgreich geprüft werden kann. ☒

Nach einer erfolgreichen Prüfung ist die Authentizität eines in einem CV-Zertifikat enthaltenen öffentlichen Schlüssels einer Chipkarte gegeben und kann zu Authentisierungszwecken verwendet werden.

Die erfolgreiche Prüfung setzt voraus, dass die CV-Zertifikate der an der Authentisierung beteiligten Chipkarten unter dem gleichen Root-Schlüssel prüfbar sind. Andernfalls kann keine erfolgreiche Authentisierung durchgeführt werden.

8.8 Zertifikatsprüfung CV-Zertifikate der 2. Generation

Im Gegensatz zur Prüfung von CV-Zertifikaten der Generation 1 beschränkt sich die Prüfung von CV-Zertifikaten der Generation 2 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. 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 vor-

nehmen, 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 105: 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 106: 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 <ul style="list-style-type: none"> das CV-Zertifikat mathematisch korrekt gebildet ist und das Certificate Expiration Date (CXD) des CV-Zertifikats noch nicht überschritten ist.
Ein CV-Zertifikat C, das von einem Herausgeber der Generation 2 (TSP-CVC oder CVC-Root-CA) erzeugt wurde, ist gültig, wenn <ul style="list-style-type: none"> das CV-Zertifikat für den öffentlichen Schlüssels des Herausgebers gültig und

Gültigkeit eines CV-Zertifikats C
<ul style="list-style-type: none">• 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 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 in der BNetzA-VL und des Dienststatus (Servicestatus) der QES-CA in der TSL und BNetzA_VL (s. Kap. 8.5).

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 Statusprüfdienst QES gemäß den Vorgaben von eIDAS**

Der TSP-X.509 QES MUSS für den Statusprüfdienst die Vorgaben gemäß [eIDAS] erfüllen. ☒

☒ **GS-A_5050 gematik-Root-CA Statusprüfdienst im Internet**

Der Anbieter der gematik Root-CA MUSS im Internet einen OCSP-Dienst für die Statusauskünfte der CAs zur Verfügung stellen, die AUT-, ENC- und OSIG-Zertifikate zur Verwendung in HBA und SMC-B 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 oder SMC-B MUSS Zertifikatsstatusinformationen zu den ausgestellten X.509-Zertifikaten im Internet bereitstellen. ☒

☒ **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 nach [RFC2560] implementiert werden und
- bei allen anderen X.509-Zertifikaten gemäß [Common-PKI] implementiert werden, wobei die CertHash-Erweiterung (PositiveStatement) obligatorisch verwendet werden muss.

9.1.1.1.1 OCSP-Request

Der OCSP-Request ist komplett in [RFC2560] beschrieben, sowie mit Erweiterungen in [Common-PKI].

Wesentliches Merkmal zur Identifizierung des Zertifikats ist dessen Seriennummer. Der Herausgeber des Zertifikats wird über Hashwerte seines öffentlichen Schlüssels und seines Namens identifiziert. OCSP-Requests können gemäß den Standards signiert sein, dies wird (s. a. Abschnitt 9.1.2.1) in der TI allerdings nicht gefordert und deshalb diese Signaturen auch nicht geprüft.

☒ **GS-A_4674 OCSP-Requests gemäß [RFC2560] und [Common-PKI]**

Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN OCSP-Requests gemäß [RFC2560] und [Common-PKI] verarbeiten können. ☒

☒ **GS-A_4957 Beschränkungen OCSP-Request**

Produkttypen der TI, die Zertifikate prüfen, DÜRFEN (abweichend von [RFC2560]) 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. ☒

9.1.1.1.2 OCSP-Response

Die OCSP-Response ist komplett in [RFC2560] beschrieben, sowie mit Erweiterungen in [Common-PKI].

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 OCSP-Responses gemäß [RFC2560]**

Der TSP-X.509 nonQES (eGK) MUSS für Statusauskünfte zu X.509-Zertifikaten von eGKs OCSP-Responses gemäß [RFC2560] erzeugen. ☒

☒ **GS-A_4676 OCSP-Responses gemäß [Common-PKI]**

Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN für Statusauskünfte zu X.509-Zertifikaten außer für eGKs OCSP-Responses gemäß [Common-PKI] erzeugen. ☒

☒ **GS-A_5124 OCSP-Responses mit Parameter Nonce [Common-PKI]**

Der TSP-X.509 QES MUSS für Statusauskünfte zu X.509-Zertifikaten den Parameter „Nonce“ für OCSP-Responses gemäß [Common-PKI] unterstützen. ☒

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, TSP-X.509 QES 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 107: 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 108: 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, und

der Referenzzeitpunkt == Systemzeit ist:

(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 109: Tab_PKI_293 Status der OCSP Antworten

OCSP Antwort	Bedeutung
good	Der Zustand „good“ sagt aus, dass zum Zeitpunkt <code>thisUpdate</code> das Zertifikat nicht gesperrt war. Good sagt aber nichts über die Gültigkeitsdauer und Existenz des Zertifikates aus.

OCSP Antwort	Bedeutung
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 Statusprüfdienst - Positive Statement**

Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN sicherstellen, dass im Falle eines im Verzeichnisdienst vorhandenen X.509-Zertifikats (außer bei nicht-qualifizierten Zertifikaten einer eGK) die Common PKI [Common-PKI] private `SingleExtension` „**certHash**“ in den OCSP-Response des zu prüfenden X.509-Zertifikats eingestellt wird. ☒

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.

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.*

A1 – KZBV

Tabelle 110: 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> (die <TSP-ID> wird für Zertifikatsprofile dieses Sektors von der KZBV vergeben) (<TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>)	1	
organizationalUnitName	nicht belegt	0	

Element	Inhalt	Kar.	
	organizationName	Telematik-ID gemäss Freigabedaten der zuständigen KZV	1
	streetAddress	nicht belegt	0
	postalCode	nicht belegt	0
	localityName	nicht belegt	0
	stateOrProvinceName	nicht belegt	0
	countryName	siehe Kap 5.3.4	1
	andere Attribute		0
	subjectPublicKeyInfo	siehe Kap 5.3.4	
	extensions		critical
	SubjectKeyIdentifier {2 5 29 14}	siehe Kap 5.3.4	1 FALSE
	KeyUsage {2 5 29 15}	siehe Kap 5.3.4	1 TRUE
	SubjectAltNames {2 5 29 17}	rfc822Name type-id= {2 5 4 3}; value= ggf. überlange Institutionsnamen, Alternativnamen oder Ergänzungen	0-1 0-1 FALSE
	BasicConstraints {2 5 29 19}	siehe Kap 5.3.4	1 TRUE
	CertificatePolicies {2 5 29 32}	siehe Kap 5.3.4 zusätzlich: policyQualifierInfo	1 0 FALSE
	CRLDistributionPoints {2 5 29 31}	CDP des TSP für das betreffende Zertifikat	1 FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap 5.3.4	1 FALSE
	AuthorityKeyIdentifier {2 5 29 35}	siehe Kap 5.3.4	1 FALSE
	Admission {1 3 36 8 3 3}	admissionAuthority = {0=<von der KZBV benannte attributbestätigende Stelle - zuständige KZV>,C=DE} professionItem = Beschreibung zu <oid_zahnarztpraxis> gemäss [gemSpec_OID#GS- A_4443] professionOID = OID <oid_zahnarztpraxis> gemäss [gemSpec_OID#GS-A_4443] registrationNumber = <Telematik-ID 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	

Tabelle 111: Tab_SMCB_KZBV_KZV SMC-B-Zertifikate für KZV (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 KZBV	1	
title	nicht belegt	0	
surName	nicht belegt	0	
givenName	nicht belegt	0	
serialNumber	TI-weit eindeutiger Identifier der Karte z.B. in der Form: <TSP-ID>.<ICCSN> (<TSP-ID> gemäß Tab PKI_109 Werte für das Präfix <TSP-ID>)	1	
streetAddress	nicht belegt	0	
postalCode	nicht belegt	0	
localityName	nicht belegt	0	
stateOrProvinceName	nicht belegt	0	
organizationalUnitName	nicht belegt	0	
organizationName	Telematik-ID gemäß Freigabedaten der KZBV	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 KZV	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: policyIdentifier = <oid_policy_gem_or_cp_smeb_erprobung>	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	siehe Kap 5.3.4	1	FALSE

Element	Inhalt	Kar.	
	{2 5 29 35}		
	Admission {1 3 36 8 3 3}	admissionAuthority = {O=Kassenzahnärztliche Bundesvereinigung,C=DE} professionItem = <oid_leo_zahnaerzte> professionOID = <oid_leo_zahnaerzte> registrationNumber <Telematik-ID gemäß Freigabedaten der KZBV>	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 112: Tab_SMCB_TSP-ID Werte für das Präfix <TSP-ID>

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

A2 – 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 113: 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		

Element	Inhalt	Kar.	
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	TI-weit eindeutiger Identifier der Karte z.B. in der Form: <TSP-ID>.<ICCSN> nicht belegt	0	
organizationalUnitName	nicht belegt	0	
organizationName	9-stellige Betriebsstättennummer (z.B. „121234512“) der Praxis als eindeutige Nummer. Für privat abrechnende Ärzte wird hier eine 10-stellige Ersatznummer eingefügt.	1	
streetAddress	Strassen-Adresse der Institution (mehrere Wörter sind durch Blank getrennt)	0-1	
postalCode	Postleitzahl des Ortes der Institution (Deutsche PLZ werden 5-stellig abgebildet)	0-1	
localityName	Stadt des Institut-Standortes	0-1	
stateOrProvinceName	Bundesland des Institut-Standortes	0-1	
countryName	siehe Kap 5.3.4	1	
andere Attribute		0	
subjectPublicKeyInfo	siehe Kap 5.3.4		
extensions			critical
SubjectKeyIdentifier {2 5 29 14}	siehe Kap 5.3.4	1	FALSE
KeyUsage {2 5 29 15}	siehe Kap 5.3.4	1	TRUE
SubjectAltNames {2 5 29 17}	siehe Kap 5.3.4	0-1	FALSE
BasicConstraints {2 5 29 19}	siehe Kap 5.3.4	1	TRUE
CertificatePolicies {2 5 29 32}	siehe Kap 5.3.4	1	FALSE
CRLDistributionPoints {2 5 29 31}	CDP des TSP für das betreffende Zertifikat	1	FALSE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap 5.3.4	1	FALSE

Element	Inhalt	Kar.	
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 = siehe Tabelle Tab_SMCB_TID_KV-T (Es wird genau eine Admission-Struktur verwendet, mit je genau einem Element: professionInfo, professionItem, registrationNumber)	0 1 1 1	FALSE
ExtendedKeyUsage {2 5 29 37}	siehe Kap 5.3.4	*)	FALSE
andere Erweiterungen		0	
signatureAlgorithm	siehe Kap 5.3.4		
signature	siehe Kap 5.3.4		

*) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und Tab_PKI_240 ist die Kardinalität gleich 0.

Tabelle 114: Tab_SMCB_TID_KV-T Aufbau Telematik-ID in SMC-B-Zertifikaten der Sektoren der KBV

Präfix	Separator	Fortsatz	SMC für:										
1 (Arztpraxen)	-	2 (SMC)	0 (KV System registrierte Betriebsstätte eines Vertragsarztes oder Vertragspsychotherapeuten)	KV-Nr.	BSNR							frei wählbar	
				x	x	x	x	x	x	x	x	x	x
			1 (privat abrechnender Arzt)	generierte, neunstellige Nummer									
				x	x	x	x	x	x	x	x	x	x

A3 – DKG

Die nachfolgende Profiltabelle der DKTIG gilt für den Sektor:

- Krankenhäuser (DKTIG)

Tabelle 115: 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

Element	Inhalt	Kar.	
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 116: 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>

A4 – GKV-Spitzenverband

Die nachfolgende Profiltabelle des GKV-Spitzenverbandes gilt für Betriebsstätten bzw. Geschäftsstellen der gesetzlichen Krankenkassen.

Tabelle 117: 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			

Element	Inhalt	Kar.	
commonName	offen Kurzbezeichnung der Krankenkasse gemäß Freigabedaten des GKV-SV	**>1	
title	offen nicht belegt	**>0	
givenName	offen nicht belegt	**>0	
surName	offen nicht belegt	**>0	
serialNumber	offen 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	offen nicht belegt	**>0	
organizationName	offen 8-stellige eindeutige Betriebsnummer (BBNR) der Krankenkassenhauptverwaltung gemäß Freigabedaten des GKV-SV	**>1	
streetAddress	offen Straßenanschrift und Hausnummer des Krankenkassen Hauptsitzes gemäß Freigabedaten des GKV-SV	**>1	
postalCode	offen Postleitzahl des Krankenkassen Hauptsitzes gemäß Freigabedaten des GKV-SV (Deutsche PLZ werden 5-stellig abgebildet)	**>1	
localityName	offen Stadt des Krankenkassen Hauptsitzes gemäß Freigabedaten des GKV-SV	**>1	
stateOrProvinceName	offen 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}	offen 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}	offen 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}	offen admissionAuthority = {O=GKV-Spitzenverband,C=DE} professionItem = Beschreibung zu <oid_kostentraeger> gemäß [gemSpec_OID#GS-A_4443]	**> 1 1	FALSE

Element	Inhalt	Kar.	
	professionOID = OID <oid_kostentraeger> gemäß [gemSpec_OID#GS-A_4443] registrationNumber = siehe Tabelle Tab_SMCB_TID_GKVS	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.

~~**) Kardinalität ist offen, abhängig von der Festlegung in der jeweiligen Inhalts-Spalte.~~

Tabelle 118: Tab_SMCB_TID_GKVS 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

A5 – Apothekerschaft

Tabelle 119: Tab_SMCB_BAK SMC-B-Zertifikate für Apotheker

Element	Inhalt	Kar.	
certificate	C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
tbsCertificate			
version	siehe Kap 5.3.4		
serialNumber	siehe Kap 5.3.4		
signature	siehe Kap 5.3.4		
issuer	siehe Kap 5.3.4		
validity	siehe Kap 5.3.4		
subject			
commonName	Name der Apotheke	1	
title	siehe Kap 5.3.4		
givenName	Vorname des Verantwortlichen/Inhabers (mehrere Vornamen sind durch Blank oder Bindestrich getrennt) <i>Hinweis: bei mehreren Personen bleibt das Feld leer</i>	0-1	
surName	Familienname des Verantwortlichen/Inhabers <i>Hinweis: bei mehreren Personen bleibt das Feld leer</i>	0-1	

Element	Inhalt	Kar.	
	serialNumber	TI-weit eindeutiger Identifier der Karte z. B. in der Form: <TSP-ID>.<ICCSN> <TSP-ID> gemäß Tab_PKI_109 Werte für das Präfix <TSP-ID>	0-1
	organizationalUnitName	nicht belegt	0
	organizationName	Telematik-ID der Institution gemäß Freigabedaten der Apothekerkammer	1
	streetAddress	Strassen-Anschrift der Institution (mehrere Wörter sind durch Blank getrennt)	1
	postalCode	Postleitzahl des Ortes der Institution (Deutsche PLZ werden 5-stellig abgebildet)	1
	localityName	Stadt des Apotheken-Standortes	1
	stateOrProvinceName	Bundesland des Apotheken-Standortes	1
	countryName	siehe Kap 5.3.4	
	andere Attribute	siehe Kap 5.3.4	
	subjectPublicKeyInfo	siehe Kap 5.3.4	
	extensions		critical
	SubjectKeyIdentifier {2 5 29 14}	siehe Kap 5.3.4	FALSE
	KeyUsage {2 5 29 15}	siehe Kap 5.3.4	TRUE
	SubjectAltNames {2 5 29 17}	ggf. überlange Institutionsnamen, Alternativnamen oder Ergänzungen	0-1 FALSE
	BasicConstraints {2 5 29 19}	siehe Kap 5.3.4	TRUE
	CertificatePolicies {2 5 29 32}	siehe Kap 5.3.4	FALSE
	CRLDistributionPoints {2 5 29 31}	nicht belegt	0 FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap 5.3.4	FALSE
	AuthorityKeyIdentifier {2 5 29 35}	siehe Kap 5.3.4	FALSE
	Admission {1 3 36 8 3 3}	admissionAuthority = {O=<von der BAK benannte attributbestätigende Stelle *>,C=DE} professionItem = Beschreibung zu <oid_oeffentliche_apotheke> gemäß [gemSpec_OID#GS-A_4443] professionOID = OID <oid_oeffentliche_apotheke> gemäß [gemSpec_OID#GS-A_4443] registrationNumber = <Telematik-ID der Institution gemäß Freigabedaten der Apothekerkammer>	0-1 1 1 1 FALSE
	ExtendedKeyUsage {2 5 29 37}	siehe Kap 5.3.4	*) FALSE
	andere Erweiterungen	siehe Kap 5.3.4	
	signatureAlgorithm	siehe Kap 5.3.4	
	signature	siehe Kap 5.3.4	

*) In AUT-Zertifikaten gemäß Tab_PKI_238 ist die Kardinalität der Erweiterung ExtendedKeyUsage gleich 1, in ENC- und OSIG-Zertifikaten gemäß Tab_PKI_239 und Tab_PKI_240 ist die Kardinalität gleich 0.

Tabelle 120: 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

A6 – AdV-Umgebung beim Leistungserbringer

Tabelle 121: Tab_SMCB_ADV_LE SMC-B-Zertifikate für die AdV-Umgebung beim Leistungserbringer

Element	Inhalt *)	Kar.	
certificate	C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
tbsCertificate			
version	siehe Kap. 5.3.4.3		
serialNumber	siehe Kap. 5.3.4.3		
signature	siehe Kap. 5.3.4.3		
issuer	siehe Kap. 5.3.4.3		
validity	siehe Kap. 5.3.4.3		
subject			
commonName	Wert aus den in den Anhängen A1, A2 und A3 beschriebenen sektorspezifischen SMC-B-Profilen ergänzt um das Präfix „AdV“	1	
title	siehe Kap. 5.3.4.3		
givenName	siehe Kap. 5.3.4.3		
surName	siehe Kap. 5.3.4.3		
serialNumber	siehe Kap. 5.3.4.3		
organizationalUnitName	siehe Kap. 5.3.4.3		
organizationName	siehe Kap. 5.3.4.3		
streetAddress	siehe Kap. 5.3.4.3		
postalCode	siehe Kap. 5.3.4.3		
localityName	siehe Kap. 5.3.4.3		
stateOrProvinceName	siehe Kap. 5.3.4.3		
countryName	siehe Kap. 5.3.4.3		
andere_Attribute		0	
subjectPublicKeyInfo	siehe Kap. 5.3.4.3		
extensions			critical
SubjectKeyIdentifier	siehe Kap. 5.3.4.3		

Element	Inhalt *)	Kar.	
{2.5.29.14}			
KeyUsage {2.5.29.15}	siehe Kap. 5.3.4.3		
SubjectAltNames {2.5.29.17}	siehe Kap. 5.3.4.3		
BasicConstraints {2.5.29.19}	siehe Kap. 5.3.4.3		
CertificatePolicies {2.5.29.32}	siehe Kap. 5.3.4.3		
CRLDistributionPoints {2.5.29.31}	siehe Kap. 5.3.4.3		
AuthorityInfoAccess {1.3.6.1.5.5.7.1.1}	siehe Kap. 5.3.4.3		
AuthorityKeyIdentifier {2.5.29.35}	siehe Kap. 5.3.4.3		
Admission {1.3.36.8.3.3}	professionItem = Beschreibung zu <oid_adv_lo> gemäß [gemSpec_OID#GS-A_4443] professionOID = OID <oid_adv_lo> gemäß [gemSpec_OID#GS-A_4443] registrationNumber = Telematik-ID der Institution (mit Verwendung des Präfix für LE-AdV gemäß Tab_PKI_101)	1 1 1	
ExtendedKeyUsage {2.5.29.37}	siehe Kap. 5.3.4.3		
andere Erweiterungen		0	
signatureAlgorithm	siehe Kap. 5.3.4.3		
signature	siehe Kap. 5.3.4.3		

*) Falls nicht explizit anders festgelegt, kann hier der Wert verwendet werden, der auch in dem entsprechenden sektorspezifischen SMC-B Zertifikats-Profil (gemäß Anhang A1, A2 oder A3) verwendet wird.

A67 – AdV-Umgebung beim Kostenträger

Tabelle 122: Tab_SMCB_ADV_KTR SMC-B-Zertifikate für die AdV-Umgebung beim 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			

Element	Inhalt *)	Kar.	
	commonName	Gemäß Freigabe-/Antrags-Daten des GKV-SV	1
	title	nicht belegt	0
	givenName	nicht belegt	0
	surName	nicht belegt	0
	serialNumber	nicht belegt	0
	organizationalUnitName	nicht belegt	0
	organizationName	nicht belegt	0
	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}	nicht belegt	0 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	

Anhang B – Verzeichnisse

B1 – Abkürzungen

Kürzel	Erläuterung
AES	Advanced Encryption Standard
AK	Anwendungskonnektor
AN	alphanumerisch
AUT	Authentisierung (Authentication)
AUTN	Technisches Authentisierungszertifikat für Nachrichten
AVS	Apothekenverwaltungssystem (Primärsystem der Apotheker)
BAEK	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

Kürzel	Erläuterung
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
ENC	Verschlüsselung (Encryption)
ENCV	Technisches Verschlüsselungszertifikat für Verordnungen
ETSI	Europäisches Institut für Telekommunikationsnormen
FIPS-140 2	Federal Information Processing Standard 140 2
FQDN	Fully Qualified Domain Name
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

Kürzel	Erläuterung
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
SHA	Secure Hash Algorithm
SIG	Elektronische Signatur
SLA	Service Level Agreement

Kürzel	Erläuterung
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

B2 – 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	<p>„Referenzzeit(punkt)“ entspricht „refTime“ in [Common-PKI#Part5] und den Corrigenda dazu (Version 1.2.1 vom 14.06.2014).</p> <p>Es handelt sich um den Zeitpunkt, für den das Zertifikat auf Gültigkeit geprüft wird und für den die Statusinformationen eingeholt werden. Dabei kann es sich um die aktuelle Systemzeit handeln (z.B. bei TLS-Verbindungsaufbau). Der Referenzzeitpunkt kann auch in der Vergangenheit liegen (z.B. Signaturzeitpunkt bei QES).</p>

Das Glossar wird als eigenständiges Dokument, vgl. [gemGlossar] zur Verfügung gestellt.

B3 – Abbildungsverzeichnis

Abbildung 1: Betriebsumgebungen aus Sicht der PKI	24
Abbildung 2: Aufbau der Krankenversichertennummer	29
Abbildung 3: Pseudonym Kodierung in X.509-Versicherten-zertifikaten	32
Abbildung 4: Das Anschriftenfeld nach DIN5008.....	65

Abbildung 5: Use Case Diagramm „Prozesse zur Nutzung des TI-Vertrauensraums“ ...	134
Abbildung 6: Aufbau der TSL	136
Abbildung 7: Aktivitätsdiagramm TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“	142
Abbildung 8: Aktivitätsdiagramm TUC_PKI_013 „Import neuer TI-Vertrauensanker“	145
Abbildung 9: Aktivitätsdiagramm TUC_PKI_017 „Lokalisierung Download-Adresse“	150
Abbildung 10: Aktivitätsdiagramm TUC_PKI_016 „Download der TSL-Datei“	152
Abbildung 11: Aktivitätsdiagramm TUC_PKI_019 „Prüfung der Aktualität der TSL“	156
Abbildung 12: Aktivitätsdiagramm TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“	159
Abbildung 13: Use Case Diagramm „Zertifikatsprüfung“	162
Abbildung 14: Aktivitätsdiagramm TUC_PKI_018 „Zertifikatsprüfung“	166
Abbildung 15: Aktivitätsdiagramm TUC_PKI_002 Gültigkeitsprüfung des Zertifikats	168
Abbildung 16: Aktivitätsdiagramm TUC_PKI_003 CA-Zertifikat in TSL-Informationen finden	170
Abbildung 17: Aktivitätsdiagramm TUC_PKI_004 Mathematische Prüfung der Zertifikatssignatur	172
Abbildung 18: Aktivitätsdiagramm TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln“	174
Abbildung 19: Aktivitätsdiagramm TUC_PKI_006 „OCSP-Abfrage“	178
Abbildung 20: Aktivitätsdiagramm TUC_PKI_021 „CRL-Prüfung“	182
Abbildung 21: Aktivitätsdiagramm TUC_PKI_009 „Rollenermittlung“	185
Abbildung 22: Aktivitätsdiagramm TUC_PKI_007 „Prüfung Zertifikatstyp“	187

B4 – Tabellenverzeichnis

Tabelle 1: Tab_PKI_201 Allgemeine Notationsvorschrift für kryptographische Objekte...	13
Tabelle 2: Tab_PKI_202: Notationsvorgaben für Objekttyp	13
Tabelle 3: Tab_PKI_203 Notationsvorgaben für Objektbesitzer	14
Tabelle 4: Tab_PKI_204 Notationsvorgaben für Objektverwendung	16
Tabelle 5: Tab_PKI_205 Notationsvorgaben für Ausprägung	18
Tabelle 6: Tab_PKI_206 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	34

Tabelle 12: Tab_PKI_224 Telematik-ID-Kennzeichnung	35
Tabelle 13: Tab_PKI_223 Aufbau der Telematik-ID	36
Tabelle 14: Tab_PKI_101 Normative Festlegung für das Präfix der Telematik-ID.	36
Tabelle 15: Tab_PKI_229 Kodierung der Attribute in X.509-Zertifikaten	37
Tabelle 16: Tab_PKI_109 Werte für das Präfix <TSP-ID>	39
Tabelle 17: Tab_PKI_226 Struktur Admission.....	40
Tabelle 18: Tab_PKI_227 Struktur CertificatePolicies	41
Tabelle 19: Tab_PKI_228 Struktur SubjectAltName.....	42
Tabelle 20: Common Name (CN) der End-Entity-Zertifikate Test-PKI	46
Tabelle 21: Tab_PKI_231 Personennamen im subjectDN	50
Tabelle 22: Tab_PKI_232 C.CH.AUT Authentisierung eGK	51
Tabelle 23: Tab_PKI_233 C.CH.ENC Verschlüsselung eGK	52
Tabelle 24: Tab_PKI_234 C.CH.QES Qualifizierte Signatur eGK	53
Tabelle 25: Tab_PKI_235 C.CH.AUTN Technische Authentisierung eGK.....	55
Tabelle 26: Tab_PKI_236 C.CH.ENCV Technische Verschlüsselung eGK.....	56
Tabelle 27: Tab_PKI_268 C.HP.AUT Authentisierung HBA	57
Tabelle 28: Tab_PKI_269 C.HP.ENC Verschlüsselung HBA	59
Tabelle 29: Tab_PKI_270 C.HP.QES Qualifizierte Signatur HBA	61
Tabelle 30: Tab_PKI_238 C.HCI.AUT Authentisierung SMC-B.....	66
Tabelle 31: Tab_PKI_239 C.HCI.ENC Verschlüsselung SMC-B	67
Tabelle 32: Tab_PKI_240 C.HCI.OSIG Signatur SMC-B	69
Tabelle 33: Tab_PKI_241 C.SMKT.AUT gSMC-KT	71
Tabelle 34: Tab_PKI_237 Statusprüfung von Konnektorzertifikaten.....	74
Tabelle 35: Tab_PKI_242 Zertifikatsprofil C.NK.VPN VPN-Authentisierung Netzkonnektor	74
Tabelle 36: Tab_PKI_243 Zertifikatsprofil C.AK.AUT Authentisierung Anwendungskonnektor	75
Tabelle 37: Tab_PKI_244 Zertifikatsprofil C.SAK.AUT Authentisierung SAK	77
Tabelle 38: Tab_PKI_245 Zertifikatsprofil C.VPNK.VPN VPN-Authentisierung Zugangsdienst TI	79
Tabelle 39: Tab_PKI_265 Zertifikatsprofil C.VPNK.VPN-SIS VPN-Authentisierung Zugangsdienst Sicherer Internetzugang	80
Tabelle 40: Tab_PKI_247 C.ZD.TLS-S Server-Authentisierung Zentrale Dienste	82
Tabelle 41: Tab_PKI_249 C.FD.TLS-C Client-Authentisierung Fachanwendungsspezifische Dienste	84
Tabelle 42: Tab_PKI_250 C.FD.TLS-S Server-Authentisierung Fachanwendungsspezifische Dienste	86

Tabelle 43: Tab_PKI_267 C.CM.TLS-CS Clientmodul-Authentisierung	88
Tabelle 44: Tab_PKI_211 GEM.R-CA<n> – Zentrale gematik Root-CA_nonQES der TI	90
Tabelle 45: Tab_PKI_212 <tsp>.<usage>-CA<n> –Aussteller- CA_nonQES der TI.....	91
Tabelle 46: Tab_PKI_215 <tsp>.HBA-qCA<n> – Aussteller- CA_QES der TI	92
Tabelle 47: Tab_PKI_253 C.GEM.OCSP Zertifikatsprofil OCSP-Signer	95
Tabelle 48: Tab_PKI_214 C.GEM.CRL Zertifikatsprofil CRL-Signer	97
Tabelle 49: Tab_PKI_252 C.TSL.SIG Zertifikatsprofil TSL-Signer.....	99
Tabelle 50: Tab_PKI_254 Zugriffsprofile für eine Rollenauthentisierung	103
Tabelle 51: Tab_PKI_255 Zugriffsprofile G2 für eine Authentisierung einer Funktionseinheit.....	107
Tabelle 52: Tab_PKI_256 Mögliche Werte für CPI	108
Tabelle 53: Tab_PKI_257 Aufbau CAR für Karten der Generation 1	108
Tabelle 54: Tab_PKI_258 Aufbau CHR	109
Tabelle 55: Tab_PKI_259 Aufbau CHA.....	110
Tabelle 56: Tab_PKI_260 Object Identifier der Registration Authority TeleTrustT.....	111
Tabelle 57: Tab_PKI_261 CV-Zertifikat einer CVC-CA mit CPI = '21', SHA-256	112
Tabelle 58: Tab_PKI_262 CV-Zertifikat zur Authentisierung mit CPI = '22', SHA-256 ..	112
Tabelle 59: Tab_PKI_263 Informationen für ein CV-Zertifikat einer CVC-CA	112
Tabelle 60: Tab_PKI_264 Informationen für ein CV-Zertifikat einer Karte	113
Tabelle 61: Tab_PKI_266 Aufbau CAR für Karten der Generation 2.....	117
Tabelle 62: Tab_PKI_901 Objektidentifizier des öffentlichen Schlüssels eines CV-Zertifikats der Generation 2.....	118
Tabelle 63: Tab_PKI_902 Punkt Q des öffentlichen Schlüssels eines CV-Zertifikats der Generation 2.....	119
Tabelle 64: Tab_PKI_904 Mögliche Objektidentifizier OID_{flags} in Certificate Holder Authorization Templates	120
Tabelle 65: Tab_PKI_905 Zu signierende Nachricht M eines CV-Zertifikates	121
Tabelle 66: Tab_PKI_906 Signatur der Nachricht M eines CV-Zertifikats.....	122
Tabelle 67: Tab_PKI_907 Struktur und Inhalt eines CV-Zertifikat	122
Tabelle 68: Tab_PKI_912 CA CV-Zertifikate für 256 bit ELC-Schlüssel, insgesamt 220 Oktett.....	123
Tabelle 69: Tab_PKI_913 CA CV-Zertifikate für 384 bit ELC-Schlüssel, insgesamt 285 Oktett.....	124
Tabelle 70: Tab_PKI_914 CA CV-Zertifikate für 512 bit ELC-Schlüssel, insgesamt 352 Oktett.....	124
Tabelle 71: Tab_PKI_937 Cross-CV-Zertifikat für ELC-Schlüssel	125

Tabelle 72: Tab_PKI_915 Endnutzer-CV-Zertifikate für 256 bit ELC-Schlüssel, insgesamt 222 Oktett.....	126
Tabelle 73: Tab_PKI_916 Endnutzer-CV-Zertifikate für 384 bit ELC-Schlüssel, insgesamt 287 Oktett.....	126
Tabelle 74: Tab_PKI_917 Endnutzer-CV-Zertifikate für 512 bit ELC-Schlüssel, insgesamt 354 Oktett.....	127
Tabelle 75: Tab_PKI_910 TI-PKI, Bedeutung der Bits innerhalb der Flagliste eines CHAT	127
Tabelle 76: Tab_PKI_918 Abbildung von Rollenberechtigungen auf äquivalente Flaglisten	129
Tabelle 77: Tab_PKI_919 Sub-CA-Flaglisten nach Kartentyp (G2) und Zugriffsprofilen	130
Tabelle 78: Tab_PKI_911 CMS-PKI, Bedeutung der Bits innerhalb der Flagliste eines CHAT.....	130
Tabelle 79: Tab_PKI_271 Erlaubte URIs als Inhalte des TSL-Elements ServiceStatus.....	138
Tabelle 80: TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“.....	139
Tabelle 81: TUC_PKI_013 „Import neuer TI-Vertrauensanker“	143
Tabelle 82: Gültige Werte für den TI-Vertrauensankerwechsel	147
Tabelle 83: Beispiel für den TSL-Eintrag zum Wechsel des TSL-Signer-CA-Zertifikats.....	147
Tabelle 84: TUC_PKI_017 „Lokalisierung Download-Adressen“	148
Tabelle 85: Tab_PKI_272 Gültige Werte zur Download-Adresse	150
Tabelle 86: TUC_PKI_016 „Download der TSL-Datei“	150
Tabelle 87: TUC_PKI_019 „Prüfung der Aktualität der TSL“	153
Tabelle 88: TUC_PKI_020 „XML-Dokument validieren“	157
Tabelle 89: TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“.....	158
Tabelle 90: TUC_PKI_012 „XML-Signatur- Prüfung“.....	160
Tabelle 91: Tab_PKI_294 TSL Zeitparameter.....	161
Tabelle 92: TUC_PKI_018 „Zertifikatsprüfung in der TI“.....	163
Tabelle 93: TUC_PKI_002 „Gültigkeitsprüfung des Zertifikats“	167
Tabelle 94: TUC_PKI_003 „CA-Zertifikat in TSL-Informationen finden“	168
Tabelle 95: TUC_PKI_004 „Mathematische Prüfung der Zertifikatssignatur“.....	170
Tabelle 96: TUC_PKI_005 „Adresse für Status- und Sperrprüfung ermitteln“.....	173
Tabelle 97: TUC_PKI_006 „OCSP-Abfrage“	174
Tabelle 98: TUC_PKI_021 „CRL-Prüfung“	179
Tabelle 99: TUC_PKI_009 „Rollenermittlung“	183
Tabelle 100: TUC_PKI_007 „Prüfung Zertifikatstyp“	186
Tabelle 101: Tab_PKI_273 Prüfparameter für TLS-Aufbau.....	188

Tabelle 102: TUC_PKI_030 „QES-Zertifikatsprüfung“	190
Tabelle 103: TUC_PKI_036 „BNetzA-VL Aktualisierung“	193
Tabelle 104: Tab_PKI_274 Fehlercodes des SubCompTyps PKI bei TSL- und Zertifikatsprüfung	197
Tabelle 105: Tab_PKI_908 Prüfung der Signatur eines CV-Zertifikats der Generation 2 mit Hilfe des CV-Zertifikats des Herausgebers.....	202
Tabelle 106: Tab_PKI_909 Gültigkeit eines CV-Zertifikats der Generation 2	202
Tabelle 107: Tab_PKI_291 OCSP-Response Status Ergebnisse.....	208
Tabelle 108: Tab_PKI_292 Zeiten in einer OCSP-Response	208
Tabelle 109: Tab_PKI_293 Status der OCSP Antworten	209
Tabelle 110: Tab_SMCB_KZBV_ZA SMC-B-Zertifikate für Zahnarzt (Sektor KZBV)	212
Tabelle 111: Tab_SMCB_KZBV_KZV SMC-B-Zertifikate für KZV (Sektor KZBV)	214
Tabelle 112: Tab_SMCB_TSP-ID Werte für das Präfix <TSP-ID>	215
Tabelle 113: Tab_SMCB_KV-T SMC-B-Zertifikate für Sektoren der KBV	215
Tabelle 114: Tab_SMCB_TID_KV-T Aufbau Telematik-ID in SMC-B-Zertifikaten der Sektoren der KBV	217
Tabelle 115: Tab_SMCB_DKTIG SMC-B-Zertifikate für Sektor der DKTIG.....	218
Tabelle 116: Tab_SMCB_TID_DKTIG Aufbau Telematik-ID in SMC-B-Zertifikaten der DKTIG	219
Tabelle 117: Tab_SMCB_KTR SMC-B-Zertifikate für Mitarbeiter Kostenträger.....	219
Tabelle 118: Tab_SMCB_TID_GKVSV Aufbau Telematik-ID in SMC-B-Zertifikaten des GKV-SV	221
Tabelle 119: Tab_SMCB_BAK SMC-B-Zertifikate für Apotheker	221
Tabelle 120: Tab_SMCB_TID_BAK Aufbau Telematik-ID in SMC-B-Zertifikaten der Apotheker	223
Tabelle 121: Tab_SMCB_ADV_LE SMC-B-Zertifikate für die AdV-Umgebung beim Leistungserbringer.....	223
Tabelle 122: Tab_SMCB_ADV_KTR SMC-B-Zertifikate für die AdV-Umgebung beim Kostenträger	224
Tabelle 123: Tab_HBA_BÄK HBA-Zertifikate (AUT, ENC, QES) für BÄK	239
Tabelle 124: Tab_HBA_BZÄK HBA-Zertifikate (AUT, ENC, QES) für BZÄK	241
Tabelle 125: Tab_HBA_BPtK HBA-Zertifikate (AUT, ENC, QES) für BPtK	242
Tabelle 126: Tab_HBA_BAK HBA-Zertifikate (AUT, ENC, QES) für Apotheker	244

B5 – Referenzierte Dokumente

B5.1 – Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer sind in der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar
[gemKPT_Arch_TIP]	gematik: 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

B5.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ALGCAT]	Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, vom 11.12.2015 (auch online verfügbar: https://www.bundesanzeiger.de mit dem Suchbegriff „BAnz AT 01.02.2016 B5“)
[baekAttr]	Zertifikatsprofile für X.509 Attributzertifikate; Version 2.3.1 vom 29.05.2009
[BÄK_ZPX.509B]	Bundesärztekammer (28.05.2009): Zertifikatsprofile für X.509 Basiszertifikate V 2.3.1; Zertifikatsaufbau und –hierarchie, Gültigkeitsmodell für Zertifikatstypen: ENC, AUT, QES, ATT sowie die Root, Cross- und CA-Zertifikate, die CRL-Signer

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
	und die OCSP-Zertifikate
[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
[BSI-TR-03111]	BSI (2012): Elliptic Curve Cryptography, Version 2.0 https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03111/index.htm
[Common-PKI]	T7 & TeleTrust (20.01.2009): Common PKI Spezifikation, Version 2.0 http://www.t7ev.org/themen/entwickler/common-pki-v20-spezifikation.html
[CP-HPC]	Bundesärztekammer et al (06.11.2012): Gemeinsame Policy für die Ausgabe der HPC – Zertifikatsrichtlinie HPC (Version 1.0.5) http://www.bundesaeztekammer.de/downloads/CP_HPC_v1.0.5.pdf
[DIN5008]	DIN 5008 (2005): Schreib- und Gestaltungsregeln für die Textverarbeitung
[eIDAS]	Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
[EN 14890-1]	EN 14890-1 (Draft: February 2007) Application Interface for smart cards used as secure signature Creation Devices - Part 1: Basic services
[ETSI EN 319 412-2]	ETSI (Februar 2016): ETSI EN 319 412-2 V2.1.1 'Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons'
[ETSI TS 102 231_v3.1.2]	ETSI (Dezember 2009): ETSI Technical Specification TS 102 231 ('Provision of harmonized Trust Service Provider (TSP) status information') Version 3.1.2
[ETSI TS 119 612]	ETSI (July 2015): ETSI TS 119 612 V2.1.1 'Electronic Signatures and Infrastructures (ESI); Trusted Lists'
[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

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
	Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://tools.ietf.org/html/rfc2109
[RFC2560]	RFC 2560 (Juni 1999): X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP http://tools.ietf.org/html/rfc2560
[RFC3629]	RFC 3629 (November 2003): UTF-8, a transformation format of ISO 10646 http://tools.ietf.org/html/rfc3629
[RFC3739]	RFC 3739 (March 2004): Internet X.509 Public Key Infrastructure Qualified Certificates Profile http://tools.ietf.org/html/rfc3739
[RFC4514]	RFC 4514 (Juni 2006): Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names http://tools.ietf.org/html/rfc4514
[RFC5019]	RFC 5019 (September 2007): The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments http://tools.ietf.org/html/rfc5019
[RFC5280]	RFC 5280 (Mai 2008): Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile http://tools.ietf.org/html/rfc5280
[RFC6960]	RFC 6960 (Juni 2013): X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP https://tools.ietf.org/html/rfc6960
[SGB V]	BGBI. I S.2477 (20.12.1988): Sozialgesetzbuch, Fünftes Buch Zuletzt geändert durch Art. 4 G v. 14.4.2010 I 410 Gesetzliche Krankenversicherung
[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/

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[XAdES]	ETSI TS 101 903 V1.4.2 (2010-12) Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)
[XMLSig]	W3C Recommendation: XML-Signature Syntax and Processing http://www.w3.org/TR/xmlsig- core/

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

C1 – BÄK

Tabelle 123: 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

Element	Inhalt	Kar.	
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}	<p>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 Physicians policyIdentifier = <OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP-spezifischen Zertifikatsrichtlinie</p>	<p>1 0-1 1 (1) 1 0-1 0-1</p>	FALSE
CRLDistributionPoints {2 5 29 31}	siehe Kap. 5.2.1		FALSE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap. 5.2.1		FALSE
AuthorityKeyIdentifier {2 5 29 35}	siehe Kap. 5.2.1		FALSE
Admission {1 3 36 8 3 3}	<p>admissionAuthority = {O=<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... (nur...für AUT und ENC zwingend... ... für QES optional</p>	<p>1 1 1 4 1 0-1</p>	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		

C2 – BZÄK

Tabelle 124: Tab_HBA_BZÄK HBA-Zertifikate (AUT, ENC, QES) für BZÄK

Element	Inhalt *)	Kar.	
certificate	C.HP.AUT, C.HP.ENC, C.HP.QES		
tbsCertificate			
version	siehe Kap. 5.2.1		
serialNumber	siehe Kap. 5.2.1		
signature	siehe Kap. 5.2.1		
issuer	siehe Kap. 5.2.1		
validity	siehe Kap. 5.2.1		
subject			
commonName	siehe Kap. 5.2.1		
title	siehe Kap. 5.2.1		
givenName	siehe Kap. 5.2.1		
surName	siehe Kap. 5.2.1		
serialNumber	siehe Kap. 5.2.1		
organizationalUnitName	siehe Kap. 5.2.1		
organizationName	siehe Kap. 5.2.1		
countryName	siehe Kap. 5.2.1		
andere Attribute	siehe Kap. 5.2.1		
subjectPublicKeyInfo	siehe Kap. 5.2.1		
extensions			critical
SubjectKeyIdentifier {2 5 29 14}	siehe Kap. 5.2.1		FALSE
KeyUsage {2 5 29 15}	siehe Kap. 5.2.1		TRUE
SubjectAltNames {2 5 29 17}	siehe Kap. 5.2.1		FALSE
BasicConstraints {2 5 29 19}	siehe Kap. 5.2.1		TRUE
CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444] policyQualifierInfo = http://policies.bzaek.de policyIdentifier = Zertifikatstyp-OID gemäß [gemSpec_OID#GS-A_4445] policyIdentifier = <id-etsi-qcp-natural-qscd> {0.4.0.194112.1.2} (nur für QES) policyIdentifier = <OID der TSP-spezifischen Policy> policyQualifierInfo = URL der TSP-spezifischen Zertifikatsrichtlinie	1 0-1 1 (1) 0-1 0-1	FALSE
CRLDistributionPoints {2 5 29 31}	CDP der ausstellenden CA zwingend... ... für AUT und ENC zwingend, ... für QES optional	0 1 0-1	FALSE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap. 5.2.1		FALSE

Element	Inhalt *)	Kar.	
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	0-1 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		

C3 – BPtK

Tabelle 125: 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		

Element	Inhalt *)	Kar.	
<i>andere Attribute</i>	<i>siehe Kap. 5.2.1</i>		
subjectPublicKeyInfo	<i>siehe Kap. 5.2.1</i>		
extensions			critical
SubjectKeyIdentifier {2 5 29 14}	<i>siehe Kap. 5.2.1</i>		FALSE
KeyUsage {2 5 29 15}	<i>siehe Kap. 5.2.1</i>		TRUE
SubjectAltNames {2 5 29 17}	<i>siehe Kap. 5.2.1</i>		FALSE
BasicConstraints {2 5 29 19}	<i>siehe Kap. 5.2.1</i>		TRUE
CertificatePolicies {2 5 29 32}	<p>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</p>	<p>1 0-1 1 (1) 0-1 0-1</p>	FALSE
CRLDistributionPoints {2 5 29 31}	<i>siehe Kap. 5.2.1</i>		FALSE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	<i>siehe Kap. 5.2.1</i>		FALSE
AuthorityKeyIdentifier {2 5 29 35}	<i>siehe Kap. 5.2.1</i>		FALSE
Admission {1 3 36 8 3 3}	<p>admissionAuthority = {O=<zuständige Landespsychotherapeutenkammer>,C=DE} Eine oder zwei professionInfo-Elemente bestehend aus: professionItem = „Psychologische/-r Psychotherapeut/-in“ und/oder professionItem = „Kinder- und Jugendlichenpsychotherapeut/-in“ (siehe [gemSpec_OID#GS-A_4442]) professionOID = <oid_ps_psychotherapeut> und/oder professionOID = <oid_kuj_psychotherapeut> (siehe [gemSpec_OID#GS-A_4442]) registrationNumber = Telematik-ID des Inhabers... ... für AUT und ENC zwingend, ... für QES optional (Diese muss dann in mindestens einem professionInfo-Element aufgeführt sein)</p>	<p>0-1 1-2 1-2 1-2 4 1-2 0-1</p>	FALSE
ExtendedKeyUsage {2 5 29 37}	<i>siehe Kap. 5.2.1</i>		FALSE
ValidityModel {1 3 6 1 4 1 8301 3 5}	<i>siehe Kap. 5.2.1</i>		FALSE
QCStatements {1 3 6 1 5 5 7 1 3}	<i>siehe Kap. 5.2.1</i>		FALSE
additionalInformation	<i>siehe Kap. 5.2.1</i>		FALSE

Element	Inhalt *)	Kar.	
	{1 3 36 8 3 15}		
	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		

C4 – Apothekerschaft

Tabelle 126: 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	policyIdentifier = <oid_policy_hba_cp> gemäß [gemSpec_OID#GS-A_4444]	1	FALSE

Element	Inhalt	Kar.		
	<p>{2 5 29 32}</p> <p>policyQualifierInfo = <URL der Apotheker, unter der die o.a. CP aufzurufen ist> https://www.abda.de/themen/positionen-und-initiativen/telematik/hba/</p> <p>policyIdentifier = Zertifikatstyp-OID gemäß [gemSpec_OID#GS-A_4445]</p> <p>policyIdentifier = <id-etsi-qcp-natural-qscd> {0.4.0.194112.1.2} (nur für QES)</p> <p>policyIdentifier =<OID der TSP-spezifischen Policy></p> <p>policyQualifierInfo = URL der TSP-spezifischen Zertifikatsrichtlinie</p>	<p>0-1</p> <p>1</p> <p>(1)</p> <p>0-1</p> <p>0-1</p>		
	<p>CRLDistributionPoints {2 5 29 31}</p>	<p>siehe Kap. 5.2.1</p>		FALSE
	<p>AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}</p>	<p>siehe Kap. 5.2.1</p>		FALSE
	<p>AuthorityKeyIdentifier {2 5 29 35}</p>	<p>siehe Kap. 5.2.1</p>		FALSE
	<p>Admission {1 3 36 8 3 3}</p>	<p>admissionAuthority = (O= <Apothekerkammer Bezeichnung>, C=DE)</p> <p>professionItem = Genau eine Beschreibung zu <oid_apotheker> bzw. <oid_apothekerassistent> bzw. ...<oid_pharmazieingenieur> bzw. <oid_apothekenassistent>. gemäß [gemSpec_OID#GS-A_4442]</p> <p>professionOID = Genau eine OID der Berufsgruppe <oid_apotheker> bzw. <oid_apothekerassistent> bzw. ...<oid_pharmazieingenieur> bzw. <oid_apothekenassistent> gemäß [gemSpec_OID#GS-A_4442]</p> <p>registrationNumber = Telematik-ID des Inhabers für AUT und ENC zwingend, ... für QES optional</p>	<p>1</p> <p>1</p> <p>1</p> <p>1</p> <p>1</p> <p>1</p> <p>1</p> <p>0-1</p>	FALSE
	<p>ExtendedKeyUsage {2 5 29 37}</p>	<p>siehe Kap. 5.2.1</p>		FALSE
	<p>additionalInformation</p>	<p>siehe Kap. 5.2.1</p>		FALSE
	<p>Restriction</p> <p>andere Erweiterungen</p>	<p>siehe Kap. 5.2.1</p> <p>siehe Kap. 5.2.1</p>		FALSE
signatureAlgorithm	<p>siehe Kap. 5.2.1</p>			
signature	<p>siehe Kap. 5.2.1</p>			