gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Elektronische Gesundheitskarte und Telematikinfrastruktur

Konzept PKI der TI-Plattform

Version:	2.7.0
Revision:	166361
Stand:	02.10.2019
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemKPT_PKI_TIP

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Datum	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
2.0.0	02.08.17		Überarbeitung Online-Produktivbetrieb (Stufe 2.1)	gematik
	06.12.17		Ausbau LE-AdV	gematik
2.1.0	18.12.17		Änderungen lt. OPB1 R1.6.4-0, Ausbau LE-AdV-Anteile	gematik
2.2.0	14.05.18		Einarbeitung P15.2, P15.3, P15.4	gematik
2.3.0	26.10.18		Einarbeitung P15.9	gematik
2.4.0	18.12.18		Einarbeitung P15.11, 17.1	gematik
2.5.0	15.05.19		Einarbeitung P18.1	gematik
2.6.0	28.06.19		Einarbeitung P19.1	gematik
			Einarbeitung P20.1, 16.1/2	gematik
2.7.0	02.10.19		freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes 7
1.1 Zielsetzung 7
1.2 Zielgruppe 7
1.3 Geltungsbereich 7
1.4 Methodik 8
2 Konzeptionelle Grundlagen 9
2.1 Einführung PKI der TI 9
2.2 Basisfunktionen der PKI 10
2.3 Vertrauensmodelle in der PKI der TI 10
2.3.1 Vertrauensmodell für QES 11
2.3.2 Vertrauensraum mittels TSL 11
2.3.2.1 TSL in der TI im Kontext ECC-Migration 11
2.3.3 Vertrauensraum mittels TSL – Umsetzung in der TI 12
2.3.3.1 Bereitstellung der TSL als Vertrauensraum der TI 12
2.3.3.2 Struktur, Signatur und Inhalt der TSL 13
2.3.3.3 Gültigkeit und Auswertung der TSL 16
2.3.3.4 Initialisierung/Reinitialisierung des Vertrauensraums 17
2.3.3.5 Sperrung von CA-Zertifikaten in der TSL 18
2.3.3.6 Aktualisierung des Vertrauensraumes 21
2.3.3.7 Vertrauensankerwechsel 21
2.3.4 Vertrauensmodell der nonQES TI-Zertifikate im Internet 23
2.3.5 Vertrauensmodell von Zertifikaten der HBA-Vorläuferkarten in der TI 23
2.3.6 Vertrauensmodell CVC 23
2.4 Gültigkeitsmodelle X.509-Zertifikate 24
2.4.1 PKIX-Schalenmodell 25
2.4.2 Kompromissmodell 25
2.4.3 QES-Kettenmodell 25
2.5 Zertifikatstypen in der TI und deren Verwendung 26
2.5.1 X.509-Zertifikate für Identitäten der TI 26
2.5.2 CV-Zertifikate für Karten in der TI 27
2.6 Verantwortliche Instanzen 27
2.7 Teilnehmer in der PKI 28
2.7.1 Trust Service Provider (TSP) 29
2.7.2 Registrierungsstellen 30
2.7.3 Kartenherausgeber 31
2.7.3.1 HBA-Herausgeber 33
2.7.3.2 eGK-Herausgeber 33
2.7.3.3 Herausgeber der SMC-B 33
2.7.3.4 Herausgeber von gSMC-K und gSMC-KT 34

2.7.3.5 Herausgeber von Prüfkarten 35
2.7.4 Anbieter TSL-Dienst 35
2.7.5 Zertifikatsantragsteller 35
2.7.6 Zertifikatsnehmer 35
2.7.7 Zertifikatsnutzer 36
2.7.8 gematik 36
2.7.9 Andere Teilnehmer 36
2.7.9.1 Rollenvergabestelle 36
2.7.9.2 Attributsbestätigende Stellen 37

2.8 Identifikation von Akteuren 37
2.8.1 Krankenversichertennummer 38
2.8.2 Telematik-ID 38

2.9 Lebenszyklus von Zertifikaten 39
2.9.1 Definition der Begriffe 40
2.9.2 Lebenszyklus für Zertifikate ohne Status-Eigenschaft 41
2.9.3 Lebenszyklus für Zertifikate mit Statuseigenschaft 41
2.9.4 Staging der Zertifikate im Kartenterminal 41
2.9.5 Staging der Zertifikate des Konnektors 41
2.9.6 Verantwortlichkeiten für den Zertifikats-Lebenszyklus 42
2.9.6.1 gematik 43
2.9.6.2 TSP 43
2.9.6.3 Kartenherausgeber 43
2.9.6.4 Kartenhersteller 44
2.9.6.5 Hersteller einer Komponente 44
2.9.6.6 Betreiber einer Komponente 44
2.9.7 Gültigkeitszeiträume für Schlüssel 45

3 CA-Strukturen 46

3.1 Einführung 46
3.1.1 Übersicht Identitäten/Zertifikate 46

3.2 TSP-übergreifende CA-Struktur 49
3.2.1 nonQES-CA-Struktur für zentralisierte PKI 49
3.2.1.1 gematik Root-CA (im Kontext nonQES X.509-Zertifikate) 50
3.2.1.2 Komponenten- und Dienste-CA 51
3.2.1.3 Bereitstellung OCSP-Signer 51
3.2.1.4 Bereitstellung CRL-Signer 51
3.2.1.5 TSL Signer-CA 51
3.2.1.6 gematik CVC-Root-CA 51
3.2.1.7 CVC-CA 52

3.3 HBA-spezifische CA-Strukturen 52
3.3.1 QES-CA-Struktur für HBA-QES 52
3.3.2 nonQES-CA-Struktur für ENC, AUT, OSIG, CV 53
3.3.3 Sektorneutrale CA für HBA, BA und SMC-B 53

4 Statusprüfung bei X.509-Zertifikaten 55

4.1 Einführung 55

4.2 Eingangsanforderungen 55

4.3 Methoden der Statusprüfung 55
4.3.1 Dezentrale Statusprüfung mittels CRL 55
4.3.2 Serverbasierte Statusprüfung mittels OCSP 55
4.3.3 Sonderfälle der Statusprüfung 56

4.4 Logisches Konzept der OCSP-Dienste 57
4.4.1 OCSP Festlegungen 57
4.4.2 OCSP-Responder-Adresse 57
4.4.3 OCSP-Request 58
4.4.4 OCSP-Response 58
4.4.4.1 Zertifikatsstatus 58
4.4.4.2 Zeitpunkte in der OCSP-Response 58
4.4.4.3 Gültigkeitsdauer eines OCSP-Response (nonQES) 59
4.4.4.4 Signatur der OCSP-Responses 59
4.4.4.5 Fehlermeldungen in der OCSP-Response 60

4.5 OCSP-Dienste 60
4.5.1 OCSP-Responder Proxy 61
4.5.2 Einsatz von HSM 62

5 CVC-Grundlagen und CVC-Hierarchie 63

5.1 Funktion von CV-Zertifikaten 63

5.2 Hierarchie der CV-Zertifikate 64

5.3 Prozesse und Verantwortlichkeiten im Kontext CV-Zertifikate 64

5.4 Aufbau und Inhalt von CV-Zertifikaten für G1-Karten 65
5.4.1 Zugriffsprofile 65

5.5 Aufbau und Inhalt von CV-Zertifikaten für G2-Karten 65
5.5.1 Aufbau und Inhalt 65
5.5.2 Zugriffsprofile 66

5.6 Gültigkeitsmodell und Prüfung der CV-Zertifikate für G2-Karten 66

5.7 Konzeptionelle Grundlagen der Zertifikatserneuerung bei CV-Zertifikaten der G2-Karten 67
5.7.1 Definition Gültigkeitsdauer, Zertifikatserneuerung und Sperrbarkeit 67
5.7.2 Infrastruktur zur Zertifikatserneuerung 68

6 Zertifikatsprüfung 69

6.1 Grundlagen 69

6.2 Abgrenzung 69

6.3 Vertrauensraumprüfung in der TI 69
6.3.1 Ablaufschritte der Vertrauensraumprüfung 69

6.4 Vertrauensraumprüfung im Internet 71

6.5 Zertifikatsprüfung (nonQES) 71
6.5.1 Konzeptionelle Festlegungen zur Zertifikatsprüfung 71
6.5.2 Ablaufschritte der Zertifikatsprüfung 72
6.5.3 Weitere Prüfungen und Auswertungen 73

6.6 QES-Zertifikatsprüfung 76

6.6.1 Konzeptionelle Festlegungen zur QES-Zertifikatsprüfung 76
6.6.2 Ablaufschritte der QES-Zertifikatsprüfung 77

6.7 Festlegungen zur Durchführung 78
6.7.1 Durchführung von Zertifikatsprüfungen 78
6.7.2 Spezialfälle der Zertifikatsprüfung 78
6.7.3 Bedingungen für eine erfolgreiche Zertifikatsprüfung 80

7 Betriebliche Aspekte der PKI 81

7.1 Einführung 81
7.1.1 Rollen 81
7.1.2 Authentisierung der Rolleninhaber 81

7.2 Zulassung von TSP in den Vertrauensraum der TI 82
7.2.1 Zulassung von TSP-X.509 zur Aufnahme in die TSL 82
7.2.2 Zulassung von CVC-CAs der zweiten Ebene 83

7.3 TSP-Dienste im Rahmen des X.509-Zertifikatslebenszyklus 83
7.3.1 Registrierungsdienst 83
7.3.2 Erstellungsdienst 85
7.3.3 Statusprüfdienst 85
7.3.4 Sperrdienst 86

7.4 Verzeichnisdienst der TI 87
7.4.1 Geltungsbereich 87
7.4.2 Datenmodell 87
7.4.2.1 Basisdaten (zertifikatsbasiert) 88
7.4.2.2 Fachanwendungsdaten (optional) 88
7.4.3 Lifecyclemanagement für Verzeichniseinträge 88
7.4.4 Aufbau und Außensicht 89
7.4.4.1 Autorisierung 89
7.4.4.2 Sichtbarkeit in der TI 89

8 Anhang A – Verzeichnisse 91

8.1 Abkürzungen 91

8.2 Glossar 96

8.3 Abbildungsverzeichnis 96

8.4 Tabellenverzeichnis 96

8.5 Referenzierte Dokumente 97
8.5.1 Dokumente der gematik 97
8.5.2 Weitere Dokumente 97

1 Einordnung des Dokumentes

1.1 Zielsetzung

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

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

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

Nach den einführenden Kapiteln werden folgende Themen behandelt:

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

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

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

Kap. 5 beschreibt die Besonderheiten von CV-Zertifikaten.

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

Kap. 7 skizziert die wesentlichen betrieblichen PKI-Prozesse.

1.2 Zielgruppe

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

1.3 Geltungsbereich

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

Schutzrechts-/Patentrechtshinweis

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

1.4 Methodik

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

Sie werden im Dokument wie folgt dargestellt:

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

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

2 Konzeptionelle Grundlagen

2.1 Einführung PKI der TI

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

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

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

TIP1-A_2030 - Bereitstellung von Sicherheitsgrundfunktionen auf Krypto-Basis
Die TI-Plattform MUSS kryptographisch basierte Verfahren zur Umsetzung der Schutzziele Authentizität, Nichtabstreitbarkeit, Integrität und Vertraulichkeit bereitstellen.
[<=]

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

TIP1-A_2032 - Abbildung von Akteuren auf elektronische Identitäten der TI
Die TI-Plattform MUSS die technisch sichere Abbildung von Akteuren auf elektronische Identitäten der TI in Form von Soft- oder Hardware-Sicherheitsmodulen (z.B. Chipkarten, HSM) realisieren.
[<=]

Die architektonische Einordnung der PKI erfolgt im Konzept „Architektur der TI-Plattform“ [gemKPT_Arch_TIP].

2.2 Basisfunktionen der PKI

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

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

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

TIP1-A_2033 - PKI-Dienste-Implementierung nach internationalen Standards
Die TI-Plattform SOLL die Konzeption der PKI-Dienste gemäß den internationalen Standards implementieren.
[<=]

2.3 Vertrauensmodelle in der PKI der TI

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

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

2.3.1 Vertrauensmodell für QES

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

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

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

TIP1-A_2034 - QES-PKI
Die TI-Plattform MUSS eine PKI für QES-Zertifikate in der TI gemäß [eIDAS] umsetzen.
[<=]

2.3.2 Vertrauensraum mittels TSL

Die vertrauenswürdigen Aussteller-CAs für X.509-Zertifikate werden in einer TSL einem einheitlichen Vertrauensraum unterstellt. Für die Implementierung wird das Konzept der „**T**rust-service **S**tatus **L**ist“ (TSL) gewählt. Dabei werden die Vertrauensinformationen der teilnehmenden Zertifikatsaussteller, der Trust Service Provider (TSP), in einer signierten XML-Datei abgelegt. Es gilt bei den nonQES-CA-Zertifikaten der TSL ihre Aufnahme in die TSL als hinreichendes Indiz für die Vertrauenswürdigkeit. Das Konzept der TSL ist durch ETSI normiert. Details sind in [ETSI_TS_102_231_V3.1.2] zu finden.

2.3.2.1 TSL in der TI im Kontext ECC-Migration

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

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

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

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

2.3.3 Vertrauensraum mittels TSL – Umsetzung in der TI

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

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

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

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

2.3.3.1 Bereitstellung der TSL als Vertrauensraum der TI

TIP1-A_2038 - Vertrauensraum mittels TSL
Die TI-Plattform MUSS für die Implementierung des Vertrauensraums das Konzept einer „Trust-service Status List“ (TSL) umsetzen.
[<=]

TIP1-A_2039 - Bereitstellung des TSL-Dienstes
Die TI-Plattform MUSS einen TSL-Dienst bereitstellen.
[<=]

TIP1-A_2683 - Bereitstellung nonQES-PKI in der TI
Die TI-Plattform MUSS eine PKI für nonQES-Zertifikate in der TI umsetzen.
[<=]

TIP1-A_2037 - Bereitstellung Vertrauensraum
Die TI-Plattform MUSS für alle X.509-nonQES-Zertifikate einen Vertrauensraum mit einer für die Kartenarten (1) eGK, (2) HBA, (3) SMC entsprechenden Policy umsetzen.
[<=]

TIP1-A_2054 - Downloadbarkeit der TSL
Der TSL-Dienst MUSS für die TSL als zentralen Vertrauensraum mehrere, voneinander unabhängige Downloadpunkte implementieren und publizieren, um die TSL hochverfügbar bereitzustellen.
[<=]

TIP1-A_2055 - Bereitstellung der TSL im Internet

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

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

2.3.3.2 Struktur, Signatur und Inhalt der TSL

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

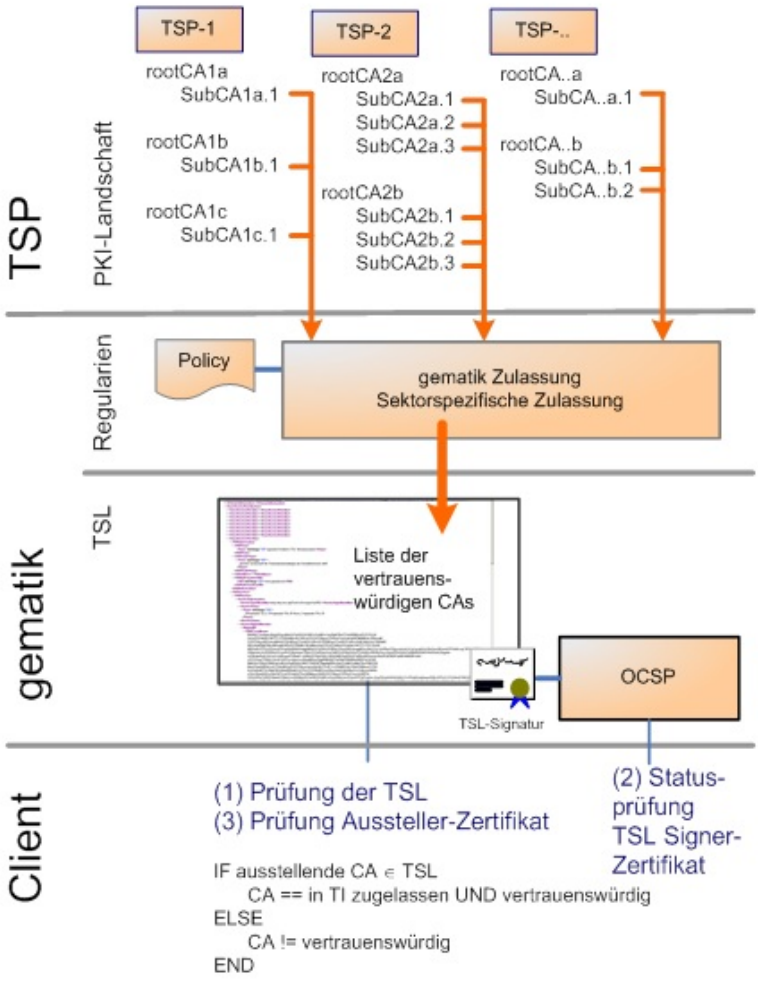

Abbildung 1: TSL-Modell

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

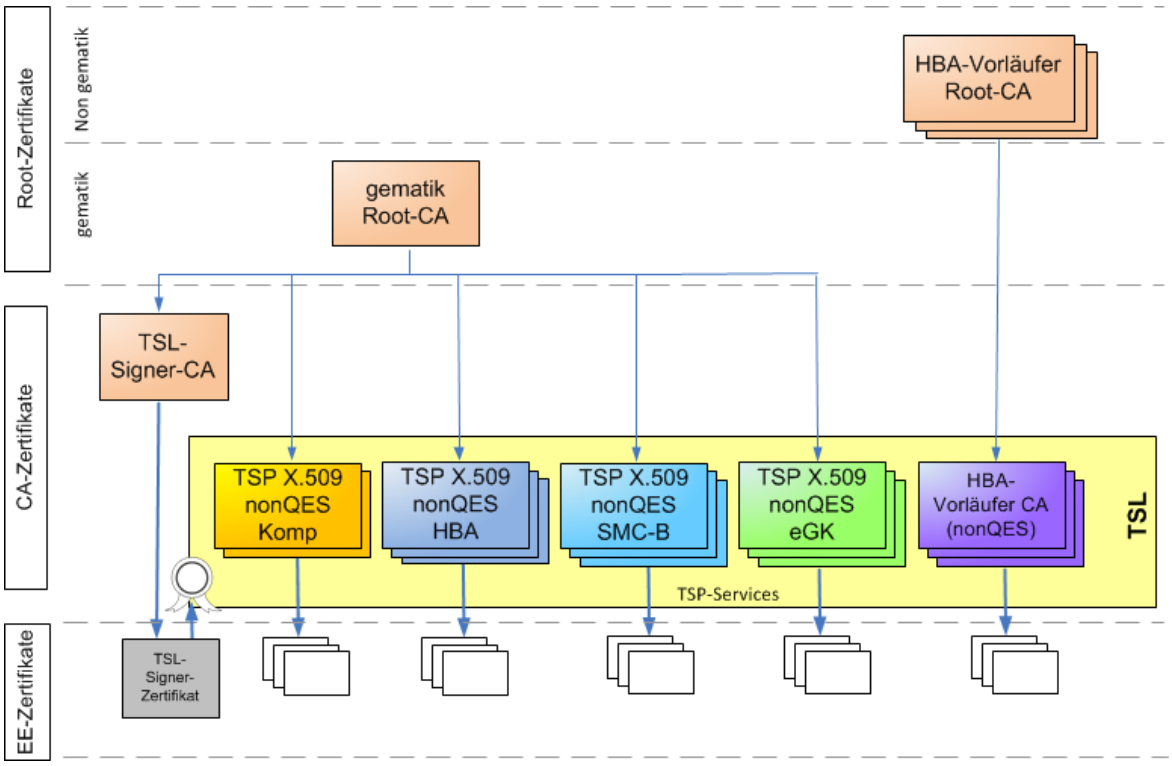

Abbildung 2: Zertifikatshierarchien und deren Abbildung in der TSL

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

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

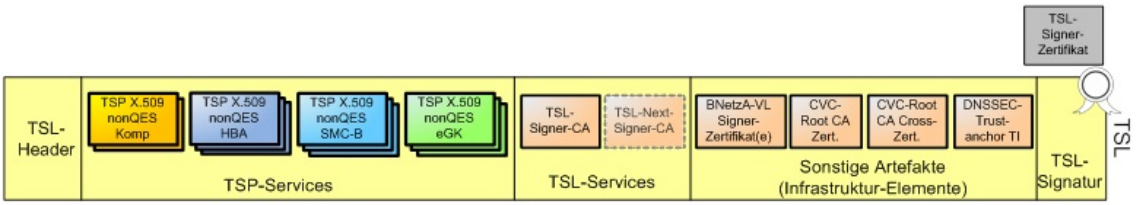

Abbildung 3: Aufbau der TSL

TIP1-A_2041 - Format der TSL nach [ETSI_TS_102_231_V3.1.2]

Der TSL-Dienst MUSS als technisches Format für die TSL das ETSI-Format nach [ETSI_TS_102_231_V3.1.2] „Provision of harmonized Trust-service status information“ umsetzen.
[<=]

TIP1-A_2040 - Signatur der TSL durch TSL-Signerzertifikat
Der TSL-Dienst MUSS jede zu publizierende TSL mit einem TSL-Signerzertifikat signieren
[<=]

TIP1-A_2042 - In TSL aufzunehmende Infos zu Zertifikatsherausgebern
Der TSL-Dienst MUSS in die TSL die folgenden Informationen bzgl. der einzelnen zugelassenen Zertifikatsherausgeber aufnehmen: (a) CA-Zertifikat, (b) Bereitstellungspunkt für Statusauskunft per OCSP (ggf. auch mehrere), (c) Signaturzertifikat des OCSP-Responders, (d) Kennung der für diesen Zertifikatsherausgeber erlaubten Zertifikatstypen.
[<=]

TIP1-A_2043 - Aufnahme von zugelassenen CAs in die TSL
Der TSL-Dienst MUSS das Aussteller-CA-Zertifikat einer CA, der innerhalb der TI ein vertrauenswürdiger Status zugewiesen werden soll, in die TSL aufnehmen.
[<=]

TIP1-A_2045 - Entfernen von abgelaufenen nonQES-CA-Zertifikaten aus der TSL
Der TSL-Dienst MUSS nonQES-CA-Zertifikate aus der TSL entfernen, sobald das Aussteller-CA-Zertifikat zeitlich abgelaufen ist.
[<=]

TIP1-A_2046 - Prüfung der Vertrauenswürdigkeit von Aussteller-CAs
Die TI-Plattform MUSS zur Feststellung der Vertrauenswürdigkeit einer Aussteller-CA zu einem gegebenen EE-Zertifikat prüfen, ob diese Aussteller-CA als Eintrag in der TSL vorhanden und zu diesem Zeitpunkt als gültig gekennzeichnet ist.
[<=]

Im Rahmen der Zertifikatsprüfung wird dann nicht das Root-Zertifikat geprüft, sondern nur der direkte Schritt zum CA-Zertifikat. Es müssen bei einer mehrstufigen Hierarchie nur die Zertifikate der ausstellenden CAs in die TSL aufgenommen werden, egal ob es sich dabei um self-signed-CA- oder Sub-CA-Zertifikate aus einer übergeordneten Root handelt.

TIP1-A_2047 - Kennzeichnung des Status von Aussteller-CAs in TSL
Der TSL-Dienst MUSS für jedes enthaltene Aussteller-CA-Zertifikat in der TSL ein Statuskennzeichen pflegen, in welchem der Status dieser CA dokumentiert ist und ab welchem Zeitpunkt (Datum) dieser Status gelten soll.
[<=]

2.3.3.3 Gültigkeit und Auswertung der TSL

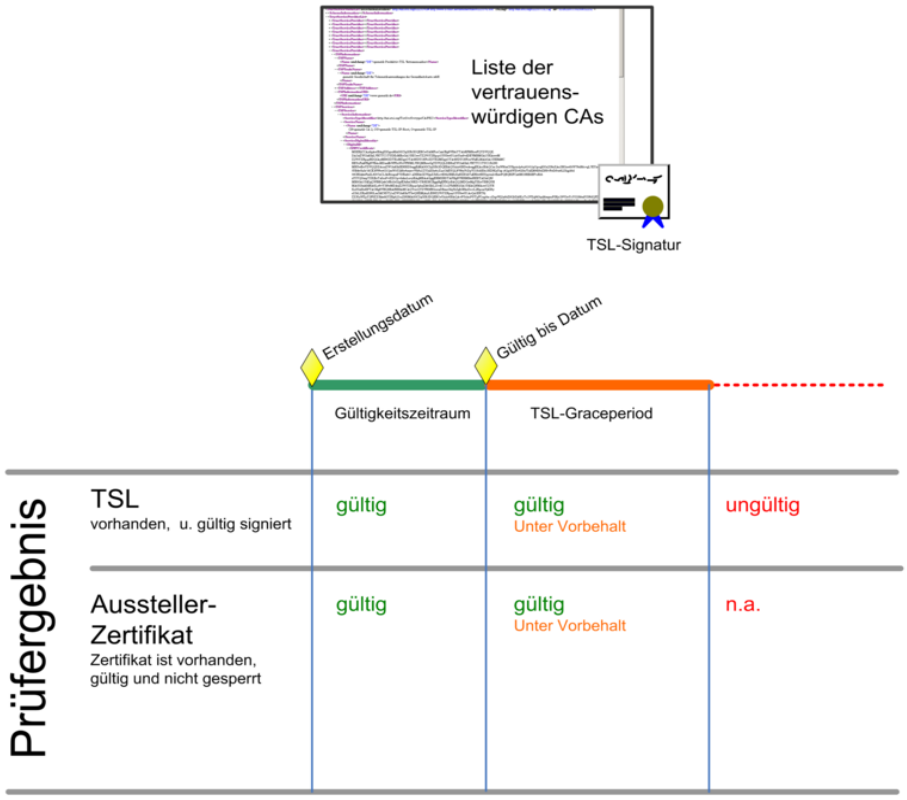

Abbildung 4: Gültigkeitszeiträume TSL

TIP1-A_2048 - Bereitstellung von TSL-Signer-CA- und –Signerzertifikat
Der TSL-Dienst MUSS den signaturprüfenden Komponenten das TSL-Signer-CA-Zertifikat, das TSL-Signerzertifikat und die URL des zugehörigen OCSP-Responder bereitstellen, um die Prüfung des Vertrauensraumes im Rahmen einer Zertifikatsprüfung zu ermöglichen.
[<=]

TIP1-A_2049 - Bereitstellung von Metainformationen zur TSL
Der TSL-Dienst MUSS in die TSL folgende Informationen zur Liste selbst bereitstellen, um die Aktualität der Liste auswertbar zu machen (a) Erstellungsdatum, ab dem die Liste als „aktuell“ gilt, (b) Geplantes Updatedatum, an dem die Liste durch eine neue Version aktualisiert werden soll, (c) inkrementelle Sequenznummer der Liste
[<=]

TIP1-A_2050 - Gültigkeit der TSL unter Vorbehalt
Die Produkttypen der TI-Plattform, die Zertifikate prüfen, MÜSSEN eine nicht mehr aktuelle TSL bis zu einem darüber hinausgehenden Zeitpunkt weiterhin als gültig unter Vorbehalt auswerten. Der Vorbehalt MUSS in einer Warnmeldung an die aufrufende Funktion bei der Zertifikatsprüfung mit dem Hinweis geliefert werden, dass die Prüfung gegen eine abgelaufene TSL erfolgte.
[<=]

Der Zeitraum nach Ablauf des Gültigkeitszeitraums der TSL, in dem gemäß [TIP1-A_2050] die TSL als „gültig unter Vorbehalt“ betrachtet wird, wird im Weiteren als „TSL-Graceperiod“ bezeichnet.

TIP1-A_2051 - CA-Zertifikatsprüfung innerhalb TSL-Graceperiod
Die Produkttypen der TI-Plattform, die Zertifikate prüfen, MÜSSEN eine TSL-Graceperiod konfigurierbar implementieren, innerhalb der die Prüfung eines enthaltenen und nicht gesperrten Aussteller-CA-Zertifikates ein Gültig-Ergebnis in Verbindung mit einer Warnmeldung liefern muss. Ein Defaultwert der TSL-Graceperiod MUSS in den Produkttypen voreingestellt sein.
[<=]

TIP1-A_2489 - CA-Zertifikatsprüfung nach Ablauf TSL-Graceperiod
Die Produkttypen der TI-Plattform, die Zertifikate prüfen, MÜSSEN nach zeitlichem Ablauf der TSL-Graceperiod bei der Prüfung eines Aussteller-CA-Zertifikates unabhängig vom Status dieses CA-Zertifikates ein Ungültig-Ergebnis der Zertifikatsprüfung in Verbindung mit einer Fehlermeldung liefern, da die TSL selbst als ungültig bewertet werden muss und damit keine valide Prüfbasis zur Verfügung steht.
[<=]

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

TIP1-A_2053 - Folgerungen des TSL-Prüfergebnisses Gültig unter Vorbehalt
Die Produkttypen der TI-Plattform, die Zertifikate prüfen, MÜSSEN die semantischen Folgerungen eines TSL-Prüfergebnisses „Gültig unter Vorbehalt (Ablaufdatum < aktueller Zeitpunkt < (Ablaufdatum + TSL-Graceperiod)) gemäß den eigenen Schutzbedarfen definieren und umsetzen.
[<=]

TIP1-A_2072 - Prüfung auf Aktualität der TSL
Alle zertifikatsprüfenden Komponenten in der TI-Plattform MÜSSEN in einem definierten Prüfintervall das Vorhandensein einer aktualisierten TSL prüfen und anhand eines optionalen Hashvergleichsverfahrens oder der Sequenznummer in der TSL entscheiden, ob die im Trust Store vorhandene TSL beibehalten wird oder durch eine neuere Version (höhere Sequenznummer) vom Verteilpunkt ersetzt werden muss.
[<=]

2.3.3.4 Initialisierung/Reinitialisierung des Vertrauensraums

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

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

TIP1-A_2056 - Sichere Einbringung des Vertrauensankers
Die TI-Plattform MUSS sicherstellen, dass in alle zertifikatsprüfenden Komponenten bei der Erstinbetriebnahme der Vertrauensanker in Form des TSL-Signer-CA-Zertifikates sicher eingebracht wird.
[<=]

TIP1-A_2435 - Verifikation des Vertrauensankers
Die TI-Plattform MUSS sicherstellen, dass bei allen zertifikatsprüfenden Komponenten im Zuge der Erstinbetriebnahme der initial eingebrachte Vertrauensanker (TSL-Signer-CA-Zertifikat) durch einen Berechtigten verifiziert wird.
[<=]

TIP1-A_2057 - Identifizierung und Verifizierung des TSL-Signer-CA-Zertifikates
Die TI-Plattform MUSS für die Bereitstellung und Übermittlung des TSL-Signer-CA-Zertifikates Verfahren zur Verfügung stellen, die eine sichere Identifizierung und Verifizierung genau dieses Zertifikates gewährleisten.
[<=]

TIP1-A_2058 - Schutz vor Überschreiben des TSL-Signer-CA-Zertifikates
Zertifikatsprüfende Komponenten in der TI-Plattform MÜSSEN sicherstellen, dass das TSL-Signer-CA-Zertifikat im komponenteninternen Trust Store durch einen geeigneten Schutzmechanismus vor missbräuchlichem Überschreiben oder Manipulation abgesichert wird.
[<=]

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

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

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

TIP1-A_2059 - Speicherung der TSL in lokalem Trust Store
Alle zertifikatsprüfenden Komponenten in der TI-Plattform MÜSSEN die Inhalte der TSL nach erfolgreicher Vertrauensraum- und syntaktischer Prüfung in einem lokalen Trust Store sicher speichern und zum weiteren Abruf lokal zugreifbar halten.
[<=]

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

2.3.3.5 Sperrung von CA-Zertifikaten in der TSL

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

Sicherheitskritischer Incident

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

- Festgestellte oder mögliche Kompromittierung des CA-Schlüssels

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

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

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

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

TIP1-A_2061 - Entzug des Vertrauensstatus einer CA bei sicherheitskritischen Incidents
Die TI-Plattform MUSS einer CA den Vertrauensstatus entziehen, wenn während des Gültigkeitszeitraumes des CA-Zertifikats Ereignisse eintreten, die eine Gewährleistung der technischen und/oder organisatorischen Sicherheit der CA hinsichtlich Registrierungs-, Erstellungs- und Sperrdienste nicht mehr ermöglichen oder auch nur substantiell in Frage stellen. Im Ergebnis MÜSSEN sowohl das CA-Zertifikat wie auch die darauf basierenden EE-Zertifikate bei einer Zertifikatsprüfung als ungültig ausgewiesen werden.
[<=]

TIP1-A_2062 - Entfernen von CA-Zertifikaten aus der TSL
Der TSL-Dienst MUSS ein gesperrtes Aussteller-CA-Zertifikat je nach Weisung des Servicebetriebsverantwortlichen der TI-Plattform zum festgelegten Termin entweder (a) mit einem Sperrdatum versehen oder (b) aus der TSL entfernen und umgehend eine aktualisierte TSL publizieren.
[<=]

Nicht-sicherheitskritischer Incident

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

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

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

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

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

TIP1-A_2064 - Entzug Vertrauensstatus einer CA bei nicht-sicherheitskritischen Incidents
Die gematik MUSS einer CA den Vertrauensstatus entziehen, wenn während des Gültigkeitszeitraumes des CA-Zertifikats Ereignisse eintreten, die gegen die Zulassungsvorgaben verstoßen, nicht aber die Sicherheit der TI und Anwendungen in Frage stellen. Im Ergebnis werden die von dieser CA bereits ausgestellten EE-Zertifikate bei einer Zertifikatsprüfung weiterhin als gültig ausgewiesen, nicht jedoch neu ausgestellte EE-Zertifikate dieser CA.
[<=]

TIP1-A_2065 - Umgang mit widerrufenen CA-Zertifikaten in der TSL
Der TSL-Dienst MUSS Aussteller-CA-Zertifikate, deren Zulassung durch die gematik aufgrund nicht-sicherheitskritischer Incidents widerrufen wurde, mit einem entsprechenden „revoked“-Status sowie dem Datum dieses Statuswechsels versehen und diese Angaben bis zum regulären Ablaufdatum des betreffenden CA-Zertifikates in der aktuellen TSL mitführen.
[<=]

TIP1-A_2066 - Verhinderung der Neuausstellung von EE-Zertifikaten bei Incidents
Ein TSP-X.509nonQES MUSS ab dem Zeitpunkt der Feststellung eines nicht-sicherheitskritischen Incidents sicherstellen, dass von der betroffenen CA keine neuen EE-Zertifikate für den Einsatz in der TI ausgestellt werden.
[<=]

TIP1-A_2067 - Operabilität von EE-Zertifikaten widerrufener CAs
TSP-X.509QES und TSP-X.509nonQES MÜSSEN sicherstellen, dass in den Fällen nicht-sicherheitskritischer Incidents bereits ausgegebene EE-Zertifikate weiterhin bis zu ihrem regulären Ablauf in der TI operabel bleiben. Hierbei MUSS er für diese Zertifikate weiterhin einen OCSP- und Sperrdienst in der vereinbarten Dienstgüte aufrecht erhalten.
[<=]

TIP1-A_2068 - Bewertung widerrufener CA-Zertifikate in der TSL
Alle zertifikatsprüfenden Komponenten in der TI-Plattform MÜSSEN bei der Prüfung von Aussteller-CA-Zertifikaten in der TSL den Status überprüfen. Ist der „revoked“-Status gesetzt, MUSS die Prüfroutine anhand des zugehörigen Datums auswerten, ob das zu prüfende EE-Zertifikat nach dem Statuswechsel der CA ausgegeben wurde. In diesem Fall MUSS die Prüfung ein negatives Ergebnis zurückliefern. Liegt das Ausgabedatum

des EE-Zertifikates vor dem Statuswechsel der CA auf „revoked“, MUSS das Aussteller-CA-Zertifikat als gültig zurückgemeldet werden.
[<=]

Übergreifende Festlegungen

TIP1-A_2069 - Bestätigung des Widerrufs von CA-Zertifikaten in der TSL
Bei dem Widerruf einer CA-Zulassung durch die gematik MUSS der betroffene TSP-X.509nonQES den Widerruf sowie die korrekte Durchführung der Auflagen (z. B. Sperrung von CA- und EE-Zertifikaten oder Sicherstellung des weiteren Betriebs von OCSP- und Sperrdienst) schriftlich gegenüber der gematik dokumentieren und die Umsetzung bestätigen.
[<=]

2.3.3.6 Aktualisierung des Vertrauensraumes

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

TIP1-A_2070 - Regelmäßige Neu-Ausstellung der TSL
Der TSL-Dienst MUSS eine neue TSL regelmäßig in Abhängigkeit des „Gültig bis Datum“ mit einer neuen Sequenznummer ausstellen, signieren und an den definierten Downloadpunkten bereitstellen – unabhängig davon, ob sich der Inhalt der TSL geändert hat oder nicht.
[<=]

Änderungen im Inhalt der TSL können sich ergeben durch:

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

2.3.3.7 Vertrauensankerwechsel

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

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

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

Ein Vertrauensankerwechsel stellt den Wechsel des TSL-Signer-CA-Zertifikates für einen TI-Vertrauensraum innerhalb einer Schlüsselgeneration (RSA oder ECDSA) dar. Ein Vertrauensankerwechsel zum Übergang (Migration) auf eine andere Schlüsselgeneration muss über andere Mechanismen (Initialisierung eines neuen Vertrauensankers z.B. über Cross-Zertifikate) realisiert werden.

TIP1-A_2074 - Neuausstellung und Verteilung des Vertrauensankers
Der TSL-Dienst MUSS rechtzeitig vor Ablauf des aktuellen TSL-Signer-CA-Zertifikates die Neuausstellung eines Folgezertifikates durchführen und dieses als „zukünftigen Vertrauensanker“ mittels der TSL an die zertifikatsprüfenden Komponenten verteilen.
[<=]

TIP1-A_2075 - Import des neuen Vertrauensankers in Trust Store
In der TI-Plattform MÜSSEN alle zertifikatsprüfenden Komponenten bei einem geplanten Wechsel des zentralen Vertrauensankers (TSL-Signer-CA-Zertifikat) bereits vor Ablauf des bestehenden Vertrauensankers das zukünftige Zertifikat in ihren lokalen Trust Store importieren und zum Aktivierungsdatum das alte mit dem neuen TSL-Signer-CA-Zertifikat ersetzen.
[<=]

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

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

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

2.3.4 Vertrauensmodell der nonQES TI-Zertifikate im Internet

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

TIP1-A_5130 - Unterstützung von HBA- und SMC-B Zertifikaten im Internet
Die TI-Plattform MUSS geeignete Maßnahmen implementieren, um die Statusauskünfte für nonQES X.509-Zertifikate im Internet bereitzustellen und diese gesichert mit den Statusauskünften in der TI zu synchronisieren.
[<=]

2.3.5 Vertrauensmodell von Zertifikaten der HBA-Vorläuferkarten in der TI

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

TIP1-A_5131 - CA-Zertifikate der HBA-Vorläuferkarten im TI-Vertrauensraum
Die TI-Plattform MUSS die zugehörigen CA-Zertifikate sowie OCSP-Signatur-Zertifikate von zu unterstützenden HBA-Vorläuferkarten (qSIG, ZOD) unter Einhaltung eines geregelten Registrierungsverfahrens in den Vertrauensraum der TI aufnehmen.
[<=]

TIP1-A_5282 - OCSP-Auskünfte der HBA-Vorläuferkarten innerhalb der TI
Die TI-Plattform MUSS die im Internet verfügbaren OCSP-Dienste von bereits zugelassenen Anbietern der HBA-Vorläuferkarten (qSIG-Karten, ZOD-Karten) innerhalb der TI verwenden.
[<=]

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

2.3.6 Vertrauensmodell CVC

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

Karten der TI müssen über folgende CV-Ausstattung verfügen:

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

Anmerkung: Für die Kartengeneration 2 werden die CV-Zertifikate auf ECC-basierte Kryptographie umgestellt. Eine Cross-Zertifizierung, die üblicherweise benutzt wird, um

die Verbindung zwischen zwei Zertifizierungsstellen herzustellen, kann nicht ohne Weiteres technologieübergreifend zwischen RSA-basierten und ECC-basierten Zertifikaten genutzt werden. Daher ist auch eine eigene, separate CVC-PKI für Kartengeneration 2 mit einer zweiten, separaten CVC-Root-CA notwendig.

TIP1-A_2077 - Umsetzung 2-stufiger CA-Hierarchie bei CVC-PKI
Die TI-Plattform MUSS das Vertrauensmodell für die Card-to-Card-Authentisierung über eine CVC-PKI mit 2-stufiger CA-Hierarchie umsetzen.
[<=]

TIP1-A_5132 - Bereitstellung einer CVC-Root-CA zur Nutzung für G2-Karten
Die TI-Plattform MUSS eine CVC-Root-CA betreiben, von der alle Sub-CAs zur Ausgabe von CV-Zertifikaten für G2-Karten (Verwendung in der TI) abgeleitet werden.
[<=]

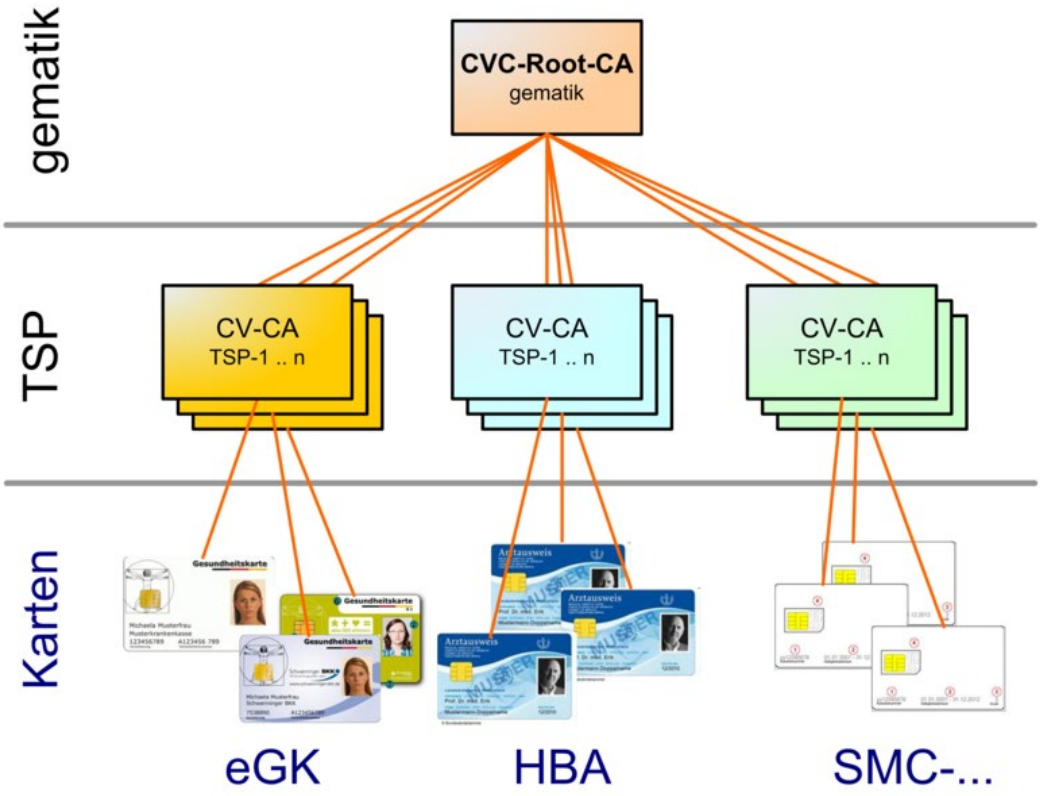

Abbildung 5: Hierarchie der CVC-PKI (je Kartengeneration)

2.4 Gültigkeitsmodelle X.509-Zertifikate

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

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

2.4.1 PKIX-Schalenmodell

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

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

Für die Nutzung in der TI reicht das Vorhandensein des Aussteller-CA-Zertifikats in der TSL als Nachweis der Vertrauenswürdigkeit aus. Die weitergehenden Prüfschritte bis zur Root-CA des Aussteller-CA-Zertifikates wurden vorgängig als Voraussetzung für die Zulassung der Aussteller-CA erfolgreich durchgeführt.

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

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

2.4.2 Kompromissmodell

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

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

2.4.3 QES-Kettenmodell

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

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

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

2.5 Zertifikatstypen in der TI und deren Verwendung

2.5.1 X.509-Zertifikate für Identitäten der TI

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

TIP1-A_4451 - Bereitstellung von X.509-Zertifikaten durch TSP-X.509
Die TI-Plattform MUSS TSPs bereitstellen, die nonQES-X.509-Zertifikate ausgeben und die dafür notwendigen Prozesse und Schnittstellen anbieten.
[<=]

TIP1-A_5133 - HBA- und SMC-B CA-Statusinformationen im Internet
Die gematik Root-CA MUSS CA-Statusinformationen für folgende Zertifikate
(a) C.HP.AUT,
(b) C.HP.ENC,
(c) C.HCI.AUT,
(d) C.HCI.ENC sowie
C.HCI.OSIG
in einem OCSP-Dienst im Internet zur Verfügung stellen.
[<=]

TIP1-A_5141 - Bereitstellung CA-Zertifikate und Fingerprints im Internet
Die gematik Root-CA MUSS CA-Zertifikate sowie deren Fingerprint (für Zertifikate, die im Internet prüfbar sein müssen) im Internet zur Verfügung stellen.
[<=]

TIP1-A_5134 - HBA- und SMC-B Statusinformationen im Internet
Ein TSP-X.509 nonQES MUSS die Statusinformationen für folgende Zertifikate
(a) C.HP.AUT,
(b) C.HP.ENC,
(c) C.HCI.AUT,
(d) C.HCI.ENC sowie C.HCI.OSIG in einem OCSP-Dienst im Internet zur Verfügung stellen.
[<=]

TIP1-A_2436 - Gültigkeitsdauer der X.509-Zertifikate
Die TI-Plattform MUSS für alle in der TI verwendeten X.509-Zertifikate einen Gültigkeitszeitraum in Form eines kalendarischen Datums „Nicht zu verwenden vor“ und „Nicht mehr verwenden nach“ zur Verfügung stellen.
[<=]

TIP1-A_4452 - Sperrung von Karten durch Sperrung der X.509-Zertifikate

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

TIP1-A_2437 - Sperrung von X.509-Zertifikaten
Die TI-Plattform MUSS für alle in der TI verwendeten X.509-Zertifikate, für die aus dem Anwendungskontext eine Statusprüfung gefordert ist, die Verfügbarkeit von Sperrprozessen und Statusauskünften sicherstellen, einschließlich der erforderlichen technischen und organisatorischen Schnittstellen.
[<=]

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

TIP1-A_2490 - Verwendungszweck von X.509-Zertifikaten
Ein TSP-X.509 MUSS sicherstellen, dass jedes für den Einsatz in der TI ausgestellte X.509-Zertifikat einen Verwendungszweck gemäß [RFC5280] enthält.
[<=]

2.5.2 CV-Zertifikate für Karten in der TI

- Zertifikate für Card-to-Card-Authentisierung und Autorisierung zwischen eGK und SMC-B, HBA sowie KTR-AdV (CV-Rollenzertifikate)
- Zertifikate für Card-to-Card-Authentisierung und Autorisierung für gerätespezifische Funktionen (gSMC-K, gSMC-KT, SMC-B, HBA – CV-Gerätezertifikate)

2.6 Verantwortliche Instanzen

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

TIP1-A_2081 - Spezifikation von Komponenten- und Dienstzertifikaten
Die TI-Plattform MUSS Zertifikate für Komponenten, zentrale Dienste und fachanwendungsspezifische Dienste sowie für Root-CAs, Aussteller-CA-Zertifikate sowie daraus abgeleitete EE-Zertifikate bereitstellen.
[<=]

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

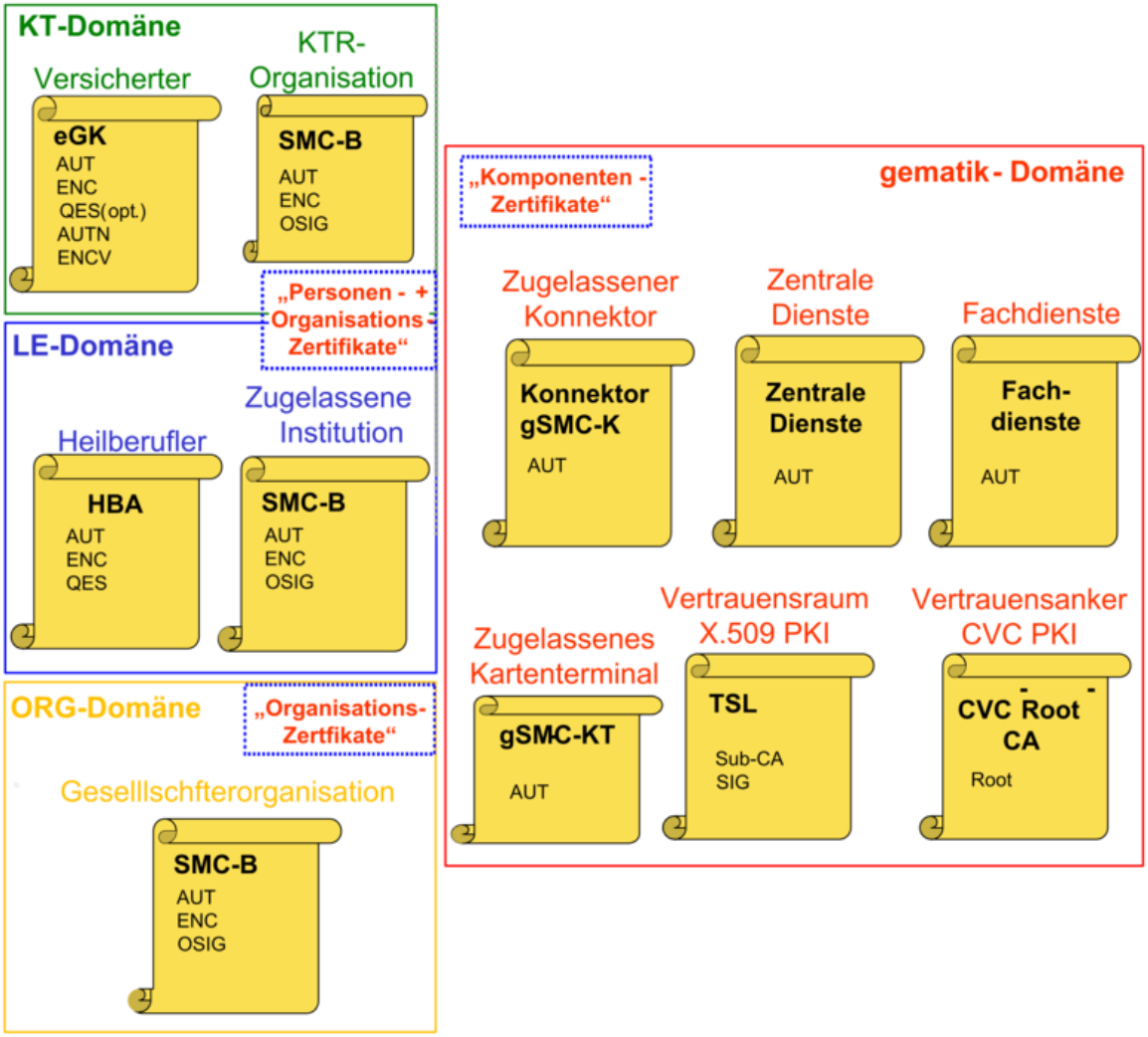

Abbildung 6: Zuordnung der Verantwortlichkeiten für die Zertifikate

TIP1-A_2084 - Vorgaben für HSM-B als SMC-B Ersatz
Ein HSM-B MUSS funktional vollständig eine (oder mehrere) SMC-B abbilden können, d. h. sich aus Sicht der Primäranwendung hinsichtlich CV- und X.509-Zertifikaten verhalten wie eine (hochperformante) SMC-B.
[<=]

2.7 Teilnehmer in der PKI

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

2.7.1 Trust Service Provider (TSP)

Trust Service Provider (TSP) stellen für den Einsatz in der Telematikinfrastruktur X.509- und CV-Zertifikate aus für natürliche und juristische Personen sowie für zentrale Dienste, fachanwendungsspezifische Dienste und technische Komponenten. Neben anderen Aufgaben sind TSP somit immer auch Zertifikatsherausgeber.

In [gemKPT_Arch_TIP] sind als TSP-Produkttypen definiert:

- gematik Root-CA
- TSP-X.509QES (auch als VDA für QES bezeichnet)
- TSP-X.509nonQES
- TSP-CVC
- CVC-Root-CA

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

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

TIP1-A_2085 - Forderung nach CP und CPS des TSP
Ein TSP-X.509 MUSS Festlegungen für Identifizierung, Registrierung, Herausgabe, Verlängerung und Sperrung von Zertifikaten in seiner Certificate Policy (CP) und seinem Certification Practice Statement (CPS) treffen sowie technisch und organisatorisch umsetzen, wobei seine Certificate Policy nicht im Widerspruch zur übergreifenden Certificate Policy der gematik bzw. der gemeinsamen HPC-Policy (für HBA-Zertifikate) stehen darf.
[<=]

TIP1-A_2086 - Zulassung von TSPs und Nachweis der Sicherheit
Ein TSP MUSS durch die gematik zugelassen sein, um in der TI Zertifikate herausgeben zu dürfen und muss dafür die Umsetzung der für ihn geltenden Sicherheitsanforderungen in einem Sicherheitskonzept beschreiben.
[<=]

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

TIP1-A_4453 - Sektorspezifische Zulassung von TSPs
TSP-X.509QES und TSP-X.509nonQES für Zertifikate der Leistungserbringer MÜSSEN eine sektorspezifische Zulassung erfolgreich durchlaufen haben, um in der TI Zertifikate herausgeben zu dürfen. Diese sektorspezifische Zulassung MUSS mindestens folgende Inhalte umfassen:
(1) Antrags- und Ausgabeprozess,
(2) Bestätigung der Sektorattribute,

(3) Produktionsfreigabe.
[<=]

TSP stehen mit den verantwortlichen Kartenherausgebern in enger Zusammenarbeit (s. a. Kapitel 2.7.3.1). Zusätzlich zu der Erfüllung der Sicherheitsanforderungen muss der TSP von der für die jeweiligen Zertifikate zuständigen Organisation für die Eintragung von bestimmten Rollen in X.509- bzw. eines bestimmten Profils in die CV-Zertifikate berechtigt werden. Die für die jeweiligen Berufs- bzw. Institutionsbezeichnungen zuständigen Organisationen legen Bedingungen für die Berechtigungserteilung fest.

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

TIP1-A_2089 - Grundaufgaben des TSP im Rahmen des Zertifikats-Lebens-zyklus
In der Rolle als Zertifikatsherausgeber MUSS ein TSP-X.509QES oder ein TSP-X.509nonQES in seinem Verantwortungsbereich
(a) die eindeutige Zuordnung von Zertifikaten zu Personen, zu ihren Rollen in der TI und zu Institutionen organisatorisch sicherstellen,
(b) die Endnutzerzertifikate sicher gemäß den für ihn geltenden Sicherheitsanforderungen erzeugen und dem Zertifikatsnutzer bereitstellen,
(c) für die identitätsbezogenen Endnutzerzertifikate die Zertifikatsantragsteller sicher gemäß den für ihn geltenden Sicherheitsanforderungen registrieren und dazu dokumentierte Registrierungsprozesse implementieren,
(d) für die identitätsbezogenen Endnutzerzertifikate den Zertifikatsnehmern gemäß den für ihn geltenden Sicherheitsanforderungen die Möglichkeit zur Sperrung ihrer Zertifikate anbieten und dazu dokumentierte Sperrprozesse implementieren.
[<=]

TIP1-A_2090 - Einbringung der Telematik-ID in HBA/SMC-B gemäß Profil
Wird ein TSP-X.509QES und TSP-X.509nonQES zur Zertifikatserstellung für HBA bzw. SMC-B beauftragt, MUSS er die dem Antragsteller zugeordnete Telematik-ID in das dafür laut Zertifikatsprofil vorgesehene Feld der X.509-Zertifikate für HBA bzw. SMC-B speichern.
[<=]

TIP1-A_2091 - Einbringung der KVNR in eGK und alternative Versichertenidentitäten gemäß Profil
Wird ein TSP-X.509QES und TSP-X.509nonQES zur Zertifikatserstellung für die eGK oder die alternativen Versichertenidentitäten beauftragt, MUSS er die dem Antragsteller zugeordnete Krankenversicherungsnummer in das dafür laut Zertifikatsprofil vorgesehene Feld der X.509-Zertifikate für die eGK speichern.
[<=]

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

2.7.2 Registrierungsstellen

Registrierungsstellen führen die Registrierungen von Zertifikatsnehmern durch, d. h. sie prüfen die eingereichten Zertifikatsanträge, erfassen deren Daten zur Zertifikatserstellung, archivieren die Anträge über definierte Zeiträume. Weiterhin nehmen die Registrierungsstellen auch Sperranträge entgegen, veranlassen die operative

Sperrung von Zertifikaten und betreiben eine Hotline für die von ihnen bereitgestellten Dienste.

Registrierungsstellen bilden die Kundenschnittstelle einer PKI zu den Zertifikatsnehmern.

2.7.3 Kartenherausgeber

Kartenherausgeber (Gesellschafterorganisationen (ORG), Leistungserbringerorganisationen (LEOs), Kostenträger (KTR) und Gerätehersteller) sind für die Herausgabe von eGK, HBA, SMC-B, gSMC-K und gSMC-KT zuständig. Die gematik ist für die Herausgabe von Prüfkarten zuständig.

TIP1-A_2094 - Rollenautorisierung von TSP durch Kartenherausgeber
Die Kartenherausgeber MÜSSEN die von ihnen beauftragten TSP (im Falle von eGK, gSMC-K und gSMC-KT) bzw. zugelassenen TSP (im Falle von SMC-B und HBA) bzgl. der Einbringung von Zertifikatsattributen für Rollen (Zugriffsprofile) in die Zertifikate autorisieren.
[<=]

TIP1-A_2098 - Umsetzung von Sperraufträgen durch Berechtigte
TSP-X.509QES und TSP-X.509nonQES MÜSSEN für die von ihm herausgegebenen Zertifikate Sperraufträge umsetzen, unter Anwendung der Berechtigungen gemäß Tab_PKI_107 sowie nach Authentifizierung und Berechtigungsprüfung der beauftragenden Person oder Organisationseinheit.
[<=]

Tabelle 1: Tab_PKI_107 Übersicht der PKI-spezifischen Sperrgründe

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

KTR **)		1a, 2					1a	2			
gematik	1a		3	3	3	3	3	3		1c,3	1c,3
BNetzA			4								

1a) Jederzeit ohne Angabe von Gründen

1b) Eventgetriggert im Rahmen eines definierten Incident-Prozesses mit den zuständigen und betroffenen Parteien

1c) Jederzeit ohne Angabe von Gründen für Zertifikate, die für den Produkttyp Service Monitoring erstellt wurden

2) Wegfall oder Entzug geforderter Eigenschaften des Antragstellers gemäß Ausgabepolicy

3) Wegfall oder Entzug geforderter Eigenschaften des TSP gemäß gematik-Zulassung

4) Verlust des Qualifikationsstatus des VDA für QES gemäß [eIDAS]

5) Wegfall oder Entzug geforderter Eigenschaften des VDA für QES /TSP gemäß Sektor-Zulassung

*) Berechtigung für organisatorische Sperrungen gilt nur für den jeweiligen Herausgeber der Zertifikate

**) In herausgeberspezifischen Policies können weitere Sperrgründe definiert sein.

***) incl. alternative Versichertenidentitäten

****) Wenn bei einer SMC-B ORG die herausgebende LEO identisch mit der zertifikatsnehmenden LEO ist, so kann sie ihre eigenen Zertifikate jederzeit ohne Angabe von Gründen sperren.

TIP1-A_2099 - Beschreibung von Herausgabeprozessen in Ausgabepolicy
Der Kartenherausgeber MUSS für die Beantragung, Herausgabe und Sperrung der in seinem Verantwortungsbereich befindlichen Karten und deren Zertifikate die dafür notwendigen Prozesse in einer Ausgabepolicy beschreiben und deren Umsetzung sicherstellen.
[<=]

TIP1-A_2100 - Verfahrensimplementierung zur Berechtigungsprüfung
TSP-X.509QES und TSP-X.509nonQES MÜSSEN die vom Kartenherausgeber vorgegebenen technischen und organisatorischen Verfahren implementieren, um die Berechtigung von Antragstellern für Sperraufträge nach den Regularien der Ausgabepolicy der betreffenden Zertifikate nachvollziehbar prüfen zu können.
[<=]

Kartenherausgeber haben je nach Kartenart unterschiedliche Aufgaben.

2.7.3.1 HBA-Herausgeber

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

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

TIP1-A_2103 - Prüfung der Berufsgruppenzugehörigkeit
Der Herausgeber des HBA MUSS die Zugehörigkeit des Antragstellers zu einer bestimmten Berufsgruppe (wie z. B. „Ärztin/Arzt“, „Apotheker/Apothekerin“) prüfen und dem TSP übermitteln, damit dieser die Information in den Zertifikaten speichert.
[<=]

Es gelten die folgenden Verantwortungsbereiche:

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

2.7.3.2 eGK-Herausgeber

Die Kostenträger sind für die eGK-Herausgabe verantwortlich.

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

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

2.7.3.3 Herausgeber der SMC-B

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

Zu unterscheiden sind dabei drei Ausprägungen der SMC-B:

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

Für die Herausgabe der SMC-B einer Gesellschafterorganisation ist verantwortlich:

- KZBV: Zertifikatsnehmer sind die Kassenzahnärztlichen Vereinigungen (KZVen) bzw. deren Geschäftsstellen
- KBV: Zertifikatsnehmer sind die Kassenärztlichen Vereinigungen (KVen) bzw. deren Geschäftsstellen
- GKV-Spitzenverband: Zertifikatsnehmer ist der GKV-Spitzenverband
- DAV: Zertifikatsnehmer sind der Deutsche Apothekerverband (DAV) und die Apothekerverbände (AVen)
- DKG: Zertifikatsnehmer sind die Deutsche Krankenhausgesellschaft (DKG), die Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH (DKTIG) sowie die Krankenhausverbände
- BÄK: Zertifikatsnehmer sind die BÄK und die Ärztekammern
- BZÄK: Zertifikatsnehmer sind die Landeszahnärztekammern

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

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

- Kassenärztliche Vereinigungen (KVen) für die Betriebsstätten ihrer Mitglieder:
  - Betriebstätte Vertragsarzt (inklusive ärztliche Psychotherapeuten) mit Zulassung gemäß [Ärzte-ZV] oder
  - Betriebstätte nicht-ärztlicher Vertragspsychotherapeut mit Zulassung gemäß [Ärzte-ZV]
- Für den jeweiligen Vertragszahnarzt/Vertragszahnarztpraxis zuständige KZV: Zahnarztpraxis mit vertragszahnärztlicher Zulassung (die jeweils zuständige KZV ist zudem berechtigt, auch SMC-B für Zahnärzte auszugeben, die sich im Zulassungsverfahren zur vertragszahnärztlichen Zulassung befinden). Die abschließenden Regelungen zur Antragsberechtigung werden von der jeweils zuständigen KZV festgelegt. Die TSP-Sektorzulassung im Bereich Vertragszahnärzteschaft für SMC-B Profil 2ZA wird von der KZBV durchgeführt.
- Offen: ausschließlich privatabrechnende Ärzte
- BZÄK: Zahnarztpraxis privat
- Für den jeweiligen Betriebserlaubnisinhaber zuständige Apothekerkammer.
- GKV-Spitzenverband: Betriebsstätten bzw. Geschäftsstellen der Kostenträger (gesetzlich),
- Kostenträger für AdV in Umgebungen in ihrem Auftrag (KTR-AdV)

2.7.3.4 Herausgeber von gSMC-K und gSMC-KT

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

2.7.3.5 Herausgeber von Prüfkarten

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

A_13539 - Auditrecht für Herausgabeprozesse der Prüfkarten
Der Kartenherausgeber von Prüfkarten eGK MUSS dem GKV-Spitzenverband als Eigentümer des Test.IK (welche auf einer Prüfkarte eGK das Institutionskennzeichen eines realen Kostenträger ersetzt) ein Auditrecht auf die Prozesse zur Herausgabe der Prüfkarte eGK gewähren.**[<=]**

2.7.4 Anbieter TSL-Dienst

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

2.7.5 Zertifikatsantragsteller

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

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

- Gesellschafterorganisationen,
- Leistungserbringer,
- medizinische Institutionen,
- Kostenträger,
- Gerätehersteller,
- Diensteanbieter.

TIP1-A_4454 - Einbringung registrierter Zulassungsdaten in X.509-Zertifikate
Die TI-Plattform MUSS sicherstellen, dass Zertifikatsantragsteller, die eine Zulassung durchlaufen, die im Rahmen der Zulassung registrierten relevanten Daten in die Zertifikate einbringen lassen.
[<=]

2.7.6 Zertifikatsnehmer

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

Bei personenbezogenen Zertifikaten sind Antragsteller und Zertifikatsnehmer identisch.

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

2.7.7 Zertifikatsnutzer

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

2.7.8 gematik

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

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

2.7.9 Andere Teilnehmer

2.7.9.1 Rollenvergabestelle

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

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

TIP1-A_2110 - Definition eines Systems für Rollenattribute
Die TI-Plattform MUSS ein System für Rollenattribute und den Zugriff auf diese definieren.
[<=]

TIP1-A_2111 - Definition und Koordination von Rollen für Akteure
Die Rollenvergabestelle MUSS die Definition der Rollen für technische und fachliche Akteure der TI mit den Teilnehmerorganisationen LEO, Kostenträger und gematik koordinieren und in eindeutige Rollenbezeichnungen überführen.
[<=]

TIP1-A_2112 - Überführung von Rollen in OIDs
Die Rollenvergabestelle MUSS die vereinbarten Rollen mittels eines Registrars in eindeutige OIDs überführen und diese in der TI verwalten und in der TI verfügbar machen.
[<=]

TIP1-A_2113 - Verwendung der zugewiesenen Rollenattribute
Alle Zertifikatsherausgeber MÜSSEN sicherstellen, dass bei der Zertifikatserstellung den EE-Zertifikaten nur genau die Rollenattribute zugewiesen werden, für die die Antragsteller gemäß Ausgabepolicy berechtigt sind.
[<=]

2.7.9.2 Attributsbestätigende Stellen

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

TIP1-A_2114 - Attributbestätigende Stelle für HBA-Berufsgruppenattribut
HBA-Kartenherausgeber MÜSSEN das Berufsgruppenattribut für die Zertifikate ihrer Mitglieder bestätigen und die Produktion des HBA gemäß ihrer Ausgabepolicy freigeben.
[<=]

TIP1-A_4455 - Attributbestätigende Stelle für SMC-B-Institutionsattribut
SMC-B-Kartenherausgeber MÜSSEN das Institutionsattribut für die Zertifikate ihrer Mitglieder bestätigen und die Produktion der SMC-B gemäß ihrer Ausgabepolicy freigeben.
[<=]

***Hinweis**: Das Institutionsattribut wird nur bei SMC-B für medizinische Institutionen gesetzt. Bei einer SMC-B für Gesellschafterorganisationen verhält sich die Attributbestätigung aber analog dazu: Der Kartenherausgeber (z.B. KZBV) bestätigt, dass es sich bei der SMC-B-haltenden Stelle um eine Gesellschafterorganisation handelt (z.B. KZV).*

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

TIP1-A_4456 - Bestätigende Stelle für technische Rollen
Herausgeber von gSMC-K/gSMC-KT respektive Dienstanbieter MÜSSEN die technische Rolle für die Zertifikate ihrer Komponenten bzw. Dienste bestätigen.
[<=]

2.8 Identifikation von Akteuren

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

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

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

2.8.1 Krankenversichertennummer

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

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

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

Für bestimmte Anwendungsfälle werden die Zertifikate C.CH.AUTN bzw. C.CH.ENCV verwendet, die anstelle der persönlichen Identifikationsdaten ein Pseudonym des Versicherten enthalten. Die versichertenindividuellen Pseudonyme werden durch den jeweiligen Kostenträger berechnet. Die Pseudonyme werden mit kryptographischen Verfahren aus dem unveränderbaren Teil der KVNR, dem Nachnamen des Versicherten und einer vom Herausgeber (Kostenträger) generierten Zusatzinformation (herausgeberspezifischer Zufallswert) gebildet.

2.8.2 Telematik-ID

Die eineindeutige elektronische Identifizierung der Teilnehmer der TI (Leistungserbringer als HBA-Halter bzw. medizinische Institutionen inklusive Einzelpraxen und Berufsausübungsgemeinschaften, Gesellschafterorganisations- und Kostenträgergeschäftsstellen als Halterinnen von SMC-B) erfolgt über die Telematik-ID. Die Sektoren des Gesundheitswesens verwalten jeweils einen Nummernkreis und weisen den Akteuren, für die sie zuständig sind, eine Telematik-ID zu. Die Granularität der Abbildung der existierenden Teilnehmer auf elektronische Identitäten obliegt den einzelnen Sektoren bzw. den konkreten Teilnehmern. So kann sich eine reale Institution

auch in unterschiedliche elektronische Identitäten aufteilen, mit jeweils eigenen SMC-B und Telematik-IDs.

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

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

A_18481 - Eineindeutigkeit der Telematik-ID
Der Kartenherausgeber MUSS sicherstellen, dass die Telematik-ID bezogen auf die elektronische Identität der betroffenen Teilnehmer in der Telematikinfrastruktur eineindeutig ist. **[**<=**]**

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

A_18482 - Keine Neuvergabe einer Telematik-ID für mindestens 5 Jahre
Ein Kartenherausgeber MUSS sicherstellen, dass eine Neuvergabe einer einmal vergebenen Telematik-ID für mindestens 5 Jahre ausgeschlossen wird. **[**<=**]**

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

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

TIP1-A_2124 - Verwendung der Telematik-ID
Ein Kartenherausgeber MUSS sicherstellen, dass als Präfix der Telematik-ID nur diejenige natürliche Zahl gesetzt wird, welche dem Sektor zugeordnet ist, den der Kartenherausgeber vertritt.
[<=**]**

2.9 Lebenszyklus von Zertifikaten

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

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

2.9.1 Definition der Begriffe

Definition: Generierung

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

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

Definition: Staging

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

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

Definition: Publizierung

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

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

Für CV-Zertifikate ist die Publizierung nicht relevant.

Definition: Sperrung

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

Eine Sperrung von CV-Zertifikaten ist technisch nicht möglich.

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

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

Es gibt zwei mögliche Varianten der Sperrung:

- Suspendierung
- endgültige Sperrung

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

Der Prozess des Widerrufs einer Suspendierung wird als Desuspendierung bezeichnet.

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

Definition: Gültigkeitsende

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

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

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

2.9.2 Lebenszyklus für Zertifikate ohne Status-Eigenschaft

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

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

2.9.3 Lebenszyklus für Zertifikate mit Statuseigenschaft

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

- Generierung
- Staging
- Publizierung
- Sperrung
- Gültigkeitsende

2.9.4 Staging der Zertifikate im Kartenterminal

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

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

2.9.5 Staging der Zertifikate des Konnektors

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

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

2.9.6 Verantwortlichkeiten für den Zertifikats-Lebenszyklus

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

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

- gematik
- TSP (Anbieter einer Aussteller-CA und/oder CVC-Sub-CA)
- Kartenherausgeber
- Kartenhersteller
- Hersteller einer Komponente
- Anbieter einer Komponente
- Karteninhaber

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

Tabelle 2: Verantwortlichkeiten in Bezug auf ein Zertifikat

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

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

Besonderheiten des Kartenterminals

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

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

Besonderheiten des Konnektors

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

2.9.6.1 gematik

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

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

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

Die gematik verantwortet Spezifikationen und übergreifende Policies.

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

2.9.6.2 TSP

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

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

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

TSP-X.509QES und TSP-X.509nonQES führen Sperrungen von X.509-Zertifikaten auf Veranlassung durch berechtigte Anbieter/Hersteller, Versicherte, Kostenträger, Leistungserbringer oder medizinische Institutionen durch. Die gematik kann in den im vorigen Abschnitt genannten Fällen sperrberechtigt sein.
Leistungserbringerorganisationen sind in der Rolle als attributsbestätigende Stelle ebenfalls sperrberechtigt.

2.9.6.3 Kartenherausgeber

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

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

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

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

2.9.6.4 Kartenhersteller

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

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

2.9.6.5 Hersteller einer Komponente

Hersteller Kartenterminal

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

Hersteller eines Konnektors

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

2.9.6.6 Betreiber einer Komponente

Organisation, die das eHealth-Kartenterminal einsetzt

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

Organisation des Gesundheitswesens, die einen Konnektor betreibt

Die Organisation lässt einen Konnektor aufbauen und installieren.

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

Anbieter eines zentralen oder fachanwendungsspezifischen Dienstes

Der Anbieter muss sich als solcher von der gematik zulassen.

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

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

2.9.7 Gültigkeitszeiträume für Schlüssel

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

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

TIP1-A_2492 - Rezertifizierung kryptographischer Schlüssel
Ein TSP-X.509 MUSS für die Ausstellung von Folgezertifikaten für eine gegebene kryptographische Identität der TI neue kryptographische Schlüssel erzeugen und verwenden.
[<=]

3 CA-Strukturen

3.1 Einführung

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

- Funktionelle Abdeckung aller benötigten Ausstelleridentitäten
- Wirtschaftliche Optimierung einer übergreifenden CA-Struktur
- Flexibilität hinsichtlich des marktoffenen Anbietermodells für spezifische CAs

3.1.1 Übersicht Identitäten/Zertifikate

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

- Zertifikate für zusätzliche Betriebsumgebungen (Referenz-BU, Test-BU, …)
- Ausprägung innerhalb der Kartenarten (Testkarten, Entwicklerkarten, …)

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

Optionale Zertifikate sind in Klammern gesetzt.

Tabelle 3: Übersicht Identitätselemente und Verantwortungsdomänen

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

medizinische Institution		OSIG, CVC		
SMC-B/HSM-B Gesellschafterorganisation		AUT, ENC, OSIG, CVC	AUT, ENC, OSIG, CVC	
SMC-B/HSM-B Kostenträger			AUT, ENC, OSIG, CVC	
gSMC-K (NK)	IPsec			
gSMC-K (AK)	TLS			
gSMC-K (SAK)	TLS CVC			
gSMC-KT	TLS			
Zentrale Dienste	gematik	LEO	KTR	BNetzA
VPN-Zugangsdienst	IPsec (TI) IPsec (SIS)			
weitere Zentrale Dienste	TLS-Server			
Fachanwendungsspezi- fische Dienste (derzeit nur VSDM)	gematik	LEO	KTR	BNetzA
Fachdienste	TLS-Client TLS-Server			
Intermediär	TLS-Client TLS-Server			
Infrastruktur	gematik	LEO	KTR	BNetzA
TSL	SIG			
OCSP	SIG	SIG	SIG	
qOCSP				QES
qOCSP-Proxy				n.a.
CRL	SIG			
Dezentrale Komponenten	gematik	LEO	KTR	BNetzA
eGK			AUT, ENC AUT-N, ENC- V CVC	(QES
HBA		AUT, ENC		QES

(alle Sektoren)		AUTO CVC		(Attribut)
SMC-B	CVC	AUT, ENC, OSIG, CVC	AUT, ENC, OSIG, CVC	
HSM-B	CVC	AUT, ENC OSIG, CVC	AUT, ENC, OSIG, CVC	
gSMC-K (NK)	IPSEC			
gSMC-K (AK)	TLS			
gSMC-K (SAK)	TLS CVC			
gSMC-KT	TLS			
Zentrale Dienste	gematik	LEO	KTR	BNetzA
VPN-Zugangsdienst	IPSEC (TI) IPSEC (SIS)			
weitere Zentrale Dienste	TLS-Server			
Fachanwendungsspezi- fische Dienste (derzeit nur VSDM)	gematik	LEO	KTR	BNetzA
Fachdienste	TLS-Client TLS-Server			
Intermediär	TLS-Client TLS-Server			
Clientmodul	TLS- Clientmodul			
Infrastruktur	gematik	LEO	KTR	BNetzA
TSL	SIG			
OCSP	SIG	SIG	SIG	
qOCSP				(QES)*)
qOCSP-Proxy				n.a.
CRL	SIG			

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

3.2 TSP-übergreifende CA-Struktur

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

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

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

TIP1-A_2127 - Zusammenfassung gleichrangiger CA-Instanzen
Die TI-Plattform SOLL funktional gleichrangige Aussteller-CA-Instanzen Sektor- und auch TSP-übergreifend zusammenfassen.
[<=]

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

Im Gegensatz dazu wird bei einem Wechsel der Schlüsselgeneration die Schlüssellänge oder der Algorithmus verändert. Dies kann durch neue kryptographische Vorgaben für CAs (vgl. auch [gemSpec_Krypt#GS-A_5079]) notwendig werden.

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

TIP1-A_6878 - Parallele Unterstützung verschiedener Schlüsselgenerationen
Die gematik Root-CA MUSS in der TI jeweils die in [gemSpec_Krypt] vorgegebenen Schlüsselgenerationen während einer Übergangszeit (s. [gemSpec_Krypt#GS-A_4357, GS-A_5079]) parallel unterstützen.
[<=]

TIP1-A_7022 - Unterstützung mindestens einer Schlüsselgeneration
Die TSP-X.509 QES und TSPX.509 nonQES MÜSSEN in der TI mindestens eine der in [gemSpec_Krypt] vorgegebenen Schlüsselgenerationen (s. [gemSpec_Krypt#GS-A_4357, GS-A_4358, GS-A_5079]) unterstützen.
[<=]

3.2.1 nonQES-CA-Struktur für zentralisierte PKI

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

Herausgeber: gematik

Anbieter: gematik

Zulassung: gematik

Policy: gematik, HBA-Herausgeber, BA-Herausgeber

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

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

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

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

Weiterhin wird die Zertifizierung von öffentlichen Aussteller-CA-Schlüsseln durch die gematik Root-CA im Sinne des marktoffenen Anbietermodells anderen in der TI zugelassenen ZDA und TSP angeboten. Hierfür stellt die gematik ein geeignetes organisatorisches Verfahren sowie der Anbieter der gematik Root-CA die erforderlichen technischen Schnittstellen und Funktionen bereit.

TIP1-A_2438 - X.509 nonQES gematik Root-CA
Die TI-Plattform MUSS in der TI eine zentrale X.509 nonQES-Root-CA unter der Bezeichnung „gematik Root-CA“ bereitstellen.
[<=]

TIP1-A_2439 - Policy der gematik Root-CA
Die gematik Root-CA MUSS die Regularien (Policy) vollständig beschreiben, unter denen die Zertifizierung von Sub-CA-Schlüsseln durch die gematik Root-CA erfolgt.
[<=]

TIP1-A_2128 - Lifecycle der gematik Root-CA
Die gematik Root-CA MUSS vollständig offline initialisiert und betrieben werden.
[<=]

TIP1-A_2129 - Sichere Signierung von Sub-CA-Zertifikaten
Der Anbieter der gematik Root-CA MUSS sicherstellen, dass die Signierung von Sub-CA-Zertifikaten der gematik Root-CA in einem geregelten und auditierten offline-Verfahren und unter Einhaltung aller Vorgaben des Sicherheits- und Betriebskonzeptes erfolgt.
[<=]

TIP1-A_2440 - Aufgaben der gematik Root-CA
Die gematik Root-CA MUSS Sub-CA-Zertifikate ausstellen, ggf. sperren und Statusinformationen zur Verfügung stellen für die nonQES-X.509-Aussteller-CAs . Dies umfasst die Einsatzbereiche:
a) nonQES HBA, BA,
b) SMC-B,
c) Komponenten und Dienste,

d) TSL-Signer,
e) nonQES eGK.
[<=**]**

TIP1-A_2441 - Sub-CA unterhalb der gematik Root-CA
Ein TSP-X.509nonQES MUSS seine Sub-CA-Zertifikate von der gematik Root-CA ableiten.**[**<=**]**

3.2.1.2 Komponenten- und Dienste-CA

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

- Geräte in den dezentralen Systemen (Konnektor, Kartenterminal, …)
- Zentrale Dienste (VPN-Zugangsdienst, KSR,…)
- Fachanwendungsspezifische Dienste (Fachdienste, Intermediär, …)

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

3.2.1.3 Bereitstellung OCSP-Signer

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

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

3.2.1.4 Bereitstellung CRL-Signer

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

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

3.2.1.5 TSL Signer-CA

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

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

3.2.1.6 gematik CVC-Root-CA

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

TIP1-A_2443 - gematik CVC-Root-CA

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

TIP1-A_2444 - Regularien der gematik CVC-Root-CA
Die TI-Plattform MUSS die Regularien zur gematik CVC-Root-CA vollständig beschreiben, unter denen die Ausstellung von CVC-CA-Zertifikaten der zweiten Ebene erfolgt.
[<=]

TIP1-A_2130 - Lifecycle der gematik CVC-Root-CA
Die TI-Plattform MUSS den Lifecycle der gematik CVC-Root-CA vollständig offline gestalten.
[<=]

TIP1-A_2131 - Sichere Signierung von CVC-Sub-CA-Zertifikaten
Die CVC-Root-CA MUSS sicherstellen, dass die Signierung von Sub-CA-Zertifikaten für in der TI zugelassene TSP-CVC in einem geregelten und auditierten offline-Verfahren und unter Einhaltung aller Vorgaben des Sicherheits- und Betriebskonzeptes erfolgt.
[<=]

3.2.1.7 CVC-CA

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

TIP1-A_2132 - Signierung von CVC-Sub-CA-Zertifikaten
Ein TSP-CVC MUSS seine CVC-Sub-CA bei der gematik CVC-Root-CA zertifizieren lassen, um CV-Zertifikate für zugelassene Kartenherausgeber erstellen zu können.
[<=]

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

3.3 HBA-spezifische CA-Strukturen

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

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

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

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

3.3.1 QES-CA-Struktur für HBA-QES

TIP1-A_2134 - gültiger Qualifikationsstatus

Ein TSP-X.509 QES als Zertifikatsherausgeber für QES-Zertifikate MUSS für den Betrieb seiner QES-Dienste deren gültigen Qualifikationsstatus gemäß [eIDAS] nachweisen.
[<=]

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

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

HBA-Herausgeber: LEO

Anbieter: am Markt agierender VDA für QES

Zulassung: LEO, gematik

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

Policy: LEO, gematik

HBA-Produktionsfreigabe: LEO

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

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

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

3.3.3 Sektorneutrale CA für HBA, BA und SMC-B

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

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

- Alle Sektoren mit ihren berufsständischen Vertretungen bzw. Leistungserbringerorganisationen (LEO)
- Einrichtungen der Kostenträger
- Perspektivisch alle Gesellschafterorganisationen (Gesellschafter der gematik und durch diese Gesellschafter vertretene Organisationen)
- Perspektivisch zusätzliche Akteure, die keiner approbierten und durch eine Ständevertretung repräsentierten Berufsgruppen angehören, sondern anderen –

den sog. Nicht-verkammerten – Berufen im Notfall-, Pflege- und Heilbereich angehören. Hierbei bestehen zahlreiche und vielfältige Kommunikations- und Datenschnittstellen zum Versicherten, zu Ärzten und Krankenhäusern sowie bei der Versorgung des Versicherten mit Heil- und Hilfsmitteln sowie therapeutischen Maßnahmen. Zukünftig besteht also Bedarf zu deren vollständigen Einbindung in die TI.
Um eine geregelte Versorgung dieser Berufsgruppen mit elektronischen Berufsausweisen (HBA) zu ermöglichen, wurde auf Beschluss der Gesundheitsminister der Länder die Etablierung eines länderübergreifenden Registers (eGBR) beschlossen, das die Rolle vergleichbar einer Ärztekammer übernehmen und deshalb im folgenden Text auch unter dem Begriff LEO subsumiert wird). Das eGBR ist derzeit im Aufbau befindlich und aktuell ist noch keine belastbare Spezifikation verfügbar.

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

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

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

Für Ausgabeprozesse und Policy gelten folgende Zuordnungen:

- für den HBA gelten die Festlegungen der gemeinsamen Policy (CP) der LEO [CP-HPC]
  Ggf. unabdingbar sektorspezifische Ausprägungen können als solche ausgewiesen und in die gemeinsame Policy aufgenommen werden.
  Für das QES-Zertifikat gelten darüber hinaus die gesetzlichen Regelungen für VDA für QES.
- für den BA muss eine entsprechende Policy durch das eGBR erstellt werden.
- für die nicht-personenbezogenen Zertifikate der Geräte und Dienste in der TI gilt die CP der gematik [gemRL_TSL_SP_CP].

4 Statusprüfung bei X.509-Zertifikaten

4.1 Einführung

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

4.2 Eingangsanforderungen

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

4.3 Methoden der Statusprüfung

4.3.1 Dezentrale Statusprüfung mittels CRL

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

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

TIP1-A_4457 - Statusprüfung von X.509-Zertifikaten des VPN-Zugangsdienstes
Die TI-Plattform MUSS die Statusprüfung der X.509-Zertifikate ID.VPNK.VPN bzw. ID.VPNK.VPN-SIS des VPN-Zugangsdienstes über im Internet verfügbare CRLs bereitstellen. Die TI-Plattform MUSS ebenfalls für die Verteilung der Sperrinformationen der eben genannten Zertifikate über OCSP im Internet Statusinformationen zur Verfügung stellen.
[<=**]**

4.3.2 Serverbasierte Statusprüfung mittels OCSP

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

Ein OCSP-Responder kann seine Informationen über verschiedene Quellen, wie der internen CA-Datenbank, aus einer LDAP-Datenbank oder einer CRL beziehen. Die Gültigkeitsangaben der originären Statusauskunft werden in der Antwort der OCSP-Response an den Client für weitere Auswertungen zurückgemeldet.

Jede OCSP-Response, welche Zertifikatsstatusinformationen enthält, wird vom OCSP-Responder signiert übermittelt, so dass auch die Authentizität des OCSP-Responder und die Integrität der Response geprüft werden kann.

4.3.3 Sonderfälle der Statusprüfung

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

Für dieses Szenario bieten sich folgende Lösungen:

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

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

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

TIP1-A_5448 - Zuordnung von CRL- und OCSP-Adressen in der TSL
Die TI-Plattform MUSS der in der TI zugelassenen CA zur Ausstellung von Zertifikaten für den VPN-Zugangsdienst innerhalb der TSL-Datenstruktur den zur Zertifikatsstatusprüfung per CRL zu verwendenden CRL Distribution Point (CDP)und die per OCSP zu verwendenden OCSP-Adressen zuordnen. Diese Adresse können von denjenigen in den zu prüfenden Zertifikaten abweichen.
[<=]

TIP1-A_4458 - Statusprüfung der ID.VPNK.VPN und ID.VPNK.VPN-SIS (Zugangspunkt TI bzw. Sicherer Internetzugang)
Produkttypen der TI, die die Zertifikate der Identitäten ID.VPNK.VPN bzw. ID.VPNK.VPN-SIS prüfen, MÜSSEN den Sperrstatus dieser Zertifikate per CRL oder OCSP prüfen.
[<=]

4.4 Logisches Konzept der OCSP-Dienste

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

4.4.1 OCSP Festlegungen

TIP1-A_2140 - Standard für OCSP-Dienste
TSP-X.509QES und TSP-X.509nonQES MÜSSEN für alle X.509-Zertifikate (außer denen für eGK) OCSP-Dienste in der TI gemäß [Common-PKI] unter obligatorischer Verwendung der CertHash-Erweiterung (Positive Statement) implementieren.
[<=]

TIP1-A_2493 - Standard für OCSP-Dienste für eGK
TSP-X.509QES und TSP-X.509nonQES MÜSSEN für alle X.509-Zertifikate der eGK OCSP-Dienste in der TI gemäß [RFC2560] implementieren.
[<=]

4.4.2 OCSP-Responder-Adresse

TIP1-A_2138 - Einbringung der OCSP-Adresse ins Zertifikat
TSP-X.509QES und TSP-X.509nonQES MÜSSEN für jedes von ihnen ausgestellte X.509-Zertifikat einer in der TI zugelassenen CA die Adresse des zur ausgebenden CA zugehörigen OCSP-Responders in das Zertifikat einbringen. Ausnahmen hiervon bilden Zertifikate, für die per Definition keine Statusprüfung vorgesehen ist.
[<=]

TIP1-A_2142 - Zuordnung von OCSP-Adressen in der TSL
Die TI-Plattform MUSS jeder in der TI zugelassenen CA innerhalb der TSL-Datenstruktur für Zertifikatstatusanfragen zu verwendende OCSP-Responder-Adresse(n) zuordnen. Diese Adressen können von denjenigen in den zu prüfenden Zertifikaten abweichen.
[<=]

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

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

Die Anwendungen außerhalb der TI im Internet prüfen den Vertrauensstatus des Zertifikates direkt über die eingetragene URI der OCSP-Adresse im EE-Zertifikat selbst, da im Internet die Umsetzung des TI-Vertrauensraumes über OCSP-Dienste realisiert

wird. Die Statusanfragen zu den EE- wie auch den CA-Zertifikaten des Zertifizierungspfades werden somit jeweils an diejenige OCSP-Responder-Adresse gerichtet, die im Zertifikat hinterlegt ist.

TIP1-A_5137 - Auflösung von OCSP-Adressen im Internet
TSP-X.509QES und TSP-X.509nonQES MÜSSEN für Zertifikatstypen, die zusätzlich zur TI auch im Internet statusgeprüft werden, sicherstellen, dass die im Zertifikat eingetragene OCSP-Responder-Adresse im Internet aufgelöst und eine Statusabfrage erfolgreich durchgeführt werden kann.
[<=]

4.4.3 OCSP-Request

TIP1-A_2143 - Umgang mit signierten OCSP-Requests
TSP-X.509QES und TSP-X.509nonQES MÜSSEN sicherstellen, dass die von ihm betriebenen OCSP-Responder signierte Requests nach [RFC2560] sowie [Common-PKI] beantworten. Aus Gründen der Performance MUSS der OCSP-Responder signierte Requests wie unsignierte Requests behandeln, d.h. die Signaturprüfung entfallen lassen.
[<=]

TIP1-A_2144 - Anzahl Zertifikate je OCSP-Request
Die TI-Plattform MUSS sicherstellen, dass je OCSP-Request nicht mehr als der Status für genau ein Zertifikat abgefragt werden darf (abweichend von [RFC2560], wonach je Request die Status mehrerer Zertifikate angefordert werden kann).
[<=]

4.4.4 OCSP-Response

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

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

4.4.4.1 Zertifikatsstatus

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

4.4.4.2 Zeitpunkte in der OCSP-Response

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

TIP1-A_2145 - Zeitpunkt in OCSP-Response auf Basis verbindlicher Zeitquelle
Der OCSP-Dienst MUSS sicherstellen, dass die OCSP-Response den Zeitpunkt, zu dem der Status des angefragten Zertifikates festgestellt wurde, enthält. Dieser Zeitpunkt muss auf einer in der TI verbindlich geltenden Zeitquelle beruhen.
[<=]

Zusätzlich bestimmen weitere Parameter die semantische Bedeutung dieses Zeitpunktes:

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

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

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

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

TIP1-A_4459 - Aktualität von OCSP-Responses
Der OCSP-Dienst MUSS die Aktualität von OCSP-Responses sicherstellen.
[<=]

4.4.4.3 Gültigkeitsdauer eines OCSP-Response (nonQES)

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

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

- Verkürzung der Response-Laufzeiten
- Reduzierung der Netzlast
- Implementierung dedizierter OCSP-Proxy (hochperformant, hochverfügbar, skalierbar)

4.4.4.4 Signatur der OCSP-Responses

TIP1-A_2146 - Signatur der OCSP-Response
Der OCSP-Dienst MUSS jede Antwort eines OCSP-Responders gemäß [RFC2560] signieren.
[<=]

TIP1-A_2147 - Signatur der nonQES-OCSP-Response
Der OCSP-Dienst MUSS die Signatur einer Statusantwort für ein nonQES-Zertifikat durch einen OCSP-Responder mit einem nonQES-Zertifikat erzeugen.
[<=]

TIP1-A_2148 - Performance-Erhöhung bei OCSP durch Caching

Der OCSP-Dienst SOLL die Performance durch Methoden des Response-Caching steigern.
[<=]

4.4.4.5 Fehlermeldungen in der OCSP-Response

TIP1-A_2149 - Auswertung von OCSP-Responses
Die Produkttypen der TI-Plattform, die OCSP-Responses auswerten, MÜSSEN für jede mögliche Ausprägung der zurückgelieferten Parameter (Exception Cases, Zeiten, Fehlercodes) eine geordnete Reaktion implementieren.
[<=]

TIP1-A_2150 - Ausschluss der Anforderung signierter OCSP-Requests
Der OCSP-Dienst DARF NICHT mit einem Fehlercode antworten, der den Client zur Übermittlung eines signierten Requests auffordert, da innerhalb der TI keine signierten OCSP-Requests gefordert sind.
[<=]

4.5 OCSP-Dienste

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

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

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

TIP1-A_2446 - Signaturzertifikate für OCSP-Responder in der TI
Produkttypen der TI, die nonQES-Statusauskünfte per OCSP bereitstellen, SOLLEN für ihre nonQES-OCSP-Responder die Signaturzertifikate gemäß [RFC6960] erstellen. Ausgenommen davon sind nach Kompromissmodell ausgestellte Zertifikate für die kein gültiges Signaturzertifikat mehr verfügbar ist. Für diese wird die OCSP-Statusauskunft durch eine andere CA übernommen und ggf. die Prüfbarkeit über die TSL sichergestellt.
[<=]

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

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

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

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

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

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

4.5.1 OCSP-Responder Proxy

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

- für Zertifikate der HBA-Vorläuferkarten

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

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

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

TIP1-A_2159 - Leistung des OCSP-Responder Proxy
Der OCSP-Responder Proxy MUSS die OCSP-Statusauskunft für Zertifikate der HBA-Vorläuferkarten in der TI verfügbar machen.
[<=]

TIP1-A_2160 - Erreichbarkeit des OCSP-Responder Proxy
Der OCSP-Responder Proxy MUSS in der TI durch alle Komponenten und Dienste erreichbar sein.
[<=]

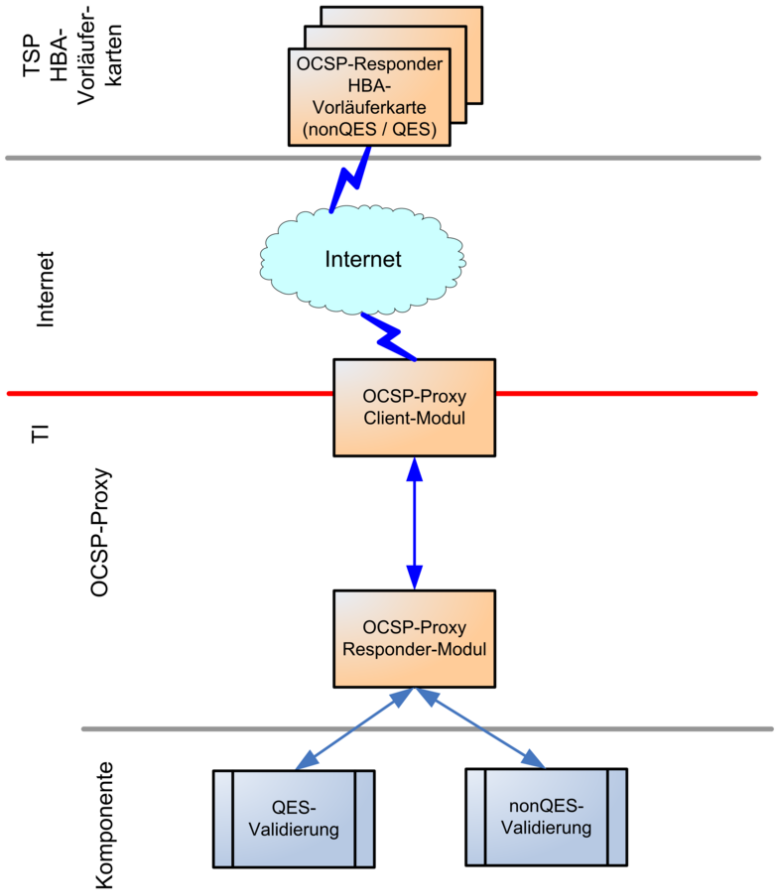

Abbildung 7: OCSP-Responder Proxy

4.5.2 Einsatz von HSM

TIP1-A_2163 - Einsatz von HSMs zur Signatur von OCSP-Responses
Der OCSP-Dienst KANN zur Signatur von OCSP-Responses ein HSM verwenden, sofern es die Anforderungen im jeweiligen Umfeld (nonQES, QES) erfüllt.
[<=]

5 CVC-Grundlagen und CVC-Hierarchie

5.1 Funktion von CV-Zertifikaten

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

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

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

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

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

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

- eGKs enthalten nur CV-Rollenzertifikate.
- gSMC-Ks und gSMC-KTs enthalten nur CV-Gerätezertifikate.
- HBAs und SMC-Bs enthalten sowohl CV-Rollenzertifikate als auch CV-Geräte-Zertifikate.
- Die KTR-AdV enthält zusätzlich zur SM-B ein zweites CV-Rollenzertifikat.

TIP1-A_2164 - Abbildung des Zugriffsprofils in CV-Rollenzertifikaten
Die TI-Plattform MUSS sicherstellen, dass für ein CV-Rollenzertifikat, das in einer eGK, einem HBA oder einer SMC-B enthalten ist, das Zugriffsprofil angegeben wird, in welcher Rolle der Karteninhaber (Person bzw. Organisation) an der TI teilnimmt.
[<=]

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

TIP1-A_2165 - Abbildung des Zugriffsprofils in CV-Gerätezertifikaten
Die TI-Plattform MUSS sicherstellen, dass für ein CV-Gerätezertifikat, das in einem HBA, einer SMC-B oder einer gSMC-K(T) enthalten ist, das für die jeweilige Funktionseinheit der Karte definierte Zugriffsprofil implementiert wird.
[<=]

5.2 Hierarchie der CV-Zertifikate

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

TIP1-A_2167 - Ausstellung von CV-Kartenzertifikaten durch CVC-Sub-CA
Die TI-Plattform MUSS sicherstellen, dass die EE-CV-Zertifikate über die kartenindividuellen CV-Schlüssel einer Chipkarte (eGK, HBA, SMC) durch eine CVC-CA der zweiten Ebene ausgestellt werden.
[<=]

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

5.3 Prozesse und Verantwortlichkeiten im Kontext CV-Zertifikate

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

TIP1-A_2169 - Definition von Ausgabepolicy und Betriebsvorgaben für CVC-Root-CA
Die TI-Plattform MUSS für die CVC-Root-CA eine Ausgabepolicy sowie Vorgaben für den Betrieb dieser CA definieren und deren Einhaltung durch geeignete Maßnahmen sicherstellen.
[<=]

TIP1-A_2170 - Definition von Betriebsvorgaben für CVC-Sub-CAs
Die TI-Plattform MUSS für die Zertifizierung von Sub-CVC-CA über alle TSP-CVC einheitlich geltende Vorgaben für den Betrieb dieser CA definieren und deren Einhaltung durch geeignete Maßnahmen sicherstellen.
[<=]

TIP1-A_2171 - Erstellung Ausgabepolicy durch TSP-CVC
Ein TSP-CVC MUSS für die Produktion von EE-CV-Zertifikaten eine Ausgabepolicy erstellen, die nicht im Widerspruch zu den übergeordneten Ausgabepolicies stehen darf.
[<=]

TIP1-A_2172 - Erstellung Sicherheitskonzept Zertifikatsprozess durch TSP-CVC
Ein TSP-CVC MUSS für den Betrieb einer Sub-CVC-CA in einem Sicherheitskonzept den Gesamtprozess von der Beantragung bis zur Einbringung des CV-Zertifikates in eine

Chipkarte beschreiben und die Einhaltung der beschriebenen Maßnahmen auf Verlangen der TI-Plattform nachweisen. Sind mehrere Organisationen an diesem Prozess beteiligt, sind die technischen und organisatorischen Schnittstellen sowie deren Absicherung zu beschreiben – ggf. auch durch Referenzierung der Sicherheitskonzepte der beteiligten Organisationen.
[<=]

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

5.4.1 Zugriffsprofile

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

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

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

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

5.5.1 Aufbau und Inhalt

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

TIP1-A_5138 - Struktur der CV-Zertifikate der Kartengeneration 2
Die TI-Plattform MUSS CV-Zertifikate der Kartengeneration 2 gemäß der in Tab_PKI_108 definierten Struktur bereitstellen.
[<=]

Tabelle 4: Tab_PKI_108 Informationen für ein CV-Zertifikat G2

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

Tabelle 5: Übersicht Felder eines CV-Zertifikats

Feld	Inhalt
CPI	Certificate Profile Identifier: Dieser legt die genaue Struktur der Nachricht fest, über die die Signatur berechnet wird.

CAR	Certification Authority Reference: Eindeutiger Bezeichner des Schlüsselpaares, mit dessen privatem Schlüssel die CVC-CA das CV-Zertifikat signiert hat.
Öffentl. Punkt Q	Öffentlicher Punkt Q des öffentlichen Schlüssels, für den das CV-Zertifikat berechnet wird.
OIDPuK	OID des Algorithmus, mit dem der öffentliche Schlüssel des Zertifikatsinhabers (CVC-CA oder Chipkarte) genutzt werden kann.
CHR	Certificate Holder Reference: Eindeutiger Bezeichner des Schlüsselpaares des Zertifikatsinhabers, dessen öffentlichen Schlüssel in dem CV-Zertifikat enthalten ist.
CHAT	Certificate Holder Authorisation Template: Legt die Rolle des Zertifikatsinhabers fest.
CED	Certificate Effective Date: Ausgabezeitpunkt, ab wann das Zertifikat gültig ist
CXD	Certificate Expiration Date: Zeitpunkt für das Gültigkeitsende

5.5.2 Zugriffsprofile

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

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

Die Zertifikatsprüfung von CV-Zertifikaten ist 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.

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

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

TIP1-A_5139 - Prüfung von CV-Zertifikaten der Kartengeneration 2

Die TI-Plattform MUSS eine Prüfmöglichkeit für CV-Zertifikate der Kartengeneration 2 bereitstellen.
[<=]

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

Nach Ablauf des Gültigkeitszeitraums kann keine erfolgreiche C2C-Authentisierung mehr durchgeführt werden. Im Gegensatz zu den CV-Zertifikaten für G1-Karten sollen für die CV-Zertifikate der G2-Karten eine Zertifikatserneuerung implementiert und damit die Gültigkeitsdauer verlängert werden.

TIP1-A_5140 - Gültigkeitsdauer bei CV-Zertifikaten der Kartengeneration 2
Die TI-Plattform MUSS die Gültigkeitsdauer von CV-Zertifikaten der Kartengeneration 2 beschränken.
[<=]

5.7 Konzeptionelle Grundlagen der Zertifikatserneuerung bei CV-Zertifikaten der G2-Karten

5.7.1 Definition Gültigkeitsdauer, Zertifikatserneuerung und Sperrbarkeit

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

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

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

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

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

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

5.7.2 Infrastruktur zur Zertifikatserneuerung

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

6 Zertifikatsprüfung

6.1 Grundlagen

Die Zertifikatsprüfung gliedert sich in zwei wesentliche Schritte:

- Prüfung des Vertrauensraums
- Prüfung des eigentlichen Zertifikats

6.2 Abgrenzung

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

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

Für die Zertifikatsprüfung im Internet gilt die Vorgehensweise nach [Common-PKI].

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

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

6.3 Vertrauensraumprüfung in der TI

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

6.3.1 Ablaufschritte der Vertrauensraumprüfung

TIP1-A_2174 - Ablaufschritte der Vertrauensraumprüfung
Die TI-Plattform MUSS die Prüfung des TI-Vertrauensraums entsprechend der in Tab_PKI_104 definierten Ablaufschritte umsetzen.
[<=]

Tabelle 6: Tab_PKI_104 Ablaufschritte der Vertrauensraumprüfung

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

6.4 Vertrauensraumprüfung im Internet

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

6.5 Zertifikatsprüfung (nonQES)

6.5.1 Konzeptionelle Festlegungen zur Zertifikatsprüfung

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

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

Als Optimierung gegenüber [Common-PKI] wird die Signaturprüfung des OCSP-Signerzertifikats nicht nach den kompletten Prüfschritten durchgeführt. Das TSL-Konzept erlaubt die OCSP-Signerzertifikate der TSP in die TSL aufzunehmen.

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

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

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

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

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

Es ist möglich, der Zertifikatsprüfung den Zeitpunkt mitzugeben, für den diese Prüfung relevant sein soll, dieser wird auch als „Referenzzeitpunkt“ bezeichnet. Dies kann die

aktuelle Systemzeit sein, wenn die Prüfung zum Zeitpunkt „Jetzt“ erfolgen soll, um bspw. Ein Verschlüsselungszertifikat des Kommunikationspartner zu prüfen, aber auch ein Zeitpunkt in der Vergangenheit, wie bspw. Im Rahmen einer Signaturprüfung der Zeitpunkt der Signaturerstellung, der sich aus der Signatur entnehmen lässt.

6.5.2 Ablaufschritte der Zertifikatsprüfung

TIP1-A_2175 - Ablaufschritte der Zertifikatsprüfung nonQES
Die TI-Plattform MUSS die Prüfung von Zertifikaten entsprechend der in Tab_PKI_105 definierten Ablaufschritte umsetzen.
[<=]

Tabelle 7: Tab_PKI_105 Ablaufschritte der Zertifikatsprüfung

Ablaufschritte der Zertifikatsprüfung nonQES **Anmerkung: Die Sequenz der Ablaufschritte ist funktional hergeleitet, kann jedoch auch anders gestaltet werden, sofern das Ergebnis der Prüfung qualitativ äquivalent ist.**	
Ablaufschritt 1	Prüfung der Vertrauenskette
Beschreibung	Prüfung, ob das zugehörige Ausstellerzertifikat in der TSL enthalten ist
Vorbedingung	TSL-Informationen in sicherem Speicher vorhanden
Anmerkungen	Die Prüfung erfolgt über den Vergleich von „Aussteller im Endnutzerzertifikat“ mit „Inhaber im CA-Zertifikat“.
Ablaufschritt 2	Signaturprüfung
Beschreibung	Prüfung der mathematischen Korrektheit des Zertifikats (Ableitung vom ermittelten Ausstellerzertifikat)
Vorbedingung	vorliegendes Ausstellerzertifikat
Anmerkungen	Die Prüfung erfolgt über Verifikation der Signatur und Hashwert-Vergleich.
Ablaufschritt 3	Prüfung der zeitlichen Gültigkeit
Beschreibung	Prüfung, ob der Referenzzeitpunkt innerhalb des im Zertifikat definierten Gültigkeitszeitraums liegt
Vorbedingung	keine
Anmerkungen	Im Zertifikat ist immer ein Zeitraum (gültig von … bis …) angegeben
Ablaufschritt 4	Prüfung des Sperrstatus
Beschreibung	Prüfung, ob Zertifikat gesperrt ist durch Abfrage des OCSP-Responders, ggf. durch Auswertung von in Signatur eingebetteter OCSP-Response
Vorbedingung	TSL-Informationen in sicherem Speicher vorhanden
Anmerkungen	OCSP-Adresse wird aus der TSL ermittelt, mehrere Adressen möglich, die der Reihe nach geprüft werden bis Prüfvorgang erfolgreich ist.

Ablaufschritt 5	Weitere Prüfungen und Auswertungen
Beschreibung	Weitere Schritte die gemäß relevanter Standards verpflichtend sind, sowie weitere TI-spezifische Auswertungen, s. Informationen in Abschnitt 6.5.3
Vorbedingung	

6.5.3 Weitere Prüfungen und Auswertungen

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

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

TIP1-A_2176 - Vorgaben zur Zertifikatsprüfung gemäß internationaler Standards
Die TI-Plattform MUSS bei der Prüfung von Zertifikaten Vorgaben hinsichtlich Prüftiefe und Prüfumfang gemäß den Standards [Common-PKI], [RFC2560] und [RFC5280] definieren.
[<=]

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

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

TIP1-A_2177 - Ermittlung von Rolleninformationen bei der Zertifikatsprüfung
Die TI-Plattform MUSS bei der Prüfung von Zertifikaten die Rolleninformation aus dem Zertifikat ermitteln und an die aufrufende Anwendung zurückgeben.
[<=]

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

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

TIP1-A_4499 - Ermittlung des Zertifikatstyps bei der Zertifikatsprüfung
Die TI-Plattform MUSS bei der Prüfung von Zertifikaten den Zertifikatstyp aus dem Zertifikat ermitteln und an die aufrufende Anwendung zurückgeben.
[<=]

Innerhalb des Prozesses zur Zulassung eines TSP-X.509 zur Aufnahme in die TSL können Informationen erfasst werden, für welche Zertifikatstypen dieser TSP mit der jeweiligen CA erstellungsberechtigt ist, z. B. nur für Komponentenzertifikate, oder nur für eGK-Zertifikate. Diese Informationen – hinterlegt im Element „ServiceInformationExtensions“ in der TSL (siehe TAB_PKI_113) – ergeben sich anhand der Beauftragungen durch die für den jeweiligen Kartentyp verantwortlichen Kartenherausgeber.

Tabelle 8: TAB_PKI_113 Zuordnung der (zugelassenen) X.509-Sub-CAs zu Zertifikatstypen

Spezifischer CA-Einsatzbereich	CN (<usage> im Feld DN)	OID-Referenz in anderen Dokumenten	Name des Zertifikatstyp	Referenz/Anmerkung
Elektronische Gesundheitskarte	<TSP>.eGK-CA<n> *) z.B. ATOS.EGK-CA201	oid_egk_enc	C.CH.ENC	[gemSpec_PKI#5.1.3;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_egk_encv	C.CH.ENCV	[gemSpec_PKI#5.1.3;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_egk_aut	C.CH.AUT	[gemSpec_PKI#5.1.3;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_egk_autn	C.CH.AUTN	[gemSpec_PKI#5.1.3;5.11] [gemSpec_OID# Tab_PKI_405]
	<TSP>.eGK-ALVI-CA<n> *)	oid_egk_aut_alt	C.CH.AUT_ALT	[gemSpec_PKI#5.1.3;5.11] [gemSpec_OID# Tab_PKI_405]
Heilberufsausweis	<TSP>.HBA-qCA<n> *) D-Trust.HBA-qCA1	oid_hba_qes	C.HP.QES	[gemSpec_PKI#5.11;5.11] [gemSpec_OID# Tab_PKI_405]
	<TSP>.HBA-CA<n> *) z.B. D-Trust.HBA-CA1	oid_hba_enc	C.HP.ENC	[gemSpec_PKI#5.11;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_hba_aut	C.HP.AUT	[gemSpec_PKI#5.11;5.11] [gemSpec_OID# Tab_PKI_405]

Institutionskarten	<TSP>.SMCB-CA<n> *) z.B. D-Trust.SMCB-CA1	oid_smc_b_enc	C.HCI.ENC	[gemSpec_PKI#5.3.4;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_smc_b_aut	C.HCI.AUT	[gemSpec_PKI#5.3.4;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_smc_b_osig	C.HCI.OSIG	[gemSpec_PKI#5.3.4;5.11] [gemSpec_OID# Tab_PKI_405]
Komponenten-PKI	<TSP>.KOMP-CA<n> *) z.B. GEM.KOMP-CA1	oid_fd_tls_s	C.FD.TLS-S	[gemSpec_PKI#5.9.3;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_zd_tls_s	C.ZD.TLS-S	[gemSpec_PKI#5.8.3;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_smkt_aut	C.SMKT.AUT	[gemSpec_PKI#5.5.2;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_nk_vpn	C.NK.VPN	[gemSpec_PKI#5.6.4;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_sak_aut	C.SAK.AUT	[gemSpec_PKI#5.6.4;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_ak_aut	C.AK.AUT	[gemSpec_PKI#5.6.4;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_cm_tls_c	C.CM.TLS-CS	[gemSpec_PKI#5.10.3;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_fd_tls_c	C.FD.TLS-C	[gemSpec_PKI#5.9.3;.11] [gemSpec_OID# Tab_PKI_405]
		oid_fd_aut	C.FD.AUT	[gemSpec_OID# Tab_PKI_405]

		oid_zd_tls_c	C.ZD.TLS-C	[gemSpec_OID# Tab_PKI_405] (derzeit nicht verwendet)
		oid_zd_aut	C.ZD.AUT	[gemSpec_OID# Tab_PKI_405] (derzeit nicht verwendet)
		oid_fd_sig	C.FD.SIG	[gemSpec_OID# Tab_PKI_405]
		oid_fd_enc	C.FD.ENC	[gemSpec_OID# Tab_PKI_405]
		oid_sgd_hsm_aut	C.SGD-HSM.AUT	[gemSpec_OID# Tab_PKI_405]
VPN-Zugangsdienst	<TSP>.VPNK-CA<n> *) z.B. GEM.VPNK-CA1	oid_vpnk_vpn	C.VPNK.VPN	[gemSpec_PKI#5.7.3;5.11] [gemSpec_OID# Tab_PKI_405]
		oid_vpnk_vpn_sis	C.VPNK.VPN-SIS	[gemSpec_PKI#5.7.3;5.11] [gemSpec_OID# Tab_PKI_405]

*) Für CA-Zertifikate der zentralen PKI wird für <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. Bei laufenden beispielshaften SubCA-Nummern können Abweichungen auftreten.

6.6 QES-Zertifikatsprüfung

6.6.1 Konzeptionelle Festlegungen zur QES-Zertifikatsprüfung

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

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

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

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

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

Generelle Prüfschritte gemäß [Common-PKI] und [RFC5280], wie die Prüfung der zeitlichen Gültigkeit , sind auch bei der QES-Prüfung obligatorisch. Sie sind in der folgenden Übersicht zwecks Vereinfachung und Übersichtlichkeit nicht aufgeführt.

6.6.2 Ablaufschritte der QES-Zertifikatsprüfung

TIP1-A_2178 - Ablaufschritte der QES-Zertifikatsprüfung
Die TI-Plattform MUSS die Prüfung von Zertifikaten entsprechend der in Tab_PKI_106 definierten Ablaufschritte umsetzen.
[<=]

Tabelle 9: Tab_PKI_106 Ablaufschritte der QES-Zertifikatsprüfung

Ablaufschritte der QES-Zertifikatsprüfung **Anmerkung: Die Sequenz der Ablaufschritte ist funktional hergeleitet, kann jedoch auch anders gestaltet werden, sofern das Ergebnis der Prüfung qualitativ äquivalent ist.**	
Ablaufschritt 1	Prüfung ob „qualifiziert“
Beschreibung	Prüfung, ob das QES-Zertifikat das spezifische QES-Attribut („QCStatement“) als Merkmal enthält
Vorbedingung	keine
Ablaufschritt 2	Prüfung des QES-CA-Zertifikates gegen die BNetzA-VL
Beschreibung	Das QES-CA-Zertifikat wird gegen die BNetzA-VL zum Referenzzeitpunkt geprüft (Prüfung auf Vorhandensein und gültigen Servicestatus des QES-CA-Zertifikates)
Vorbedingungen	BnetzA-VL
Anmerkungen	Gültiger Servicestatus des QES-CA-Zertifikates gemäß [ETSI TS 119 612#Annex J] zum Referenzzeitpunkt
Ablaufschritt 3	Validierung der Zertifikatssignatur
Beschreibung	Prüfung der mathematischen Korrektheit des QES-Zertifikats (Ableitung vom ermittelten QES-CA-Zertifikat)
Vorbedingungen	QES- und QES-CA-Zertifikat vorhanden
Anmerkungen	Die Prüfung erfolgt über Verifikation der Signatur
Ablaufschritt 4	Prüfung des Sperrstatus

Beschreibung	Prüfung, ob Zertifikat gesperrt ist durch Abfrage des OCSP-Responders, ggf. durch Auswertung von in Signatur eingebetteter OCSP-Response. Dabei sind die Sonderfälle für die Ermittlung der OCSP-Responder-Adresse (aus End-Entity-Zertifikat bzw. TSL, s. Kap. 4.4.2) und die Prüfung des OCSP-Signer-Zertifikats (s. Kap. 4.5) zu beachten.
Vorbedingung	QES-Zertifikat vorhanden
Anmerkungen	OCSP-Dienste für QES-Zertifikate müssen den Vorgaben von [eIDAS] genügen. Die Ableitung des OCSP-Signer-Zertifikates erfolgt normalerweise gemäß [RFC6960] (zu Abweichungen davon vgl. Kap. 4.5)

6.7 Festlegungen zur Durchführung

6.7.1 Durchführung von Zertifikatsprüfungen

Kryptographische Identitäten werden zur Erreichung folgender Schutzziele eingesetzt:

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

TIP1-A_2179 - Anwendungskontext für Zertifikatsprüfungen
Die TI-Plattform MUSS die Zertifikatsprüfung durchführen im Kontext der
(a) Authentisierung von Akteuren und Komponenten,
(b) Verschlüsselung von Daten und der
(c) Signaturprüfung inkl. QES-Signaturprüfung.
[<=]

6.7.2 Spezialfälle der Zertifikatsprüfung

Offline-Prüfung

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

Prinzipiell wird die Offline-Prüfung erfolgen:

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

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

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

TIP1-A_2180 - Warnmeldung bei Offline-Fall der Zertifikatsprüfung
Die TI-Plattform MUSS die Zertifikatsprüfung so gestalten, dass auf besondere Anforderung der aufrufenden Funktion ein Sperrstatus als gültig bewertet wird, auch wenn eine Online-Prüfung nicht erfolgreich abgeschlossen werden konnte. Es MUSS dabei eine Warnmeldung zurückgegeben werden mit einem Hinweis, dass nur offline geprüft wurde. Dabei MUSS sichergestellt werden, dass eine technisch mögliche Online-Prüfung nicht verhindert wird.
[<=]

Caching-Modus

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

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

TIP1-A_2181 - Default-Lebensdauer einer Statusantwort
Die TI-Plattform MUSS die Zertifikatsprüfung so gestalten, dass eine Default-Lebensdauer einer Statusantwort über die gesamte TI festgelegt und dynamisch nach Vorgaben der TI-Plattform verändert werden kann.
[<=]

TIP1-A_2182 - Lebensdauer einer Statusantwort
Die TI-Plattform MUSS bei der Zertifikatsprüfung die akzeptierte Lebensdauer einer Statusantwort wählbar gestalten.
[<=]

Nutzung eingebetteter OCSP-Responses

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

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

6.7.3 Bedingungen für eine erfolgreiche Zertifikatsprüfung

TIP1-A_2184 - Bedingungen für Zertifikatsprüfung
Die TI-Plattform DARF als Prüfergebnis einer Zertifikatsprüfung NICHT das Zertifikat als gültig bewerten, wenn nicht alle definierten Ablaufschritte der Zertifikatsprüfung erfolgreich durchlaufen sind. Als Ausnahmen bei Ablaufschritt 4 „Prüfung des Sperrstatus“ sind erlaubt: Prüfung mit tolerierter Nichterreichbarkeit des OCSP-Responders.
[<=]

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

Der Prüfvorgang kann folgende Status haben:

- Prüfvorgang komplett durchgeführt
- Prüfvorgang durchgeführt mit Einschränkungen (einzelne Prüfschritte konnten nicht durchgeführt werden)
- Prüfvorgang fehlgeschlagen (kritische Prüfschritte konnten nicht durchgeführt werden)

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

- Zertifikat ist gültig
- Zertifikat ist gültig mit Einschränkung (Online-Prüfung des Gültigkeitsstatus konnte nicht durchgeführt werden, TSL ist abgelaufen); die Einschränkung wird in Form einer Warnung mit ausgegeben
- Zertifikat ist gesperrt seit <Sperrdatum>

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

TIP1-A_2185 - Prüfung und Interpretation der TSL-Graceperiod
Die Produkttypen der TI-Plattform, die Zertifikate prüfen, MÜSSEN im Falle einer abgelaufenen TSL auch auf die zeitliche Überschreitung der TSL-Graceperiod prüfen:
(a) TSL-Graceperiod nicht überschritten: es müssen die Einträge in der TSL als „gültig“ gewertet werden und die prüfende Einheit muss einen Warnhinweis an die aufrufende Funktion/Anwendung zurückmelden.
(b) TSL-Graceperiod überschritten: die prüfende Einheit muss eine Fehlermeldung an die aufrufende Funktion/Anwendung zurückgeben, da keine valide Prüfbasis vorliegt. Eine Aussage über die Gültigkeit des angefragten Aussteller-CA-Zertifikates wird in diesem Falle nicht gegeben.
[<=]

7 Betriebliche Aspekte der PKI

7.1 Einführung

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

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

Die hier dargestellte Sicht konzentriert sich auf zwei Aspekte:

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

7.1.1 Rollen

Im Zertifikatslebenszyklus sind folgende Rollen relevant:

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

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

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

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

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

7.1.2 Authentisierung der Rolleninhaber

Bei der Bearbeitung eines Antrags zur Erstellung oder Sperrung eines Zertifikats muss durch den TSP sichergestellt werden, dass die jeweilige Person in ihrer Rolle sicher und

eindeutig identifiziert und authentifiziert, und ihre Berechtigung anhand der von der berechtigungsprüfenden Stelle mitgeteilten Daten überprüft wird.

TIP1-A_2186 - Sichere Authentifizierung von PKI-Prozess-Rolleninhabern
Die TI-Plattform MUSS sicherstellen, dass die Rolleninhaber der PKI-Prozesse sicher authentifiziert werden.
[<=]

7.2 Zulassung von TSP in den Vertrauensraum der TI

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

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

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

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

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

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

Zu berücksichtigende Eckpunkte sind:

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

Hieraus werden folgende Rollen abgeleitet:

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

Rolle	Aufgabe/Funktion
Anbieter TSL-Dienst	erzeugt die TSL zyklisch und ad-hoc auf besondere Anforderung der gematik

TSP-X.509	beantragt die Aufnahme in die TSL
gematik	Gesamtverantwortung für den TI-Betrieb und Zulassung der TSP

7.2.2 Zulassung von CVC-CAs der zweiten Ebene

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

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

Zu berücksichtigende Eckpunkte sind:

- Die gematik trägt die Gesamtverantwortung für die Sicherheit von CV-Zertifikaten und definiert somit die Sicherheitsvorgaben für die Anbieter der CVC-Sub-CA und auch der CVC-Root-CA. Daraus leitet sich auch die Verantwortung für die Prüfung der Sicherheitseignung der Anbieter ab, die in einem entsprechenden Verfahren durchgeführt und bestätigt werden muss.
- Nur die CVC-Root-CA als Besitzer des übergeordneten Root-Schlüsselpaares kann die Ausstellung der CV-CA-Zertifikate vornehmen.
- Die CV-Zertifikate enthalten Rollenattribute, über die Zugriffsprofile umgesetzt werden. Die Bestätigung, dass in ein CV-Zertifikat ein bestimmtes Zugriffsprofil eingebracht werden darf, muss durch eine zuständige Qualifizierende Stelle gemäß [gemSpec_PKI#Tab_PKI_254] erfolgen, bspw. Ärztekammer für das Arztattribut, vgl. dazu auch Kap 2.7.9.2.

Hieraus werden folgende Rollen abgeleitet:

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

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

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

7.3.1 Registrierungsdienst

Der Registrierungsdienst nimmt die Zertifikatsanträge eines Antragsberechtigten entgegen und leitet diese nach erfolgreicher Authentifizierung und Autorisierung an den

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

Zu berücksichtigende Eckpunkte sind:

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

Basierend auf diesen Eckpunkten ergeben sich folgende Rollen:

Tabelle 12: Übersicht der Rollen und deren Aufgaben beim Registrierungsdienst

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

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

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

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

Spezifische Ausprägungen des Registrierungsdienstes im Kontext Leistungserbringer- und Organisationszertifikate:

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

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

- Antragsberechtigter ist nicht der Versicherte selbst, sondern der für ihn zuständige Kostenträger.
- Berechtigungsprüfende Stelle ist der Kostenträger selbst.
- Schlüsselerzeugung erfolgt beim jeweiligen TSP-X.509 oder alternativ beim Antragsteller, die Zertifikatsbeantragung erfolgt über eine technische Schnittstelle. Für die AUT_ALT-Identität erfolgt die Schlüsselerzeugung beim Signaturdienst (s. gemKPT_Arch_TIP#5.4.17).
- Zertifikatsausgabe erfolgt nach Einbringung der Zertifikate in die eGK, der Versicherte erhält die eGK inkl. der Zertifikate.
  Für die alternativen Versichertenidentitäten erfolgt die Zertifikatsausgabe an den Signaturdienst (AUT_ALT-Identität)

TIP1-A_2193 - Implementierung der Schnittstellen des Registrierungsdienstes
Der TSP-X.509 MUSS in der Umsetzung des Registrierungsdienstes der PKI die geforderten technischen und organisatorischen Schnittstellen implementieren.
[<=]

7.3.2 Erstellungsdienst

Der Erstellungsdienst dient der Erstellung der Endnutzerzertifikate.

Zu berücksichtigende Eckpunkte sind:

- Der TSP-X.509 ist bei der Erstellung der jeweiligen Zertifikate zur Umsetzung der von der TI-Plattform definierten Zertifikatsprofile verpflichtet.
- Um die Nachprüfbarkeit der erzeugten Zertifikate zu ermöglichen, müssen diese einem Statusprüfdienst zur Prüfbarkeit per OCSP zugeführt werden.

Basierend auf diesen Eckpunkten ergeben sich folgende Rollen:

Tabelle 13: Übersicht der Rollen und deren Aufgaben beim Erstellungsdienst

Rolle	Aufgabe/Funktion
TSP-X.509	nimmt Zertifikatsrequests entgegen, erzeugt die Zertifikate und liefert Zertifikate nach Erstellung an den Registrierungsdienst zurück

TIP1-A_2194 - Implementierung der Schnittstellen des Erstellungsdienstes
Der TSP-X.509 MUSS in der Umsetzung des Erstellungsdienstes der PKI die geforderten technischen und organisatorischen Schnittstellen implementieren.
[<=]

7.3.3 Statusprüfdienst

Der Statusprüfdienst stellt Zertifikatstatusinformationen für eine automatisierte Gültigkeitsüberprüfung zur Verfügung.

Zu berücksichtigende Eckpunkte sind:

- Im Rahmen der Nutzung von Zertifikaten besteht die Notwendigkeit zur Zertifikatsprüfung inkl. Prüfung des Sperrstatus.
- Der TSP-X.509, der ein Zertifikat erzeugt hat, muss eine Statusauskunft dazu bereitstellen.
- Der TSP-X.509, der ein Zertifikat erzeugt hat, dessen Status zusätzlich auch im Internet prüfbar sein muss, muss die zugehörigen Statusinformationen zeitgleich in der TI und im Internet zur Verfügung stellen.

Basierend auf diesen Eckpunkten ergeben sich folgende Rollen:

Tabelle 14: Übersicht der Rollen und deren Aufgaben beim Statusprüfdienst

Rolle	Aufgabe/Funktion
TSP-X.509	nimmt Statusanfragen entgegen und liefert die Statusinformation zu dem angefragten Zertifikat
Zertifikatsnutzer	stellt über ein technisches System eine Statusanfrage (OCSP-Request) an den für das angefragte Zertifikat relevanten OCSP-Responder

TIP1-A_2195 - Implementierung der Schnittstellen des Statusprüfdienstes
Der TSP-X.509 MUSS in der Umsetzung des Statusprüfdienstes der PKI die geforderten technischen und organisatorischen Schnittstellen implementieren.
[<=]

7.3.4 Sperrdienst

Der Sperrdienst nimmt Sperraufträge von berechtigten Personen entgegen und leitet die Änderung des Zertifikatstatus an den Statusprüfdienst weiter. Daraufhin ergibt die Abfrage der Zertifikatsgültigkeit ein negatives Ergebnis.

Zu berücksichtigende Eckpunkte sind:

- Im Rahmen der Nutzung von Zertifikaten besteht die Notwendigkeit zu deren Sperrung, bspw. Nach Verlust der zugehörigen Karte oder des Gerätes.
- Der TSP-X.509, der ein Zertifikat erzeugt hat, muss eine Sperrmöglichkeit bereitstellen.
- Der TSP-X.509 muss das zu sperrende Zertifikat eindeutig identifizieren.
- Der Nachweis der Sperrberechtigung muss erbracht werden, dazu muss der TSP-X.509 den Anfragenden sicher authentifizieren.
- Der Sperrberechtigte muss nach erfolgreicher Sperrung eine Rückinformation erhalten.

Basierend auf diesen Eckpunkten ergeben sich folgende Rollen:

Tabelle 15: Übersicht der Rollen und deren Aufgaben beim Sperrdienst

Rolle	Aufgabe/Funktion

TSP-X.509	nimmt Sperranfragen entgegen, prüft diese auf Authentizität und Autorisierung und sperrt ggf. das angefragte Zertifikat
Sperrberechtigter	stellt über eine technische order organisatorische Schnittstelle einen Sperrauftrag an den TSP-X.509

TIP1-A_2196 - Implementierung der Schnittstellen des Sperrdienstes
Der TSP-X.509 MUSS in der Umsetzung des Sperrdienstes der PKI die geforderten technischen und organisatorischen Schnittstellen implementieren.
[<=]

7.4 Verzeichnisdienst der TI

Der Verzeichnisdienst im Sinne dieses Kapitels ist das TI-eigene Verzeichnis („das Telefonbuch“) für Einträge von Leistungserbringern und Institutionen.

NICHT Gegenstand dieses Kapitels sind die Verzeichnisdienste zur Zertifikatsstatusprüfung (mittels OCSP) sowie die ggf. im Internet bereitgestellten Verzeichnisdienste (X.500/LDAP/OCSP) der TSPs. Hierzu siehe Kap. 4.4.

7.4.1 Geltungsbereich

Verzeichniseinträge müssen einer bereits bestehenden elektronischen Identität zuordenbar sein. Dabei handelt es sich um:

- Natürliche Personen, denen aufgrund ihrer bestätigten Berufszugehörigkeit als Leistungserbringer des deutschen Gesundheitswesens ein HBA/BA (oder HBA-Vorläuferkarte) ausgestellt wurde.
- Juristische Personen (Organisationen/Institutionen) des deutschen Gesundheitswesens denen eine SMC-B ausgestellt wurde.

Die Teilnahme am Verzeichnisdienst ist freiwillig.

TIP1-A_5455 - Teilnehmer des Verzeichnisdienstes
Die TI-Plattform MUSS einen Verzeichnisdienst für Einträge von Leistungserbringern und medizinischen Institutionen realisieren.
[<=]

TIP1-A_5456 - Freiwillige Teilnahme am Verzeichnisdienst
Die gematik MUSS sicherstellen, dass die Teilnahme am Verzeichnisdienst auf freiwilliger Basis erfolgt.
[<=]

7.4.2 Datenmodell

TIP1-A_5457 - Datenmodell Verzeichnisdienst
Die TI-Plattform MUSS für den Verzeichnisdienst ein Datenmodell mit folgenden logischen Elementen eines Eintrags definieren:
1) Basisdaten (zertifikatsbasiert)

2) Fachanwendungsdaten (optional)
[<=]

7.4.2.1 Basisdaten (zertifikatsbasiert)

Die bei der Registrierung des Teilnehmers aus dem Zertifikat übernommenen Basisdaten enthalten u.a. die Telematik-ID als eindeutigen Identifikator des Teilnehmers im Verzeichnisdienst. Dieser wird aus Datenschutzgründen nicht als öffentliches Attribut genutzt.

Ein weiterer wesentlicher Bestandteil eines Basisdatensatzes ist das (oder sind die) Verschlüsselungszertifikat(e) eines Teilnehmers. Für eine sichere Ende-zu-Ende-Kommunikation zwischen den Teilnehmern ist es unabdingbar, dass der Sender einer Nachricht Zugriff auf das Verschlüsselungszertifikat des Empfängers hat. Der Verzeichnisdienst dient dazu, diesen Zugriff zu gewährleisten.

(Hinweis: Ein Teilnehmer kann im Besitz mehrerer gültiger Verschlüsselungszertifikate sein. Z.B. entsteht bei der Neuausstellung einer Karte eine Überlappung zwischen der Gültigkeitsdauer der Zertifikate der alten und der neuen Karte. Der Verzeichnisdienst gibt dem Akteur die Möglichkeit, alle gültigen Verschlüsselungszertifikate zu veröffentlichen.)

Die Basisdaten sind zwingender Bestandteil eines Eintrages. Werden die unveränderlichen Basisdaten gelöscht, zieht dies auch die Löschung der zugehörigen Fachanwendungsdaten nach sich. (Vgl. folgende Kapitel.)

7.4.2.2 Fachanwendungsdaten (optional)

Der Verzeichnisdienst dient auch den Fachdiensten als Medium, um identitätsspezifische, also auf einen eingetragenen Teilnehmer bezogene Daten der Fachanwendung direkt im Verzeichnisdienst ablegen und bedarfsweise publizieren zu können.

Anlage und Pflege dieser fachanwendungsspezifischen Ergänzungsdaten erfolgen über den Fachdienst. Dafür werden Schreib- und Löschrecht für diese Ergänzungen im Verzeichniseintrag vom Teilnehmer an den Fachdienst, bzw. an einen Fachdienst-anbieter erteilt. Dieser Anbieter trägt somit die Verantwortung für die Richtigkeit der von ihm gepflegten Daten. Die Rechte sind eingeschränkt auf diejenigen Daten, die über den Fachdienst selbst verwaltet werden.

7.4.3 Lifecyclemanagement für Verzeichniseinträge

TIP1-A_5458 - Kartenbasierte Registrierung
Der Verzeichnisdienst MUSS eine Teilnehmer- und eine Zertifikats-Eintragung, Aktualisierung und Austragung ermöglichen, welche neben den Karten eines HBA oder einer SMC-B keine weiteren Identifikations- und Registrierungsprozesse fordert.
[<=]

Die gegenseitige Authentisierung zwischen Fachdienst und Verzeichnisdienst erfolgt zertifikatsbasiert über TLS. Die Zertifikate werden dabei von der zentralen Dienste- und Komponenten-CA ausgestellt.

7.4.4 Aufbau und Außensicht

Die in Kapitel 7.4.2 angesprochene Partitionierung der Daten zieht auch unterschiedliche Zuständigkeiten bzw. Hoheiten über diese Daten nach sich. Diese müssen auch auf Ebene Autorisierung berücksichtigt werden.

Die Datenbestände aus verschiedenen Quellen müssen aber unter einer für den Benutzer einheitlichen logischen Sicht genutzt und verwaltet werden können.

7.4.4.1 Autorisierung

Die technischen Zuständigkeiten für Datenbestände, die einer bestimmten Identität zugeordnet sind, können bei verschiedenen Akteuren und Anbietern liegen:

Die Basisdaten des Teilnehmers werden aus dessen Zertifikaten übernommen und können durch den Teilnehmer selbst nicht modifiziert werden. Er kann nur über die Publizierung des Datensatzes als Ganzes oder in Teilen (Name, Vorname optional) entscheiden. Fachanwendungsspezifische Ergänzungsdaten werden durch den jeweiligen FA-Anbieter verwaltet.

TIP1-A_5459 - Autorisierung
Der Verzeichnisdienst MUSS seine Administrationsschnittstellen so zur Verfügung stellen, dass zu einem Verzeichniseintrag Datenstrukturen verschiedener Art und von verschiedenen Verantwortlichen gepflegt werden können:
1) Zertifikatsdaten dürfen nur durch die Übernahme aus Zertifikaten erstellt werden.
2) Fachanwendungsdaten dürfen nur vom jeweiligen FA-Anbieter gepflegt werden.
[<=]

7.4.4.2 Sichtbarkeit in der TI

Der Verzeichnisdienst ist ein zentraler Dienst in der TI. Er erlaubt die Abfrage der Daten eines eingetragenen Teilnehmers unter einer einheitlichen Schnittstelle. Die architektonische Partitionierung, welche sich aus den verschiedenen Datentypen und Zuständigkeiten ergibt, bleibt einem abfragenden Client gegenüber verborgen.

TIP1-A_5460 - Eine logische Sicht auf das Verzeichnis
Der Verzeichnisdienst MUSS für Fachdienste und dezentrale Systeme eine logische Sicht auf das Verzeichnis für Identitäten von Leistungserbringern und Institutionen bereitstellen.
[<=]

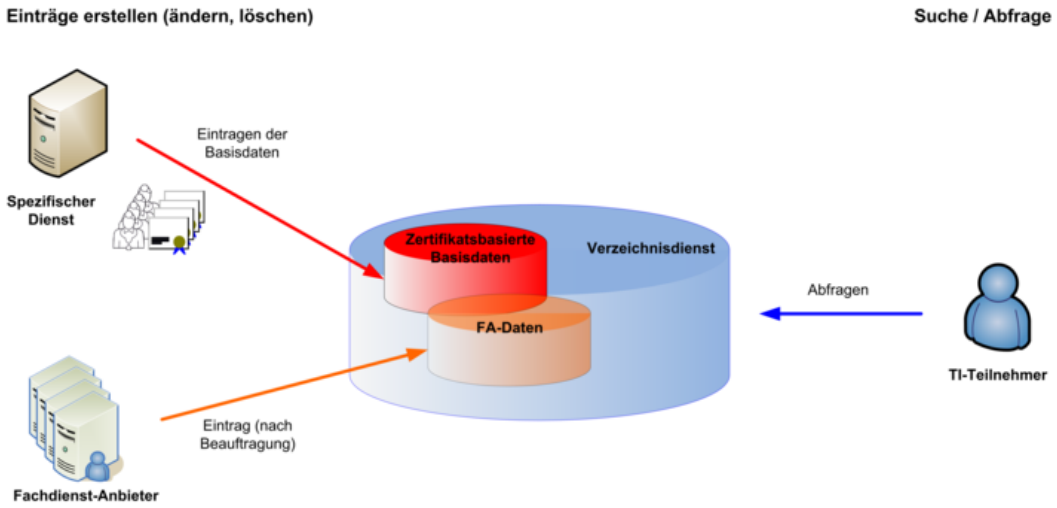

Abbildung 8: Außenschnittstellen des Verzeichnisdienstes

8 Anhang A – Verzeichnisse

8.1 Abkürzungen

Kürzel	Erläuterung
AES	Advanced Encryption Standard
AK	Anwendungskonnektor
AN	alphanumerisch
AUT	Authentisierung (Authentication)
AUT_ALT	Authentisierung mit alternativer Identität
AUTN	Technisches Authentisierungszertifikat für Nachrichten
AVS	Apothekenverwaltungssystem (Primärsystem der Apotheker)
BAEK	Bundesärztekammer
BAK	Bundesapothekerkammer
BMG	Bundesministerium für Gesundheit
BnetzA	Bundesnetzagentur
BPTK	Bundespsychotherapeutenkammer
BSI	Bundesamt für Sicherheit in der Informationstechnik
BZÄK	Bundeszahnärztekammer
C2C	card to card
CA	certification authority
CAMS	Card Application Management System
CAR	Certificate Authority Reference
CC	Common Criteria

Kürzel	Erläuterung
CH	Card Holder
CHA	Certificate Holder Authorisation
CHR	Certificate Holder Reference
CMS	Karten Management System, Card Management System
CP	Certificate Policy
CPI	Certificate Profile Identifier
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CV	Card Verifiable
CVC	Card Verifiable Certificate
CVC-CA	CA für CV-Zertifikate
CV-Zertifikate	Card Verifiable-Zertifikate
DES	Data Encryption Standard
DIMDI	Deutsches Institut für Medizinische Dokumentation und Information
DN	Distinguished Name
DNS	Domain Name Service
ECC	Elliptic Curve Cryptography (Kryptographie auf Basis elliptischer Kurven
EE	End Entity
eGBR	Elektronisches Gesundheitsberuferegister
eGK	Elektronische Gesundheitskarte
ENC	Verschlüsselung (Encryption)
ENCV	Technisches Verschlüsselungszertifikat für Verordnungen
ETSI	Europäisches Institut für Telekommunikationsnormen

Kürzel	Erläuterung
EU-LOTL	List of Trusted Lists der Europäischen Kommission
FIPS-140 2	Federal Information Processing Standard 140 2
FQDN	Fully Qualified Domain Name
GKV	Gesetzliche Krankenversicherung
gSMC	Gerätebezogene Security Module Card
HBA	Heilberufsausweis
HCI	Health Care Institution
HP	Health Professional
HPC	Health Professional Card
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ICCSN	ICC Serial Number
ID	Identität (Identity)
IK	Individual Key
IPSec	Internet Protocol Security
ISM	Information Security Management
ISO	International Standard Organization
KOM-LE	Kommunikation für Leistungserbringer
KSR	Konfigurationsdienst
KT	Kartenterminal
KTR	Kostenträger
KV	Kassenärztliche Vereinigung
KVNR	Krankenversichertennummer

Kürzel	Erläuterung
KZBV	Kassenzahnärztliche Bundesvereinigung
LAK	Landesapothekerkammer
LÄK	Landesärztekammer
LDAP	Lightweight Directory Access Protocol
LEI	Leistungserbringerinstitution
LEO	Leistungserbringer-Organisation
LZÄK	Landeszahnärztekammer
MAC	Message Authentication Code
MON	Monitoring
NK	Netzkonnektor
OCSP	Online Certificate Status Protocol
OCSP-R	OCSP-Responder
OID	Object Identifier
ORG	Gesellschafterorganisation
OSIG	Organizational Signature
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	PKI nach X.509 Standard der IETF
PrK	Private Key
PuK	Public Key
QES	Qualifizierte elektronische Signatur
RA	Registration Authority
RCA	Root-CA

Kürzel	Erläuterung
RFC	Request For Comment
RSA	Rivest Shamir Adleman (Verfahren)
SAK	Signaturanwendungskomponente
SGB	Sozialgesetzbuch
SHA	Secure Hash Algorithm
SIG	Elektronische Signatur
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen
SigV	Signaturverordnung
SIS	Secure Internet Service
SLA	Service Level Agreement
SM	Security Module
SMC-B	Sicherheitsmodul vom Typ B
SMC	Security Module Card
gSMC-K	Security Module Card Konnektor als <holder>
gSMC-KT	Security Module Kartenterminal als <holder>
SubjectDN	Subject Distinguished Name
TCL	Trusted Component List
TI	Telematikinfrastruktur
TLS	Transport Layer Security
TSL	Trust-service Status List
TSP	Trust Service Provider
VDA	Vertrauensdiensteanbieter
VPN	Virtual Private Network

Kürzel	Erläuterung
XML	Extensible Markup Language
ZOD	Zahnärzte Online Deutschland

8.2 Glossar

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

8.3 Abbildungsverzeichnis

Abbildung 1: TSL-Modell 13
Abbildung 2: Zertifikatshierarchien und deren Abbildung in der TSL 14
Abbildung 3: Aufbau der TSL 14
Abbildung 4: Gültigkeitszeiträume TSL 16
Abbildung 5: Hierarchie der CVC-PKI (je Kartengeneration) 24
Abbildung 6: Zuordnung der Verantwortlichkeiten für die Zertifikate 28
Abbildung 7: OCSP-Responder Proxy 62
Abbildung 8: Außenschnittstellen des Verzeichnisdienstes 90

8.4 Tabellenverzeichnis

Tabelle 1: Tab_PKI_107 Übersicht der PKI-spezifischen Sperrgründe 31
Tabelle 2: Verantwortlichkeiten in Bezug auf ein Zertifikat 42
Tabelle 3: Übersicht Identitätselemente und Verantwortungsdomänen 46
Tabelle 4: Tab_PKI_108 Informationen für ein CV-Zertifikat G2 65
Tabelle 5: Übersicht Felder eines CV-Zertifikats 65
Tabelle 6: Tab_PKI_104 Ablaufschritte der Vertrauensraumprüfung 70
Tabelle 7: Tab_PKI_105 Ablaufschritte der Zertifikatsprüfung 72
Tabelle 8: TAB_PKI_113 Zuordnung der (zugelassenen) X.509-Sub-CAs zu Zertifikatstypen 74
Tabelle 9: Tab_PKI_106 Ablaufschritte der QES-Zertifikatsprüfung 77
Tabelle 10: Übersicht der Rollen und deren Aufgaben bei der TSP-Zulassung 82
Tabelle 11: Übersicht der Rollen und deren Aufgaben bei der Zulassung von CVC-CAs 83

Tabelle 12: Übersicht der Rollen und deren Aufgaben beim Registrierungsdienst 84
Tabelle 13: Übersicht der Rollen und deren Aufgaben beim Erstellungsdienst.....85
Tabelle 14: Übersicht der Rollen und deren Aufgaben beim Statusprüfdienst.....86
Tabelle 15: Übersicht der Rollen und deren Aufgaben beim Sperrdienst 86

8.5 Referenzierte Dokumente

8.5.1 Dokumente der gematik

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

[Quelle]	**Herausgeber: Titel**
[gemSpec_PK_eGK]	Spezifikation für Prüfkarten eGK der Generation 2.1
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_Arch_TIP]	gematik: Architektur der TI-Plattform
[gemRL_Betr_TI]	gematik: Übergreifende Richtlinien zum Betrieb der TI
[gemRL_TSL_SP_CP]	gematik: Certificate Policy – Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation, Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_DS_Anbieter]	gematik: Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter

8.5.2 Weitere Dokumente

[Quelle]	**Herausgeber (Erscheinungsdatum): Titel**

[Ärzte-ZV]	Zulassungsverordnung für Vertragsärzte (Ärzte-ZV) Zulassungsverordnung für Vertragsärzte auf der Grundlage des Artikel 9 des Gesetzes zur Verbesserung der Versorgungsstrukturen in der gesetzlichen Krankenversicherung (GKV-Versorgungsstrukturgesetz – GKV-VStG) vom 28.12.2011 (BGBl. I S. 3016)
[Common-PKI]	T7 & TeleTrust (20.01.2009): Common PKI Spezifikation, Version 2.0; Aktuelle Quelle http://www.t7ev.org/themen/entwickler/common-pki -v20-spezifikation.html
[CP-HPC]	Bundesärztekammer et al (08.06.2009): Gemeinsame Policy für die Ausgabe der HPC – Zertifikatsrichtlinie HPC (Version 1.0.0) http://www.bundesaerztekammer.de/downloads/CP_HPC_v1.0.0_19062009.pdf
[baekValidity Model]	Bundesärztekammer (29.05.2009) Gültigkeitsmodell der elektronischen Arztausweise und Laufzeit der Zertifikate (Version 2.3.1)
[eIDAS]	Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
[ETSI_TS_102_231_V3.1.2]	ETSI (Dezember 2009): ETSI Technical Specification TS 102 231 (‘Provision of harmonized Trust Service Provider (TSP) status information’) Version 3.1.2
[ETSI_TS_119_612]	ETSI (July 2015): ETSI TS 119 612 V2.1.1 ‘Electronic Signatures and Infrastructures (ESI); Trusted Lists’
[EU_LOTL]	https://ec.europa.eu/information_society/policy/esignature/trusted-list/
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://www.ietf.org/rfc/rfc2119.txt
[RFC2560]	RFC 2560 (Juni 1999): X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP http://www.ietf.org/rfc/rfc2560.txt
[RFC5280]	RFC 5280 (Mai 2008): Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile http://www.ietf.org/rfc/rfc3280.txt
[RFC6960]	RFC 6960 (Juni 2013): X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP https://tools.ietf.org/html/rfc6960

[SGB V]	BGBl. I S.2477 (20.12.1988): Sozialgesetzbuch, Fünftes Buch Zuletzt geändert durch Art. 4 G v. 14.4.2010 I 410 Gesetzliche Krankenversicherung
[BSI-TR-03110 Part3]	BSI (2012): Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3 – Common Specifications, Version 2.10 https://www.bsi.bund.de/ContentBSI/EN/Publications/Techguidelines/TR03110/BSITR03110.html
[VDG]	"Vertrauensdienstegesetz vom 18. Juli 2017 (BGBl. I S. 2745), das durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist" Stand: Geändert durch Art. 2 G v. 18.7.2017 I 2745 https://www.gesetze-im-internet.de/vdg/BJNR274510017.html