gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Übergreifende Spezifikation

Spezifikation PKI

Version:	1.7.0
Revision:	\main\rel_online\rel_ors1\71
Stand:	23.07.2015
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemSpec_PKI]

Dokumentinformationen

Änderungen zur Vorversion

Es wurden KOM-LE-bedingte Änderungen (inklusive Clientmodul-Zertifikat) eingearbeitet, diese sind grün markiert. Die durch Errata bedingten Änderungen sind in gelb markiert.

Dokumentenhistorie

Version	Datum	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.5.1	16.07.12	5.7	Einarbeitung CR 0029	P77
0.6.0	17.07.12		zur Abstimmung freigegeben	PL P77
	31.08.12	Alle	Einarbeitung Kommentierung Gesellschafter	P77
0.7.0	06.09.12		zur Abstimmung freigegeben	PL P77
			Korrekturen	P77
1.0.0	15.10.12		freigegeben	gematik
			Einarbeitung Kommentare aus der übergreifenden Konsistenzprüfung	P77
1.1.0	12.11.12		freigegeben	gematik
	15.02.13		Überarbeitung anhand interner Änderungsliste (Fehlerkorrekturen, Inkonsistenzen)	P77
1.1.9	22.04.13		zur Abstimmung freigegeben	PL P77
			Einarbeitung Kommentare aus Kommentierung Gesamtpaket	P77
1.2.0 RC	30.05.13		zur Freigabe empfohlen	PL P77
1.2.0	06.06.13		freigegeben	gematik
1.2.9	08.08.13		Einarbeitung gemäß Änderungsliste	P77
1.3.0	15.08.13		freigegeben	gematik
			Einarbeitung KOM-LE-bedingte Änderungen	P77
1.3.1_ KOM-LE	05.02.14		zur Angebotserstellung freigegeben	gematik
	27.02.14		Clientmodul-Zertifikat angepasst	P77
1.3.2_ KOM-LE	28.02.14		zur Angebotserstellung freigegeben	gematik
			Definition für kryptischen Bezeichner ergänzt (Kap. 2.6/2.7), „<tsp>“ für „GEM“ (Kap. 5.10.3/4), CVC-Rollenprofil „Krankenhaus“ ergänzt	P77

Version	Datum	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
			(Tab_PKI_918), Aufteilung Tab_PKI_257 für G1 und G2, Optimierung Tab_PKI_906 gemäß P11-Änderungsliste.	
1.5.0	17.06.14		freigegeben	gematik
			Einarbeitung gemäß P12-Änderungsliste	P77
1.6.0	26.08.14		freigegeben	gematik
			Merge mit ORS1-Version 1.6.0 und KOM-LE-bedingte Änderungen	P77
1.6.1_KOM-LE	22.09.14		zur Angebotserstellung freigegeben	gematik
			Errata 1.4.3 und 1.4.6 engearbeitet	
1.7.0	17.07.15		freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes

1.1 Zielsetzung

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

1.2 Zielgruppe

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

1.3 Geltungsbereich

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

Schutzrechts-/Patentrechtshinweis

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

1.4 Abgrenzungen

Im vorliegenden Dokument werden Verfahren und Profile für digitale Zertifikate (X.509, CVC für die Generation G1 und G2), beschrieben. Nicht beschrieben werden die Prozesse und Verfahren zur Personalisierung der Karten selbst.

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

1.5 Methodik

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

Sie werden im Dokument wie folgt dargestellt:

⌦ **GS-A_0000 <Titel der Afo>**

Text / Beschreibung⌫

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

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

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

2 Notation kryptographischer Objekte

2.1 Basis-Bezeichner

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

<Objekttyp>.<Objektbesitzer>.<Objektverwendung>

Im weiteren Dokument werden dafür die kürzeren englischen Begriffe verwendet:

<type>.<holder>.<usage>

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

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

2.2 Optionale Bezeichnung der technischen Ausprägung

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

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

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

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

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

2.3 Optionales Unterscheidungsmerkmal bei gleicher technischer Ausprägung

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

Beispiel:
PrK.CH.ENCn.R2048S256, wobei n mit 1 beginnt und fortlaufend nummeriert wird

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

2.4 Allgemeine Notationsvorschrift

Die Benennung kryptographischer Objekte erfolgt gemäß der Notationsvorschrift in Tab_PKI_201.

Tabelle 1: Tab_PKI_201 Allgemeine Notationsvorschrift für kryptographische Objekte

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

2.5 Type (Objekttyp)

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

Tabelle 2: Tab_PKI_202: Notationsvorgaben für Objekttyp

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

Wertebereich von <key>

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

Wertebereich von <certificate>

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

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

Wertebereich von <ID>

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

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

2.6 Holder (Objektbesitzer)

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

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

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

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

Tabelle 3: Tab_PKI_203 Notationsvorgaben für Objektbesitzer

<holder> ::= <holder X.509 | SK> | <holder CVC>
<holder X.509 | SK> ::= <root certification authority> | <health professional> | <card holder> | <Clientmodul>| <health care institution> | <security module Kartenterminal> | <Anwendungskonnektor> | <Netzkonnektor> | <VPN Zugangsdienst> | <gematik Trust-service Status List> | <Trust Service Provider> | <Signatur Anwendungs Komponente> | <Fachanwendungsspezifischer Dienst> | <Zentraler Dienst> | <Generischer Holder>
<holder CVC> ::=

<root certification authority> | <certification authority> | <certification authority eGK> | <certification authority HPC> | <certification authority SMC> | <certification authority SAK> | <health professional card> | <health professional card role> | <health professional card device> | <electronic health card> | <security module card> | <security module card role> | <security module card device> | <certification authority CAMS_HPC> | <certification authority CAMS_SMC> | <CAMS of HPC> | <CAMS of SMC>

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

Wertebereich von <holder X.509 | SK>

<root certification authority>	::=	RCA
<health professional>	::=	HP
<card holder>	::=	CH (Versicherte)
<Clientmodul>	::=	CM
<health care institution>	::=	HCI
<security module Kartenterminal>	::=	SMKT
<Anwendungskonnektor>	::=	AK
<Netzkonnektor>	::=	NK
<VPN Zugangsdienst>	::=	VPNK
<gematik Trust-service Status List>	::=	TSL
<Signatur Anwendungs Komponente>	::=	SAK
<TLS>	::=	TLS
<Fachdienst VSD>	::=	VSD
<Zentraler Dienst>	::=	ZD
<Trust Service Provider>	::=	<Generischer Holder> **|** <tsp>
<Generischer Holder>	::=	GEM (anbieter- u. diensteunabhängig)

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

Wertebereich von <holder CVC>

<root certification authority>	::=	RCA
<certification authority>	::=	CA
<certification authority eGK>	::=	CA_eGK
<certification authority HPC>	::=	CA_HPC
<certification authority SMC>	::=	CA_SMC
<certification authority SAK>	::=	CA_SAK
<certification authority for CAMS of HPC>	::=	CA_CAMS_HPC (opt.)
<certification authority for CAMS of SMC>	::=	CA_CAMS_SMC (opt.)
<CAMS of HPC>	::=	CAMS_HPC (opt.)
<CAMS of SMC>	::=	CAMS_SMC (opt.)
<health professional card>	::=	HPC
<health professional card role>	::=	HPC_Role
<health professional card device>	::=	HPC_Device
<electronic health card>	::=	eGK (elektronische Gesundheitskarte)
<security module card>	::=	SMC
<security module card role>	::=	SMC_role
<security module card device>	::=	SMC_device
<Signatur Anwendungs Komponente>	::=	SAK
<Komfort-Merkmal>	::=	KM (RFID-Token)

2.7 Usage (Objektverwendung)

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

Tabelle 4: Tab_PKI_204 Notationsvorgaben für Objektverwendung

<usage> ::= <usage X.509 | SK> | <usage CVC>
<usage X.509 | SK> ::= <qualified electronic signature> | <electronic signature> | <electronic signature of an organization > | <encipherment> | <authentication X509> | <certsign X509> | <VPN Tunnel> | <VPN-Tunnel secure internet service> | <TLS> | <TLS-Client> | <TLS-Server> |

<TLS-Clientmodul> | <authentication message X509> | <authentication X509 organisation> | <encipherment prescription> | <OCSP> | <CRL> | <calculation message auth. code> | <key generation>| <certification authority component> | <certification authority VPNservice> | <certification authority SMC-B> | <certification authority HBA> |
usage CVC> ::= <authentication CVC> | <authentication role CVC> | <authentication device CVC> | <certsign CVC> | <authentication device CVC RPE> | <authentication device CVC RPS> | <authentication device CVC SUK>

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

Wertebereich von <usage X.509 | SK>

<qualified electronic signature>	::=	QES
<electronic signature>	::=	SIG
<electronic signature of an organization>	::=	OSIG
<encipherment>	::=	ENC
<encipherment prescription>	::=	ENCV
<authentication X509>	::=	AUT
<authentication X509 organisation>	::=	AUTO (opt.)
<authentication message X509>	::=	AUTN
<certsign X509>	::=	CA
<VPN-Tunnel>	::=	VPN
<VPN-Tunnel secure internet service>	::=	VPN-SIS
<TLS>	::=	TLS
<TLS-Client>	::=	TLS-C
<TLS-Server>	::=	TLS-S
<TLS-Clientmodul>	::=	TLS-CS
<OCSP>	::=	OCSP
<calculation message auth. code>	::=	MAC
<key generation>	::=	KG
<CRL>	::=	CRL
<certification authority component>	::=	KOMP

<certification authority VPNservice>	::=	VPNK
<certification authority SMC-B>	::=	SMCB
<certification authority HBA>	::=	HBA

Wertebereich von <usage CVC>

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

2.8 n (lfd. Nummer)

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

Wertebereich von <lfd. Nummer>

~~<n> ::= 1 .. 9~~

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

2.9 Instance (Ausprägung)

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

Tabelle 5: Tab_PKI_205 Notationsvorgaben für Ausprägung

<instance>::= <instance X.509> | <instance CVC> | <instance SYM>

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

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

Wertebereich von <instance X.509>

<X.509 RSA 2048 > ::= R2048

<X.509 RSA 3072 > ::= R3072

<X.509 ECC 256 > ::= E256

<X.509 ECC 384 > ::= E384

Wertebereich von <instance CVC>

<CVC RSA 2048 > ::= R2048

<CVC ECC 256 > ::= E256

<CVC ECC 384 > ::= E384

Wertebereich von <instance SYM>

<2KeyTripleDES> ::= 2DES

<3KeyTripleDES> ::= 3DES

<AES mit 128 Bit> ::= AES128

<AES mit 256 Bit> ::= AES256

2.10 Beispiele zur Umsetzung

2.10.1 Beispiele für asymmetrische Objekte

Tabelle 6: Tab_PKI_206 Beispiele für asymmetrische Objekte

Komponente	Fachliche Beschreibung	Name des Zertifikats	Name des privaten Schlüssels	Name des öffentlichen Schlüssels mit einer konkreten technischen Ausprägung
eGK	X.509-Zertifikat/Schlüssel des Versicherten für die Verschlüsselung	C.CH.ENC	PrK.CH.ENC	PuK.CH.ENC2.R2048S256
	CV-Zertifikat der eGK zur C2C-Authentisierung	C.eGK.AUT_CVC	PrK.eGK.AUT_CVC	PuK.eGK.AUT_CVC.E256S256
HBA	X.509-Zertifikat/Schlüssel des Heilberuflers für eine QES	C.HP.QES	PrK.HP.QES	PuK.HP.QES.R2048S256
	CV-Zertifikat des HBA zur C2C-Geräteauthenti-sierung	C.HPC.AUTD_SUK_CVC	PrK.HPC.AUTD_SUK_CVC	PuK.HPC.AUTD_SUK_CVC.R2048S256
SMC	X.509-Zertifikat/Schlüssel der Institution für eine elektronische Signatur	C.HCI.OSIG	PrK.HCI.OSIG	PuK.HCI.OSIG.E256S512
	CV-Zertifikat der SMC zur C2C-Rollenauthentisierung	C.SMC.AUTR_CVC	PrK.SMC.AUTR_CVC	PuK.SMC.AUTR_CVC.E256S256
VPN-Zugangs-dienst	X.509-Zertifikat/Schlüssel des VPN-Zugangsdienstes	C.VPNK.VPN	PrK.VPNK.VPN	PuK.VPNK.VPN.R2048S256
Fachanw. spez. Dienst allgem.	X.509-Zertifikat/Schlüssel eines Fachanwendungsspez. Dienstes als Server für TLS-Verbindung	C.FD.TLS-S	PrK.FD.TLS-S	PuK.FD.TLS-S.R2048S256
Fach-dienst VSD	X.509-Zertifikat/Schlüssel des VSD-Fachdienstes zum	C.VSD.AUT	PrK.VSD.AUT	PuK.VSD.AUT R2048S384

Komponente	Fachliche Beschreibung	Name des Zertifikats	Name des privaten Schlüssels	Name des öffentlichen Schlüssels mit einer konkreten technischen Ausprägung
	Signieren einer Nachricht			

2.10.2 Beispiele für symmetrische Objekte

Tabelle 7: Tab_PKI_207 Beispiele für symmetrische Objekte

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

3 CA-Strukturen

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

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

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

3.1 Übergreifende Festlegung für CA der TI

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

3.1.1 Übersicht der Identitäten/Zertifikate

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

3.1.2 Laufzeiten der CA

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

3.2 TI-Betriebsumgebungen

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

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

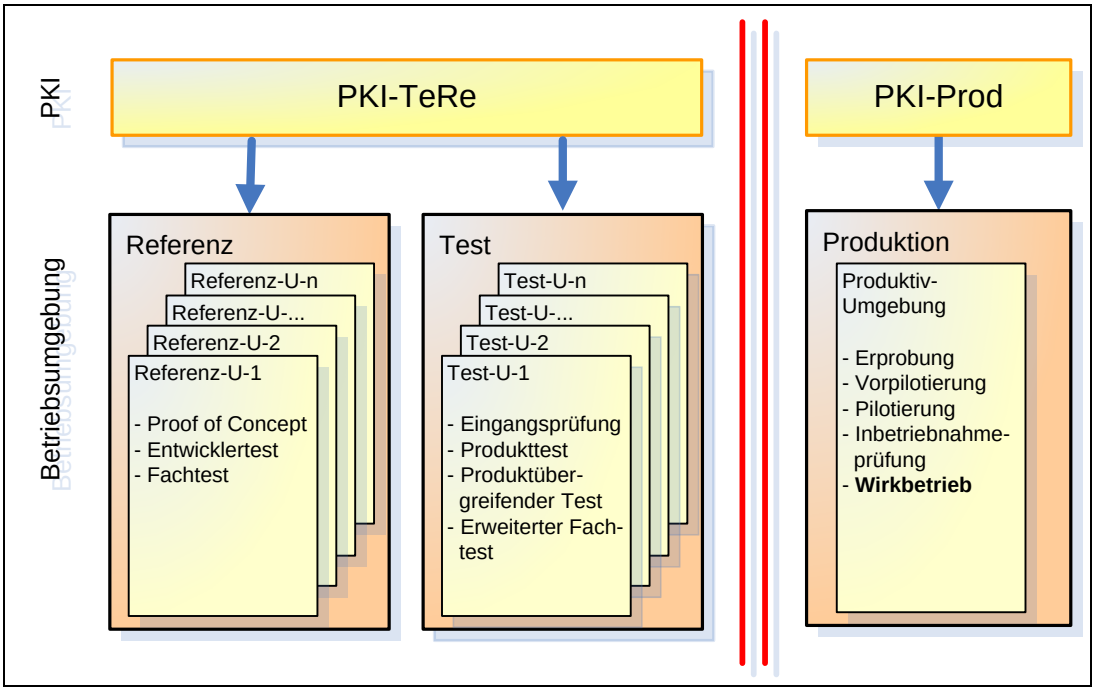

Abbildung 1 Betriebsumgebungen aus Sicht der PKI

3.2.1 PKI-Sicht auf die Produktivumgebung

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

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

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

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

⌦ **GS-A_4695 Zentrale Root-CA für Test- und Referenzumgebung**

Der Anbieter der gematik Root-CA MUSS in der Test- und Referenzumgebung eine zentrale TeRe-Root-CA bereitstellen und hieraus TeRe-CAs der zweiten Ebene zertifizieren.⌫

⌦ **GS-A_4696 OCSP-Responder für gematik TeRe-Root-CA im Internet**

Der Anbieter der gematik Root-CA MUSS einen OCSP-Responder für die CA-Zertifikate der TeRe-Root-CA im Internet bereitstellen.⌫

⌦ **GS-A_4697 PKI für Test- und Referenzumgebung**

Der TSP-X.509 nonQES MUSS für jede von ihm betriebene CA der Produktivumgebung eine korrespondierende CA für die Test- und Referenzumgebung implemen-

tieren und für diese die Namenskonventionen gemäß [GS-A_4588], [GS-A_4589], [GS-A_4590] umsetzen.⌫

Die CA-Struktur entspricht insgesamt derjenigen der Produktivumgebung.

Ausnahme: QES-CA - hier gilt, dass ein TSP die CA-Struktur eines ZDA im angezeigten Betrieb für die Test- und Referenzumgebung nachbilden kann, um die Testung von QES-Funktionalitäten zu ermöglichen.

3.2.3 PKI-Substitut für QES in Test- u. Referenzumgebung

Für die PKI-TeRe müssen – im Unterschied zur PKI-Prod – zusätzliche CAs aufgebaut werden zur Ausgabe von Zertifikaten, die denen der QES-Zertifikate aus der Produktivumgebung soweit syntaktisch und funktional äquivalent sind, dass die zugehörigen Funktionalitäten hinreichend getestet werden können.

Ein Zertifikatsherausgeber für HBA-Zertifikate muss eine separate nonQES-PKI für HBA-Testkarten und HBA-Entwicklerkarten als funktionales QES-Äquivalent für Test- und Referenzumgebung aufbauen.

In der nachfolgenden Darstellung ist dies bezeichnet mit

- TeRe
  CA für Test- und Referenzumgebung, die das Äquivalent der entsprechenden CA in Produktions-BU darstellen.

- Pseudo-Validierung der QES
  Validierung einer Signatur, die mit einem Zertifikat einer TeRe-CA in der Test- und Referenzumgebung erstellt wurde.

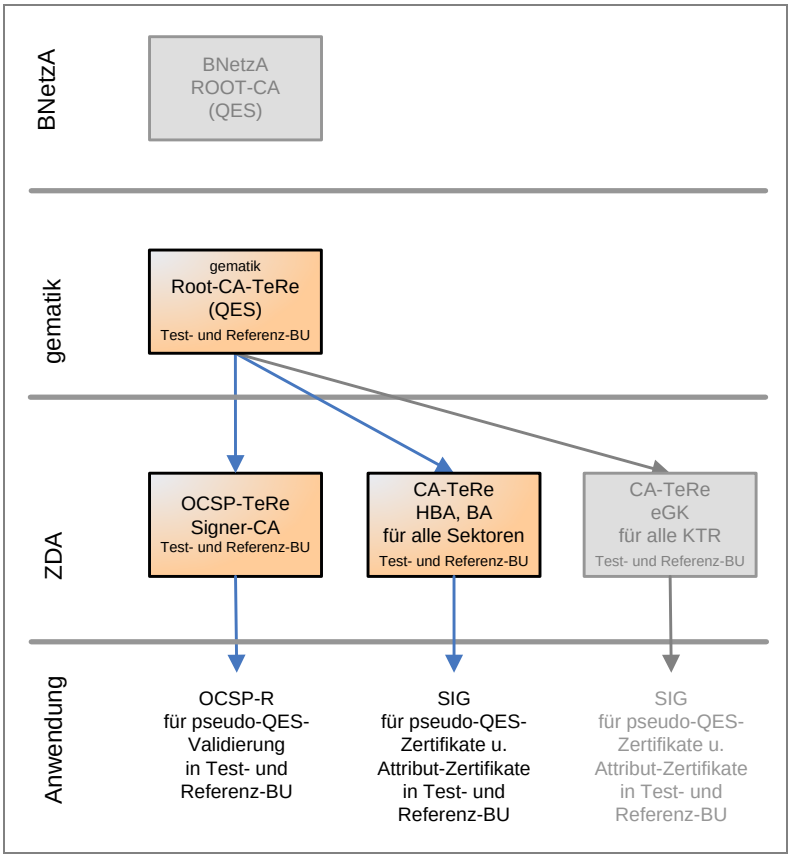

Abbildung 2 QES-Substitut für Referenz- u. Testumgebung

GS-A_4698 QES-Substitut PKI für PKI-TeRe

Der TSP-X.509 QES SOLL für jede von ihm betriebene QES-CA der Produktivumgebung eine funktional äquivalente CA in der PKI-TeRe implementieren und für diese die Namenskonventionen gemäß [GS-A_4588], [GS-A_4589], [GS-A_4590] umsetzen.

GS-A_4699 Ableitung der QES-Substitut-CA

Der TSP-X.509 QES MUSS jede von ihm betriebene CA in der PKI-TeRe von der Test-QES-Root-CA der gematik ableiten.

GS-A_4700 Separation der QES-Substitut-CA

Der TSP-X.509 QES DARF eine von ihm betriebene CA in der PKI-TeRe NICHT von einer CA ableiten, die über eine Root der BNetzA oder die QES-Root eines ZDA im angezeigten Betrieb validiert werden kann.

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

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

GS-A_4702 Zentrale Aussteller-CA für nonQES-Zertifikate

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

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

GS-A_5212 Zentrale Aussteller-CA für VPN-Zugangsdienst-Zertifikate

Der TSP-X.509 nonQES, der eine zentrale Aussteller-CA in der TI für die Ausgabe von nonQES-X.509-Zertifikaten für VPN-Zugangsdienste bereitstellt, MUSS (1) die Zertifikatsstruktur gemäß Tab_PKI_212 und (2) im **`commonName`** die <usage> = VPNK, sowie (3) im **`organizationalUnitName`** den <usageName> = 'VPN-Zugangsdienst' umsetzen. ⌫

3.4 Spezifische Aussteller-CA in der TI

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

GS-A_4703 CA-Zertifikatsprofil für nonQES-Zertifikate

Ein TSP-X.509 nonQES und der Anbieter des TSL-Dienstes MÜSSEN für die Beantragung einer Aussteller-CA unterhalb der zentralen gematik-Root-CA die Zertifikatsstruktur gemäß Tab_PKI_212 und einem CA-Namen entsprechend der Tabelle Tab_PKI_213 umsetzen.⌫

GS-A_4704 Nutzung von CA mit spezifischem Verwendungszweck

Ein TSP-X.509 nonQES; TSP-X.509 QES und der Anbieter des TSL-Dienstes DÜRFEN aus einer Aussteller-CA mit einem spezifischen Verwendungszweck NICHT weitere EE-Zertifikate für andere Zwecke ausgeben.⌫

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

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

Tabelle 8: Tab_PKI_213 <tsp>.<usage>-CA<n> – Aussteller-CA_nonQES der TI

Spezifischer CA-Einsatzbereich	<usage> im Feld commonName	<usageName> im Feld organizationalUnitName
Heilberufsausweis	HBA	Heilberufsausweis
Berufsausweis	BA	Berufsausweis

Spezifischer CA-Einsatzbereich	<usage> im Feld commonName	<usageName> im Feld organizationalUnitName
Institutionskarten	SMCB	Institution des Gesundheitswesens
eHealth-Kartenterminals	SMKT	Kartenterminal
Konnektor	KON NK AK SAK	Konnektor Netzkonnektor Anwendungskonnektor SigAnwendKomponente
Zentrale Dienste	ZD	ZentraleDienste
Fachanwendungsspezif. Dienst	FD	FachanwendungsspezifischerDienst
OCSP-Dienst	OCSP	OCSP-Signer
CRL-Dienst	CRL	CRL-Signer
TSL-Dienst	TSL	TSL-Signer
VPN-Zugangsdienst	VPNK	VPN-Zugangsdienst
Elektronische Gesundheitskarte	EGK	Elektronische Gesundheitskarte

3.5 Sperrungen von QES-CAs

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

⌦ **GS-A_5065 Sperrung einer QES-CA**

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

4 Kodierung von X.509-Identitäten

4.1 Namensregeln und -formate

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

4.1.1 Verarbeitung von Sonderzeichen

⌦ **GS-A_4705 Verarbeitung von Sonderzeichen in PKI-Komponenten**

gematik-Root-CA, TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN sicherstellen, dass von ihnen eingesetzte Komponenten in der Lage sind, Sonderzeichen wie ä, ü, ö, ß etc., in den einzelnen Namenselementen zu verarbeiten und darzustellen. Es MUSS dazu ein Zeichensatz gemäß [Common-PKI#Part1] unterstützt werden.⌫

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

Für TI-interne SSL-Server und SSL-Client-Zertifikate können Umlaute und UTF-8-Codierungen verwendet werden, da auch für diese Komponenten eine Unterstützung eines Zeichensatzes gemäß [Common-PKI#Part 1] (s. o.) gefordert ist.

4.1.2 Definition der Subject-DNs für Personen und Komponenten

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

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

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

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

kunftsland des TSP (Land der Anschrift des TSP) enthalten. (e) Die Attribute serialNumber und organizationalUnitName können enthalten sein, sollen jedoch nur dann verwendet werden, falls sie für die Eindeutigkeit des subjectDN notwendig sind. Darüber hinaus sollen keine weiteren Attribute enthalten sein.⌫

4.2 Schlüssel der Versichertenidentität (eGK)

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

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

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

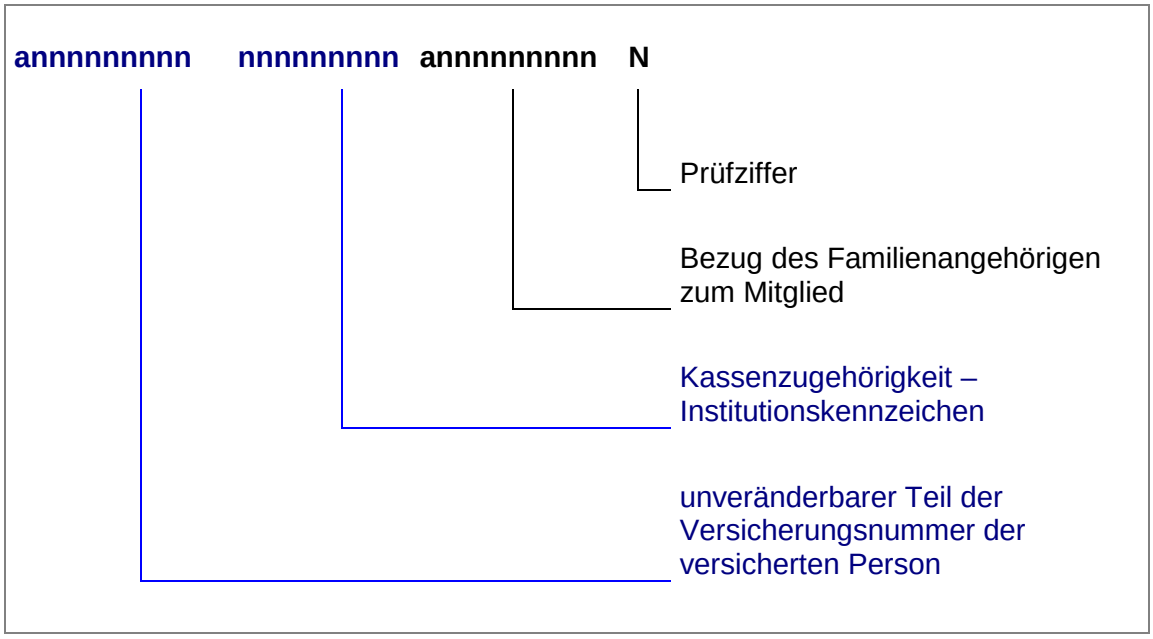

Abbildung 3: Aufbau der Krankenversichertennummer

4.3 Pseudonym der Versichertenidentität (eGK)

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

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

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

Der TSP-X.509 nonQES MUSS im Feld **commonName** der Zertifikatstypen C.CH.AUTN bzw. C.CH.ENCV das Pseudonym des Versicherten aufnehmen.

4.3.2 Eindeutigkeit des Pseudonym

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

GS-A_4573 Eindeutigkeit des Pseudonyms innerhalb Herausgeber-Domäne

Der TSP-X.509 nonQES MUSS das im AUTN- und ENCV-Zertifikat des Versicherten gespeicherte Pseudonym innerhalb der Herausgeber-Domäne (IssuerDomain) eindeutig gestalten.

4.3.3 Pseudonym-Erstellungsregel

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

GS-A_4574 Pseudonym-Erstellungsregel

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

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

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

Bei Kenntnis des Nachnamens sowie der KVNR eines Versicherten und sofern der vom Herausgeber verwendete Zufallswert zur Verfügung gestellt wird, kann das Pseudonym nachgerechnet werden.

Beispiel:

Nachname =
„**Mustername1**“

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

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

Konkatenation =
„**Mustername1M331784849A32C93C6946314A9**“

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

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

commonName =
“**E3F3555165491A7FBE3F**”

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

Der TSP-X.509 nonQES MUSS nach Erzeugung des Pseudonyms prüfen, ob dieses Pseudonym vom Kartenherausgeber bereits vergeben wurde. Ist dies der Fall, MUSS das Pseudonym mit inkrementiertem hs-ZW neu generiert und erneut auf Eindeutigkeit geprüft werden. ⌫

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

Der TSP-X.509 nonQES MUSS bei Ausstellung eines eGK-Ersatzausweises innerhalb der definierten Verwendungsperiode des herstellerspezifischen Zufallswertes (hs-ZW) dasselbe Pseudonym verwenden wie auf der vorgängigen Karte.⌫

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

Der TSP-X.509 nonQES MUSS bei Ausstellung eines eGK-Ersatzausweises nach Ablauf der definierten Verwendungsperiode des hs-ZW oder bei Ausstellung einer Folgekarte nach Ablauf des Gültigkeitszeitraums der vorgängigen Karte ein neues Pseudonym auf Grundlage des geänderten hs-ZW vergeben. ⌫

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

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

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

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

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

Der eGK-Herausgeber MUSS den aktuellen hs-ZW für alle Versichertenzertifikate für eine bestimmte Verwendungsperiode verwenden und mindestens einmal jährlich wechseln. ⌫

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

Der eGK-Herausgeber MUSS alle nicht mehr verwendeten hs-ZW für Zwecke der Rekonstruktion von Pseudonymen für mindestens 10 Jahre sicher speichern und berechtigten Teilnehmern der TI verfügbar machen.⌫

4.3.5 Kodierung des Pseudonyms

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

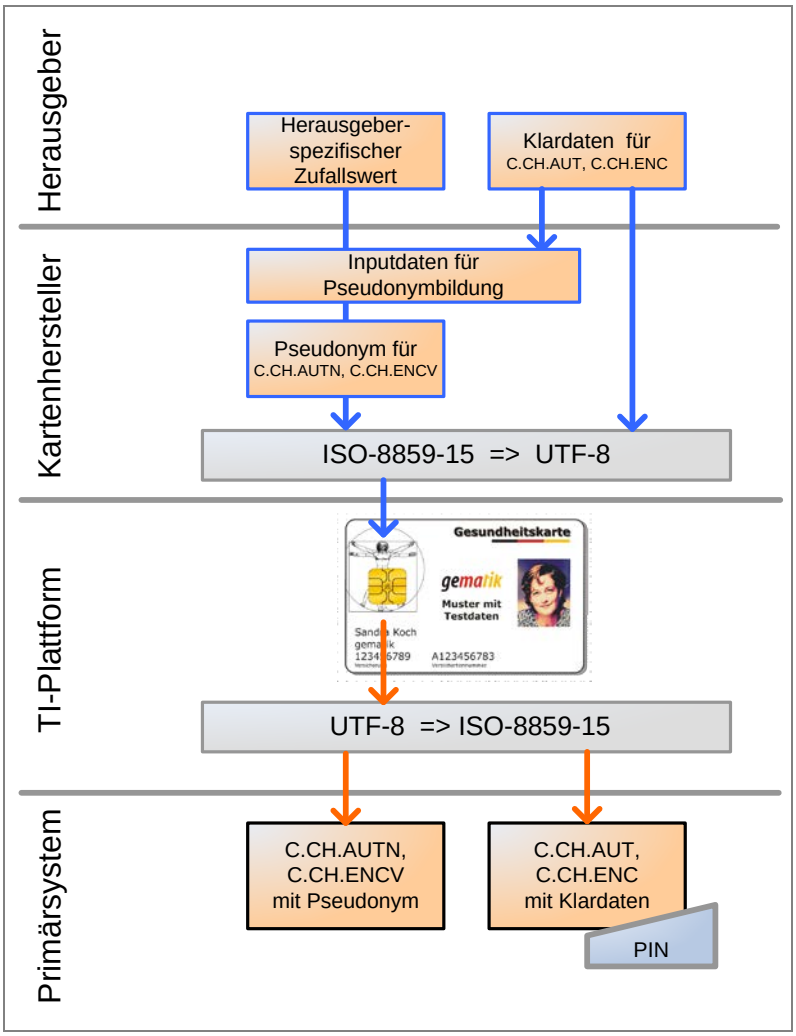

Abbildung 4 Pseudonym Kodierung in X.509-Versichertenzertifikaten

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

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

4.4 Berufsgruppen-ID der Leistungserbringer

4.4.1 Berufsgruppe des Heilberuflers

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

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

⌦ **GS-A_4583 Berufsgruppenkennzeichen für HBA**

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

⌦ **GS-A_4584 Verwendung von Berufsgruppenkennzeichen**

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

Tabelle 9: Tab_PKI_221 Berufsgruppenkennzeichnung

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

4.5 ID der Organisation/Einrichtung des Gesundheitswesens

4.5.1 Typ und Exemplar der Organisation/Einrichtung des Gesundheitswesens

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

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

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

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

GS-A_4586 Verwendung von Institutionskennzeichen

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

Tabelle 10: Tab_PKI_222 Institutionstypkennzeichnung

Art der ID	Ort	X.509 Feldname	Format	Inhalt	Beispiel
Institutionstyp	Admission	**ProfessionItem**	Text	<Institutionstyp>	Zahnarztpraxis
		ProfessionOID	OID	oid_<institutionstyp>	1.2.276.0.76.4.51
Einzelne Institution	Admission	**RegistrationNumber**	AN	<Telematik-ID>	1-1a25sd-d529

4.6 Technische Rolle von Komponenten und Diensten

4.6.1 Technische Rolle im Komponentenzertifikat

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

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

GS-A_4707 Kennzeichen für Technische Rolle für Komponenten und Dienste

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

GS-A_4708 Verwendung von Kennzeichen für Technische Rolle

TSP-X.509 nonQES MÜSSEN ausschließlich solche Kennzeichen für technische Rollen in Komponentenzertifikate einbringen, für die der Antragsteller nachweislich berechtigt ist.

Tabelle 11: Tab_PKI_230 Kennzeichnung Technische Rolle

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

4.7 Telematik-ID

Die Telematik-ID repräsentiert als eindeutiges Merkmal die Identität eines Leistungserbringers im HBA respektive einer Organisation/Einrichtung des Gesundheitswesens in einer SMC-B. Die Telematik-ID muss daher über alle Sektoren hinweg eindeutig sein.

Für Ersatz-/Folgekarten muss die Telematik-ID nicht identisch zur Vorgängerkarte sein. Der Arzt und die medizinische Institution können eine neue Telematik-ID beantragen oder auch die bisherige in der Folgekarte wieder verwenden. Ein Suffix zum Hochzählen bei Ersatz-/Folgekarten wird nicht verwendet.

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

Der Kartenherausgeber MUSS bei der Ausgabe von Folgekarten dem Antragsteller die Möglichkeit bieten, eine neue Telematik-ID zu beziehen.⌫

⌦ **GS-A_4960 System für Sektorkennzeichen**

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

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

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

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

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

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

TSP-X.509 QES und TSP-X.509 nonQES SOLLEN die Admission Extension in allen X.509-Zertifikaten einer Karte identisch einbringen. In den Herausgabe-Policies können Ausnahmen hiervon definiert sein.⌫

Tabelle 12: Tab_PKI_224 Telematik-ID-Kennzeichnung

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

4.7.2 Aufbau der Telematik-ID

Offener Punkt:

Detaillierte Festlegungen für den Aufbau der Telematik-ID der SMC-B liegen derzeit von den Leistungserbringerorganisationen für die SMC-Bs der medizinischen Institutionen vor.

GS-A_4587 Gesamtlänge der Telematik-ID

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

Tabelle 13: Tab_PKI_223 Aufbau der Telematik-ID

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

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

4.7.2.1 Sektoraler Präfix

GS-A_4710 Präfix der Telematik-ID

Herausgeber von HBA und SMC-B MÜSSEN sicherstellen, dass das Präfix der Telematik-ID eine natürliche Zahl ist, wobei einem Sektor eine ganz bestimmte Zahl zugeordnet sein muss.

Die normativen Werte des Präfixes sind in [gemKPT_PKI_TIP#Tab_PKI_101] aufgelistet. Der Nummernraum des Präfixes wird durch die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) verwaltet. Ein Präfix für weitere Sektoren kann unter der E-Mail-Adresse Industriepartnermanagement@gematik.de formlos beantragt werden.

4.7.2.2 Separator

GS-A_4711 Separator der Telematik-ID

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

4.7.2.3 Fortsatz der Telematik-ID

GS-A_4712 Definition und Eindeutigkeit der Telematik-ID

Kartenherausgeber von HBA und SMC-B in den jeweiligen Sektoren MÜSSEN Syntax, Semantik und Vergabe des Fortsatzes der Telematik-ID so definieren, dass die Eindeutigkeit des sektorspezifischen Anteils der Telematik-ID gewährleistet ist.

Beispiele für die weiterführende Unterteilung für den Bereich der Ärzteschaft:

- Die Telematik-ID beginnt mit 1-1 bei einem eArztausweis (HPC),

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

⌦ **GS-A_4713 Zeichensatz für den Fortsatz der Telematik-ID**

TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN als Zeichensatz für den Fortsatz der Telematik-ID printableString verwenden.⌫

4.7.3 Beispiele der Telematik-ID

In Tabelle 14 sind mögliche Telematik-IDs beispielhaft aufgeführt, sie erheben allerdings nur den Anspruch, die Aufteilung des Nummernraums durch das Präfix zu verdeutlichen.

Tabelle 14: Tab_PKI_225 Beispiele für mögliche Telematik-IDs

Beispielhafte Telematik-ID	Zuordnung
1-1001	Mögliche Telematik-ID des Sektors der Ärzteschaft
1-1x25sd-d 5dd	
1-2/01-d5d5d	
2-0001	Mögliche Telematik-ID des Sektors der Zahnärzteschaft
2-x25sd-d 5dd	
2-/01-d5d5d	

4.8 Kodierung der Zertifikate

4.8.1 Kodierung der Attribute

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

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

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

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

Attribut / Attribut-OID ([Common-PKI], [RFC 5280])	**Kodierung**	**Max. Stringlänge (Zeichen)**
commonName {id-at 3}	UTF-8 [RFC3629] *)	64
surName {id-at 4}	UTF-8 [RFC3629] *)	64

Attribut / Attribut-OID ([Common-PKI], [RFC 5280])	Kodierung	Max. Stringlänge (Zeichen)
localityName {id-at 7}	UTF-8 [RFC3629] *)	128
stateOrProvinceName {id-at 8}	UTF-8 [RFC3629] *)	128
streetAdress {id-at 9}	UTF-8 [RFC3629] *)	128
organizationName {id-at 10}	UTF-8 [RFC3629] *)	64
organizationalUnitName {id-at 11}	UTF-8 [RFC3629] *)	64
title {id-at 12}	UTF-8 [RFC3629] *)	64
postalCode {id-at 17}	UTF-8 [RFC3629] *)	40
givenName {id-at 42}	UTF-8 [RFC3629] *)	64
serialNumber {id-at 5}	PrintableString [RFC5280]	64
countryName {id-at 6}	PrintableString [RFC5280] gültiger "ISO 3166-1 alpha-2 country code" [ISO 3166-1]	2
*) Einschränkung des erlaubten Zeichensatzes auf dedizierte ISO-Subsets gemäß Vorgaben der jeweiligen Kartenherausgeber		

4.8.2 Stringlänge der Attribute

⌦ **GS-A_4715 Maximale Stringlänge der Attribute im SubjectDN**

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

⌦ **GS-A_4716 Umgang mit überlangen Organisationsnamen im SubjectDN**

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

4.8.3 Struktur

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

4.8.3.1 serialNumber

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

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

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

⌦ **GS-A_4726 Verwendung von serialNumber zur Schaffung eindeutiger SubjectDNs**

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

4.8.3.2 Admission

Die Extension Admission beinhaltet die Berufsgruppen (HBA, eGK), den Typ der Institution (SMC-B) oder die technische Rolle (Komponentenzertifikate) sowohl als Text als auch in Form einer maschinenlesbaren OID. Außerdem wird die Telematik-ID (nur in HBA-, BA und SMC-B-Zertifikaten) in Admission abgelegt.

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

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

Tabelle 16: Tab_PKI_226 Struktur Admission

#	ASN.1 DEFINITION	TI-SPEZIFISCHE VORGABEN
1	**id-isismtt-at-admission** OBJECT IDENTIFIER ::= {id-isismtt-at 3}	
2	**id-isismtt-at-namingAuthorities** OBJECT IDENTIFIER ::= {id-isismtt-at 11}	
3	**AdmissionSyntax ::=** SEQUENCE {	
4	admissionAuthority GeneralName OPTIONAL,	Angabe der admissionAuthority auf der obersten Ebene der Extension
5	contentsOfAdmissions SEQUENCE OF Admissions }	Diese Sequenz MUSS genau ein Element vom Typ Admissions enthalten.
6	**Admissions** ::= SEQUENCE {	
7	admissionAuthority [0] EXPLICIT GeneralName OPTIONAL,	
8	namingAuthority [1] EXPLICIT NamingAuthority OPTIONAL,	

9	professionInfos SEQUENCE OF ProfessionInfo }	Diese Sequenz MUSS ein Element vom Typ ProfessionInfo enthalten.
…		
14	**ProfessionInfo** ::= SEQUENCE {	
15	namingAuthority [0] EXPLICIT NamingAuthority OPTIONAL,	
16	professionItems SEQUENCE OF DirectoryString (SIZE(1..128)),	professionItems enthält ein Element von Typ DirectoryString Für DirectoryString MUSS die Kodierung UTF8String verwendet werden.
17	professionOIDs SEQUENCE OF OBJECT IDENTIFIER OPTIONAL,	Dieses Element MUSS eine OID enthalten.
18	registrationNumber PrintableString(SIZE(1..128)) OPTIONAL,	Dieses Feld SOLL genau ein Element enthalten. (Telematik-ID SOLL in allen Zertifikaten von HBA, BA und SMC-B enthalten sein. Ausnahme: QES-Zertifikat des HBA der Ärzte)
19	addProfessionInfo OCTET STRING OPTIONAL }	

4.8.3.3 CertificatePolicies

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

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

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

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

Tabelle 17: Tab_PKI_227 Struktur CertificatePolicies

#	ASN.1 DEFINITION	TI-SPEZIFISCHE VORGABEN
1	CertificatePolicies ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation	In allen End-Entity-Zertifikaten MUSS genau ein Element dieser Sequenz enthalten.
2	PolicyInformation ::= SEQUENCE {	
3	policyIdentifier CertPolicyId,	Dieses Element MUSS mindestens zweimal enthalten sein: 1 – Policy-OID (einmal oder mehrfach) 2 – Zertifikatstyp-OID (genau einmal bei EE-Zertifikaten, nicht bei Signer-EE-Zertifikaten)
4	policyQualifiers SEQUENCE SIZE(1..MAX) OF PolicyQualifierInfo OPTIONAL }	Enthält das Element PolicyIdentifier die Zertifikatstyp-OID, DARF das Element policyQualifiers NICHT verwendet werden
5	CertPolicyId ::= OBJECT IDENTIFIER	

6	PolicyQualifierInfo ::= SEQUENCE {	
7	policyQualifierId PolicyQualifierId,	
8	qualifier ANY DEFINED BY policyQualifierId }	
9	id-qt OBJECT IDENTIFIER ::= {id-pkix 2}	
10	id-qt-cps OBJECT IDENTIFIER ::= {id-qt 1}	
11	id-qt-unotice OBJECT IDENTIFIER ::= {id-qt 2}	
12	PolicyQualifierId ::= OBJECT IDENTIFIER {id-qt-cps | id-qt-unotice }	
13	CPSUri ::= IA5String	
14	UserNotice ::= SEQUENCE {	
15	noticeRef NoticeReference OPTIONAL,	
16	explicitText DisplayText OPTIONAL }	
17	NoticeReference ::= SEQUENCE {	
18	organization DisplayText,	
19	noticeNumber SEQUENCE OF INTEGER }	
20	DisplayText ::= CHOICE {	
20a	ia5String IA5String (SIZE (1..200)),	
21	visibleString VisibleString (SIZE (1..200)),	
22	bmpString BMPString (SIZE (1..200)),	
23	utf8String UTF8String (SIZE (1..200)) }	

4.8.3.4 CRLDistributionPoints

Zertifikate des Zugangsdienstes C.VPNK.VPN und C.VPNK.VPN-SIS werden im Internet mittels einer CRL auf ihren Sperrstatus geprüft.

GS-A_5074 Bereitstellung CRL für Zertifikate des VPN-Zugangsdienstes

Der TSP-X.509 nonQES, der eine Aussteller-CA für die Ausgabe von C.VPNK.VPN und C. VPNK.VPN-SIS Zertifikaten betreibt, MUSS für diese Zertifikate eine CRL im Internet bereitstellen.

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

4.8.3.5 SubjectAltNames

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

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

Tabelle 18: Tab_PKI_228 Struktur SubjectAltName

#	ASN.1 DEFINITION	TI-SPEZIFISCHE VORGABEN
1	SubjectAltNames ::= GeneralNames	Der GeneralName KANN in der Form rfc822Name angegeben werden.

2	OtherName ::= SEQUENCE
	{
	type-id OBJECT IDENTIFIER
	value [0] EXPLICIT ANY DEFINED BY type-id
	}
		Type-id MUSS den Wert {id-at 10} haben.

4.9 Erläuterungen zu Zertifikatsprofilen

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

4.9.1 Allgemeine Erläuterungen

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

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

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

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

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

4.9.2 Festlegung der Feldinhalte für subjectDN

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

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

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

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

⌦ **GS-A_4722 Belegung der Felder `professionInfos`**

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

⌦ **GS-A_4723 Einzelsperrbarkeit von Zertifikaten**

Der TSP-X.509 nonQES MUSS sicherstellen, dass jedes Zertifikat einzeln sperrbar ist, sofern für diesen Zertifikatstyp die Bereitstellung von Statusinformationen gefordert ist.⌫

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

TSP-X.509 nonQES und TSP-X.509 QES SOLLEN sicherstellen, dass ein Set von Zertifikaten, die von unterschiedlichem Typ, für genau eine kryptographische Identität zusammen in ein Kartenexemplar eingebracht werden, durch einen Sperrauftrag unter Angabe von Kartenexemplar und Identität gemeinsam gesperrt werden können, sofern für die jeweiligen Zertifikatstypen die Statusinformationsbereitstellungen gefordert sind.⌫

4.9.3 Benennung der Zertifikatsprofile

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

4.10 Kodierung der Betriebsumgebungen in Zertifikaten

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

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

Der TSP-X.509 und der Anbieter des TSL-Dienstes DÜRFEN für die Generierung von EE-Zertifikaten der Produktivumgebung NICHT eine CA der Testumgebung verwenden. Umgekehrt DÜRFEN der TSP-X.509 und der Anbieter des TSL-Dienstes für die Generierung von EE-Zertifikaten der Testumgebung NICHT eine CA der Produktivumgebung verwenden.⌫

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

Der TSP-X.509 und der Anbieter des TSL-Dienstes MÜSSEN die Namen (CN: und O:) sämtlicher CAs in der Test-PKI entsprechend den korrespondierenden CAs der Produktivumgebung vergeben und diese um den String „TEST-ONLY“ im CN-Feld sowie „NOT-VALID“ im O-Feld ergänzen.⌫

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

TSP-X.509 nonQES und TSP-X.509 QES und der Anbieter des TSL-Dienstes MÜSSEN die Namen (CN: und O:) sämtlicher EE-Zertifikate in der Test-PKI entsprechend den korrespondierenden Zertifikatsprofilen der Produktivumgebung verwenden und ergänzen (a) für Personen-, Institutions- und Signer-Zertifikate um den String „TEST-ONLY“ im CN-Feld sowie „NOT-VALID“ im O-Feld, (b) für alle anderen Zertifikate um den String "TEST-ONLY - NOT-VALID" im O-Feld.⌫

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

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

4.11 Kartenverlust und Deaktivierung von Chipkarten

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

Der Kartenherausgeber MUSS den Zertifikatsnehmer verpflichten, den Verlust seiner Karte bzw. seines Sicherheitsmoduls sowie Änderungen zu registrierungsrelevanten persönlichen Daten an den Kartenherausgeber zu melden (bspw. Änderung der Zugehörigkeit zu einer Berufsgruppe).⌫

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

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

5 X.509-Zertifikate

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

Die Schreibweise der Termini entspricht [Common-PKI].

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

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

Die X.509-Zertifikate kann ein Kartenherausgeber entweder aus einer eigenen – von der gematik Root-CA abgeleiteten CA erstellen oder von der zentralen PKI der TI als Zulieferung beziehen.

⌦ **GS-A_4964 Bezug von X.509-Zertifikaten aus der zentralen PKI der TI**

Ein Kartenherausgeber und Anbieter von Diensten in der TI KANN X.509-Zertifikate nach entsprechender Registrierung aus der zentralen PKI vom TSP-X.509nonQES beziehen.⌫

Mangels praktischer Nutzeffekte und zur Vereinfachung der Implementierungen und Straffung organisatorischer Prozesse bei Kartenherausgebern und TSP ist eine Suspendierung von X.509-Zertifikaten in der TI nicht vorgesehen.

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

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

5.1 eGK - Versichertenkarte

5.1.1 Definition der Versichertenidentität

Folgende Datenfelder bilden die Namensidentität des Versicherten

(1) Vorname des Versicherten

(2) Familienname des Versicherten

(3) Titel des Versicherten

(4) Namenszusatz

(5) Vorsatzwort

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

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

⌦ **GS-A_4966 Nutzung bestehender Versichertendatensätze für eGK-Zertifikate**

Für die Erstellung von Versichertenzertifikaten SOLL der Kartenherausgeber bestehende Versichertendatensätze für die Registrierung von Zertifikatsnehmern verwenden.⌫

5.1.2 Belegung der Felder im SubjectDN

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

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

Titel Vorname Namenszusatz Vorsatzwort Familienname

⌦ **GS-A_4967 Vergabe und Übermittlung eindeutiger Versicherten-ID**

Die Kostenträger MÜSSEN für den Versicherten eine eindeutige ID vergeben und zur Zertifikatserstellung an den Zertifikatsherausgeber zur Einbringung in die Zertifikate übermitteln.⌫

⌦ **GS-A_4968 Erzeugung und Einbringung der KVNR**

Der eGK-Kartenherausgeber MUSS als eindeutigen Identifier des Versicherten die KVNR gemäß gesetzlicher Vorgaben erzeugen und Festlegungen treffen, welche Anteile der KVNR in die Versichertenzertifikate einzubringen sind.⌫

⌦ **GS-A_4592 Bildung des surname im SubjectDN eGK-Zertifikat**

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

⌦ **GS-A_4593 Bildung des givenName im SubjectDN eGK-Zertifikat**

Der Kartenherausgeber MUSS für das Feld **givenName** im SubjectDN der eGK-Zertifikate die Attribute *Vorname Namenszusatz Vorsatzwort* verwenden und MUSS bei erforderlichen Kürzungen bis zur maximal zulässigen Länge des Feldes folgende Regel anwenden: (a) ein ggf. vorhandener dritter Rufname ist auf den Anfangsbuchstaben zu verkürzen und die Kürzung durch Punkt kenntlich zu machen. Ist die

Kürzung nicht ausreichend, MUSS zusätzlich gelten: (b) ein zweiter Rufname ist ggf. bis auf den Anfangsbuchstaben zu kürzen und die Kürzung durch Punkt kenntlich zu machen.⌫

⌦ **GS-A_4594 Bildung des title im SubjectDN eGK-Zertifikat**

Der Kartenherausgeber MUSS für das Feld **`title`** im SubjectDN der eGK-Zertifikate das Attribut *Titel* verwenden. Kürzungen können bei Überschreitung der maximal zulässigen Länge vorgenommen werden; Kürzungsregeln sind nicht definiert.⌫

Beispielsatz der Feldinhalte

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

Im Zertifikat wären folgende Attribute zu verwenden:

Tabelle 19: Tab_PKI_231 Personennamen im subjectDN

Feld	Inhalt
title	Dr.-Ing. oder bei gekürztem Titel nur Dr.
givenName	Peter-Wilhelm Markgraf von
surname	Meckelburg-Vorpommeln
commonName	Dr. Peter-W. Markgraf von Meckelburg-Vorpommeln

5.1.3 X.509-Zertifikatsprofile der eGK

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

⌦ **GS-A_4969 Suspendierung von eGK-Zertifikaten (nonQES)**

Ein Kartenherausgeber SOLL für die X.509-Zertifikate der eGK eine Suspendierung und Desuspendierung von nonQES-Zertifikaten NICHT implementieren. Für das optional auf der eGK befindliche QES-Zertifikat ist eine Suspendierung/Desuspendierung nicht möglich.⌫

5.1.3.1 C.CH.AUT – Authentisierung eGK

⌦ **GS-A_4595 Umsetzung Zertifikatsprofil C.CH.AUT**

Der TSP-X.509 nonQES MUSS C.CH.AUT gemäß Tab_PKI_232 umsetzen.⌫

Tabelle 20 Tab_PKI_232 C.CH.AUT Authentisierung eGK

Element	Inhalt	Kar.	
certificate	C.CH.AUT		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
issuer	DN der ausstellenden CA		
validity	Gültigkeit des Zertifikats (von - bis)		
subject			
CommonName	CN = Aufgedruckte Namenszeilen der Karte	1	
title	Titel des Versicherten	0-1	
givenName	Vorname des Versicherten	1	
surname	Nachname des Versicherten	1	
organizationalUnitName	OU = unveränderbarer Teil der KV-Nummer	1	
organizationalUnitName	OU = Institutionskennzeichen	1	
organizationName	O = Herausgeber	1	
countryName	C = DE	1	
subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers	1	
extensions			critical
SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Versicherten	1	FALSE
KeyUsage {2 5 29 15}	digitalSignature keyEncipherment	1 0-1	**TRUE**
SubjectAltNames {2 5 29 17}	rfc822Name	0-1	FALSE
BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie policyIdentifier = <oid_egk_aut>	1 0-1 1	FALSE
CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
Admission {1 3 36 8 3 3}	professionItem = <oid_versicherter> professionOID = <oid_versicherter>	1	FALSE
ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth	0-1	FALSE
andere Erweiterungen		0	
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
signature	Wert der Signatur		

5.1.3.2 C.CH.ENC – Verschlüsselung eGK

GS-A_4596 Umsetzung Zertifikatsprofil C.CH.ENC

Der TSP-X.509 nonQES MUSS C.CH.ENC gemäß Tab_PKI_233 umsetzen.

Tabelle 21 Tab_PKI_233 C.CH.ENC Verschlüsselung eGK

Element			Inhalt	Kar.	
certificate			C.CH.ENC		
tbsCertificate					
version			2 (v3)		
serialNumber			gemäß [RFC5280#4.1.2.2.]		
signature			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt# GS-A_4362]		
issuer			DN der ausstellenden CA		
validity			Gültigkeit des Zertifikats (von - bis)		
subject					
	CommonName		CN = Aufgedruckte Namenszeilen der Karte	1	
	title		Titel des Versicherten	0-1	
	givenName		Vorname des Versicherten	1	
	surname		Nachname des Versicherten	1	
	organizationalUnitName		OU = unveränderbarer Teil der KV-Nummer	1	
	organizationalUnitName		OU = Institutionskennzeichen	1	
	organizationName		O = Herausgeber	1	
	countryName		C = DE	1	
subjectPublicKeyInfo			Algorithmus gemäß [gemSpec_Krypt#GS-A_4362] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers	1	
extensions			Erweiterungen		critical
	SubjectKeyIdentifier {2 5 29 14}		keyIdentifier = ID des öffentlichen Schlüssels des Versicherten	1	FALSE
	KeyUsage {2 5 29 15}		keyEncipherment dataEncipherment	1 1	**TRUE**
	SubjectAltNames {2 5 29 17}		rfc822Name	0-1	FALSE
	BasicConstraints {2 5 29 19}		ca = FALSE	1	**TRUE**
	CertificatePolicies {2 5 29 32}		policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie policyIdentifier = <oid_egk_enc>	1 0-1 1	FALSE
	CRLDistributionPoints {2 5 29 31}		keine Festlegung	0-1	FALSE
	AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}		URL für OCSP-Statusdienst	1	FALSE
	AuthorityKeyIdentifier {2 5 29 35}		keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
	Admission {1 3 36 8 3 3}		professionItem = <oid_versicherter> professionOID = <oid_versicherter>	1	FALSE
	ExtendedKeyUsage			0	

Element				Inhalt	Kar.	
			{2 5 29 37}			
			andere Erweiterungen		0	
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt# GS-A_4362]		
	signature			Wert der Signatur		

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

⌦ GS-A_4597 Umsetzung Zertifikatsprofil C.CH.QES

Der TSP-X.509 QES MUSS C.CH.QES gemäß Tab_PKI_234 umsetzen.⌫

Tabelle 22 Tab_PKI_234 C.CH.QES Qualifizierte Signatur eGK

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

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

5.1.3.4 C.CH.AUTN - Technische Authentisierung eGK

GS-A_4598 Umsetzung Zertifikatsprofil C.CH.AUTN

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

Tabelle 23 Tab_PKI_235 C.CH.AUTN Technische Authentisierung eGK

Element			Inhalt	Kar.	
certificate			C.CH.AUTN		
	tbsCertificate				
		version	2 (v3)		
		serialNumber	gemäß [RFC5280#4.1.2.2.]		
		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
		issuer	DN der ausstellenden CA		
		validity	Gültigkeit des Zertifikats (von - bis)		
		subject			
		CommonName	CN = Pseudonym der Versichertenidentität	1	
		organizationalUnitName	OU = Institutionskennzeichen	1	
		organizationName	O = Herausgeber	1	
		countryName	C = DE	1	
		subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers	1	

Element			Inhalt	Kar.	
	extensions		Erweiterungen		critical
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Versicherten	1	FALSE
		KeyUsage {2 5 29 15}	digitalSignature keyEncipherment	1 0-1	**TRUE**
		SubjectAltNames {2 5 29 17}	rfc822Name	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie policyIdentifier = <oid_egk_autn>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = <oid_versicherter> professionOID = <oid_versicherter>	1	FALSE
		ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth	1	FALSE
		andere Erweiterungen		0	
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	signature		Wert der Signatur		

5.1.3.5 C.CH.ENCV - Technische Verschlüsselung eGK

⌦ GS-A_4599 Umsetzung Zertifikatsprofil C.CH.ENCV

Der TSP-X.509 nonQES MUSS C.CH.ENCV gemäß Tab_PKI_236 umsetzen.⌫

Tabelle 24 Tab_PKI_236 C.CH.ENCV Technische Verschlüsselung eGK

Element			Inhalt	Kar.	
certificate			C.CH.ENCV		
	tbsCertificate				
		version	2 (v3)		
		serialNumber	gemäß [RFC5280#4.1.2.2.]		
		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4362]		
		issuer	DN der ausstellenden CA)		
		validity	Gültigkeit des Zertifikats (von – bis)		
		subject			
		CommonName	CN = Pseudonym der Versichertenidentität	1	
		organizationalUnitName	OU = Institutionskennzeichen	1	
		organizationName	O = Herausgeber	1	
		countryName	C = DE	1	

		subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt# GS-A_4362] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers	1	
		extensions	Erweiterungen		critical
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Versicherten	1	FALSE
		KeyUsage {2 5 29 15}	keyEncipherment dataEnciperment	1 1	**TRUE**
		SubjectAltNames {2 5 29 17}	rfc822Name	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie policyIdentifier = <oid_egk_encv>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = <oid_versicherter> professionOID = <oid_versicherter>	1	FALSE
		ExtendedKeyUsage {2 5 29 37}		0	
		andere Erweiterungen		0	
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4362]		
	signature		Wert der Signatur		

5.2 HBA - Heilberufeausweis

Die Zertifikatsprofile der HBA-Zertifikate sind in den folgenden Dokumenten beschrieben:

- Zertifikatsprofile für X.509 Basiszertifikate der Ärzte [baekCerts]
- Zertifikatsprofil des elektronischen Zahnarztausweises [bzaekCert]
- Zertifikatsprofile für X.509 Attributzertifikate [baekAttr]
- Gemeinsame Policy für die Herausgabe der HPC [CP-HPC]

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

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

⌦ **GS-A_4970 Nutzung bestehender LE-Datensätze für HBA- / SMC-B-Zertifikate**

Für die Erstellung von HBA-Zertifikaten sowie SMC-B-Zertifikaten SOLL der Kartenherausgeber bestehende LE-Datensätze für die Registrierung von Zertifikatsnehmern verwenden.⌫

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

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

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

5.3.1 Definition der Organisationsidentität

Der eindeutige Identitätsname der Organisation wird durch folgende Felder gebildet:

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

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

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

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

Die Kartenherausgeber MÜSSEN die eindeutige Zuordnung von SMC-B zur berechtigten Institution sicherstellen. ⌫

5.3.2 Aufbau Anschriftzone nach [DIN5008]

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

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

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

Beispiel

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

Abbildung 5: Das Anschriftenfeld nach DIN5008

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

5.3.3 Umgang mit überlangen Attributen im SubjectDN

Überlange Attribute des SubjectDN werden zusätzlich in der Extension „SubjectAltNames“ in voller Länge abgebildet.

Felder des „SubjectAltNames“ werden im Format GeneralName gespeichert, welches eine Vielzahl von Ausprägungen hat. Für die Verwendung von überlangen Namen wird der Typ `OtherName` benutzt. Der Aufbau ist wie folgt:

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

Die `type-id` entspricht der OID des zu verlängernden Feldes (Für weitere Informationen, siehe ITU-T Rec. X.501 | [ISO/IEC9594-2]). Das Format des `value` wird entsprechend des Attributes festgelegt.

Beispiel:

SubjectDN:

organizationName: „gematik Institution“

SubjectAltNames:

OtherName: type-id: ‚2.5.4.10’

value: „gematik Institution in 10117 Berlin, Inhaber: Prof. Dr. Getein gematik“

5.3.4 X.509 Zertifikatsprofile der SMC-B

5.3.4.1 C.HCI.AUT – Authentisierung SMC- B

⌦ GS-A_4600 Umsetzung Zertifikatsprofil C.HCI.AUT

Der TSP-X.509 nonQES MUSS C.HCI.AUT gemäßTab_PKI_238 umsetzen.⌫

Tabelle 25: Tab_PKI_238 C.HCI.AUT Authentisierung SMC-B

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

Element			Inhalt *)	Kar.	
			Zertifikatsinhabers		
		extensions			critical
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels der Organisation/Einrichtung des Gesundheitswesens	1	FALSE
		KeyUsage {2 5 29 15}	digitalSignature keyEncipherment	1 1	**TRUE**
		SubjectAltNames {2 5 29 17}	rfc822Name ggf. überlange Institutionsnamen	0-1 0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie policyIdentifier = <oid_smc_b_aut>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = Beschreibung der Institution gemäß [gemSpec_OID#GS-A_4443] professionOID = OID der Institution gemäß [gemSpec_OID#GS-A_4443] registrationNumber = Telematik-ID der Institution	1	FALSE
		ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth	1	FALSE
		andere Erweiterungen		0	
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	signature		Wert der Signatur		

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

5.3.4.2 C.HCI.ENC – Verschlüsselung SMC-B

GS-A_4601 Umsetzung Zertifikatsprofil C.HCI.ENC

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

Tabelle 26: Tab_PKI_239 C.HCI.ENC Verschlüsselung SMC-B

Element			Inhalt *)	Kar.	
certificate			C.HCI.ENC		
	tbsCertificate				
		version	2 (v3)		
		serialNumber	gemäß [RFC5280#4.1.2.2.]		
		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4362]		

Element			Inhalt *)	Kar.	
	issuer		Distinguished Name (DN) der Aussteller-CA		
	validity		Gültigkeit des Zertifikats (von – bis)		
	subject				
		commonName	Erste zwei Zeilen des Anschriftenfeldes	1	
		title	Titel des Verantwortlichen/Inhabers	0-1	
		surName	Nachname des Verantwortlichen/Inhabers	0-1	
		givenName	Vorname des Verantwortlichen/Inhabers	0-1	
		serialNumber	Ti-weit eindeutige Identifikationsnummer	1	
		streetAddress	Strasse, Hausnummer	0-1	
		postalCode	Postleitzahl	0-1	
		localityName	Stadt	0-1	
		stateOrProvinceName	Bundesland	0-1	
		organizationalUnitName	Organisationseinheit der Organisation/Einrichtung des Gesundheitswesens	0-1	
		organizationName	Name der Organisation/Einrichtung des Gesundheitswesens	1	
		countryName	DE	1	
		andere Attribute		0	
	subjectPublicKeyInfo		Algorithmus gemäß [gemSpec_Krypt# GS-A_4362] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
	extensions				critical
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels der Organisation/Einrichtung des Gesundheitswesens	1	FALSE
		KeyUsage {2 5 29 15}	keyEncipherment dataEncipherment	1 1	**TRUE**
		SubjectAltNames {2 5 29 17}	rfc822Name ggf. überlange Institutionsnamen	0-1 0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie policyIdentifier = <oid_smc_b_enc>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = Beschreibung der Institution gemäß [gemSpec_OID#GS-A_4443] professionOID = OID der Institution gemäß [gemSpec_OID#GS-A_4443] registrationNumber = Telematik-ID der Institution	1	FALSE
		ExtendedKeyUsage {2 5 29 37}		0	
		andere Erweiterungen		0	

Element		Inhalt *)	Kar.	
	signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4362]		
	signature	Wert der Signatur		

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

5.3.4.3 C.HCI.OSIG – Signatur SMC-B

GS-A_4602 Umsetzung Zertifikatsprofil C.HCI.OSIG

Der TSP-X.509 nonQES MUSS C.HCI.OSIG gemäß Tab_PKI_240 umsetzen.

Tabelle 27: Tab_PKI_240 C.HCI.OSIG Signatur SMC-B

Element			Inhalt *)	Kar.	
certificate			C.HCI.OSIG		
	tbsCertificate				
		version	2 (v3)		
		serialNumber	gemäß [RFC5280#4.1.2.2.]		
		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
		issuer	Distinguished Name (DN) der Aussteller-CA		
		validity	Gültigkeit des Zertifikats (von – bis)		
		subject			
			commonName	Erste zwei Zeilen des Anschriftenfeldes	1
			title	Titel des Verantwortlichen/Inhabers	0-1
			surName	Nachname des Verantwortlichen/Inhabers	0-1
			givenName	Vorname des Verantwortlichen/Inhabers	0-1
			serialNumber	Ti-weit eindeutige Identifikationsnummer	1
			streetAddress	Strasse, Hausnummer	0-1
			postalCode	Postleitzahl	0-1
			localityName	Stadt	0-1
			stateOrProvinceName	Bundesland	0-1
			organizationalUnitName	Organisationseinheit der Organisation/Einrichtung des Gesundheitswesens	0-1
			organizationName	Name der Organisation/Einrichtung des Gesundheitswesens	1
			countryName	DE	1
			andere Attribute		0
		subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4357] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
		extensions			critical
			SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels der Organisation/Einrichtung des Gesundheitswesens	1	FALSE
			KeyUsage {2 5 29 15}	nonRepudiation	1	**TRUE**

Element			Inhalt *)	Kar.	
		SubjectAltNames {2 5 29 17}	rfc822Name ggf. überlange Institutionsnamen	0-1 0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie policyIdentifier = <oid_smc_b_osig>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = Beschreibung der Institution gemäß [gemSpec_OID#GS-A_4443] professionOID = OID der Institution gemäß [gemSpec_OID#GS-A_4443] registrationNumber = Telematik-ID der Institution	1	FALSE
		ExtendedKeyUsage {2 5 29 37}		0	
		andere Erweiterungen		0	
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
	signature		Wert der Signatur		

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

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

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

5.5 gSMC-KT – eHealth-Kartenterminal

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

⌦ **GS-A_4603 Statusprüfung von Zertifikaten der gSMC-KT**

Der TSP-X.509 nonQES SOLL NICHT für die von ihm ausgestellten gSMC-KT X.509-Zertifikate Statusinformationen bereitstellen.⌫

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

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

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

5.5.1 Definition der Kartenterminalidentität

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

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

5.5.2 X.509 Zertifikatsprofile der gSMC-KT

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

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

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

Tabelle 28: Tab_PKI_241 C.SMKT.AUT gSMC-KT

Element			Inhalt	Kar.	
certificate			C.SMKT.AUT		
	tbsCertificate				
		version	2 (v3)		
		serialNumber	gemäß [RFC5280#4.1.2.2.]		
		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
		issuer	DN der ausstellenden CA		
		validity	Gültigkeit des Zertifikats (von – bis)		
		subject			
		commonName	ICCSN der gSMC-KT	1	
		streetAddress	Anschrift des Kartenterminal-Herstellers	0-1	
		postalCode	Postleitzahl der Anschrift des Kartenterminal-Herstellers	0-1	
		localityName	Stadt der Anschrift desKartenterminal-Herstellers	0-1	
		stateOrProvinceName	Bundesland der Anschrift desKartenterminal-Herstellers	0-1	
		organizationalUnitNam	Relevante Einheit des Kartenterminal-Herstellers	0-1	

Element			Inhalt	Kar.	
		e			
		organizationName	Name des Kartenterminal-Herstellers	1	
		countryName	DE	1	
		andere Attribute		0	
	subjectPublicKeyInfo		Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
	extensions				**critical**
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Kartenterminals	1	FALSE
		KeyUsage {2 5 29 15}	digitalSignature keyEncipherment	1 1	**TRUE**
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Kartenterminal-Herstellers	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie policyIdentifier = <oid_smkt _aut>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}		0	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}		0	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = <oid_kt> professionOID = <oid_kt>	1	FALSE
		ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-serverAuth	1	FALSE
		andere Erweiterungen		0	
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	signature		Wert der Signatur		

5.6 gSMC-K – Konnektor

5.6.1 Definition und Zuweisung der Konnektoridentität

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

⌦ **GS-A_4605 Verwendung registrierter Daten für gSMC-K-Zertifikatsbeantragung**

Der Konnektor-Hersteller MUSS sicherstellen, dass bei der Beantragung von X.509-Zertifikaten für Konnektoren für die Felder **`SubjectDN`** nur die Werte verwenden werden, die im Rahmen seiner Herstellerzulassung registriert sind.⌫

GS-A_4606 Identischer ICCSN in allen Zertifikaten einer gSMC-K

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

GS-A_4607 Zuordnung Konnektorinstanz zu verbauter gSMC-K

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

5.6.2 Aufbau des SubjectDN

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

- **commonName = [ICCSN der gSMC-K] + "-" + [Erstausgabedatum der C.NK.VPN für diese ICCSN]**
  (ICCSN der gSMC-K + Delimiter "-" + Erstausgabedatum der C.SMK.AUT für diese ICCSN in der Form JJJJMMTT)
- **organizationName = [Name des Konnektor-Herstellers],**
- **countryName = [Herkunftsland des Konnektor-Herstellers, DE]**

5.6.3 Statusprüfung von Konnektorzertifikaten

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

GS-A_4608 Statusprüfung von Konnektorzertifikaten

Der TSP-X.509 nonQES MUSS für die von ihm ausgestellten X.509-Zertifikate des Konnektors eine Statusprüfung per OCSP gemäß Tabelle Tab_PKI_237 vorsehen.

Tabelle 29: Tab_PKI_237 Statusprüfung von Konnektorzertifikaten

Konnektorzertifikat	Statusprüfung per OCSP
C.NK.VPN	Ja
C.AK.AUT	Nein
C.SAK.AUT	Nein

5.6.4 X.509 Zertifikatsprofile des Konnektors

5.6.4.1 C.NK.VPN – VPN-Authentisierung Netzkonnektor

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

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

Der TSP-X.509 nonQES MUSS C.NK.VPN gemäß Tab_PKI_242 umsetzen.⌫

Tabelle 30: Tab_PKI_242 Zertifikatsprofil C.NK.VPN VPN-Authentisierung Netzkonnektor

Element			Inhalt	Kar.	
certificate			C.NK.VPN		
tbsCertificate					
	version		2 (v3)		
	serialNumber		gemäß [RFC5280#4.1.2.2.]		
	signature		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4360]		
	issuer		DN der ausstellenden CA		
	validity		Gültigkeit des Zertifikats (von – bis)		
	subject				
		commonName	<ICCSN der gSMC-K>-<Datum>	1	
		streetAddress	Anschrift desKonnektor-Herstellers	0-1	
		postalCode	Postleitzahl der Anschrift des Konnektor-Herstellers	0-1	
		localityName	Stadt der Anschrift des Konnektor-Herstellers	0-1	
		stateOrProvinceName	Bundesland der Anschrift des Konnektor-Herstellers	0-1	
		organizationalUnitName	Relevante Einheit des Konnektor-Herstellers	0-1	
		organizationName	Name des Konnektor-Herstellers	1	
		countryName	DE	1	
		andere Attribute		0	
	subjectPublicKeyInfo		Algorithmus gemäß [gemSpec_Krypt# GS-A_4360] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
	extensions				**critical**
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Konnektors	1	FALSE
		KeyUsage {2 5 29 15}	digitalSignature keyEncipherment	1 1	**TRUE**
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Konnektor-Herstellers	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie policyIdentifier = <oid_nk_vpn>	1 0-1 1	FALSE

Element			Inhalt	Kar.	
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = <oid_nk> professionOID = <oid_nk>	1	FALSE
		ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth keyPurposeId = id-kp-serverAuth	1	FALSE
		andere Erweiterungen		0	
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4360]		
	signature		Wert der Signatur		

5.6.4.2 C.AK.AUT - Authentisierung Anwendungskonnektor

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

⌦ GS-A_4610 Umsetzung Zertifikatsprofil C.AK.AUT

Der TSP-X.509 nonQES MUSS C.AK.AUT gemäß Tab_PKI_243 umsetzen.⌫

Tabelle 31: Tab_PKI_243 Zertifikatsprofil C.AK.AUT Authentisierung Anwendungskonnektor

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

Element			Inhalt	Kar.	
			und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
		extensions			**critical**
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Konnektors	1	FALSE
		KeyUsage {2 5 29 15}	digitalSignature keyEncipherment	1 1	**TRUE**
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Konnektor-Herstellers	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie policyIdentifier = <oid_ak_aut>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	keine Festlegung	0-1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = <oid_ak> professionOID = <oid_ak>	1	FALSE
		ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth keyPurposeId = id-kp-serverAuth	1	FALSE
		andere Erweiterungen		0	
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	signature		Wert der Signatur		

5.6.4.3 C.SAK.AUT - Authentisierung SAK

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

⌦ **GS-A_4611 Umsetzung Zertifikatsprofil C.SAK.AUT**

Der TSP-X.509 nonQES MUSS C.SAK.AUT gemäß Tab_PKI_244 umsetzen.⌫

Tabelle 32: Tab_PKI_244 Zertifikatsprofil C.SAK.AUT Authentisierung SAK

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

Element			Inhalt	Kar.	
	signature		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	issuer		DN der ausstellenden CA		
	validity		Gültigkeit des Zertifikats (von – bis)		
	subject				
		commonName	<ICCSN der gSMC-K>-<Datum>	1	
		streetAddress	Anschrift des Konnektor-Herstellers	0-1	
		postalCode	Postleitzahl der Anschrift des Konnektor-Herstellers	0-1	
		localityName	Stadt der Anschrift des Konnektor-Herstellers	0-1	
		stateOrProvinceName	Bundesland der Anschrift des Konnektor-Herstellers	0-1	
		organizationalUnitName	Relevante Einheit des Konnektor-Herstellers	0-1	
		organizationName	Name des Konnektor-Herstellers	1	
		countryName	DE	1	
		andere Attribute		0	
	subjectPublicKeyInfo		Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
	extensions				**critical**
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Konnektors	1	FALSE
		KeyUsage {2 5 29 15}	digitalSignature keyEncipherment	1 1	**TRUE**
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Konnektor-Herstellers	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie policyIdentifier = <oid_sak_aut>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	keine Festlegung	0-1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = <oid_sak> professionOID = <oid_sak>	1	FALSE
		ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth keyPurposeId = id-kp-serverAuth	1	FALSE
		andere Erweiterungen		0	
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	signature		Wert der Signatur		

5.7 VPN-Zugangsdienst

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

5.7.1 Definition und Zuweisung der Zugangsdienstidentitäten

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

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

5.7.2 Aufbau des SubjectDN

Der *SubjectDN* (*subject distinguishedName*) des Zertifikats verbindet den Dienste-FQDN mit der Identität des Anbieters:

- **`commonName = [FQDN des Dienstes]`**
- **`serialNumber = [Instanz-Nr des Dienstes]`**
- **`organizationName = [Name Zugangsnetz-Diensteanbieter]`**
- **`countryName = [Herkunftsland Zugangsnetz-Diensteanbieter]`**

5.7.3 X.509-Zertifikatsprofile des Zugangsdienstes

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

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

Der TSP-X.509 nonQES MUSS C.VPNK.VPN gemäß Tab_PKI_245 umsetzen.⌫

Tabelle 33: Tab_PKI_245 Zertifikatsprofil C.VPNK.VPN VPN-Authentisierung Zugangsdienst TI

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

Element			Inhalt	Kar.	
	validity		Gültigkeit des Zertifikats (von – bis)		
	subject				
		commonName	FQDN des Zugangsdienstes gemäß Festlegung aus Dienstezulassung	1	
		serialNumber	Zur Unterscheidung gleichartiger Instanzen	0-1	
		streetAddress	Anschrift Zugangsdienstanbieters	0	
		postalCode	Postleitzahl Zugangsdienstanbieters	0	
		localityName	Stadt Zugangsdienstanbieters	0	
		stateOrProvinceName	Bundesland Zugangsdienstanbieters	0	
		organizationalUnitName	Organisationseinheit Zugangsdienstanbieters	0	
		organizationName	Name des Zugangsdienstanbieters	1	
		countryName	DE	1	
		andere Attribute		0	
	subjectPublicKeyInfo		Algorithmus gemäß [gemSpec_Krypt#GS-A_4360] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
	extensions				**critical**
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Konzentrators	1	FALSE
		KeyUsage {2 5 29 15}	digitalSignature keyEncipherment	1 1	**TRUE**
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Zugangsdienstanbieters	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie policyIdentifier = <oid_vpnk_vpn>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}	URL für CRL-Statusdienst	1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	keine Festlegung	0-1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = <oid_vpnz_ti> professionOID = <oid_vpnz_ti>	1 1	FALSE
		ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth keyPurposeId = id-kp-serverAuth	1 1	FALSE
		andere Erweiterungen		0	
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4360]		
	signature		Wert der Signatur		

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

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

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

Tabelle 34: Tab_PKI_265 Zertifikatsprofil C.VPNK.VPN-SIS VPN-Authentisierung Zugangsdienst Sicherer Internetzugang

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

Element				Inhalt	Kar.	
			CRLDistributionPoints {2 5 29 31}	URL für CRL-Statusdienst	1	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	keine Festlegung	0-1	FALSE
			AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
			Admission {1 3 36 8 3 3}	professionItem = <oid_vpnz_sis> professionOID = <oid_vpnz_sis>	1 1	FALSE
			ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth keyPurposeId = id-kp-serverAuth	1 1	FALSE
			andere Erweiterungen		0	
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4360]		
	signature			Wert der Signatur		

5.7.3.3 VPN-Zugangsdienst – Verwendung mehrerer Schlüsselpaare

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

GS-A_4728 Verwendung von zwei Schlüsselpaaren im VPN-Zugangsdienst

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

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

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

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

5.8 ZD - Zentrale Dienste

5.8.1 Definition der Identität der Zentralen Dienste

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

5.8.2 Aufbau des SubjectDN

Der *SubjectDN* (*subject distinguishedName*) des Zertifikats verbindet den Dienste-FQDN mit der Identität des Anbieters:

- **`commonName = [FQDN des Dienstes]`**
- **`serialNumber = [Instanz-Nr des Dienstes]`**
- **`organizationName = [Name Diensteanbieter]`**
- **`countryName = [Herkunftsland Diensteanbieter]`**

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

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

5.8.3 X.509 Zertifikatsprofile der Zentralen Dienste

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

⌦ GS-A_4615 Umsetzung Zertifikatsprofil C.ZD.TLS-S

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

Tabelle 35: Tab_PKI_247 C.ZD.TLS-S Server-Authentisierung Zentrale Dienste

Element			Inhalt	Kar.	
certificate			C.ZD.TLS-S		
	tbsCertificate				
		version	2 (v3)		
		serialNumber	gemäß [RFC5280#4.1.2.2.]		
		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
		issuer	DN der ausstellenden CA		
		validity	Gültigkeit des Zertifikats (von – bis)		
		subject			
		commonName	FQDN des Dienstes gemäß Zuweisung	1	
		serialNumber	bei Bedarf zur Unterscheidung gleichartiger Instanzen	0-1	
		organizationName	Name des verantwortlichen Anbieters	1	
		countryName	DE	1	
		andere Attribute		0	
		subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels		

Element			Inhalt	Kar.	
			des Zertifikatsinhabers		
		extensions			**critical**
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Zentralen Dienstes	1	FALSE
		KeyUsage {2 5 29 15}	digitalSignature keyEncipherment	1 1	**TRUE**
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie policyIdentifier = <oid_zd_tls_s>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = Beschreibung der technischen Rolle gemäß [gemSpec_OID#GS-A_4446] professionOID = OID der technischen Rolle gemäß [gemSpec_OID#GS-A_4446]	1	FALSE
		ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-serverAuth	1	FALSE
		andere Erweiterungen		0	
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	signature		Wert der Signatur		

5.9 FD – Fachanwendungsspezifische Dienste

5.9.1 Definition der Identität der Fachanwendungsspezifischen Dienste

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

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

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

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

Anbieter von zentralen und fachanwendungsspezifischen Diensten in der TI MÜSSEN bei der Beantragung von X.509-Zertifikaten für den FQDN im

SubjectDN ausschließlich Werte aus dem im Rahmen ihrer Anbieterzulassung zugewiesenen Domainnamen aus dem Namensraum der TI verwenden.⌫

5.9.2 Aufbau des SubjectDN

Der *SubjectDN* (*subject distinguishedName*) des Zertifikats verbindet den Dienste-FQDN mit der Identität des Anbieters:

- **commonName = [FQDN des Dienstes]**
- **serialNumber = [Instanz-Nr des Dienstes]**
- **organizationName = [Name Diensteanbieter]**
- **countryName = [Herkunftsland Diensteanbieter]**

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

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

5.9.3 X.509 Zertifikatsprofile der Fachanwendungsspezifischen Dienste

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

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

Der TSP-X.509 nonQES MUSS C.FD.TLS-C gemäß Tab_PKI_249 umsetzen.⌫

Tabelle 36: Tab_PKI_249 C.FD.TLS-C Client-Authentisierung Fachanwendungsspezifische Dienste

Element			Inhalt	Kar.	
certificate			C.FD.TLS-C		
	tbsCertificate				
		version	2 (v3)		
		serialNumber	gemäß [RFC5280#4.1.2.2.]		
		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
		issuer	DN der ausstellenden CA		
		validity	Gültigkeit des Zertifikats (von – bis)		
		subject			
		commonName	FQDN des Dienstes gemäß Zuweisung	1	
		serialNumber	bei Bedarf zur Unterscheidung gleichartiger Instanzen	0-1	
		organizationName	Name des verantwortlichen Anbieters	1	
		countryName	DE	1	

Element			Inhalt	Kar.	
		andere Attribute		0	
	subjectPublicKeyInfo		Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
	extensions				**critical**
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Fachanwendungsspezifischen Dienstes	1	FALSE
		KeyUsage {2 5 29 15}	digitalSignature keyEncipherment	1 1	**TRUE**
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie policyIdentifier = <oid_fd_tls_c>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = Beschreibung der technischen Rolle gemäß [gemSpec_OID#GS-A_4446] professionOID = OID der technischen Rolle gemäß [gemSpec_OID#GS-A_4446]	1	FALSE
		ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth	1	FALSE
		andere Erweiterungen		0	
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	signature		Wert der Signatur		

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

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

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

Tabelle 37: Tab_PKI_250 C.FD.TLS-S Server-Authentisierung Fachanwendungsspezifische Dienste

Element			Inhalt	Kar.	
certificate			C.FD.TLS-S		
	tbsCertificate				
		version	2 (v3)		
		serialNumber	gemäß [RFC5280#4.1.2.2.]		

Element			Inhalt	Kar.	
	signature		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	issuer		DN der ausstellenden CA		
	validity		Gültigkeit des Zertifikats (von – bis)		
	subject				
		commonName	FQDN des Dienstes gemäß Zuweisung	1	
		serialNumber	bei Bedarf zur Unterscheidung gleichartiger Instanzen	0-1	
		organizationName	Name des verantwortlichen Anbieters	1	
		countryName	DE	1	
		andere Attribute		0	
	subjectPublicKeyInfo		Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
	extensions				**critical**
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Fachanwendungsspezifischen Dienstes	1	FALSE
		KeyUsage {2 5 29 15}	digitalSignature keyEncipherment	1 1	**TRUE**
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie policyIdentifier = <oid_fd_tls_s>	1 0-1 1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = Beschreibung der technischen Rolle gemäß [gemSpec_OID#GS-A_4446] professionOID = OID der technischen Rolle gemäß [gemSpec_OID#GS-A_4446]	1	FALSE
		ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-serverAuth	1	FALSE
		andere Erweiterungen		0	
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
	signature		Wert der Signatur		

5.10 CM – Clientmodul

5.10.1 Definition der Identität eines Clientmoduls

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

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

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

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

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

5.10.2 Aufbau des SubjectDN

Der *SubjectDN* (*subject distinguishedName*) des Zertifikats verbindet das Clientmodul mit der Identität des Fachanwendungsspezifischen Dienstes und des Anbieters:

- **`commonName = [Name des Clientmoduls]`**
- **`serialNumber = [Release- oder Instanz-Nr]`**
- **`organizationName = [Name Diensteanbieter]`**
- **`countryName = [Herkunftsland Diensteanbieter]`**

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

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

5.10.3 X.509 Zertifikatsprofil des Clientmoduls

5.10.3.1 C.CM.TLS-CS Clientmodul-Authentisierung

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

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

Tabelle 38: Tab_PKI_267 C.CM.TLS-CS Clientmodul-Authentisierung

Element			Inhalt	Kar.	
certificate			C.CM.TLS-CS		
	tbsCertificate				
		version	2 (v3)		
		serialNumber	gemäß [RFC5280#4.1.2.2.]		
		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
		issuer	DN der ausstellenden CA		
		validity	Gültigkeit des Zertifikats (von – bis)		
		subject			
		commonName	keine Festlegung	1	
		serialNumber	bei Bedarf zur Unterscheidung gleichartiger Instanzen (z.B. Release-Nr.)	0-1	
		organizationName	Name des verantwortlichen Anbieters	1	
		countryName	DE	1	
		andere Attribute		0	
		subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
		extensions			**critical**
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Clientmoduls	1	FALSE
		KeyUsage {2 5 29 15}	digitalSignature keyEncipherment	1 1	**TRUE**
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_cm_tls_c>	1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	keine Festlegung	0-1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}	professionItem = Beschreibung der technischen Rolle gemäß [gemSpec_OID#GS-A_4446] professionOID = OID der technischen Rolle gemäß [gemSpec_OID#GS-A_4446]	1	FALSE
		ExtendedKeyUsage {2 5 29 37}	keyPurposeId = id-kp-clientAuth keyPurposeId = id-kp-serverAuth	1	FALSE
		andere Erweiterungen		0	
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		

Element		Inhalt	Kar.	
	signature	Wert der Signatur		

5.11 CA - Zertifikatsprofile

GS-A_4730 Eindeutige Identifizierung der CA-Zertifikate

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

GS-A_4731 Attribute der CA-Zertifikate

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

GS-A_4732 Extension der CA-Zertifikate

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

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

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

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

Der Suffix <n> kennzeichnet hierbei die fortlaufende Generation innerhalb eines Typs von CA-Zertifikaten – beginnend ab dem Wert 1.

GS-A_4735 Namenskonvention für CA-Zertifikate

Der TSP-X.509 nonQES und TSP-X.509 QES MUSS für jede von ihm betriebene CA die Namenskonventionen gemäß [GS-A_4588], [GS-A_4589], [GS-A_4590] umsetzen sowie die Namensbildung im Feld commonName nach dem Schema <holder>.<usage>-CA<n> vornehmen.⌫

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

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

Die gematik-Root-CA MUSS die Namenskonvention und Attributsbelegung der Felder für folgende CA-Zertifikate umsetzen gemäß:
a) Tab_PKI_211 für gematik-Root-CA,
b) Tab_PKI_212 für i) Zentrale Aussteller-CA_nonQES, ii) Aussteller-CA_nonQES, iii) OCSP-Signer-CA, iv) CRL-Signer-CA, v) TSL-Signer-CA. ⌫

Tabelle 39: Tab_PKI_211 GEM.R-CA<n> – Zentrale gematik Root-CA_nonQES der TI

Element			Inhalt	Kar.	
certificate			C.GEM.RCA<n>		
	tbsCertificate				
		version	2 (v3)		
		CertificateSerialNumber	gemäß [RFC5280#4.1.2.2]		
		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
		issuer	DN der ausstellenden CA		
		validity	Gültigkeit des Zertifikats (von - bis)		
		subject			
			commonName	GEM.RCA<n>	1	
			serialNumber	Zur Unterscheidung gleichartiger Instanzen	0-1	
			organizationName	gematik GmbH	1	
			organizationalUnitName	Zentrale Root-CA der Telematikinfrastruktur	1	
			countryName	DE	1	
			andere Attribute		0	
		subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4357] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
		extensions			**critical**
			SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels der Zentralen gematik Root-CA, für die dieses Zertifikat ausgestellt wird.	1	FALSE
			KeyUsage {2 5 29 15}	keyCertSign crlSign	1 0-1	**TRUE**
			SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	FALSE
			BasicConstraints {2 5 29 19}	ca = TRUE pathLength	1 0	**TRUE**
			CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie	1 0-1	FALSE
			CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
			AuthorityKeyIdentifier {2 5 29 35}		0	FALSE
			Admission {1 3 36 8 3 3}		0	FALSE
			ExtendedKeyUsage {2 5 29 37}		0	FALSE
			andere Erweiterungen		0	
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus			

Element		Inhalt	Kar.	
		gemäß [gemSpec_Krypt#GS-A_4357]		
	signature	Wert der Signatur		

5.11.2 <tsp>.<usage>-CA<n> - Aussteller-CAs_nonQES

GS-A_4737 Umsetzung Zentrale nonQES-CA-Zertifikate

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

Tabelle 40: Tab_PKI_212 <tsp>.<usage>-CA<n> –Aussteller- CA_nonQES der TI

Element			Inhalt	Kar.	
certificate			C.<tsp>.<usage>-CA<n>		
	tbsCertificate				
		version	2 (v3)		
		CertificateSerialNumber	gemäß [RFC5280#4.1.2.2]		
		signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
		issuer	DN der ausstellenden CA		
		validity	Gültigkeit des Zertifikats (von - bis)		
		subject			
		commonName	<tsp>.<usage>-CA<n> *)	1	
		serialNumber	Zur Unterscheidung gleichartiger Instanzen	0-1	
		organizationName	<tspName> *)	1	
		organizationalUnitName	<usageName>-CA der Telematikinfrastruktur	1	
		countryName	DE	1	
		andere Attribute		0	
		subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4357] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
		extensions			**critical**
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels der CA, für die dieses Zertifikat ausgestellt wird	1	FALSE
		KeyUsage {2 5 29 15}	keyCertSign crlSign	1 0-1	**TRUE**
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = TRUE pathLength = 0	1 1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> davon abweichend: CAs für HBA-AUT/ENC-Zertifikate: policyIdentifier = <oid_policy_hba_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie	1 0-1	FALSE

Element				Inhalt	Kar.	
			CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
			AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
			Admission {1 3 36 8 3 3}		0	FALSE
			ExtendedKeyUsage {2 5 29 37}		0	FALSE
			andere Erweiterungen		0	
	signatureAlgorithm			zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
	signature			Wert der Signatur		

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

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

Neben dem Bezug von nonQES-Zertifikaten aus der zentralen PKI der TI besteht für TSP alternativ die Möglichkeit, von der gematik Root-CA abgeleitete Sub-CAs selbst zu betreiben. Die CA-Zertifikate dieser Sub-CAs unterscheiden sich durch das Schlüsselpaar sowie durch den Namen des Zertifikatherausgebers im Feld organizationName.

GS-A_4902 Umsetzung nonQES-CA-Zertifikate

Der TSP-X.509 nonQES MUSS für die von ihm betriebenen CAs die Attributsbelegung der Felder gemäß Tab_PKI_212 umsetzen (wobei das Attribut ***organizationName*** den Namen des TSP-X.509 nonQES enthält) und die Namenskonvention gemäß Tab_PKI_213 umsetzen.

5.11.4 <tsp>.<usage>-QCA<n> - Aussteller-CA_QES

GS-A_4948 Umsetzung QES-CA-Zertifikate

Der TSP-X.509 QES MUSS für die von ihm betriebenen CAs die Attributsbelegung der Felder gemäß Tab_PKI_215 und die Namenskonvention gemäß Tab_PKI_213 umsetzen.

Tabelle 41: Tab_PKI_215 <tsp>.<usage>-qCA<n> – Aussteller- CA_QES der TI

Element			Inhalt	Kar.	
certificate			C.<tsp>.<usage>-qCA<n>		
	tbsCertificate				
		version	2 (v3)		
		CertificateSerialNumber	gemäß [RFC5280#4.1.2.2]		
		signature	zur Signatur des Zertifikats verwendeter		

Element			Inhalt	Kar.	
			Algorithmus gemäß [gemSpec_Krypt#GS-A_4358]		
		issuer	DN der BNetzA Root-CA		
		validity	Gültigkeit des Zertifikats (von - bis)		
		subject			
		commonName	<tsp>.<usage>-qCA<n>:PN	1	
		organizationName	Name des ZDA	1	
		organizationalUnitName	HBA-qCA – TI der Gesundheitskarte mit Anbieterakkreditierung	1	
		countryName	DE	1	
		andere Attribute		0	
		subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4358] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
		extensions			**critical**
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels der CA, für die dieses Zertifikat ausgestellt wird	1	FALSE
		KeyUsage {2 5 29 15}	keyCertSign crlSign	1 0-1	**TRUE**
		SubjectAltNames {2 5 29 17}		0	FALSE
		BasicConstraints {2 5 29 19}	ca = TRUE pathLength = 0	1 1	**TRUE**
		CertificatePolicies {2 5 29 32}	[1]Zertifikatsrichtlinie: Richtlinienkennung=id-commonpki-cp-accredited policyQualifierInfo = URL der Zertifikatsrichtlinie	1 0-1	FALSE
		CRLDistributionPoints {2 5 29 31}	CDP der BNetzA	1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		Admission {1 3 36 8 3 3}		0	FALSE
		ExtendedKeyUsage {2 5 29 37}		0	FALSE
		QCStatements {1.3.6.1.5.5.7.1.3}	id-etsi-qcs-QcCompliance = 0.4.0.1862.1.1	1	FALSE
		andere Erweiterungen	Ggf. weitere Erweiterungen durch die BNetzA gesetzt, die hier jedoch nicht spezifiziert sind.		
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4358]		
	signature		Wert der Signatur		

5.12 OCSP - Statusauskunftsdienst

5.12.1 Definition der OCSP-Signer-Identität

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

GS-A_4738 Eindeutige Identifizierung der OCSP-Signer-Zertifikate

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

GS-A_4739 Attribute der OCSP-Signer-Zertifikate

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

GS-A_4921 Ableitung des OCSP-Signer-Zertifikates

Ein TSP-X.509 nonQES und der Anbieter des TSL-Dienstes MÜSSEN das OCSP-Signer-Zertifikat für die von ihnen betriebenen OCSP-Dienste aus einer OCSP-Signer-CA beziehen, die von der gematik Root-CA abgeleitet ist.

5.12.2 Aufbau des SubjectDN

Der *SubjectDN* (*subject distinguishedName*) des Zertifikats wird gebildet wie folgt:

- **commonName = [eindeutiger Name des OCSP-Dienstes]**
- **serialNumber = [Instanz-Nr des OCSP-Dienstes]**
- **organizationName = [Name des OCSP-Diensteanbieters]**
- **countryName = [Herkunftsland des zugehörigen OCSP-Diensteanbieters, DE]**

5.12.3 X.509 Zertifikatsprofil der OCSP-Signer-CA

GS-A_4740 Zentrale OCSP-Signer-CA-Zertifikate

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

5.12.4 X.509 Profil des OCSP-Signer-Zertifikates

5.12.4.1 C.GEM.OCSP OCSP-Signer-Zertifikat

GS-A_4741 Umsetzung Zertifikatsprofil C.GEM.OCSP

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

Tabelle 42: Tab_PKI_253 C.GEM.OCSP Zertifikatsprofil OCSP-Signer

Element	Inhalt	Kar.	
certificate	C.GEM.OCSP		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
issuer	DN der ausstellenden CA		
validity	Gültigkeit des Zertifikats (von – bis)		
subject			
commonName	Name des OCSP-Responders	1	
serialNumber	Zur Unterscheidung gleichartiger Instanzen	0-1	
organizationName	Name des OCSP-Dienstanbieters	1	
organizationalUnitName	Name der Abteilung für den Betrieb des OCSP	0-1	
countryName	Land der Anschrift des OCSP-Dienstanbieters	1	
andere Attribute		0	
subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4357] und individueller Wert des öffentlichen Schlüssels des Zertifikatsbesitzers		
extensions			**critical**
SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des OCSP-Signers	1	FALSE
KeyUsage {2 5 29 15}	nonRepudiation	1	**TRUE**
SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	FALSE
BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie	1 0-1	FALSE
CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
ExtendedKeyUsage {2 5 29 37}	KeyPurposeId = id-kp-OCSPSigning	1	FALSE
id-pkix-ocsp-nocheck {1.3.6.1.5.5.7.48.1.5}	OCSP-Nocheck = NULL	0-1	FALSE
andere Erweiterungen		0	

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

5.13 CRL – Statusauskunftsdienst

⌦ **GS-A_5066 CRL gemäß [Common-PKI]**

Der TSP-X.509 nonQES MUSS CRLs für X.509-Zertifikate gemäß [Common-PKI] erzeugen. ⌫

5.13.1 Definition der CRL-Signer-Identität

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

⌦ **GS-A_4935 Eindeutige Identifizierung der CRL-Signer-Zertifikate**

Der TSP-X.509 nonQES MUSS bei der Beantragung von X.509-CRL-Signer-Zertifikaten sicherstellen, dass der subjectDN das CRL-Signer-Zertifikat eindeutig innerhalb der TI identifiziert.⌫

⌦ **GS-A_4936 Attribute der CRL-Signer-Zertifikate**

Der TSP-X.509 nonQES SOLL bei der Beantragung von X.509-CRL-Signer-Zertifikaten nur die Attribute mit der Kardinalität 1 verwenden. ⌫

⌦ **GS-A_4937 Ableitung des CRL-Signer-Zertifikates**

Ein TSP-X.509 nonQES MUSS das CRL-Signer-Zertifikat für die von ihm betriebenen CRL-Dienste aus einer CRL-Signer-CA beziehen, die von der gematik Root-CA abgeleitet ist.⌫

5.13.2 Aufbau des SubjectDN

Der *SubjectDN* (*subject distinguishedName*) des Zertifikats wird gebildet wie folgt:

- **`commonName = [eindeutiger Name des CRL-Dienstes]`**
- **`serialNumber = [Instanz-Nr des CRL-Dienstes]`**
- **`organizationName = [Name des CRL-Diensteanbieters]`**
- **`countryName = [Herkunftsland des zugehörigen CRL-Diensteanbieters, DE]`**

5.13.3 X.509 Zertifikatsprofil der CRL-Signer-CA

⌦ **GS-A_4938 Zentrale CRL-Signer-CA-Zertifikate**

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

5.13.4 X.509 Profil des CRL-Signer-Zertifikates

5.13.4.1 C.GEM.CRL CRL-Signaturzertifikat

⌦ GS-A_4939 Umsetzung Zertifikatsprofil C.GEM.CRL

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

Tabelle 43: Tab_PKI_214 C.GEM.CRL Zertifikatsprofil CRL-Signer

Element			Inhalt	Kar.	
certificate			C.GEM.CRL		
tbsCertificate					
	version		2 (v3)		
	serialNumber		gemäß [RFC5280#4.1.2.2.]		
	signature		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
	issuer		DN der ausstellenden CA		
	validity		Gültigkeit des Zertifikats (von – bis)		
	subject				
		commonName	Name des CRL-Signers	1	
		serialNumber	Zur Unterscheidung gleichartiger Instanzen	0-1	
		organizationName	Name des CRL-Dienstanbieters	1	
		organizationalUnitName	Name der Abteilung für den Betrieb des CRL-Signer	0-1	
		countryName	Land der Anschrift des CRL-Dienstanbieters	1	
		andere Attribute		0	
	subjectPublicKeyInfo		Algorithmus gemäß [gemSpec_Krypt#GS-A_4357] und individueller Wert des öffentlichen Schlüssels des Zertifikatsbesitzers		
	extensions				**critical**
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des CRL-Signers	1	FALSE
		KeyUsage {2 5 29 15}	crlSign	1	**TRUE**
		SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	FALSE
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = URL der Zertifikatsrichtlinie	1 0-1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE

Element			Inhalt	Kar.	
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	keine Festlegung	0-1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		ExtendedKeyUsage {2 5 29 37}		0	FALSE
		andere Erweiterungen		0	
	signatureAlgorithm		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
	signature		Wert der Signatur		

5.14 TSL - Zertifikatsprofile

5.14.1 Definition der TSL-Signer-Identität

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

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

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

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

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

5.14.2 Aufbau des SubjectDN

Der *SubjectDN* (*subject distinguishedName*) des Zertifikats wird gebildet wie folgt:

- commonName = [eindeutiger Name des TSL-Signers]
- serialNumber = [Instanz-Nr des TSL-Dienstes]
- organizationName = [Name des TSL-Diensteanbieters]
- countryName = [Herkunftsland des zugehörigen TSL-Diensteanbieters, DE]

5.14.3 X.509 Zertifikatsprofil der TSL-Signer-CA

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

Der Anbieter des TSL-Dienstes MUSS für die von ihm betriebenen TSL-Signer-CAs die Attributsbelegung der Felder gemäß Tab_PKI_212 und die Namenskonvention für den TSL-Dienst gemäß Tab_PKI_213 umsetzen.⌫

5.14.4 TSL-Signer- Zertifikat

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

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

Tabelle 44: Tab_PKI_252 C.TSL.SIG Zertifikatsprofil TSL-Signer

Element			Inhalt	Kar.	
certificate			C.TSL.SIG		
tbsCertificate					
	version		2 (v3)		
	serialNumber		gemäß [RFC5280#4.1.2.2.]		
	signature		zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4357]		
	issuer		DN der ausstellenden CA		
	validity		Gültigkeit des Zertifikats (von – bis)		
	subject				
		commonName	TSL Signing Unit <n>	1	
		serialNumber	Zur Unterscheidung gleichartiger Instanzen	0-1	
		organizationName	Name des Anbieters TSL-Dienst	1	
		organizationalUnitName	Name der Abteilung für den Betrieb des TSL-Dienstes	0-1	
		countryName	Land der Anschrift des TSP	1	
		andere Attribute		0	
	subjectPublicKeyInfo		Algorithmus gemäß [gemSpec_Krypt#GS-A_4357] und individueller Wert des öffentlichen Schlüssels des Zertifikatsbesitzers		
	extensions				**critical**
		SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des TSL-Signers	1	FALSE
		KeyUsage {2 5 29 15}	nonRepudiation	1	**TRUE**
		BasicConstraints {2 5 29 19}	ca = FALSE	1	**TRUE**
		CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_tsl_signer>	1	FALSE
		CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
		AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
		AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
		ExtendedKeyUsage {2 5 29 37}	KeyPurposeId = id-tsl-kptslSigning gemäß [ETSI_TS_102_231_v3.1.2#6.2]	1	FALSE
		andere Erweiterungen		0	

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

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

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

5.14.5 TSL-OCSP-Responder-Zertifikat

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

Der Anbieter des TSL-Dienstes MUSS für die OCSP-Prüfung des TSL-Signer-Zertifikats ein OCSP-Signer-Zertifikat C.GEM.OCSP gemäß Tab_PKI_253 umsetzen.⌫

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

Der Anbieter des TSL-Dienstes MUSS das OCSP-Signer-Zertifikat aus der zentral in der TI bereitgestellten OCSP-Signer-CA beziehen.⌫

6 CV-Zertifikate

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

Die CV-Zertifikate kann ein Kartenherausgeber dabei entweder aus einer eigenen – von der gematik Root-CA abgeleiteten CVC-CA erstellen oder diese von der zentralen PKI der TI als Zulieferung beziehen.

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

Ein Kartenherausgeber KANN das nicht-personenbezogene CV-Zertifikat nach entsprechender Registrierung vom TSP-CVC-CA beziehen.⌫

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

Der Kartenherausgeber MUSS sicherstellen, dass alle zu einer Chipkarte gehörenden CV-Zertifikate durch dieselbe CA der zweiten Ebene erzeugt werden.⌫

6.1 Festlegungen zur Abgrenzung

Grundsätzlich sind CV-Zertifikatsprofile zu unterscheiden für

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

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

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

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

6.2 Namensregeln und -formate

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

Der Herausgeber eines CV-Zertifikats wird über das Datenelement Certificate Authority Reference (CAR) identifiziert. Anforderungen an die Formatierung und den Inhalt der CAR sind im Abschnitt 6.4.1.2 beschrieben.

Der Inhaber eines CV-Zertifikats wird im Datenelement Certificate Holder Reference (CHR) angegeben. Anforderungen an die Formatierung und den Inhalt der CHR sind im Abschnitt 6.4.1.3 beschrieben.

6.3 Rollen und Profile

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

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

Die technische Umsetzung der Zuordnung zu Profilen in CV-Zertifikaten erfolgt für Karten der Generation 1 anders als für Karten der Generation 2:

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

6.3.1 Rollenauthentisierung

⌦ **GS-A_4620 Zugriffsprofil einer eGK**

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

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

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

In der folgenden Tabelle werden die Zugriffsprofile im Kontext der sie nutzenden fachlichen Akteure dargestellt. Der Kern der Tabelle wurde mit den LEOs, Kostenträgern und dem BMG abgestimmt. Sie bilden die Basis für die Rechtezuweisung auf den Smartcards der Generation 1 und der Generation 2.

Die Tabelle enthält auch, welche Organisation als sog. „Qualifizierende Stelle“ die Berechtigung für die Zugriffsprofile in CV-Zertifikaten vergibt und damit die Betreiber von

CVC-CAs der zweiten Ebene autorisiert, diese Profile in die CV-Zertifikate einzubringen. Im Rahmen ihrer Zulassung bei der gematik müssen diese Betreiber den Nachweis der Qualifizierung erbringen. Für derzeit nicht verwendete Profile ist diese Zuordnung offen.

Es werden die Zugriffsprofile 0 – 10 für eine Rollenauthentisierung unterschieden:

Tabelle 45: Tab_PKI_254 Zugriffsprofile für eine Rollenauthentisierung

Profile / Akteure / Rollen und OID aus gemSpec_PKI					X.509 Admission Extension	
Zugriffs-profil	**Kartentyp**	**Beschreibung fachlicher Akteur**	**Fachliche Rolle**	**Qualifizierende Stelle**	**professionItem**	**OID-Referenz**
0						
CHA.0	eGK	Versicherter	Versicherter	keine Qualifizierung	Versicherte/-r	oid_versicherter
1						
CHA.1	SMC–B eKiosk	eKiosk	Versicherter	Nicht definiert	Nicht definiert	Nicht definiert
2						
CHA.2A	HBA – Arzt	Arzt in einer Institution (z. B. eigene Praxis, Gemeinschaftspraxis, Krankenhaus).	Arzt	BÄK	Ärztin/Arzt	oid_arzt
CHA.2ZA	HBA – Zahnarzt	Zahnarzt in einer Institution	Zahnarzt	BZÄK	Zahnärztin/Zahnarzt	oid_zahnarzt
CHA.2A	(H)BA für Mitarbeiter(innen) in Arztpraxis, oder Krankenhaus	Mitarbeiter medizinische Institution (z. B. in Arztpraxis, Krankenhaus). Der „Mitarbeiter medizinische Institution" verkörpert gegenüber der TI die Institution des Arztes	Nicht definiert	Nicht definiert	Nicht definiert	Nicht definiert
CHA.2ZA	(H)BA für Mitarbeiter(innen) in Zahnarztpraxis	Mitarbeiter medizinische Institution (z. B. in Zahnarztpraxis). Der „Mitarbeiter medizinische Institution" verkörpert gegenüber der TI die Institution des Zahnarztes	Nicht definiert	Nicht definiert	Nicht definiert	Nicht definiert
CHA.2A	SMC-B	Mitarbeiter medizinische Institution Arztpraxis mit Autorisierung und Protokollierung gemäß § 291a Abs. 5 Satz 4 SGB V. Der „Mitarbeiter medizinische Institution" verkörpert gegenüber der TI die Institution des	Mitarbeiter Arzt	KV, KV-Telematik ARGE, KBV	Betriebsstätte Arzt	oid_praxis_arzt

Profile / Akteure / Rollen und OID aus gemSpec_PKI					X.509 Admission Extension	
Zugriffs-profil	**Kartentyp**	**Beschreibung fachlicher Akteur**	**Fachliche Rolle**	**Qualifizierende Stelle**	**professionItem**	**OID-Referenz**
		Arztes.				
CHA.2ZA	SMC-B	Mitarbeiter medizinische Institution Zahnarztpraxis mit Autorisierung und Protokollierung gemäß § 291a Abs. 5 Satz 4 SGB V. Der „Mitarbeiter medizinische Institution" verkörpert gegenüber der TI die Institution des Zahnarztes.	Mitarbeiter Zahnarzt	KZBV	Zahnarztpraxis	oid_zahnarztpraxis
CHA.2A	SMC-B	Mitarbeiter medizinische Institution Krankenhaus mit Autorisierung und Protokollierung gemäß § 291a Abs. 5 Satz 4 SGB V. Der „Mitarbeiter medizinische Institution" verkörpert gegenüber der TI die Institution des Arztes.	Mitarbeiter Krankenhaus	DKTIG	Krankenhaus	oid_krankenhaus
3						
CHA.3	HBA – Apotheker	Apotheker in einer öffentlichen Apotheke oder einer Krankenhausapotheke, jeweils mit Sitz in Deutschland.	Apotheker	BAK	Apotheker/in	oid_apotheker
CHA.3	(H)BA für Mitarbeiter(-innen) der Apotheke	Mitarbeiter Apotheke als berufsmäßiger Gehilfe oder Person, die zur Vorbereitung auf den Beruf tätig ist, gemäß § 291a Abs. 4 [SGB V]. Der „Mitarbeiter Apotheke" verkörpert gegenüber der TI die Institution des Apothekers.	Apotheker	BAK	Apotheker-assistent/in Pharmazie-ingenieur/in Apotheken-assistent/-in	oid_apothekerassisten oid_pharmazieingenieur oid_apothekenassistent
CHA.3	SMC–B	Mitarbeiter Apotheke mit Autorisierung und Protokollierung gemäß § 291a Abs.5 Satz4 SGB V. Der „Mitarbeiter Apotheke" verkörpert gegenüber der TI die Institution des Apothekers.	Mitarbeiter Apotheke	BAK	Öffentliche Apotheke Krankenhausapotheke Bundeswehrapotheke Pharmazeutische/-r Assistent/-in	oid_öffentliche_apotheke oid_krankenhausapotheke oid_bundeswehrapotheke oid_pharm_assisten

Profile / Akteure / Rollen und OID aus gemSpec_PKI					X.509 Admission Extension	
Zugriffs-profil	**Kartentyp**	**Beschreibung fachlicher Akteur**	**Fachliche Rolle**	**Qualifizierende Stelle**	**professionItem**	**OID-Referenz**
						t
					Pharmazeutisch-technische/-r Assistent/-in	oid_pharm_techn_assistent
					pharmazeutisch-kaufmännische/-r Angestellte	oid_pharm_kaufm_angestellter
					Pharmaziepraktikant/-in	oid_pharmazieprakti kant
					Apothekenhelfer/-in	oid_apothekenhelfer
					Apothekenfach-arbeiter/-in	oid_apothekenfacharbeiter
					Stud.pharm. oder Famulant/-in	oid_famulant
					PTA-Praktikant/-in	oid_pta_praktikant
					PKA Auszubildende/-r	oid_pka_auszubildender
4						
CHA.4	HBA – Psychotherapeut	Psychologischer Psychotherapeut, Kinder- und Jugendlichenpsychotherapeut (Für ärztliche Psychotherapeuten gelten im Kontext der Fachanwendungen der eGK die gleichen Ausführungen wie für den Akteur „Arzt“.)	Psychotherapeut	BPTK	Psychotherapeut/ in	oid_psychotherapeut
					Psychologische/r Psychotherapeut/ in	oid_ps_psychotherapeut
					Kinder und Jugendlichen Psychotherapeut/ in	oid_kuj_psychotherapeut
CHA.4	SMC–B	Institutionskarte eines Psychotherapeuten.	Mitarbeiter Arzt	KV-Telematik ARGE	Betriebsstätte Psychotherapeut	oid_praxis_psychotherapeut
5						

Profile / Akteure / Rollen und OID aus gemSpec_PKI					X.509 Admission Extension	
Zugriffs-profil	**Kartentyp**	**Beschreibung fachlicher Akteur**	**Fachliche Rolle**	**Qualifizierende Stelle**	**professionItem**	**OID-Referenz**
CHA.5	(H)BA sonstige Leistungserbringer	Heilmittelerbringer mit (H)BA Hilfsmittelerbringer mit BA	Sonstige Leistungserbringer	Nicht definiert	Nicht definiert	Nicht definiert
6						
CHA.6	SMC	Kein fachlicher Akteur - wird nicht verwendet	Nicht definiert	Nicht definiert	Nicht definiert	Nicht definiert
7						
CHA.7	(H)BA	Rettungsassistent Bei den Akteuren handelt es sich um „Angehörige eines anderen Heilberufs, die für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung“ (§ 291a Abs. 4 Satz 1 Nr. 2e) absolviert haben.	Anderer Heilberuf	Nicht definiert	Rettungsassistent/-in	oid_rettungsassistert
CHA.7	SMC-B	Mobile Einrichtung Rettungsdienst	Nicht definiert	Nicht definiert	Betriebsstätte Mobile Einrichtung Rettungsdienst	oid_mobile_einrichtung_rettungsdienst
8						
CHA.8	SMC-B (ohne Zugriff auf med. Daten)	Mitarbeiter von Gesundheitseinrichtungen ohne eigenen HBA oder BA	Mitarbeiter Medizinische Institution	Nicht definiert	Nicht definiert	Nicht definiert
CHA.8		Mitarbeiter von Krankenkassen	Mitarbeiter Kostenträger	Nicht definiert	Nicht definiert	oid_kostenträger
CHA.8		Verifikationskarten Kostenträger	Mitarbeiter Kostenträger	GKV-SV	Betriebsstätte Kostenträger	oid_kostenträger
9						
CHA.9	SMC-B (mit Zugriff auf med. Daten)	a) Mitarbeiter von Gesundheitseinrichtungen ohne eigenen HBA oder BA	a) Mitarbeiter Medizinische Institution	Nicht definiert	Nicht definiert	Nicht definiert
CHA.9		b) ohne zugeordneten Akteur, sichere Einsatzumgebung für Versicherten	b) Versicherter	Nicht definiert	Nicht definiert	Nicht definiert

Profile / Akteure / Rollen und OID aus gemSpec_PKI					X.509 Admission Extension	
Zugriffs-profil	**Kartentyp**	**Beschreibung fachlicher Akteur**	**Fachliche Rolle**	**Qualifizierende Stelle**	**professionItem**	**OID-Referenz**
10						
CHA.10	SMC-B UzWdRdV	Versicherter in der „Umgebung zur Wahrnehmung der Rechte des Versicherten" (UzWdRdV) im Kontrollbereich eines Leistungserbringers	Versicherter	Nicht definiert	Nicht definiert	Nicht definiert
51		Funktionseinheit				
CHA.51	SMC-B UzWdRdV	Signaturanwendungskomponente (SAK)	N.A.	N.A.	N.A.	N.A.
52		Funktionseinheit				
CHA.52	Nicht definiert	Nicht definiert	N.A.	N.A.	N.A.	N.A.
53		Funktionseinheit				
CHA.53	HBA	Stapelfähige SSEE und Remote-PIN-Empfänger	N.A.	N.A.	N.A.	N.A.
54		Funktionseinheit				
CHA.54	SM-B/gSMC-KT	Remote-PIN-Sender	N.A.	N.A.	N.A.	N.A.
55		Funktionseinheit				
CHA.55	SMC-B	Remote-PIN-Empfänger	N.A.	N.A.	N.A.	N.A.

6.3.2 Authentisierung einer Funktionseinheit

Es werden die Zugriffsprofile 51, 53 – 55 für eine Authentisierung einer Funktionseinheit unterschieden:

Tabelle 46: Tab_PKI_255 Zugriffsprofile für eine Authentisierung einer Funktionseinheit

Zugriffsprofil	Kodierung	CV-Zertifikate für	Funktionseinheit
51	'33'	gSMC-K	Signaturanwendungskomponente (SAK)
53	'35'	HBA	Stapelfähige SSEE und Remote-PIN-Empfänger
54	'36'	gSMC-KT	Remote-PIN-Sender
55	'37'	SM-B	Remote-PIN-Empfänger

Hinweis: Das Zugriffsprofil 52 ('34') wurde für die SMC-RFID vorgesehen, diese wird derzeit nicht verwendet.

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

Der Kartenherausgeber MUSS sicherstellen, dass das CV-Gerätezertifikat einer gSMC-K als Zugriffsprofile den Wert ’33’ (G1) bzw. ’00 0000 0000 0001’ (G2) hat.⌫

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

Der Kartenherausgeber MUSS sicherstellen, dass das CV-Gerätezertifikat einer gSMC-KT als Zugriffsprofile den Wert ’36’ (G1) bzw. ’00 0000 0000 0002’ (G2) hat.⌫

⌦ **GS-A_4623 Zugriffsprofil eines HBA**

Der Kartenherausgeber MUSS sicherstellen, dass das CV-Gerätezertifikat eines HBA als Zugriffsprofile den Wert ’35’ (G1) bzw. ’00 0000 0000 000C’ (G2) hat.⌫

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

Der Kartenherausgeber MUSS sicherstellen, dass das CV-Gerätezertifikat einer SM-B als Zugriffsprofil den Wert '37' (G1) bzw. ’00 0000 0000 0004’ (G2) hat.⌫

6.4 Aufbau und Bestandteile eines CV-Zertifikats der Generation 1

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

6.4.1 Bestandteile eines CV-Zertifikats

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

6.4.1.1 Certificate Profile Identifier (CPI)

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

Tabelle 47: Tab_PKI_256 Mögliche Werte für CPI

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

⌦ **GS-A_4625 CPI für CV-Zertifikate einer CVC-CA**

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

GS-A_4626 CPI für CV-Zertifikate einer Karte

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

6.4.1.2 Certification Authority Reference (CAR)

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

Tabelle 48: Tab_PKI_257 Aufbau CAR für Karten der Generation 1

	CA Name	Service-Indikator	CA-spezifische Information	Algorithmen-referenz	Datum
Länge	5 Byte	1 BCD	1 BCD	2 BCD	2 BCD
zugelassene Werte	CA Name gemäß Registrierung bei Fraunhofer SIT	Individuell belegbar	nicht festgelegt	individuell belegbar zur Unterscheidung div. PuK-Algortithmen	letzte 2 Ziffern des Jahres der CA-Schlüssel-erzeugung

GS-A_4627 Verwendung des Feldes Certificate Authority Reference

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

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

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

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

6.4.1.3 Certificate Holder Reference (CHR)

Die Certificate Holder Reference (CHR) wird dazu verwendet, dem im Zertifikat enthaltenen öffentlichen Schlüssel einen eindeutigen Identifier zuzuordnen. Bei dem Aufbau und der Belegung des Feldes CHR wird unterschieden zwischen einem CV-Zertifikat für eine CVC-CA und einem CV-Zertifikat für eine Chipkarte:

Tabelle 49: Tab_PKI_258 Aufbau CHR

CV-Zertifikat für	Länge CHR	Inhalt
CVC-CA	8 Bytes	CAR zu dem Schlüsselpaar
Chipkarte	12 Bytes	'xx xx' || ICCSN der Chipkarte

⌦ **GS-A_4629 CHR des CV-Zertifikats einer CVC-CA**

Die CVC-Root-CA MUSS als Wert für die CHR gemäß Tab_PKI_258 die CAR der CVC-CA zu dem Schlüsselpaar eintragen, für den das CV-Zertifikat erzeugt wird. ⌫

⌦ **GS-A_4630 CHR des CV-Zertifikats einer Chipkarte**

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

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

6.4.1.4 Certificate Holder Authorisation (CHA)

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

Tabelle 50: Tab_PKI_259 Aufbau CHA

AID	Zugriffsprofil

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

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

6.4.1.5 Object Identifier (OID)

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

Es werden nur folgende OID-Werte verwendet:

Tabelle 51: Tab_PKI_260 Object Identifier der Registration Authority TeleTrusT

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

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

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

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

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

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

6.4.1.6 Öffentlicher Schlüssel

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

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

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

6.4.2 Aufbau eines CV-Zertifikats

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

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

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

GS-A_4636 Aufbau eines CV-Zertifikats zur Authentisierung

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

Tabelle 52: Tab_PKI_261 CV-Zertifikat einer CVC-CA mit CPI = ´21´, SHA–256

Tag	L	Wert		
´7F21´	´820146´	CV–Zertifikat		(´0146´ = 326 Byte)
		Tag	L	Wert
		´5F37´	´820100´	Signatur SIG.CA (´0100´ = 256 Byte)
		´5F38´	´3E´	Non-Recoverable Part NRP (´003E´ = 62 Byte)

Tabelle 53: Tab_PKI_262 CV-Zertifikat zur Authentisierung mit CPI = ´22´, SHA–256

Tag	L	Wert		
´7F21´	´820150´	CV–Zertifikat		(´0150´ = 336 Byte)
		Tag	L	Wert
		´5F37´	´820100´	Signatur SIG.CA (´0100´ = 256 Byte)
		´5F38´	´48´	Non-Recoverable Part NRP (´0048´ = 72 Byte)

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

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

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

Tabelle 54: Tab_PKI_263 Informationen für ein CV-Zertifikat einer CVC-CA

Element	Länge	Wert	Erläuterung
CPI	1 Byte	´21´	CPI eines CV-Zertifikats einer CVC-CA
Modulus	256 Byte		Modulus des öffentlichen Schlüssels. Die Länge des Modulus muss 28 Byte kleiner als die zu signierende Nachricht M sein.
Exponent	4 Byte		Exponent des öffentlichen Schlüssels

Element		Länge	Wert	Erläuterung
OID		7 Byte	´2B24 0304 0202 04´	Es wird lediglich der OID {1.3.36.3.4.2.2.4} verwendet
CHR		8 Byte		CAR der CVC-CA für die das CV-Zertifikat ausgestellt wird
	CA-Name	5 Byte	DEXXX	CA-Name gemäß Registrierung bei Fraunhofer SIT
	Service-Indikator	1 BCD	Individuell belegbar	
	CA-spez. Info	1 BCD	Nicht festgelegt	
	Algorithmen-Referenz	2 BCD	Individuell belegbar	Ggf. Unterscheidung diverser PuK-Algorithmen
	Datum	2 BCD	Letzte zwei Ziffern des Jahres der Schlüsselaktivierung	
CAR		8 Byte		CAR der CVC-CA, die das CV-Zertifikat ausstellt
	CA-Name	5 Byte	DEXXX	CA-Name gemäß Registrierung bei Fraunhofer SIT
	Service-Indikator	1 BCD	Individuell belegbar	
	CA-spez. Info	1 BCD	Nicht festgelegt	
	Algorithmen-Referenz	2 BCD	Individuell belegbar	Ggf. Unterscheidung diverser PuK-Algorithmen
	Datum	2 BCD	Letzte zwei Ziffern des Jahres der Schlüsselaktivierung	

6.6 Gesamtübersicht CV-Zertifikatsprofil einer Chipkarte der Generation 1

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

Tabelle 55: Tab_PKI_264 Informationen für ein CV-Zertifikat einer Karte

Datum		Länge	Wert	Erläuterung
CPI		1 Byte	´22´	CPI eines CV-Zertifikats einer Karte
Modulus		256 Byte		Modulus des öffentlichen Schlüssels. Die Länge des Modulus muss 38 Byte kleiner als die zu signierende Nachricht M sein.
Exponent		4 Byte		Exponent des öffentlichen Schlüssels
OID		6 Byte	´2B24 0305 0204´	Es wird lediglich der OID {1.3.36.3.5.2.4} verwendet
CHA		7 Byte		Zertifikatsinhaber ist die Karte
	AID	6 Byte	'D27600004000'	AID der Gesundheitsanwendung
	Zugriffsprofil	1 Byte	´00´	Rollenprofil eGK
			´01´	Rollenprofil SM-B eKiosk
			´02´	Rollenprofil HBA/SM-B
			´03´	Rollenprofil HBA/SM-B
			´04´	Rollenprofil HBA/SM-B
			´05´	Rollenprofil (H)BA
			´06´	SMC
			´07´	Rollenprofil (H)BA
			´08´	Rollenprofil SM-B
			´09´	Rollenprofil SM-B
			´0A´	Rollenprofil SM-B.
			'33'	Geräteprofil gSMC-K
			'35'	Geräteprofil HBA
			'36'	Geräteprofil SM-B
			'37'	Geräteprofil SM-B
CHR		12 Byte		'xx xx' || ICCSN der Karte
	Zuordnung Schlüsselpaar	2 Byte	´xx xx´	Zuordnung Schlüsselpaar zu CV-Zertifikat (Key Identifier)
	Major Industry Identifier	2 BCD	´80´	Gesundheitswesen
	Country Code	3 BCD	´276´	Germany

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

6.7 CV-Zertifikatsprofile der Generation 2

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

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

6.7.1 Berechtigung einer CVC-CA zur Zertifikatserstellung

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

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

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

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

- CVC-CA für eGK
  Diese CV-Zertifikate sind immer aus einer dedizierten CVC-CA zu erstellen. Eine Kombination mit anderen Zugriffsprofilen ist nicht zulässig.

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

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

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

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

6.7.2 Aufbau und Bestandteile der CV-Zertifikate der Generation 2

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

1) Certificate Profile Identifier (CPI) gemäß 6.7.3.1

2) Certification Authority Reference (CAR) gemäß 6.4.1.2

3) Öffentlicher Schlüssel: Die Abbildung des öffentlichen Schlüssels ändert sich gegenüber 6.4.1.6 aufgrund der Umstellung von RSA-basierten Schlüsseln (Darstellung von Modulus und öffentlichem Exponent) auf ELC-basierte Schlüssel. Das Datenobjekt zum öffentlichen Schlüssel enthält neben einer OID, welche den Verwendungszweck des öffentlichen Schlüssels kennzeichnet, den öffentlichen Punkt Q (siehe [EN 14890-1#Table 234]).

4) Certificate Holder Reference (CHR) gemäß 6.4.1.3

5) Certificate Holder Autorisation Template (CHAT): Anders als bei Karten der Generation 1 wird die Rolle eines Zertifikatsinhabers nicht durch einen sieben Oktett langen String ausgedrückt, sondern gemäß [EN 14890-1#14.9.3.6] beschreibt eine Flagliste die Rechte, die einem Zertifikatsinhaber nach einer erfolgreichen Authentisierung eingeräumt werden.

6) Certificate Effective Date (CED): Dieses Datenobjekt enthält das Datum des Inkrafttretens des Zertifikates. (Objekt neu für G2)

7) Certificate Expiration Date (CXD): Dieses Datenobjekt enthält das Datum mit dem Gültigkeitsende des Zertifikates. (Objekt neu für G2)

Berechtigungssteuerung über die Flagliste im Feld CHAT

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

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

In späteren Ausbaustufen der TI ist durch Zertifikatserneuerung und dadurch mögliche kurze Laufzeiten der CV-Zertifkate eine flexible Anpassung der Berechtigungsvergabe über diese Flagliste vorgesehen.

Für weitere Informationen zur Zertifikatserneuerung von CV-Zertifikaten der Generation 2 siehe auch [gemSpec_CVC_Root#3.4] und [gemSpec_CVC_Root#6.1.1].

6.7.3 Zertifikatsprofil eines CV-Zertifikates für ELC-Schlüssel

Im Gegensatz zu 6.4.2 ist für ELC-Schlüssel genau ein Zertifikatsprofil zu berücksichtigen. Dieses Zertifikatsprofil gilt sowohl für CV-Zertifikate, welche den öffentlichen Schlüssel einer CA transportieren, als auch für CV-Zertifikate, welche öffentliche Schlüssel zu Authentisierungszwecken transportieren.

6.7.3.1 Certificate Profile Identifier (CPI)

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

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

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

⌦ **GS-A_4987 Wert des Card Profile Identifier in G2**

Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS als Wert für den CPI ´70´ eintragen. ⌫

6.7.3.2 Certification Authority Reference (CAR)

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

Tabelle 56: Tab_PKI_266 Aufbau CAR für Karten der Generation 2

	CA Name	Service-Indikator	CA-spezifische Information	Algorithmen-referenz	Datum
Länge	5 Byte	1 BCD	1 BCD	2 BCD	2 BCD

zugelassene Werte	CA Name gemäß Registrierung bei Fraunhofer SIT	Verwendungszweck des PrK: '8' für die Ausstellung von CA-Zertifikaten '1' für die Ausstellung von EE-Zertifikate	nicht festgelegt	'02' für ELC/ECC	letzte 2 Ziffern des Jahres der CA-Schlüssel-erzeugung

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

Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS den Wert für die CAR in das Datenobjekt ´42´ einstellen ⌫

GS-A_4989 Länge der Certificate Authority Reference in G2

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

GS-A_4990 Verwendung des Feldes Certificate Authority Reference in G2

Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS das Feld CAR weiter unterteilen in die Konkatenation der Datenelemente CA Name, Service-Indikator, CA-spezifische Information, Algorithmenreferenz und Datum sowie dabei die Festlegungen bzgl. Länge und zugelassener Werte gemäß Tab_PKI_266 berücksichtigen.⌫

GS-A_4991 Zuordnung von CAR zu Schlüsselpaar des Herausgebers für G2

Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS sicherstellen, dass die Zuordnung zwischen Certificate Authority Reference (CAR) und Schlüsselpaar eindeutig ist. ⌫

6.7.3.3 Öffentlicher Schlüssel

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

GS-A_4992 Datenobjekt für den öffentlichen Schlüssel

Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS den öffentlichen Schlüssel in das Datenobjekt ´7F49´ einstellen. ⌫

GS-A_4993 Aufbau eines öffentlichen Schlüssel

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

Tabelle 57: Tab_PKI_901 Objektidentifier des öffentlichen Schlüssels eines CV-Zertifikats der Generation 2

Verwendungszweck des CV-Zertifikats	Domain-parameter	Objektidentifier
Transport des öffentlichen Signaturprüfschlüssels einer CA	brainpoolP256r1	OID_{PuK} = ´06-L_{06}-ecdsa-with-SHA256´ OID_{Hex} = ´06 08 2A8648CE3D040302´ OID_{Dez} = ´1.2.840.10045.4.3.2´
	brainpoolP384r1	OID_{PuK} = ´06-L_{06}-ecdsa-with-SHA384´ OID_{Hex} = ´06 08 2A8648CE3D040303´ OID_{Dez} = ´1.2.840.10045.4.3.3´
	brainpoolP512r1	OID_{PuK} = ´06-L_{06}-ecdsa-with-SHA512´ OID_{Hex} = ´06 08 2A8648CE3D040304´ OID_{Dez} = ´1.2.840.10045.4.3.4´
Transport eines öffentlichen Authentisierungsschlüssels	brainpoolP256r1	OID_{PuK} = ´06-L_{06}-authS_gemSpec-COS-G2_ecc-with-sha256´ OID_{Hex} = ´06 06 2B2403050301´ OID_{Dez} = ´1.3.36.3.5.3.1´
	brainpoolP384r1	OID_{PuK} = ´06-L_{06}-authS_gemSpec-COS-G2_ecc-with-sha384´ OID_{Hex} = ´06 06 2B2403050302´ OID_{Dez} = ´1.3.36.3.5.3.2´
	brainpoolP512r1	OID_{PuK} = ´06-L_{06}-authS_gemSpec-COS-G2_ecc-with-sha512´ OID_{Hex} = ´06 06 2B2403050303´ OID_{Dez} = ´1.3.36.3.5.3.3´

Tabelle 58: Tab_PKI_902 Punkt Q des öffentlichen Schlüssels eines CV-Zertifikats der Generation 2

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

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

6.7.3.4 Certificate Holder Reference (CHR)

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

⌦ **GS-A_4994 Datenobjekt für die Certificate Holder Reference**

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

GS-A_4995 Wertfeld der Certificate Holder Reference

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

6.7.3.5 Certificate Holder Autorisation Template (CHAT)

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

GS-A_4996 Wertfeld des Certificate Holder Autorisation Templates

Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS das Certificate Holder Autorisation Template in das Datenobjekt ´7F4C´ einstellen. ⌫

GS-A_4997 Aufbau der Certificate Holder Autorisation Templates

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

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

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

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

6.7.3.6 Certificate Effective Date (CED)

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

GS-A_4998 Datenobjekt des Certificate Effective Date

Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS das Certificate Effective Date in das Datenobjekt ´5F25´ einstellen. ⌫

GS-A_4999 Länge des Certificate Effective Date

Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS für das Certificate Effective Date ein Wertfeld der Länge sechs Oktett einstellen. ⌫

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

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

6.7.3.7 Certificate Expiration Date (CXD)

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

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

Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS das Certificate Expiration Date in das Datenobjekt ´5F24´ einstellen. ⌫

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

Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS für das Certificate Expiration Date ein Wertfeld der Länge sechs Oktett einstellen. ⌫

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

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

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

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

Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS die zu signierende Nachricht des CV-Zertifikats in das Datenobjekt ´7F4E´ einstellen. ⌫

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

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

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

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

)

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

GS-A_5006 Signatur des Zertifikatsdatenobjekts

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

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

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

GS-A_5007 Tag eines Zertifikatsdatenobjekts

Der Herausgeber eines CV-Zertifikats der Generation 2 (TSP-CVC oder CVC-Root-CA) MUSS die Inhalte des Zertifikatsdatenobjekts in das Datenobjekt ´7F21´ einstellen. ⌫

GS-A_5008 Aufbau eines Zertifikatsdatenobjekts

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

Tabelle 62: Tab_PKI_907 Struktur und Inhalt eines CV-Zertifikat

Tag	**L**	**Wert**		
´7F21´	L7F21	CV–Zertifikat		
		Tag	L	Wert

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

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

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

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

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

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

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

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

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

Tag	L	Wert					
´7F21´	´82015B´	CV–Zertifikat					
		Tag	**L**	**Wert**			
		´7F4E´	´81D3´	Nachricht *M*			
				Tag	**L**	**Wert**	
				´5F29´	´01´	CPI = ´70´	
				´42´	´08´	CAR	
				´7F49´	´818E´	öffentlicher Schlüssel	
						Tag	**L**	**Wert**
						´06	´08´	´2A8648CE3D040304´
						´86´	´8181´	P2OS(Q, 64)
				´5F20´	´08´	CHR		
				´7F4C´	´13´	CHAT		
						Tag	**L**	**Wert**
						´06´	´08´	OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}
						´53´	´07´	´XX...XX´, Flagliste
				´5F25´	´06´	CED		
				´5F24´	´06´	CXD		
		´5F37´	´8180´	Signatur = *R* || *S*			

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

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

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

Tag	L	Wert					
´7F21´	*	CV–Zertifikat					
		Tag	**L**	**Wert**			
		´7F4E´	*	Nachricht *M*			
				Tag	**L**	**Wert**	
				´5F29´	´01´	CPI = ´70´	
				´42´	´08´	CAR	
				´7F49´	*	öffentlicher Schlüssel	
						Tag	**L**	**Wert**
						´06	´08´	*
						´86´	*	*
				´5F20´	´08´	CHR		
				´7F4C´	´13´	CHAT		
						Tag	**L**	**Wert**
						´06´	´08´	OID = oid_cvc_fl_ti
						´53´	´07´	´FF FFFF FFFF FFFF´
				´5F25´	´06´	CED		
				´5F24´	´06´	CXD		
		´5F37´	*	Signatur = *R* || *S*			

*Anmerkung: Die mit * gefüllten Feldinhalte müssen anhand der in 6.7.5.1 spezifizierten Zertifikatsprofile für 256/356/512 bit ELC-Schlüssel ermittelt bzw. berechnet werden.*

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

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

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

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

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

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

<table>
<tr><th>Tag</th><th>L</th><th colspan="4">Wert</th></tr>
<tr><td>´7F21´</td><td>´82015D´</td><td colspan="4">CV–Zertifikat</td></tr>
<tr><td rowspan="19"></td><td>Tag</td><td>L</td><td colspan="3">Wert</td></tr>
<tr><td>´7F4E´</td><td>´81D5´</td><td colspan="3">Nachricht M</td></tr>
<tr><td rowspan="18"></td><td>Tag</td><td>L</td><td colspan="2">Wert</td></tr>
<tr><td>´5F29´</td><td>´01´</td><td colspan="2">CPI = ´70´</td></tr>
<tr><td>´42´</td><td>´08´</td><td colspan="2">CAR</td></tr>
<tr><td>´7F49´</td><td>´818C´</td><td colspan="2">öffentlicher Schlüssel</td></tr>
<tr><td rowspan="3"></td><td>Tag</td><td>L</td><td>Wert</td></tr>
<tr><td>´06</td><td>´06´</td><td>´2B2403050303´</td></tr>
<tr><td>´86´</td><td>´8181´</td><td>P2OS(Q, 64)</td></tr>
<tr><td>´5F20´</td><td>´0C´</td><td colspan="2">CHR</td></tr>
<tr><td>´7F4C´</td><td>´13´</td><td colspan="2">CHAT</td></tr>
<tr><td rowspan="3"></td><td>Tag</td><td>L</td><td>Wert</td></tr>
<tr><td>´06´</td><td>´08´</td><td>OID aus {oid_cvc_fl_ti, oid_cvc_fl_cms}</td></tr>
<tr><td>´53´</td><td>´07´</td><td>´XX...XX´, Flagliste</td></tr>
<tr><td>´5F25´</td><td>´06´</td><td colspan="2">CED</td></tr>
<tr><td>´5F24´</td><td>´06´</td><td colspan="2">CXD</td></tr>
<tr><td>´5F37´</td><td>´8180´</td><td colspan="2">Signatur = R || S</td></tr>
</table>

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

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

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

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

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

Bitnummer	Bedeutung
b03	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b04	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b05	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b06	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b07	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b08	eGK: Verwendung der ESIGN-AUTN-Funktionalität mit PIN.CH
b09	eGK: Verwendung der ESIGN-AUTN Funktionalität ohne PIN
b10	eGK: Verwendung der ESIGN-ENCV Funktionalität mit PIN.CH
b11	eGK: Verwendung der ESIGN-ENCV Funktionalität ohne PIN
b12	eGK: Verwendung der ESIGN-AUT Funktionalität
b13	eGK: Verwendung der ESIGN-ENC Funktionalität
b14	eGK: Notfalldatensatz verbergen und sichtbar machen
b15	eGK: Notfalldatensatz schreiben, löschen (hier „erase“, nicht „delete“) mit PIN.NFD
b16	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b17	eGK: Notfalldatensatz lesen mit MRPIN.NFD
b18	eGK: Notfalldatensatz lesen ohne PIN
b19	eGK: Persönliche Erklärungen (DPE) verbergen und sichtbar machen
b20	eGK: DPE schreiben, löschen (hier „erase“, nicht „delete“) mit MRPIN.DPE
b21	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b22	eGK: DPE lesen mit MRPIN.DPE_READ
b23	eGK: DPE lesen ohne PIN
b24	eGK: Einwilligungen und Verweise im DF.HCA verbergen und sichtbar machen
b25	eGK: Einwilligungen im DF.HCA lesen und löschen (hier „erase“, nicht „delete“)
b26	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b27	eGK: Einwilligungen im DF.HCA schreiben
b28	eGK: Verweise im DF.HCA lesen und schreiben
b29	eGK: Geschützte Versichertendaten lesen mit PIN.CH
b30	eGK: Geschützte Versichertendaten lesen ohne PIN
b31	eGK: Loggingdaten schreiben mit PIN.CH
b32	eGK: Loggingdaten schreiben ohne PIN
b33	eGK: Loggingdaten lesen
b34	eGK: Prüfungsnachweis lesen und schreiben
b35	eGK: Testkennzeichen lesen mit PIN.CH
b36	eGK: Testkennzeichen lesen ohne PIN
b37	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b38	RFU, im Rahmen dieser Dokumentenversion auf 0 zu setzen
b39	eGK: Gesundheitsdatendienste verbergen und sichtbar machen
b40	eGK: Gesundheitsdatendienste lesen, schreiben und löschen (hier „erase“)
b41	eGK: Organspendedatensatz lesen mit MRPIN.OSE
b42	eGK: Organspendedatensatz lesen ohne PIN
b43	eGK: Organspendedatensatz schreiben, löschen (hier „erase“, nicht „delete“) mit MRPIN.OSE

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

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

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

Tabelle 71: Tab_PKI_918 Abbildung von Rollenberechtigungen auf äquivalente Flaglisten

Zugriffsprofil		CHA-Wert (G1)	CHAT-Wert / Flagliste (G2)
Rolle	CHA.0	´D276 0000 4000 00´	´00 0000 0000 0000´
	CHA.1	´D276 0000 4000 01´	´00 AC1A CD51 DC00´
	CHA.2A Ärztin/Arzt Fachliche Institution des Arztes Krankenhaus	´D276 0000 4000 02´	´00 5D29 DAA8 BB00´
	CHA.2ZA Zahnärztin/Zahnarzt Fachliche Institution des Zahnarztes	´D276 0000 4000 02´	´00 5D20 DAA8 8300´
	CHA.3	´D276 0000 4000 03´	´00 5C40 DAA8 8300´
	CHA.4	´D276 0000 4000 04´	´00 4C40 DAA8 8200´
	CHA.5	´D276 0000 4000 05´	´00 5C00 02A8 0000´
	CHA.6	wird nicht verwendet	wird nicht verwendet
	CHA.7	´D276 0000 4000 07´	´00 0020 0488 0000´
	CHA.8	´D276 0000 4000 08´	´00 4000 02A8 0000´
	CHA.9	´D276 0000 4000 09´	´00 6800 0AA8 0000´
	CHA 10	´D276 0000 4000 0A´	´00 AF5A CD51 DF00´
Gerät	CHA.51	´D276 0000 4000 33´	´00 0000 0000 0001´
	CHA.53	´D276 0000 4000 35´	´00 0000 0000 000C´
	CHA.54	´D276 0000 4000 36´	´00 0000 0000 0002´
	CHA.55	´D276 0000 4000 37´	´00 0000 0000 0004´

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

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

Die Flagliste für das Profil CHA.2ZA des Rollen-Zertifikates lautet `´00 5D20 DAA8 B300´.`
Die Flagliste für das Profil CHA.53 des Geräte-Zertifikates lautet `´00 0000 0000 000C´.`

Die Kombination, bzw. Veroderung der beiden Flaglisten ergibt `´00 5D20 DAA8 B30C´.`

Die Flagliste einer Sub-CA beginnt mit der Bit-Folge ´10´ (vgl. Tab_PKI_910). Der Wert für die Flagliste des CA-Zertifikates des TSP-CVC in Tab_PKI_919 lautet `´80 5D20 DAA8 B30C´.`

Tab_PKI_919 Beispiele von Sub-CA-Flaglisten nach Kartentyp (G2) und Zugriffsprofilen

Kartentyp / Geräte-Zugriffsprofil	Rollen-Zugriffsprofil	Sub-CA
CHAT-Wert / Flagliste für ein bestimmtes Zugriffsprofil		
eGK	CHA.0	´80000000000000´
gSMC-K / CHA.51	-	´80000000000001´
gSMC-KT / CHA.54	-	´80000000000002´
HBA / CHA.53	CHA.2A	´805D29DAA8BB0C´
HBA / CHA.53	CHA.2ZA	´805D20DAA8830C´
HBA / CHA.53	CHA.3	´805C40DAA8830C´
HBA / CHA.53	CHA.4	´804C40DAA8820C´
HBA / CHA.53	CHA.5	´805C0002A8000C´
HBA / CHA.53	CHA.7	´8000200488000C´
SMC-B / CHA.55	CHA.1	´80AC1ACD51DC04´
SMC-B / CHA.55	CHA.2A	´805D29DAA8BB04´
SMC-B / CHA.55	CHA.2ZA	´805D20DAA88304´
SMC-B / CHA.55	CHA.3	´805C40DAA88304´
SMC-B / CHA.55	CHA.4	´804C40DAA88204´
SMC-B / CHA.55	CHA.8	´80400002A80004´
SMC-B / CHA.55	CHA.9	´8068000AA80004´
SMC-B / CHA.55	CHA.10	´80AF5ACD51DF04´
CHAT-Wert / Flagliste für kombinierte Zugriffsprofile		
eGK	CHA.0	-
gSMC-K und gSMC-KT / CHA.51 & 54	-	´80000000000003´
HBA und SMC-B / CHA.51 & 55	CHA.1-5 & 7-10	´80FF7BDFF9FF0C´

Tabelle 72: Tab_PKI_911 CMS-PKI, Bedeutung der Bits innerhalb der Flagliste eines CHAT

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

7 Festlegung von OIDs

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

8 Prüfung von Zertifikaten

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

- Das TSL-Signer-CA-Zertifikat bildet den Vertrauensanker für die TI.
- Die TSL stellt (i. S. einer Whitelist) den Vertrauensraum für die in der TI zugelassenen Aussteller-CA.
- nonQES-Aussteller-CA-Zertifikate werden ausschließlich gegen die TSL geprüft
- QES-Aussteller-CA-Zertifikate werden (a) hinsichtlich ihrer Zulassung in der TI gegen die TSL und (b) hinsichtlich ihres Sperrstatus über den gesamten Zertifizierungspfad bis zu deren Root-CA geprüft.
- End-Entity-Zertifikate werden gegen den OCSP-Dienst der Aussteller-CA geprüft, außer die Statusprüfung für einen bestimmten Zertifikatstyp ist explizit optional oder nicht vorgesehen.

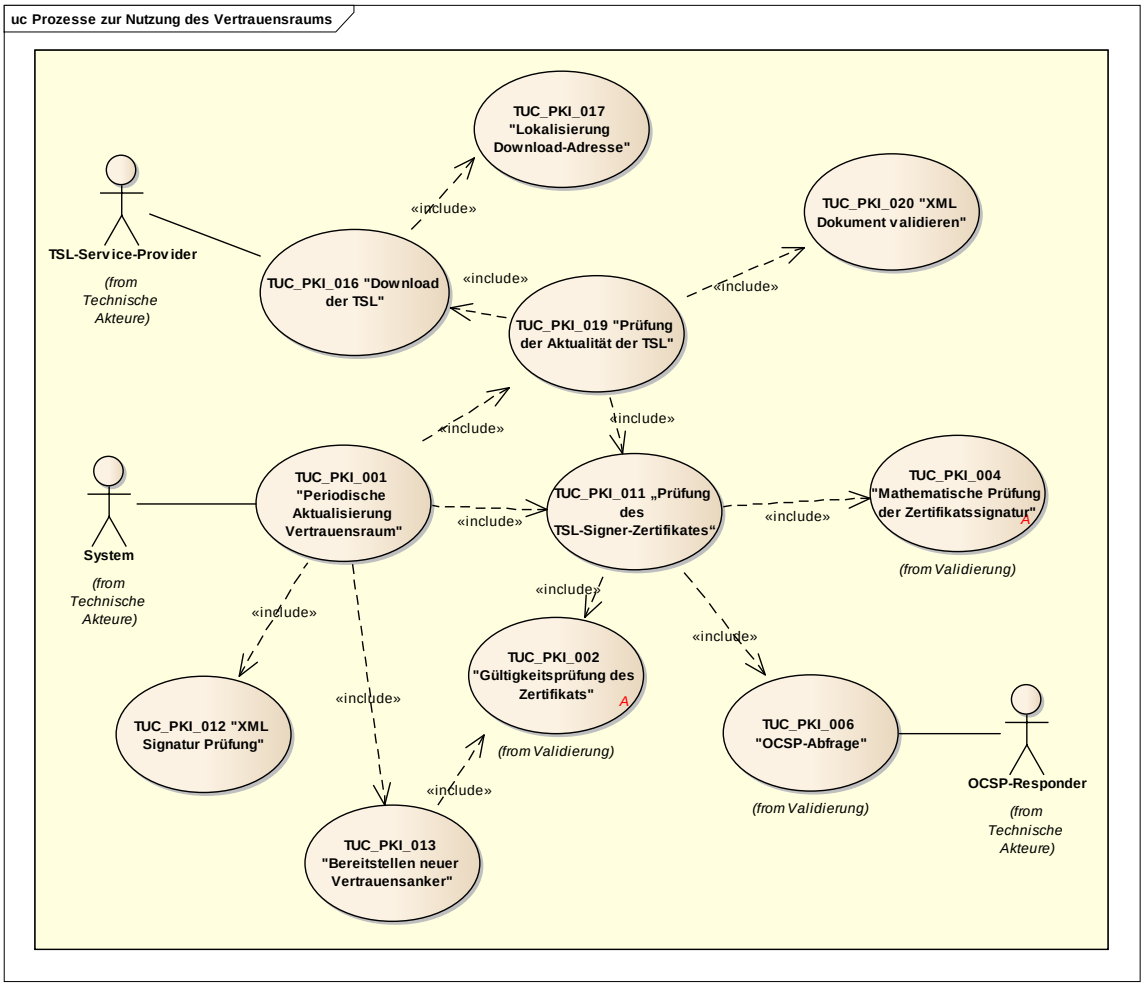

Abbildung 6: Use Case Diagramm "Prozesse zur Nutzung des TI-Vertrauensraums"

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

⌦ **GS-A_4637 TUCs, Durchführung Fehlerüberprüfung**

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN bei der Ausführung eines TUC auf Verarbeitungsfehler prüfen und eine definierte Fehlerbehandlung einleiten**.**⌫

⌦ **GS-A_4829 TUCs, Fehlerbehandlung**

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN bei der Fehlerbehandlung von TUCs Systemmeldungen ausgeben und der Prozess muss beendet werden, sofern der TUC keine spezifische Fehlerbehandlung beschreibt. ⌫

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

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

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

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

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

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

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

8.1 Vertrauensraum der TI

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

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

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

Die TSL spielt also in zertifikatsprüfenden Komponenten die zentrale Rolle.

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

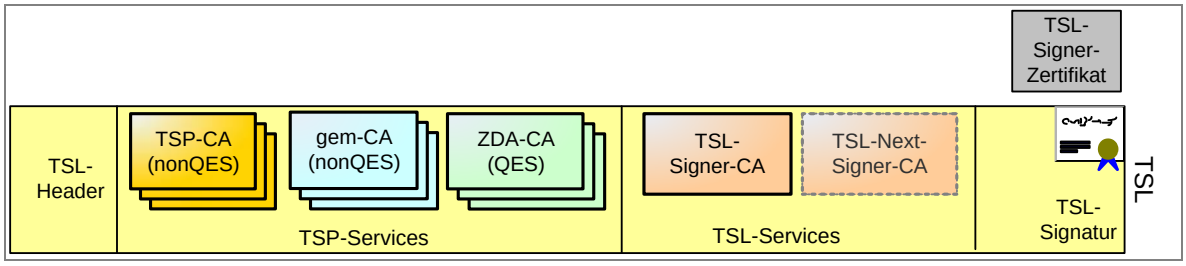

Abbildung 7: Aufbau der TSL

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

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

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

- Initialisierung / Aktualisierung des TI-Vertrauensraumes
- Lokalisieren der TSL-Datei
- Download der TSL-Datei
- Validierung der TSL-Datei
- Prüfung der Integrität und Authentizität der TSL-Datei durch die Prüfung ihrer Signatur

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

8.1.1 Initialisierung TI-Vertrauensraum

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

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

Dies gilt für die Anwendungsfälle

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

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

Hersteller von Produkttypen der TI, die Zertifikate prüfen, MÜSSEN bei der initialen Einbringung das aktuell gültige TSL-Signer-CA-Zertifikat eindeutig identifizieren und mittels Fingerprint validieren, bevor dieses Zertifikat als TI-Vertrauensanker in die Komponente eingebracht werden darf.⌫

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

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN die initiale Einbringung des aktuell gültigen TSL-Signer-CA-Zertifikat als TI-Vertrauensanker in die Komponente nachweislich sicher vor Manipulation vornehmen.⌫

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

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN die initiale Einbringung der TSL-Datei in die Komponente nachweislich sicher vor Manipulation vornehmen.⌫

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

Die in der TI zugelassenen Zertifikate der vertrauenswürdigen Herausgeber (TSPs) sind in der TSL enthalten. Bei der Initialisierung des TI-Vertrauensraumes wird der Truststore befüllt, d.h. die Zertifikate können aus der TSL-Datei ausgelesen und z. B. in den Truststore des Systems importiert werden. Der Status der bezeichneten CA- und OCSP-Dienste wird jeweils im Inhalt des TSL-Elementes „ServiceStatus“ mit einem URI identifiziert. Die untenstehende Tabelle zeigt die erlaubten Stati, erklärt deren Bedeutung in der TI und gibt an, ob ein entsprechend markiertes Zertifikat dem aktuellen TI-Vertrauensraum hinzugefügt werden darf.

Tabelle 73: Tab_PKI_271 Erlaubte URIs als Inhalte des TSL-Elements ServiceStatus

URI	Dienstart	Bedeutung
http://uri.etsi.org/TrstSvc/Svcstatus/inaccord	X.509-CA OCSP CVC-Root-CA DNSSEC-Trust-Anchor	Der Dienst ist für die TI zugelassen und ist in Betrieb.
http://uri.etsi.org/TrstSvc/Svcstatus/revoked	X.509-CA	Die Zulassung des Dienstes wurde wegen eines nicht-sicherheitskritischen Incidents widerrufen und die CA stellt keine End-Entity-Zertifikate mehr aus. Bis zum Widerrufsdatum (im Element StatusStartingTime) ausgegebene End-Entity-Zertifikate müssen aber normal (also als gültig, falls nicht widerrufen) behandelt werden.
http://uri.etsi.org/TrstSvc/Svcstatus/expired	X.509-CA	Der Dienst war für die TI zugelassen und war bis zum angegebenen Datum (im Element StatusStartingTime) in Betrieb und im TI-Vertrauensraum.
Andere URI	-	Der TSL-Dienst darf nicht andere URIs als die oben angegebenen verwenden.

8.1.1.1 TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“

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

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

Tabelle 74: TUC_PKI_001 "Periodische Aktualisierung TI-Vertrauensraum"

Element	Beschreibung
Name	TUC_PKI_001 "Periodische Aktualisierung TI-Vertrauensraum"
Beschreibung	Dieser Use Case beschreibt den gesamten Ablauf zur periodischen Aktualisierung des TI-Vertrauensraumes mittels einer TSL-Datei. Dabei verwendet er weitere TUCs, die im Laufe des Kapitels detailliert spezifiziert werden Ein Offline-Modus ist zu berücksichtigen für a) das Mobile-Kartenterminal b) Konnektor ohne Anbindung an die TI Beide verfügen nicht über die automatischen Online-Möglichkeiten zum Bezug von Statusinformationen oder TSL-Aktualisierungen aus der TI.
Anwendungsumfeld	System, das die TSL auswertet
Auslöser	Produkttypspezifischer Trigger Zeitpunkt MUSS durch Facharchitekturen vorgegeben werden. (Standardmäßig ist eine tägliche Prüfung der Aktualität vorzusehen.)
Eingangsdaten	• TSL im System • Neu eingebrachte TSL-Datei (optional)

Element	Beschreibung
	• OCSP-Graceperiod (legt bei der Verwendung von gecachten OCSP-Antworten den maximal zulässigen Zeitraum fest, den die Systemzeit der prüfenden Komponente noch nach dem Zeitpunkt der OCSP-Antwort liegen darf) • Flag für Offline-Modus (Im Offline-Fall kann keine Sperrstatusprüfung des TSL-Signer-Zertifikates durchgeführt werden.)
Komponenten	System, TSL-Download-Punkt, OCSP-Responder
Ausgangsdaten	Status der Initialisierung
Referenzen	[ETSI_TS_102_231]
Standardablauf	1. [System:] System startet die Initialisierung des TI-Vertrauensraums. 2. [System:] Die TSL im System wird auf Aktualität geprüft (TUC_PKI_019 „Prüfung der Aktualität der TSL"). Diese Prüfung kann mit der neu eingebrachten TSL-Datei als Eingangsparameter erfolgen. (Ansonsten wird die aktuelle TSL-Datei bei diesem Schritt heruntergeladen.) Die Prüfung ergibt, dass die im System abgelegten TSL-Informationen erneuert werden müssen. 3. [System:] Das verwendete TSL-Signer-Zertifikat wird aus der TSL-Datei extrahiert. 4. [System:] OCSP-Abfrage für das extrahierte TSL-Signer-Zertifikat durch das System (TUC_PKI_006 "OCSP-Abfrage") (Sämtliche anderen Schritte einer Prüfung des Zertifikates und der XML-Signatur sind im TUC_PKI_019 „Prüfung der Aktualität der TSL" referenziert, vgl. im Schritt 2.) 5. [System:] Es wird ermittelt, ob in der neuen TSL ein neuer TI-Vertrauensanker vorliegt (Geplanter Wechsel TI-Vertrauensanker, TUC_PKI_013 „Import TI-Vertrauensanker aus TSL“). 6. [System:] Aus den CA-Zertifikaten aus der neuen TSL wird der neue TI-Vertrauensraum gebildet. Dazu werden sie aus der TSL-Datei extrahiert, z. B. in einen System-eigenen Truststore gespeichert und dem System bereitgestellt. Falls ein solcher Truststore nur den Vertrauensraum der TI enthält, wird er vor der Neubefüllung geleert, so dass anschließend nur die Zertifikate aus der aktuellen TSL dem System zur Verfügung stehen. Falls der Truststore auch für die sichere Speicherung von Zertifikaten benutzt wird, die nicht in der TSL stehen, muss keine komplette Leerung des Truststores erfolgen. Das System muss aber sicherstellen, dass im Truststore nur diejenigen Zertifikate der TI enthalten sind, die den aktuellen Vertrauensraum der TI aufspannen bzw. in der aktuellen TSL-Datei enthalten sind. Die Form des Truststore wird nicht näher spezifiziert, dieser muss nur den gestellten Anforderungen (z. B. bezüglich Sicherheit oder Performance) genügen. Das System muss den TI-Vertrauensraum mit den in der TSL als vertrauenswürdig bezeichneten CA-Zertifikaten gemäß Tab_PKI_271 „Erlaubte Inhalte des TSL-Elements ServiceStatus“ befüllen.

Element	Beschreibung
	7. [System:] Der Truststore wird für Zertifikatsprüfung (wieder) bereitgestellt. 8. [System:] Ende des Use Case
Varianten/Alternativen	Der Standardablauf stellt die Prüfungen dar, die vollzogen werden müssen. Eine Trennung in zwei Prozesse oder eine Umstrukturierung, bei der alle notwendigen Prüfungen erfolgen, ist zulässig. Im Falle einer aktuellen TSL im System endet der Ablauf nach Schritt 2: 2a. [System:] TSL aus Download ist gleich TSL im System; und TSL ist noch gültig. 2a.1 [System:] Ende des Use Case 3a. [System:] Wenn das Offline-Flag gesetzt ist (offline==true), dann wird mit Schritt 5 weitergefahren. (Im Offline-Fall kann keine OCSP-Abfrage stattfinden.)
Fehlerfälle/Warnung	Ein Fehlerfall ist, dass dem System keine gültige TSL (Signatur) vorliegt und es nicht mehr in der Lage ist, Prozesse in der TI abzubilden: 1a. [System:] Es ist keine TSL im System vorhanden. Abbruch mit Fehlermeldung (TSL_INIT_ERROR) 3b. [System:] Das TSL-Signer-Zertifikat lässt sich nicht aus der TSL-Datei extrahieren (TSL_CERT_EXTRACTION_ERROR). 6a. [System:] Abbruch mit Fehlermeldung (TSL_CERT_EXTRACTION_ERROR) Weitere Fehlerfälle sind in den jeweiligen referenzierten TUCs beschrieben.
Technische Fehlermeldung	Es ist keine TSL im System vorhanden. Zertifikat(e) lässt/lassen sich nicht extrahieren. Weitere technische Fehlermeldungen sind in den jeweiligen referenzierten TUCs beschrieben
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_001 "Periodische Aktualisierung TI-Vertrauensraum"

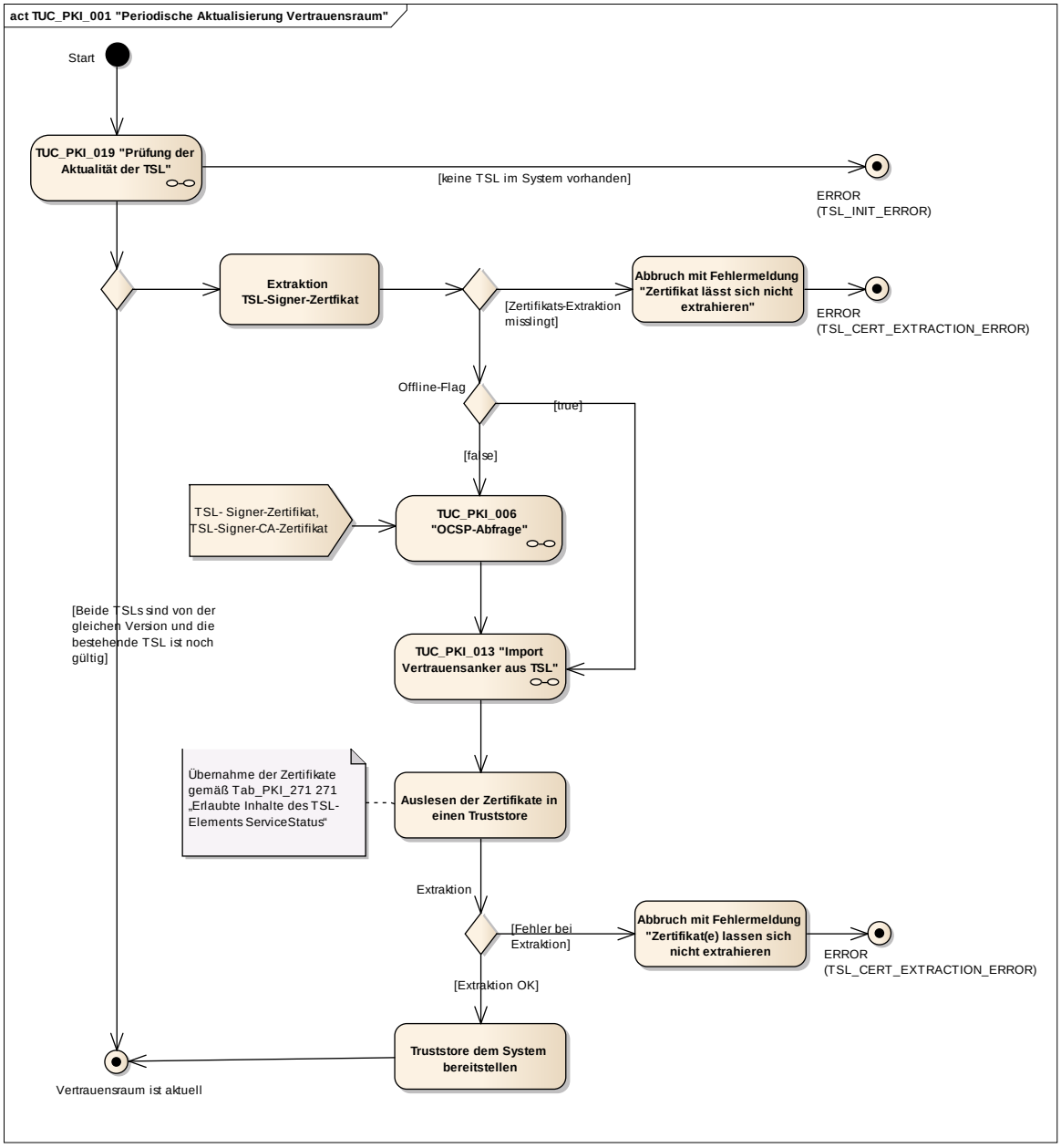

Abbildung 8: Aktivitätsdiagramm TUC_PKI_001 "Periodische Aktualisierung TI-Vertrauensraum"

8.1.2 Geplanter Wechsel TI-Vertrauensanker

8.1.2.1 TUC_PKI_013 „Import TI-Vertrauensanker aus TSL“

⌧ GS-A_4643 TUC_PKI_013: Import TI-Vertrauensanker aus TSL

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_013 zum Import neuer TI-Vertrauensanker umsetzen.⌫

Tabelle 75: TUC_PKI_013 "Import neuer TI-Vertrauensanker"

Element	Beschreibung
Name	TUC_PKI_013 "Import neuer TI-Vertrauensanker"
Beschreibung	Als TI-Vertrauensanker gilt das aktuell gültige TSL-Signer-CA-Zertifikat. Das neue TSL-Signer-CA-Zertifikat wird rechtzeitig vor dem geplanten Aktivierungsdatum in die TSL integriert und als zukünftiger TI-Vertrauensanker markiert. Über diesen Weg wird es an Komponenten und Systeme ausgeliefert. Die Integrität des neuen Schlüssels wird somit durch den gültigen alten gesichert.
Anwendungsumfeld	System, das die TSL verwendet
Vorbedingungen	TSL mit gültiger Signatur
Auslöser	TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“
Eingangsdaten	neue, heruntergeladene TSL-Datei, deren Gültigkeit und Integrität bereits geprüft sind
Komponenten	System
Ausgangsdaten	Status des Prozesses, im Erfolgsfall eine Erweiterung des sicheren Speichers des Systems um den neuen TI-Vertrauensanker und dessen Aktivierungsdatum.
Referenzen	[ETSI_TS_102_231]
Standardablauf	1. [System:] Das System sucht in der TSL nach den Einträgen für den neuen TI-Vertrauensanker. Die Identifikation erfolgt gemäß Kapitel 8.1.2.2. Es wird immer das CA-Zertifikat bereitgestellt. Alle anderen Zustände (z.B. wenn nur der unzertifizierte Schlüssel bereitgestellt wird) müssen als Fehler behandelt werden. Parameter: heruntergeladene TSL 2. [System:] Aus dem gefundenen Eintrag wird das Zertifikat extrahiert. Ergebnis: zukünftiges TSL-Signer-CA-Zertifikat 3. [System:] Aus dem Eintrag des zukünftigen TSL-Signer-CA-Zertifikats wird die „StatusStartingTime“ extrahiert. Ergebnis: StatusStartingTime 4. [System:] Für das zukünftige TSL-Signer-CA-Zertifikat wird TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats" durchlaufen. Parameter: zukünftiges TSL-CA-Zertifikat, StatusStartingTime. 5. [System:] Der zukünftige TI-Vertrauensanker wird parallel zum aktiven TI-Vertrauensanker abgelegt. Parameter: zukünftiges TSL-Signer-CA-Zertifikat 6. [System:] Der zukünftige TI-Vertrauensanker darf nicht vor dem Zeitpunkt „StatusStartingTime“ aktiviert werden. Der zukünftige TI-Vertrauensanker muss spätestens dann aktiviert werden, wenn nach Erreichen der „StatusStartingTime“ ein Update der TSL durchgeführt wird. Bei Aktivierung des zukünftigen TI-Vertrauensankers wird der alte TI-

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

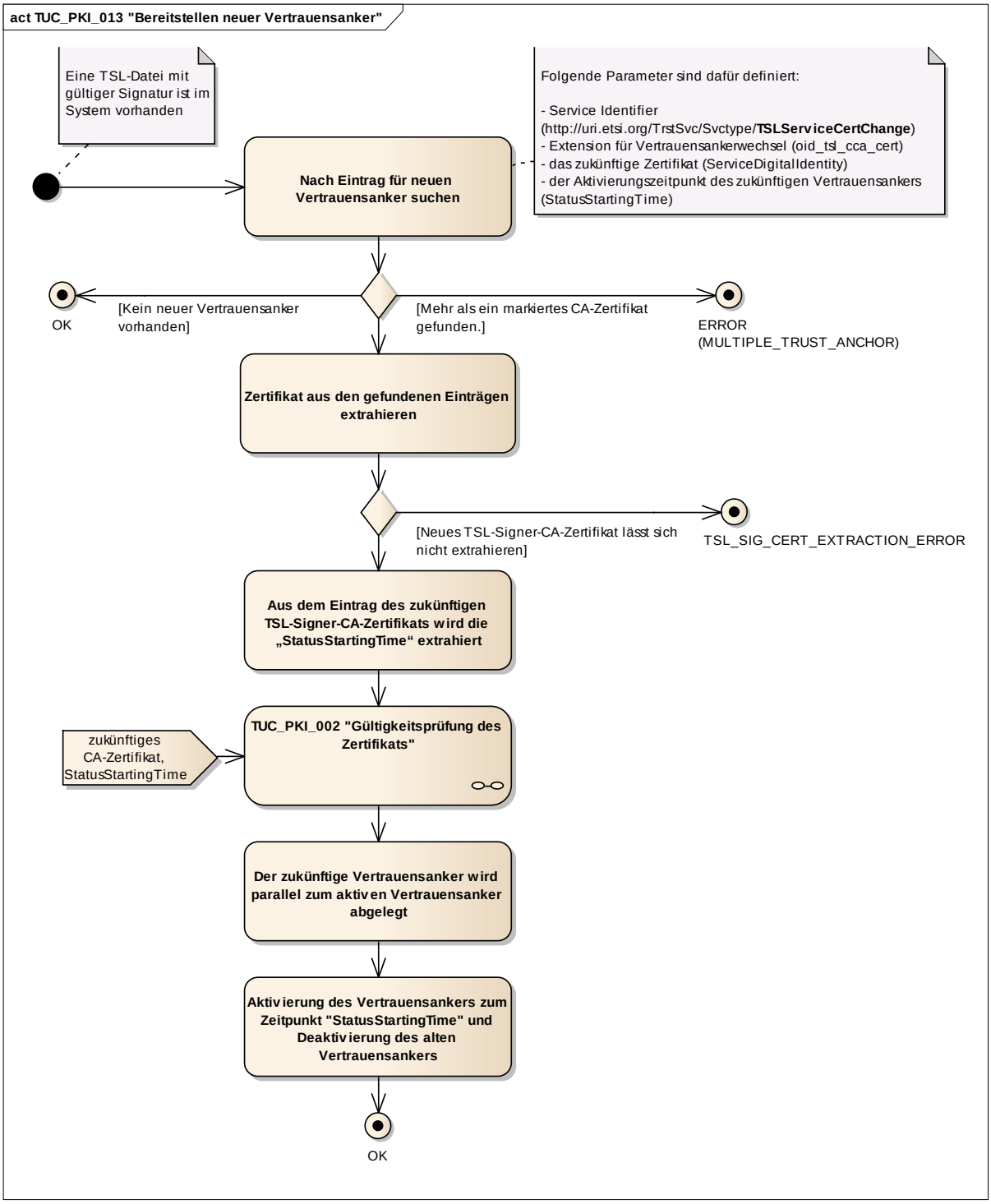

Abbildung 9: Aktivitätsdiagramm TUC_PKI_013 "Import neuer TI-Vertrauensanker"

8.1.2.2 TSL-Einträge für die Bereitstellung neuer TI-Vertrauensanker

Für einen Wechsel des TSL-Signer-CA-Zertifikates wird dieses in der TSL aufgenommen unter Berücksichtigung folgender Rahmenbedingungen:

- die Aufnahme des Zertifikates erfolgt rechtzeitig, also einen definierten Zeitraum vor dem geplanten Aktivierungsdatum, um temporär offline befindlichen

Komponenten eine als zumutbar angenommene Zeitspanne zur Migration zu gewähren.

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

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

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

⌦ **GS-A_4644 TSL-Vertrauensankerwechsel**

Der TSL-Dienst MUSS für einen TI-Vertrauensankerwechsel die folgenden Einträge aufnehmen: (a) Innerhalb Element ServiceTypeIdentifier: URI *http://uri.etsi.org/TrstSvc/Svctype/TSLServiceCertChange* (b) Einen durch die gematik vorgegeben Aktivierungszeitpunkt im Element StatusStartingTime (c) die Extension für den TI-Vertrauensankerwechsel {oid_tsl_cca_cert} gemäß [gemSpec_OID#GS-A_4447] (in ServiceInformationExtension) ⌫

Das vorliegende Dokument trifft keine Festlegungen zu den konkret einzutragenden OID-Werten, sondern verwendet stattdessen eine OID-Referenz, die in der Spalte "Inhalt" der Tabelle 76genannt ist. Die normative Festlegung der OIDs trifft das Dokument [gemSpec_OID], dort ist die Zuordnung zur OID-Referenz ersichtlich.

Tabelle 76: Gültige Werte für den TI-Vertrauensankerwechsel

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

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

Tabelle 77: Beispiel für den TSL-Eintrag zum Wechsel des TSL-Signer-CA-Zertifikats

```
<TSPService>
       <ServiceInformation>
       <ServiceTypeIdentifier>
              http://uri.etsi.org/TrstSvc/Svctype/TSLServiceCertChange
       </ ServiceTypeIdentifier>
       <ServiceName>
              <Name xml:lang="DE">{Name des neuen TSL-Vertrauensankers}</Name>
</ServiceName>
       <ServiceDigitalIdentity>
              <DigitalId>
                           <X509Certificate>{Base64-codiertes X.509-
                     Zertifikat}</X509Certificate>
              </DigitalId>
       </ServiceDigitalIdentity>
       <ServiceStatus>http://uri.etsi.org/TrstSvc/Svcstatus/inaccord
       </ServiceStatus>
       <StatusStartingTime>2008-04-01T09:30:47.0Z</StatusStartingTime>
       <ServiceSupplyPoints>
              <ServiceSupplyPoint>http://pki01ocsp02.gematik.net
              </ServiceSupplyPoint>
       </ServiceSupplyPoints>
       <ServiceInformationExtensions>
              <Extension Critical="true">
                     <ExtensionOID>{oid_tsl_cca_cert}</ExtensionOID>
                     <ExtensionValue>oid_tsl_cca_cert</ExtensionValue>
              </Extension>
       </ServiceInformationExtensions>
       </ServiceInformation>
</TSPService>
```

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

8.1.2.3 Prüfung der TSL nach Wechsel des TI-Vertrauensanker

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

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

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

Der TSL-Dienst MUSS ab dem Aktivierungsdatum eines über die TSL publizierten TI-Vertrauensankers (TSL-Signer-CA-Zertifikat) die TSL mit einem TSL-Signer-Zertifikat signieren, das von dieser TSL-Signer-CA ausgestellt wurde. Dieses TSL-Signer-CA-Zertifikat MUSS genau ab diesem Aktivierungsdatum gültig sein.⌫

8.1.3 Ungeplanter Wechsel des TI-Vertrauensanker

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

8.2 TSL-Prüfung

8.2.1 Erreichbarkeit und Download der TSL

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

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

Die TSL verweist auf die Download-Punkte, wo die jeweils aktuellste Version der TSL heruntergeladen werden kann (siehe Kap8.2.1.1).

Die Lokalisierung der Adresse ist in Abschnitt 8.2.1.1 detailliert beschrieben.

8.2.1.1 TUC_PKI_017 „Lokalisierung TSL Download-Adressen“

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

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

Tabelle 78: TUC_PKI_017 "Lokalisierung Download-Adressen"

Element	Beschreibung
Name	TUC_PKI_017 "Lokalisierung Download-Adressen“
Beschreibung	Die TSL enthält im Element "PointersToOtherTSL“ die Zugriffsadresse für die jeweilige Liste. Zusätzlich ist ein Eintrag für eine Backup-Zugriffsadresse vorhanden. Dieser Use Case beschreibt, wie diese Adressen lokalisiert werden.
Anwendungsumfeld	System, das die TSL verwendet
Vorbedingungen	TSL mit gültiger Signatur
Auslöser	TUC_PKI_016 "Download der TSL"
Eingangsdaten	TSL
Komponenten	System
Ausgangsdaten	PointersToOtherTSL[Primär-Zugriffsadresse, Backup-Zugriffsadresse]
Referenzen	[ETSI_TS_102_231] Annex H und B.2.13
Standardablauf	1. [System:] System startet die Lokalisierung der Adressen 2. [System:] Das Element „PointersToOtherTSL“ wird ausgewählt. 3. [System:] Übergabe des Elements 4. [System:] Ende des Use Cases mit Rückgabe des Adressen-Elements
Fehlerfälle	2a.

Element	Beschreibung
	[System:] Das Element ist nicht vorhanden und der Vorgang wird mit Fehlermeldung abgebrochen. (TSL_DOWNLOAD_ADDRESS_ERROR)
Technische Fehlermeldung	Download der TSL nicht möglich Das System meldet entsprechende Fehlercodes.
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	Die Kennzeichnung der Adressen in der TSL als primär oder als backup erfolgt gemäß Tab_PKI_272
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_017 "Lokalisierung Download-Adresse"

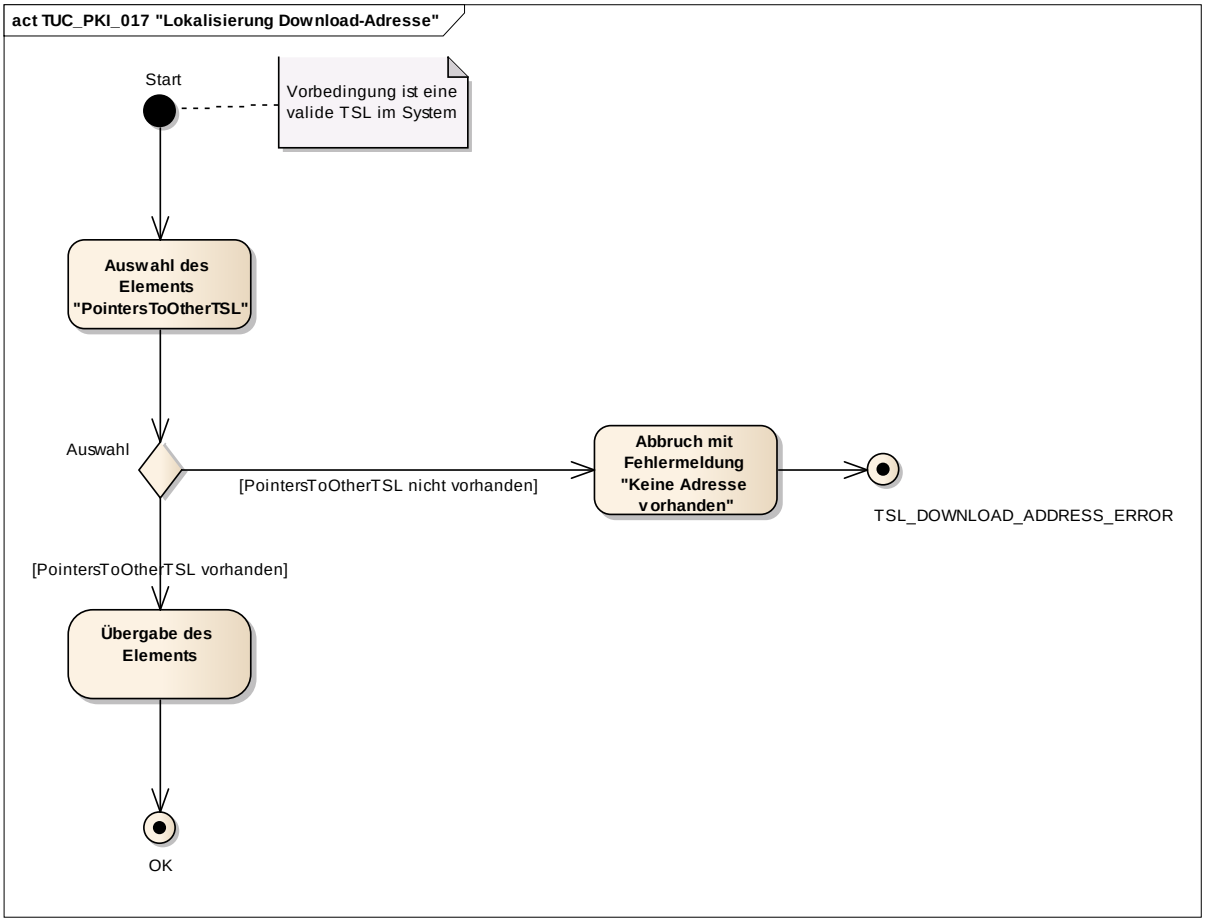

Abbildung 10: Aktivitätsdiagramm TUC_PKI_017 "Lokalisierung Download-Adresse"

Tabelle 79: Tab_PKI_272 Gültige Werte zur Download-Adresse

Beschreibung	Ort	Bezeichnung	Format	Inhalt
Bezeichner der Eintragsdaten für die Primär-Adresse der TSL	TSL	Primär-Adresse	OID	oid_tsl_p_loc
Bezeichner der Eintragsdaten für die Backup-Adresse der TSL	TSL	Backup-Adresse	OID	oid_tsl_b_loc

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

8.2.1.2 TUC_PKI_016 "Download der TSL-Datei"

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

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

Tabelle 80: TUC_PKI_016 "Download der TSL-Datei"

Element	Beschreibung
Name	TUC_PKI_016 "Download der TSL-Datei"
Beschreibung	Es wird der Download-Prozess der TSL-Datei und das Verhalten des Systems bei Fehlerfällen, wie nicht erfolgreicher Download bzw. Netzwerkproblemen beschrieben.
Anwendungsumfeld	System, das die TSL verwendet
Vorbedingungen	Lokalisierung der Download-Adresse
Auslöser	TUC_PKI_019 „Prüfung der Aktualität der TSL"
Eingangsdaten	TSL
Komponenten	System, TSL-Download-Punkt
Ausgangsdaten	Status des Prozesses
Referenzen	[ETSI_TS_102_231]
Standardablauf	1. [System:] Das System startet den Prozess zum Download der TSL-Datei. 2. [System:] Lokalisierung der Downloadadresse (TUC_PKI_017 „Lokalisierung TSL Download-Adressen“) 3. [System:] Auswahl der Primär-Download-Adresse aus dem Element „PointersToOtherTSL“ 4. [System:] Download der TSL-Datei. 5. [System:] Ende des Use Case mit entsprechender Rückmeldung
Varianten/Alternati-ven	4a. [System:] Bei Fehlern wird ein einfaches Fehlerhandling angestoßen. 4a.1 [System:] Wiederholung des Downloads. Der Download von der Primär-Download-Adresse wird dreimal wiederholt. Konnte die TSL dabei nicht erfolgreich geladen werden, erfolgt die Ausführung von 4a.2. 4a.2 [System:] Wechsel auf die Backup-Adresse. Bei Fehlern wird auch dieser Download wiederholt. Die Wiederholung erfolgt dreimal.
Fehlerfälle	5a. [System:] Sollte der wiederholte Download über keine der Adressen

Element	Beschreibung
	erfolgreich sein, meldet das System einen Fehler und es werden für den Moment keine weiteren Download-Versuche mehr unternommen. (TSL_DOWNLOAD_ERROR)
Technische Fehlermeldung	Download der TSL nicht möglich Das System meldet entsprechende Fehlercodes Weitere technische Fehlermeldungen sind in den jeweiligen referenzierten TUCs beschrieben.
Sicherheitsanforde-rungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	
Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_016 "Download der TSL-Datei"

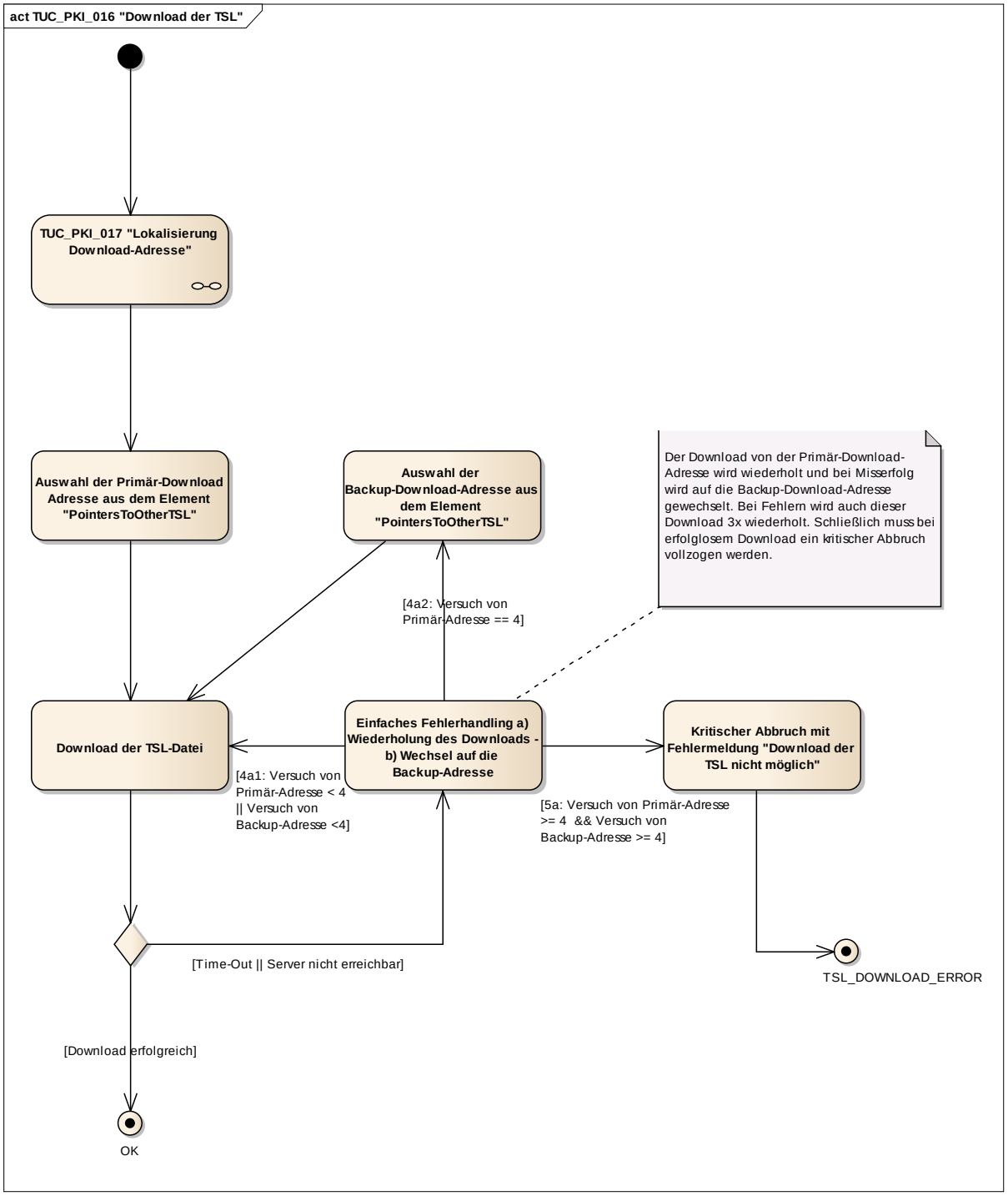

Abbildung 11: Aktivitätsdiagramm TUC_PKI_016 "Download der TSL-Datei"

8.2.2 Vertrauensstatus und Authentifizieren der TSL

8.2.2.1 TUC_PKI_019 „Prüfung der Aktualität der TSL"

Eine TSL-prüfende Komponente oder Anwendung kann den übergreifend festgelegten maximalen Wert der TSL-Graceperiod (30 Tg) mit dem Eingangsparameter TSL-Grace-Period überschreiben. Je nach Kritikalität der prüfenden Anwendung kann die TSL-Grace-Period damit zwischen 0 .. 30 Tagen gewählt werden.

Wird der TUC mit dem Wert „0“ aufgerufen, kann die Bedingung für Validity-Warning-1 nicht erfüllt werden, so dass die TSL mit Überschreitung des „nextUpdate“ auf jeden Fall als „ungültig“ mit der Rückmeldung "Validity_Warning_2" reklamiert wird. Damit gilt:

a) OK - nextUpdate > aktuelles Datum

b) Validity_Warning_1 - nextUpdate < aktuelles Datum < (nextUpdate + TSL-Grace-Period)

c) Validity_Warning_2 - nextUpdate < aktuelles Datum > (nextUpdate + TSL-Grace-Period)

⌦ **GS-A_4648 TUC_PKI_019: Prüfung der Aktualität der TSL**

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_019 zur Prüfung der Aktualität der TSL umsetzen.⌫

Tabelle 81: TUC_PKI_019 "Prüfung der Aktualität der TSL"

Element	Beschreibung
Name	TUC_PKI_019 "Prüfung der Aktualität der TSL"
Beschreibung	Das System überprüft (standardmäßig täglich) die Aktualität der TSL. Dies geschieht anhand eines Vergleichs der TSL aus dem System und der TSL aus dem Download: Die jeweilige ID und die jeweilige Sequenznummer der beiden TSL werden verglichen.
Anwendungsumfeld	System, das die TSL auswertet
Vorbedingungen	Eine geprüfte TSL im System
Auslöser	TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“
Eingangsdaten	TSL im System, neu eingebrachte TSL-Datei (optional), TSL-Grace-Period
Komponenten	System
Ausgangsdaten	Status der Prüfung
Referenzen	[ETSI_TS_102_231]
Standardablauf	1. [System:] System lädt die aktuelle TSL-Datei herunter (TUC_PKI_016 "Download der TSL-Datei"). 2. [System:] TSL-Datei aus dem Download wird validiert (TUC_PKI_020

Element	Beschreibung
	„XML-Dokument validieren“) Das entsprechende von der gematik benannte Schema muss verwendet werden. 3. [System:] Das TSL-Signer-Zertifikat der neuen TSL-Datei wird geprüft. (TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“). 4. [System:] Die Signatur der TSL-Datei aus dem Download oder aus den Eingangsdaten muss geprüft werden (TUC_PKI_012 „XML-Signatur-Prüfung“) 5. [System:] Aus der TSL im System und der TSL-Datei aus dem Download werden die jeweilige ID und das jeweilige TSLSequenceNumber-Element selektiert. 6. [System:] System prüft die ID-Attribute und das TSLSequenceNumber-Element aus Schritt 5 auf Gleichheit. Sind sie identisch, muss keine Aktualisierung erfolgen. 7. [System:] (Die IDs und TSLSequenceNumber-Elemente aus Schritt 5 sind identisch.) Prüfung, ob die TSL im System noch aktuell ist. Dies geschieht anhand des aktuellen Datums und des Elements „NextUpdate“ aus der TSL. Eine TSL wird als aktuell bezeichnet, wenn ihr NextUpdate in der Zukunft liegt. 8. [System:] TSL im System ist gültig. Ende des Use Case mit entsprechender Rückmeldung
Varianten/Alterna-tiven	1a. [System:] Wenn eine TSL-Datei als Eingangsparameter eingebracht wurde, dann wird diese TSL-Datei verwendet, und es erfolgt kein Download. 6a. [System:] Die ID-Attribute aus Schritt 5 sind nicht gleich und das TSLSequenceNumber-Element der TSL im System ist kleiner als die aus dem Download. Somit ist die TSL im System älter als die aus dem Download. 6a1. [System:] Rückmeldung an den aufrufenden Use Case (TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“)
Fehlerfälle	6b. [System:] Keine der beschriebenen Varianten des Vergleichs der ID und SequenceNumber tritt ein. Ende des Use Case mit Fehlermeldung (TSL_ID_INCORRECT) 7a. [System:] Warnung (VALIDITY_WARNING_1) mit der entsprechenden Meldung. (Die TSL ist nicht mehr aktuell.) Rückmeldung des Warnhinweises. 7a1. [System:] Warnung (VALIDITY_WARNING_2) mit der entsprechenden Meldung, nach Überschreitung des Elements NextUpdate um die TSL-

Element	Beschreibung
	Grace-Period. (Ablauf der TSL-Grace-Period, die TSL ist nicht mehr vertrauenswürdig.) Rückmeldung des Warnhinweises. Weitere Fehlerfälle sind in den referenzierten Use Cases beschrieben.
Technische Fehlermeldung	Aktualitäts-Warnung: Die TSL ist nicht mehr aktuell. Das aktuelle Datum ist neuer als das Element NextUpdate der TSL (TSL_ NEXTUPDATE_EXPIRED) Weitere Fehlermeldungen finden sich in den jeweiligen referenzierten Use Cases.
Sicherheitsanforde-rungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.

Anmerkungen	Die ID der TSL-Datei befindet sich als Attribut im Root-Tag des XML-Dokuments.
	`<xsd:attribute name="Id" type="xsd:ID" use="optional"/>`
	Das Attribut Id wird vom TSL-Service-Provider immer gefüllt.
	`Das Element TSLSequenceNumber beschreibt die Folgenummer der TSL. Sein erstmaliger Inhalt ist gleich 1 und wird jeweils um 1 hoch gezählt.`

Zugehörige Diagramme	Aktivitätsdiagramm TUC_PKI_019 "Prüfung der Aktualität der TSL"

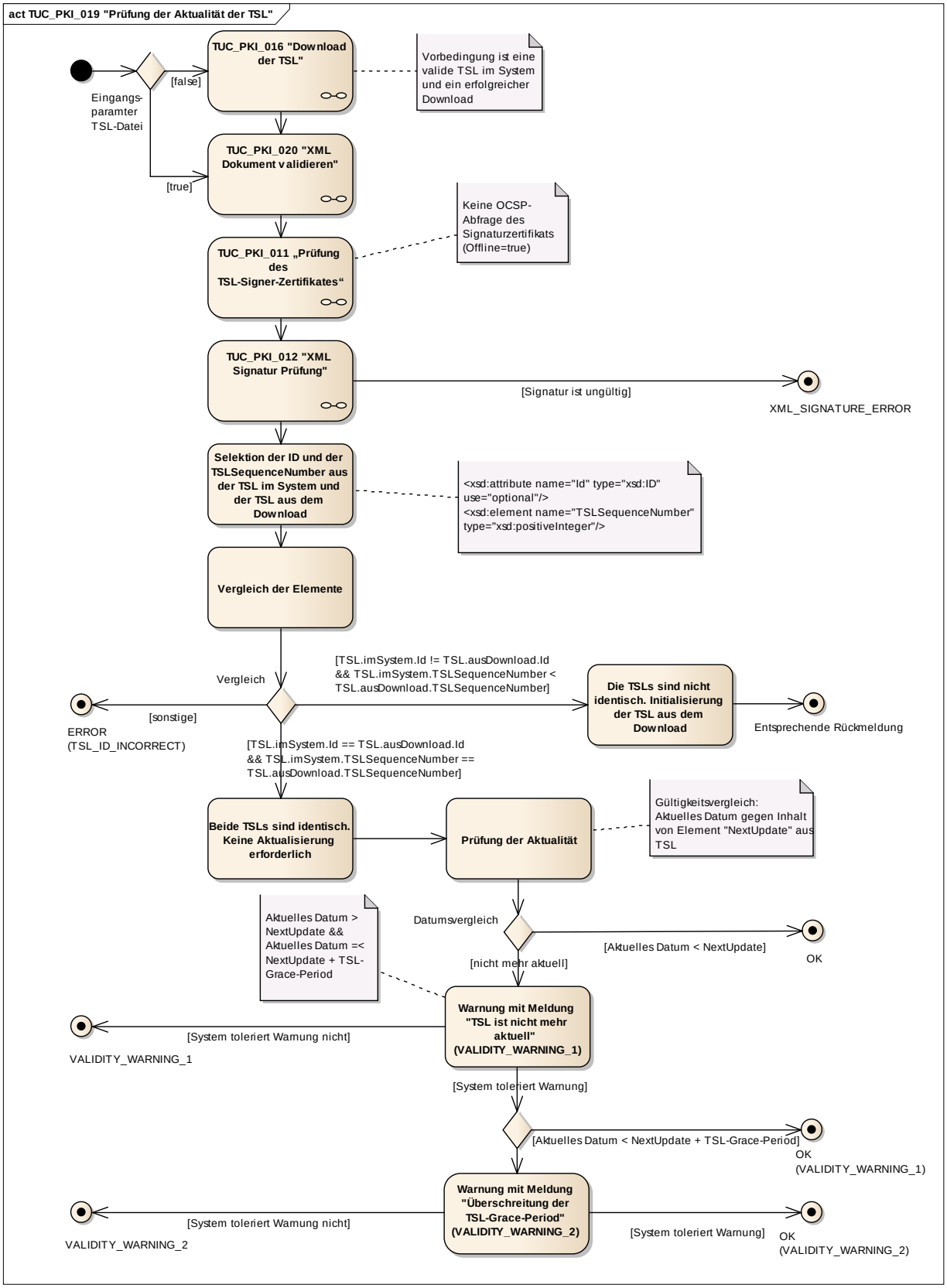

Abbildung 12: Aktivitätsdiagramm TUC_PKI_019 "Prüfung der Aktualität der TSL"

8.2.2.2 TUC_PKI_020 „XML-Dokument validieren“

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

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

Tabelle 82: TUC_PKI_020 "XML-Dokument validieren"

Element	Beschreibung
Name	TUC_PKI_020 "XML-Dokument validieren"
Beschreibung	Ein XML-Dokument wird gegen ein XML-Schema validiert.
Anwendungsumfeld	Dieser Use Case wird verwendet, um XML-Dokumente zu validieren. In diesem Dokument betrifft das die Validierung der TSL.
Vorbedingungen	Eine vollständig vorliegende TSL-Datei im XML-Format
Auslöser	TUC_PKI_019 „Prüfung der Aktualität der TSL"
Eingangsdaten	TSL-Datei XML-Schema (und alle in ihm referenzierten Schemata). Das System muss sicherstellen, dass zur Validierung nur das von der gematik spezifizierte bzw. benannte Schema benutzt wird.
Komponenten	System
Ausgangsdaten	Entsprechendes Ergebnis der Validierung (Erfolg | Misserfolg)
Referenzen	[XML]
Standardablauf	Das System prüft die Wohlgeformtheit des Dokumentes und validiert es gegen das Schema. 1. [System:] System startet Prüfung der TSL-Datei. 2. [System:] System prüft Wohlgeformtheit der TSL-Datei. 3. [System:] System validiert die TSL-Datei gegen die Schemata. 4. [System:] Ende des Use Case mit positivem Ergebnis
Fehlerfälle	Die übergebenen Schemata könnten selbst invalide oder unvollständig sein. 2a. [System:] Ende des Use Case mit Fehlermeldung (TSL_NOT_WELLFORMED) 3a. [System:] Ende des Use Case mit Fehlermeldung (TSL_SCHEMA_NOT_VALID)
Technische Fehlermeldung	Das System meldet entsprechende Fehlercodes

8.2.2.3 TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“

⌦ **GS-A_4650 TUC_PKI_011: Prüfung des TSL-Signer-Zertifikates**

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

Tabelle 83: TUC_PKI_011 "Prüfung des TSL-Signer-Zertifikates"

Element	Beschreibung
Name	TUC_PKI_011 "Prüfung der Integrität des TSL-Signer-Zertifikates"
Beschreibung	Es wird der Prozess zur Prüfung des TSL-Signer-Zertifikates gegen ein sicher verwahrtes TSL-Signer-CA-Zertifikat spezifiziert. Der Prozess verläuft analog demjenigen für Zertifikatsprüfung im Allgemeinen (TUC_PKI_018 "Zertifikatsprüfung in der TI "), berücksichtigt aber die Besonderheiten des TSL-Signer-Zertifikates. Außerdem erfolgt hier keine Statusprüfung des TSL-Signer-Zertifikates. (Der Aufruf von TUC_PKI_006 "OCSP-Abfrage erfolgt in TUC_PKI_001 "Periodische Aktualisierung TI-Vertrauensraum".)
Anwendungsumfeld	System, das die TSL verwendet
Vorbedingungen	TSL-Signer-CA-Zertifikat in einem sicheren Speicher des Systems
Auslöser	TUC_PKI_019 „Prüfung der Aktualität der TSL"
Eingangsdaten	• TSL-Datei • Referenzzeitpunkt (aktuelles Datum)
Komponenten	System
Ausgangsdaten	Status der Prüfung
Referenzen	[ETSI_TS_102_231], [XMLSig]
Standardablauf	1. [System:] Das verwendete TSL-Signer-Zertifikat wird aus der TSL-Datei extrahiert. 2. [System] Prüfung der Extension KeyUsage auf vorhanden sein. Zudem wird die KeyUsage auf die richtige Belegung (nonRepudiation) geprüft. Weiter wird die ExtendedKeyUsage auf die richtige Belegung mit {id-tsl-kp-tslSigning} geprüft (vgl. Kap.5.13.1 TSL-Signer-Zertifikat). 3. [System:] Der Use Case TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats"wird durchlaufen. 4. [System:] Das TSL-Signer-CA-Zertifikat aus dem sicheren Speicher des Systems wird geladen. 5. [System:] Anhand dieses CA-Zertifikates wird die mathematische Prüfung der Signatur des TSL-Signer-Zertifikats durchgeführt (TUC_PKI_004 "Mathematische Prüfung der Zertifikatssignatur"). (Jedes System muss Initial dieses CA-Zertifikat als TI-Vertrauensanker auf sicherem Wege integrieren.) 6. [System:] Ende des Use Case mit Status Rückmeldung

Element	Beschreibung
Varianten/Alternati-ven	
Fehlerfälle	1a. [System:] Das TSL-Signer-Zertifikat lässt sich nicht aus der TSL-Datei extrahieren (TSL_CERT_EXTRACTION_ERROR). 2a. [System:] KeyUsage ist nicht vorhanden bzw. entspricht nicht der vorgesehenen KeyUsage (WRONG_KEYUSAGE). 2a1. [System:] ExtendedKeyUsage entspricht nicht der vorgesehenen ExtendedKeyUsage (WRONG_EXTENDEDKEYUSAGE). 4a. [System:] Das TSL-Signer-CA-Zertifikat kann nicht aus dem sicheren Speicher des Systems geladen werden (TSL_CA_NOT_LOADED). Fehlerfälle sind in den referenzierten Use Cases beschrieben.
Technische Fehlermeldung	Das System meldet entsprechende Fehlercodes. Weitere technische Fehlermeldungen sind in den jeweiligen referenzierten TUCs beschrieben.
Sicherheitsanforde-rungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	Die Gestaltung des sicheren Speichers des Systems ist durch den Betreiber des Systems auszuarbeiten. TUC_PKI_018 "Zertifikatsprüfung in der TI "fordert zusätzlich die Ermittlung von Autorisierungsinformationen. Dies wird im vorliegenden Use Case nicht benötigt und kann entfallen. Der Aufruf von TUC_PKI_006 "OCSP-Abfrage erfolgt nicht hier, sondern in TUC_PKI_001 "Periodische Aktualisierung TI-Vertrauensraum".
Zugehörige Diagramme	Abbildung 13 Aktivitätsdiagramm TUC_PKI_011 "Prüfung des TSL-Signer-Zertifikates"

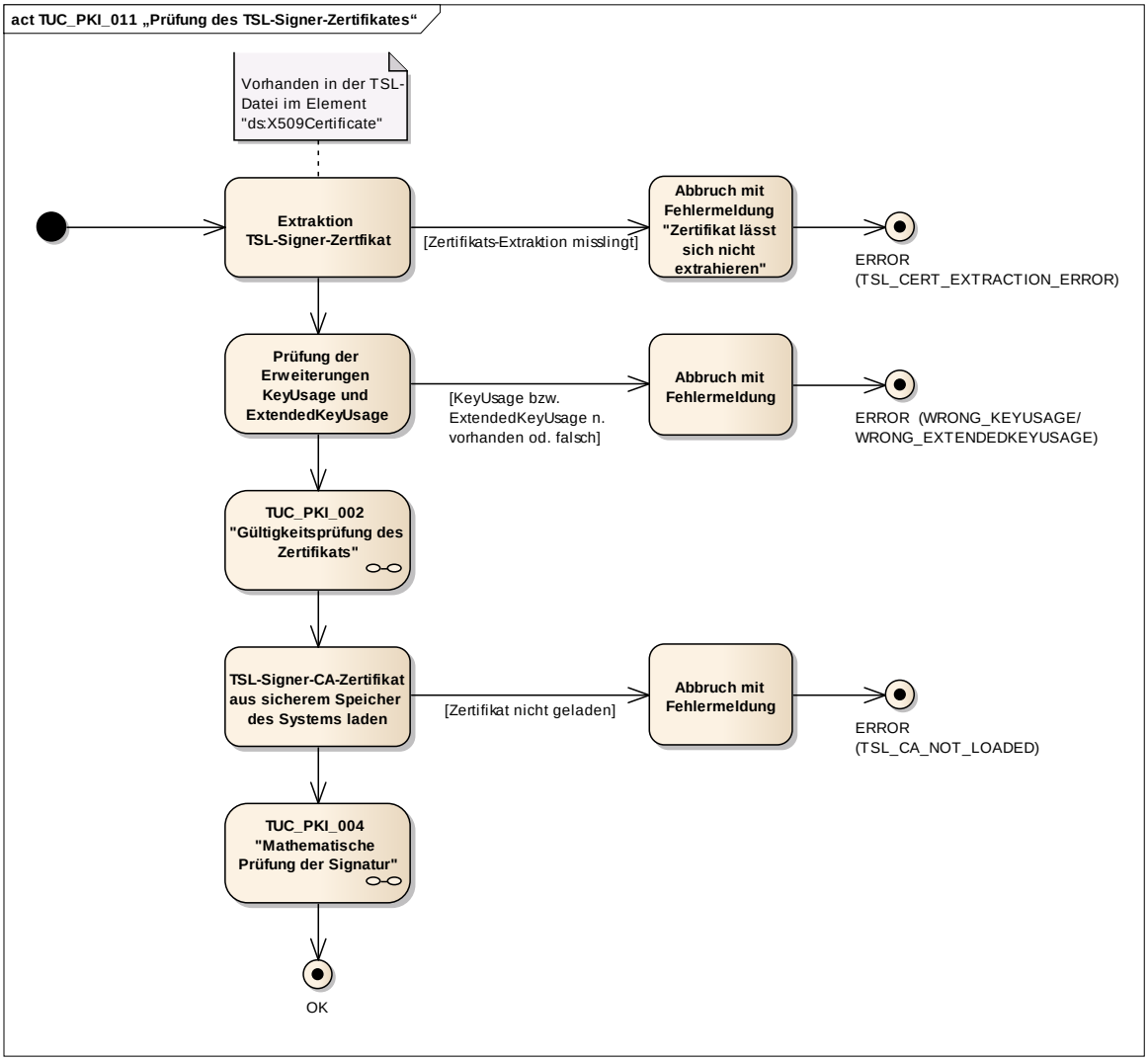

Abbildung 13 Aktivitätsdiagramm TUC_PKI_011 "Prüfung des TSL-Signer-Zertifikates"

8.2.2.4 TUC_PKI_012 „XML-Signatur-Prüfung“

GS-A_4651 TUC_PKI_012: XML-Signatur-Prüfung

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

Tabelle 84: TUC_PKI_012 "XML-Signatur- Prüfung"

Element	Beschreibung
Name	TUC_PKI_012 "XML-Signatur-Prüfung"
Beschreibung	In diesem Use Case wird die Prüfung der XML-Signatur der TSL beschrieben. Die Prüfung wird nicht näher spezifiziert, sondern richtet sich nach den Vorgaben und Standards von W3C.
Anwendungsumfeld	Dieser Use Case umfasst die Prüfung der XML-Signatur und wird durch jedes System verwendet, dass eine XML-Signatur prüfen muss.
Vorbedingungen	TSL-Datei mit Signatur. Das Signaturzertifikat dieser TSL-Datei muss

Element	Beschreibung
	erfolgreich geprüft worden sein. (TUC_PKI_019 und TUC_PKI_011)
Auslöser	XML-Dokument-Prüfung, TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“
Eingangsdaten	signierte XML-Datei und Signaturzertifikat
Komponenten	System
Ausgangsdaten	Status der Prüfung
Referenzen	[XMLSig]
Standardablauf	Der Ablauf richtet sich nach den Vorgaben von W3C.
Fehlerfälle	[System:] Die Signatur ist nicht gültig. Ende des Use Case. Abbruch mit Fehlermeldung (XML_SIGNATURE_ERROR)
Technische Fehlermeldung	Signaturprüfung der TSL-Datei war nicht erfolgreich. (SIGNATUREVERIFICATION_NOT_SUCCESSFUL) Signatur-Zertifikat nicht gültig (TSL_SIGNATURE_NOT_VALID) Weitere Fehlermeldungen befinden sich in den referenzierten Spezifikationen.
Anmerkungen	Vorgaben für die verwendeten Algorithmen und Schlüssellängen der Signatur werden hier nicht getroffen. Siehe dazu [gemSpec_Krypt#GS-A_4371].

8.2.3 TSL-Sicherheitsaspekte

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

8.2.4 TSL-Zeitparameter

GS-A_4897 Gültigkeitsdauer einer TSL

Der TSL-Dienst MUSS die Gültigkeitsdauer der TSL gemäß Tab_PKI_294 umsetzen.

GS-A_4898 TSL-Grace-Period einer TSL

Produkttypen der TI, die die TSL zur Validierung des TI-Vertrauensraums einsetzen, MÜSSEN die TSL-Grace-Period gemäß Tab_PKI_294 umsetzen.

GS-A_4899 TSL Update-Prüfintervall

Produkttypen der TI, die die TSL zur Validierung des TI-Vertrauensraums einsetzen, MÜSSEN gemäß den in Tab_PKI_294 festgelegten TSL-Update Intervall prüfen, ob eine aktuellere als die vom System verwendete TSL bereitgestellt wurde.

GS-A_5214 TSL Neuausstellung

Der TSL-Dienst MUSS mindestens 7 Tage vor Ablauf der Gültigkeit der TSL eine neue Version der TSL erstellen.

Tabelle 85: Tab_PKI_294 TSL Zeitparameter

Beschreibung	Zeitparameter
Gültigkeitsdauer einer TSL	Ausstellungsdatum + 30 Tage
TSL-Grace-Period für zentrale Dienste mit Anschluss an das zentrale Netz	0 Tage
TSL-Grace-Period für sonstige Dienste und Komponenten	0-30 Tage
TSL Update-Prüfintervall	24 Stunden

8.3 Zertifikatsprüfung X.509 nonQES

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

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

Die folgende Use Case Übersicht verdeutlicht die Aktionen des Systems.

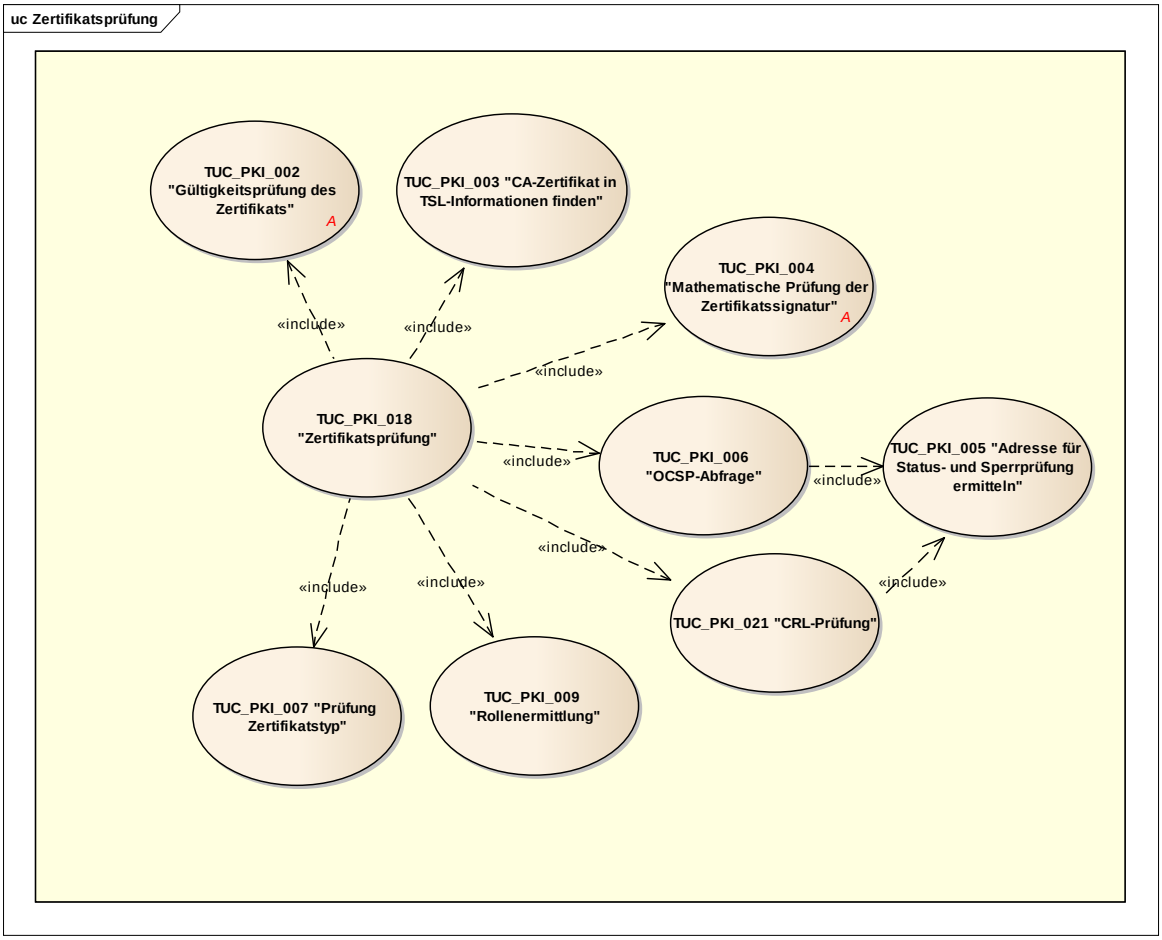

Abbildung 14: Use Case Diagramm "Zertifikatsprüfung"

Die folgenden Schritte sind für eine nonQES-Zertifikatsprüfung durchzuführen:

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

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

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

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

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

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

8.3.1 Zertifikatsprüfung in der TI

8.3.1.1 TUC_PKI_018 "Zertifikatsprüfung in der TI "

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

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

Tabelle 86: TUC_PKI_018 "Zertifikatsprüfung in der TI "

Element	Beschreibung
Name	TUC_PKI_018 "Zertifikatsprüfung"
Beschreibung	Dieser Use Case beschreibt die Prüfung nicht-qualifizierter Zertifikate und umfasst die Offline- wie Online-Prüfung.
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	Etablierter Vertrauensraum der TI in der zertifikatsprüfenden Komponente
Auslöser	Zertifikats-Check
Eingangsdaten	• Das zu prüfende Zertifikat • Referenzzeitpunkt: Zeitpunkt, für den das Zertifikat geprüft werden soll (optional; bei Nichtangabe Verwendung der aktuellen Systemzeit) • PolicyList Liste der im aktuellen Aufruf zulässigen Zertifikatstyp-OIDs. Die Liste muss mindestens eine OID enthalten. • Vorgesehene KeyUsage (intendedKeyUsage, mehrere Werte möglich) • Vorgesehene ExtendedKeyUsage (intendedExtendedKeyUsage, mehrere Werte möglich) • OCSP-Graceperiod (legt bei der Verwendung von OCSP- Antworten den maximal zulässige Zeitraum fest, den die Systemzeit der prüfenden Komponente noch nach dem Zeitpunkt der OCSP- Antwort liegen darf, falls dieser nicht nach dem Referenzzeitpunkt liegt) • Offline-Modus (ja/nein) • Beigefügte OCSP-Response zum angefragten Zertifikat (optional; z.B.

Element	Beschreibung
	in der Signatur eingebettet) • Timeout-Parameter (Default: 10s) • TOLERATE_OCSP_FAILURE (true/false, Default: false) - Der Parameter definiert das Verhalten für den Fall, dass die OCSP-Prüfung nicht durchgeführt werden konnte, weil kein OCSP-Responder implementiert oder der OCSP-Responder technisch nicht erreichbar ist. • Prüfmodus (OCSP, CRL)
Komponenten	System, OCSP-Responder
Ausgangsdaten	Status der Prüfung, OCSP-Response, im Zertifikat enthaltene Rollen-OIDs
Referenzen	[Common-PKI]
Standardablauf	Die Zertifikatsprüfung setzt sich aus folgenden Schritten zusammen: 1. [System] Prüfung der Extension KeyUsage auf vorhanden sein. Zudem wird die KeyUsage und ExtendedKeyUsage (falls vorhanden) auf die richtige Belegung entsprechend der vorgesehenen (intendedKeyUsage bzw. intendedExtendedKeyUsage) KeyUsage geprüft. Die intendedKeyUsage sowie die intendedExtendedKeyUsage können aus einer Liste mehrerer erlaubter Werte bestehen. 2. [System] Die Gültigkeit des Zertifikats wird geprüft (TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats") 3. [System] Das passende CA-Zertifikat wird in den TSL-Informationen gesucht (TUC_PKI_003 "CA-Zertifikat in TSL-Informationen finden") 4. [System] Mathematische Prüfung der Signatur des Zertifikats (TUC_PKI_004 "Mathematische Prüfung der Zertifikatssignatur"). 5. [System] Der ServiceStatus (vgl. Tab_PKI_271) des CA-Zertifikats wird geprüft. Im Fall von „revoked“ wird das Ausgabedatum des End-Entity-Zertifikats mit dem Datum des Statuswechsels (StatusStartingTime) verglichen. Das Ausgabedatum des End-Entity-Zertifikats liegt vor dem Datum des Statuswechsels. 6. [System, Prüfmodus Offline] Falls JA, weiter mit Schritt 9, sonst mit 7. 7. [System, Prüfmodus CRL] Statusinformation zum Zertifikat aus der zugehörigen CRL ermitteln (Tabelle 92: TUC_PKI_021 "CRL-Prüfung") 8. [System, Prüfmodus OCSP] Statusinformation zum Zertifikat durch Abfrage des zugeordneten OCSP-Dienstes ermitteln (TUC_PKI_006 "OCSP-Abfrage") 9. [System:] Ermittlung (TUC_PKI_009 "Rollenermittlung") der Rolle 10.

Element	Beschreibung
	[System:] Prüfung, ob eine der übergebenen Zertifikatstyp-OIDs (aus der Parameter PolicyList) im Zertifikat enthalten ist (TUC_PKI_007 "Prüfung Zertifikatstyp"). Zur Prüfung muss die Liste (PolicyList s.o.) mindestens eine OID enthalten. 11. [System:] Ende des Use Cases mit Rückgabe des/der im Zertifikat enthaltenen Rollen-OID(s).
Varianten/Alternati-ven	6a. [System:] Der Offline-Modus ist aktiviert. Es werden keine Statusinformationen zum Zertifikat eingeholt. 7a. [System, Prüfmodus CRL] Prüfung der Sperrinformation des Zertifikates mittels CRL (TUC_PKI_021 "CRL-Prüfung") 8a. [System] Eine OCSP-Response zu dem zu prüfenden Zertifikat wurde im Aufruf mit übergeben. Falls diese zum Referenzzeitpunkt gültig ist, wird nicht der TUC_PKI_006 aufgerufen, sondern die beigefügte OCSP-Response zur weiteren Prüfung verwendet. 9a. [System:] Abbruch und Rückmeldung. Kein Element PolicyIdentifier vorhanden (CERT_TYPE_INFO_MISSING).
Fehlerfälle	1a. [System:] KeyUsage ist nicht vorhanden bzw. entspricht nicht der vorgesehenen KeyUsage (WRONG_KEYUSAGE). 1a1. [System:] ExtendedKeyUsage entspricht nicht der vorgesehenen ExtendedKeyUsage (WRONG_EXTENDEDKEYUSAGE). 5a. [System:] Das Ausgabedatum des End-Entity-Zertifikats liegt nach dem Datum des Statuswechsels. Abbruch mit Fehlermeldung (CA_CERTIFICATE_REVOKED_IN_TSL) 7a. [System] Eine OCSP-Response zu dem zu prüfenden Zertifikat wurde im Aufruf mit übergeben, ergab bei den weiteren Prüfschritten jedoch kein gültiges Ergebnis (Überprüfung und Auswertung der Gültigkeit der OCSP-Response in TUC_PKI_006 schlägt fehl). Eine erneute Prüfung wird in diesem Fall durch Aufruf des TUC_PKI_006 durchgeführt, als wäre keine OCSP-Response beigefügt. In den Rückgabewerten dieses TUC wird die Warnmeldung (PROVIDED_OCSP_RESPONSE_NOT_VALID) an die aufrufende Funktion übergeben. 9a. [System:] Zertifikatstyp-OID stimmt nicht überein (CERT_TYPE_ERROR). Weitere Fehlerfälle werden in den jeweiligen referenzierten TUCs beschrieben.
Technische Fehlermeldung	Das System meldet entsprechende Fehlercodes. Weitere technische Fehlermeldungen sind in den jeweiligen referenzierten TUCs beschrieben.

Element	Beschreibung
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Zugehörige Diagramme	Abbildung 15: Aktivitätsdiagramm TUC_PKI_018 "Zertifikatsprüfung"

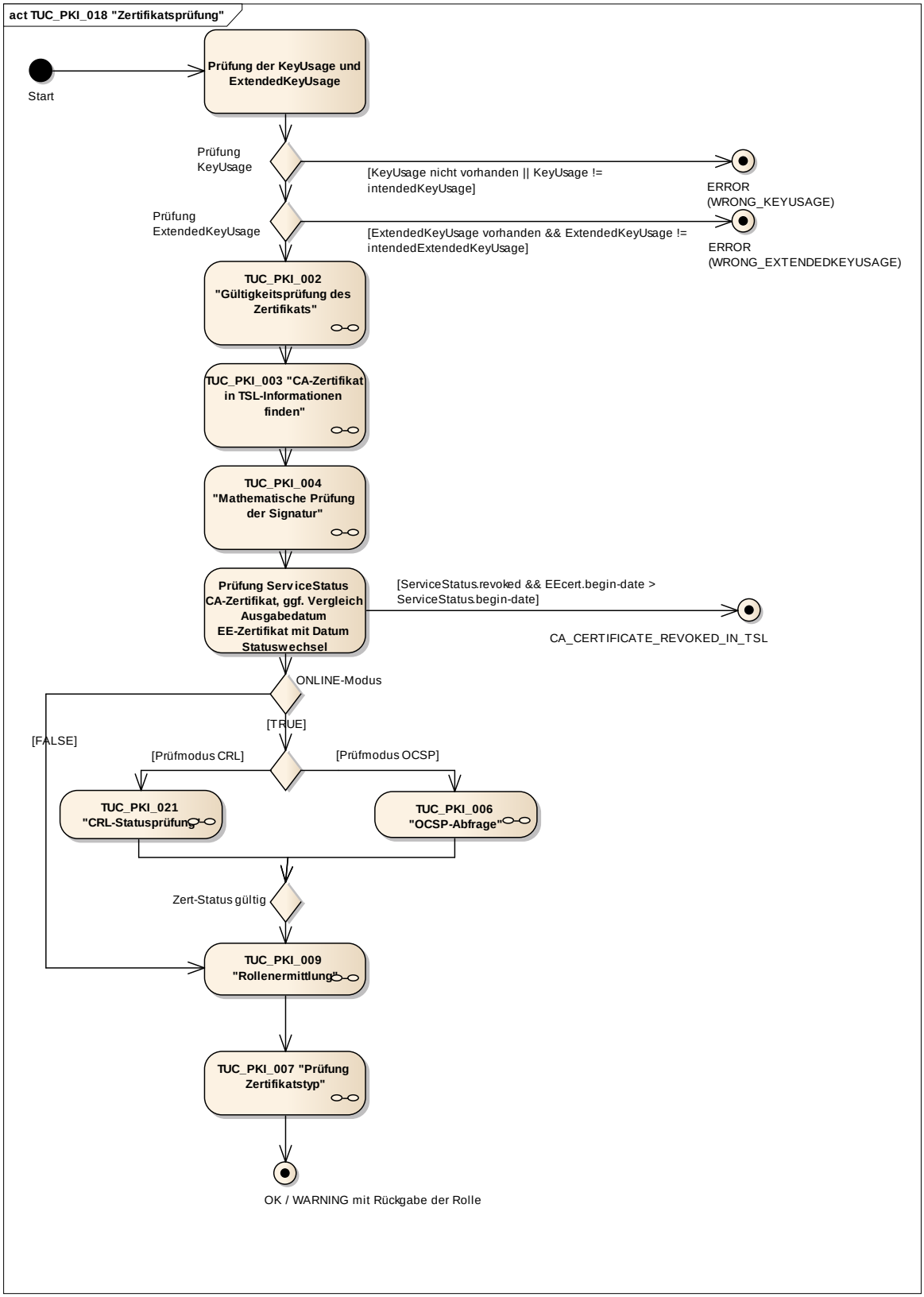

Abbildung 15: Aktivitätsdiagramm TUC_PKI_018 "Zertifikatsprüfung"

8.3.1.2 TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats"

GS-A_4653 TUC_PKI_002: Gültigkeitsprüfung des Zertifikats

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

Tabelle 87: TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats"

Element	Beschreibung
Name	TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats"
Beschreibung	Dieser Use Case beschreibt die Prüfung des Zertifikats auf seine aktuelle zeitliche Gültigkeit. Damit ist der Zeitraum gemeint, der im Zertifikat steht.
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	Zertifikat vorhanden
Auslöser	TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“, Geplanter Wechsel TI-Vertrauensanker, TUC_PKI_018 "Zertifikatsprüfung in der TI "
Eingangsdaten	• Das zu prüfende Zertifikat • Referenzzeitpunkt
Komponenten	System
Ausgangsdaten	Status der Prüfung
Referenzen	[Common-PKI]
Standardablauf	1. [System:] Zertifikat lesen 2. [System:] Aus dem Zertifikat das Feld Validity ermitteln und auslesen. 3. [System:] Anhand der ermittelten Daten wird die Gültigkeit geprüft. Dabei kommt folgender Algorithmus zu tragen: notBefore < Referenzzeitpunkt && notAfter > Referenzzeitpunkt entspricht einem zeitlich gültigem Zertifikat 4. [System:] Rückmeldung des Status
Fehlerfälle	1a. [System:] Zertifikat ist nicht lesbar (CERT_READ_ERROR). 3a. [System:] Prüfzeitpunkt nicht innerhalb der Gültigkeitsdauer des Zertifikats (CERTIFICATE_NOT_VALID_TIME).
Technische Fehlermeldung	Das Zertifikat ist zum Referenzzeitpunkt nicht gültig (CERTIFICATE_NOT_VALID_TIME) Das System meldet entsprechende Fehlercodes.
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.

Anmerkungen	Aufbau der Gültigkeit:
	`Validity ::= SEQUENCE {`
	`notBefore Time,`
	`notAfter Time }`

Zugehörige	Abbildung 16: Aktivitätsdiagramm TUC_PKI_002 Gültigkeitsprüfung des

Element	Beschreibung
Diagramme	Zertifikats

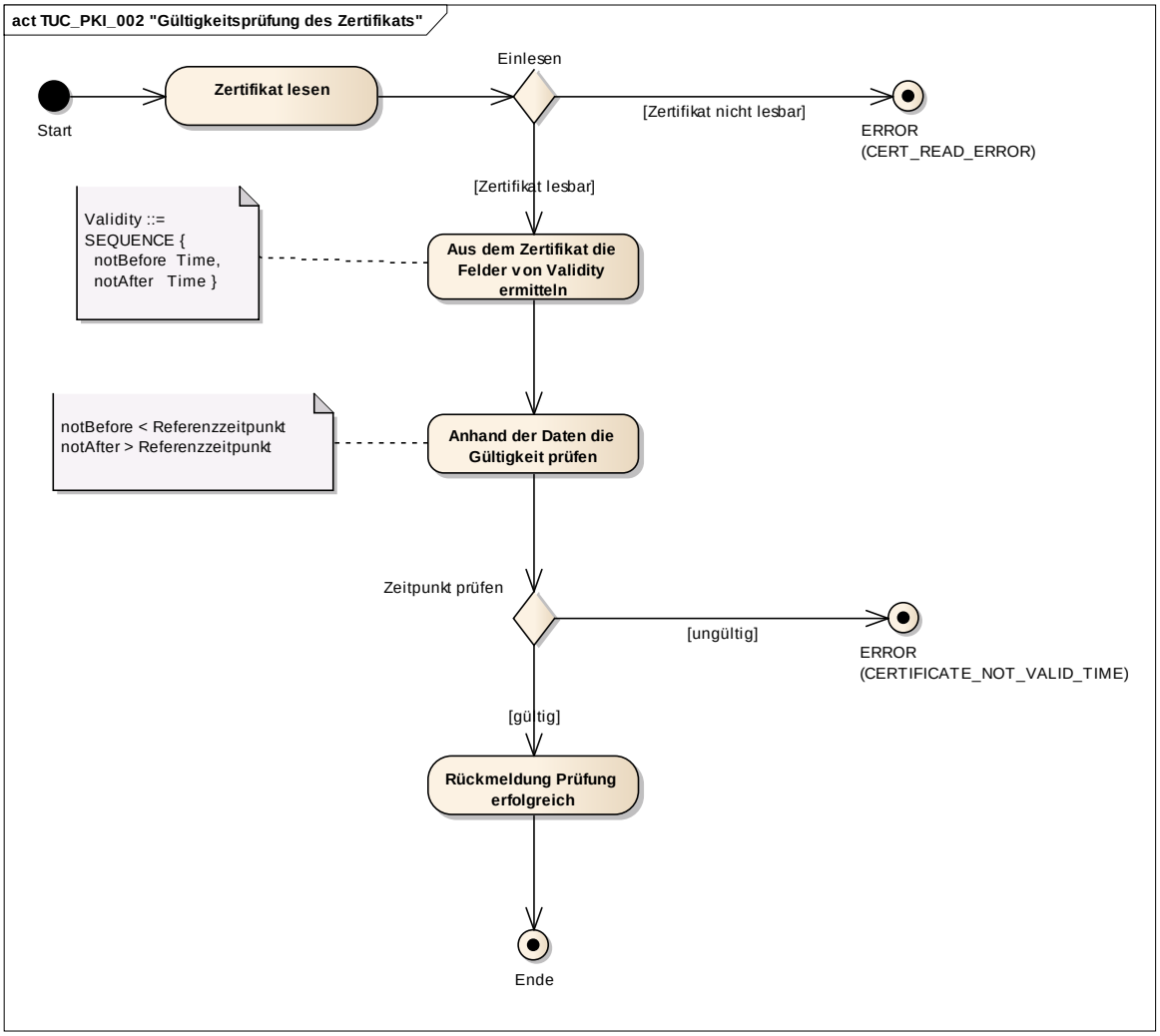

Abbildung 16: Aktivitätsdiagramm TUC_PKI_002 Gültigkeitsprüfung des Zertifikats

8.3.1.3 TUC_PKI_003 "CA-Zertifikat in TSL-Informationen finden"

⌦ GS-A_4654 TUC_PKI_003: CA-Zertifikat finden

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

Tabelle 88: TUC_PKI_003 "CA-Zertifikat in TSL-Informationen finden"

Element	Beschreibung
Name	TUC_PKI_003 "CA-Zertifikat in TSL-Informationen finden"
Beschreibung	Anhand der Daten aus dem Zertifikat wird versucht das CA-Zertifikat in der TSL zu finden.

Element	Beschreibung
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	Zertifikat innerhalb des definierten Gültigkeitszeitraums Eine TSL mit gültiger Signatur
Auslöser	TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln", Zertifikatsprüfung in der TI, TUC_PKI_018 "Zertifikatsprüfung in der TI "
Eingangsdaten	End-Entity-Zertifikatsdaten, TSL-Informationen
Komponenten	System
Ausgangsdaten	Status der Prüfung, (Referenz auf) CA-Zertifikat
Referenzen	[Common-PKI]
Standardablauf	1. [System:] Anhand der End-Entity-Zertifikatsdaten werden die TSL-Informationen durchsucht, um das passende CA-Zertifikat zu finden. 2. [System:] Vergleich 1: IssuerDN des End-Entity-Zertifikats mit dem subjectDN des CA-Zertifikats 3. [System:] Vergleich 2: AuthorityKeyIdentifier des End-Entity-Zertifikats mit SubjectKeyIdentifier des CA-Zertifikats 4. [System:] Selektion (Referenz auf) CA-Zertifikat und Rückgabe
Varianten/Alternativen	2a. [System:] Keine Übereinstimmung. Der Vorgang wird mit einem anderen CA-Zertifikat wiederholt (Iteration)
Fehlerfälle	2b. [System:] Ende der Liste erreicht UND keine Übereinstimmung im DN gefunden. Abbruch des TUC mit Fehlermeldung (CA_CERT_MISSING) 3a. [System:] CA mit passendem DN gefunden, aber Ausstellerschlüssel (SubjectKeyIdentifier) und die Referenz (AuthorityKeyIdentifier) stimmen nicht überein. Abbruch des TUC mit Fehlermeldung (AUTHORITYKEYID_DIFFERENT)
Technische Fehlermeldung	Das System meldet entsprechende Fehlercodes.
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	
Zugehörige Diagramme	Abbildung 17: Aktivitätsdiagramm TUC_PKI_003 CA-Zertifikat in TSL-Informationen finden

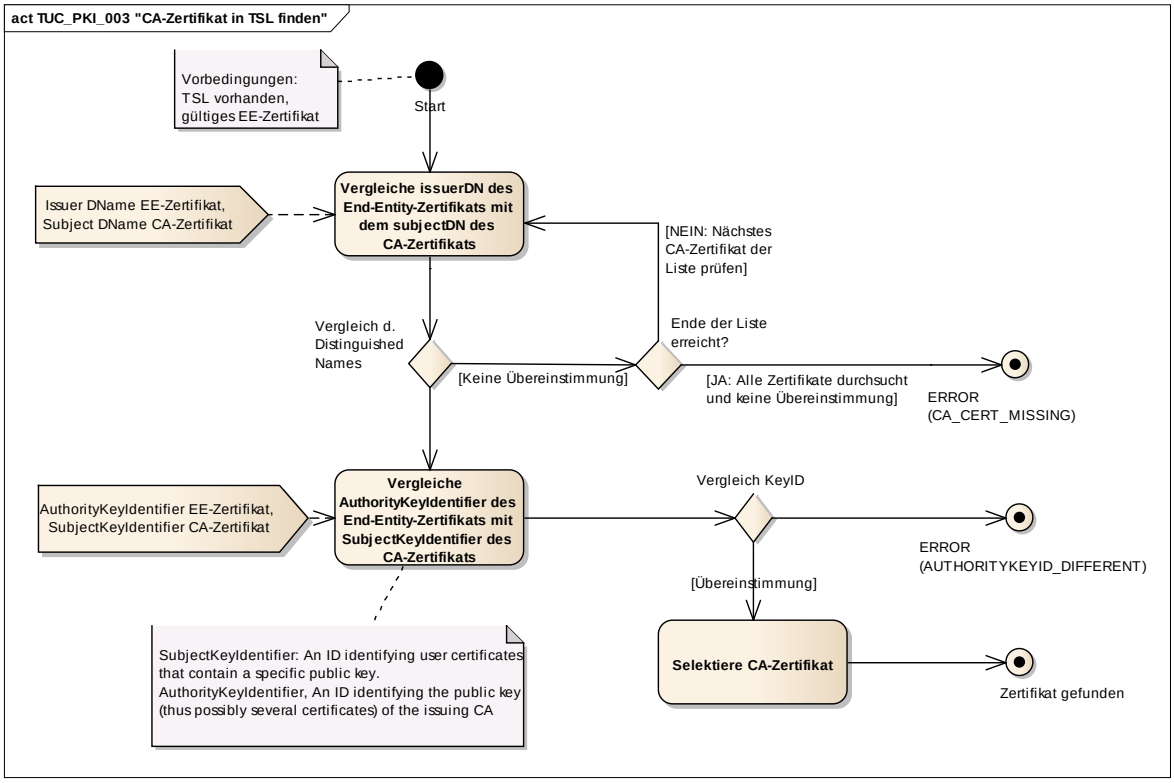

Abbildung 17: Aktivitätsdiagramm TUC_PKI_003 CA-Zertifikat in TSL-Informationen finden

8.3.1.4 TUC_PKI_004 "Mathematische Prüfung der Zertifikatssignatur"

⌦ GS-A_4655 TUC_PKI_004: Mathematische Prüfung der Zertifikatssignatur

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

Tabelle 89: TUC_PKI_004 "Mathematische Prüfung der Zertifikatssignatur"

Element	Beschreibung
Name	TUC_PKI_004 "Mathematische Prüfung der Zertifikatssignatur"
Beschreibung	Dieser Use Case beschreibt die mathematische Prüfung der Signatur des End-Entity-Zertifikats mit Hilfe des CA-Zertifikats.
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	Gültiges CA-Zertifikat und passendes End-Entity-Zertifikat innerhalb des definierten Gültigkeitszeitraums
Auslöser	TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“, Geplanter Wechsel TI-Vertrauensanker, TUC_PKI_018 "Zertifikatsprüfung in der TI "
Eingangsdaten	End-Entity-Zertifikat, CA-Zertifikat
Komponenten	System
Ausgangsdaten	Status der Prüfung
Referenzen	[Common-PKI]
Standardablauf	1.

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

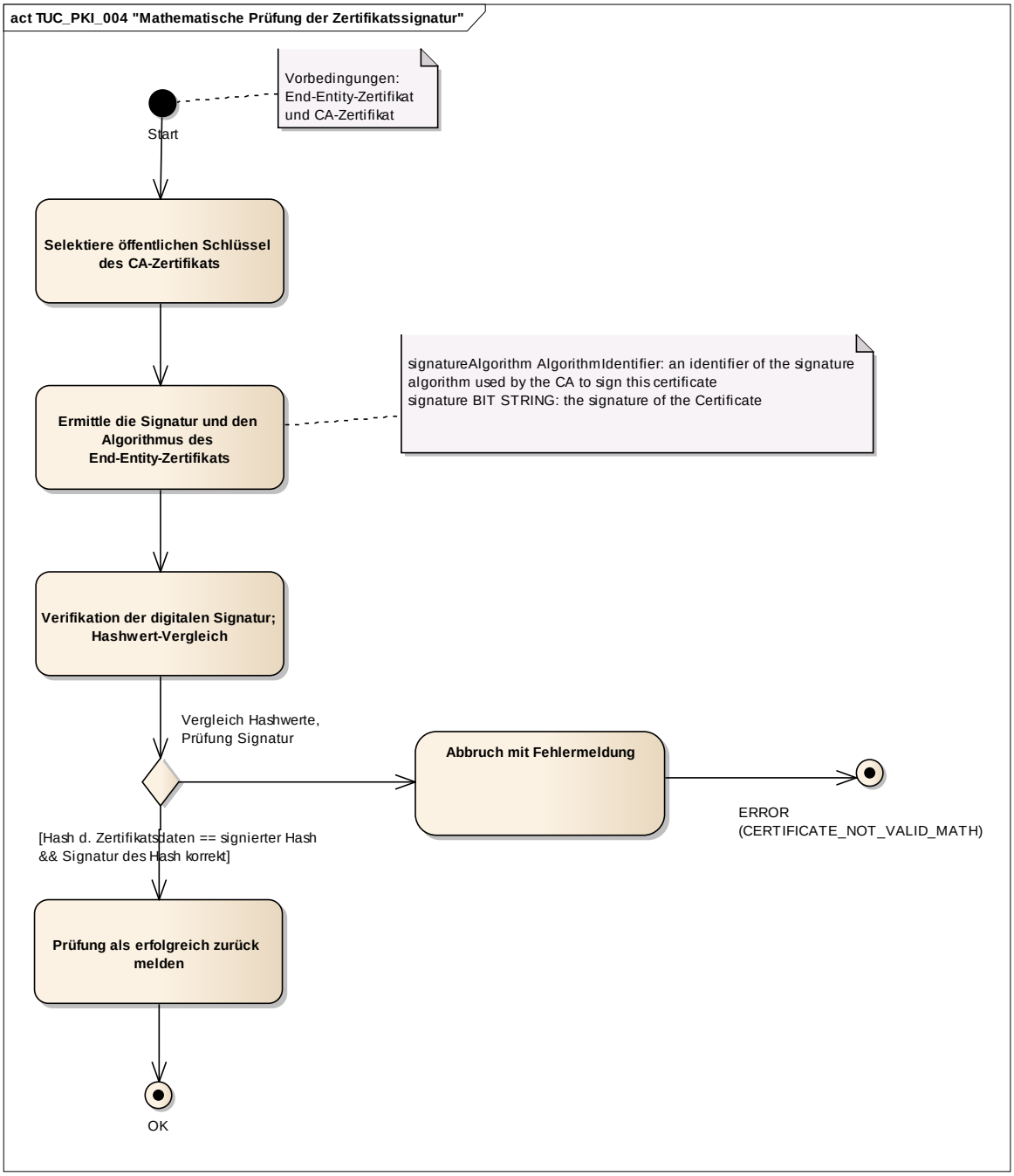

Abbildung 18: Aktivitätsdiagramm TUC_PKI_004 Mathematische Prüfung der Zertifikatssignatur

8.3.2 Statusprüfung

8.3.2.1 TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln"

GS-A_4656 TUC_PKI_005: Adresse für Status- und Sperrprüfung ermitteln

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_005 zur Ermittlung der Adresse für Status- und Sperrprüfung umsetzen.

Tabelle 90: TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln"

Element	Beschreibung
Name	TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln"
Beschreibung	In diesem Use Case wird die Ermittlung der Adresse für Status- und Sperrprüfung beschrieben. Default-mäßig handelt es sich dabei um die Adresse des OCSP-Responders, alternativ um diejenige des CRL-Downloadpunktes. Hierbei wird auf die TSL-Informationen zurückgegriffen. Die Adresse ist im CA-Eintrag der TSL hinterlegt. Für das Verhalten in spezifizierten Offline-Szenarien gilt [GS-A_4658].
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	Eine TSL mit gültiger Signatur
Auslöser	TUC_PKI_006 "OCSP-Abfrage"oder TUC_PKI_021 "CRL-Prüfung"
Eingangsdaten	• End-Entity-Zertifikatsdaten • TSL-Informationen
Komponenten	System
Ausgangsdaten	OCSP-Adresse oder Adresse des CRL-Downloadpunktes
Standardablauf	1. [System:] (Referenz auf) CA-Zertifikat in TSL-Informationen finden (TUC_PKI_003 "CA-Zertifikat in TSL-Informationen finden") 2. [System:] Das Element "ServiceSupplyPoint" (bzw. via referenziertes CA-Zertifikat die Referenz auf den bezeichneten Statusprüfdienst- oder CRL Downloadpunkt) auswählen und URI selektieren. 3. [System:] Adresse zurückmelden
Fehlerfälle	2a. [System:] Das Element "ServiceSupplyPoint" konnte nicht gefunden werden oder enthält keinen URI (SERVICESUPPLYPOINT_MISSING). Weitere Fehlerfälle werden in den jeweiligen referenzierten TUCs beschrieben.
Technische Fehlermeldung	CA kann nicht in den TSL-Informationen ermittelt werden. (CA_CERT_MISSING) Das System meldet entsprechende Fehlercodes. Weitere technische Fehlermeldungen sind in den jeweiligen referenzierten TUCs beschrieben.
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	Die Adresse des Statusprüfdienstes oder des CRL-Downloadpunktes muss nicht zwingend in der TSL-Datei vorgehalten werden, sondern kann z.B. im Truststore des Systems gespeichert und aufgerufen werden.
Zugehörige Diagramme	Abbildung 19 Aktivitätsdiagramm TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln "

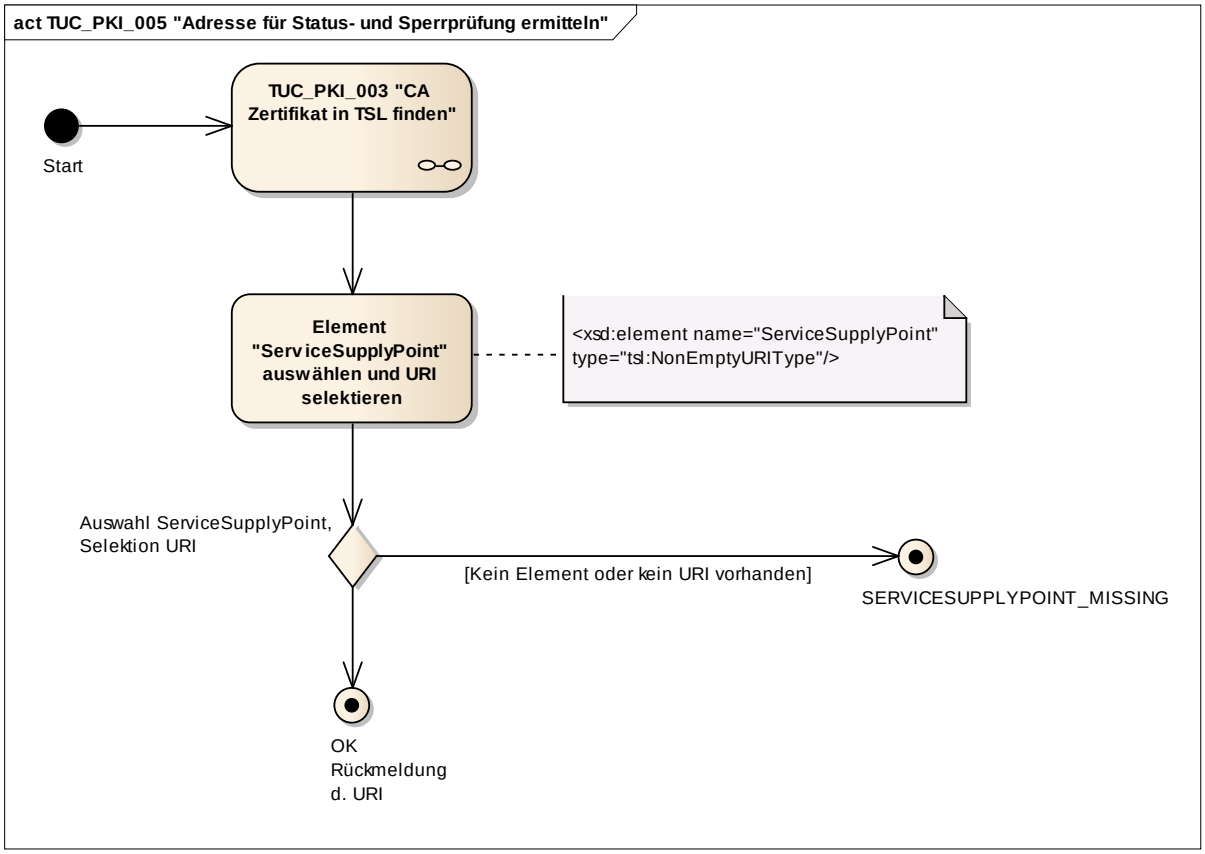

Abbildung 19 Aktivitätsdiagramm TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln "

8.3.2.2 TUC_PKI_006 "OCSP-Abfrage"

GS-A_4657 TUC_PKI_006: OCSP-Abfrage

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

Tabelle 91: TUC_PKI_006 "OCSP-Abfrage"

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

Element	Beschreibung
	TSL-Informationen sind vorhanden.
Auslöser	Zertifikats-Check
Eingangsdaten	• End-Entity-Zertifikatsdaten • CA-Zertifikatsdaten • TSL-Informationen • Referenzzeitpunkt • OCSP-Graceperiod (Default: 10min) • Timeout-Parameter (Default: 10s) • TOLERATE_OCSP_FAILURE (true/false, Default: false) • ENFORCE_CERTHASH_CHECK (true/false, Default: false)
Komponenten	System, OCSP-Responder
Ausgangsdaten	Status der Prüfung OCSP-Response
Referenzen	[Common-PKI] Part 4#3
Standardablauf	1. [System:] Prüfung, ob (zum Referenzzeitpunkt unter Berücksichtigung der OCSP-Graceperiod) gültige Statusinformationen bereits vorliegen (z.B. im lokalen Cache bereitgestellt). 2. [System:] Ermittlung der OCSP-Adresse (TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln") 3. [System:] Aufbau des OCSP-Request anhand der passenden Zertifikatsdaten 4. [System:] Absenden des Request an die ermittelte Adresse Der Timeout-Parameter definiert hier, zu welchem Zeitpunkt das System ein Timeout bei Nichterreichbarkeit des Dienstes meldet. 5. [System, OCSP-Responder:] Überprüfung der OCSP-Response (Signatur) auf Integrität. Das dazu benötigte OCSP-Responder-Zertifikat in den TSL-Informationen ermitteln. Die OCSP-Responder-Zertifikate sind alle in den TSL-Informationen enthalten. Somit kann direkt nach dem Zertifikat gesucht werden. (OCSP-Responder sind in der TSL-Datei mit dem „ServiceTypeIdentifier“ "http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP" markiert.) 6. [System:] Auswertung der OCSP-Response. Details siehe [Common-PKI#Part4#3] 7. [System:] Wenn ENFORCE_CERTHASH_CHECK auf ´true´ gesetzt ist, wird das End-Entity-Zertifikat mit dem in der certHash-Erweiterung bezeichneten Algorithmus gehasht (vgl. [gemSpec_Krypt#GS-A_4393]). Das Resultat stimmt mit dem gelieferten certificateHash überein. Details siehe [Common-PKI#Part4#3.1.2] und [Common-PKI#Part5#2.3]. 8. [System:] Überprüfung der Gültigkeit anhand des Referenzzeitpunkts. Der CertStatus "good“ wird gemeldet.

Element	Beschreibung
	9. [System:] Rückmeldung, dass das Zertifikat gültig ist und Rückgabe der OCSP-Response. 10. [System:] Ende des UseCase
Varianten/Alternati-ven	2a. [System:] Prüfung der Gültigkeit des Zertifikats gegen vorliegende Informationen. 2a1. [System:] Zertifikat ist gesperrt. Weiter mit Schritt 5, falls die entsprechenden Prüfungen nicht bereits erfolgt sind. Ansonsten Rückmeldung analog 8. 2a2. Die Statusinformationen sind zu alt (Zertifikat nicht gesperrt && (Referenzzeit > Statusinfo.producedAt && (Systemzeit - Statusinfo.producedAt) > OCSP-Graceperiod)). Neue Informationen müssen eingeholt werden. Es geht weiter mit Schritt 2 (Standardablauf). 2a3. [System:] Zertifikat ist nicht gesperrt und Referenzzeitpunkt <= Datum der Statusinformationen (producedAt) des Zertifikats oder (Systemzeit - Statusinfo.producedAt) <= OCSP-Graceperiod. Rückmeldung: Zertifikat ist gültig. 7a. [System:] ENFORCE_CERTHASH_CHECK ist auf ´false´ gesetzt. Weiter mit nächstem Schritt 8a. [System:] Das Zertifikat ist für den Referenzzeitpunkt gültig, obwohl der CertStatus "revoked“ gemeldet wird, da "revocationTime“ > Referenzzeitpunkt. Rückmeldung Zertifikat ist für den Referenzzeitpunkt gültig und Rückgabe der OCSP-Response. 8b. [System:] Zertifikat ist gesperrt und die Referenzzeit liegt nach dem Sperrzeitpunkt (CertStatus revoked UND revocationTime <= des Referenzzeitpunkts). Rückmeldung Zertifikat ist gesperrt und Rückgabe der OCSP-Response. (CERT_REVOKED) 8c. [System:] Zertifikat ist unbekannt (Status unknown) Rückmeldung, dass das Zertifikat ungültig ist und Rückgabe der OCSP-Response.. (CERT_UNKNOWN)
Fehlerfälle/War-nungen	4a. [System:] Die OCSP-Prüfung konnte nicht durchgeführt werden: Im Falle von TOLERATE_OCSP_FAILURE=true wird als Ergebnis eine Warnung generiert (OCSP_CHECK_REVOCATION_FAILED). 4b. [System:] Die OCSP-Prüfung konnte nicht durchgeführt werden: Im Falle von TOLERATE_OCSP_FAILURE=false wird mit einer Fehlermeldung abgebrochen. (OCSP_CHECK_REVOCATION_ERROR) 5a. [System:] OCSP-Zertifikat nicht in TSL-Informationen enthalten. Abbruch mit Fehlermeldung. (OCSP_CERT_MISSING) 5a1.

Element	Beschreibung
	[System:] Signatur der Response ist nicht gültig. Abbruch mit Fehlermeldung (OCSP_SIGNATURE_ERROR) 6a. [System:] Die Response enthält einen Statuscode („OCSPResponseStatus“), der ungleich 0 (für „successful“) ist. (Damit zeigt der OCSP-Responder eine Exception an. Z. B. kann der Wert für den Status auf 3 für „tryLater“ gesetzt sein.) Abbruch mit Fehlermeldung (OCSP_STATUS_ERROR) 7b. ENFORCE_CERTHASH_CHECK ist auf ´true´ gesetzt und die OCSP-Response enthält keine certHash-Erweiterung. (CERTHASH_EXTENSION_MISSING) 7c. Der errechnete Zertifikats-Hash stimmt nicht mit demjenigen aus der in der Erweiterung certHash überein. (CERTHASH_MISMATCH)
Technische Fehlermeldung	Der OCSP-Responder ist nicht verfügbar. (OCSP_NOT_AVAILABLE) OCSP-Responder-Zertifikat steht nicht in der TSL. (OCSP_CERT_MISSING) Die OCSP-Response enthält eine Exception-Meldung. (OCSP_STATUS_ERROR) certHash-Erweiterung fehlt. (CERTHASH_EXTENSION_MISSING) Nicht übereinstimmende Zertifikats-Hashes (CERTHASH_MISMATCH) Das System meldet entsprechende Fehlercodes. Weitere technische Fehlermeldungen sind in den jeweiligen referenzierten TUCs beschrieben.
Sicherheitsanforde-rungen	Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.
Anmerkungen	Der genaue Aufbau des OCSP-Requests und der OCSP-Response ist in Kapitel 9 spezifiziert. Zur Abfrage beim OCSP-Responder MUSS ein Timeout-Parameter konfiguriert werden können. Dieser definiert, zu welchem Zeitpunkt das System ein Timeout bei Nichterreichbarkeit des Dienstes meldet.
Zugehörige Diagramme	Abbildung 20: Aktivitätsdiagramm TUC_PKI_006 "OCSP-Abfrage"

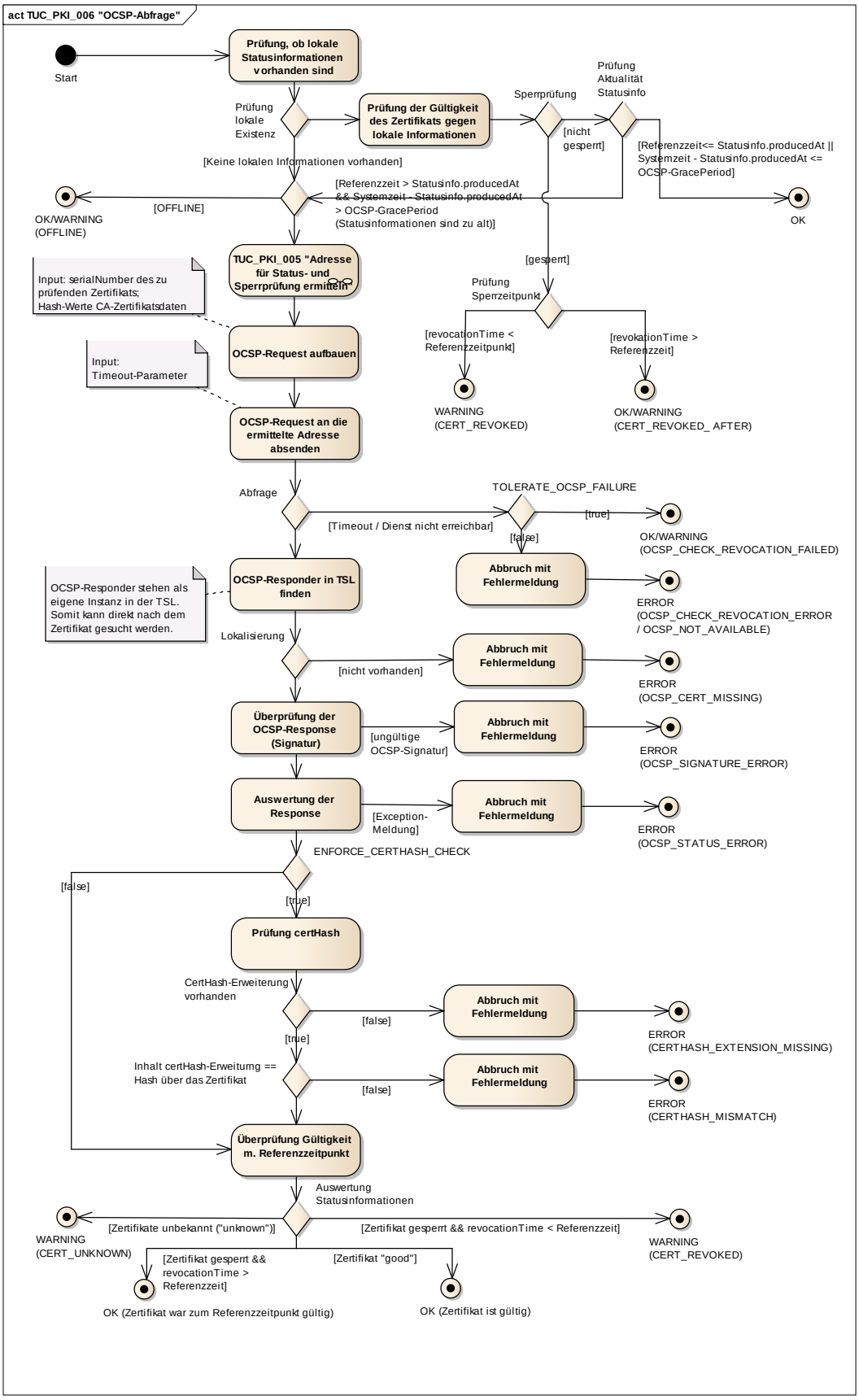

Abbildung 20: Aktivitätsdiagramm TUC_PKI_006 "OCSP-Abfrage"

8.3.2.3 TUC_PKI_021 "CRL-Prüfung"

⌦ GS-A_4900 TUC_PKI_021 "CRL-Prüfung"

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

Tabelle 92: TUC_PKI_021 "CRL-Prüfung"

Element	Beschreibung
Name	TUC_PKI_021 "CRL-Prüfung"
Beschreibung	Dieser Use Case beschreibt den Prozess zur Validierung einer CRL (Certificate Revocation List) sowie den Prozess zur Ermittlung der Sperrinformationen zu einem End-Entity-Zertifikat mittels einer CRL .
Anwendungsumfeld	Use Case für den Anwendungsfall zur Prüfung der Sperrinformationen eines End-Entity-Zertifikats.
Vorbedingungen	Ein End-Entity-Zertifikat (mathematisch und zeitlich gültig) Eine CRL ist vorhanden oder kann heruntergeladen werden.
Auslöser	TUC_PKI_018 "Zertifikatsprüfung in der TI "
Eingangsdaten	CRL End-Entity-Zertifikatsdaten (Zertifikats-Seriennummer, CertificateIssuer) Timeout-Parameter (alternativ zu CRL) CRL-Downloadpunkt-Adresse (optional, alternativ zu CRL)
Komponenten	System (nur Konnektor)
Ausgangsdaten	Status der Prüfung
Referenzen	[COMMON-PKI#Part1#4], [COMMON-PKI#Part5#2.3], [RFC5280#5.2.5.], [RFC5280#5.3.3.]
Standardablauf	1. [System:] Selektion der CRL 2. [System:] Prüfen der zeitlichen Gültigkeit der CRL (Systemzeit < crl.NextUpdate) 3. [System:] Auswertung der Art der CRL. Es wird anhand der IssuingDistributionPoint-Erweiterung in der Sperrliste (CRL) geprüft, ob es sich um eine indirekte CRL handelt (indirectCRL-bit). 4. [System:] Für eine indirekte CRL wird das zugehörige CRL-Signer-Zertifikat in den TSL-Informationen ermittelt. In der TSL-Datei ist der CRL-Signer mit „http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL“ im Element ServiceTypeIdentifier gekennzeichnet. 5. [System:] Prüfung der Signatur der CRL 6. [System:] Auswertung der CRL-Einträge. Es wird nach der Zertifikatsseriennummer des zu überprüfenden End-Entity-Zertifikats in der CRL gesucht. 7.

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

Element	Beschreibung
	6a. [System:] Die CRL ist fehlerhaft aufgebaut und kann nicht geprüft werden. 7a. [System:] Die CRL ist fehlerhaft aufgebaut und ihre Einträge können nicht ausgewertet werden. 8b. [System:] Die CRL-Einträge sind fehlerhaft aufgebaut und können nicht weiter geprüft werden.
Technische Fehlermeldung	1a3a. [System:] Fehlermeldung CRL_DOWNLOAD_ERROR 2a. [System:] Fehlermeldung CRL_OUTDATED_ERROR. 4b. [System:] Fehlermeldung CRL_SIGNER_CERT_MISSING 5a. [System:] Fehlermeldung CRL_SIGNATURE_ERROR 6a. [System:] Fehlermeldung CRL_CHECK_ERROR 7a. [System:] Fehlermeldung CRL_CHECK_ERROR 8b. [System:] Fehlermeldung CRL_CHECK_ERROR
Anmerkungen, Bemerkungen	Dieser TUC kommt z.B. bei der Konzentrator-Zertifikatsprüfung zur Anwendung. Der Downloadpunkt der CRL ist aus dem Internet erreichbar. Als Übertragungsprotokoll für den allfälligen Download ist "HTTP“ zu verwenden. Aufbau CRL nach [COMMON-PKI#Part1#4] (als indirekte CRL) Die Schritte 1-5 beinhalten die Validierung der CRL. Diese können vorgängig durchgeführt werden und müssen also nicht bei jeder einzelnen CRL-Prüfung eines End-Entity-Zertifikats durchlaufen werden, solange gewährleistet ist, dass die CRL zeitlich gültig ist.
Zugehörige Diagramme	Abbildung 21: Aktivitätsdiagramm TUC_PKI_021 "CRL-Prüfung"

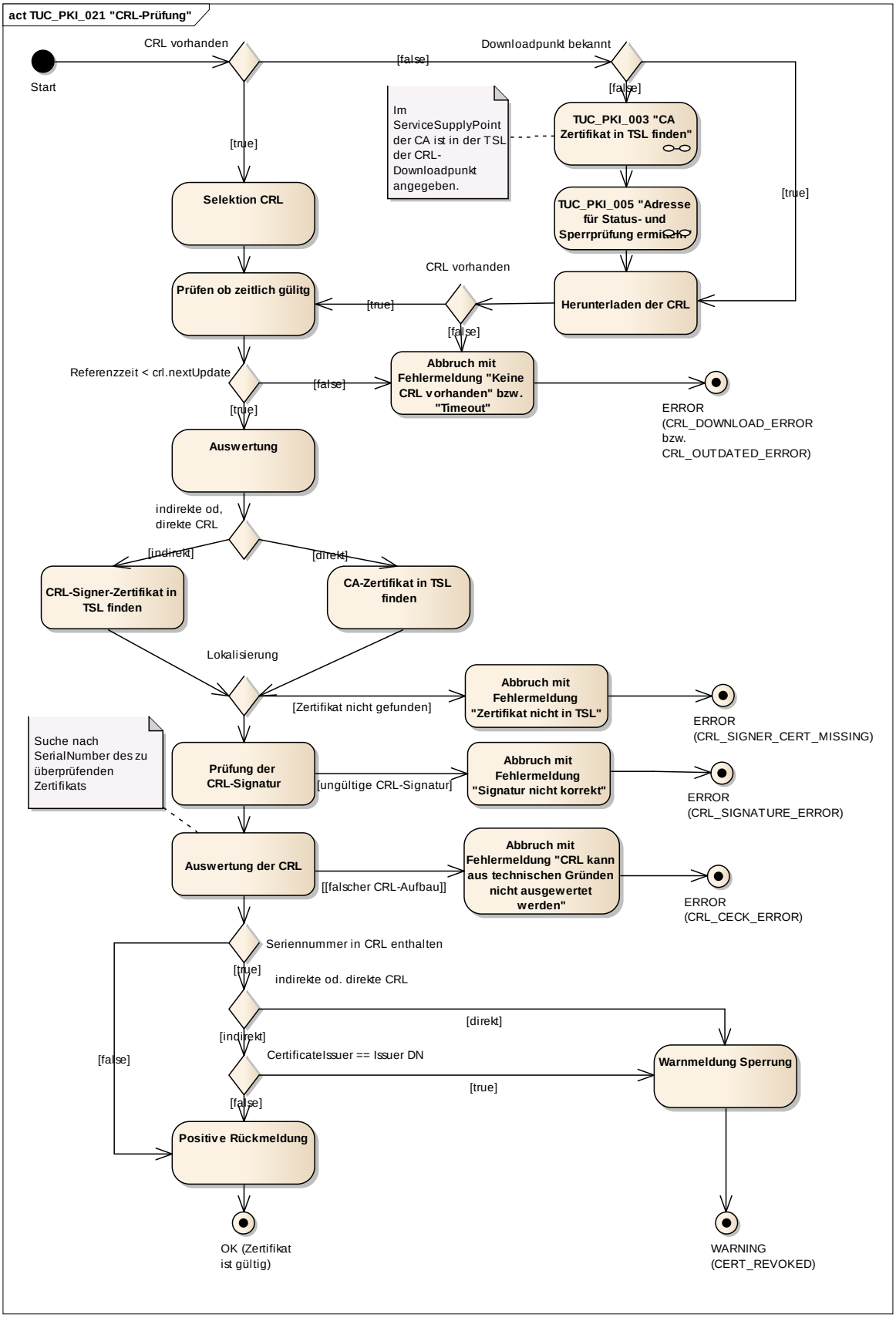

Abbildung 21: Aktivitätsdiagramm TUC_PKI_021 "CRL-Prüfung"

8.3.2.4 Szenarien für Offline und Timeout von OCSP

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

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

Die Produkttypen der TI, die Zertifikate prüfen und per Spezifikation ihre Funktionen zeitweise oder ständig offline von der TI erbringen, MÜSSEN für die explizit spezifizierten Offline-Szenarien bei der Zertifikatsprüfung die TUCs *TUC_PKI_005 OCSP-Adresse ermitteln* und *TUC_PKI_006 OCSP-Abfrage* auslassen.⌫

⌦ **GS-A_4659 Zertifikatsprüfung bei Nichterreichbarkeit des OCSP**

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN für die explizit spezifizierten Szenarien für Nichterreichbarkeit des OCSP-Responders die Zertifikatsprüfung fortführen, auch wenn im TUC *TUC_PKI_006 OCSP-Abfrage* keine OCSP-Response ermittelt werden konnte .⌫

8.3.2.5 Statusprüfung von eGK-Zertifikaten

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

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

Die Produkttypen der TI, die Zertifikate der elektronischen Gesundheitskarte (eGK) prüfen, DÜRFEN NICHT OCSP-Responses für die Statusprüfung verwenden, deren Alter die OCSP-Graceperiod (maximale Caching-Dauer) übersteigt. Dies beinhaltet auch OCSP-Responses, die den Status „revoked“ enthalten. ⌫

8.3.3 Ermittlung von Autorisierungsinformationen

8.3.3.1 Bestätigte Zertifikatsinformationen

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

- Zertifikatstypen
- Die Rolle der Zertifikatsidentität

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

8.3.3.2 TUC_PKI_009 "Rollenermittlung"

⌦ **GS-A_4660 TUC_PKI_009: Rollenermittlung**

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

Tabelle 93: TUC_PKI_009 "Rollenermittlung"

Element	Beschreibung
Name	TUC_PKI_009 "Rollenermittlung"
Beschreibung	Die Rolle einer Identität steht im jeweiligen Zertifikat. Dieser Use Case beschreibt die Ermittlung dieser Rolle aus dem Zertifikat. Jede Rolle wird in der Struktur `professionInfo` als OID gespeichert (siehe Kap 4.4, 4.5, 4.6). In allen Zertifikaten, die eine Rolle besitzen, steht diese in der Extension Admission, aus welcher der OID ausgelesen wird.
Anwendungsumfeld	System, das spezifische Inhalte von Zertifikaten verwendet
Vorbedingungen	Gültiges End-Entity-Zertifikat
Auslöser	Zertifikatsprüfung in der TI TUC_PKI_018 "Zertifikatsprüfung in der TI ", TUC_PKI_030 "QES-Zertifikatsprüfung"
Eingangsdaten	End-Entity-Zertifikatsdaten
Komponenten	System
Ausgangsdaten	OID der Rolle
Referenzen	[Common-PKI#Part1#3.1]
Standardablauf	1. [System:] Prozess zur Ermittlung der Rolle beginnt 2. [System:] Extension Admission aus dem Zertifikat auslesen. 3. [System] Admission ist vorhanden und die Rolle aus dem Feld `professionOIDs` ermittelt. Sind weitere Einträge `professionInfo` enthalten, wird dieser Schritt so oft durchlaufen, bis alle `professionOIDs` ermittelt sind. 4. [System:] Mindestens eine OID ist vorhanden und wird zurück geliefert. Bei mehreren OID wird die Liste der OID als Rückgabewert geliefert. Ende des Use Case mit vorhandener Rolle
Varianten/Alternativen	3a. [System:] Extension Admission ist nicht vorhanden. 3a1. [System:] Meldung des Systems, dass keine Rolle vorhanden ist. 3a2. [System:] Ende des Use Case ohne Rolle 4a. [System:] OID nicht vorhanden 4a1. [System:] Meldung des Systems, dass keine Rolle vorhanden ist.

Element	Beschreibung
	4a2. [System:] Ende des Use Case ohne Rolle
Fehlerfälle	Es werden keine spezifischen Fehlerfälle beschrieben.
Technische Fehlermeldung	Das System meldet entsprechende Fehlercodes.
Anmerkungen	Die Rolle in der Extension Admission befindet sich im Feld `professionOIDs` und ist als OID abgelegt. Die genaue Festlegung der OID wird im Dokument [gemSpec_OID] spezifiziert. Syntax der Extension Admission siehe [Common-PKI#Part1#3.1]
Zugehörige Diagramme	Abbildung 22 Aktivitätsdiagramm TUC_PKI_009 „Rollenermittlung“

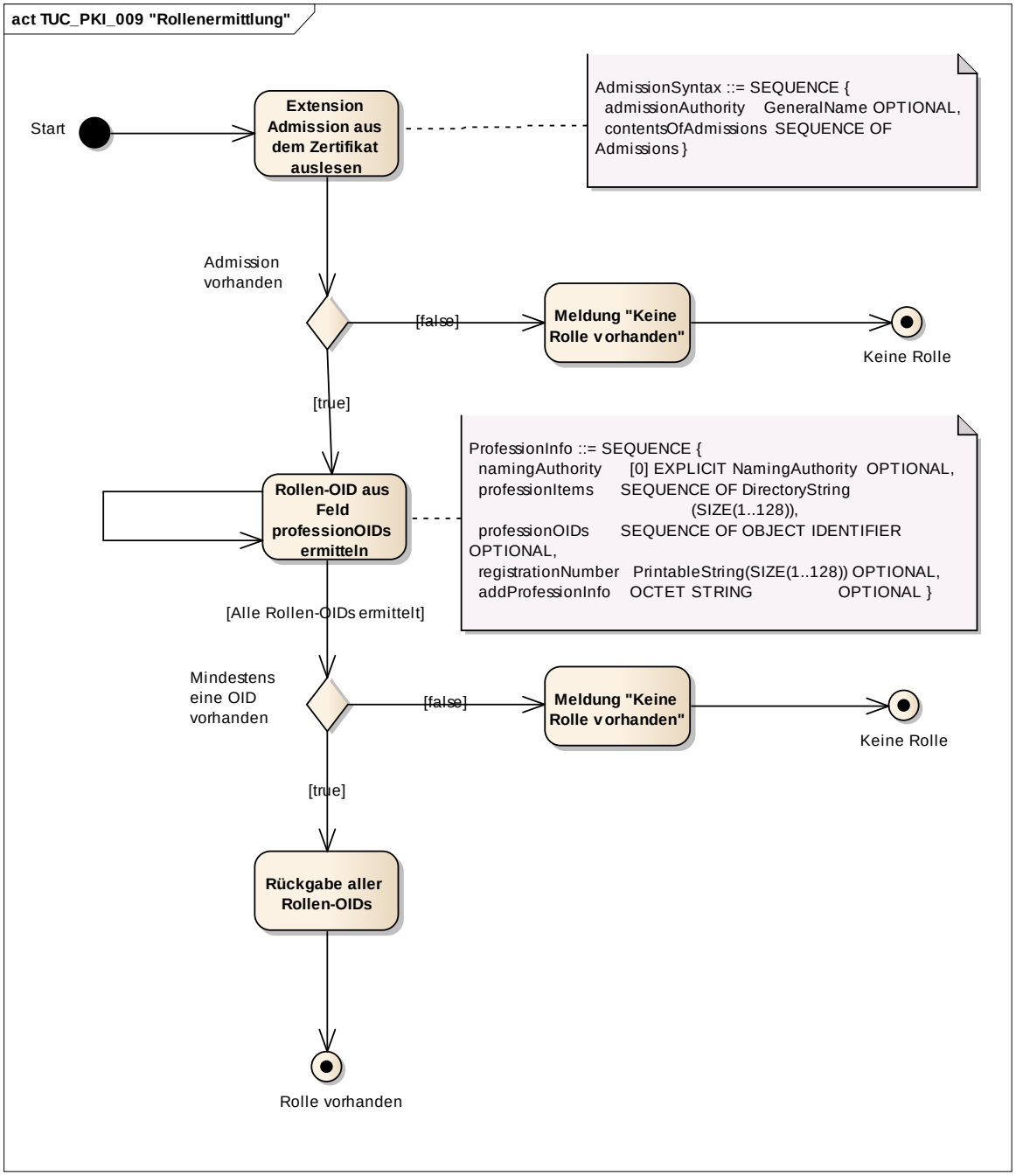

Abbildung 22 Aktivitätsdiagramm TUC_PKI_009 "Rollenermittlung"

8.3.3.3 TUC_PKI_007 "Prüfung Zertifikatstyp"

⌦ GS-A_4749 TUC_PKI_007: Prüfung Zertifikatstyp

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

Tabelle 94: TUC_PKI_007 "Prüfung Zertifikatstyp"

Element	Beschreibung
Name	TUC_PKI_007 "Prüfung Zertifikatstyp"
Beschreibung	In diesem Use Case wird der Soll-/Ist-Vergleich des Zertifikatstyps im Zuge einer Zertifikatsprüfung beschrieben. Verglichen wird die im Zertifikat hinterlegte Zertifikatstyp-OID (abgelegt in einem Element PolicyIdentifier der X.509-Extension CertificatePolicies) mit der als Eingangsparameter dieses TUC übergebenen Liste der erwarteten Zertifikatstyp-OIDs.
Anwendungsumfeld	System, das spezifische Inhalte von Zertifikaten verwendet
Vorbedingungen	Gültiges End-Entity-Zertifikat
Auslöser	TUC_PKI_018 "Zertifikatsprüfung in der TI "
Eingangsdaten	• Das zu prüfende Zertifikat • PolicyList
Komponenten	System
Ausgangsdaten	• Status der Prüfung • OID des Zertifikatstyps
Referenzen	[RFC5280], [Common-PKI]
Standardablauf	1. [System:] Start des Prozesses zur Ermittlung des Zertifikatstyps. 2. [System:] Zertifikat laden 3. [System:] Auswahl der CertificatePolicies aus dem Zertifikat 4. [System:] Auswahl des Elements PolicyInformation. Es können mehrere Elemente vorkommen, da es eine SEQUENCE ist. In jedem Schritt wird ein Element aus der SEQUENCE entnommen. 5. [System:] Selektion der CertPolicyId aus dem Element PolicyInformation 6. [System:] Prüfung der OID aus dem Zertifikat gegen Liste der Zertifikatstyp-OIDs aus dem Parameter PolicyList der Eingangsdaten. 7. [System:] Übereinstimmung der OIDs und Ende des Use Case mit Rückmeldung des logischen Wertes TRUE. Mit dem ersten OID-Match wird der TUC beendet und die geforderte Bedingung als erfüllt gewertet.
Varianten/Alternativen	6a. [System:] Keine Übereinstimmung, nächstes Element PolicyInformation des Zertifikates wird analysiert. Wiederholung des Vorgangs ab Schritt 4.
Fehlerfälle/Warnungen	4a. [System:] Abbruch und Rückmeldung. Kein Element PolicyIdentifier vorhanden. (CERT_TYPE_INFO_MISSING) 7a. [System:] Abbruch und Rückmeldung. Ende der SEQUENCE ist erreicht und es wurde keine Übereinstimmung festgestellt. (CERT_TYPE_MISMATCH)

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

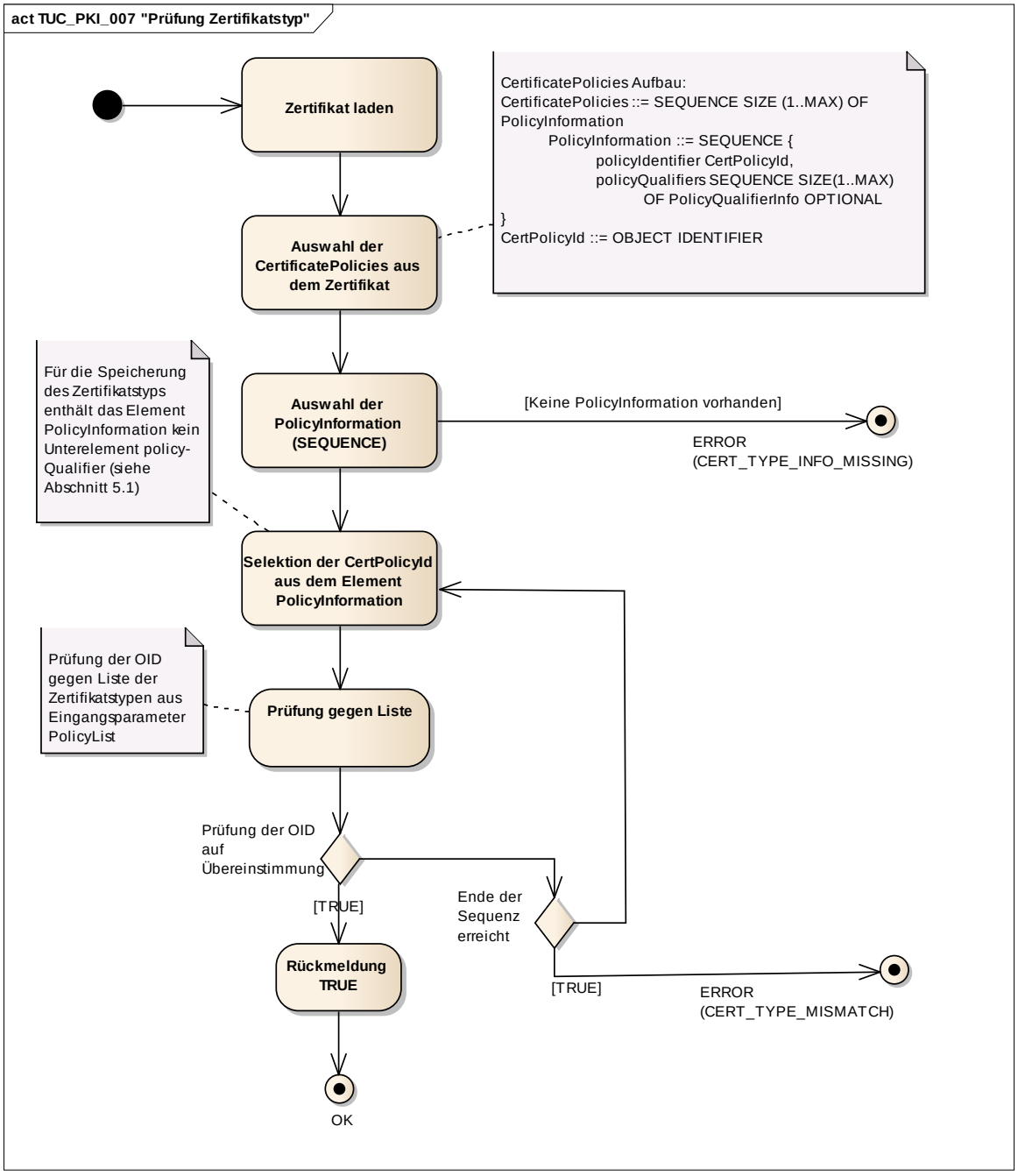

Abbildung 23 Aktivitätsdiagramm TUC_PKI_007 "Prüfung Zertifikatstyp"

8.3.4 Weitere Prüfungen

8.3.4.1 Umgang mit kritischen Extensions

⌦ **GS-A_4661 kritische Erweiterungen in Zertifikaten**

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

8.4 Überprüfung der Zertifikate auf Netzwerk- und Transportebene

8.4.1 TLS-Verbindungsaufbau

⌦ **GS-A_4662 Bedingungen für TLS-Handshake**

Produkttypen der TI die TLS nutzen, MÜSSEN sicherstellen, dass eine HTTPS-Verbindung nur zustande kommt, wenn beide Zertifikate aktuell gültig sind und zusätzlich der TLS-Handshake erfolgreich absolviert wurde.⌫

⌦ **GS-A_4663 Zertifikats-Prüfparameter für den TLS-Aufbau**

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

Tabelle 95: Tab_PKI_273 Prüfparameter für TLS-Aufbau

TUC_PKI_018 Eingangsdaten	Beschreibung
Zertifikat	Das zu prüfende Zertifikat vom Kommunikationspartner
Referenzzeitpunkt	Aktuelle Systemzeit
Prüfmodus	OCSP
PolicyList	Zulässige Policy-OID <oid_policy_gem_or_cp>
Vorgesehene KeyUsage	Der Wert MUSS konfigurierbar sein. Die zu konfigurierenden Werte sind. in den Zertifikatsprofilen der TLS-nutzenden Komponenten enthalten.
Vorgesehene ExtendedKeyUsage	Der Wert MUSS konfigurierbar sein. Die zu konfigurierenden Werte sind. in den Zertifikatsprofilen der TLS-nutzenden Komponenten enthalten.
Vorgesehene Rollen	Der Wert MUSS konfigurierbar sein. Die zu konfigurierenden OIDs werden aus [gemSpec_OID#Tab_PKI_406] entnommen.
OCSP-Graceperiod	Der Wert muss konfigurierbar sein
Offline-Modus	Nein, mit Ausnahme dezentraler Komponenten, bei denen ein Offline-Modus möglich ist

⌦ **GS-A_5077 FQDN-Prüfung beim TLS-Aufbau**

Produkttypen der TI die beim Aufbau einer TLS-Verbindung das TLS-Serverzertifikat prüfen, MÜSSEN sicherstellen, dass für den HTTPS-Verbindungsaufbau

der FQDN im SubjectDN des Zertifikats C.ZD.TLS-S bzw. C.FD.TLS-S mit dem der Komponente zugeordneten FQDN übereinstimmt.⌫

8.4.2 IPsec-Verbindungsaufbau

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

Produkttypen der TI die beim Aufbau einer IPsec-Verbindung das IPsec-Serverzertifikat prüfen, MÜSSEN sicherstellen, dass der FQDN im SubjectDN des Zertifikats C.VPNK.VPN bzw. C.VPNK.VPN-SIS mit dem der Komponente zugeordneten FQDN übereinstimmt.⌫

8.5 Zertifikatsprüfung X.509 QES

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

(1) Die Zertifikatsüberprüfende Komponente muss die Gültigkeit des Zertifikats in Bezug auf den Signaturerstellungszeitpunkt und dem zu Grunde liegenden Gültigkeitsmodell überprüfen.

(2) Die Zertifikatsüberprüfende Komponente muss den Zertifikatsstatus aller im Zertifikatspfad enthaltenen Zertifikate mit dem vom jeweiligen ZDA bzw. der BNetzA zur Verfügung gestellten Statusprüfdienst überprüfen. Auch der Status der OCSP-Responder-Zertifikate muss mit gleicher Güte geprüft werden.

(3) Die Zertifikatsüberprüfende Komponente muss auf die Anwendungsbereiche des Zertifikats und die damit verbundenen Einschränkungen achten.

(4) Das Schlüsselpaar QES ist ausschließlich für die qualifizierte elektronische Signatur nach [SigG01] im Sinne der „Nicht-Abstreitbarkeit“ („nonrepudiation“ bzw. „content commitment“) einzusetzen. Die Schlüsselpaare und Zertifikate dürfen nur für ihren jeweiligen Anwendungsbereich benutzt werden. Eine Benutzung außerhalb des zugehörigen Anwendungsbereichs ist nicht zulässig.

(5) Die Zertifikatsüberprüfende Komponente muss das QES-Zertifikat auf Vorhandensein der Extension QCStatement und einen darin enthaltenen Wert für QES-Konformität prüfen.

(6) Der Überprüfer hat die Sorgfaltspflicht, seine IT-Infrastruktur zu schützen:

a. Er muss die Auflagen der Signaturanwendungskomponente (SAK), wie sie in der Bedienungsanleitung beschrieben sind, erfüllen.

b. Er muss evtl. Nutzungsbeschränkungen im Zertifikat berücksichtigen.

(7) Eine Aussage über die Gültigkeit der Signatur wird über eine zugelassene, im Amtsblatt der BNetzA aufgeführte Signaturanwendungskomponente getroffen.

Der folgende Use Case verdeutlicht die Aktionen des Systems.

Für die QES-Zertifikatsprüfung ist nur der TUC_PKI_030 "QES-Zertifikatsprüfung" für andere gematik Dokumente referenzierbar.

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

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

8.5.1 TUC_PKI_030 "QES-Zertifikatsprüfung"

Tabelle 96: TUC_PKI_030 "QES-Zertifikatsprüfung"

Element	Beschreibung
Name	TUC_PKI_030 "QES-Zertifikatsprüfung"
Beschreibung	In diesem Use Case wird die Prüfung von Zertifikaten mit qualifizierter Signatur beschrieben. Initial muss in das System das QES-Root-Zertifikat der BNetzA sicher eingebracht werden. Dieses ist dann Root-Teil der finalen Zertifikatsliste (tbvPath).
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	QES-CA-Zertifikat im Truststore vorhanden QES-Root-Zertifikat der BNetzA (QES-Vertrauensanker) sicher im System eingebracht eine TSL mit gültiger Signatur
Auslöser	Zertifikats-Check
• Eingangsdaten	• Zertifikat (tbvCert – „to be verified Certificate“, also das zu überprüfende Zertifikat) • Zertifikatsliste (tbvCerts – Die Liste der Zertifikate, die die Kette zur Root bilden) • Referenzzeitpunkt (refTime): Zeitpunkt, für den das Zertifikat geprüft werden soll • PolicyList: Liste der im aktuellen Aufruf zulässigen Zertifikatstyp-OIDs. Die Liste muss mindestens eine OID enthalten. • Offline-Modus (ja/nein) • Beigefügte OCSP-Responses, die zur Prüfung des angefragten Zertifikates erforderlich sind (optional; z.B. in Signatur eingebettet) • Nonce (optional; Wert zur Verwendung bei der OCSP-Prüfung ausschliesslich des zu prüfenden QES-EE-Zertifikates) • TSL-Informationen (Adressen für OCSP-Abfragen) • Timeout-Parameter für OCSP-Abfragen (Default: 10s)
Komponenten	System
Ausgangsdaten	Status der Prüfung, OCSP-Response-Liste, im Zertifikat enthaltene Rollen-OIDs
Standardablauf	0. Die QES-Zertifikatsprüfung setzt sich aus den in [Common-PKI#Part5] und [Common-PKI#9] beschriebenen Schritten zusammen. [Common-PKI] umfasst dabei die Zertifikatsprüfungen für QES-Basis- und Attributszertifikate. (Diese Schritte sowie deren Tests sind Gegenstand einer Evaluierung und Bestätigung nach [SigG01], es sind also keine TI-spezifischen Evaluierungen notwendig.) Zusätzlich zu den in [Common-PKI] beschriebenen Schritten werden

Element	Beschreibung
	folgende Schritte durchgeführt: 1. [System:] Ermittlung der OCSP-Adresse aus der TSL (TUC_PKI_005 "Adresse **für Status- und Sperrprüfung** ermitteln") 2. [System:] alle bei der BNetzA abzufragenden Statusinformationen werden über den OCSP-Responder Proxy (OCSP-Responder Proxy) durchgeführt. 3. [System:] Prüfung, ob das ausstellende QES-CA-Zertifikat des QES-Zertifikates in der TSL enthalten ist (TUC_PKI_003 "CA-Zertifikat in TSL-Informationen finden"). 4. [System:] Prüfung, ob das QES-CA-Zertifikat (zum Referenzzeitpunkt) in der TSL als gültig gekennzeichnet ist. 5. [System:] Ermittlung der Rolle (TUC_PKI_009 "Rollenermittlung") 6. [System:] Prüfung, ob eine der übergebenen Zertifikatstyp-OIDs (aus der Parameter PolicyList) im Zertifikat enthalten ist (TUC_PKI_007 "Prüfung Zertifikatstyp"). Zur Prüfung muss die Liste (PolicyList s.o.) mindestens eine OID enthalten. 7. [System:] Ende des Use mit Rückgabe des/der im Zertifikat enthaltenen Rollen-OID(s)
Varianten/Alternativen	Der Standardablauf stellt die üblichen Schritte dar, die durchgeführt werden müssen. Eine Trennung in zwei Prozesse oder eine Umstrukturierung, bei der alle notwendigen Schritte erfolgen, ist zulässig, sofern die SigG-Konformität gewährleistet ist. 0a. [System:] Wird im optionalen Parameter Nonce ein Wert übergeben, dann muss für QES-EE-Zertifikate dieser Wert als OCSP-Parameter in den OCSP-Request integriert und im Response geprüft werden. 0b. [System:] Bei der Validierung des Zertifikatspfades tritt diese Variante auf: Ein CA-Zertifikat liegt im Zertifikatspfad unter einem BNetzA-Link-Zertifikat oder dem QES-Vertrauensanker. Dieses übergeordnete CA-Zertifikat war noch nicht gültig, als das untergeordnete CA-Zertifikat ausgestellt wurde. (CACertSub.notBefore < CACertSuper.notBefore) Diese Variante verhindert ein positives Ergebnis der Validierung nicht. 1a. [System:] Der Offline-Modus ist aktiviert. Es werden keine Statusinformationen eingeholt. (Schritte 1 und 2 entfallen.) 2a. [System:] OCSP-Responses zu dem zu prüfenden Zertifikat wurden im Aufruf mit übergeben. Falls diese zum Referenzzeitpunkt gültig sind, werden keine OCSP-Requests erzeugt (an den OCSP-Responder Proxy für QES-CA-Zertifikate; an den Herausgeber OCSP-Responder für QES-EE-Zertifikate), sondern die beigefügten OCSP-Responses zur weiteren Prüfung verwendet.
Fehlerfälle	In jedem der beschriebenen Schritte können Fehler auftreten. Diese sind durch das System zu melden und der Prozess muss beendet werden. 0c. In [Common-PKI#Part5] und [Common-PKI#9] sind Fehlerfälle für die QES-Zertifikatsprüfung beschrieben. Diese beinhalten: QES_BUILD_CHAIN_FAILED, QC_STATEMENT_ERROR 0d. Wenn die in einer OCSP-Response zurückgelieferte Nonce nicht mit der

Element	Beschreibung
	Nonce des OCSP-Requests für ein QES-EE-Zertifikat übereinstimmt, wird die Prüfung abgebrochen mit der Fehlermeldung OCSP_NONCE_MISMATCH. 2b. [System:]. OCSP-Responder Proxy nicht erreichbar. Abbruch mit Fehlermeldung (OCSP_PROXY_NOT_AVAILABLE). 2c. [System:] OCSP-Responses zu dem zu prüfenden Zertifikat wurden im Aufruf mit übergeben, ergaben bei den weiteren Prüfschritten jedoch kein gültiges Ergebnis. Eine erneute Prüfung wird in diesem Fall durchgeführt, als wären keine OCSP-Responses beigefügt. In den Rückgabewerten dieses TUC wird die Warnmeldung (PROVIDED_OCSP_RESPONSE_NOT_VALID) an die aufrufende Funktion übergeben. 4a. [System:] QES-CA-Zertifikat des QES-Zertifikates ist in TSL als revoked gekennzeichnet und QES-Zertifikat ist nach Sperrzeitpunkt erstellt worden. Abbruch mit Fehlermeldung (CA_CERTIFICATE_REVOKED_IN_TSL). 6a. [System:] Warnmeldung, dass keine Online-Statusprüfung durchgeführt wurde (NO_OCSP_CHECK).
Technische Fehlermeldung	Das System meldet entsprechende Fehlercodes.
Sicherheits-anforderungen	Maßgeblich sind die Anforderungen, die im Rahmen [SigG01]/[SigV01] an die Signaturanwendungskomponenten gestellt werden.
Zugehörige Diagramme/Tabelle	

Die Einträge der QES-Zertifikate in der TSL für Personen und Organisationen besitzen den ServiceTypeIdentifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC.

8.5.2 QES-Vertrauensanker

Systeme, die akkreditierte QES-Zertifikate validieren, müssen auf ein von der Bundesnetzagentur (BNetzA) ausgestelltes Root-CA-Zertifikat (QES-Root) zugreifen. Dieses wird außerhalb des normalen Speicherortes für den TI-Vertrauensraum sicher abgelegt (also nicht einfach im Truststore). Konkret befindet sich dieser sichere Speicherort auf der SMC-K des Konnektors.

Wenn eine neue BNetzA-Root-CA[1] erzeugt wird, stellt sie der zeitlich vorhergehenden ein Cross-Zertifikat aus und wird auch von dieser Cross-zertifiziert. Diese speziellen Cross-Zertifikate werden als Link-Zertifikate bezeichnet. Die BNetzA stellt ihre Link-Zertifikate öffentlich zur Verfügung, um die Vertrauenskette sicherzustellen.

[1] Eine spezifische BNetzA-Root hat eine begrenzte Laufzeit. Das aktuelle BNetzA-Root-Zertifikat ist fünf Jahre (2011-2016) gültig. Gemäß [SigV01] beträgt die maximal mögliche Gültigkeitsdauer von qualifizierten Zertifikaten 10 Jahre. Bisher wurden BNetzA-Root-Zertifikate jedoch mit einer Laufzeit von maximal 5 Jahren ausgestellt.

Bei einem Update der BNetzA-Root wird die TSL als Transportmedium genutzt, um in der TI das neue BNetzA-Zertifikat in den QES-Vertrauensraum zu integrieren. Es wird dabei keine eigentliche Migration des BNetzA-Root-Zertifikates durchgeführt. Das erstmalig eingeführte BNetzA-Root-Zertifikat (BNCA-0) kann somit weiterhin als QES-Vertrauensanker wirken und im sicheren Speicher vorgehalten werden.

Wenn eine neue BNetzA-Root-CA (BNCA-1) aufgesetzt wird, wird das von der BNCA-0 ausgestellte Link-Zertifikat für BNCA-1 in die TSL mit aufgenommen. Dieses kann dann als Sub-CA-Zertifikat in den für QES-CA-Zertifikate vorgesehenen Speicher importiert werden.

Somit kann der Pfad weiterhin bis zum Root-Zertifikat BNCA-0 geprüft werden.

Außerdem muss das QES-validierende System auch QES-Zertifikate unterstützen, welche ursprünglich unter älteren BNetzA-Root-CA-Zertifikaten ausgestellt wurden (z.B. QES-Zertifikate der Vorläuferkarten). Die entsprechenden Aussteller-CA-Zertifikate sind in der TSL enthalten. Weiter muss auch der Pfad von diesen Zertifikaten zum QES-Vertrauensanker auf der SMC-K gebildet werden können. Auch dieser Pfad wird über Cross-Zertifikate gebildet. In diesem Fall handelt es sich um die Cross-Zertifikate, welche jeweils eine neue BNetzA-Root-CA ihrer Vorgängerin ausstellte.
(Solche Cross-Zertifikate, werden auch als Link-Zertifikate bezeichnet.)

⌦ **GS-A_5045 Cross-Zertifikate der BNetzA**

Der TSL-Dienst MUSS für alle in der TI zu prüfenden QES-CA-Zertifikate sämtliche Cross-Zertifikate der BNetzA als QES-CA-Zertifikate in die TSL aufnehmen, die benötigt werden, um den Zertifizierungspfad
a) vom neusten QES-CA-Zertifikat zum ältesten QES-Vertrauensanker zu bilden, welches in der TI (von Konnektoren) verwendet wird
(Diese Cross-Zertifikate wurden jeweils von einer BNetzA-Root-CA auf ihre Nachfolger-Root-CA ausgestellt.),
b) vom in der TI verwendeten ältesten QES-CA-Zertifikat zum neusten QES-Vertrauensanker zu bilden.
(Diese Cross-Zertifikate wurden jeweils von einer BNetzA-Root-CA auf ihre Vorgänger-Root-CA ausgestellt.).
Die Cross-Zertifikate müssen solange in der TSL verbleiben, wie es die gemäß SigV, §4 (2) geforderte Zeitspanne erfordert. ⌫

Die obige Anforderung bezieht sich auf die zeitlichen Extreme (neuester/ältester QES-Vertrauensanker und QES-Aussteller-CA-Zertifikat). Somit deckt sie auch die zeitlich dazwischen liegenden QES-Vertrauensanker und QES-Aussteller-CA-Zertifikate ab.

Die Prüfung einer QES beinhaltet die Prüfung des QES-EE-Zertifikates und damit auch die Prüfung des (in der TSL enthaltenen) QES-Aussteller-CA-Zertifikates bis zum QES-Vertrauensanker, welcher von einem System (Konnektor) verwendet wird.

8.6 Fehlercodes bei TSL- und Zertifikatsprüfung X.509

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

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

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

Tabelle 97: Tab_PKI_274 Fehlercodes des SubCompTyps PKI bei TSL- und Zertifikatsprüfung

Code	Severity	ErrorType	ErrorText	Detail	Meldungskürzel
1001	Error	Technical	Es liegt keine gültige TSL vor		TSL_INIT_ERROR
1002	Error	Technical	Zertifikate lassen sich nicht extrahieren		TSL_CERT_EXTRACTION_ERROR
1003	Error	Security	Mehr als ein markierter V-Anker gefunden		MULTIPLE_TRUST_ANCHOR
1004	Error	Technical	TSL-Signer-CA lässt sich nicht extrahieren		TSL_SIG_CERT_EXTRACTION_ERROR
1005	Error	Technical	Element "PointerToOtherTSL" nicht vorhanden		TSL_DOWNLOAD_ADDRESS_ERROR
1006	Error	Technical	TSL-Downloadadressen wiederholt nicht erreichbar		TSL_DOWNLOAD_ERROR
1007	Error	Security	Vergleich der ID und SequenceNumber entspricht nicht der Vergleichsvariante 6a		TSL_ID_INCORRECT
1008	Warning	Security	Die TSL ist nicht mehr aktuell		VALIDITY_WARNING_1
1009	Warning	Security	Überschreitung des Elements NextUpdate um TSL-Grace-Period		VALIDITY_WARNING_2
1010	Warning	Security	Das aktuelle Datum ist neuer als das Element NextUpdate der TSL		TSL_ NEXTUPDATE_EXPIRED
1011	Error	Technical	TSL-Datei nicht wellformed		TSL_NOT_WELLFORMED
1012	Error	Technical	Schemata der TSL-Datei nicht korrekt		TSL_SCHEMA_NOT_VALID
1013	Error	Security	Signatur ist nicht gültig		XML_SIGNATURE_ERROR
1014	Error	Technical	Signaturprüfung war nicht erfolgreich		SIGNATUREVERIFICATION_NOT_SUCCESSFUL
1015	Error	Security	Signatur-Zertifikat nicht gültig		TSL_SIGNATURE_NOT_VALID

Code	Severity	ErrorType	ErrorText	Detail	Meldungskürzel
1016	Error	Security	KeyUsage ist nicht vorhanden bzw. entspricht nicht der vorgesehenen KeyUsage		WRONG_KEYUSAGE
1017	Error	Security	ExtendedKeyUsage entspricht nicht der vorgesehenen ExtendedKeyUsage		WRONG_EXTENDEDKEYUSAGE
1018	Error	Security	Zertifikatstyp-OID stimmt nicht überein		CERT_TYPE_MISMATCH
1019	Error	Technical	Zertifikat nicht lesbar		CERT_READ_ERROR
1020	Error	Security	Prüfzeitpunkt nicht innerhalb der Gültigkeitsdauer des Zertifikats		CERT_EXPIRED
1021	Error	Security	Zertifikat ist zeitlich nicht gültig		CERTIFICATE_NOT_VALID_TIME
1022	Error	Technical	Kein passendes CA-Zertifikat gefunden		APPROPRIATE_CA_CERTIFICATE_NOT_FOUND
1023	Error	Security	AuthorityKeyIdentifier des End-Entity-Zertifikats von SubjectKeyIdentifier des CA-Zertifikats unterschiedlich		AUTHORITYKEYID_DIFFERENT
1024	Error	Security	Zertifikats-Signatur ist mathematisch nicht gültig.		CERTIFICATE_NOT_VALID_MATH
1026	Error	Technical	Das Element "ServiceSupplyPoint" konnte nicht gefunden werden oder enthält PKI keinen URI		OCSP_SERVICESUPPLYPOINT_MISSING
1027	Error	Technical	CA kann nicht in den TSL-Informationen ermittelt werden.	Keine Adresse hinterlegt.	CA_CERT_MISSING
1028	Warning	Technical	Die OCSP-Prüfung konnte nicht durchgeführt werden (1)	TOLERATE_OCSP_FAILURE=true	OCSP_CHECK_REVOCATION_FAILED
1029	Error	Technical	Die OCSP-Prüfung konnte nicht durchgeführt werden (2)	TOLERATE_OCSP_FAILURE=false	OCSP_CHECK_REVOCATION_ERROR
1030	Error	Security	OCSP-Zertifikat nicht in TSL-		OCSP_CERT_MISSING

Code	Severity	ErrorType	ErrorText	Detail	Meldungskürzel
			Informationen enthalten		
1031	Error	Security	Signatur der Response ist nicht gültig.		OCSP_SIGNATURE_ERROR
1032	Error	Technical	OCSP-Responder nicht verfügbar		OCSP_NOT_AVAILABLE
1033	Error	Security	Kein Element PolicyInformation vorhanden		CERT_TYPE_INFO_MISSING
1034	Error	Technical	OCSP-Responder Proxy nicht erreichbar		OCSP_PROXY_NOT_AVAILABLE
1036	Error	Security	QES-CA-Zertifikat des QES-EE-Zertifikates ist in TSL als revoked gekennzeichnet.		CA_CERTIFICATE_REVOKED_IN_TSL
1039	Warning	Security	Warnung, dass Offline-Modus aktiviert ist und keine OCSP-Statusabfrage durchgeführt wurde		NO_OCSP_CHECK
1040	Error	Security	Bei der Onlinestatusprüfung ist ENFORCE_CERTHASH_CHECK auf ´true´ gesetzt, die OCSP-Response enthält jedoch keine certHash-Erweiterung		CERTHASH_EXTENSION_MISSING
1041	Error	Security	Der certHash in der OCSP-Response stimmt nicht mit dem certHash des vorliegenden Zertifikats überein.		CERTHASH_MISMATCH
1042	Error	Technical	Das TSL-Signer-CA-Zertifikat kann nicht aus dem sicheren Speicher des Systems geladen werden.		TSL_CA_NOT_LOADED
1043	Error	Technical	CRL kann aus technischen Gründen nicht ausgewertet werden.		CRL_CHECK_ERROR
1044	Warning	Technical	Warnung, dass zum angefragten Zertifikat keine Statusinformationen		CERT_UNKNOWN

Code	Severity	ErrorType	ErrorText	Detail	Meldungskürzel
			verfügbar sind.		
1046	Error	Technical	Es konnte keine ununterbrochene Kette zu einem vertrauenswürdigen QES-Wurzelzertifikat gefunden werden.		QES_BUILD_CHAIN_FAILED
1047	Warning	Security	Das Zertifikat wurde vor oder zum Referenzzeitpunkt widerrufen.		CERT_REVOKED
1048	Error	Technical	Es ist ein Fehler bei der Prüfung des QCStatements aufgetreten (z. B. nicht vorhanden, obwohl gefordert).		QC_STATEMENT_ERROR
1050	Warning	Technical	Die einem TUC zur Zertifikatsprüfung beigefügte OCSP-Response zu dem zu prüfenden Zertifikat kann nicht erfolgreich gegen das Zertifikat validiert werden.		PROVIDED_OCSP_RESPONSE_NOT_VALID
1051	Error	Security	Die in einem OCSP-Response zurückgelieferte Nonce stimmt nicht mit der Nonce des OCSP-Requests überein.		OCSP_NONCE_MISMATCH
1052	Error	Security	Attribut-Zertifikat kann dem übergebenen Basis-Zertifikat nicht zugeordnet werden.		ATTR_CERT_MISMATCH
1053	Error	Technical	Die CRL kann nicht heruntergeladen werden.		CRL_DOWNLOAD_ERROR
1054	Error	Technical	Eine verwendete CRL ist zum aktuellen Zeitpunkt nicht mehr gültig.		CRL_OUTDATED_ERROR
1055	Error	Security	CRL-Signer-Zertifikat nicht in TSL-Informationen enthalten		CRL_SIGNER_CERT_MISSING

Code	Severity	ErrorType	ErrorText	Detail	Meldungskürzel
1056	Error	Security	Das CRL-Signer-Zertifikat nicht in TSL-Informationen enthalten.		CRL_SIGNER_CERT_MISSING
1057	Error	Security	Signatur der CRL ist nicht gültig.		CRL_SIGNATURE_ERROR
1058	Error	Technical	Die OCSP-Response enthält eine Exception-Meldung.		OCSP_STATUS_ERROR

8.7 Zertifikatsprüfung CVC

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

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

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

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

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

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

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

8.8 Zertifikatsprüfung CV-Zertifikate der 2. Generation

Im Gegensatz zur Prüfung von CV-Zertifikaten der Generation 1 beschränkt sich die Prüfung von CV-Zertifikaten der Generation 2 nicht nur auf die Prüfung der Vertrauenskette und die Signaturprüfung. Zusätzlich werden einige der verwendeten Schlüsselattribute des CV-Zertifikats und der weiteren CV-Zertifikate in der Vertrauenskette geprüft bzw. ausgewertet, insbesondere das Certificate Effective Date (CED) und das Certificate Expiration Date (CXD). Die Prüfung der Signatur eines CV-Zertifikats erfolgt mittels eines öffentlichen Schlüssels, der vor der Zertifikatsprüfung ausgewählt wird. Handelt es sich bei dem Produkttyp der TI, der das CV-Zertifikat prüfen soll, um eine Chipkarte, dann wird dieser öffentliche Schlüssel durch ein MSE-Set-Kommando der Karte bekannt gegeben.

⌦ **GS-A_5009 Prüfung der mathematischen Korrektheit von CV-Zertifikate der Generation 2**

Die Produkttypen der TI, die CV-Zertifikate prüfen, MÜSSEN bei der Prüfung von CV-Zertifikaten der Generation 2 die Prüfung der mathematischen Korrektheit vor-

nehmen, d. h. ob die Signatur des CV-Zertifikats mit dem CV-Zertifikat der ausstellenden TSP-CVC und ob die Signatur des TSP-CVC -Zertifikats mit dem CV-Zertifikat der ausstellenden CVC-Root-CA erfolgreich geprüft werden kann. ⌫

⌦ **GS-A_5010 Prüfung der Signatur eines CV-Zertifikats der Generation 2 mit Hilfe des CV-Zertifikats des Herausgebers**

Die Produkttypen der TI, die CV-Zertifikate prüfen, MÜSSEN bei der Prüfung der mathematischen Korrektheit der Signatur eines CV-Zertifikates *C* die im CV-Zertifikat des öffentlichen Schlüssels des Herausgebers enthaltenen Schlüsselattribute dieses öffentlichen Schlüssels anwenden. Die Prüfung MUSS den Vorgaben aus Tabelle TAB_PKI_908 folgen.⌫

Tabelle 98: Tab_PKI_908 Prüfung der Signatur eines CV-Zertifikats der Generation 2 mit Hilfe des CV-Zertifikats des Herausgebers

Prüfung der Korrektheit der Signatur eines CV-Zertifikats *C*
Sei die Nachricht M die gemäß Tabelle Tab_PKI_905 zu signierende Nachricht M des CV-Zertifikates C. Sei Signatur = R || S gemäß Tabelle Tab_PKI_906 die Signatur der Nachricht M des CV-Zertifikats *C.* *Sei PuK* der im CV-Zertifikat des Herausgebers enthaltene öffentliche Signaturschlüssel des Herausgebers.
Bei der Prüfung der Signatur MUSS der domainParameter des Schlüssels *PuK* gemäß des CV-Zertifikats des Herausgebers genutzt werden (gemäß Tab_PKI_901). Falls das Wertfeld von DO´86´ im CV-Zertifikat des Herausgebers eine Länge von A. ´41´= 65 hat, gilt PuK.domainParameter = brainpoolP256r1. B. ´61´= 97 hat, gilt PuK.domainParameter = brainpoolP384r1. C. ´81´= 129 hat, gilt PuK.domainParameter = brainpoolP512r1.
Bei der Prüfung der Signatur MUSS das Hashverfahren gemäß dem domainParameter genutzt werden (gemäß Tab_PKI_906).
Falls CAR und CHAT aus CV-Zertifikat *C* und CV-Zertifikat des Herausgebers nicht miteinander korrespondieren sind, dann ist das CV-Zertifikat *C* nicht korrekt.

⌦ **GS-A_5011 Prüfung der Gültigkeit von CV-Zertifikaten der Generation G2**

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN bei der Prüfung von CV-Zertifikaten der Generation 2 die Prüfung der Gültigkeit vornehmen, d. h. die Gültigkeit des CV-Zertifikats gemäß Tabelle TAB_PKI_909 prüfen. ⌫

Tabelle 99: Tab_PKI_909 Gültigkeit eines CV-Zertifikats der Generation 2

Gültigkeit eines CV-Zertifikats *C*
Ein CV-Zertifikat einer CVC-Root-CA ist gültig, wenn • das CV-Zertifikat mathematisch korrekt gebildet ist und • das Certificate Expiration Date (CXD) des CV-Zertifikats noch nicht überschritten ist.
Ein CV-Zertifikat *C*, das von einem Herausgeber der Generation 2 (TSP-CVC oder CVC-Root-CA) erzeugt wurde, ist gültig, wenn • das CV-Zertifikat für den öffentlichen Schlüssels des Herausgebers gültig und

• das CV-Zertifikat mathematisch korrekt gebildet ist und • das Certificate Expiration Date (CXD) des CV-Zertifikats *C* nicht überschritten ist.
In allen anderen Fällen ist das CV-Zertifikat ungültig.

GS-A_5012 Prüfung von CV-Zertifikaten der Generation 2

Die Produkttypen der TI, die CV-Zertifikate prüfen, MÜSSEN bei der Prüfung von CV-Zertifikaten der Generation 2 die Prüfung der mathematischen Korrektheit und die Prüfung der Gültigkeit des CV-Zertifikats vornehmen. ⌫

9 OCSP-Statusinformation

Dieses Kapitel enthält die Festlegung von Schnittstellen, die durch mehrere Produkttypen der PKI bereitgestellt werden müssen. Diese Schnittstellen werden in der vorliegenden Spezifikation beschrieben. Eine wiederholte Darstellung dieser Schnittstellen in den Spezifikationen der Produkttypen erfolgt nicht, vielmehr wird in diesen Dokumenten auf die folgenden Beschreibungen verwiesen.

9.1 Statusprüfung

Gemäß [gemKPT_Arch_TIP] ist zur Statusprüfung die Schnittstelle I_OCSP_Status_Information durch die Produkttypen

- TSL-Dienst,
- gematik Root-CA
- TSP-X.509 nonQES,
- TSP-X.509 QES und
- OCSP-Responder Proxy

anzubieten. Darüber können Nutzer, wie z.B. Konnektor und VPN-Zugangsdienst, Statusinformationen zu X.509-Zertifikaten von OCSP-Respondern erhalten. Die Schnittstelle implementiert die logische Operation check_Revocation_Status mit der der Sperrstatus eines X.509-Zertifikats ermittelt werden kann (vgl. auch [gemKPT_PKI_TIP]).

⌦ **GS-A_4669 Umsetzung Statusprüfdienst**

Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES, TSP-X.509 QES und OCSP-Responder Proxy MÜSSEN die Schnittstelle I_OCSP_Status_Information implementieren.⌫

Die Algorithmen und Parameter für die Erstellung der Signaturen über die OCSP-Responses des OCSP werden in [gemSpec_Krypt] festgelegt. Für die Statusauskünfte von qualifizierten X.509-Zertifikaten gelten die Anforderungen von SigG/SigV sowie die Vorgaben gemäß [ALGCAT].

9.1.1 Schnittstelle I_OCSP_Status_Information

⌦ **GS-A_4670 Statusprüfdienst über Gültigkeitszeitraum des X.509-Zertifikats**

Die Produkttypen TSL-Dienst, gematik Root-CA und TSP-X.509 nonQES MÜSSEN den Statusprüfdienst über den gesamten Gültigkeitszeitraum des zu prüfenden Zertifikats sicherstellen. Darüber hinausgehende Anforderungen an die Verfügbarkeit von Statusinformationen MÜSSEN in der Policy des Zertifikatsherausgebers definiert sein.⌫

Die gematik Root-CA sowie TSP-X.509 nonQES können Dritte mit der Bereitstellung des Statusprüfdienstes beauftragen.

⌦ **GS-A_4672 Statusprüfdienst QES gemäß den Vorgaben SigG/SigV**

Der TSP-X.509 QES MUSS für den Statusprüfdienst die Vorgaben gemäß [SigG01/SigV01] erfüllen.⌫

⌦ **GS-A_5049 TSP-X.509 nonQES Statusprüfdienst in TI und Internet**

Der TSP-X.509 nonQES MUSS den Statusprüfdienst in der TI und im Internet zur Verfügung stellen.⌫

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

Der Anbieter der gematik Root-CA MUSS im Internet einen OCSP-Dienst für die Statusauskünfte der CAs zur Verfügung stellen, die AUT-, ENC- und OSIG-Zertifikate zur Verwendung in HBA und SMC-B herausgeben.⌫

⌦ **GS-A_5051 TSP-X.509 nonQES Zertifikatsstatus**

Der TSP-X.509 nonQES MUSS sicherstellen, dass die Zertifikatsstatusinformation zu einem X.509-Zertifikat in der TI und im Internet identisch ist.⌫

⌦ **GS-A_5052 gematik Root-CA Zertifikatsstatus**

Die gematik Root-CA MUSS sicherstellen, dass die Zertifikatsstatusinformation zu einem X.509-CA-Zertifikat im Internet identisch ist zum Status dieses CA-Zertifikates in der TSL.⌫

⌦ **GS-A_5053 TI-Zertifikatstypen im Internet**

Der TSP-X.509 nonQES MUSS ausschliesslich Zertifikatsstatusinformation zu folgenden X.509-Zertifikaten im Internet bereitstellen:

- HP.ENC
- HCI.ENC
- HP.AUT
- HCI.AUT
- HCI.OSIG⌫

9.1.1.1 Schnittstellendefinition

Gemäß [gemKPT_PKI_TIP#TIP1-A_2140] muss die Schnittstelle zur Statusprüfung

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

9.1.1.1.1 OCSP-Request

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

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

⌦ **GS-A_4673 OCSP-Requests gemäß [RFC2560]**

Der TSP-X.509 nonQES MUSS OCSP-Requests gemäß [RFC2560] verarbeiten können.⌫

⌦ **GS-A_4674 OCSP-Requests gemäß [Common-PKI]**

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

⌦ **GS-A_4896 Nicht-Verwendung der OCSP-Extension Nonce**

Produkttypen der TI, die QES-CA- und QES-Root-Zertifikate prüfen, DÜRFEN in OCSP-Requests, die an den Produkttyp OCSP-Responder Proxy gesendet werden, NICHT die OCSP-Extension „Nonce“ verwenden.⌫

⌦ **GS-A_4957 Beschränkungen OCSP-Request**

Produkttypen der TI, die Zertifikate prüfen, DÜRFEN (abweichend von [RFC2560]) je OCSP-Request NICHT mehr als den Status für genau ein Zertifikat abfragen.Ist hierbei die Verwendung der OCSP-Extension „Nonce“ zulässig, DARF diese die Länge von 256 Bit NICHT überschreiten.⌫

9.1.1.1.2 OCSP-Response

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

Wesentlicher Inhalt ist der Status des angefragten Zertifikats, sowie zeitliches Aussagen zu dem gelieferten Status und dessen Aktualität. Die Antwort ist signiert. Weitere Details siehe Abschnitt 9.1.2.2 und folgende.

⌦ **GS-A_4675 OCSP-Responses gemäß [RFC2560]**

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

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

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

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

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

9.1.1.2 Umsetzung

GS-A_4677 Spezifikationskonforme OCSP-Responses

Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN sicherstellen, dass ihr OCSP-Responder spezifikationskonform antwortet, wenn der OCSP-Request „well formed“ spezifikationskonform formuliert ist und der Responder für diesen Service konfiguriert ist.

GS-A_4678 Signierte OCSP-Responses

Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN sicherstellen, dass ihr OCSP-Responder alle Antworten (Responses) digital signiert.

GS-A_4679 Signatur zu Statusauskünften von nonQES-Zertifikaten

Die Produkttypen TSL-Dienst, gematik Root-CA, und TSP-X.509 nonQES MÜSSEN zur Erzeugung von Signaturen über OCSP-Responses mit Statusauskünften zu nicht-qualifizierten X.509-Zertifikaten ein Schlüsselpaar einsetzen, für das ein nicht-qualifiziertes X.509-Zertifikat ausgestellt wurde.

GS-A_4680 Verwendung eines HSMs zur Erzeugung von Signaturen zu OCSP-Responses

Die Produkttypen TSL-Dienst, gematik Root-CA, und TSP-X.509 nonQES KÖNNEN zur Erzeugung von Signaturen über OCSP-Responses ein HSM verwenden.

GS-A_4684 Auslassung der Signaturprüfung bei OCSP-Requests

Zur Gewährleistung der Performance MÜSSEN die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 QES und TSP-X.509 nonQES OCSP-Responder so konfigurieren, dass signierte Requests wie unsignierte Requests behandelt werden und die Signaturprüfung der Requests entfällt.

GS-A_4685 Statusprüfdienst - Steigerung der Performance

Die Produkttypen TSL-Dienst, gematik Root-CA und TSP-X.509 nonQES SOLLEN Methoden des Response-Caching anwenden, um die Performance des Statusprüf-dienstes zu steigern.

GS-A_4940 OCSP-Proxy Updateintervall

Der Produkttyp OCSP-Responder Proxy MUSS für alle in der TSL gelisteten QES-Zertifikate einmal innerhalb von 24 Stunden eine Statusprüfung vollständig bis zur BNetzA-Root-CA vornehmen und die Ergebnisse in seinem Cache vorhalten zur Beantwortung entsprechender QES-OCSP-Requests.

9.1.1.3 Nutzung

Gemäß [gemKPT_PKI_TIP] müssen anfragende Komponenten sicherstellen, dass je OCSP-Request nicht mehr als der Status für ein X.509-Zertifikat abgefragt wird (vgl. [gemKPT_PKI_TIP#TIP1-A_2144]).

Weiterhin müssen Produkttypen der TI, die OCSP-Responses auswerten, sicherstellen, dass für jede mögliche Ausprägung der zurückgegebenen Parameter eine geordnete Reaktion implementiert wird (vgl. [gemKPT_PKI_TIP#TIP1-A_2149]).

9.1.2 Artefakte

9.1.2.1 OCSP-Response – Response Status

⌦ **GS-A_4686 Statusprüfdienst - Response Status**

Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN sicherstellen, dass für den Response Status die Werte „successful“, „malformedRequest“, „internalError“, „tryLater“ und „unauthorised“ gemäß Tab_PKI_291 unterstützt werden.⌫

Tabelle 100: Tab_PKI_291 OCSP-Response Status Ergebnisse

Ergebnis Anfrage	Bedeutung
successful	Erfolgreiche Bearbeitung einer Anfrage
malformed Request	Wegen fehlerhaftem Anfrageformat konnte keine erfolgreiche Bearbeitung der Anfrage erfolgen.
internalError	Auftretung eines internen Fehlers beim OCSP-Server
tryLater	Nicht-Verfügbarkeit des OCSP-Servers (temporär)
unauthorised	Der Client ist nicht berechtigt

⌦ **GS-A_4687 Statusprüfdienst - Response Status sigRequired**

Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN sicherstellen, dass für den Response Status der Wert „sigRequired“ nicht verwendet wird. ⌫

Mit dem Response Status „sigRequired“ fordert der OCSP-Responder explizit, dass die Anfrage vom OCSP-Client signiert werden muss. Da keine signierten OCSP-Requests in der TI gefordert sind, darf der Exception Case „sigRequired“ vom OCSP-Responder nicht verwendet werden.

9.1.2.2 OCSP-Response - Zeiten

⌦ **GS-A_4688 Statusprüfdienst - Angabe von Zeitpunkten**

Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN sicherstellen, dass die Angabe zu den Zeitpunkten **pro-**

ducedAt, **thisUpdate** und **nextUpdate** spezifikationskonform gemäß Tab_PKI_292 erfolgt. ⌫

Tabelle 101: Tab_PKI_292 Zeiten in einer OCSP-Response

Zeiten	Bedeutung
thisUpdate	„**thisUpdate**“ enthält den Zeitpunkt, für den die gemachte Aussage gültig ist. Es gibt den Zeitpunkt an zu der die Statusinformation als korrekt angesehen wurde.
nextUpdate	“**nextUpdate**“ enthält die Zeit, wann neue Informationen über das angefragte Zertifikat verfügbar sein werden. OCSP-Antworten, die keinen “nextUpdate“ Zeitpunkt enthalten, zeigen an, dass jederzeit neuere Statusinformationen zu Zertifikaten vorhanden sein können.
producedAt	Der Zeitpunkt der Signierung einer OCSP-Response.

Der Zeitpunkt **nextUpdate** ist nur für OCSP-Antworten sinnvoll, die auf CRLs basieren. Der Zeitpunkt kann in der Zukunft liegen, sofern die Antwort auf einer Sperrliste mit einem festgelegten Gültigkeitszeitraum basiert.

⌦ **GS-A_4689 Statusprüfdienst - Zeitquelle von producedAt**

Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN sicherstellen, dass der Zeitpunkt **producedAt** auf einer in der TI verbindlichen Zeitquelle beruht.⌫

⌦ **GS-A_5215 Festlegung der zeitlichen Toleranzen in einer OCSP-Response**

Produkttypen der TI, die Zertifikate prüfen, MÜSSEN die Angaben zu den Zeitpunkten **producedAt**, **thisUpdate** und **nextUpdate** in der OCSP-Response mit einer Toleranz von 75 Sekunden bezüglich der lokalen Systemzeit interpretieren.⌫

9.1.2.3 OCSP-Response - CertStatus

⌦ **GS-A_4690 Statusprüfdienst - Status des X.509-Zertifikats**

Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN sicherstellen, dass ein OCSP-Responder den Status eines Zertifikats mit einem der drei Werte a) good, b) revoked, c) unknown gemäß Tab_PKI_293 zurückgibt.⌫

[3]

Tabelle 102: Tab_PKI_293 Status der OCSP Antworten

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

OCSP Antwort	Bedeutung
revoked	Der Zustand „revoked“ sagt aus, dass das Zertifikat von der zugehörigen Zertifizierungsstelle ausgestellt wurde, dem OCSP-Responder bekannt ist und temporär oder endgültig gesperrt ist.
unknown	Diese Antwort bedeutet, dass der OCSP-Responder das nachgefragte Zertifikat nicht kennt. Entweder ist dieser von der entsprechenden CA nicht für die Beantwortung von Statusabfragen autorisiert oder es können keine Informationen zu dem Zertifikat gefunden werden.

9.1.2.4 OCSP-Response - CertID

GS-A_4691 Statusprüfdienst - X.509-Zertifikat mit Status „unknown“

Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN sicherstellen, dass im Falle eines `certStatus` mit Wert „unknown“ im Feld `certID` der Struktur `SingleResponse` der Inhalt des `certID`-Feldes in der Struktur `Request` des OCSP-Requests wiederholt wird.

9.1.2.5 OCSP-Response – Sperrzeitpunkt und Sperrgrund

GS-A_4692 Statusprüfdienst - Angabe Sperrzeitpunkt

Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN sicherstellen, dass im Falle eines gesperrten X.509-Zertifikats die Angabe des Sperrzeitpunkts im Teilfeld **`revocationTime`** in einer OCSP-Response erfolgt.

GS-A_5090 Statusprüfdienst – Keine Angabe von Sperrgründen

Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES SOLLEN sicherstellen, dass kein Sperrgrund mit der OCSP-Response geliefert wird.

9.1.2.6 OCSP-Response – CertHash

GS-A_4693 Statusprüfdienst - Positive Statement

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

9.1.3 Testunterstützung

Bei der PKI für X.509-Zertifikate wird zwischen einer Produktiv-PKI und einer Test-PKI unterschieden.

GS-A_4694 Betrieb von OCSP-Responder für Test-PKI-CAs

Die Produkttypen TSL-Dienst, gematik Root-CA und TSP-X.509 nonQES MÜSSEN neben OCSP-Respondern für die produktive PKI ebenfalls OCSP-Responder für die Test-PKI betreiben.⌫

9.1.4 Hardwaremerkmale

Die Statusprüfung setzt keine besonderen Hardwaremerkmale voraus.

Anhang A
Sektorspezifische Ausprägungen der SMC-B Zertifikate

Die nachfolgenden Profiltabellen der Sektoren referenzieren auf die Festlegungen aus Kap 5.3.4 für alle sektorübergreifenden Attribute und ergänzen/ersetzen diese um sektorspezifische Ausprägungen.

Die Profiltabellen gelten einheitlich für die Zertifikate:

- C.HCI.AUT
- C.HCI.ENC
- C.HCI.OSIG

Während der Erprobungsphase ORS1 enthalten die Zertifikate im Feld **`CertificatePolicies`** zusätzlich die Policy-OID der „Policy für SMC-B Zertifikate während Erprobung“[2]. Nach Abschluss der Erprobungsphase sowie Finalisierung sektorspezifischer Parameter und Prozesse wird diese OID entsprechend abgelöst. Die während der Erprobungsphase ausgegebenen Zertifikate behalten ihre Gültigkeit bis zu ihrem zeitlichen Ablauf.

9.2 KZBV

Tabelle 103: Tab_SMCB_KZBV SMC-B-Zertifikate für Sektor KZBV

Element			Inhalt	Kar.	
certificate			C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
	tbsCertificate				
		version	siehe Kap 5.3.4		
		serialNumber	siehe Kap 5.3.4		
		signature	siehe Kap 5.3.4		
		issuer	siehe Kap 5.3.4		
		validity	siehe Kap 5.3.4		
		subject			
		`commonName`	**`Gemäß Freigabedaten der zuständigen KZV`**	**`1`**	
		`title`	**`nicht belegt`**	**`0`**	
		`surName`	**`nicht belegt`**	**`0`**	
		`givenName`	**`nicht belegt`**	**`0`**	
		`serialNumber`	**`TI-weit eindeutiger Identifier der Karte z.B. in der Form: <TSP-ID>.<ICCSN>`**	**`1`**	
		`streetAddress`	**`nicht belegt`**	**`0`**	

[2] „Certificate Policy – Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL - Sektorspezifische Präzisierung für SMC-B-Zertifikate in Erprobungsphase ORS1“. [oid_policy_gem_or_cp_smcb_erprobung].

Element				Inhalt	Kar.	
			postalCode	**nicht belegt**	**0**	
			localityName	**nicht belegt**	**0**	
			stateOrProvinceName	**nicht belegt**	**0**	
			organizationalUnitName	**nicht belegt**	**0**	
			organizationName	~~**Gemäß Freigabedaten der zuständigen KZV**~~ **Telematik-ID gemäss Freigabedaten der zuständigen KZV**	**1**	
			countryName	siehe Kap 5.3.4	1	
			andere Attribute		0	
		subjectPublicKeyInfo		siehe Kap 5.3.4		
		extensions				critical
			SubjectKeyIdentifier {2 5 29 14}	siehe Kap 5.3.4	1	FALSE
			KeyUsage {2 5 29 15}	siehe Kap 5.3.4	1	**TRUE**
			SubjectAltNames {2 5 29 17}	~~**E-Mail-Adresse gemäss Freigabedaten der zuständigen KZV**~~ siehe Kap 5.3.4	0-1	FALSE
			BasicConstraints {2 5 29 19}	siehe Kap5.3.4	1	**TRUE**
			CertificatePolicies {2 5 29 32}	siehe Kap 5.3.4 zusätzlich: **policyIdentifier = <oid_policy_gem_or_cp_smcb_erprobung>**	**1**	**FALSE**
			CRLDistributionPoints {2 5 29 31}	**CDP des TSP für das betreffende Zertifikat**	**1**	**FALSE**
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap 5.3.4	1	FALSE
			AuthorityKeyIdentifier {2 5 29 35}	siehe Kap 5.3.4	1	FALSE
			Admission {1 3 36 8 3 3}	**professionItem = <oid_zahnarztpraxis>** **professionOID = <oid_zahnarztpraxis>** **registrationNumber = <~~Online-Kennung~~ Telematik-ID gemäss Freigabedaten der zuständigen KZV>**	**1**	**FALSE**
			ExtendedKeyUsage {2 5 29 37}	siehe Kap 5.3.4	1	FALSE
			andere Erweiterungen		0	
	signatureAlgorithm			siehe Kap 5.3.4		
	signature			siehe Kap 5.3.4		

9.3 KV-Telematik ARGE

Die nachfolgende Profiltabelle der durch die KV-Telematik ARGE betreuten Sektoren gilt für die Sektoren:

- Niedergelassene Vertragsärzte (KV)
- Niedergelassene Psychologische Psychotherapeuten (KV)
- Niedergelassene Kinder- und Jugendlichenpsychotherapeuten (KV)
- Nicht-Vertragsärzte (KBV)

Tabelle 104: Tab_SMCB_KV-T SMC-B-Zertifikate für Sektoren der KV-Telematik-ARGE

Element			Inhalt	Kar.	
certificate			C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
tbsCertificate					
	version		siehe Kap 5.3.4		
	serialNumber		siehe Kap 5.3.4		
	signature		siehe Kap 5.3.4		
	issuer		siehe Kap 5.3.4		
	validity		siehe Kap 5.3.4		
	subject				
		commonName	**Erste zwei Zeilen der Anschriftenzone (DIN5008), somit „Kurzname“ der Institution, so wie für das Anschriftenfeld definiert.**	**1**	
		title	**Titel des Verantwortlichen/Inhabers**	**0-1**	
		surName	**Familienname des Verantwortlichen/Inhabers**	**0-1**	
		givenName	**Vorname des Verantwortlichen/Inhabers (mehrere Vornamen sind durch Blank oder Bindestrich getrennt)**	**0-1**	
		serialNumber	**TI-weit eindeutiger Identifier der Karte z.B. in der Form: <TSP-ID>.<ICCSN>**	**1**	
		streetAddress	**Strassen-Anschrift der Institution (mehrere Wörter sind durch Blank getrennt)**	**0-1**	
		postalCode	**Postleitzahl des Ortes der Institution (Deutsche PLZ werden 5-stellig abgebildet)**	**0-1**	
		localityName	**Stadt des Institut-Standortes**	**0-1**	
		stateOrProvinceName	**Bundesland des Institut-Standortes**	**0-1**	
		organizationalUnitName	**nicht belegt**	**0**	
		organizationName	**9-stellige Betriebsstättennummer (z.B. „121234512“) der Praxis als eindeutige Nummer.** **Für privat abrechnende Ärzte wird hier eine 10-stellige Ersatznummer eingefügt.**	**1**	
		countryName	siehe Kap 5.3.4	1	
		andere Attribute		0	
	subjectPublicKeyInfo		siehe Kap 5.3.4		
	extensions				critical
		SubjectKeyIdentifier {2 5 29 14}	siehe Kap 5.3.4	1	FALSE
		KeyUsage	siehe Kap 5.3.4	1	**TRUE**

Element	Inhalt	Kar.	
{2 5 29 15}			
SubjectAltNames {2 5 29 17}	siehe Kap 5.3.4	0-1	FALSE
BasicConstraints {2 5 29 19}	siehe Kap 5.3.4	1	**TRUE**
CertificatePolicies {2 5 29 32}	siehe Kap 5.3.4 zusätzlich: **policyIdentifier = <oid_policy_gem_or_cp_smcb_erprobung>**	**1**	**FALSE**
CRLDistributionPoints {2 5 29 31}	**CDP des TSP für das betreffende Zertifikat**	**1**	**FALSE**
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap 5.3.4	1	FALSE
AuthorityKeyIdentifier {2 5 29 35}	siehe Kap 5.3.4	1	FALSE
Admission {1 3 36 8 3 3}	**professionItem = <oid_praxis_arzt> bzw. <oid_praxis_psychotherapeut>** **professionOID = <oid_praxis_arzt> bzw. <oid_praxis_psychotherapeut>** **registrationNumber = siehe Tabelle Tab_SMCB_TID_KV-T** **(Es wird genau eine Admission-Struktur verwendet, mit je genau einem Element: professionInfo, professionItem, registrationNumber)**	**1**	**FALSE**
ExtendedKeyUsage {2 5 29 37}	siehe Kap 5.3.4	1	FALSE
andere Erweiterungen		0	
signatureAlgorithm	siehe Kap 5.3.4		
signature	siehe Kap 5.3.4		

Tabelle 105: Tab_SMCB_TID_KV-T Aufbau Telematik-ID in SMC-B-Zertifikaten der Sektoren der KV-Telematik-ARGE

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

9.4 DKG

Die nachfolgende Profiltabelle der DKTIG gilt für den Sektor:

- Krankenhäuser (DKTIG)

Tabelle 106: Tab_SMCB_KV-T SMC-B-Zertifikate für Sektor der DKTIG

Element			Inhalt	Kar.	
certificate			C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
tbsCertificate					
	version		siehe Kap 5.3.4		
	serialNumber		siehe Kap 5.3.4		
	signature		siehe Kap 5.3.4		
	issuer		siehe Kap 5.3.4		
	validity		siehe Kap 5.3.4		
	subject				
		commonName	**Gemäss Freigabedaten der DKTIG.**	**1**	
		title	**nicht belegt**	**0**	
		surName	**nicht belegt**	**0**	
		givenName	**nicht belegt**	**0**	
		serialNumber	**Institutskennzeichen des Krankenhauses**	**1**	
		streetAddress	**Strassen-Anschrift der Institution (mehrere Wörter sind durch Blank getrennt)**	**1**	
		postalCode	**Postleitzahl des Ortes der Institution (Deutsche PLZ werden 5-stellig abgebildet)**	**1**	
		localityName	**Stadt des Institut-Standortes**	**1**	
		stateOrProvinceName	**Bundesland des Institut-Standortes**	**1**	
		organizationalUnitName	**nicht belegt**	**0**	
		organizationName	**nicht belegt**	**0**	
		countryName	siehe Kap 5.3.4	1	
		andere Attribute		0	
	subjectPublicKeyInfo		siehe Kap 5.3.4		
	extensions				critical
		SubjectKeyIdentifier {2 5 29 14}	siehe Kap 5.3.4	1	FALSE
		KeyUsage {2 5 29 15}	siehe Kap 5.3.4	1	**TRUE**
		SubjectAltNames {2 5 29 17}	siehe Kap 5.3.4	0-1	FALSE
		BasicConstraints {2 5 29 19}	siehe Kap 5.3.4	1	**TRUE**
		CertificatePolicies {2 5 29 32}	siehe Kap 5.3.4 zusätzlich: **policyIdentifier =**	**1**	**FALSE**

Element				Inhalt	Kar.	
				<oid_policy_gem_or_cp_smcb_erprobung>		
			CRLDistributionPoints {2 5 29 31}	siehe Kap 5.3.4	0-1	FALSE
			AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	siehe Kap 5.3.4	1	FALSE
			AuthorityKeyIdentifier {2 5 29 35}	siehe Kap 5.3.4	1	FALSE
			Admission {1 3 36 8 3 3}	**professionItem = <Krankenhaus>** **professionOID = <oid_krankenhaus>** **registrationNumber =** **siehe Tabelle Tab_SMCB_TID_DKTIG**	**1**	**FALSE**
			ExtendedKeyUsage {2 5 29 37}	siehe Kap 5.3.4	1	FALSE
			andere Erweiterungen		0	
	signatureAlgorithm			siehe Kap 5.3.4		
	signature			siehe Kap 5.3.4		

Tabelle 107: Tab_SMCB_TID_DKTIG Aufbau Telematik-ID in SMC-B-Zertifikaten der DKTIG

Präfix s. Kap 4.7.2.1	Separator s. Kap 4.7.2.2	Fortsatz s. Kap 4.7.2.3
Krankenhaus		SMC-B Kennzeichen + Institutsindividuelle Kennzeichnung
5	-	2 <gem. Freigabedaten der DKTIG>

Anhang B - Verzeichnisse

B1 – Abkürzungen

Kürzel	Erläuterung
AES	Advanced Encryption Standard
AK	Anwendungskonnektor
AN	alphanumerisch
AUT	Authentisierung (Authentication)
AUTN	Technisches Authentisierungszertifikat für Nachrichten
AVS	Apothekenverwaltungssystem (Primärsystem der Apotheker)
BAEK	Bundesärztekammer
BAK	Bundesapothekerkammer
BCD	Binary coded decimal
BMG	Bundesministerium für Gesundheit
BNetzA	Bundesnetzagentur
BPTK	Bundespsychotherapeutenkammer
BSI	Bundesamt für Sicherheit in der Informationstechnik
BZÄK	Bundeszahnärztekammer
C2C	card to card
CA	certification authority
CAMS	Card Application Management System
CAR	Certificate Authority Reference
CC	Common Criteria
CH	Card Holder
CHA	Certificate Holder Authorisation
CHR	Certificate Holder Reference
CMS	Karten Management System, Card Management System
CP	Certificate Policy
CPI	Certificate Profile Identifier
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CV	Card Verifiable

Kürzel	Erläuterung
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
DNs	Distinguished Names
EE	End Entity
eGK	Elektronische Gesundheitskarte
ENC	Verschlüsselung (Encryption)
ENCV	Technisches Verschlüsselungszertifikat für Verordnungen
ETSI	Europäisches Institut für Telekommunikationsnormen
FIPS-140 2	Federal Information Processing Standard 140 2
FQDN	Fully Qualified Domain Name
GBSM	Gerätebezogenes Sicherheitsmodul
GKV	Gesetzliche Krankenversicherung
gSMC	Gerätebezogene Security Module Card
HBA	Heilberufsausweis
HCI	Health Care Institution
HP	Health Professional
HPC	Health Professional Card
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ICCSN	ICC Serial Number
ID	Identität (Identity)
IK	Individual Key
IPSec	Internet Protocol Security
ISM	Information Security Management
ISO	International Standard Organization
KIS	Krankenhausinformationssystem (Primärsystem der Krankenhäuser)
KT	Kartenterminal
KTR	Kostenträger
KV	Kassenärztliche Vereinigung
KVK	Krankenversichertenkarte

Kürzel	Erläuterung
KVNR	Krankenversichertennummer
KZBV	Kassenzahnärztliche Bundesvereinigung
LÄK	Landesärztekammer
LDAP	Lightweight Directory Access Protocol
LEO	Leistungserbringer-Organisation
LZÄK	Landeszahnärztekammer
MAC	Message Authentication Code
MON	Monitoring
NK	Netzkonnektor
OCSP	Online Certificate Status Protocol
OCSP-R	OCSP-Responder
OID	Object Identifier
OSIG	Organizational Signature
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	PKI nach X.509 Standard der IETF
PrK	Private Key
PuK	Public Key
PVS	Praxisverwaltungssystem (Primärsystem des Arztes)
QES	Qualifizierte elektronische Signatur
RA	Registration Authority
RCA	Root-CA
RFC	Request For Comment
RSA	Rivest Shamir Adleman (Verfahren)
SAK	Signaturanwendungskomponente
SGB	Sozialgesetzbuch
SHA	Secure Hash Algorithm
SIG	Elektronische Signatur
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen
SigV	Signaturverordnung
SLA	Service Level Agreement
SM	Security Module
SMC-B	Sicherheitsmodul vom Typ B <medizinische Institution>
SMC	Security Module Card
gSMC-K	Security Module Card Konnektor als <holder>

Kürzel	Erläuterung
SM-KT-Zertifikat	X.509-Komponentenzertifikat zu einem SM-KT
SubjectDN	Subject Distinguished Name
TCL	Trusted Component List
TI	Telematikinfrastruktur
TLS	Transport Layer Security
TSL	Trust-service Status List
TSP	Trust Service Provider
VPN	Virtual Private Network
XML	Extensible Markup Language
ZDA	Zertifizierungsdiensteanbieter
ZOD	Zahnärzte Online Deutschland

B2 – Glossar

Begriff	Erläuterung
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.

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

B3 – Abbildungsverzeichnis

B4 – Tabellenverzeichnis

B5 - Referenzierte Dokumente

B5.1 – Dokumente der gematik

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

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar
[gemKPT_Arch_TIP]	gematik: Architektur der TI-Plattform
[gemKPT_PKI_TIP]	gematik: Konzept PKI der TI-Plattform
[gemRL_TSL_SP_CP]	gematik: Certificate Policy - Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL
[gemSpec_COS]	gematik: Spezifikation des Card Operating System (COS), Elektrische Schnittstelle
[gemSpec_CVC_Root]	gematik: Spezifikation CVC-Root
[gemSpec_Krypt]	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_OID]	gematik: Spezifikation Festlegung von OIDs
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance

B5.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ALGCAT]	Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) – Geeignete Algorithmen zur Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 SigG in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV Übersicht: http://www.bundesnetzagentur.de/cln_1931/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/algorithmen_node.html
[baekAttr]	Zertifikatsprofile für X.509 Attributzertifikate; Version 2.3.1 vom 29.05.2009
[baekCerts]	Zertifikatsprofile für X.509 Basiszertifikate; Version 2.3.1 vom 29.05.2009
[BÄK_ZPX.509B]	Bundesärztekammer (28.05.2009):

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
	Zertifikatsprofile für X.509 Basiszertifikate V 2.3.1; Zertifikatsaufbau und –hierarchie, Gültigkeitsmodell für Zertifikatstypen: ENC, AUT, QES, ATT sowie die Root, Cross- und CA-Zertifikate, die CRL-Signer und die OCSP-Zertifikate
[BSI-TR-03110]	BSI, Advanced Security Mechanisms for Machine Readable Travel Documents, Version 2.10, 20.03.2012 https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03110/index_htm.html
[BSI-TR-03111]	BSI (2012): Elliptic Curve Cryptography, Version 2.0 https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03111/index_htm.html
[bzaekCert]	Zertifikatsprofil des elektronischen Zahnarztausweises; Version 1.0 vom 29.02.2012
[Common-PKI]	T7 & TeleTrust (20.01.2009): Common PKI Spezifikation, Version 2.0 http://www.t7ev.org/themen/entwickler/common-pki-v20-spezifikation.html
[CP-HPC]	Bundesärztekammer et al (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
[DIN5008]	DIN 5008 (2005): Schreib- und Gestaltungsregeln für die Textverarbeitung
[EN 14890-1]	EN 14890-1 (Draft: February 2007) Application Interface for smart cards used as secure signature Creation Devices - Part 1: Basic services
[ETSI_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
[FIPS 180-4]	Federal Information Processing Standards Publication 180-4 Secure Hash Standard (SHS), March 2012 http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf
[ISO/IEC9594-2]	ISO/IEC 9594-2:2008-12 Information technology - Open Systems Interconnection - The Directory: Models
[ISO3166-1]	ISO/IEC 3166-1:1997 Codes for the representations of names of countries – Part 1: Country codes
[ISO8859-1]	ISO/IEC 8859-1 (1998): Information technology - 8-bit single-byte coded graphic character sets - Part 1: Latin alphabet No. 1
[ISO9796-2]	ISO9796-2: 2002 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://tools.ietf.org/html/rfc2109
[RFC2560]	RFC 2560 (Juni 1999): X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP http://tools.ietf.org/html/rfc2560
[RFC3629]	RFC 3629 (November 2003): UTF-8, a transformation format of ISO 10646 http://tools.ietf.org/html/rfc3629
[RFC3739]	RFC 3739 (March 2004): Internet X.509 Public Key Infrastructure Qualified Certificates Profile http://tools.ietf.org/html/rfc3739
[RFC5280]	RFC 5280 (Mai 2008): Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile http://tools.ietf.org/html/rfc5280
[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
[SigG01]	Bundesgesetzblatt I (2001), S.876: Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. I S. 179)
[SigV01]	Bundesgesetzblatt I (2001), S. 3074: Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch Artikel 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631)
[XML]	World Wide Web Consortium (2006): Extensible Markup Language (XML) 1.0 http://www.w3.org/TR/REC-xml/
[XMLSig]	W3C Recommendation: XML-Signature Syntax and Processing http://www.w3.org/TR/xmldsig-core/