Einführung der Gesundheitskarte

Errata zu Release 1.5.2 Online-Rollout (Stufe 1) Erprobung und Produktivbetrieb

führt zu

Release 1.5.3

Version:	1.0.1
Stand:	02.08.2016
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemErrata_1.5.3]

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	**Anpassungen** an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_5035			Erweiterung des Teilnehmerkreises für die Erprobung der Kommunikation Leistungsbringer (KOM-LE). Das Errata enthält alle wesentlichen Änderungen, die für die Beauftragung zur Erweiterung des Teilnehmerkreises relevant sind. Rein editorielle Änderungen, die technisch ohne Auswirkung sind, werden nicht berücksichtigt.	siehe Anlage zu C_5035	gemProdT_SMC-B, gemSpec_SMC-B_ObjSys, gemSpec_VZD, gemSpec_SMC_OPT, gemSpec_X.509_TSP, gemRL_SMC-B_ORS1, gemRL_TSL_SP_CP, gemSpec_PKI, gemSpec_OID, gemKPT_PKI_TIP, gemSpec_TK,
C_5353	gemSpec_Krypt	Kapitel 3.3.2 TLS-Verbindungen	Die Vielzahl der Primärsysteme arbeitet über .NET mit der Standard-Microsoft-SChannel-Crypto-API. Um eine leichtere Anbindbarkeit dieser Primärsysteme an den Konnektor über das TLS-Protokoll zu erreichen, sollen im Konnektor zusätzliche Ciphersuiten für TLS unterstützt werden.	siehe Anlage zu C_5353	gemSpec_Krypt
C_5345	gemSpec_FM_VSDM	Kapitel 4.7.3	Der Konnektor speichert Fehlermeldungen abhängig vom Errortyp im Sicherheitsprotokoll oder im Fehlerprotokoll des Fachmodules VSDM. Für die Analyse technischer Vorgänge und aufgetretener Fehler ist es notwendig, dass sicherheitsrelevante Fehler auch im Fehlerprotokoll des Fachmodules geloggt werden. Insbesondere wird bei der Auswertung der Erprobung durch das Projekt VSDM das Auftreten der Fehler 106 (Zertifikat auf eGK ungültig (online)) und 107 (Zertifikat auf eGK ungültig (offline)) analysiert. Im dafür verwendeten Fehlerprotokoll des FM VSDM werden diese Fehler nicht geloggt.	*In Kap 4.7.3 wird direkt hinter dem Absatz* Die Protokolleinträge im Fehlerprotokoll enthalten mindestens die in Tab_FM_VSDM_12 aufgezählten Felder. Für jeden in der eigenen Verarbeitung oder in der Kommunikation mit den Fachdiensten bzw. Intermediär aufgetretenen Fehler wird ein Protokolleintrag geschrieben. ... [VSDM-A_2749] *der folgende Absatz ergänzt* In TUC_KON_271 werden das Sicherheits-, System- und fachmodulspezifische Protokoll beschrieben. Um eine Analyse von Fehlern im fachlichen Ablauf zu ermöglichen, müssen für die im Fachmodul VSDM aufgetretenen sicherheitsrelevanten Fehler Einträge im Sicherheitsprotokoll sowie auch im Fehlerprotokoll des Fachmodules VSDM erfolgen. [VSDM-A_3053] *In den Anforderungshaushalt (Anhang B) fließt folgende Information ein:* [VSDM-A_3053] Das Fachmodul VSDM MUSS für alle in der eigenen Verarbeitung oder in der Kommunikation mit den Fachdiensten VSDM, Intermediär VSDM oder dem Primärsystem auftretenden Fehler einen Eintrag im Fehlerprotokoll schreiben.	gemSpec_FM_VSDM gemProdT_Kon
C_5429	gemSysL_VSDM, Schema_VSD.xsd	Anhang C1.3	Änderung gemäß des Asylverfahrensbeschleunigungsgesetzes: "Erweiterung des genutzten Wertebereiches zum Element „Besondere Personengruppe“ um den Wert 9 9 = Empfänger von Gesundheitsleistungen nach §§ 4 und 6 des Asylbewerberleistungsgesetzes (AsylbLG)"	siehe Anlage zu C_5038 und C_5429	gemSysL_VSDM Schema_VSD.xsd

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	Anpassungen an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_5038	gemSysL_VSDM	Anhang C1.2	Entsprechend PStG §22 Abs 3 wird eine Ergänzung der zulässigen Werte innerhalb des VSD-Schema notwendig. (3) Kann das Kind weder dem weiblichen noch dem männlichen Geschlecht zugeordnet werden, so ist der Personenstandsfall ohne eine solche Angabe in das Geburtenregister einzutragen. Die Beschreibung des Wertebereiches für das Merkmal Geschlecht, um "X = unbestimmt" wird erweitert. Aktualisierung des Diagramms zum Element UC_PersoenlicheVersichertendatenXML/Versicherter/Person	siehe Anlage zu C_5038 und C_5429	gemSysL_VSDM Schema_VSD.xsd
C_4952	gemSpec_PK gemSpec_OCSP-Proxy	Kap. 8.5.2 TIP1-A_5844, Tab_OCSP-Proxy_001	Der OCSP-Proxy liest die selbstsignierten QES-Root-Zertifikate der Bundesnetzagentur (BNetzA) aus der TSL aus. Deshalb müssen diese Root-Zertifikate in die TSL eingetragen werden. D.h. die Anforderungslage zu BNetzA-Root-Zertifikaten in der TSL muss aktualisiert bzw. erstellt werden, und der Unterschied zwischen BNetzA-Root- und BNetzA-Cross-Zertifikaten muss erläutert werden. Auch müssen die Beschreibung und die Anforderungslage dazu in gemSpec_OCSP-Proxy geschärft werden.	Siehe Anlage zu C_4952	gemSpecPKI gemSpec_OCSP-Proxy gemProdT_TSL gemProdT_OCSP_Proxy

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	Anpassungen an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_5045	gemSpec_OCSP_Proxy	Tab_OCSP-Proxy_002 Tab_OCSP-Proxy_003 Tab_OCSP-Proxy_005	Es sind Anpassungen der Fehlerbehandlung für den Fehlerfall 3a 1a (Anfrage von HBA-Vorläuferkarten) notwendig und eine Konkretisierung bezüglich der Anzahl an Wiederholungen.	Tab_OCSP-Proxy_002: alt: 3a 1a [OCSP-Proxy]: Der OCSP-Responder im Internet ist nicht erreichbar: OCSP-Response mit einer unsignierten Error-Response des Typs "tryLater" (siehe [RFC2560#2.3]) zurückgeben. neu: 3a 1a [OCSP-Proxy]: Der OCSP-Responder im Internet ist nicht erreichbar: OCSP-Response mit einer unsignierten Error-Response des Typs "internalError" (siehe [RFC2560#2.3]) zurückgeben. Tab_OCSP-Proxy_003: alt: Anzahl Wiederholungen (bei Nicht-Erreichen des OCSP-Responders der BNetzA) neu: Anzahl Wiederholungen (bei Nicht-Erreichen des OCSP-Responders der BNetzA) Anzahl der Versuche = Wiederholungen + 1, d.h. für den Defaultwert "3 Wiederholungen" werden 4 Anfragen gesendet Tab_OCSP-Proxy_005: alt: " ServiceSupplyPoint Internet (Extrahierte Adresse des OCSP-Responders im Internet (BNetzA-OCSP-Responder oder OCSP-Responder der HBA-Vorläuferkarten) aus dem Path der OCSP-Proxy-URI im Element ServiceSupplyPoint). neu: " ServiceSupplyPoint Internet (Extrahierte Adresse des OCSP-Responders im Internet (OCSP-Responder der HBA-Vorläuferkarten) aus dem Path der OCSP-Proxy-URI im Element ServiceSupplyPoint).	gemSpec_OCSP_Proxy, gemProdT_OCSP-Proxy

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	Anpassungen an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_5371	gemSpec_Perf	Kapitel 4.2.4, Anhang C	Zu den Zertifikaten • HBA-Zertifikate (C.HP.QES) • SMC-B-Zertifikate (C.HCI.OSIG) werden sowohl in der TI als auch im Internet gemäß Anforderungslage die Operation check_Revocation_Status zur Abfrage des Sperrstatus bereitgestellt. Es fehlt in [gemSpec_Perf] die Unterscheidung nach der Quelle Internet bzw. TI in Tabelle Tab_gemSpec_Perf_OCSP_Responder für beide Zertifikate und in der Tabelle Tab_gemSpec_Perf_Performance-Kenngroessen für C.HP.QES.	Anpassung in Tab_gemSpec_Perf_OCSP_Responder: alt C.HP.QES: Prüfung von HBA-Zertifikate (C.HP.QES): EE-Zert E: 3,3 P: 500 neu C.HP.QES: Prüfung von HBA-Zertifikate aus der TI (C.HP.QES): EE-Zert E: 3,3 P: 500 ------ Prüfung von HBA-Zertifikate aus dem Internet (C.HP.QES): EE-Zert E: 1 P: 30 alt C.HCI.OSIG: Prüfung von SMC-B-Zertifikaten (C.HCI.OSIG) E: 4 P: 620 neu C.HCI.OSIG: Prüfung von SMC-B-Zertifikaten aus der TI (C.HCI.OSIG) E: 4 P: 620 ---------- Prüfung von SMC-B-Zertifikaten aus dem Internet (C.HCI.OSIG)	gemSpec_Perf
C_5455	gemSpec_SST_Komponenten-PKI	ganzes Dokument	Zur Bedienung der Schnittstellen der PKI für Dienste und Komponenten zur Ausstellung und Sperrung von Zertifikaten sind in der Version 1.9.6 von gemSpec_SST_Komponenten-PKI gegenüber der Version 1.9.3 des Dokumentes Ergänzungen bezüglich zusätzlicheer Zertifikate für den Fachdienst KOM-LE und den neuen Produkttyp Verzeichnisdienst sowie ein zusätzliches CV-Zertifikat für die gSMC-K nötig geworden.	Siehe gemSpec_SST_Komponenten-PKI, Version 1.9.6 mit Änderungsmarkierungen.	gemSpec_SST_Komponenten-PKI

[gemSpec_PKI]

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 Cross~~Link~~-Zertifikate öffentlich zur Verfügung, um die Vertrauenskette sicherzustellen.

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 Cross~~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-

[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.

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.

Diese Prüfung beinhaltet auch eine OCSP-Abfrage zu den Zertifikaten im Prüfpfad. Dafür wird der OCSP-Responder der BNetzA abgefragt. (Vgl. auch TUC_PKI_030 "QES-Zertifikatsprüfung".) Dieser steht im Internet und ist deshalb in der TI nicht direkt erreichbar. Darum stellt der OCSP-Proxy (vgl. gemKPT_PKI_TIP#4.5.1) die OCSP-Responses des OCSP-Responders der BNetzA in der TI bereit.

Der OCSP-Proxy liest alle relevanten QES-CA-Zertifikate aus der TSL aus. Dies umfasst auch die die selbstsignierten Root-Zertifikate der BNetzA. Deshalb werden diese auch in die TSL eingetragen.

⌦ GS-A_5321 Root-Zertifikate der BNetzA

Der TSL-Dienst MUSS für alle in der TI zu prüfenden QES-CA-Zertifikate (inklusive derjenigen für die HBA-Vorläuferkarten) die selbstsignierten Zertifikate der ausstellenden Root-CAs der BNetzA in die TSL aufnehmen.
Der TSL-Dienst MUSS diese Root-CA-Zertifikate in der TSL als QES-CA-Zertifikate markieren.

Die Root-CA-Zertifikate müssen solange in der TSL verbleiben, wie es die gemäß SigV, §4 (2) geforderte Zeitspanne erfordert. ⌫

[gemSpec_OCSP-Proxy]

2 Systemüberblick

Im Rahmen der Telematikinfrastruktur (TI) kommen qualifizierte Signaturzertifikate zum Einsatz, die von akkreditierten Zertifizierungsdiensteanbietern (ZDA) herausgegeben werden. Der Aussteller der CA-Zertifikate für die akkreditierten ZDAs ist in Deutschland die Bundesnetzagentur (BNetzA). Für Statusprüfungen von QES-Zertifikaten in der Telematikinfrastruktur (TI) muss die gesamte Zertifikatskette vom CA-Zertifikat bis zum QES-Wurzelzertifikat der BNetzA geprüft werden. Der OCSP-Responder der BNetzA ist jedoch (a) nicht innerhalb der TI verfügbar und (b) leistungsmäßig nicht für das erwartete Volumen von OCSP-Requests ausgelegt. Daher wird der OCSP-Proxy (OCSP-Proxy) eingesetzt, der als OCSP-Requestor regelmäßig den OCSP-Responder der BNetzA abfragt und mit den zwischengespeicherten Ergebnissen die Anfragen aus der TI bedient.

Ergänzend wird der Produkttyp OCSP-Proxy eingesetzt, um die Statusinformation der Zertifikate der zeitlich begrenzt durch die TI unterstützten HBA-Vorläuferkarten in der TI-Plattform verfügbar zu machen.

Alle ZDA-CA-Zertifikate sowie die Cross- und Wurzelzertifikate der BNetzA und die CA-Zertifikate der HBA-Vorläuferkarten werden in die gematik Trust-service Status List (TSL) aufgenommen. Der Fully Qualified Domain Name (FQDN) des OCSP-Proxys wird als OCSP-Responder-Adresse im TSL-Eintrag für~~des jeweiligen~~ HBA-Vorläufer- und QES-Root-CA-Dienste~~s~~ eingetragen. Der OCSP-Proxy lädt in periodischen Abständen die TSL herunter, identifiziert die relevanten TSL-Einträge anhand des FQDNs für HBA-Vorläufer-Einträge sowie für die QES-Root- und QES-CA-Zertifikate anhand des TSL ServiceTypeIdentifier „http://uri.etsi.org/TrstSvc/Svctype/CA/QC“. Die erkannten Dienste werden anschließend aus der TSL extrahiert ~~diese aus der TSL~~ und ~~legt~~ die erworbenen Informationen im Speicher des OCSP-Proxys abgelegt.

Auf Basis der aus der TSL extrahierten Informationen sendet der OCSP-Proxy in regelmäßigen Abständen OCSP-Anfragen an alle aus der TSL extrahierten ZDA-CA-Zertifikate sowie Cross- und Wurzelzertifikate der BNetzA über das Internet an den OCSP-Responder der BNetzA und speichert die empfangenen OCSP-Antworten (einschließlich der zugehörigen Signatur) zwischen. Der OCSP-Proxy besitzt keine eigene Signaturfunktionalität und verändert die Signatur des OCSP-Responders der BNetzA nicht.

Bei OCSP-Anfragen aus der TI für ZDA-CA-Zertifikate sowie Cross- und Wurzelzertifikate der BNetzA antwortet der OCSP-Proxy mit den zwischengespeicherten OCSP-Antworten des OCSP-Responders der BNetzA. Im Falle von Anfragen für nonQES-End Entity- und QES-End Entity-Zertifikate leitet der OCSP-Proxy die Anfrage an den zuständigen OCSP-Responder im Internet weiter und gibt die vom OCSP-Responder zurück gelieferte OCSP-Antwort an die zertifikatsvalidierende Komponente zurück.

6.1.1 Schnittstelle I_Init_OCSP_Proxy

[..]

⌦ **TIP1-A_5844 Identifizierung und Extraktion der relevanten TSL-Einträge**

Der OCSP-Proxy MUSS die relevanten TSL-Einträge (~~QES-Root-, QES-CA- und~~ CA-Zertifikate der zu unterstützenden HBA-Vorläuferkarten) anhand des FQDN des OCSP-Proxys und für QES-Root-, bzw. QES-CA-Zertifikate anhand des TSL ServiceTypeIdentifier „http://uri.etsi.org/TrstSvc/Svctype/CA/QC“ identifizieren und aus der TSL-Datei extrahieren. ⌫

[..]

⌦ **TIP1-A_5847 Periodische Initialisierung des OCSP-Proxys**

Der OCSP-Proxy MUSS den "TUC_OCSP-Proxy_001 OCSP-Proxy Speicher initialisieren" periodisch gemäß des in Tab_OCSP-Proxy_003 definierten Parameters Periodische Initialisierung durchführen. ⌫

Tabelle 1: Tab_OCSP-Proxy_001 TUC_OCSP-Proxy_001 OCSP-Proxy Speicher initialisieren

Element	Beschreibung
Name	TUC_OCSP-Proxy_001 "OCSP-Proxy Speicher initialisieren"
Beschreibung	Dieser Use Case beschreibt die Ermittlung der QES-Root-, QES-CA-Zertifikate sowie der CA-Zertifikate der unterstützten HBA-Vorläuferkarten aus der TSL-Datei sowie die Befüllung des OCSP-Proxy Speichers mit den relevanten Informationen.
Auslöser	Periodische Initialisierung
Vorbedingungen	Das TSL-Signer-CA-Zertifikat wurde im OCSP-Proxy hinterlegt. Die TSL ist im TSL-Download-Dienst verfügbar.
Eingangsdaten	FQDN des OCSP-Proxys (Zur Identifizierung der relevanten TSL-Einträge) Konfiguration des Parameters Periodische Initialisierung
Komponenten	TSL-Download-Dienst, OCSP-Proxy
Ausgangsdaten	Zertifikatsinformationen der relevanten QES-Root- und QES-CA-Zertifikate sowie der CA-Zertifikate der unterstützten HBA-Vorläuferkarten
Nachbedingungen	
Standardablauf	1. [OCSP-Proxy]: Durchführung des technischen Use Cases "Periodische Aktualisierung TI-Vertrauensraum" gemäß [gemSpec_PKI# TUC_PKI_001]. 2. [OCSP-Proxy]: TSL-Einträge (Element TSPService) der relevanten ~~QES-Root-, QES-CA-Zertifikate sowie~~ CA-Zertifikate der unterstützten HBA-Vorläuferkarten anhand des FQDNs des OCSP-Proxys im Element ServiceSupplyPoint und die QES-Root-, QES-CA-Zertifikate anhand des TSL ServiceTypeIdentifier „http://uri.etsi.org/TrstSvc/Svctype/CA/QC“ Identifizieren. 3. [OCSP-Proxy]: Benötige Zertifikatsinformationen (siehe Tab_OCSP-Proxy_005) aus identifizierten TSL-Einträgen der TSL extrahieren. 4. [OCSP-Proxy]: Vorhandene Zertifikats- und Statusinformationen aus dem Speicher des OCSP-Proxy löschen. 5. [OCSP-Proxy]: Extrahierte Zertifikatsinformationen im Speicher des OCSP-Proxys ablegen. 6. [OCSP-Proxy]: Initiierung der Durchführung des technischen Use Cases "TUC_OCSP-Proxy_003 OCSP-Abfrage an OCSP-Responder der BNetzA senden" zur Abfrage und Speicherung der OCSP-Antworten des BNetzA-OCSP-Responders für QES-Root- und QES-CA-Zertifikate.

Element	Beschreibung
Varianten/Alternativen	1a. [OCSP-Proxy]: Es liegt keine neue TSL-Datei vor. Der Prozess wird beendet. 1b. [OCSP-Proxy]: Es liegt eine neue TSL-Datei vor. Weiter mit Schritt 2.
Fehlerfälle	In jedem der beschriebenen Schritte können Fehler auftreten. Diese werden durch das System protokolliert. Der Prozess wird beendet.
Nichtfunktionale Anforderungen	
Zugehörige Diagramme	
Ergebnisse (Output)	Initialisierter OCSP-Proxy Speicher.
Anmerkungen	

6.4 OCSP-Proxy Speicher

Der OCSP-Proxy legt für jeden notwendigen und damit aus der TSL extrahierten Dienst einen Eintrag mit den benötigten Informationen im Speicher des OCSP-Proxys ab. Die OCSP-Antwort des OCSP-Responders der BNetzA wird dem entsprechenden Eintrag hinzugefügt.

Nachfolgende Tabelle stellt die Attribute des OCSP-Proxy Speichers dar.

Tabelle 5: Tab_OCSP-Proxy_005 Beschreibung der Attribute des OCSP-Proxy Speichers

Informationsobjekt	Attribute
Zertifikatsinformation	ServiceName ServiceTypeIdentifier X509Certificate IssuerNameHash (aus X509Certificate) Für alle zu unterstützenden Hash-Algorithmen gemäß [gemSpec_Krypt] IssuerKeyHash (aus X509Certificate) Für alle zu unterstützenden Hash-Algorithmen gemäß [gemSpec_Krypt] Seriennummer (aus X509Certificate) ServiceSupplyPoint Internet (Extrahierte Adresse des OCSP-Responders im Internet (~~BNetzA-OCSP-Responder oder~~ OCSP-Responder der HBA-Vorläuferkarten) aus dem Path der OCSP-Proxy-URI im Element ServiceSupplyPoint). Authority Information Access (AIA) (aus X509Certificate)
Statusinformationen	OCSP-Antwort des BNetzA-OCSP-Responders

Inhaltsverzeichnis

Änderungen in gemProdT_SMC-B

5.2.Optionale Ausprägungen

In diesem Kapitel werden die optionalen Ausprägungen des Produkttyps SMC-B beschrieben Die Spezifikationen des COS und des Objektsystems der SMC-B. lassen folgende Optionen zu:

- Bereitstellung einer USB-Schnittstelle gemäß [gemSpec_SMC-B_ObjSys#4.3.2]
- Bereitstellung der Funktion Kryptobox gemäß [gemSpec_SMC-B_ObjSys #4.3.3]
- Falls die SMC-B administriert werden soll, müssen bei der Personalisierung
  - o entweder symmetrische Schlüssel für die Authentisierung mit einem CMS / CUpS gemäß [gemSpec_SMC-B_ObjSys#2]
  - o oder asymmetrische Schlüssel für die Authentisierung mit einem CMS / CUpS [gemSpec_SMC-B_ObjSys#2]

  in die entsprechenden Objekte der Karte eingebracht werden.
- Für die Personalisierung der CV-Zertifikate und privaten Schlüssel sind die unterschiedlichen Vorgaben für SMC-Bs der Leistungserbringer-Institutionen (nicht gekennzeichnet) und SMC-Bs in der Ausprägung_ORG (als „Ausprägung_

ORG“ gekennzeichnet) zu berücksichtigen, die in den Anforderungen Card-G2-A_3346, Card-G2-A_3348, Card-G2-A_3349, Card-G2-A_3353 und Card-G2-A_3355 festgelegt sind.

- Die SMC-B kann gemäß [gemSpec_SMC-B_ObjSys#2] als Testkarte ausgestaltet werden.

Änderungen in gemSpec_SMC-B_ObjSys

2.2. Ausprägung ohne Zugriff auf die eGK

SMC-Bs können auch in Organisationen eingesetzt werden, die an der TI teilnehmen, aber nicht zum Zugriff auf die eGK berechtigt sind. Um zu verhindern, dass eine solche SMC-B den Zugriff auf eine eGK freischalten kann, werden ihre Rollen-Zertifikate EF.C.SMC.AUTR_CVC.R2048 und EF.C.SMC.AUTR_CVC.E256 sowie das Zertifikat EF.C.CA_SMC.CS.R2048 der RSA-Sub-CA bei der Personalisierung entweder gar nicht oder mit Nullen befüllt. Die entsprechenden Schlüssel bleiben herstellerspezifisch „unbefüllt“ oder werden mit nichtnutzbaren Dummy-Daten befüllt.

Dies wird in den entsprechenden Personalisierungsfestlegungen mit dem Zusatz „Ausprägung_ORG“ gekennzeichnet.

5.3.5 MF / EF.C.CA_SMC.CS.R2048

Diese Datei enthält ein CV-Zertifikat für die Kryptographie mit RSA gemäß [gemSpec_COS], welches den öffentlichen Schlüssel PuK.CA_SMC.CS.R2048 einer CA enthält. Für die Ausprägung_ORG bleibt diese Datei leer oder wird mit Nullen befüllt.

⌦ **Card-G2-A_3346 K_Personalisierung: Personalisierte Attribute von MF / EF.C.CA_SMC.CS.R2048**

Bei der Personalisierung von EF.C.CA_SMC.CS.R2048 MÜSSEN die in Tab_SMC-B_ObjSys_068 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 10: Tab_SMC-B_ObjSys_068 Personalisierte Attribute von MF / EF.C.CA_SMC.CS.R2048

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	‘01 4B’ Oktett = 331 Oktett	
positionLogicalEndOfFile Ausprägung_ORG	Wildcard	Entsprechend dem Verfahren des Personalisierers und

Attribute	Wert	Bemerkung
		dem Attribut body
body	C.CA_SMC.CS.R2048 gemäß [gemSpec_PKI]	
body Option_Erstellung_von_Testkarten	C.CA_SMC.CS.R2048 gemäß [gemSpec_PKI] aus Test-CVC-CA	Details siehe [gemSpec_TK#3.1.2]
body *Ausprägung_ORG*	Leer oder '00 … 00'	Entsprechend dem Verfahren des Personalisierers und dem Wert von positionLogicalEndOf File

⌫

5.3.7.MF / EF.C.SMC.AUTR_CVC.R2048

EF.C.SMC.AUTR_CVC.R2048 enthält das CV-Zertifikat der SMC-B für die Kryptographie mit RSA für rollenbasierte C2C-Authentisierung zwischen SMC-B und eGK. Das zugehörende private Schlüsselobjekt PrK.SMC.AUTR_CVC.R2048 ist im Kapitel 5.3.11 definiert. Für die Ausprägung_ORG bleibt diese Datei leer oder wird mit Nullen befüllt.

⌦ **Card-G2-A_3348 K_Personalisierung: Personalisierte Attribute von MF / EF.C.SMC.AUTR_CVC.R2048**

Bei der Personalisierung von EF.C.SMC.AUTR_CVC.R2048 MÜSSEN die in Tab_SMC-B_ObjSys_071 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 14: Tab_SMC-B_ObjSys_071 Personalisierte Attribute von MF / EF.C.SMC.AUTR_CVC.R2048

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	'0155' Oktett = 341 Oktett	
positionLogicalEndOfFile *Ausprägung_ORG*	Wildcard	Entsprechend dem Verfahren des Personalisierers und passend zu body
body	C.SMC.AUTR_CVC.R2048 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.SMC.AUTR_CVC.R2048	
body *Ausprägung_~~LEO~~ORG*	Leer oder '00 … 00'	Entsprechend dem Verfahren des Personalisierers und passend zu positionLogicalEndOfFile

⌫

5.3.8.MF / EF.C.SMC.AUTR_CVC.E256

EF.C.SMC.AUTR_CVC.E256 enthält das CV-Zertifikat der SMC-B für die Kryptographie mit elliptischen Kurven für rollenbasierte C2C-Authentisierung zwischen SMC-B und eGK. Das zugehörende private Schlüsselobjekt PrK.SMC.AUTR_CVC.E256 ist im Kapitel 5.3.12 definiert. Für die Ausprägung_ORG bleibt diese Datei leer oder wird mit Nullen befüllt.

⌦ **Card-G2-A_3349 K_Personalisierung: Personalisierte Attribute von MF / EF.C.SMC.AUTR_CVC.E256**

Bei der Personalisierung von EF.C.SMC.AUTR_CVC.E256 MÜSSEN die in Tab_SMC-B_ObjSys_072 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 1: Tab_SMC-B_ObjSys_072 Personalisierte Attribute von MF / EF.C.SMC.AUTR_CVC.E256

Attribute	Wert	Bemerkung
positionLogicalEndOfFile	'00DE' Oktett = 222 Oktett	
positionLogicalEndOfFile Ausprägung_~~LEO~~ORG	Wildcard	Entsprechend dem Verfahren des Personalisierers und passend zu body
body	C.SMC.AUTR_CVC.E256 gemäß [gemSpec_PKI] passend zu dem privaten Schlüssel in PrK.SMC.AUTR_CVC.E256	
body Ausprägung_~~LEO~~ORG	Leer bzw. '00 … 00'	Entsprechend dem Verfahren des Personalisierers und passend zu positionLogicalEndOf File

⌫

5.3.11.MF / PrK.SMC.AUTR_CVC.R2048

PrK.SMC.AUTR_CVC.R2048 ist der globale private Schlüssel für die Kryptographie mit RSA für die C2C-Authentisierung zwischen SMC-B/eGK. Der zugehörige öffentliche Schlüssel PuK.SMC.AUTR_CVC.R2048 ist in C.SMC.AUTR_CVC.R2048 (siehe Kapitel 5.3.7) enthalten. Für die Ausprägung_ORG bleibt dieser Schlüssel herstellerspezifisch „unbefüllt" oder wird mit Zufallswerten befüllt.

⌦ **Card-G2-A_3353 K_Personalisierung: Personalisierte Attribute von MF / PrK.SMC.AUTR_CVC.R2048**

Bei der Personalisierung von PrK.SMC.AUTR_CVC.R2048 MÜSSEN die in Tab_SMC-B_ObjSys_077 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 23: Tab_SMC-B_ObjSys_077 Personalisierte Attribute von MF / PrK.SMC.AUTR_CVC.R2048

Attribute	Wert	Bemerkung
privateKey	Moduluslänge 2048 Bit	
privateKey Ausprägung_ *~~LEO~~ORG*	Moduluslänge 2048 Bit Herstellerspezifisch „nicht nutzbar“ (z.B. mit Zufallswerten)	Entsprechend dem Verfahren des Personalisierers
keyAvailable	True	
keyAvailable Ausprägung_ *~~LEO~~ORG*	False, ggf. True	Entsprechend dem Verfahren des Personalisierers

⌫

5.3.12.MF / PrK.SMC.AUTR_CVC.E256

PrK.SMC.AUTR_CVC.E256 ist der globale private Schlüssel für die Kryptographie mit elliptischen Kurven für die C2C-Authentisierung zwischen SMC-B/eGK. Der zugehörige öffentliche Schlüssel PuK.SMC.AUTR_CVC.E256 ist in C.SMC.AUTR_CVC.E256 (siehe Kapitel 5.3.8) enthalten. Für die Ausprägung_ORG bleibt dieser Schlüssel herstellerspezifisch „unbefüllt“ oder wird mit Zufallswerten befüllt.

⌦ **Card-G2-A_3355 K_Personalisierung: Personalisierte Attribute von MF / PrK.SMC.AUTR_CVC.E256**

Bei der Personalisierung von PrK.SMC.AUTR_CVC.E256 MÜSSEN die in Tab_SMC-B_ObjSys_078 angegebenen Attribute mit den dort angegebenen Inhalten personalisiert werden.

Tabelle 25: Tab_SMC-B_ObjSys_078 Personalisierte Attribute von MF / PrK.SMC.AUTR_CVC.E256

Attribute	Wert	Bemerkung
keyAvailable	True	
keyAvailable Ausprägung_ *~~LEO~~ORG*	False, ggf. True	Entsprechend dem Verfahren des Personalisierers
privateElcKey	keyData = Wildcard	
privateElcKey Ausprägung_	Herstellerspezifisch „nicht nutzbar“ (z.B. mit Zufallswerten)	Entsprechend dem Verfahren des

Attribute	Wert	Bemerkung
~~LEO~~ORG		Personalisierers

⌫

Änderungen in gemSpec_VZD

⌦ **TIP1-A_5610 VZD, Einwilligung muss vorliegen**

Der Anbieter des VZD muss sicherstellen, dass die informierte Einwilligung des betroffenen Leistungserbringers oder der durch die Gesellschafter vertretenen Organisation vorliegt, bevor er dessen Daten auf dem Verzeichnisdienst der TI speichert.⌫

⌦ **TIP1-A_5611 VZD, Widerspruch der Einwilligung**

Der Anbieter des VZD muss die Daten des Leistungserbringers oder der durch die Gesellschafter vertretenen Organisation unverzüglich vom Verzeichnisdienst löschen, sobald ihm der Widerruf der Einwilligung durch den Leistungserbringer oder die durch die Gesellschafter vertretene Organisation bekannt wird.⌫

⌦ **TIP1-A_5606 VZD, Mandat zur Löschung von Einträgen.**

Der Anbieter des VZD MUSS einen Prozess implementieren, der es Leistungserbringern oder der durch die Gesellschafter vertretenen Organisationen ermöglicht ihren Eintrag im VZD ohne zugehörige Smartcard zu löschen.

Der Anbieter des VZD MUSS vom Leistungserbringer oder von der durch die Gesellschafter vertretenen Organisationen einen Nachweis fordern und prüfen, dass die zu löschenden Daten dem Leistungserbringer oder der durch die Gesellschafter vertretenen Organisation gehören. Erst nach positivem Ergebnis der Prüfung darf gelöscht werden.

Der VZD-Anbieter dokumentiert den Prozess und legt ihn dem GBV zur Freigabe vor.⌫

Änderungen in gemSpec_SMC_OPT

⌦ **Card-G2-A_2012 Layout Vorderseite SMC-B, Profil**

Auf die Vorderseite der SMC-B MUSS gemäß Abbildung Abb_SMCOPT_02, Region 3, das Wort „Profil“ und rechtsbündig darüber die ~~Profilnummer~~ Profilbezeichnung des organisationsbezogenen Profils aufgedruckt werden ~~(Profilnummer < 50).~~ SMC-Bs, die keinem Profil zugeordnet werden und damit keine Rechte zum Zugriff auf die eGK besitzen, MÜSSEN anstelle der Profilbezeichnung den Aufdruck „-“ erhalten.

Die Profilbezeichnung ist die auf den Text „CHA.“ folgende Zeichenkette in der Spalte Zugriffsprofil der Tabelle „Tab_PKI_254 Zugriffsprofile für eine Rollenauthentisierung“.
⌫

Änderungen in gemSpec_X.509_TSP

Tabelle 2: Tab_PKI_502 Berechtigte Zertifikatsantragsteller für nonQES Leistungserbringer-, LEO bzw. KTR-Organisation und Versichertenzertifikate

Zertifikatstyp	Berechtigte Zertifikatsantragsteller	Berechtigungsprüfende Stelle	Zertifikatsnehmer
C.HP.AUT C.HP.ENC	Leistungserbringer	herausgebende LEO	Leistungserbringer
C.HCI.AUT C.HCI.ENC C.HCI.OSIG	Leistungserbringer der med. Institution	herausgebende LEO	med. Institution
	Zeichnungsberechtigter Mitarbeiter d. zertifikatsnehmenden Gesellschafterorganisation	Herausgebende Organisation (z.B. Spitzenverband d. zertifikatsnehmenden Gesellschafterorganisation)	Gesellschafterorganisation
	KTR-Organisation	KTR-Organisation	Kostenträger-Geschäftsstelle
C.CH.AUT C.CH.ENC C.CH.AUTN C.CH.ENCV	herausgebender Kostenträger	herausgebender Kostenträger	Versicherter

Tabelle 6: Tab_PKI_511 Berechtigte Zertifikatsantragsteller für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate

Zertifikatstyp	Berechtigte Zertifikatsantragsteller	Berechtigungsprüfende Stelle	Zertifikatsnehmer
C.NK.VPN	Hersteller	gematik	Konnektor
C.SAK.AUT	Hersteller	gematik	Konnektor
C.AK.AUT	Hersteller	gematik	Konnektor
C.SMKT.AUT	Hersteller	gematik	Kartenterminal
C.FD.TLS-C	Diensteanbieter	gematik	Fachanwendungsspezifischer Dienst
C.FD.TLS-S	Diensteanbieter	gematik	Fachanwendungsspezifischer Dienst
C.ZD.AUT	Diensteanbieter	gematik	Fachanwendungsspezifischer Dienst
C.ZD.TLS-C	Diensteanbieter	gematik	Zentraler Dienst
C.ZD.TLS-S	Diensteanbieter	gematik	Zentraler Dienst

Zertifikatstyp	Berechtigte Zertifikatsantragsteller	Berechtigungsprüfende Stelle	Zertifikatsnehmer
C.VPNK.VPN	Diensteanbieter	gematik	VPN-Zugangsdienst
C.VPNK.VPN-SIS	Diensteanbieter	gematik	VPN-Zugangsdienst
C.GEM.OCSP	TSP-X.509 nonQES	gematik	TSP-X.509 nonQES
C.GEM.CRL	TSP-X.509 nonQES	gematik	TSP-X.509 nonQES
C.HP.AUT	TSP-X.509 QES	gematik Kartenherausgeber	Leistungserbringer
C.HP.ENC	TSP-X.509 QES	gematik Kartenherausgeber	Leistungserbringer
C.HCI.AUT	Kartenherausgeber	gematik Kartenherausgeber	med. Institution Gesellschafterorganisations-Geschäftsstelle/Betriebsstätte Kostenträgergeschäftsstelle
C.HCI.ENC	Kartenherausgeber	gematik Kartenherausgeber	med. Institution Gesellschafterorganisations-Geschäftsstelle/Betriebsstätte Kostenträgergeschäftsstelle
C.HCI.OSIG	Kartenherausgeber	gematik Kartenherausgeber	med. Institution Gesellschafterorganisations-Geschäftsstelle/Betriebsstätte Kostenträgergeschäftsstelle

Tabelle 8: Tab_PKI_514 Berechtigte Sperrantragsteller für nonQES-Personen- und Organisationszertifikate

Zertifikatstyp	Berechtigte Sperrantragsteller	zulässiger Sperrgrund
C.HP.AUT C.HP.ENC	Leistungserbringer selbst	zu jeder Zeit ohne Angabe von Gründen
	herausgebende LEO	bei Entzug oder Wegfall des Berufsattributes in einem geregelten Verfahren gemäß Ausgabepolicy
C.HCI.AUT C.HCI.ENC C.HCI.OSIG	Zertifikatsnehmende med. Institution, Gesellschafter-organsations- oder Kosten-trägergeschäftsstelle	zu jeder Zeit ohne Angabe von Gründen
	Herausgebende Organisation (LEO bei SMC-B für medizinische Institutionen, Vertretende	festgestellter Wegfall der Voraussetzungen für den Betrieb einer SMC-B gemäß deren Ausgabepolicy

Zertifikatstyp	Berechtigte Sperrantragsteller	zulässiger Sperrgrund
	Gesellschafterorganisation bei SMC-B für Gesellschafterorganisationen, Vertretende Kostenträger-Organisation für SMC-B für Kostenträger)	

Änderungen in gemRL_SMC-B_ORS1

1.1.Überblick

Das vorliegende Dokument beschreibt die Regelungen zur Beantragung, Herausgabe und Verwendung von SMC-B-Zertifikaten während der Erprobungsphase „Online-Rollout (Stufe 1)“ zur Einführung der Gesundheitskarte.

Die hierin getroffenen Regelungen bilden widerspruchsfrei zur „Certificate Policy – Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL“[1] als sektorspezifische Präzisierung diejenigen Sachverhalte ab, die für Vergabe- und Auftragserteilung in ORS1 relevant sind.

Es werden die übergreifenden Regelungen beschrieben, wie sie für alle Teilnehmer der Telematikinfrastruktur einheitlich gelten. Der Geltungsbereich umfasst die TSP, die der gematik Root-CA nachgeordnet sind (TSP-X.509 nonQES). Sowie auch den TSP, der CV-Zertifikate für die Ausstattung der SMC-B herausgibt.

Konzeptionell existieren drei Ausprägungen der SMC-B:

- SMC-B einer Gesellschafterorganisation
  (Diese erlaubt keinen Zugriff auf eGKs)
- SMC-B einer medizinischen Institution bzw. Leistungserbringerinstitution
- SMC-B eines Kostenträgers
  Diese wird zu einem späteren Zeitpunkt eingeführt. Deshalb wird sie in diesem Dokument nicht weiter besprochen.

1.2.3.Zertifikatsnehmer (Subscribers)

Der Zertifikatsnehmer einer SMC-B ist die medizinische Institution oder Organisation des Gesundheitswesens, die über die Zertifikate der SMC-B repräsentiert wird.

- Für die SMC-B für medizinische Institutionen ist dies eine medizinische Institution bzw. Leistungserbringerinstitution.

[1] [gemRL_TSL_TSP_CP]

- Für die SMC-B für Gesellschafterorganisationen ist dies eine Gesellschafterorganisationen bzw. deren Geschäftsstelle / Betriebsstätte.

Antragsteller der SMC-B und somit der enthaltenen Zertifikate ist immer eine natürliche Person, die für die medizinische Institution oder Organisation des Gesundheitswesens vertretungs- und zeichnungsberechtigt ist.

1.2.5. Attributbestätigende Stellen / SMC-B-Herausgeber

Die Hoheit zur Verwaltung und Vergabe der institutions- bzw. organisationsspezifischen X.509-Attribute und die Herausgabe der SMC-B obliegen den vertretungsberechtigten Organisationen.

Für medizinische Institutionen sind dies:

- KBV – Bestätigt die institutionsspezifischen Attribute der SMC-B für Praxen der Vertragsärzte, privat abrechnender Ärzte und der Vertragspsychotherapeuten[2]
- KZV – Bestätigt die institutionsspezifischen Attribute der SMC-B für Zahnarztpraxen
- DKTIG – Bestätigt die institutionsspezifischen Attribute der SMC-B für Krankenhäuser

Für Gesellschafterorganisationen ist dies:

- KZBV – Bestätigt (als Spitzenverband) das Attribut einer KZV als Betriebsstätte einer Gesellschafterorganisation

Kapitel 1.5.1 SMC-B:

Tabelle 1: Tab_PKI_960 Sektorinterne Alternativbezeichnung der SMC-B

Sektor	Sektorinterne Bezeichnung / Alternativbezeichnung der SMC-B
Vertragsärzte, Vertragspsychotherapeuten	Institutionsausweis
Zahnärzteschaft	Praxisausweis
Krankenhäuser	SMC-B
KZVen	SMC-B

Kapitel 1.5.5 Attributbestätigende Stelle und Zertifikatsherausgeber:

Tabelle 2: Tab_PKI_961 Übersicht der Attributbestätigenden Stellen / SMC-B-Herausgeber

[2] Durch die KVen werden die Niederlassungen der Berufsgruppen der „Psychologischen Psychotherapeuten“ und der „Kinder- und Jugendlichenpsychotherapeuten“ vertreten. Im Dokument werden diese beiden Professionen der besseren Lesbarkeit wegen, unter der Kurzbezeichnung „Psychotherapeuten“ geführt.

Sektor	Attributbestätigende Stelle / SMC-B-Herausgeber
Niedergelassene Vertragsärzte Vertragspsychotherapeuten Psychologische Psychotherapeuten Kinder- und Jugendlichen-psychotherapeuten	Kassenärztliche Vereinigung (KV dezentral)
Institutionen der Vertragszahnärzteschaft	Kassenzahnärztliche Vereinigung (KZV dezentral)
KZV-Geschäftsstellen	Kassenzahnärztliche Bundesvereinigung (KZBV zentral)
Nicht-Vertragsärzte (privat abrechnende Ärzte) und Psychotherapeuten)	Kassenärztliche Bundesvereinigung (KBV zentral)
Krankenhaus	Deutsche Krankenhaus TrustCenter und Informations-verarbeitung GmbH (DKTIG zentral)

3.2.5.Überprüfung der Berechtigung

Die Überprüfung der Berechtigung einer medizinischen Institution oder einer Organisation des Gesundheitswesens zum Erhalt und zur Verwendung einer SMC-B wird durch den Herausgeber (jeweils zuständige Vereinigung dieser medizinischen Institutionen oder Organisationen des Gesundheitswesens) durchgeführt.

Die Überprüfung der Berechtigung einer natürlichen Person zur Beantragung einer SMC-B zur Vertretung einer medizinischen Institution oder einer Organisation des Gesundheitswesens, wird durch den Herausgeber durchgeführt.

- Im Falle der Leistungserbringerinstitutionen ist dies die jeweils zuständige Vereinigung dieser medizinischen Institutionen.
- Im Falle der KZV-Geschäftsstellen ist dies die KZBV.

Die Person muss dort als vertretungsberechtigt eingetragen sein.

Kapitel 4.1 Zertifikatsantrag

Tabelle 3: Tab_ PKI_962 Erforderliche Antragsdaten

	KZV	KV, KBV	DKTIG	KZBV
Antrag				
Art des Antrags	Auswahl: Erstantrag	Auswahl: Erstantrag		

	KZV	**KV, KBV**	**DKTIG**	**KZBV**
	Folgeantrag	Folgeantrag Löschantrag		
Antragsteller				
Name	Name (optional: Titel)			Name (optional: Titel)
Vorname	Vorname(n)			Vorname(n)
Geburtsdatum	Datum			Datum
Meldeanschrift	Straße Hausnummer Postleitzahl Ort			Straße Hausnummer Postleitzahl Ort
~~Legitimationsnachweis~~	~~- - -~~	~~- Vorlage amtl. Lichtbildausweis~~ ~~- Nachweis der Approbation~~		~~- - -~~
Medizinische Institution / Organisation d. Gesundheits-wesens				
Name	Name (optional: Namenszusatz)			Name (optional: Namenszusatz)
Rechtsform	- - -	Auswahl: Einzelgesellschaft GmbH AG Sonstige …		- - -
Organisationsform der medizinischen Institution	Auswahl: Einzelpraxis BAG ÜBAG KÜBAG MVZ			
Namen aller Gesellschafter (bei Nicht-Ein-Personen-Praxen)	Name(n) (optional: Titel)			
Zuständige Stelle	Auswahl: Zuständige KZV			

	KZV	KV, KBV	DKTIG	KZBV
Institutionsnummer bei der zuständigen Stelle	Nummer			
Abrechnungsnummer bei der zuständigen Stelle	Nummer			
Anschrift	Straße Hausnummer Postleitzahl Ort			Straße Hausnummer Postleitzahl Ort
Lieferanschrift (falls abweichend; optional)	Straße Hausnummer Postleitzahl Ort			Straße Hausnummer Postleitzahl Ort
E-Mail-Adresse	E-Mail-Adresse gem. RFC-822			E-Mail-Adresse gem. RFC-822

4.1.1. Wer kann ein SMC-B Zertifikat beantragen?

Antragsberechtigt sind medizinische Institutionen und Organisationen des Gesundheitswesens. Juristische Personen werden dabei vertreten durch nachgewiesen vertretungs- / zeichnungsberechtigte natürliche Personen.

Die Berechtigung der medizinische Institution zum Bezug einer SMC-B ~~LEI~~ mit den entsprechenden Autorisierungsinformationen wird dieser zugewiesen durch die Bestätigung eines qualifizierenden Rollenattributs (z. B. „Arztpraxis“, „Zahnarztpraxis“, „Krankenhaus“ o. ä.) einer anerkannten Standesorganisation.[3]

Analog wird die Berechtigung zum Bezug einer SMC-B für Gesellschafterorganisation vergeben. Diese enthält aber keine Berechtigungen zum Zugriff auf eGKs.

Antragsberechtigt in diesem Sinne sind die medizinischen Institutionen und Organisationen des Gesundheitswesens gemäß

- [gemSpec_OID#3.5.1]

4.1.2.3.Sektor: Vertragszahnärzteschaft (KZV-Geschäftsstellen)

Die Beantragung einer SMC-B für Gesellschafterorganisation erfolgt durch

- eine vertretungsberechtigte natürliche Person (Mitglied des Vorstandes der jeweiligen KZV) oder

[3] [gemSpec_PKI], Kap 6.3, GS-A_4621 und Tab_PKI_254

- durch einen Mitarbeiter, welcher durch eine vertretungsberechtigte Person schriftlich dazu ermächtigt wurde (Delegation).

4.1.2.4 Sektor: Vertragszahnärzteschaft (KZV-Geschäftsstellen)

Zuständig für Freigabe und Sperrung von Zertifikaten auf der SMC-B ist die KZBV.

Der Ablauf der Antragstellung verläuft analog wie in 4.1.2.1 beschrieben.

Kapitel 4.4.2 Veröffentlichung des Zertifikats durch die Zertifizierungsstelle

Tabelle 4: Tab_PKI_963 Bereitstellung der SMC-B-Statusauskünfte

	KZV	**KV, KBV**	**DKTIG**	**KZBV**
Innerhalb der TI	OCSP	OCSP	OCSP	OCSP
Internet	CRL, OCSP	CRL	-	CRL, OCSP

Kapitel 4.9.2 Wer kann Widerruf / Sperrung beantragen

Tabelle 5: Tab_PKI_964 SMC-B – Sperrberechtigte und Sperrgründe

Sperrberechtigte Stellen *)	Zertifikate der Kartenarten				
		HBA			
	eGK	nonQES	**SMC-B**	gSMC-K	FD, ZD
Praxis / med. Institution / KZV-Geschäftsstelle			**1**		
KV / KZV / KBV / DKTIG / KZBV			**2, 4**		
gematik			**3**		

1) Jederzeit ohne Angabe von Gründen
2) Wegfall oder Entzug geforderter Eigenschaften des Antragstellers gemäß Ausgabepolicy
3) Wegfall oder Entzug geforderter Eigenschaften des TSP gemäß gematik-Zulassung
4) Wegfall oder Entzug geforderter Eigenschaften des ZDA/TSP gemäß Beauftragung bzw. sektoraler Zulassung

Änderungen in gemRL_TSL_SP_CP

Kap. 5.9.1 Bedingungen für eine Sperrung

Tabelle 2: Tab_PKI_305 Übersicht der PKI-spezifischen Sperrgründe

	Zertifikate der Kartenarten

Sperrberechtigte Stellen *)	eGK	HBA nonQES	SMC-B LEI	SMC-B ORG	SMC-B KTR	gSMC-K	FD, ZD
LE		1a	1a				
med. Institution			1a				
Hersteller						1b	
Anbieter **)							1b, 3
Herausgebende LEO **)		2,5	2,5	~~21a~~	~~2~~		
Zertifikatsnehmende LEO				1a			
GKV-Spitzenverband **)				2	2		
KTR **)	1a, 2		~~2~~	1a	1a		
gematik		3	3	3	3	3	3

Änderungen in gemSpec_PKI

Kap. 6.3.1 Rollenauthentisierung

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

Der Kartenherausgeber MUSS sicherstellen, dass bei einem HBA bzw. einer SM-B das Zugriffsprofil in einem CV-Zertifikat der Rolle des Karteninhabers bzw. der Organisation gemäß Tabelle Tab_PKI_254 entspricht. Eine Ausnahme hiervon ist die SM-B für Gesellschafterorganisationen, da sie keine CV-Rollenzertifikate erhält. ⌫

Tabelle 103: Tab_SMCB_KZBV_KZV SMC-B-Zertifikate für KZV (Sektor KZBV)

Element	Inhalt	Kar.	
certificate	C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG		
tbsCertificate			
version	siehe Kap 5.3.4		
serialNumber	siehe Kap 5.3.4		
signature	siehe Kap 5.3.4		
issuer	siehe Kap 5.3.4		

Element	Inhalt	Kar.	
validity	siehe Kap 5.3.4		
subject			
commonName	**Gemäß Freigabedaten der KZBV**	**1**	
title	**nicht belegt**	**0**	
surName	**nicht belegt**	**0**	
givenName	**nicht belegt**	**0**	
serialNumber	**TI-weit eindeutiger Identifier der Karte z.B. in der Form: <TSP-ID>.<ICCSN>**	**1**	
streetAddress	**nicht belegt**	**0**	
postalCode	**nicht belegt**	**0**	
localityName	**nicht belegt**	**0**	
stateOrProvinceName	**nicht belegt**	**0**	
organizationalUnitName	**nicht belegt**	**0**	
organizationName	**Telematik-ID gemäß Freigabedaten der KZBV**	**1**	
countryName	siehe Kap 5.3.4	1	
andere Attribute		0	
subjectPublicKeyInfo	siehe Kap 5.3.4		
extensions			critical
SubjectKeyIdentifier {2 5 29 14}	siehe Kap 5.3.4	1	FALSE
KeyUsage {2 5 29 15}	siehe Kap 5.3.4	1	**TRUE**
SubjectAltNames {2 5 29 17}	**Komplettangabe zur bertreffenden KZV**	**0-1**	**FALSE**
BasicConstraints {2 5 29 19}	siehe Kap 5.3.4	1	**TRUE**
CertificatePolicies {2 5 29 32}	siehe Kap 5.3.4 zusätzlich: **policyIdentifier = <oid_policy_gem_or_cp_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}	**admissionAuthority = {O=Kassenzahnärztliche Bundesvereinigung,C=DE}** **professionItem = <oid_leo_zahnaerzte>** **professionOID = <oid_leo_zahnaerzte>** **registrationNumber <Telematik-ID gemäß Freigabedaten der KZBV>**	**1** **1** **1** **1**	**FALSE**
ExtendedKeyUsage {2 5 29 37}	siehe Kap 5.3.4	1	FALSE
andere Erweiterungen		0	
signatureAlgorithm	siehe Kap 5.3.4		

Element		Inhalt	Kar.	
	signature	siehe Kap 5.3.4		

Änderungen in gemSpec_OID

Kap. 3.5.1.3 OID-Festlegung für Institutionstypen für die SMC-B

⌦ **GS-A_4443 OID-Festlegung für Institutionen**

Ein TSP-X.509 MUSS die Institutionen für die Nutzung in X.509-Zertifikaten der TI mit OIDs entsprechend der Tabelle Tab_PKI_403 referenzieren. ⌫

Tabelle 3: Tab_PKI_403 OID-Festlegung Institutionen im X.509-Zertifikat der SMC-B

OID-Referenz in anderen Dokumenten	**Profession Item** (Beschreibung der Institution)	**ProfessionOID** (OID der Institution)
oid_praxis_arzt	Betriebsstätte Arzt	1.2.276.0.76.4.50
oid_zahnarztpraxis	Zahnarztpraxis	1.2.276.0.76.4.51
oid_praxis_psychotherapeut	Betriebsstätte Psychotherapeut	1.2.276.0.76.4.52
oid_krankenhaus	Krankenhaus	1.2.276.0.76.4.53
oid_oeffentliche_apotheke	Öffentliche Apotheke	1.2.276.0.76.4.54
oid_krankenhausapotheke	Krankenhausapotheke	1.2.276.0.76.4.55
oid_bundeswehrapotheke	Bundeswehrapotheke	1.2.276.0.76.4.56
oid_mobile_einrichtung_ rettungsdienst	Betriebsstätte Mobile Einrichtung Rettungsdienst	1.2.276.0.76.4.57
oid_bs_gematik	Betriebsstätte gematik	1.2.276.0.76.4.58
oid_kostentraeger	Betriebsstätte Kostenträger	1.2.276.0.76.4.59
oid_leo_zahnaerzte	Betriebsstätte Leistungserbringerorganisation Vertragszahnärzte	1.2.276.0.76.4.187

Änderungen in gemKPT_PKI_TIP

2.5.2.CV-Zertifikate für Karten in der TI

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

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

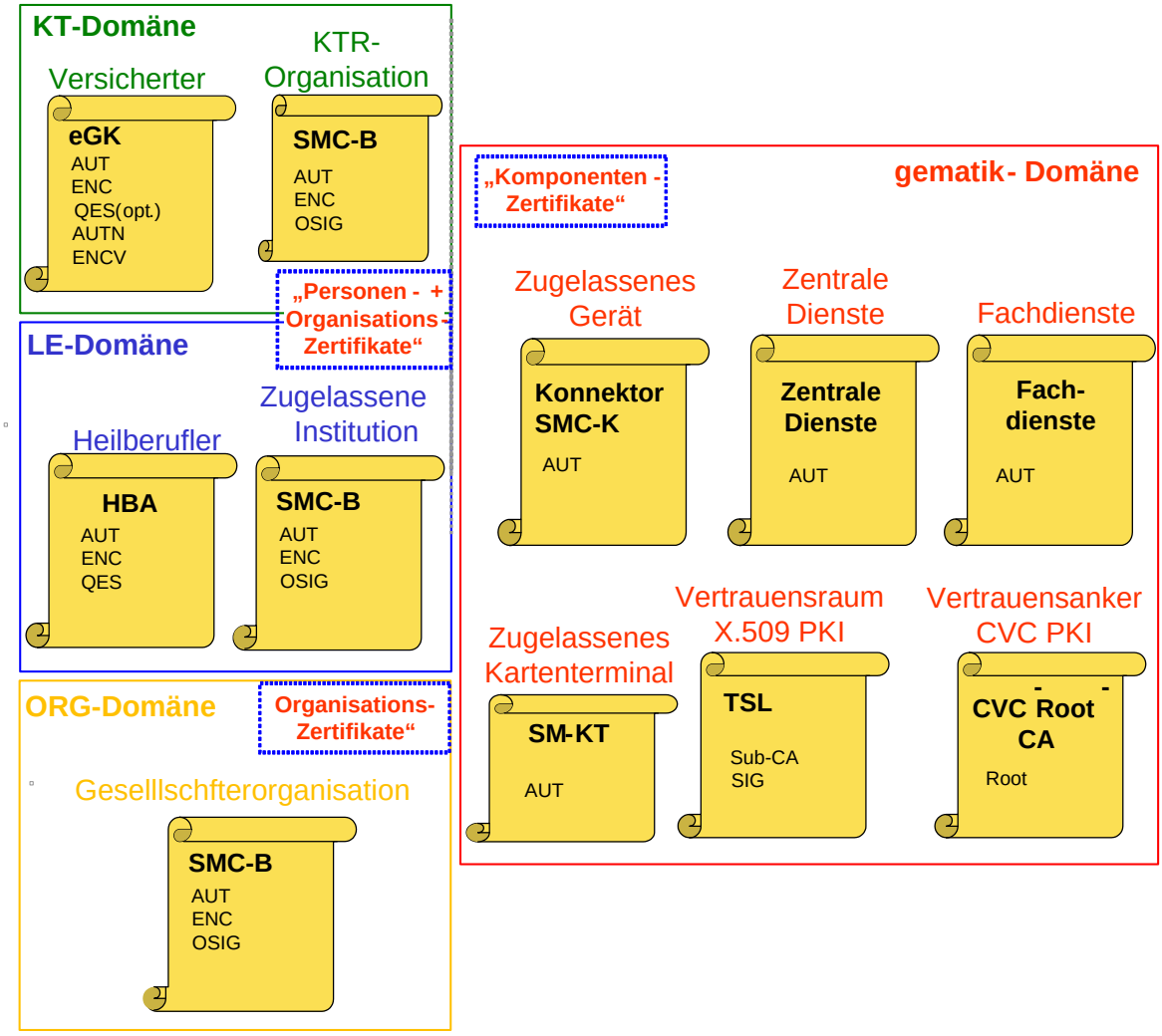


Abbildung 1: Zuordnung der Verantwortlichkeiten für die Zertifikate

Tabelle 4: Tab_PKI_107 Übersicht der PKI-spezifischen Sperrgründe

Sperrberechtigte Stellen *)			Zertifikate der Kartenarten					
		HBA	HBA	SMC-B	SMC-B	SMC-B		
	eGK	QES	nonQES	LEI	ORG	KTR	gSMC-K	FD, ZD

LE		1a	1a	1a				
med. Institution				1a				
Hersteller							1b	
Anbieter **)								1b, 3
Herausgebende LEO **)		2,5	2,5	2,5	2			
Zertifikatsnehmende LEO					1a			
GKV-Spitzenverband **)					2	2		
KTR **)	1a, 2			~~2~~	1a	1a		
gematik		3	3	3	3	3	3	3
BNetzA		4						

2.7.3.3 Herausgeber der SMC-B

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

Zu unterscheiden sind dabei drei Ausprägungen der SMC-B:

- SMC-B einer Gesellschafterorganisation
  (Diese erlaubt keinen Zugriff auf eGKs)
- SMC-B einer medizinischen Institution bzw. Leistungserbringerinstitution
- SMC-B eines Kostenträgers
  Diese wird zu einem späteren Zeitpunkt eingeführt.

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

- KZBV: Zertifikatsnehmer sind die KZV-Betriebsstätten bzw. -Geschäftsstellen.

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

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

- KV-Telematik ARGE: Betriebstätte Arzt oder Psychotherapeut; mit Kassenzulassung und privat,
- für den jeweiligen Vertragszahnarzt /Vertragszahnarztpraxis zuständige KZV: Zahnarztpraxis mit Kassenzulassung,
- BZÄK: Zahnarztpraxis privat,

- Bundesapothekerkammer (BAK): Öffentliche Apotheke, Krankenhausapotheke, Bundeswehrapotheke,
- BPTK: Betriebstätte Psychotherapeut mit bzw. ohne Kassenzulassung,

Herausgeberorganisation der Kostenträger: Zertifikatsnehmer sind die Betriebsstätten bzw. Geschäftsstellen der Kostenträger (gesetzlich).

Änderungen in gemSpec_TK

7.2 Erstellung der X.509-Zertifikate für die SMC-B-Testkarten GE

…

⌦ Card-G2-A_2789 OID-Vorgaben für die SMC-B-Testkarten GE

In die X.509-Zertifikate der SMC-B-Testkarten der Generation 2 MÜSSEN gemäß den Festlegungen durch die ausgebenden Organisationen OIDs und Texte eingetragen werden. In Tab_TK_003 sind die Referenzbezeichnungen angegeben. Die zugehörigen OIDs/Texte befinden sich im Dokument [gemSpec_OID].

Tabelle 5: Tab_TK_003 OID-Referenzen für SMC-B-Testkarten GE (verpflichtend)

…	…
Admission: ProfessionItem und ProfessionOID in allen Zertifikaten (C.HCI.OSIG.R2048, C.HCI.AUT.R2048, C.HCI.ENC.R2048) für KZV-Betriebsstätten bzw. -Geschäftsstellen	oid_leo_zahnaerzte

7.5 Optische Gestaltung der SMC-B-Testkarten GE der Generation 2

…

⌦ Card-G2-A_2801 Quelle für Daten zum Karteninhaber und zum Profil für die SMC-B-Testkarten GE

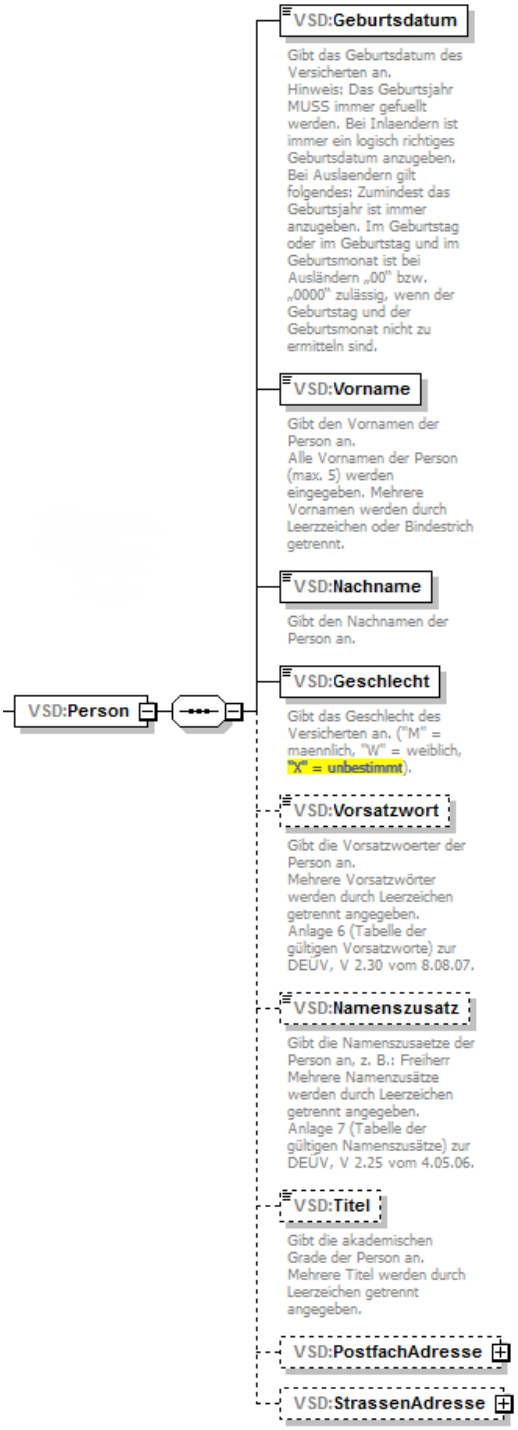
Die Daten zur Institution und zum zugehörigen Profil (Arztpraxis, Krankenhaus = Profil 2 A, Zahnarztpraxis = Profil 2 ZA, Apotheke = Profil 3, Psychotherapeutische Praxis = Profil 4, Kostenträger = Profil 8, SMC-ORG = Profil -) MÜSSEN aus den von der gematik gelieferten Datensätzen extrahiert und auf die Karten gedruckt werden.⌫

Änderungen an gemSysL_VSDM

C 1.2 – Persönliche Versichertendaten

…

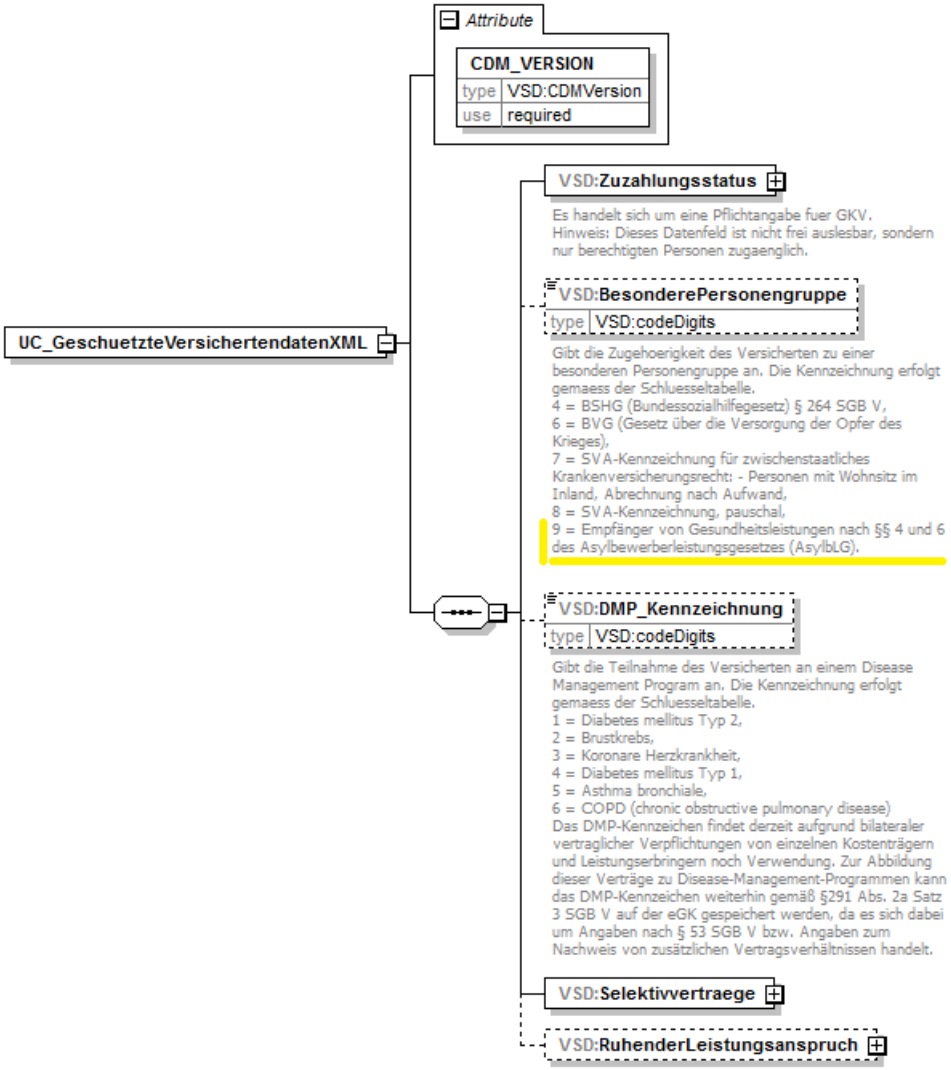
element UC_PersoenlicheVersichertendatenXML/Versicherter/Person



C 1.3 – Geschützte Versichertendaten

element UC_GeschuetzteVersichertendatenXML

…



In gemSpec_Krypt wird in Abschnitt „3.3.2 TLS-Verbindung“ folgende neue Anforderung eingefügt:

Für eine verbesserte Interoperabilität zu bestimmten TLS-Implementierungen (bspw. SChannel)[1] sollen im Konnektor zusätzlich zu den Ciphersuiten aus GS-A_4384 weitere Ciphersuiten unterstützt werden. Mit der mittelfristigen Anhebung des zu erreichenden Sicherheitsniveaus auf 120 Bit (vgl. [ALGCAT] und BSI-TR-03116-1]) werden die folgenden Ciphersuiten mittelfristig verpflichtend. In diesem Kontext spielt die Performanz (3000 Bit Diffie-Hellman vs. 256 Bit elliptic Curve Diffie-Hellman) bei embedded-Geräten wie dem Konnektor eine wichtige Rolle.

⌦ GS-A_5345 TLS-Verbindungen Konnektor

Der Konnektor MUSS für die TLS gesicherten Verbindungen neben den in [gemSpec_Krypt#GS-A_4384] aufgeführten Ciphersuiten folgende Vorgaben umsetzen:

(1) Der Konnektor SOLL zusätzlich folgende Ciphersuiten unterstützen:

- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC0, 0x13)`,
- `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC0, 0x14)`,
- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC0, 0x27)`,
- `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC0, 0x28)`,
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2f)` und
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x30)`.

(2) Der Konnektor KANN weitere Ciphersuiten aus [TR-02102-2, Abschnitt 3.3.1 Tabelle 1] unterstützen.

(3) Falls Ciphersuiten aus Spiegelstrich (1) oder (2) unterstützt werden,

- MÜSSEN bei dem ephemeren Elliptic-Curve-Diffie-Hellman-Schlüsselaustausch die Kurven P-256 oder P-384 [FIPS-186-4] unterstützt werden,
- MÜSSEN die Kurven brainpoolP256r1 und brainpoolP384r1 (vgl. [RFC-5639] und [RFC-7027]) unterstützt werden.

andere Kurven SOLLEN NICHT verwendet werden.

(4) Falls Ciphersuiten aus (1) oder (2) unterstützt werden, so MÜSSEN diese im CC-Zertifizierungsverfahren berücksichtigt werden.⌫

[1] https://en.wikipedia.org/wiki/Comparison_of_TLS_implementations
https://www.ssllabs.com/ssltest/clients.html