

Elektronische Gesundheitskarte und Telematikinfrastruktur

Feature: Personalisierung SM-B im HSM (HSM-B)

Version:	1. 0 <u>1</u> .0
Revision:	<u>9801931062422</u>
Stand:	<u>23.02</u> <u>09.08</u> .2024
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemF_Personalisierung_HSM-B

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0 CC	11.01.2024		zur Abstimmung freigegeben	gematik
1.0.0	23.02.2024		freigegeben	gematik
<u>1.1.0</u>	<u>09.08.2024</u>		<u>Einarbeitung CI_24.3</u>	<u>gematik</u>

Inhaltsverzeichnis

1 Einordnung des Dokuments.....	7
1.1 Zielsetzung.....	7
1.2 Zielgruppe.....	7
1.3 Abgrenzungen.....	7
1.4 Methodik.....	8
1.4.1 Epic und User Story.....	8
1.4.2 Anforderungen.....	8
2 Einordnung in die Telematikinfrastruktur.....	9
3 Konzept.....	10
3.1 Beteiligte Rollen & Komponenten.....	10
3.1.1 Für vorbereitende Schritte.....	10
3.1.2 Für die Herausgabe.....	11
3.1.2.1 Herausgebende Seite.....	11
3.1.2.2 Beantragende Seite.....	11
3.2 Vorbereitende Schritte.....	12
3.2.1 Personalisierung von HSK-Identitäten durch Hersteller HSK.....	12
3.2.2 Vertrauensbeziehungen herstellen.....	14
3.2.2.1 HSK-Eigenbetrieb.....	14
3.2.2.2 TI-Gateway.....	14
3.3 Herausgabe von Institutionsidentitäten.....	15
3.3.1 Antragstellung.....	17
3.3.1.1 Auswahl des Identitätsträgers.....	17
3.3.1.2 Auswahl des Anbieters.....	18
3.3.1.3 TI-Gateway: Verifikation des Antragstellerkontos beim TI-Gateway.....	18
3.3.1.4 Identifikation Antragsteller.....	19
3.3.1.5 Freigabe durch Herausgeber einholen.....	19
3.3.2 Zertifikatsbezug.....	19
3.3.2.1 Auslösung der Schlüsselerzeugung.....	20
3.3.2.1.1 im HSK-Eigenbetrieb.....	20
3.3.2.1.2 im TI-Gateway.....	20
3.3.2.2 CSR-Erzeugung im HSK.....	20
3.3.2.3 Zertifikatserstellung & Zertifikatsversand.....	20
3.3.2.4 Zertifikats-Import und HSM-B-Zuordnung.....	21
3.3.2.4.1 HSK-Eigenbetrieb.....	21
3.3.2.4.2 TI-Gateway.....	21
3.3.3 Inbetriebnahme.....	22
4 Anforderungshaushalt.....	23
4.1 Änderung in gemF_Highspeed-Konnektor.....	23
4.1.1 Anforderungen an den Anbieter SMC-B und dessen TSPs.....	23
4.1.1.1 Einbindung des TSP-CVC im Innenverhältnis von Anbieter SMC-B zu seinen TSPs.....	23

4.1.1.2 Herstellen von Vertrauensbeziehungen.....	24
4.1.1.2.1 Eigene Bekanntmachung über die TSL.....	24
4.1.1.2.2 Ermitteln von Anbietern TI-Gateway über die TSL.....	24
4.1.1.2.3 Ermitteln von Schlüsselverwaltern.....	25
4.1.1.3 Auswahl HSM-B und im Fall TI-Gateway Verifikation Nutzerregistrierung...25	
4.1.1.4 Zertifikatserstellung.....	28
4.1.1.4.1 Aufforderung zur Schlüsselerzeugung.....	28
4.1.1.4.2 Abholen des CSR-Pakets.....	29
4.1.1.4.3 Zertifikatsproduktion.....	29
4.1.2 Anforderungen an den Hersteller HSK.....	31
4.1.3 Anforderungen an den Anbieter HSK.....	31
4.1.4 Produkteigenschaften des HSK.....	32
4.2 Änderung in gemF_TI-Gateway.....	37
4.2.1 Anforderungshaushalt.....	37
4.2.1.1 Herstellen von Vertrauensbeziehungen.....	38
4.2.1.1.1 Eigene Bekanntmachung des Anbieters TI-Gateway.....	38
4.2.1.1.2 Ermitteln von Anbietern SMC-B über die TSL.....	39
4.2.1.2 Nutzerauthentifizierung.....	39
4.2.1.3 SMB-Service.....	41
4.2.1.3.1 Token-Endpoint.....	41
4.2.1.3.2 CSR erzeugen und senden.....	43
4.2.1.3.3 Zertifikate importieren.....	44
4.2.1.4 Verwalten von Institutionsidentitäten.....	45
4.3 Änderung in gemSpec_PKI.....	45
4.3.1.1 Kapitel 5.6.4.4 C.HSK.Sig – Authentisierung HSK.....	45
4.3.1.2 Kapitel 5.6.4.5 C.HSK.ENC – Verschlüsselung HSK.....	47
4.4 Änderung in gemSpec_OID.....	49
4.4.1 Kapitel 3.5.4 OID-Vorgabe für technische Rollen.....	49
4.5 Anpassung in gemSpec_TSL.....	52
4.6 Änderung in gemSpec_X_509_TSP.....	52
5 Dokumentenhaushalt.....	54
5.1 Neue Dokumente.....	54
5.2 Übersicht betroffener Dokumente.....	54
5.3 Übersicht Produkt- und Anbietertypen.....	54
6 Beispiele und Referenzimplementierungen.....	57
7 Anhang A – Verzeichnisse.....	58
7.1 Abkürzungen.....	58
7.2 Referenzierte Dokumente.....	58
7.2.1 Dokumente der gematik.....	58
7.2.2 Weitere Dokumente.....	59

1 Einordnung des Dokuments.....	9
1.1 Zielsetzung.....	9
1.2 Zielgruppe.....	9
1.3 Abgrenzungen.....	9
1.4 Methodik.....	10
1.4.1 Epic und User Story.....	10
1.4.2 Anforderungen.....	10
2 Einordnung in die Telematikinfrastruktur.....	11
3 Konzept.....	12
3.1 Beteiligte Rollen & Komponenten.....	12
3.1.1 Für vorbereitende Schritte.....	12
3.1.2 Für die Herausgabe.....	13
3.1.2.1 Herausgebende Seite.....	13
3.1.2.2 Beantragende Seite.....	13
3.2 Vorbereitende Schritte.....	14
3.2.1 Personalisierung von HSK-Identitäten durch Hersteller HSK.....	14
3.2.2 Vertrauensbeziehungen herstellen.....	16
3.2.2.1 HSK-Eigenbetrieb.....	16
3.2.2.2 TI-Gateway.....	16
3.3 Herausgabe von Institutionsidentitäten.....	17
3.3.1 Antragstellung.....	22
3.3.1.1 Auswahl des Identitätsträgers.....	22
3.3.1.2 Auswahl des Anbieters.....	23
3.3.1.3 TI-Gateway: Verifikation des Antragstellerkontos beim TI-Gateway.....	23
3.3.1.4 Identifikation Antragsteller.....	24
3.3.1.5 Freigabe durch Herausgeber einholen.....	24
3.3.2 Zertifikatsbezug.....	24
3.3.2.1 Auslösung der Schlüsselerzeugung.....	25
3.3.2.1.1 im HSK-Eigenbetrieb.....	25
3.3.2.1.2 im TI-Gateway.....	25
3.3.2.2 CSR-Erzeugung im HSK.....	25
3.3.2.3 Zertifikatserstellung & Zertifikatsversand.....	25
3.3.2.4 Zertifikats-Import und HSM-B-Zuordnung.....	26
3.3.2.4.1 HSK-Eigenbetrieb.....	26
3.3.2.4.2 TI-Gateway.....	26
3.3.3 Inbetriebnahme.....	27
4 Anforderungshaushalt.....	28
4.1 Änderung in gemF_Highspeed-Konnektor.....	28
4.1.1 Anforderungen an den Anbieter SMC-B und dessen TSPs.....	28
4.1.1.1 Einbindung des TSP-CVC im Innenverhältnis von Anbieter SMC-B zu seinen TSPs.....	28
4.1.1.2 Herstellen von Vertrauensbeziehungen.....	29
4.1.1.2.1 Eigene Bekanntmachung über die TSL.....	29
4.1.1.2.2 Ermitteln von Anbietern TI-Gateway über die TSL.....	29
4.1.1.2.3 Ermitteln von Schlüsselverwaltern.....	30

4.1.1.3 Auswahl HSM-B und im Fall TI-Gateway Verifikation Nutzerregistrierung...	30
4.1.1.4 Zertifikatserstellung.....	33
4.1.1.4.1 Aufforderung zur Schlüsselerzeugung.....	33
4.1.1.4.2 Abholen des CSR-Pakets.....	34
4.1.1.4.3 Zertifikatsproduktion.....	34
4.1.2 Anforderungen an den Hersteller HSK.....	36
4.1.3 Anforderungen an den Anbieter HSK.....	36
4.1.4 Produkteigenschaften des HSK.....	37
4.2 Änderung in gemF_TI-Gateway.....	42
4.2.1 Anforderungshaushalt.....	42
4.2.1.1 Herstellen von Vertrauensbeziehungen.....	43
4.2.1.1.1 Eigene Bekanntmachung des Anbieters TI-Gateway.....	43
4.2.1.1.2 Ermitteln von Anbietern SMC-B über die TSL.....	44
4.2.1.2 Nutzerauthentifizierung.....	45
4.2.1.3 SMB-Service.....	46
4.2.1.3.1 Token-Endpunkt.....	46
4.2.1.3.2 CSR erzeugen und senden.....	48
4.2.1.3.3 Zertifikate importieren.....	49
4.2.1.4 Verwalten von Institutionsidentitäten.....	50
4.3 Änderung in gemSpec_PKI.....	50
4.3.1.1 Kapitel 5.6.4.4 C.HSK.Sig – Authentisierung HSK.....	50
4.3.1.2 Kapitel 5.6.4.5 C.HSK.ENC– Verschlüsselung HSK.....	52
4.4 Änderung in gemSpec_OID.....	54
4.4.1 Kapitel 3.5.4 OID-Vorgabe für technische Rollen.....	54
4.5 Anpassung in gemSpec_TSL.....	57
4.6 Änderung in gemSpec_X_509_TSP.....	57
5 Dokumentenhaushalt.....	59
5.1 Neue Dokumente.....	59
5.2 Übersicht betroffener Dokumente.....	59
5.3 Übersicht Produkt- und Anbietertypen.....	59
6 Beispiele und Referenzimplementierungen.....	62
7 Anhang A – Verzeichnisse.....	63
7.1 Abkürzungen.....	63
7.2 Referenzierte Dokumente.....	63
7.2.1 Dokumente der gematik.....	63
7.2.2 Weitere Dokumente.....	64

1 Einordnung des Dokuments

Der HSK verfügt über ein HSM, welches die sichere Speicherung und Nutzung von privatem Schlüsselmaterial und eine performante Ausführung von kryptographischen Operationen ermöglicht. Da die Anwendungen VSDM, KIM und ePA die Institutionsidentität intensiv nutzen, soll ein Prozess definiert werden, wie eine Institutionsidentität sicher in einen HSK-HSM eingebracht werden kann. Neben den technischen Voraussetzungen am HSK sind auch die TSP und die Herausgeber von dieser Änderung betroffen.

Mit dem Feature wird es möglich, viele Institutionsidentitäten in einen HSK einzubringen und einer oder mehreren virtuellen Konnektor-Instanzen im HSK zuzuweisen, wo sie dann im Informationsmodell konfiguriert werden. Die Performancebeschränkungen von SMC-B wird damit entfernt. Der HSK kann HSM-B und SMC-B parallel nutzen (z.B. weil nicht für alle Institutionsidentitäten eine HSM-B Personalisierung etabliert ist). Der HSK kann aber weiterhin auch ausschließlich mit kartengebundenen Institutionsidentitäten (SMC-B) verwendet werden, ebenso wie ausschließlich mit HSM-Bs. Für den Betrieb des HSK ist lediglich die Verfügbarkeit einer Institutionsidentität erforderlich, unabhängig von deren Speicherort.

1.1 Zielsetzung

Spezifikation für die Personalisierung und Nutzung von Institutionsidentitäten im HSM eines Highspeed-Konnektors sowohl im Eigenbetrieb als auch im TI-Gateway.

1.2 Zielgruppe

Hersteller, Anbieter, Nutzer und andere Stakeholder.

1.3 Abgrenzungen

Das Dokument spezifiziert Anforderungen an die Produkte Highspeed-Konnektor, TI-Gateway und TSP-Komponenten, an die Anbieter TI-Gateway, Highspeed-Konnektor, SMC-B sowie an den TSP-X.509 nonQES Komponenten (kurz TSP-Komponenten), den TSP-X.509 nonQES SMC-B und den TSP-CVC. Der Identitäten-Herausgabeprozess wird für das Gesamtverständnis des Ablaufs mit beschrieben, jedoch nicht mit diesem Dokument geregelt (sondern weiterhin in [gemRL_TSL_SP_CP]). Basis- und KTR-Consumer sind von diesem Dokument nicht betroffen.

Das Dokument beinhaltet nur neue bzw. geänderte Anforderungen. Die vollständige Anforderungslage der Produkt- und Anbietertypen ergeben sich aus den Produkttypsteckbriefen, dem Anbietersteckbrief und den darin referenzierten Anforderungen.

1.4 Methodik

1.4.1 Epic und User Story

<Methodik von Epic und User Story erläutern>

Epics und zugeordnete User Stories werden durch eine eindeutige ID gekennzeichnet.

Epic und UserStory werden im Dokument wie folgt dargestellt:

<Jira-ID> - <Zusammenfassung des Jira-Issue>

Text / Beschreibung

[<=]

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

1.4.2 Anforderungen

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

Da in dem Beispielsatz „Eine leere Liste DARF NICHT ein Element besitzen.“ die Phrase „DARF NICHT“ semantisch irreführend wäre (wenn nicht ein, dann vielleicht zwei?), wird in diesem Dokument stattdessen „Eine leere Liste DARF KEIN Element besitzen.“ verwendet. Die Schlüsselworte werden außerdem um Pronomen in Großbuchstaben ergänzt, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.

Anforderungen werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>

Text / Beschreibung

[<=]

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

2 Einordnung in die Telematikinfrastruktur

Es wird der Herausgabe- und Personalisierungsprozess von Institutionsidentitäten (SM-B) spezifiziert, die auf einem HSM (Hardware Security Module) eines Highspeed-Konnektors (HSK) personalisiert werden. Diese SM-B-Identitäten stehen dann im HSK sowohl für TI-Gateway-Nutzer als auch für Nutzer, die einen eigenen HSK in Eigennutzung betreiben (Anbieter HSK), zur Verfügung. Für diese Nutzer ist dann nicht mehr zwingend eine SMC-B (Smartcard), die über ein eHealth-Kartenterminal (eH-KT) an den HSK angebunden ist, notwendig. Die Nutzung von SMC-Bs ist aber weiterhin möglich. Zudem wird weiterhin ein eH-KT benötigt, um HBAs und eGKs nutzen zu können.

Aus der übergreifenden Bezeichnung SM-B (Security Module Typ B) leitet sich die kartengebundene Variante der Identität mit der Bezeichnung SMC-B (Security Module Card Typ B) ab. Analog dazu wird die Ausprägung auf einem HSM im HSK im folgenden **HSM-B** genannt (Hardware Security Module Typ B). Somit können beide Ausprägungen im folgenden unterschieden werden, auch wenn die Identitäten, die sie repräsentieren, nicht unterscheidbar sind (Zertifikate gleichen Typs unterscheiden sich nicht, unabhängig davon, ob sie auf einem HSM-B oder einer SMC-B gespeichert sind).

3 Konzept

Für die Personalisierung des HSM-B im HSK eines TI-Gateway wird ein Vorgehen entworfen, für welches bis auf die Interaktion des Antragstellers bzw. TI-Gateway-Nutzers (Inhaber der Identität) keine manuellen Schritte notwendig sind. Dies ist sowohl auf Grund der erwarteten Menge an zu personalisierenden Identitäten als auch wegen des notwendigen Betreiberausschluss notwendig.

Für die Personalisierung des HSM-B im HSK-Eigenbetrieb sind manuelle Schritte vorgesehen, weshalb es hier die Rolle Schlüsselverwalter gibt, die diese Schritte durchführt, da in diesen Fällen aufwändige technische Umsetzungen für die erwartete geringere Menge an Identitäten nicht gerechtfertigt sind, und zudem die Umsetzung der Prozesse in direkter Verantwortung der identitätsinhabenden Organisation selbst erfolgt.

Der Unterschied in der HSM-B-Personalisierung zwischen TI-Gateway und HSK-Eigenbetrieb liegt hauptsächlich in der notwendigen Kommunikation zum Anbieter SMC-B, welche im Falle des TI-Gateway durch das Zugangsmodul umgesetzt und im Falle des Eigenbetriebs eines HSK durch die Rolle Schlüsselverwalter manuell durchgeführt wird.

Da die Verwaltung des HSM vom HSK-Basissystem vorgenommen wird, muss dort Funktionalität umgesetzt werden, die an der Personalisierung beteiligt ist und die einer virtuellen Konnektor-Instanz im HSK (im folgenden kurz **vInstanz**) das HSM-B zur Verfügung stellt, damit dieses dort vom Nutzer bzw. dem DVO konfiguriert und vom Nutzer verwendet werden kann.

3.1 Beteiligte Rollen & Komponenten

Im Folgenden werden die am Prozess beteiligten Rollen und Komponenten beschrieben. Da das Feature HSM-B sowohl für das TI-Gateway als auch für den HSK-Eigenbetrieb betrachtet wird, ist eine entsprechende Fall-Unterscheidung notwendig an den Stellen, bei denen sich Rollen für diese beiden Szenarien unterscheiden.

3.1.1 Für vorbereitende Schritte

- **gematik:** Zulassungsstelle für Anbieter TI-Gateway, Anbieter HSK, Anbieter SMC-B (inklusive Produkt TSP).
- **Hersteller HSK:** Entwickelt den HSK und bringt ihn zur Zulassung. Der Hersteller erzeugt / beantragt und personalisiert HSK-Identitäten auf das HSM des HSK. Ebenso koppelt der Hersteller das HSM mit dem HSK, sodass nur der HSK die Identitäten auf dem HSM nutzen kann.
- **TSP Komponenten:** Stellt Komponenten- und Dienst-Zertifikate aus (hier relevant HSK-Identitäten auf Antrag der HSK-Hersteller und TLS- und Signatur-Identitäten für Anbieter SMC-B und Anbieter TI-Gateway).
- **Anbieter SMC-B:** Etabliert Vertrauensbeziehungen zu zugelassenen Anbietern TI-Gateway bzw. zu den Schlüsselverwaltern von zugelassenen Anbietern HSK. Beantragt TLS-Zertifikat aus vom TSP Komponenten.
- **Anbieter TI-Gateway:** Etabliert Vertrauensbeziehungen zu zugelassenen Anbietern SMC-B. Beantragt TLS- und Signatur-Zertifikat vom TSP Komponenten.

- **Anbieter HSK:** Registriert seinen Schlüsselverwalter beim Anbieter SMC-B.

3.1.2 Für die Herausgabe

3.1.2.1 Herausgebende Seite

- **Herausgeber:** Verantwortliche Institution für die Herausgabe von Institutionsidentitäten, Bestätigung von berechtigten Antragstellern und Institutionen und Attributbestätigung für die Organisation des Antragstellers
- **Anbieter SMC-B:** Erstellung von SM-B Zertifikaten, Bereitstellung OCSP-Responder, Aktivierung der Zertifikate am OCSP-Responder, Bereitstellung der Prozesse und Portale für Antrag und Freigabe der SM-B-Identitäten, umfasst die Produkte TSP X.509 nonQES SMC-B und TSP-CVC, die die Zertifikate für SM-B-Identitäten ausstellen und technische Anforderungen im Zuge der Antragstellung und Personalisierung umsetzen.

3.1.2.2 Beantragende Seite

- **Identitätsträger** (Institutionsidentität): Der Identitätsträger (die Institution) nimmt über möglicherweise verschiedene Akteure an dem Prozess teil. Die Interaktionen zwischen den Akteuren einer Institution liegen in der Verantwortung der Institution:
 - **Antragsteller:** Die zur Beantragung der Institutionsidentität berechtigten Personen und zur Aktivierung der Institutionsidentität berechtigten Personen (bzw. berechtigt, den Aktivierungscode zu empfangen und an weitere berechtigte Personen weiterzugeben).
 - **vInstanz-Admin:** Administrator für die vInstanz(en) des Identitätsträgers, der in dessen Auftrag agiert (=> DVO)
Da die Aktivierung des HSM-B über die vInstanz-Managementoberfläche stattfindet, müssen vInstanz-Admin und Antragsteller zusammenarbeiten oder der vInstanz-Admin berechtigt sein, den Aktivierungscode übergeben zu bekommen.
 - **vInstanz-Nutzer:** Fachlicher Nutzer einer oder mehrerer vInstanzen als TI-Gateway-Kunde oder im HSK-Eigenbetrieb und somit berechtigter Nutzer des HSM-B. Da im Fall TI-Gateway im Rahmen der Antragstellung verifiziert wird, dass eine Beziehung zum gewählten TI-Gateway-Anbieter besteht, müssen der vInstanz-Nutzer als TI-Gateway-Kunde und der Antragsteller zusammenarbeiten (oder beide Rollen werden von der selben Person ausgefüllt).

Fall TI-Gateway

- **TI-Gateway**, bestehend aus technischen Komponenten und deren Betreiber:
 - **Highspeed-Konnektor (HSK):** Von der gematik zugelassene Komponente, bestehend aus einem Basissystem, virtuellen Konnektor-Instanzen (**vInstanzen**) und einem HSM. Das zum HSK gehörende HSM speichert die hier betrachteten SM-B-Identitäten. Das HSM-B ist somit ein Teil des HSK und keine eigenständige Komponente.
 - **TI-Gateway Zugangsmodul:** Von der gematik zugelassene Komponente, die im TI-Gateway u.a. ein Nutzer-Portal anbietet und administrative Zugriffe auf den HSK - insbesondere auch bezüglich HSM-B-Personalisierung - anstelle eines menschlichen Administrators umsetzt.
 - **Anbieter TI-Gateway:** Von der gematik zugelassener Anbieter, der HSK und Zugangsmodul betreibt.

Fall HSK-Eigenbetrieb

Der **Anbieter HSK** betreibt einen HSK für sich selbst bzw. für eine Unternehmensgruppe, der er angehört. **Antragsteller** ist er entweder selbst oder jemand anderes aus dieser Unternehmensgruppe. Für diese Spezifikation werden beim Anbieter HSK unterschieden:

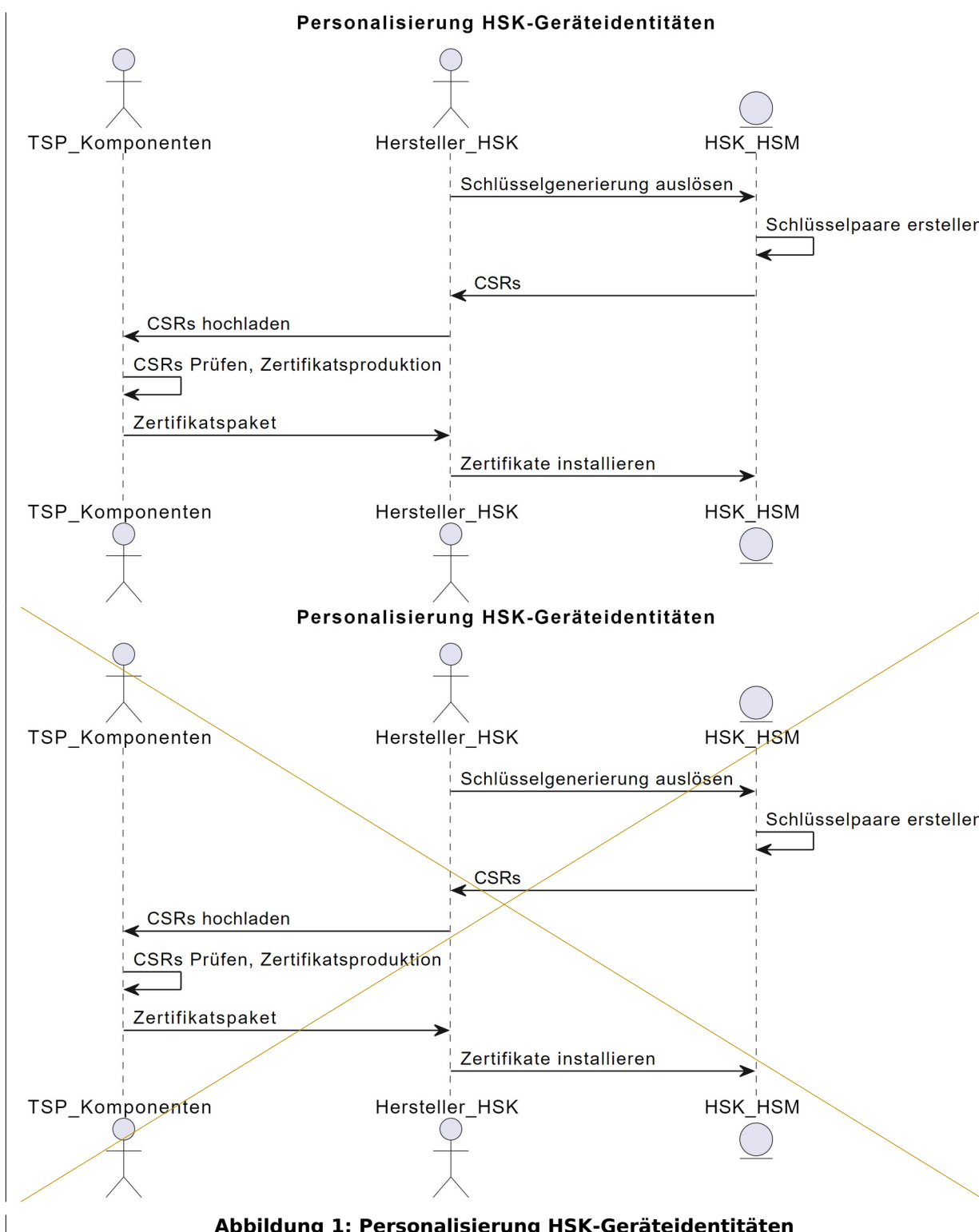
- **Schlüsselverwalter:** Dieser Akteur gehört zum Anbieter HSK und vermittelt zwischen den technischen Systemen des Anbieters SMC-B und dem HSK. Administrative Zugriffe auf den HSK zur HSM-B-Personalisierung (Erzeugung Schlüssel im HSM über HSK, Zertifikatsbezug vom Anbieter SMC-B, Zertifikatsimport in HSK) erfolgen durch die neue Rolle Schlüsselverwalter, die direkt durch Personal des Anbieters HSK ausgefüllt oder von diesem beauftragt wird.
- **HSK:** technische Komponente (siehe oben)

3.2 Vorbereitende Schritte

3.2.1 Personalisierung von HSK-Identitäten durch Hersteller HSK

Beteiligte Rollen: Hersteller HSK, TSP Komponenten

Dieser Schritt erfolgt vorbereitend und ist nicht für jede einzelne HSM-B-Personalisierung erneut notwendig.



Der Hersteller des HSK personalisiert im HSM des HSK die notwendigen Identitäten, die (neben AK.AUT und SAK.AUT, wie sie auch auf der gSMC-K vorhanden sind) die Identitäten HSK.SIG und HSK.ENC umfassen. Der Hersteller erzeugt die Schlüsselpaare auf dem HSM, beantragt beim TSP Komponenten die Zertifikate C.HSK.SIG und C.HSK.ENC und bringt diese in den HSK ein. Dies geschieht in der

Entwicklungs-/Fertigungsumgebung des Herstellers oder im Falle bereits im Feld betriebener HSKs durch einen Wartungseinsatz des Herstellers vor Ort beim Betreiber. Die Personalisierungsprozesse des Herstellers werden im Rahmen eines Sicherheitsgutachtens regelmäßig geprüft. Andere als der Hersteller und die Komponente HSK haben keinen Zugriff auf das HSM, wodurch die Identitäten HSK.SIG/ENC im Betrieb nur vom HSK selbst verwendet werden können. Antragsberechtigt für diese Identitäten beim TSP Komponenten sind ebenfalls nur Hersteller HSK (die Freigabe zum Bezug solcher Zertifikate wird von der gematik erteilt).

Die Identitäten werden zum einen zur Signatur/Signaturprüfung von CSR-Paketen (C.HSK.SIG) und zum anderen zur Ver-/Entschlüsselung von Zertifikatspaketen (C.HSK.ENC) genutzt. Die Zertifikate enthalten eine für den jeweiligen HSK eindeutige ID in Form einer Pseudo-ICCSN, welche sich nach der für diesen HSK personalisierten HSK-Identität richtet, also identisch ist zur Pseudo-ICCSN in C.AK.AUT und C.SAK.AUT. Die Pseudo-ICCSN ist in Struktur und Handhabung identisch zur ICCSN in den Zertifikaten der gSMC-K. Die Pseudo-ICCSN ist entsprechend bei einem Zertifikatspaar (Signatur & Verschlüsselung) für einen HSK identisch. Da die Zertifikate aus der Komponenten-PKI stammen, sind sie gegen die TSL prüfbar. Werden HSKs außer Betrieb genommen oder HSK-Zertifikate/Schlüssel als kompromittiert angenommen, meldet der Hersteller HSK die entsprechende HSK-ID an den TSP Komponenten in Form eines Sperrauftrags, sodass das C.HSK.SIG als "revoked" per OCSP verauskunftet wird.

3.2.2 Vertrauensbeziehungen herstellen

Dieser Schritt erfolgt vorbereitend und ist nicht für jede einzelne HSM-B-Personalisierung erneut notwendig.

3.2.2.1 HSK-Eigenbetrieb

Beteiligte Rollen: gematik, Anbieter SMC-B, Anbieter HSK, Schlüsselverwalter

Im Falle des HSK-Eigenbetriebs muss der Schlüsselverwalter registriert werden. Die Schlüsselverwalter von zugelassenen Anbietern HSK werden der gematik von diesem Anbieter HSK benannt. Die gematik gibt diese Information (Schlüsselverwalter als Person und zugehörige Organisation, also Anbieter HSK) weiter an die Anbieter SMC-B. Die potentiellen Schlüsselverwalter wenden sich an den Anbieter SMC-B und bekommen - sofern sie dem Anbieter SMC-B von der gematik genannt wurden - Zugang zum Trust-Management-System bzw. Antrags- und Freigabeportal des Anbieter SMC-B mit der Rolle Schlüsselverwalter. Damit kann der Schlüsselverwalter Aufträge zur Schlüsselgenerierung erhalten, CSR-Pakete hochladen und Zertifikatspakete herunterladen. Schlüsselverwalter wenden sich zur Registrierung an die Anbieter SMC-B. Anbieter SMC-B sind verpflichtet alle Schlüsselverwalter von zugelassenen Anbietern HSK zu registrieren, wenn diese sich beim Anbieter SMC-B melden und der Anbieter SMC-B die Kontaktdaten dieser Personen von der gematik gemeldet bekommen hat.

3.2.2.2 TI-Gateway

Beteiligte Rollen: gematik, Anbieter SMC-B, Anbieter TI-Gateway

Die Kommunikation erfolgt zwischen Anbieter SMC-B und den Zugangsmodulen bei den Anbietern TI-Gateway. Um die n-zu-m Beziehung zwischen den Anbietern SMC-B und den Anbietern TI-Gateway effizient herzustellen, wird die Vertrauensliste der TI (**TSL**) erweitert. Die Anbieter TI-Gateway werden als Trust Service Provider (TSP) mit einem TSP-Service (TSPService) vom Typ "unspecified" in die TSL aufgenommen. Der Eintrag der Anbieter SMC-B wird ebenso jeweils um einen Eintrag vom Typ "unspecified" erweitert. Die TSL kann von den Prozessbeteiligten automatisiert gelesen und ausgewertet werden. Über den Namen des Anbieters im Feld Name unterhalb TSPName

(TSPName/Name) aus dem TSL-Eintrag ist auch eine eindeutige Zuordnung von den dort hinterlegten Daten zu einem Anbieter möglich.

Die neu in die TSL aufzunehmenden Daten sind statisch und sollten sich pro Anbieter im Normalfall nur ca. alle 5 Jahre ändern, wenn Zertifikate ablaufen und neue hinterlegt werden. Über die im Rahmen der Zulassung aufgebaute Beziehung zu den Anbietern erhält die gematik deren Daten auf einem hinsichtlich Integrität geschützten Weg.

Die Einträge vom Typ "unspecified" für die Anbieter TI-Gateway und Anbieter SMC-B in der TSL werden genutzt:

- von den Anbietern SMC-B:
 - Extrahieren der zugelassenen Anbieter TI-Gateway um diese den Antragstellern zur Auswahl anzubieten,
 - Extrahieren die SMB-Service-URLs der Anbieter TI-Gateway für den Prozess zum Nachweis der TI-Gateway-Nutzer-Registrierung des Antragstellers und
 - Extrahieren des jeweiligen C.FD.TLS-S Zertifikats der Anbieter TI-Gateway.
- von den Anbietern TI-Gateway:
 - Extrahieren der redirect_uri jedes zugelassenen Anbieters SMC-B für den Prozess zum Nachweis der TI-Gateway-Nutzer-Registrierung des Antragstellers
 - Extrahieren des C.FD.TLS-C Zertifikats jedes zugelassenen Anbieters SMC-B für den Abgleich des beim TLS-Verbindungsaufbaus präsentierten Zertifikats

Weiterhin wird die TSL wie bei allen TI Komponenten für sämtliche Zertifikatsprüfungen verwendet. Durch Codierung der technischen Rollen Anbieter-TI-Gateway und Anbieter-SMB in deren TLS-Zertifikaten, wird die Kommunikation zwischen den Systemen dieser Anbieter abgesichert.

3.3 Herausgabe von Institutionsidentitäten

Im folgenden wird der Gesamtablauf der HSM-B-Personalisierung dargestellt, wobei für einige Teilprozesse zwischen dem Fall TI-Gateway und HSK-Eigenbetrieb unterschieden wird.

Einige Schritte, die so auch bereits bei der Beantragung und Herausgabe von SMC-Bs durchlaufen werden, sind teilweise nicht oder nicht vollständig beschrieben, da sie unverändert bleiben.

Vorbereitende, einmaligen Schritte, die vorab notwendig sind, werden hier nicht mehr betrachtet sondern wurden in den vorangegangenen Absätzen erläutert.

Für ein besseres Gesamtverständnis soll der grundlegende Ablauf einer Identitätsherausgabe in Kurzform skizziert werden, wobei bereits eine Identität auf einem HSK-HSM betrachtet wird:

- Antragsteller füllt Antrag im Antragsportal des zuständigen Anbieters SMC-B aus. Sollte dem Antrag ein Fachverfahren des Herausgebers vorausgehen, kann der Antrag vom Herausgeber bereits vorbefüllt sein.
- Anbieter SMC-B identifiziert Antragsteller und lässt die Berechtigung vom Herausgeber prüfen
- Anbieter SMC-B veranlasst über Anbieter HSK / TI-Gateway Schlüsselerzeugung im HSM des HSK
- HSK löst Schlüsselerzeugung am HSM an, erzeugt CSRs und lässt diese vom HSM signieren

- Anbieter HSK / TI-GW übergeben CSRs an Anbieter SMC-B
- Anbieter SMC-B führt Zertifikatserstellung durch
- Anbieter SMC-B veranlasst die Übertragung der Identität in den HSK
- Anbieter SMC-B lässt dem Antragsteller das Geheimnis zur Aktivierung der Identität (Aktivierungscode) zukommen
- Antragsteller aktiviert die Identität mit Hilfe des Geheimnisses
- Antragsteller führt Freischaltung der Identität beim Anbieter SMC-B durch, der diese am OCSP-Responder freischaltet

Im Folgenden wird jeweils der Gesamtprozess der Herausgabe für die beiden Fälle TI-Gateway und HSK-Eigennutzung dargestellt.

Fall TI-Gateway

Im Fall des TI-Gateways erfolgt eine technische Kommunikation zwischen den Systemen des Anbieters SMB und dem Zugangsmodul des TI-Gateway. Das Zugangsmodul steuert daraufhin den HSK. Damit der Zertifikatsbezug automatisch ablaufen kann, wird im Rahmen der Antragstellung geprüft, dass der Antragsteller auch Kunde beim TI-Gateway ist.

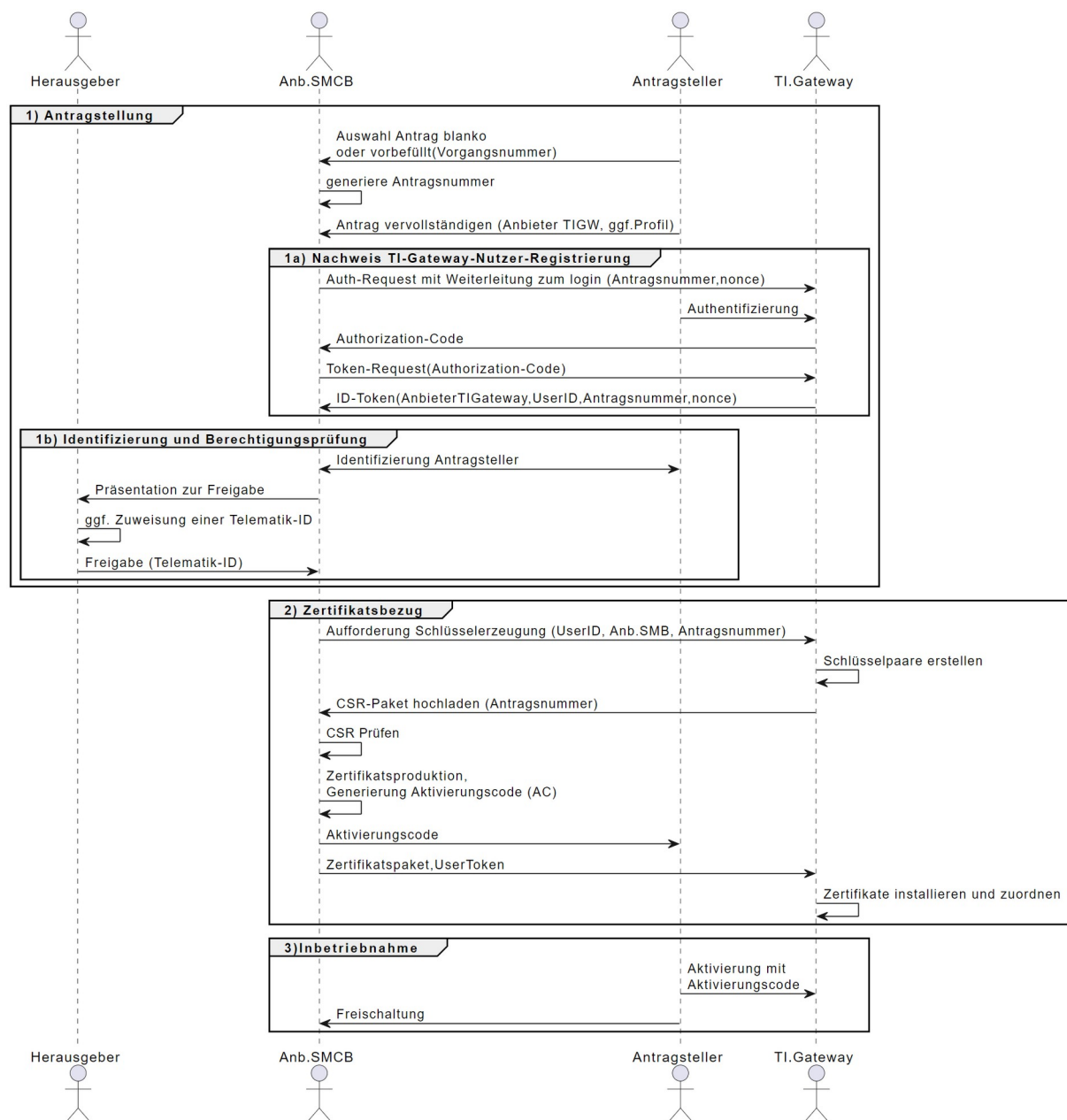
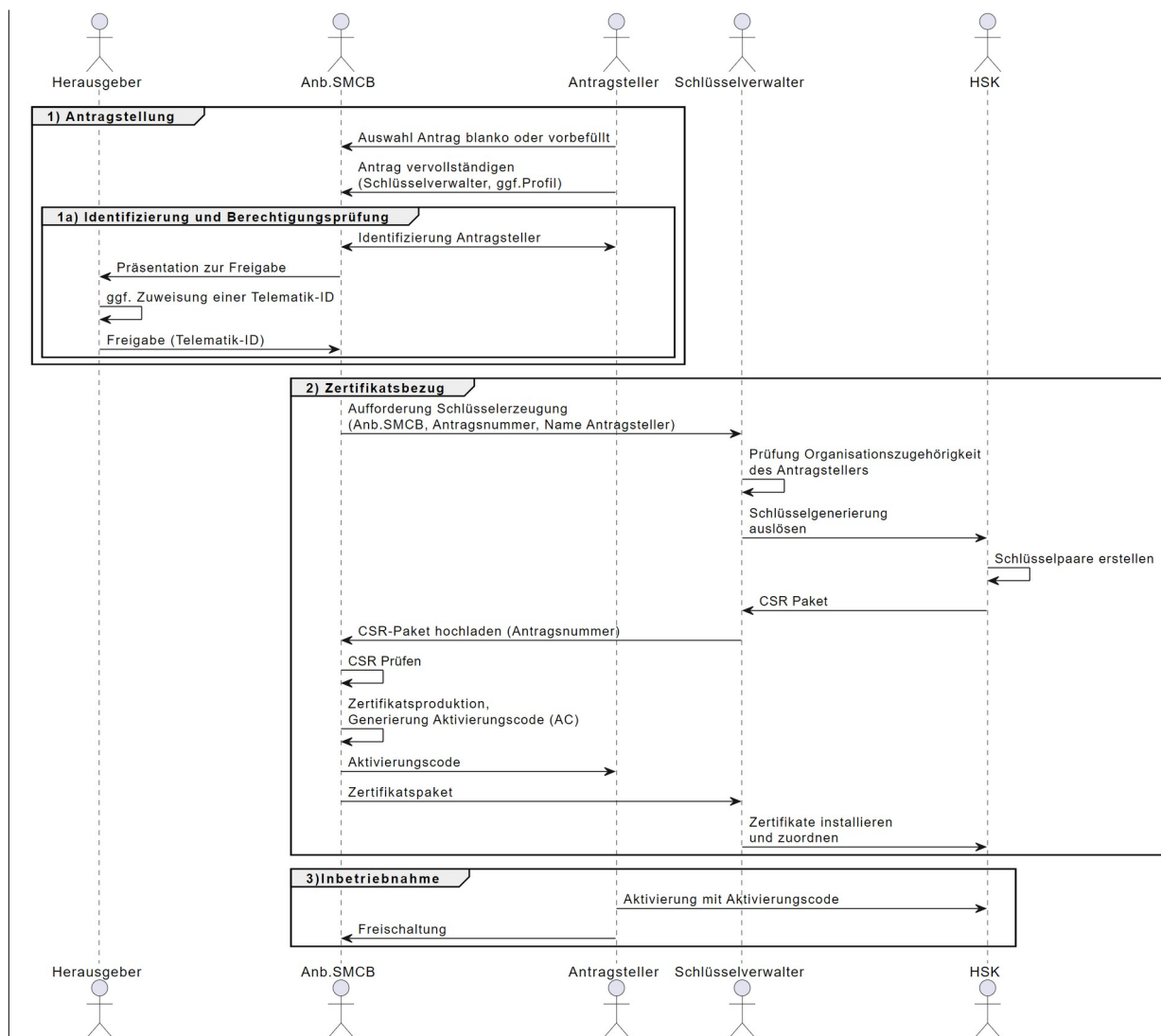


Abbildung 2: Übersicht HSM-B-Personalisierung TI-Gateway

Fall HSK-Eigenbetrieb

Im Fall des HSK-Eigenbetriebs vermittelt der Schlüsselverwalter zwischen den Systemen des Anbieters SMB und dem HSK.



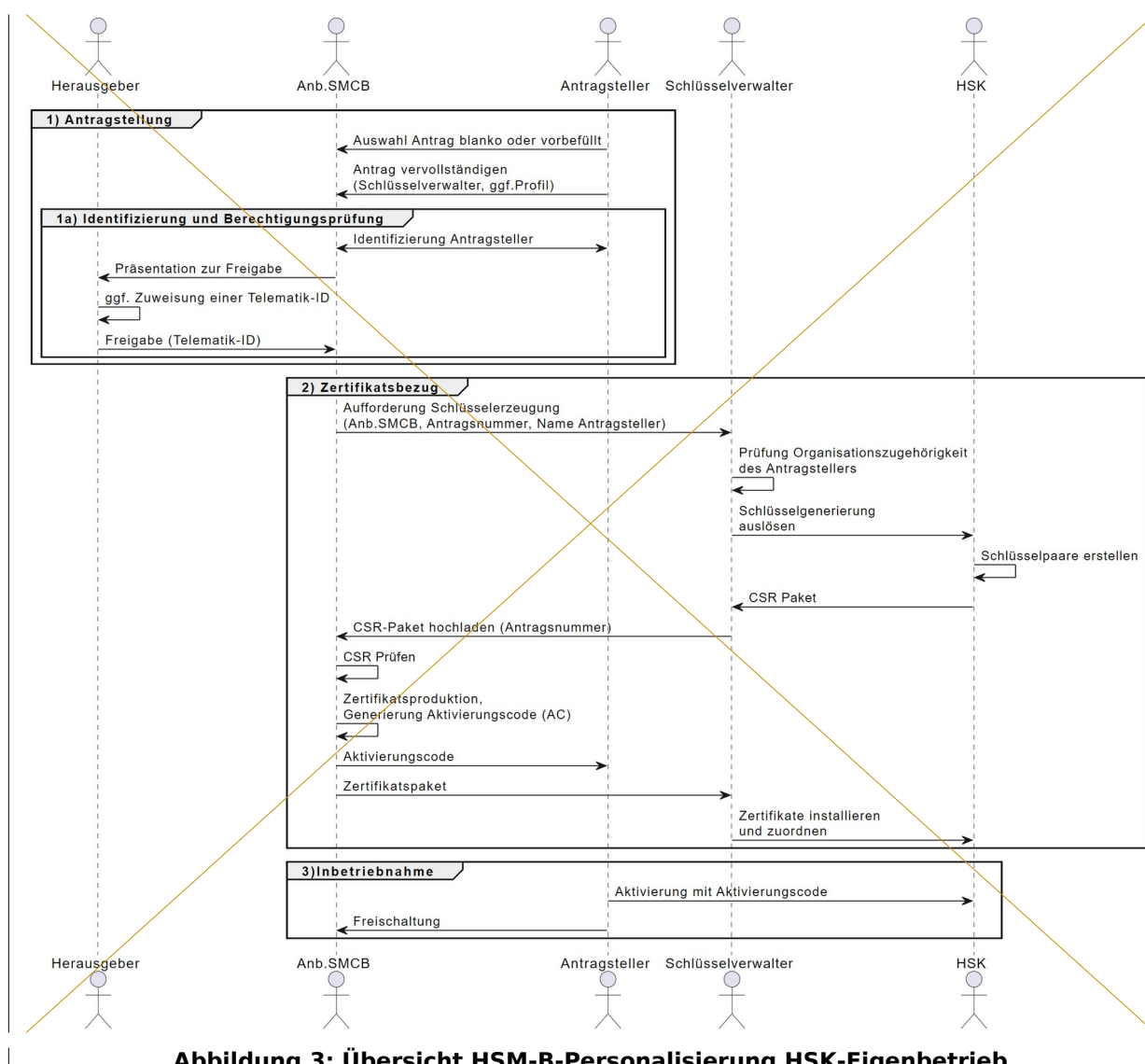


Abbildung 3: Übersicht HSM-B-Personalisierung HSK-Eigenbetrieb

Im Folgenden werden die einzelnen Teilschritte detailliert betrachtet, da dort zum Teil auch zusätzliche Rollen beteiligt sind.

3.3.1 Antragstellung

Die Antragstellung erfolgt für jede einzelne HSM-B-Personalisierung.

3.3.1.1 Auswahl des Identitätsträgers

Beteiligte Rollen: Anbieter SMC-B, Antragsteller

Der Antragsteller meldet sich im Portal seines Anbieters SMC-B an und wählt entweder einen leeren Antrag oder über eine Vorgangsnummer einen vorbefüllten Antrag aus. Es wird automatisch eine Antragsnummer vom Anbieter SMC-B für diesen Antrag erzeugt. Dies ist bereits heute für die SMC-B-Herausgabe der Fall.

Der Antragsteller wählt nun aus, dass er eine kartenungebundene SM-B-Identität beantragen möchte (HSM-B).

Im Folgenden wird nur der Bezug von HSM-Bs betrachtet.

3.3.1.2 Auswahl des Anbieters

Beteiligte Rollen: Anbieter SMC-B, Antragsteller

Der Anbieter SMC-B präsentiert dem Antragsteller die Liste der Anbieter HSK und Anbieter TI-Gateway, aus der der Antragsteller seinen Anbieter HSK (im Falle des HSK-Eigenbetrieb) bzw. Anbieter TI-Gateway (wenn das TI-Gateway genutzt wird) auswählt. Es werden alle zugelassenen Anbieter TI-Gateway und alle zugelassenen Anbieter HSK, deren Schlüsselverwalter bereits beim Anbieter SMC-B registriert wurden, gelistet. Der Anbieter SMC-B muss alle Schlüsselverwalter von zugelassenen Anbietern HSK registrieren, wenn diese sich dahingehend bei ihm melden (vgl. [13.2.2.13.2.2.1](#)).

Der Anbieter SMC-B unterstützt den Antragsteller, indem er den Antragsteller eine Vorauswahl bzgl. HSK Eigenbetrieb oder TI-Gateway treffen lässt und dann die Zugehörigkeit des Antragstellers zu einem bestimmten Sektor oder einer Unternehmensgruppe abfragt. Daraufhin werden die Anbieter HSK bzw. Anbieter TI-Gateway dann entsprechend vorselektiert.

Der Anbieter SMC-B ermittelt vorab die Anbieter HSK über die Schlüsselverwalter, die bei ihm registriert sind und die Anbieter TI-Gateway aus der TSL (siehe [23.2.23.2.2](#)).

Nach der vollständigen Befüllung des Antrags sendet der Antragsteller diesen ab. Wurde ein TI-Gateway gewählt, erfolgt direkt die Verifikation des Antragstellerkontos beim Anbieter TI-Gateway (siehe [33.3.1.33.3.1.3](#)).

3.3.1.3 TI-Gateway: Verifikation des Antragstellerkontos beim TI-Gateway

Beteiligte Rollen: Anbieter SMC-B, Antragsteller / vInstanz-Nutzer, Anbieter TI-Gateway, Zugangsmodul

Die Verifikation, dass der Antragsteller auch als Nutzer des während der Antragstellung ausgewählten TI-Gateways registriert ist, erfolgt mittels OAuth2/OIDC Authorization Code Flow. Es geschieht am Ende der Antragstellung, während sich der Antragsteller also noch am Browser im Antragsportal des Anbieters SMC-B befindet.

Der Anbieter SMC-B ermittelt aus der TSL mit der SMB-Service-URL den Konfigurationsinformation-Endpunkt und über letzteren die URL des Authentisierungs-Endpunkts, des Token-Endpunkts und das Signaturzertifikat C.FD.OSIG des gewählten Anbieters TI-Gateway. Der Anbieter SMC-B erzeugt einen Auth-Request, wofür die Antragsnummer, eine Zufallszahl und eine Redirect-URI notwendig ist. Er leitet den Antragsteller im Browser unter Übermittlung des Auth-Request zum Authentisierungs-Endpunkt des Anbieters TI-Gateway.

Der Antragsteller erhält eine Login-Seite im Nutzer-Portal seines TI-Gateway Anbieters auf der ihm angezeigt wird, dass zur Bestellung des HSM-B eine Authentisierung gegenüber dem Anbieter TI-Gateway notwendig ist. Dabei wird ihm auch der Namen des Anbieters SMC-B und die Antragsnummer angezeigt. Der Antragsteller authentifiziert sich beim Portal seines TI-Gateway Anbieters bzw. des Zugangsmoduls und weist somit nach, dass er vInstanz-Nutzer bei diesem TI-Gateway ist (eine explizite Authentisierung wird vom Zugangsmodul erzwungen). Das Zugangsmodul merkt sich die Zufallszahl aus dem Auth-Request des Anbieters SMC-B und lehnt spätere Aufrufe mit der selben Zufallszahl ab. Das Zugangsmodul erzeugt einen Authorization-Code, verknüpft diesen intern mit dem Auftrag und anhand der Redirect-URI aus dem Auth-Request leitet das Zugangsmodul den Antragsteller zurück zum Anbieter SMC-B unter Übermittlung des Authorization-Codes und der Antragsnummer aus dem Auth-Request.

Der Antragsteller befindet sich somit im Browser wieder im Antragsportal des Anbieters SMC-B. Letzterer fragt im Hintergrund über einen beidseitig authentisierten TLS-Kanal einen ID-Token beim Zugangsmodul des Anbieters TI-Gateway ab und gibt dabei den Authorization-Code an. Ist der Code gültig, erzeugt das Zugangsmodul einen ID-Token aus der GatewayUserID des authentifizierten vInstanz-Nutzers (Antragsteller), dem Zufallswert aus dem initialen Auth-Request des Anbieters SMC-B und der Antragsnummer und signiert das ID-Token mit seiner FD.OSIG Identität. Über den TLS-Kanal wird der ID-Token zum Anbieter SMC-B als Antwort übertragen. Das Zugangsmodul merkt sich im Erfolgsfall die Verbindung von GatewayUserID und Antragsnummer.

Der Anbieter SMC-B prüft die Signatur des ID-Token und prüft den Inhalt (Zufallswert, Antragsnummer). Der Antrag ist damit entweder automatisch abgesendet oder wird nochmal explizit vom Antragsteller abgesendet. Der Anbieter SMC-B speichert die Zuordnung von Antragsnummer zu GatewayUserID.

Für den Anbieter SMC-B und den Anbieter TI-Gateway (bzw. das Zugangsmodul) gibt es keinen direkten Nachweis, dass es sich beim Antragsteller (beim Anbieter SMC-B) und dem vInstanz-Nutzer (beim Anbieter TI-Gateway) um exakt dieselbe Person handelt. Aus dem Ablauf des Prozesses kann jedoch mit hinreichender Sicherheit darauf geschlossen werden, dass genau der Antragsteller sich als vInstanz-Nutzer am Zugangsmodul des TI-Gateways authentisieren konnte.

3.3.1.4 Identifikation Antragsteller

Beteiligte Rollen: Anbieter SMC-B, Antragsteller

Dieser Schritt erfolgt, genau wie zur Herausgabe der SMC-B, grundsätzlich für jeden Antrag.

Der Anbieter SMC-B muss den Antragsteller identifizieren, bevor Identitäten herausgegeben werden dürfen. Die Anforderungen dafür finden sich in [gemRL_TSL_SP_CP].

Der Schritt erfolgt nach der Antragstellung.

3.3.1.5 Freigabe durch Herausgeber einholen

Beteiligte Rollen: Anbieter SMC-B, Herausgeber

Dieser Schritt erfolgt, genau wie zur Herausgabe einer SMC-B, grundsätzlich für jeden Antrag gemäß Herausgeberrichtlinie und Freigabeprozess.

Der Anbieter SMC-B holt eine Freigabe für den Antragsteller beim Herausgeber ein, als Nachweis, dass der Antragsteller und die antragstellende Institution berechtigt sind, eine SM-B zu beantragen und zu nutzen.

Der Schritt erfolgt nach der Identifikation des Antragstellers.

3.3.2 Zertifikatsbezug

Dieser Schritt erfolgt für jede einzelne HSM-B-Personalisierung und erfolgt erst, wenn die Prozesse zur Identifikation ([43.3.1.4](#)) und Freigabe ([53.3.1.5](#)) erfolgreich durchlaufen wurden. Dies ist also zeitlich entkoppelt von der Antragstellung.

3.3.2.1 Auslösung der Schlüsselerzeugung

3.3.2.1.1 im HSK-Eigenbetrieb

Beteiligte Rollen: Anbieter SMC-B, Schlüsselverwalter, HSK

Der Schlüsselverwalter erhält vom Anbieter SMC-B unter Angabe der Antragsnummer, des Namens des Antragstellers und des Anbieternamens (TSPName/Name aus TSL-Eintrag) des Anbieter SMC-B die Aufforderung zur Schlüsselgenerierung. Vor der Schlüsselerzeugung verifiziert der Schlüsselverwalter, dass der Antragsteller tatsächlich Teil der Organisation ist, die den HSK im Eigenbetrieb nutzt. Über die Funktionalität des HSK-Basissystems erzeugt der Schlüsselverwalter ebenfalls unter Angabe der Antragsnummer alle notwendigen Schlüsselpaare und exportiert das signierte CSR-Paket (siehe [63.3.2.23.3.2.2](#)). Dieses Paket lädt der Schlüsselverwalter im Portal des Anbieter SMC-B hoch.

3.3.2.1.2 im TI-Gateway

Beteiligte Rollen: Anbieter SMC-B, Anbieter TI-Gateway, Zugangsmodul, HSK

Der Anbieter TI-Gateway erhält vom Anbieter SMC-B unter Angabe der Antragsnummer und GatewayUserID die Aufforderung zur Schlüsselgenerierung. Dies findet über eine technische Schnittstelle am Zugangsmodul und einen beidseitig authentisierten TLS-Kanal (mTLS) statt. Das jeweilige TLS-Zertifikat wird dabei gegen die TSL und über eine Rollenprüfung geprüft. Das Zugangsmodul prüft, dass ihm Antragsnummer und UserID als solche Kombination bekannt ist und löst in seiner Administratorrolle am HSK unter Angabe der Antragsnummer und des Anbieternamens (TSPName/Name aus TSL-Eintrag) des Anbieters SMC-B die Schlüsselgenerierung aus und erhält das signierte CSR-Paket (siehe [73.3.2.23.3.2.2](#)), welches es an den Anbieter SMC-B über den mTLS-Kanal sendet.

3.3.2.2 CSR-Erzeugung im HSK

Beteiligte Rollen: HSK, Schlüsselverwalter, Zugangsmodul, Anbieter SMC-B

Der HSK erzeugt alle für eine SM-B-Identität notwendigen Schlüsselpaare im HSM und verknüpft diese in seiner Datenbank mit der Antragsnummer und dem Anbieternamen (TSPName/Name aus TSL-Eintrag) des Anbieters SMC-B, um sie später den Zertifikaten zuordnen zu können. Zu jedem Schlüsselpaar wird ein CSR erstellt, in den jeweils die Antragsnummer eingebettet wird. Die einzelnen CSRs werden jeweils mit dem dazu gehörigen privaten Schlüssel im HSM signiert. Das CSR-Paket aus allen CSRs und dem HSK-Verschlüsselungszertifikat C.HSK.ENC wird vom HSK mit dem privaten Signaturschlüssel zu C.HSK.SIG signiert und das Signaturzertifikat C.HSK.SIG in die Signatur eingebettet (bzgl. HSK-Identitäten siehe [83.2.13.2.1](#)). Das signierte CSR-Paket enthält die Antragsnummer und den Anbieternamen (TSPName/Name aus TSL-Eintrag) des Anbieters SMC-B im Namen und wird an den Aufrufer (Schlüsselverwalter oder Zugangsmodul) zurückgegeben und von diesen zum Anbieter SMC-B übertragen.

3.3.2.3 Zertifikatserstellung & Zertifikatsversand

Beteiligte Rollen: Anbieter SMC-B (Schlüsselverwalter, Anbieter TI-Gateway, Zugangsmodul)

Dieser Schritt erfolgt für jede einzelne HSM-B-Personalisierung.

Der Anbieter SMC-B prüft, dass die Antragsnummer im CSR-Paket-Dateinamen und den einzelnen CSRs der erwarteten Antragsnummer entspricht und die Signatur des CSR-Paketes korrekt ist (mathematische Korrektheit Signatur und Zertifikatsprüfung C.HSK.SIG mit zeitlicher Gültigkeit, Prüfung gegen TSL und OCSP). Im Positivfall prüft er, ob das

enthaltene C.HSK.ENC dieselbe Pseudo-ICCSN im Feld commonName beinhaltet, wie das geprüfte C.HSK.SIG. Sind alle Prüfungen positiv verlaufen, erstellt der Anbieter SMC-B (nach den üblichen Prüfungen der CSRs) die Zertifikate (CV-Zertifikate einer SM-B-Identität beinhalten eine Pseudo-ICCSN, X.509-Zertifikate beinhalten die Telematik-ID als Identitätsmerkmal) und generiert einen Aktivierungscode. Ist je nach der sektorspezifischen Ausprägung im X.509-Zertifikat die Verwendung der ICCSN im Feld serialNumber vorgesehen, wird dort die selbe Pseudo-ICCSN verwendet wie im CV-Zertifikat. Alle Zertifikate einer Identität und den Aktivierungscode fasst er zu einem Zertifikatspaket zusammen und verschlüsselt dieses mittels des zuvor hinsichtlich Pseudo-ICCSN geprüften C.HSK.ENC. Das Zertifikatspaket enthält die Antragsnummer und den Anbieternamen (TSPName/Name aus TSL-Eintrag) des Anbieters SMC-B im Dateinamen.

Der Anbieter SMC-B liefert im Falle des HSK-Eigenbetriebs das verschlüsselte Zertifikatspaket an den Schlüsselverwalter aus (Bereitstellung im Portal des Anbieters SMC-B).

Im Falle des TI-Gateway liefert der Anbieter SMC-B das verschlüsselte Zertifikatspaket zusammen mit den Auftragsdaten (inkl. GatewayUserID) der Antragstellung (siehe [93.3.1.33.3.1.3](#)) an das Zugangsmodul des Anbieter TI-Gateway aus (über technische Schnittstelle mittels mTLS-Kanal).

3.3.2.4 Zertifikats-Import und HSM-B-Zuordnung

Dieser Schritt erfolgt für jede einzelne HSM-B-Personalisierung.

3.3.2.4.1 HSK-Eigenbetrieb

Beteiligte Rollen: Schlüsselverwalter, HSK

Der Schlüsselverwalter importiert das Zertifikatspaket in den HSK, wo es mit dem dort über das HSM verfügbaren privaten HSK.ENC-Schlüssel entschlüsselt wird. Anhand der Antragsnummer und des Anbieternamens (TSPName/Name aus TSL-Eintrag) werden die Zertifikate den entsprechenden privaten Schlüsseln im HSM zugeordnet und mathematisch geprüft, dass diese zusammengehören. Der HSK speichert den Aktivierungscode verschlüsselt ab und verknüpft ihn mit diesem HSM-B. Anschließend ordnet der Schlüsselverwalter das HSM-B auf Ebene des HSK-Basissystems manuell den vInstanzen zu, die dieses HSM-B nutzen sollen.

3.3.2.4.2 TI-Gateway

Beteiligte Rollen: Anbieter TI-Gateway, Zugangsmodul, HSK

Das Zugangsmodul importiert das Zertifikatspaket in den HSK. Dabei müssen zusätzlich die Identifikatoren für die vInstanzen des Nutzers übergeben werden. Dies sind für einen HSK eindeutige IDs, anhand derer das HSK-Basissystem eine vInstanz identifizieren kann. Somit kann später vom HSK-Basissystem genau diesen vInstanzen das HSM-B zugeordnet werden. Diese Identifikatoren sind herstellersistemspezifisch. Das Zertifikatspaket wird mit dem im HSK über das HSM verfügbaren privaten HSK.ENC-Schlüssel entschlüsselt. Anhand der Antragsnummer und des Anbieternamens (TSPName/Name aus TSL-Eintrag) werden die Zertifikate den entsprechenden privaten Schlüsseln im HSM zugeordnet und mathematisch geprüft, dass diese zusammengehören. Der HSK speichert den Aktivierungscode verschlüsselt ab und verknüpft ihn mit diesem HSM-B. Anhand der vom Zugangsmodul übergebenen Identifikatoren der vInstanzen, werden die erzeugten HSM-Bs allen vInstanzen dieses Nutzers zugeordnet.

Hinweis: Werden mehrere HSKs eingesetzt muss das Zugangsmodul die Information vorhalten, auf welchem HSK (bzw. dessen HSM) Schlüssel erzeugt wurden und das Zertifikatspaket auch genau dort wieder importieren, da nur dieser HSK das

Zertifikatspaket entschlüsseln kann. Werden die vInstanzen eines Nutzers nicht immer auf dem selben HSK betrieben, kann es sein, dass die vInstanz des Nutzers, für den das HSM-B personalisiert werden soll, dann bereits auf einem anderen HSK betrieben wird. Hier muss eine entsprechende sichere Synchronisation stattfinden, damit das HSM-B auf dem HSK verfügbar wird, auf dem auch die vInstanz des entsprechenden Nutzer läuft.

3.3.3 Inbetriebnahme

Beteiligte Rollen: HSK, Antragsteller, vInstanz-Admin, Anbieter TI-Gateway (, Zugangsmodul)

Der vInstanz-Nutzer (Antragsteller) bzw. sein vInstanz-Admin (DVO) konfiguriert die in der vInstanz verfügbaren HSM-Bs im Infomodell (als SM-B_Verwaltet). Bevor diese einem Mandanten zugeordnet werden können, muss der Aktivierungscode über die vInstanz-Management-GUI eingegeben werden. Der HSK (vInstanz oder Basissystem) prüft die Eingabe und aktiviert im Erfolgsfall das HSM-B (Zuordnung zum Mandanten im Infomodell wird umgesetzt).

Der Nutzer muss seine SM-B-Identität beim Anbieter SMC-B freischalten, damit die X.509-Zertifikate der Identität beim TSP im OCSP-Responder freigeschalten werden und somit zu den Zertifikaten auch ein Sperrstatus per OCSP abgefragt werden kann.

4 Anforderungshaushalt

Im Folgenden werden die neuen Anforderungen für die am HSM-B-Herausgabeprozess Beteiligten definiert, wobei das Kapitel nach Zieldokumenten für die Anforderungen in Unterkapitel unterteilt ist.

4.1 Änderung in gemF_Highspeed-Konnektor

Änderung in "5.2.1.2 HSM"

[...]

Die Nutzung eines HSMs für die Identitäten der LEI ist in der Feature-Spezifikation "Personalisierung SM-B mit HSM (HSM-B)" [gemF_Personalisierung_HSM] geregelt. {für zukünftige Versionen des Highspeed-Konnektors angedacht. Aktuell müssen hier weiterhin SMC-Bs verwendet werden.}

[...]

Das Folgende wird als Absatz 5.2.1.2.1 hinzugefügt.

Im Folgenden werden die neuen Anforderungen für die am HSM-B-Herausgabeprozess Beteiligten definiert.

4.1.1 Anforderungen an den Anbieter SMC-B und dessen TSPs

4.1.1.1 Einbindung des TSP-CVC im Innenverhältnis von Anbieter SMC-B zu seinen TSPs

Bei der Herausgabe einer kartengebundenen SM-B-Identität (SMC-B) gibt es für den Antragsteller ein Portal und die Einbindung der verschiedenen TSPs findet anschließend für den Nutzer transparent im Innenverhältnis des Anbieters SMC-B statt. Dies soll bezogen auf den Schlüsselverwalter bzw. das TI-Gateway Zugangsmodul auch im Folgenden für die technischen Umsetzungen im Zuge der Beantragung und Personalisierung eines HSM-B gelten, bei denen die TSPs beteiligt sind. In der vorliegenden Spezifikation werden technische Anforderungen an den TSP-X.509 nonQES SMC-B gerichtet. Für eine HSM-B-Identität, die CV-Zertifikate umfasst, ist entsprechend auch der TSP-CVC einzubinden. Dies geschieht im Innenverhältnis des Anbieters SMC-B und der TSPs, wird nicht ausspezifiziert und ist für den Schlüsselverwalter bzw. das TI-Gateway Zugangsmodul transparent.

A_25243 - HSM-B - Einbindung des TSP-CVC durch Anbieter SMC-B

Der Anbieter SMC-B MUSS durchsetzen, dass technische Umsetzungen, die entsprechend [gemF_Personalisierung_HSM] vom TSP-X.509 nonQES SMC-B verlangt werden, für HSM-B-Identitäten, die CV-Zertifikate umfassen auch vom TSP-CVC umgesetzt werden bzw. die notwendigen Daten intern, geschützt zum und vom TSP-CVC gelangen, ohne dass Schlüsselverwalter bzw. TI-Gateway Zugangsmodul den TSP-CVC individuell kommunizieren müssen.[<=]

Sicherheitsgutachten

4.1.1.2 Herstellen von Vertrauensbeziehungen

4.1.1.2.1 Eigene Bekanntmachung über die TSL

Damit Anbieter TI-Gateway eine Vertrauensbeziehung zu Anbietern SMC-B aufbauen können, müssen die dafür notwendigen Informationen der Anbieter SMC-B in der TSL hinterlegt werden. Konkret ist das TLS-Zertifikat eines Anbieters SMC-B innerhalb dessen bestehenden TSL-Eintrag mit einem Service-Eintrag vom Typ "unspecified" zu hinterlegen. Ein Anbieter TI-Gateway wertet diese Einträge täglich aus und hält alle aktuellen Zuordnung von "TSPName/Name" und TLS-Zertifikat für die notwendigen Prüfungen vor.

A_25253 - TLS-Zertifikat für Anbieter SMC-B

Der Anbieter SMC-B MUSS ein TLS-Zertifikat vom Profil C.FD.TLS-C mit der technischen Rolle oid_zert_smb beim TSP-X.509 nonQES der Komponenten-PKI beantragen. [≤]

Anbietererklärung

A_25092 - TSL Eintrag für TLS-Zertifikat Anbieter SMC-B

Der Anbieter SMC-B MUSS für seinen bestehenden Eintrag als "TrustServiceProvider" einen "TSPService"-Eintrag vom Typ "unspecified" für das TLS-Clientzertifikat C.FD.TLS-C in der TSL beantragen.

Tabelle 1: TSP-Service für Anbieter SMC-B

ServiceTypeldentifizier	http://uri.etsi.org/TrstSvc/Svctype/unspecified
ServiceSupplyPoint	<Redirect-URI für Authentifizierungsanfragen>
ServiceDigitalIdentity/DigitalId/X509Certificate	TLS-Clientzertifikat C.FD.TLS-C
ServiceInformationExtensions/Extension/ExtensionOID	entsprechend gemSpec_OID
ServiceInformationExtensions/Extension/ExtensionValue	oid_zert_smb

[≤]

Anbietererklärung

A_25255 - TSL Eintrag für TLS-Zertifikat Anbieter SMC-B löschen lassen bei Zertifikatsungültigkeit

Der Anbieter SMC-B MUSS den Eintrag in der TSL für sein TLS-Clientzertifikat C.FD.TLS-C umgehend löschen lassen, wenn dieses auf Grund einer vermuteten oder bestätigten Kompromittierung nicht mehr gültig ist. [≤]

Sicherheitsgutachten

4.1.1.2.2 Ermitteln von Anbietern TI-Gateway über die TSL

A_25090 - Anbieterliste TI-GW aus TSL erstellen

Der TSP-X.509 nonQES SMC-B MUSS täglich die TSL beziehen, diese prüfen und den Service-Einträgen vom Typ "unspecified" und mit dem ServiceInformationExtensions/Extension/ExtensionValue "oid_tigw_zugm" den vollständigen Service-Namen (TSPName/Name), die SMB-Service-URL für den

Konfigurationsinformations-Endpunkt (bzw. den OIDC-Issuer) und das Zertifikat C.FD.TSL-S extrahieren und für spätere Prüfungen vorhalten. [≤]

~~fkt.~~ Eig. Test

Hinweis: Neben den Service-Einträgen der Anbieter TI-Gateway und SMC-B sind in Service-Einträgen des Typs "unspecified" aktuell auch die Zertifikate der Schlüsselgenerierungsdienste (SGD) für die ePA aufgeführt.

A_25116 - OIDC-Konfiguration laden

Der TSP-X.509 nonQES SMC-B MUSS die OpenID Provider Configuration vom Konfigurationsinformations-Endpunkt des Anbieters TI-Gateway (A_25115*) laden und daraus den Authentisierungs-Endpunkt, den Token-Endpunkt und das Signaturzertifikat C.FD.OSIG extrahieren. [OpenID Connect Discovery] [≤]

~~fkt.~~ Eig. Test

4.1.1.2.3 Ermitteln von Schlüssilverwaltern

A_25091 - Onboarding von Schlüssilverwaltern

Der Anbieter SMC-B MUSS es allen von der gematik gemeldeten Schlüssilverwaltern der zugelassenen Anbieter HSK ermöglichen, eine Vertrauensbeziehung für den hinsichtlich Integrität geschützten Austausch von Schlüsselgenerierungsaufforderungen, CSR-Paketen und Zertifikatspaketen herzustellen und dabei prüfen, dass die Kontaktdaten der Schlüssilverwalter mit den von der gematik gemeldeten Daten übereinstimmen. [≤]

~~Sicherheitsgutachten~~

4.1.1.3 Auswahl HSM-B und im Fall TI-Gateway Verifikation Nutzerregistrierung

Anforderungen an das technische System:

A_25093 - Auswahl des Anbieters HSK/TI-Gateway

Der TSP-X.509 nonQES SMC-B MUSS dem Antragsteller - nachdem dieser HSM-B ausgewählt hat - die Anbieter HSK und Anbieter TI-Gateway zur Auswahl anbieten. Der Anbieter SMC-B KANN durch zusätzliche ihm bekannte oder vom Antragsteller eingeholte Informationen die angezeigten Anbieter auf die für den Antragsteller relevanten Anbieter reduzieren. [≤]

~~fkt.~~ Eig. Test

A_25095 - Prüfung Nutzerkonto TI-Gateway

Der TSP-X.509 nonQES SMC-B MUSS, wenn der Antragsteller einen Anbieter TI-Gateway ausgewählt hat, technisch prüfen, dass der Antragsteller beim ausgewählten Anbieter als Nutzer registriert ist. Dies muss nach Auswahl des TI-Gateways im Antragsprozess und über eine Funktion "TI-Gateway Registrierung überprüfen" auslösbar sein. [≤]

~~fkt.~~ Eig. Test und Sicherheitsgutachten

~~48960~~ **A_25086-01 - Redirect zur Authentifizierung am TI-Gateway**

Der TSP-X.509 nonQES SMC-B MUSS zur Prüfung nach A_25095 einen Auth-Request nach RFC 6749 mittels Redirect zum Authentisierungs-Endpunkt des gewählten Anbieters TI-Gateway senden. Der Auth-Request muss folgendermaßen parametrisiert werden: ⚡

Location: <URL Authentisierungs-Endpunkt entsprechend A_25116*>?
 response_type=code-~~id_token~~
 &scope=openid

```
&client_id=<TSPName/Name aus TSL-Eintrag des Anbieters SMC-B>
&state=<Antragsnummer>
&nonce=<individuelle 10 Minuten gültige Zufallszahl>
&redirect_uri=<Endpunkt zur Verarbeitung von Auth-Codes>
```

Der Anbieter SMC-B muss für die späteren Auswertungen die Kombination von Anbieter TI-Gateway, Antragsnummer und nonce persistieren, wobei der Anbieter SMC-B durchsetzen MUSS, dass jede nonce nur einmalig verwendet und nach 10 Minuten gelöscht wird.【<=】

flkt. Eig. Test und Sicherheitsgutachten

Kann sich der Antragsteller am TI-Gateway erfolgreich authentisieren wird er im Browser unter Rückgabe eines Auth-Codes und der Antragsnummer an die redirect_uri des Anbieters SMC-B zurückgeleitet.

A_25096 - Verarbeitung Auth-Code

Der TSP-X.509 nonQES SMC-B MUSS unter der redirect_uri eine Operation zum Empfang und zur Verarbeitung von Auth-Codes bereitstellen:

Eingangsparameter	state=Antragsnummer code=Auth-Code
Verarbeitung	<ol style="list-style-type: none"> 1. Prüfe ob Antragsnummer bekannt 2. Baue eine beidseitig authentifizierte TLS-Verbindung zum Token-Endpunkt des mit der Antragsnummer verknüpften Anbieters TI-Gateway auf mit dem eigenen C.FD.TLS-C Zertifikat als Clientzertifikat und unter Prüfung des TLS-Serverzertifikats, dass dies: <ol style="list-style-type: none"> a. entsprechend A_25090* in der TSL enthalten ist, b. das Zertifikatsprofil C.FD.TLS-S aufweist, c. zeitlich gültig ist und d. die Rolle oid_tigw_zugm besitzt. 3. sende einen Token-Requests nach RFC 6749 an den Token-Endpunkt des Anbieters TI-Gateway (getToken, vgl. A_25102*) mit grant_type=authorization_code code=<Auth-Code> redirect_uri=<URL identisch wie in A_25086*> client_id=<TSPName/Name aus TSL-Eintrag des Anbieters SMC-B> 4. extrahiere und prüfe den ID-Token aus der von getToken erhaltenen Response entsprechend A_25097*
Fehlerfälle	In allen Fehlerfällen müssen dem Nutzer im Browser eindeutige Fehlermeldungen angezeigt werden, die Informationen über die Fehlerursache und Handlungsanweisungen enthalten, wie der Nutzer die jeweilige Fehlersituation auflösen kann.

【<=】

fkt. Eig. Test

Hinweis: RFC 6749#4.1.3 verlangt, dass `redirect_uri` im Token-Request enthalten sein muss, sofern er auch im Auth-Request enthalten war und dass die Werte jeweils identisch sind. Für den konkreten Ablauf entsprechend dieser Spezifikation ist der Parameter `redirect_uri` im Token-Request irrelevant, da die Antwort des Anbieters TI-Gateway innerhalb des mTLS Kanals stattfindet, also der Parameter `redirect_uri` am Token-Endpunkt des TI-Gateways ignoriert wird.

Hinweis: RFC 8705#2 fordert die Angabe der Client-ID in allen Requests, die über einen mTLS-Kanal gesendet werden. Dadurch kann der Client zugeordnet werden und geprüft werden, dass das präsentierte TLS-Clientzertifikat dem für diesen Client erwarteten Zertifikat entspricht. Letztere Prüfung wird zudem auch in A_25109* gefordert.

A_25097 - Auswertung ID-Token

Der TSP-X.509 nonQES SMC-B MUSS für empfangene ID-Token (`id_token`)

- anhand des im Token im Feld `iss` angegebenen Anbieters TI-Gateway das von diesem geladene C.FD.OSIG Zertifikat ermitteln (vgl. A_25116*),
- die Signatur gegen das ermittelte C.FD.OSIG prüfen,
- die nonce auf Gültigkeit prüfen,
- anhand der nonce den ID-Token der ursprünglichen Authentisierungsanfrage (A_25086*) zuordnen,
- aus dem Feld `sub` die Antragsnummer extrahieren (vgl. A_25108*) und prüfen, ob sie gleich der Antragsnummer in der Anfrage ist und
- anhand des Zeitstempels im Feld `iat` prüfen, dass der Token nicht älter als 5 Minuten ist.

Bei erfolgreichen Prüfungen :

- aus dem Feld `sub` die GatewayUserID extrahieren (vgl. A_25108*) und mit der Antragsnummer persistieren.

Fehlerfälle dem Anwender mitteilen (s. A_25096)[<=]

fkt. Eig. Test und Sicherheitsgutachten

Sämtliche durch die Richtlinie gemRL_TSL_SP_CP vorgegebenen Aktivitäten des Anbieters SMC-B zur Identifizierung und Berechtigungsprüfung des Antragstellers und zum Versand des Aktivierungscodes (analog zur PIN bei der SMC-B) bleiben von diesem Dokument unberührt. Der Versand des Aktivierungscodes muss den Anforderungen des PIN-Versands in der Richtlinie gemRL_TSL_SP_CP genügen. Der Vollständigkeit halber wird dies durch die folgenden Anforderungen noch einmal normativ reguliert.

A_25098 - HSM-B - Einhaltung der sicheren Herausgabeprozesse entsprechend gemRL_TSL_SP_CP

Der Anbieter SMC-B MUSS durchsetzen, dass auch im Fall der Herausgabe einer Identität als HSM-B die Vorgaben zur sicheren Herausgabe entsprechend der gematik Certificate Policy gemRL_TSL_SP_CP (insbesondere Absatz 4.2.7) umgesetzt werden. Dies umfasst u.a. die Identifizierung des Antragstellers und den Versand des Aktivierungscodes, der wie eine PIN zu behandeln ist. Es muss für den Fall, dass Identifizierung und Versand/Übergabe kombiniert werden, berücksichtigt werden, dass ein HSM-B nur einen Versand (Aktivierungscode) umfasst, da keine Karte versendet wird.[<=]

Sicherheitsgutachten**A_25099 - Bestätigung durch Herausgeber**

Der Anbieter SMC-B MUSS die Berechtigung des Antragstellers bzw. der Institution, für die die Identität ausgestellt werden soll, entsprechend der Herausgeberrichtlinie

gemRL_TSL_SP_CP und den geltenden Freigabeprozessen vom Herausgeber einholen.
[<=]

Sicherheitsgutachten

4.1.1.4 Zertifikatserstellung

Für den Fall der Herausgabe für ein TI-Gateway wird der Ablauf zur Zertifikatserstellung zwischen Anbieter SMC-B und Anbieter TI-Gateway über eine technische Schnittstelle des TI-Gateway Zugangsmodul abgebildet, welche der Anbieter SMC-B als Client verwendet.

A_25121 - Nutzung SMB-Service des TI-Gateway Zugangsmoduls

Der TSP-X.509 nonQES SMC-B MUSS für die Prozesse der Zertifikatserstellung die Operationen requestCSR, getCSR und loadCerts des SMB-Service des TI-Gateway Zugangsmoduls verwenden und dabei stets:

- einen beidseitig authentisierten TLS-Kanal aufbauen,
- dabei sein TLS-Clientzertifikat C.FD.TLS-C verwenden,
- das TLS-Serverzertifikat des TI-Gateway Zugangsmoduls prüfen, dass dies:
 - entsprechend A_25090* in der TSL enthalten ist,
 - das Zertifikatsprofil C.FD.TLS-S aufweist,
 - zeitlich gültig ist und
 - die Rolle oid_tigw_zugm besitzt.
- die folgenden Informationen aus dem ID-Token als "Auftragsdaten" im json Format verwenden:


```
{
  "client_id": "<TSPName/Name aus TSL-Eintrag des Anbieters SMC-B>",
  "state": "<Antragsnummer>",
  "user": "<GatewayUserID>"
}
```

[<=]

fkt. Eig. Test

4.1.1.4.1 Aufforderung zur Schlüsselerzeugung

A_25100 - Aufforderung zur Schlüsselerzeugung Anbieter HSK

Der TSP-X.509 nonQES SMC-B MUSS für HSM-B-Anträge, bei denen ein Anbieter HSK vom Antragsteller ausgewählt wurde, den Schlüsselverwalter der ausgewählten Unternehmensgruppe zur Schlüsselgenerierung auffordern und dabei den Namen des Antragstellers mit übergeben. [<=]

fkt. Eig Test

A_25101 - Aufforderung zur Schlüsselerzeugung Anbieter TI-Gateway

Der TSP-X.509 nonQES SMC-B MUSS für HSM-B-Anträge, bei denen ein Anbieter TI-Gateway vom Antragsteller ausgewählt wurde, dem ausgewählten TI-Gateway Anbieter einen Request zur Schlüsselerzeugung senden, dafür die Operation requestCSR des SMB-Service des Zugangsmoduls des TI-Gateways verwenden und dabei die Auftragsdaten entsprechend A_25121* verwenden.[<=]

fkt. Eig. Test

4.1.1.4.2 Abholen des CSR-Pakets

A_25124 - Abholen CSR-Paket beim Anbieter HSK

Der TSP-X.509 nonQES SMC-B MUSS für HSM-B-Anträge, bei denen ein Anbieter HSK vom Antragsteller ausgewählt wurde, den Schlüsselverwalter der ausgewählten Unternehmensgruppe zum Upload des CSR-Pakets auffordern. [\leq]

fkt. Eig Test

A_25123 - Abholen CSR-Paket beim Anbieter TI-Gateway

Der TSP-X.509 nonQES SMC-B MUSS für HSM-B-Anträge, bei denen ein Anbieter TI-Gateway vom Antragsteller ausgewählt wurde, dem ausgewählten TI-Gateway Anbieter einen Request zur Abholung des CSR-Pakets senden, dafür die Operation getCSR des SMB-Service des Zugangsmoduls des TI-Gateways verwenden und dabei die Auftragsdaten entsprechend A_25121* verwenden.

Der Anbieter SMC-B MUSS aus dem Body der Antwort der Operation getCSR (vgl. A_25112*) das BASE64-kodierte CSR-Paket (CSR-Paket-zip) und dessen Signatur (CSR-Paket-sig) extrahieren. [\leq]

fkt. Eig. Test

4.1.1.4.3 Zertifikatsproduktion

A_23731 - HSM-B Aktivierungscode

Der TSP-X.509 nonQES SMC-B MUSS bei der Zertifikatsproduktion für ein HSM-B einen individuellen, zufälligen Aktivierungscode analog zur Transport-PIN als 6-stellige Zahl generieren.

Der Anbieter SMC-B MUSS den Aktivierungscode in einer Datei mit dem Namen <Antragsnummer>_Aktivierungscode.txt dem Zertifikatspaket hinzufügen, welches entsprechend A_23758* für den HSK verschlüsselt wird.

Der Anbieter SMC-B MUSS genau nur dem Antragsteller den Aktivierungscode im Klartext zugänglich machen und diesen dabei so behandeln wie die PIN im Falle einer SMC-B, also einer kartengebundenen Identität (vgl. gemRL_TSL_SP_CP#4.2.7). [\leq]

fkt. Eig. Test und Sicherheitsgutachten

A_23759 - HSM-B-Identitäten - Prüfgrundlage für CSRs

Der Anbieter SMC-B MUSS für die Zertifikatsproduktion für ein HSM-B als Prüfgrundlage eine tagesaktuelle, geprüfte TSL aus der TI verwenden. [\leq]

Sicherheitsgutachten

A_23758 - HSM-B-Identitäten - Signaturprüfung CSR-Paket und Verschlüsselung Zertifikatspaket

Der TSP-X.509 nonQES SMC-B MUSS bei der Zertifikatsproduktion für ein HSM-B folgendes umsetzen:

- Zertifikate werden nur erstellen, wenn erfolgreich geprüft wurde, dass:
 - die Auftragsnummer im Dateinamen des CSR-Pakets und dessen Signatur mit der im getCSR-Request übergebenen Auftragsnummer übereinstimmt,
 - die Signatur des empfangenen CSR-Pakets korrekt ist, konkret:
 - mathematische Korrektheit der Signatur,
 - Signaturzertifikat, dass dies:
 - gegen die TSL verifiziert werden kann, also das Aussteller-CA-Zertifikat in der TSL enthalten ist und die Signatur des Zertifikats dagegen erfolgreich geprüft werden kann,

- das Zertifikatsprofil C.HSK.SIG aufweist,
- zeitlich gültig ist,
- per OCSP als "good" ausgewiesen wird und
- die Rolle oid_hsk besitzt.
- die Auftragsnummer im Dateinamen der individuellen CSRs der aus dem Dateinamen des CSR-Pakets entspricht,
- das im Request enthaltene C.HSK.ENC-Zertifikat die gleiche Pseudo-ICCSN beinhaltet, wie das zuvor geprüfte C.HSK.SIG-Zertifikat,
- die Signatur der individuellen CSRs mit dem darin enthaltenen öffentlichen Schlüssel prüfbar ist.
- Als Zertifikatspaket wird ein zip-Archiv mit den Zertifikaten im PEM-Format und der Namenskonvention [Antragsnummer]_SMB_[AUT|ENC|OSIG|CVC|CVC_CA|CVC_ROOT]_[RSA|ECC].crt sowie dem Aktivierungscode als <Antragsnummer>_Aktivierungscode.txt gebildet. CVC_CA ist das CV-CA-Zertifikat der zweiten Ebene passend zum mit CVC benannten End-Entity-Zertifikat und CVC_ROOT der öffentliche Schlüssel der passenden CVC-Root-CA. CV-Zertifikate werden nur erzeugt und deren CA- und Root-CA-Zertifikat hinzugefügt, sofern diese für die Identität benötigt werden. CSRs für CV-Zertifikate werden entsprechend ignoriert, wenn für die Identität keine CV-Zertifikate benötigt werden.
- Dem zip-Archiv wird die Bezeichnung <Anbietername>_<Antragsnummer>_SMB_CRT.zip geben, wobei <Anbietername> aus dem Namen des zugehörigen CSR-zip-Archiv übernommen wird.
- Das fertige Zertifikatspaket wird mit dem öffentlichen Schlüssel aus dem zuvor geprüften C.HSK.ENC hybrid mittels AES-GCM verschlüsselt wobei die Vorgaben aus gemSpec_Krypt umgesetzt (GS-A_4368*, GS-A_4389*, A_17220*) werden.
- Die fertige Datei wird <Anbietername>_<Antragsnummer>_SMB_CRT.zip.enc genannt.

Das Signaturformat für das eingangs zu prüfende CSR-Paket entspricht dem für die detached Signatur einer TSL entsprechend gemSpec_Kon#A_21185* mit der Beschränkung auf den Fall ECDSA (vgl. A_23655*).

[<=]

fkt. Eig. Test und Sicherheitsgutachten

A_25125 - Abholen des Zertifikatspakets beim Anbieter SMC-B

Der TSP-X.509 nonQES SMC-B MUSS für HSM-B-Anträge, bei denen ein Anbieter HSK vom Antragsteller ausgewählt wurde, den Schlüsselvehalter der ausgewählten Unternehmensgruppe zum Download des Zertifikatspakets auffordern. [<=]

fkt. Eig Test

A_25122 - Übergabe des Zertifikatspakets an Anbieter TI-Gateway

Der TSP-X.509 nonQES SMC-B MUSS für HSM-B-Anträge, bei denen ein Anbieter TI-Gateway vom Antragsteller ausgewählt wurde, dem ausgewählten TI-Gateway Anbieter einen Request mit dem Zertifikatspaket (A_23758*) senden, dafür die Operation loadCerts des SMB-Service des Zugangsmoduls des TI-Gateways verwenden und dabei die Auftragsdaten entsprechend A_25121* verwenden. [<=]

fkt. Eig. Test

4.1.2 Anforderungen an den Hersteller HSK

A_23906 - HSK - HSM-B - Einbringen C.HSK.SIG und C.HSK.ENC

Der Hersteller des HSK MUSS im Rahmen der HSM-Personalisierung individuell für jeden HSK zwei Schlüsselpaare erzeugen und dafür beim TSP Komponenten ein C.HSK.SIG und ein C.HSK.ENC Zertifikat beantragen, wobei beide zu einem HSK gehörende Zertifikate jeweils die selbe Identifikationsnummer (Pseudo-ICCSN) im Feld commonName enthalten müssen. Die Pseudo-ICCSN MUSS sich nach der für diesen HSK personalisierten HSK-Identität richten, also identisch sein zur Pseudo-ICCSN der Zertifikate C.AK.AUT und C.SAK.AUT. Eine Pseudo-ICCSN ist zu behandeln wie eine normale ICCSN.

Falls der Hersteller Highspeed-Konnektoren, die bereits im Feld in Betrieb sind, mit der Funktion Institutionsidentitäten im HSM (HSM-B) nachrüsten will, MUSS er selbst die Schlüssel vor Ort direkt im HSM erzeugen, im Nachgang die Zertifikate C.HSK.SIG und C.HSK.ENC beim TSP Komponenten beantragen und danach die Zertifikate in den HSK importieren. Genau nur der Schritt des Zertifikatsimports KANN durch den Schlüsselverwalter erfolgen.【<=】

SiGu HSM-Perso

A_23907 - HSK - HSM-B - Sichere Prozesse bzgl. C.HSK.SIG und C.HSK.ENC

Der Hersteller HSK MUSS durchsetzen, dass der Prozess der Schlüsselerzeugung im HSM und der Zertifikatsbeantragung beim TSP Komponenten im Rahmen des Einbringens der Zertifikate C.HSK.SIG und C.HSK.ENC nur im 4-Augen-Prinzip durchgeführt werden kann. Er MUSS zudem die Nutzung dieser Prozesse auf das absolut notwendige Minimum an Personen begrenzen.【<=】

SiGu-HSM-Perso

4.1.3 Anforderungen an den Anbieter HSK

A_23634 - Benennung von Schlüsselverwaltern

Der Anbieter eines Highspeed-Konnektors MUSS Mitarbeiter seiner Organisation benennen, welche die Rolle Schlüsselverwalter übernehmen, diese Mitarbeiter mit Vorname, Name, berufliche postalische Adresse, berufliche Telefonnummern und berufliche E-Mail-Adresse an die gematik melden und die gematik über Änderungen der Schlüsselverwalter informieren.

【<=】

Sicherheitsgutachten

Die geschützte Übermittlung der Daten wird mit den einzelnen Anbietern HSK vereinbart. Kontaktpunkt bei der gematik ist das Funktionspostfach kartenherausgabe@gematik.de.

Die von zugelassenen Anbietern HSK benannten Mitarbeiter werden von der gematik an den Anbieter SMC-B gemeldet.

A_23635 - Registrierung der Schlüsselverwalter

Der Anbieters Highspeed-Konnektor MUSS sicherstellen, dass Schlüsselverwalter (dedizierte Personen) sich für den Zugang zum Trust-Management-System (TMS) bzw. Antrags- und Freigabeportal des Anbieter SMC-B gegenüber diesem identifizieren/registrieren und die Prozesse des Anbieters SMC-B für den Zertifikatsabruf einhalten, damit der Anbieter SMC-B diese Personen im Betrieb zum Zwecke des Uploads von CSR-Paketen und des Downloads von Zertifikatspaketen authentifizieren kann.【<=】

Sicherheitsgutachten

Der Schlüsselverwalter führt dann Schlüsselerzeugung, Zertifikatsbeantragung und Zertifikatsbezug entsprechend den Vorgaben des Anbieters SMC-B durch. Vor der Ausführung dieser Schritte muss verifiziert werden, dass der Antragsteller tatsächlich Teil

der Organisation ist, die den HSK, auf den das HSM-B erstellt werden soll, im Eigenbetrieb verwendet.

A_25240 - Prüfung Antragsteller Teil der Organisation

Der Anbieter Highspeed-Konnektor MUSS durchsetzen, dass der Schlüsselverwalter eingehende Aufforderungen zur Schlüsselerzeugung für ein HSM-B dahingehend prüft, dass der angegebene Antragsteller (Name) tatsächlich Teil der den HSK betreibenden Organisation ist. [≤]

Sicherheitsgutachten

Nach erfolgreicher Zuordnung und Aktivierung der HSM-B in einer vInstanz beantragt der Antragsteller die Freischaltung seiner HSM-B-Identität im TMS/Antragsportal des Anbieters SMC-B, so dass diese für OCSP und VZD freigeschaltet wird.

Die für den Schutz des Verfahrens genutzten Schlüssel und Zertifikate im HSM des HSK müssen durch den Schlüsselverwalter unter Nutzung der entsprechenden Funktionalität des HSK (siehe A_23757*) hinsichtlich ihrer Laufzeit überwacht und rechtzeitig vor deren Ablauf eine Ausstellung neuer Schlüssel und Zertifikate beim Hersteller des HSK beauftragt werden.

A_23760 - Beauftragung neuer C.HSK.SIG und C.HSK.ENC

Der Anbieters Highspeed-Konnektor bzw. der Anbieter TI-Gateway MUSS sicherstellen, dass er die Laufzeit der Zertifikate C.HSK.SIG und C.HSK.ENC der von ihm betriebenen HSKs überwacht und spätestens 3 Monate vor Ablauf der aktuellen Zertifikate eine Ausstellung neuer Schlüssel und Zertifikate beim Hersteller des HSK beauftragt. [≤]

Sicherheitsgutachten

A_24017 - HSM-B - Löschen nicht mehr verwendeter Institutionsidentitäten

Der Anbieter HSK MUSS sicherstellen, dass Prozesse definiert und etabliert werden, die eine Löschung nicht mehr verwendeter Institutionsidentitäten durch den Schlüsselverwalter am HSK gewährleisten. [≤]

Sicherheitsgutachten

4.1.4 Produkteigenschaften des HSK

A_23654 - HSK - Optionales Feature virtuelle Institutionsidentitäten (HSM-B)

Der Highspeed-Konnektor KANN die Speicherung und Nutzung von Institutionsidentitäten im HSM unterstützen [≤]

~~fkt., Eig., Test, CC-Prüfstelle~~

A_24016 - HSM-B - Kein Zugriff des Betreibers auf das HSM

Der Highspeed-Konnektor mit virtuellen Institutionsidentitäten MUSS sicherstellen, dass kein externer Zugriff des Betreibers auf das HSM möglich ist, also entsprechende Schnittstellen entweder nicht erreichbar sind oder deren Sicherheit innerhalb von Sicherheitsnachweisverfahren verifiziert wurde. Somit schließt die Umsetzung des Features HSM-B eine Nutzung des HSM des HSK durch andere externe Komponenten wie bspw. einem TI-Gateway-Zugangsmodule (A_23473*) aus. Lediglich ein Zugriff durch den Hersteller des HSK KANN ermöglicht werden. [≤]

~~CC-Prüfstelle, Produktgutachten~~

A_23628 - HSM-B - Schlüsselerzeugung für Institutionsidentitäten

Ein Highspeed-Konnektor mit virtuellen Institutionsidentitäten MUSS die Erzeugung von Schlüsselpaaren für Institutionsidentitäten durch den Schlüsselverwalter und das Zugangsmodule unterstützen. So erzeugte Schlüsselpaare MÜSSEN die Anforderungen aus gemSpec_Krypt erfüllen. Die Erzeugung und Speicherung der Schlüssel MUSS durch den HSK gesteuert im HSM erfolgen und für jede Identität bzw. jedes zu beantragende

Zertifikat MUSS eine neues individuelles Schlüsselpaar erzeugt werden. So erzeugte private Schlüssel dürfen nicht auslesbar oder im Klartext exportierbar sein.【<=】

CC-Prüfstelle

A_23757 - HSM-B - Management von C.HSK.SIG und C.HSK.ENC

Ein Highspeed-Konnektor mit virtuellen Institutionsidentitäten MUSS für die Erneuerung seiner Zertifikate C.HSK.SIG und C.HSK.ENC eine Funktion anbieten, die es ausschließlich dem Hersteller ermöglicht, neue Schlüsselpaare für eben diese Identitäten im HSM zu erzeugen. Die Schlüsselpaare MÜSSEN auf elliptischen Kurven basieren und die entsprechenden Vorgaben aus gemSpec_Krypt erfüllen. Der Import der vom Hersteller beim TSP Komponenten beantragten Zertifikate KANN neben dem Hersteller auch für den Schlüsselverwalter möglich sein, wobei stets vom HSK technisch geprüft werden muss, dass importierte Zertifikate zum im HSM gespeicherten privaten Schlüssel passen. Sobald neue Zertifikate importiert wurden, SOLL für die Signatur neuer HSM-B-CSR-Pakete nur der zum neuen C.HSK.SIG gehörende private Schlüssel verwendet werden. Dies KANN durch den Schlüsselverwalter konfigurierbar sein. Verschlüsselungsidentitäten (C.HSK.ENC) können bis zu deren Ablauf für die Entschlüsselung verwendet werden. Die Management-Oberfläche des HSK muss die Laufzeit aller Zertifikate C.HSK.SIG und C.HSK.ENC sowie die in allen Zertifikaten verwendete Pseudo-ICCSN anzeigen.【<=】

CC-Prüfstelle

A_23655 - HSM-B - Export von CSR

Ein Highspeed-Konnektor mit virtuellen Institutionsidentitäten MUSS bei der Erzeugung von CSRs folgendes durchsetzen:

- Bei der Anfrage zur Erzeugung muss der HSK
 - im Falle des Eigenbetriebs vom Schlüsselverwalter die Antragsnummer und einen vom Schlüsselverwalter gewählten Identifikator für den Anbieter SMC-B abfragen, welcher im folgenden als [Anbietername] bezeichnet wird.
 - im Falle des TI-Gateways vom Zugangsmodul den [Anbieternamen] des Anbieters SMC-B (TSPName/Name aus dem TSL-Eintrag des Anbieters SMC-B) und die Antragsnummer aus der Schnittstelle zum Zugangsmodul übernehmen.
- Die im folgenden erzeugten Schlüssel werden intern im HSK mit den übergebenen Identifikatoren (Antragsnummer und Anbieter SMC-B) verknüpft für die spätere Zuordnung der Zertifikate
- Jeder CSR darf nur einen öffentlichen Schlüssel enthalten.
- Es müssen für X.509-Zertifikate je ein CSR für RSA und ECC Schlüssel jeweils für Authentisierung, Verschlüsselung und Signatur erzeugt werden.
- Im CSR müssen der CN (vom Anbieter SMC-B vergebene Antragsnummer) und der zu zertifizierende öffentliche Schlüssel übergeben werden.
- Es muss zudem ein CSR für das CVC mit dem dem Zertifikatsprofil C.SMC.AUTR_CVC.E256 erzeugt werden, mit dem die Antragsnummer im CN und der öffentliche Schlüssel übergeben werden.
- Die Signatur eines CSRs muss mit dem zu zertifizierenden öffentlichen Schlüssel prüfbar sein.
- Die CSRs müssen im PKCS#10 Format als BASE64 kodierte PEM-Dateien gespeichert werden.
- Die Dateinamen der exportierten CSR müssen dem Muster [Antragsnummer]_SMB_[AUT|ENC|OSIG|CVC]_[RSA|ECC].csr entsprechen.
- Die CSRs müssen zusammen mit dem Zertifikat C.HSK.ENC des HSK in einem ZIP-Archiv mit der Bezeichnung nach dem Muster

[Anbietername]_[Antragsnummer]_SMB_CSR.zip zusammengefasst werden und mit dem zu C.HSK.SIG gehörenden privaten Schlüssel signiert werden.

- Das Signaturformat für das CSR-Paket entspricht dem für die detached Signatur einer TSL entsprechend A_21185* mit der Beschränkung auf den Fall ECDSA.
- Die Signatur-Datei muss [Anbietername]_[Antragsnummer]_SMB_CSR.sig genannt werden

[<=]

CC-Prüfstelle, fkt.-Eig-Test

Die einzelnen CSRs im PKCS#10 Format haben als Bsp. für ECDSA (brainpool256) folgende Struktur:

```
SEQUENCE
  SEQUENCE
    INTEGER 00
    SEQUENCE
      SET
        SEQUENCE
          ObjectIdentifier commonName (2 5 4 3)
          UTF8String '<Antragsnummer>'
        SEQUENCE
          SEQUENCE
            ObjectIdentifier ecPublicKey (1 2 840 10045 2 1)
            ObjectIdentifier (1 3 36 3 3 2 8 1 1 7)
          BITSTRING <öffentlicher Schlüssel>
        [0]
      SEQUENCE
        ObjectIdentifier SHA256withECDSA (1 2 840 10045 4 3 2)
      BITSTRING, encapsulates
        SEQUENCE
          INTEGER <Signatur...>
          INTEGER <...Signatur>
```

A_23629 - HSM-B - Import von Zertifikaten zu Institutionsidentitäten

Ein Highspeed-Konnektor mit virtuellen Institutionsidentitäten MUSS dem Schlüsselverwalter und dem Zugangsmodul ermöglichen Zertifikatspakete von Institutionsidentitäten zu importieren. Der HSK muss die importierten Zertifikatspakete mit dem zu C.HSK.ENC passenden privaten Schlüssel entschlüsseln und dabei implizit die Integrität des Chiffrats prüfen (AES-GCM). Der HSK MUSS im Erfolgsfall die so importierten Zertifikate den privaten Schlüsseln zuordnen und die Korrektheit der Zuordnung überprüfen. Der HSK MUSS ggf. fehlende CV-Zertifikate ignorieren und die Identität ohne CV-Zertifikate anlegen. Der HSK MUSS die Gültigkeit der Zertifikate im Vertrauensraum der TI prüfen. Der HSK MUSS zu jeder Institutionsidentität den mit der Identität zusammen importierten Aktivierungscode so verschlüsselt speichern, dass nur der HSK selbst darauf zugreifen kann.[<=]

CC-Prüfstelle

A_23630 - HSM-B - Handhabung von Institutionsidentitäten als HSM-B

Der Highspeed-Konnektor muss die Zertifikate (AUT, ENC, SIG, CVC) einer Institutionsidentität mit ihren privaten Schlüssel und das zum CV-Zertifikat passende CV-CA-Zertifikat der zweiten Ebene und dem öffentlichen Schlüssel der dazu passenden CVC-Root-CA zu einer virtuellen Karte (HSM-B) zusammenfassen und mit einer Identifikationsnummer (Pseudo-ICCSN), einer eindeutigen [CtID:SlotID] verknüpfen, so dass sie wie eine SMC-B verwendet werden kann. Der HSK MUSS ggf. fehlende CV-

Zertifikate ignorieren und die Identität ohne CV-Zertifikate anlegen. Der Highspeed-Konnektor muss für eine HSM-B die Parameter CardHandle und InsertTime füllen. [≤]

fkt. Eig. Test

A_23631 - HSM-B - Zuordnung von Institutionsidentitäten zu vInstanzen

Der Highspeed-Konnektor MUSS dem Schlüsselverwalter und dem Zugangsmodul ermöglichen eine HSM-B-Identität einer oder mehreren vInstanzen zuzuordnen und MUSS gewährleisten, dass die Identität auch nur von diesen vInstanzen verwendet werden kann. [≤]

fkt. Eig. Test, CC-Prüfstelle

A_23632 - HSM-B - Mandantenzuordnung mit Aktivierungscode

Der Highspeed-Konnektor MUSS einem vInstanz-Administrator ermöglichen eine HSM-B einem Mandanten als SM-B_Verwaltet zuzuordnen. Der Highspeed-Konnektor MUSS dabei zur Eingabe eines Aktivierungscode auffordern. Die Zuordnung darf nur gespeichert werden, wenn der eingegebene Aktivierungscode dem mit den Zertifikaten importierten Aktivierungscode entspricht. Der Highspeed-Konnektor MUSS bei Falscheingaben des Aktivierungscode eine Verzögerung bis zur nächsten möglichen Eingabe des Aktivierungscode umsetzen um Brute-Force-Angriffe zu verhindern.

Der Highspeed-Konnektor MUSS beim Löschen der Zuordnung des HSM-B als SM-B_Verwaltet auch dessen Aktivierung für diese vInstanz zurücksetzen und somit bei der erneuten Zuordnung auch erneut die Aktivierung erzwingen. [≤]

fkt. Eig. Test, CC-Prüfstelle

Gemäß Regel 7 in TUC_KON_000 (TIP1-A_4524* / TAB_KON_512) darf nur dann auf eine SM-B zugegriffen werden, wenn diese als SM-B_Verwaltet konfiguriert ist.

A_25252 - Aufforderung zur Freischaltung

Der Highspeed-Konnektor MUSS den vInstanz-Administrator nach Aktivierung der HSM-B durch Eingabe des Aktivierungscode auf die Notwendigkeit zur Freischaltung beim Anbieter SMC-B hinweisen.

[≤]

fkt. Eig. Test

A_23633 - getCards mit HSM-B

Der Highspeed-Konnektor MUSS bei der Operation getCards für eine HSM-B, die dem Mandanten über SM-B_Verwaltet zugeordnet ist, CardHandle, Pseudo-ICCSN, CardType "HSM-B", InsertTime, CardHolderName und CertificateExpirationDate zurückmelden.

[≤]

Das HSM-B muss wie eine SMC-B verwendet werden können. Das umfasst mindestens:

- Zugriff über CardHandle, Zertifikatstyp und Crypt-Parameter
- Anzeige in der Liste der gesteckten Karte (Admin-GUI)
- Auslesen von C.AUT, C.ENC, C.SIG, für Crypt=[RSA, ECC]
- Operation SignDocument mit C.SIG (eAU, ePA u.a.)
- DecryptDocument mit C.ENC
- ExternalAuthenticate mit C.AUT
- readVSD (C2C und TUC_KON_110)
- Anwendung NFDM (C2C)
- Anwendung eMP (C2C)
- Anwendung ePA

Sofern das HSM-B keine CV-Zertifikate besitzt, müssen und können die C2C-Anwendungsfälle entsprechend nicht unterstützt werden.

137215A_23359-013 - Administration des HSK-Basis Systems

Der Highspeed-Konnektor MUSS eine Administration für das Basissystem bereitstellen und folgende separate Administratoren-Rollen umsetzen:

- Hersteller (HSK-Basis)
 - ~~Aktivierung der kryptographischen Kopplung zum SZZP-light-plus~~
 - ~~Konfiguration des Schlüssels für die Verbindung zum SZZP-light-plus~~
 - ~~Konfiguration der Kopplung zum HSM und Management HSM~~
 - Leserechte auf das Logging des Basissystems ohne die Logs der vInstanzen
 - Nutzer mit Rolle "Hersteller" erzeugen/ändern/löschen
 - Nutzer mit Rolle "Schlüsselverwalter" erzeugen/ändern/löschen
 - Rolle "Schlüsselverwalter" einem Nutzer der Rolle Basissystem-Administrator zuweisen oder entziehen
 - Neue Schlüssel für C.HSK.SIG, C.HSK.ENC, C.AK.AUT, C.SAK.AUT und C.SAK.AUTD_CVC erzeugen und CSRs exportieren
 - Zertifikate C.HSK.SIG, C.HSK.ENC, C.AK.AUT, C.SAK.AUT, C.SAK.AUTD_CVC und C.CA_SAK.CS importieren.
- Basissystem-Administrator
 - Verwaltung der instanzenübergreifenden HSK-Konfigurationen inkl. Einspielen Updates
 - Ressourcenkonfiguration von vInstanzen
 - Leserechte auf das Logging des Basissystems ohne die Logs der vInstanzen
 - Backup/Restore von vInstanzen (Snapshots)
 - Löschen von vInstanzen
 - Nutzer mit Rolle "HSK-Admin" erzeugen/ändern/löschen
 - im technisch unterstützten 4 Augenprinzip Nutzer mit Rolle "Zugangsmodul" erzeugen/ändern/löschen
- Schlüsselverwalter
 - Erzeugen von Schlüsselpaaren für Institutionsidentitäten und exportieren von mit C.HSK.SIG signierten CSR-Paketen (öffentliche Schlüssel der SM-B-Identität in mit vom jeweiligen privaten Schlüssel signierten CSRs)
 - Einspielen von verschlüsselten Zertifikatspaketen zu Institutionsidentitäten
 - Zuordnen von Institutionsidentitäten zu vInstanzen
 - Zertifikate C.HSK.SIG, C.HSK.ENC, C.AK.AUT, C.SAK.AUT, C.SAK.AUTD_CVC und C.CA_SAK.CS importieren
 - Institutionsidentitäten löschen
- Zugangsmodul (technischer user)
 - Erzeugen und löschen von vInstanzen
 - Zuordnen von IP-Adressen zu vInstanzen
 - Backup/Restore von vInstanzen

- Ressourcenkonfiguration von vInstanzen
- Erzeugen von Schlüsselpaaren für Institutionsidentitäten und exportieren von mit C.HSK.SIG signierten CSR-Paketen (öffentliche Schlüssel der SM-B-Identität in mit vom jeweiligen privaten Schlüssel signierten CSRs)
- Einspielen von verschlüsselten Zertifikatspaketen zu Institutionsidentitäten
- Zuordnen von Institutionsidentitäten zu vInstanzen
- Institutionsidentitäten löschen

[<=]

4.2 Änderung in gemF_TI-Gateway

4.2.1 Anforderungshaushalt

Im Folgenden werden die neuen Anforderungen für die am Herausgabeprozess Beteiligten definiert.

Zum Nachweis, dass der Antragsteller für ein HSM-B tatsächlich Nutzer des von ihm im Antrag ausgewählten TI-Gateway ist, wird seitens Anbieter SMC-B ein ID-Token vom Anbieter TI-Gateway eingeholt, im Zuge dessen sich der Antragsteller erfolgreich gegenüber dem Anbieter TI-Gateway authentisieren muss. Hierzu werden die Standards OAuth2 (konkret Authorization Code Flow) nach [RFC 6749] und [OpenID Connect] verwendet.

4.2.1.1 Herstellen von Vertrauensbeziehungen

4.2.1.1.1 Eigene Bekanntmachung des Anbieters TI-Gateway

Damit Anbieter SMC-B eine Vertrauensbeziehung zu Anbietern TI-Gateway aufbauen können, müssen die dafür notwendigen Informationen der Anbieter TI-Gateway in der TSL hinterlegt werden. Konkret muss der Anbieter TI-Gateway zunächst in der TSL aufgenommen werden über einen "TrustServiceProvider"-Eintrag. Unter diesem Eintrag ist das TLS-Zertifikat eines Anbieters TI-Gateway in einem Service-Eintrag vom Typ "unspecified" zu hinterlegen. Für den OIDC-Flow im Zuge der HSM-B-Antragstellung muss der Anbieter TI-Gateway zudem seine OIDC-Konfiguration bekanntmachen. Die url dafür wird im o.g. TSLEintrag hinterlegt. Ein Anbieter SMC-B wertet diese Einträge täglich aus und hält alle aktuellen Zuordnung von "TSPName/Name" und TLS-Zertifikat für die notwendigen Prüfungen vor und ruft zu jedem Anbieter TI-Gateway über die url aus dem Service-Eintrag die OIDC-Konfiguration ab.

A_25254 - TLS-Zertifikat für Anbieter TI-Gateway

Der Anbieter TI-Gateway MUSS ein TLS-Zertifikat vom Profil C.FD.TLS-S mit der technischen Rolle oid_tigw_zugm beim TSP-X.509 nonQES der Komponenten-PKI beantragen. [<=]

Anbietererklärung

A_25104 - TSL Eintrag für TLS-Zertifikat Anbieter TI-Gateway

Der Anbieter TI-Gateway MUSS einen Eintrag als "TrustServiceProvider" in der TSL beantragen. Der Anbieter TI-Gateway MUSS für seinen Eintrag als "TrustServiceProvider" einen "TSPService"-Eintrag vom Typ "unspecified" für die SMB-Service-URL für den

Konfigurationsinformations-Endpunkt und für das TLS-Zertifikat C.FD.TLS-S in der TSL beantragen.

Tabelle 2: TSP-Service für Anbieter TI-Gateway

ServiceTypIdentifizier	http://uri.etsi.org/TrstSvc/Svctype/unspecified
ServiceSupplyPoint	<SMB-Service-URL> für Konfigurationsinformations- Endpunkt und gleichzeitig OIDC-Issuer (A_25115*)
ServiceDigitalIdentity/DigitalId/X509Certificate	TLS-Server-Zertifikat C.FD.TLS-S
ServiceInformationExtensions/Extension/ ExtensionOID	entsprechend gemSpec_OID
ServiceInformationExtensions/Extension/ ExtensionValue	oid_tigw_zugm

[<=]

Anbietererklärung

A_25256 - TSL Eintrag für TLS-Zertifikat Anbieter TI-Gateway löschen lassen bei Zertifikatsungültigkeit

Der Anbieter TI-Gateway MUSS den Eintrag in der TSL für sein TLS-Serverzertifikat C.FD.TLS-S umgehend löschen lassen, wenn dieses auf Grund einer vermuteten oder bestätigten Kompromittierung nicht mehr gültig ist. [<=]

Sicherheitsgutachten

~~49000~~A_25115-01 - Bereitstellung OIDC Konfiguration am Konfigurationsinformations-Endpunkt

Das Zugangsmodul MUSS unter "<SMB-Service-URL aus TSL-Eintrag (A_25104)>/well-known/openid-configuration" einen Konfigurationsinformations-Endpunkt und an diesem folgende Konfigurationsinformationen entsprechend [OpenID Connect Discovery] bereitstellen:

- issuer (URL entsprechend TSL-Eintrag nach A_25104)
- authorization_endpoint
- token_endpoint
- jwks_uri (URL unter der C.FD.OSIG im RFC 7517 JWK Format erreichbar ist)
- response_types_supported (mindestens code ~~und id_token~~)

Dabei MUSS das Zugangsmodul für den Konfigurationsinformations-Endpunkt selbst und für den Downloadpunkt des C.FD.OSIG Zertifikats (jwks_uri) ausschließlich serverseitig authentifizierte https-Verbindungen zulassen unter Verwendung seines C.FD.TLS-S als Serverzertifikat. [<=]

~~flkt. Eig. Test, Produktgutachten~~

A_25257 - Löschen C.FD.OSIG Zertifikat vom Konfigurationsinformations-Endpunkt bei Zertifikatsungültigkeit

Der Anbieter TI-Gateway MUSS die am Konfigurationsinformations-Endpunkt (vgl. A_25115*) bereitgestellten Daten umgehend anpassen, wenn bzgl. seines C.FD.OSIG Zertifikat eine vermutete oder bestätigte Kompromittierung vorliegt, sodass an diesem Endpunkt stets nur gültige Zertifikate bereitgestellt werden. [≤]

Sicherheitsgutachten

4.2.1.1.2 Ermitteln von Anbietern SMC-B über die TSL

A_25103 - Namen Anbieter SMB und redirect_uri aus TSL extrahieren

Das Zugangsmodul MUSS täglich die TSL beziehen, diese prüfen und aus den Service-Einträgen vom Typ "unspecified" und mit dem ServiceInformationExtensions/Extension/ExtensionValue "oid_zert_smb" den vollständigen Service-Namen (TSPName/Name), die unter ServiceSupplyPoint eingetragene redirect_uri und das C.FD.TLS-C Zertifikat extrahieren und für spätere Prüfungen vorhalten. [≤]

Produktgutachten

Hinweis: Neben den Service-Einträgen der Anbieter TI-Gateway und SMC-B sind in Service-Einträgen des Typs "unspecified" auch die Zertifikate der Schlüsselgenerierungsdienste (SGD) für die ePA aufgeführt.

4.2.1.2 Nutzerauthentifizierung

A_25118 - Authentisierungs-Endpunkt - Bereitstellung

Das Zugangsmodul MUSS einen Authentisierungs-Endpunkt bereitstellen und an diesem ausschließlich serverseitig authentifizierte https-Verbindungen zulassen. [≤]

flt. Eig. Test, Produktgutachten

~~48991~~A_25105-01 - Authentisierungs-Endpunkt - Auswertung Requests

Das Zugangsmodul MUSS die an seinem Authentisierungs-Endpunkt entsprechend A_25086 eingehenden Requests wie folgt verarbeiten:

- Prüfung, dass response_type = "code~~-id_token~~",
- Ermittlung von Anbieter SMC-B (client_id), Antragsnummer (state), redirect_url und nonce für Verarbeitung entsprechend A_25106*,
- Prüfung, dass nonce nicht bereits für einen bestehenden aktuellen Auftrag des Anbieters SMC-B (entsprechend client_id) verwendet wird (aktuell = innerhalb der Laufzeit einer nonce entsprechend A_25086*),
- Prüfung, dass die redirect_uri der URL aus dem TSL-Eintrag mit ServiceType "unspecified" des ermittelten Anbieters SMC-B entspricht.

[≤]

Produktgutachten

A_25106 - Authentisierungs-Endpunkt - Response im Erfolgsfall

Das Zugangsmodul MUSS genau nur wenn die Prüfungen in A_25105* positiv durchlaufen wurden

- dem Nutzer eine Login-Seite präsentieren, die eindeutig besagt, dass es um die Authentisierung im Zuge der Bestellung einer HSM-B geht und dabei Anbieter SMC-B und Antragsnummer anzeigen,
- eine vollständige Nutzerauthentifizierung (siehe A_23242*) durchführen, eine bestehende Session darf also explizit nicht nachgenutzt werden, und

- im Erfolgsfall einen Authorization-Code erzeugen und intern verknüpft mit Name Anbieter SMC-B, Gateway-UserID, Erstellungszeit und Antragsnummer, ablegen und
- den Nutzer wie folgt zum Anbieter SMC-B zurückleiten:

```
HTTP/1.1 302 Found
Location: <redirect_uri>?code=<Authorization-Code>&state=<Antragsnummer>
```

[<=]

flkt. Eig. Test, Produktgutachten

A_25107 - Authentisierungs-Endpunkt - Response im Fehlerfall

Das Zugangsmodul MUSS im Fall von Fehlern bei der Auswertung von Requests (A_25105*) oder bei der Nutzerauthentifizierung (A_25106*) mit einer Fehlermeldung entsprechend [RFC 6749] Absatz 4.1.2.1 reagieren.

[<=]

flkt. Eig. Test, Produktgutachten

A_25119 - Authentisierungs-Endpunkt - Löschen von Authorization-Codes

Das Zugangsmodul MUSS nach A_25106 erzeugte und versendete Authorization-Codes nach 10 min aus seinem Speicher löschen, darf diese also nach Ablauf dieser Zeit nicht mehr bei der Prüfung nach A_25102* akzeptieren. [<=]

Produktgutachten

4.2.1.3 SMB-Service

A_25109 - SMB-Service

Das Zugangsmodul MUSS einen Service-Endpunkt "SMB-Service" für den Austausch mit den Anbietern SMC-B anbieten. Das Zugangsmodul MUSS dabei durchsetzen, dass

- ausschließlich beidseitig authentifizierte TLS-Verbindungen genutzt werden,
- das Zugangsmodul als Serveridentität C.FD.TLS-S des TI-Gateway verwendet,
- ausschließlich Verbindungen von Clients akzeptiert werden, die sich mit einem C.FD.TLS-C eines Anbieters SMC-B (technische Rolle oid_anb_smcb) ausweisen und
- das präsentierte TLS-Clientzertifikat, dem für den Anbieters SMC-B (TSPName/Name aus dessen TSL-Eintrag), wie er entsprechend des innerhalb dieses TLS-Kanals empfangenen Requests identifiziert wurde (Client-ID), entspricht, wobei zur Prüfung auf die Daten entsprechend A_25103* zurückgegriffen wird.

[<=]

flkt. Eig. Test, Produktgutachten

A_25126 - SMB-Service - Responses

Der SMB-Service des Zugangsmoduls MUSS Fehler- und Statusmeldungen mit http 200 und einer JSON-Struktur im Body der Response transportieren, falls nicht anders spezifiziert:

```
{
  "status": "ok | error"
  "code": "<Status- bzw. Fehlercode>",
  "message": "<Meldungstext>"
}[<=]
```

4.2.1.3.1 Token-Endpoint

A_25102 - SMB-Service - Operation getToken

Das Zugangsmodul MUSS in seinem SMB-Service die Operation getToken als Token-Endpoint bereitstellen

ServiceEndpoint	<SMB-Service-URL>/getToken
Eingangsparameter	POST parameter: <ul style="list-style-type: none"> grant_type = "authorization_code" und code ist ein noch gültiger vom Authentisierungs-Endpoint des Zugangsmodul erzeugter Authorization-Code.
Verarbeitung	Das Zugangsmodul prüft auf grant_type = "authorization_code". Das Zugangsmodul prüft, ob es zu diesem Code eine Nutzerauthentifizierung gespeichert hat, die noch nicht gelöscht wurde gemäß A_25119. Das Zugangsmodul erstellt einen ID-Token wie in A_25108 beschrieben.
Response	wie in A_25108
Fehler	<ul style="list-style-type: none"> message: "Authorization-Code unbekannt oder abgelaufen", code: "SMBS_0002" message: "grant_type ungültig", Code: "SMBS_0003" message: "Interner Fehler bei der Token-Erzeugung", Code: "SMBS_0004"

[<=]

flkt. Eig. Test, Produktgutachten**A_25108 - SMB-Service - Token-Endpoint - Response im Erfolgsfall**

Das Zugangsmodul MUSS genau nur, wenn die Prüfungen nach A_25102* erfolgreich waren:

- den folgenden signierten ID-Token anhand der dem Authorization-Code zugeordneten Daten erzeugen:

ID-Token:

```
{ "iss": "<URL entsprechend TSL-Eintrag nach A_25104>",
  "sub": "<Antragsnummer aus Anfrage>.<GatewayUserID
authentifizierter Nutzer>",
  "aud": "<TSPName/Name des Anbieter-SMC-B aus Anfrage
(client_id)>",
  "nonce": "<nonce aus Anfrage>",
  "exp": "<Ausstellungsdatum iat + 300 Sekunden>",
  "iat": "<aktuelle Zeit als Sekunden seit 1970-01-01T00:00:00Z
in UTC>" }
```

Token Signatur:

JSON Web Signature (JWS) nach RFC7515 mit ECDSA mit P-256 und SHA-256 und entsprechendem Header:

```
{ "typ": "JWT",
  "alg": "HS256" }
```

- diesen im weiteren als JWS in Compact Serialization verwenden:
`BASE64(Header).BASE64(ID-Token).BASE64(Signature)`

- und dem Anbieter SMC-B wie folgt antworten:

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache
```

```
{
  "access_token": "",
  "token_type": "bearer",
  "expires_in": 300,
  "id_token": <ID-Token in JWS Compact Serialization>,
}
```

[<=]

~~flkt. Eig. Test, Produktgutachten~~~~flkt. Eig. Test~~

4.2.1.3.2 CSR erzeugen und senden

A_25110 - SMB-Service - Operation requestCSR

Das Zugangsmodul MUSS am SMB-Service die Operation requestCSR anbieten

Service Endpunkt	<SMB-Service-URL>/requestCSR
Eingangsparameter	GET-Parameter: auftrag=<BASE64(Auftragsdaten)> Body: leer
Verarbeitung	<ol style="list-style-type: none"> 1. Extrahiere TSPName/Name des Anbieter-SMB, Antragsnummer und GatewayUserID aus den Auftragsdaten (vgl. A_25121*) 2. Prüfe ob das Tripel Anbieter-SMB, Antragsnummer, GatewayUserID bereits persistiert ist 3. Löse Erstellung CSR-Paket im HSK aus und persistiere den Status CSR-creation-HSK 4. Rückmeldung an den Aufrufer
Rückgabe	code: "SMBS_0001", message: "CSR-Erstellung im HSK ausgelöst"
Fehlermeldung	zu 2. code: "SMBS_0005", message: "Nutzerauthentisierung notwendig" sonst code: "SMBS_0006", message: "Fehler bei Verarbeitung"

[<=]

~~flkt. Eig. Test~~

A_25111 - Übernahme CSR-Pakete vom HSK

Das Zugangsmodul MUSS vom HSK erzeugte CSR-Pakete (zip-Datei und dazugehörige Signatur als sig-Datei entsprechend A_23655*) abholen und mit dem Tripel Anbieter-SMB, Antragsnummer, GatewayUserID und dem Status CSR-ready persistieren.【<=】

flkt.-Eig.-Test

A_25112 - SMB-Service - Operation getCSR

Das Zugangsmodul MUSS am SMB-Service die Operation getCSR anbieten

Service Endpunkt	<SMB-Service-URL>/getCSR
Eingangsparameter	GET-Parameter: auftrag=<BASE64(Auftragsdaten)> Body: leer
Verarbeitung	1. Extrahiere TSPName/Name des Anbieter-SMB, Antragsnummer und GatewayUserID aus den Auftragsdaten (vgl. A_25121*) 2. Prüfe den Status für das Tripel Anbieter-SMB, Antragsnummer, GatewayUserID 3. Rückmeldung an Aufrufer
Rückgabe	<pre>{ "status": "ok", "code": "SMBS_0016", "message": "CSR erstellt", "csr": "BASE64-zip", "sig": "BASE64-sig" }</pre>
Fehlerfälle	message: "CSR noch nicht erstellt", code: "SMBS_0007" message: "Fehler im Aufruf", code: "SMBS_0008" message: "Antragsnummer unbekannt", code: "SMBS_0009" message: "GatewayUserID unbekannt", code: "SMBS_0010" message: "CSR nicht vorhanden", code: "SMBS_0011"

【<=】

flkt.-Eig.-Test

4.2.1.3.3 Zertifikate importieren

A_25113 - Liste der vInstanzen eines Nutzers

Das Zugangsmodul MUSS für alle Nutzer eine aktuelle vInstanz-Liste (incl. Zuordnung zu einem HSK) mit allen Identifikatoren der vInstanzen zu der GatewayUserID des Nutzers vorhalten.【<=】

flkt.-Eig.-Herstellererklärung

A_25114 - SMB-Service - Operation loadCerts

Das Zugangsmodul MUSS am SMB-Service die Operation loadCerts anbieten

Service Endpunkt	<SMB-Service-URL>/loadCerts
------------------	-----------------------------

Eingangsparameter	POST-parameter: auftrag=BASE64(Auftragsdaten) Body: BASE64(Zertifikatspaket)
Verarbeitung	<ol style="list-style-type: none"> 1. Extrahiere TSPName/Name des Anbieter-SMB, Antragsnummer und GatewayUserID aus den Auftragsdaten (vgl. A_25121*) 2. Prüfe den Status für das Tripel Anbieter-SMB, Antragsnummer, GatewayUserID 3. Lade Zertifikatspaket und vInstanz-Liste (A_25113*) in HSK 4. Nach Erfolgreicher Rückmeldung vom HSK setze Status certs-loaded 5. Rückmeldung an Aufrufer
Rückgabe	message: "Zertifikate erfolgreich geladen", code: "SMBS_0017";
Fehler	message: "Parameter nicht extrahierbar", code: "SMBS_0012" message: "Kein unbeantworteter CSR identifiziert", code: "SMBS_0013" message: "Keine virtuelle Instanz", code: "SMBS_0014" message: "Fehler vom HSK", code: "SMBS_0015"

[<=]

| **flkt. Eig. Test**

4.2.1.4 Verwalten von Institutionsidentitäten

A_25251 - Löschen von Institutionsidentitäten

Das Zugangsmodul MUSS das Löschen von Institutionsidentitäten in folgenden Fällen beim HSK anstoßen:

- Der TI-Gateway-Kunde löscht eine Institutionsidentität.
- Der TI-Gateway-Kunde wird gelöscht.

[<=]

| **flkt. Eig. Test**

4.3 Änderung in gemSpec_PKI

Die neuen Zertifikatsprofile C.HSK.SIG und C.HSK.ENC müssen im Dokument an den relevanten Stellen hinzugefügt werden. Die Anforderungen zu den Profilen selbst sind entsprechend neu. Bzgl. Tabelle "Common Name (CN) der End-Entity-Zertifikate Test-PKI" werden nur die neuen Einträge dargestellt. Anforderungen, die auf die angepasste Tabelle verweisen sind ggf. entsprechend ebenso anzupassen.

Die Zertifikatsprofile C.HSK.SIG und C.HSK.ENC müssen vom TSP Komponenten umgesetzt werden.

4.3.1.1 Kapitel 5.6.4.4 C.HSK.Sig - Authentisierung HSK

A_23979 - Umsetzung Zertifikatsprofil C.HSK.SIG

Der TSP-X.509 nonQES MUSS C.HSK.SIG gemäß Tab_PKI_246 umsetzen.

Tabelle 3: Tab_PKI_246 Zertifikatsprofil C.HSK.SIG Authentisierung HSK (nur in ECC-Variante)

Element		Inhalt	Kar.	
certificate		C.HSK.SIG		
	tbsCertificate			
	version	2 (v3)		
	serialNumber	gemäß [RFC5280#4.1.2.2.]		
	signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359-*)]		
	issuer	DN der ausstellenden CA		
	validity	Gültigkeit des Zertifikats (von - bis)		
	subject			
	commonName	<Pseudo-ICCSN>	1	
	organizationalUnitName	Relevante Einheit des Konnektor-Herstellers	0-1	
	organizationName	Name des Konnektor-Herstellers	1	
	streetAddress	Anschrift des Konnektor-Herstellers	0-1	
	postalCode	Postleitzahl der Anschrift des Konnektor-Herstellers	0-1	
	localityName	Stadt der Anschrift des Konnektor-Herstellers	0-1	
	stateOrProvinceName	Bundesland der Anschrift des Konnektor-Herstellers	0-1	
	countryName	Herkunftsland des Konnektor-Herstellers	1	
	andere Attribute		0	
	subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359-*)] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
	extensions			critical
	SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Konnektors	1	FALSE
	KeyUsage {2 5 29 15}	Nur für Schlüsselgeneration ECDSA: nonRepudiation	1	TRUE
	SubjectAltNames {2 5 29 17}	dNSName = „konnektor.konlan“ bei überlangem organizationName: Langname des Konnektor-Herstellers	1 0-1	FALSE
	BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE

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

[<=]

4.3.1.2 Kapitel 5.6.4.5 C.HSK.ENC- Verschlüsselung HSK

A_23981 - Umsetzung Zertifikatsprofil C.HSK.ENC

Der TSP-X.509 nonQES MUSS C.HSK.ENC gemäß Tab_PKI_247 umsetzen.

Tabelle 4: Tab_PKI_247 C.HSK.ENC Verschlüsselung fachanwendungsspezifische Dienste (nur in ECC-Variante)

Element		Inhalt	Kar.	
certificate		C.HSK.ENC		
	tbsCertificate			
	version	2 (v3)		
	serialNumber	gemäß [RFC5280#4.1.2.2.]		
	signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS- A_4359-*]		
	issuer	DN der ausstellenden CA		
	validity	Gültigkeit des Zertifikats (von - bis)		
	subject			
	commonName	<Pseudo-ICCSN>	1	
	organizationalUnitName	Relevante Einheit des Konnektor- Herstellers	0-1	

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

--	--	--	--

[<=]

Tabelle 5: Common Name (CN) der End-Entity-Zertifikate Test-PKI

Zertifikatstyp	Halter / Art	CN Test-PKI gleich CN Produktiv-PKI?
C.HSK.SIG	Gerät	Ja
C.HSK.ENC	Gerät	Ja

4.4 Änderung in gemSpec_OID

4.4.1 Kapitel 3.5.4 OID-Vorgabe für technische Rollen

Es müssen die neuen technischen Rolle (OIDs) für TI-Gateway Zugangsmodul und die technische Schnittstelle beim Anbieter SMC-B hinzugefügt werden. Anforderungen, die auf die angepasste Tabelle verweisen sind ggf. entsprechend ebenso anzupassen.

GS-A_4446-12 - OID-Festlegung für technische Rollen

Ein TSP-X.509 MUSS die technischen Rollen für die Nutzung in X.509-Zertifikaten der TI mit OIDs entsprechend der Tabelle Tab_PKI_406-* referenzieren.

Tabelle 6: Tab_PKI_406-* OID-Festlegung technische Rolle in X.509-Zertifikaten

OID-Referenz in anderen Dokumenten	ProfessionItem (Beschreibung der technischen Rolle)	ProfessionOID (OID der technischen Rolle)	Zertifikatsprofil(e) in denen die ProfessionOID im Element Admission vorkommen darf
oid_vsdd	Versichertenstammdatendienst	1.2.276.0.76.4.97	C.FD.TLS-S
oid_ocsp	Online Certificate Status Protocol	1.2.276.0.76.4.99	In keinem Zertifikatsprofil verwendet.
oid_cms	Card Management System	1.2.276.0.76.4.100	C.FD.TLS-S
oid_ufs	Update Flag Service	1.2.276.0.76.4.101	C.FD.TLS-S
oid_ak	Anwendungskonnektor	1.2.276.0.76.4.103	C.AK.AUT
oid_nk	Netzkonnektor	1.2.276.0.76.4.104	C.NK.VPN

oid_kt	Kartenterminal	1.2.276.0.76.4.105	C.SMKT.AUT
oid_sak	Signaturanwendungs- komponente	1.2.276.0.76.4.119	C.SAK.AUT
oid_int_vsdm	Intermediär VSDM	1.2.276.0.76.4.159	C.FD.TLS-S, C.FD.TLS-C
oid_konfigdienst	Konfigurationsdienst	1.2.276.0.76.4.160	C.ZD.TLS-S
oid_vpnz_ti	VPN-Zugangsdienst-TI	1.2.276.0.76.4.161	C.VPNK.VPN C.ZD.TLS-S
oid_vpnz_sis	VPN-Zugangsdienst-SIS	1.2.276.0.76.4.166	C.VPNK.VPN-SIS
oid_cmfd	Clientmodul	1.2.276.0.76.4.174C	C.CM.TLS-CS
oid_vzd_ti	Verzeichnisdienst-TI	1.2.276.0.76.4.171	C.ZD.TLS-S C.FD.SIG
oid_komle	KOM-LE Fachdienst	1.2.276.0.76.4.172	C.FD.TLS-S C.FD.TLS-C
oid_komle- recipient-emails	KOM-LE S/MIME Attribut recipient-emails	1.2.276.0.76.4.173	In keinem Zertifikatsprofil verwendet.
oid_stamp	Störungsampel	1.2.276.0.76.4.184	C.ZD.TLS-S
oid_tsl_ti	TSL-Dienst-TI	1.2.276.0.76.4.189	C.ZD.TLS-S
oid_wadg	Weitere elektronische Anwendungen des Gesundheitswesens sowie für die Gesundheitsforschung n. P. 291a Abs. 7 Satz 3 SGB V	1.2.276.0.76.4.198	C.FD.TLS-S C.FD.SIG C.FD.AUT C.FD.ENC
oid_epa_authn	ePA Authentisierung	1.2.276.0.76.4.204	C.FD.TLS-S C.FD.SIG
oid_epa_authz	ePA Autorisierung	1.2.276.0.76.4.205	C.FD.TLS-S C.FD.SIG
oid_epa_dvw	ePA Dokumentenverwaltung	1.2.276.0.76.4.206	C.FD.TLS-S
oid_epa_mgmt	ePA Management	1.2.276.0.76.4.207	C.FD.TLS-S C.FD.TLS-C
oid_epa_recover y	ePA automatisierter Berechtigungserhalt	1.2.276.0.76.4.208	C.FD.ENC

oid_epa_vau	ePA vertrauenswürdige Ausführungsumgebung	1.2.276.0.76.4.209	C.FD.AUT C.FD.ENC C.FD.SIG
oid_vz_tsp	Zertifikatsverzeichnis TSP X.509	1.2.276.0.76.4.215	In keinem Zertifikatsprofil verwendet.
oid_whk1_hsm	HSM Wiederherstellungskomponente 1	1.2.276.0.76.4.216	In keinem Zertifikatsprofil verwendet.
oid_whk2_hsm	HSM Wiederherstellungskomponente 2	1.2.276.0.76.4.217	In keinem Zertifikatsprofil verwendet.
oid_whk	Wiederherstellungskomponente	1.2.276.0.76.4.218	In keinem Zertifikatsprofil verwendet.
oid_sgd1_hsm	HSM Schlüsselgenerierungsdienst 1	1.2.276.0.76.4.219	C.SGD-HSM.AUT
oid_sgd2_hsm	HSM Schlüsselgenerierungsdienst 2	1.2.276.0.76.4.220	C.SGD-HSM.AUT
oid_sgd	Schlüsselgenerierungsdienst	1.2.276.0.76.4.221	C.FD.TLS-S
oid_erp-vau	E-Rezept vertrauenswürdige Ausführungsumgebung	1.2.276.0.76.4.258	C.FD.ENC C.FD.AUT
oid_erezept	E-Rezept	1.2.276.0.76.4.259	C.FD.TLS-S C.FD.SIG C.FD.OSIG C.FD.TLS-C
oid_idpd	IDP-Dienst	1.2.276.0.76.4.260	C.FD.TLS-S C.FD.SIG
oid_epa_logging	ePA-Aktensystem-Logging	1.2.276.0.76.4.261	C.FD.SIG
oid_bestandsnetze	Bestandsnetze.xml Signatur	1.2.276.0.76.4.288	C.ZD.SIG
oid_epa_vst	ePA Vertrauensstelle	1.2.276.0.76.4.289	C.FD.TLS-S C.FD.ENC
oid_epa_fdz	ePA	1.2.276.0.76.4.290	C.FD.TLS-S

	Forschungsdatenzentrum		C.FD.ENC
oid_tim	TI-Messenger	1.2.276.0.76.4.294	C.FD.SIG
oid_hsk	Highspeed-Konnektor	1.2.276.0.76.4.302	C.HSK.SIG C.HSK.ENC
oid_idpd_sek	sektoraler IDP	1.2.276.0.76.4.307	C.FD.SIG
oid_tigw_zugm	TI-Gateway Zugangsmodul	1.2.276.0.76.4.***3 09	C.FD.OSIG C.FD.TLS-S
oid_zert_smb	Technische Zertifikatsausgabestelle eines Anbieters SMC-B	1.2.276.0.76.4.***3 10	C.FD.TLS-C

[<=]

4.5 Anpassung in gemSpec_TSL

Bzgl. der Einträge vom Typ "unspecified" müssen Änderungen am Hinweis-Satz in Kap 7.9 und an einer Anforderung vorgenommen werden.

Hinweis: Es wird auch ein Element ServiceSupplyPoint gesetzt und mit einer Platzhalter-URL befüllt, falls keine andere URL benötigt wird. Im Falle eines Eintrages für Anbieter TI-Gateway und Anbieter SMC-B wird eine für den Dienst notwendige URL verwendet. Siehe dazu [TIP1-A_4106] und die nachfolgenden Erklärungen.

A_17936-01 - TSL Unspecified Extension

Der TSL-Dienst MUSS für Unspecified-Dienste im Element ServiceInformationExtensions ein Element Extension eintragen, welches den Platzhalter-OID (oid_tsl_placeholder) gemäß [gemSpec_OID#Tab_PKI_407] enthält, falls keine andere OID benötigt wird. Im Falle eines Eintrags für ein TLS-Zertifikat für einen Anbieter TI-Gateway wird die technische Rolle oid_tigw_zugm und für ein TLS-Zertifikat für einen Anbieter SMC-B die technische Rolle oid_zert_smb verwendet.

[<=]

4.6 Änderung in gemSpec_X_509_TSP

Die neuen Zertifikatsprofile C.HSK.SIG und C.HSK.ENC müssen hinzugefügt werden. Dies betrifft drei Tabellen, wobei im Folgenden nur die jeweils neuen Einträge gezeigt werden und nicht die vollständigen Tabellen. Anforderungen, die auf die Tabellen verweisen sind ggf. entsprechend ebenso anzupassen.

Tabelle 7: Tab_PKI_511-01 Berechtigte Zertifikatsantragsteller für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate

Zertifikatstyp	Berechtigte Zertifi-	Berechtigungs-	Zertifikatsnehmer
----------------	----------------------	----------------	-------------------

	katsantragsteller	prüfende Stelle	
C.HSK.SIG	Hersteller	gematik	Highspeed-Konnektor
C.HSK.ENC	Hersteller	gematik	Highspeed-Konnektor

Tabelle 8: Tab_PKI_512-02 Bereitstellungszeitpunkte der Zertifikatsstatusinformation durch den Erstellungsdiens

Zertifikatstyp	Bereitstellungszeitpunkt der Zertifikatsstatusinformation
C.HSK.SIG	unmittelbar nach Erstellung
C.HSK.ENC	unmittelbar nach Erstellung

Tabelle 9: Tab_PKI_516-01 Berechtigte Sperrantragsteller für Komponenten- und Signerzertifikate

Zertifikatstyp	Berechtigte Sperrantragsteller	zulässiger Sperrgrund
C.NK.VPN C.SAK.AUT C.AK.AUT C.HSK.SIG C.HSK.ENC C.SMKT.AUT C.FD. TLS-C C.FD. TLS-S C.FD.SIG C.FD.OSIG C.FD.AUT C.FD.ENC C.CM.TLS-CS C.SGD-HSM.AUT C.ZD.TLS-C *) C.ZD.TLS-S C.VPNK.VPN C.VPNK.VPN-SIS	Zertifikatsnehmender Hersteller und Anbieter, gematik	zu jeder Zeit ohne Angabe von Gründen Wegfall der Voraussetzung für den Betrieb gemäß Ausgabepolicy

5 Dokumentenhaushalt

<optional: Auswirkungen auf den Dokumentenhaushalt>

5.1 Neue Dokumente

<Optional: Eine Übersicht betroffener Dokumente mit kurzer Charakterisierung, z.B. Inhalt, etc.>

5.2 Übersicht betroffener Dokumente

<Optional: Eine Übersicht betroffener Dokumente, z. B. Spezifikationen, Konzepte, SystemDesign etc.>

5.3 Übersicht Produkt- und Anbietertypen

Änderungen in gemProdT_Highspeed-Konnektor

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_...]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

**Tabelle 10: Anforderungen zur funktionalen Eignung
"Produkttest/Produktübergreifender Test"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	[...]	

Änderungen in gemAnbT_Highspeed-Konnektor

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemAnbT_Highspeed-Konnektor]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

**Tabelle 11: Anforderungen zur funktionalen Eignung
"Produkttest/Produktübergreifender Test"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_23634	Benennung von Schlüsselverwaltern	
A_23635	Registrierung der Schlüsselverwalter	
A_23760	Erzeugung HSK-Signatur- und Verschlüsselungszertifikate am HSK und Übermittlung an Anbieter SMC-B	

Änderungen in gemAnbT_SMC-B_ATV

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemAnbT_SMC-B]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 12: Anforderungen zur funktionalen Eignung "Sicherheitsgutachten"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_23731	HSM-B Aktivierungscode	
A_23759	HSM-B-Identitäten - Empfang und Speicherung HSK-Signatur- und Verschlüsselungszertifikat	
A_23758	HSM-B-Identitäten - Signaturprüfung CSR-Paket und Verschlüsselung Zertifikatspaket	

Änderungen in gemProdT_X509_TSP_nonQES_Komp_PTV

**Tabelle 13: Anforderungen zur funktionalen Eignung
"Produkttest/Produktübergreifender Test"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A-23979	Umsetzung Zertifikatsprofil C.HSK.SIG	gemSpec_PKI
A-23981	Umsetzung Zertifikatsprofil C.HSK.ENC	gemSpec_PKI
GS-A_4446-10	OID-Festlegung für technische Rollen	gemSpec_OID

Änderungen in gemProdT_X509_TSP_nonQES_SMC-B

Tabelle 14

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
--------	-----------------	-------------------

6 Beispiele und Referenzimplementierungen

<Optional: Beispiele für Aufrufsequenzen, ausgetauschte Daten, etc. zur Unterstützung der Implementierung>

7 Anhang A - Verzeichnisse

7.1 Abkürzungen

Kürzel	Erläuterung
HSK	Highspeed-Konnektor
SM-B	Security Module Typ B (übergreifend)
HSM-B	Hardware Security Module Typ B (Ausprägung auf HSM im HSK)
TSP Komponenten	TSP-X.509 nonQES der Komponenten-PKI
TSL	Trust Service Status-List; Vertrauensliste der TI
vInstanz	virtuelle Konnektor-Instanz in einem HSK
CSR	Certificate Signing Request

7.2 Referenzierte Dokumente

7.2.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemRL_TSL_SP_CP]	Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL
[gemSpec_Kon]	Spezifikation Konnektor
[gemSpec_Krypt]	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur

[gemSpec_OID]	Spezifikation Festlegung von OIDs
[gemSpec_PKI]	Übergreifende Spezifikation Spezifikation PKI
[gemSpec_TSL]	Spezifikation TSL-Dienst

7.2.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[OpenID Connect]	https://openid.net/specs/openid-connect-core-1_0.html 15.12.2023 https://openid.net/specs/openid-connect-basic-1_0.html 15.12.2023
[OpenID Connect Discovery]	https://openid.net/specs/openid-connect-discovery-1_0.html 15.12.2023
[RFC2119]	RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels, March 1997
[RFC5280]	RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008
[RFC6749]	RFC 6749 - The OAuth 2.0 Authorization Framework, October 2012, https://datatracker.ietf.org/doc/html/rfc6749
[RFC7515]	RFC 7515 - JSON Web Signature (JWS), May 2015
[RFC7517]	RFC 7517 - JSON Web Key (JWK), May 2015
[RFC8705]	RFC 8705 - OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens, February 2020