Änderung in gemF_Highspeed-Konnektor

1 Personalisierung von Institutsidentitäten im HSK

Mit diesem Feature wird es möglich, eine Institutsidentität eines Krankenhauses - also alle dazu gehörigen kryptographischen Schlüssel und Zertifikate - im HSM eines HSK zu speichern, sodass eine HSK-Instanz diese direkt vom HSM nutzen kann, statt über eine SMC-B in einem eH-KT. In Abgrenzung zur SMC-B wird eine Identität im HSM des HSK im folgenden als ***HSM-B*** bezeichnet. Auch wenn Krankenhäuser erste Nutzergruppe für dieses Feature sind, soll es in einem zweiten Schritt auch auf andere Nutzergruppen ausgeweitet werden.

Der Personalisierungsprozess sowie technische Maßnahmen im HSK stellen sicher, dass die für eine LEI erzeugte Identität auch nur von dieser LEI genutzt werden kann.

1.1 Gesamtablauf

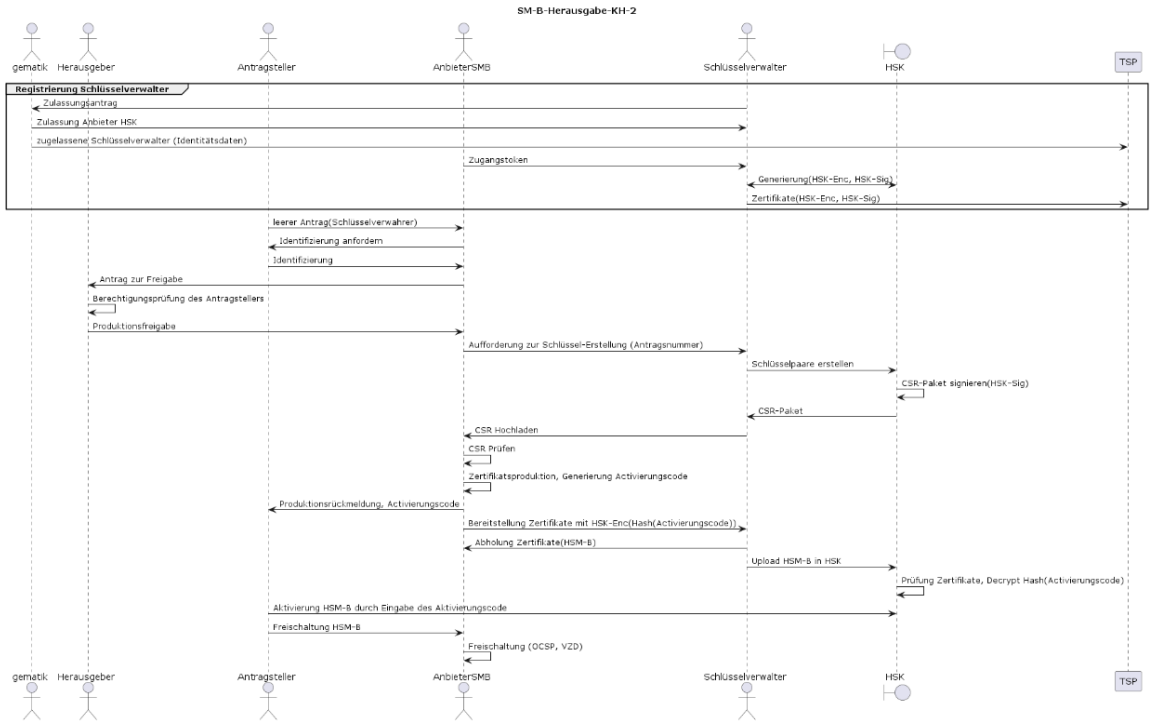
Im Folgenden wird der Gesamtablauf sowie die beteiligten Rollen beschrieben.

- Beteiligte Rollen sind:
  - Antragsteller: zur Beantragung der Institutionsidentität berechtigte Person bzw. zur Administration/Aktivierung der Institutsidentität berechtigte Person, also eine (oder mehrere) dafür verantwortliche Person im Krankenhaus
  - Schlüsselverwalter: Verwaltung der Schlüssel (bspw. Erzeugung), Administration des HSM bzgl. HSM-Bs, Administration des HSK bzgl. HSM-Bs
  - Hersteller HSK: Erzeugt pro HSK zwei Schlüssel-Paare im HSM des HSK und beantragt und bezieht dafür die Zertifikate C.HSK.SIG und C.HSK.ENC dafür vom TSP-Komponenten . Die Definition der Zertifikatsprofile erfolgt mit Änderung C_11501.
  - AZPD / TSP-Komponenten: Stellt Zertifikate C.HSK.SIG & C.HSK.ENC auf Antrag der HSK-Hersteller aus.
  - Anbieter SM-B: Erstellung von SM-B Zertifikaten, Aktivierung dieser Zertifikate am OCSP-Responder
  - Herausgeber: Verantwortliche Institution für die Herausgabe von Krankenhaus-Identitäten, Bestätigung von berechtigten Antragstellern
  - gematik: Zulassungsstelle für Anbieter HSK. In dieser Funktion kommuniziert die gematik die vom Anbieter benannten Schlüsselverwalter an die Anbieter SM-B.
  - HSK-Instanz-Admin: Admin für die HSK-Instanz(en) des Antragstellers
- Die Verwaltung der Schlüssel und die Administration des HSMs (indirekt über den HSK) erfolgt durch die neue Rolle **Schlüsselverwalter**, die direkt durch Personal des Krankenhauses ausgefüllt oder vom Krankenhaus beauftragt wird.
- Die Schlüsselverwalter von zugelassenen Anbietern HSK bekommen Zugang zum Trust-Management-System des Anbieter SM-B mit der Rolle Schlüsselverwalter.

Damit erhält er Aufträge zur Schlüsselgenerierung, kann CSR-Pakete hochladen und Zertifikatspakete herunterladen.

- Um sicherzustellen, dass Schlüssel im HSM des HSK erzeugt wurden und gleichzeitig Sicherheitslast von der Rolle Schlüsselverwalter zu nehmen, werden vom Hersteller des HSK während der Produktion (bzw. bei bestehenden Installationen durch einen vor-Ort-Wartungseinsatz) jeweils für jeden HSK individuell zwei ECC-Schlüsselpaare im HSM des HSK erzeugt und dafür beim TSP-Komponenten die Zertifikate C.HSK.SIG bzw. C.HSK.ENC beantragt und bezogen. Ein Schlüsselpaar wird zur Signatur / Signaturprüfung von CSR-Paketen (*C.HSK.SIG*) und eines zur Ver-/Entschlüsselung von Zertifikatspaketen (*C.HSK.ENC*) genutzt. Die Zertifikate enthalten eine für den jeweiligen HSK eindeutige ID (pseudo-ICCSN, welche sich nach der für diesen HSK personalisierten HSK-Identität richtet), die entsprechend bei einem Zertifikatspaar (Signatur & Verschlüsselung) für einen HSK identisch ist.
- Die Anbieter SM-B beziehen regelmäßig die TSL als Prüfgrundlage für die HSK-Zertifikate.
- 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" verauskunftet wird.
- Zudem wird perspektivisch eine Attestierung von erzeugten SM-B Schlüsseln durch das HSM selbst erforderlich, also mittels Maßnahmen, die direkt im HSM umgesetzt sind. HSK-Hersteller werden also entsprechende HSMs mit solch einer Funktion nutzen müssen bzw. an solchen Funktionen im HSM mitarbeiten und Anbieter SM-B müssen solche Attestierungen prüfen können.
- Der Antragsteller wählt im Antragsportal des Anbieters SM-B aus, ob die Identität als Karte (SMC-B) zugestellt werden soll, oder er wählt einen von der gematik dafür zugelassenen "Schlüsselverwalter-HSK" aus.
- Mit dem Auftrag des Antragserstellers erhält der Schlüsselverwalter-HSK vom Anbieter SM-B die Aufforderung Schlüsselpaare zu generieren und die öffentlichen Schlüssel in CSRs zum Anbieter SM-B hochzuladen. Im CSR wird die Antragsnummer des Anbieters SM-B eingebettet und die CSRs werden mit dem zugehörigen privaten Schlüssel signiert. Das CSR-Paket wird zusammen mit dem C.HSK.ENC automatisch vom HSK vor dem Export mit dem privaten Signaturschlüssel zu C.HSK.SIG signiert und das Signaturzertifikat C.HSK.SIG in die Signatur eingebettet.
- Der Anbieter SM-B prüft die Signatur des CSR-Paketes (mathematische Korrektheit Signatur und Zertifikatsprüfung C.HSK.SIG mit zeitlicher Gültigkeit, Prüfung gegen TSL und OCSP). Perspektivisch prüft der Anbieter SM-B zudem die Attestierung der SMB-Schlüssel durch das HSM. Im Positivfall prüft er, ob das enthaltene C.HSK.ENC dieselbe pseudo-ICCSN im Feld commonName beinhaltet, wie das geprüfte C.HSK.SIG. Im Positivfall erstellt der Anbieter SM-B (nach den üblichen Prüfungen der CSRs) die Zertifikate und generiert einen Aktivierungscode. Alle Zertifikate einer Identität und den SHA-256-Hashwert des Aktivierungscodes fasst er zu einem Zertifikatspaket zusammen und verschlüsselt dieses mittels des zuvor geprüften C.HSK.ENC. Der Anbieter SM-B liefert das verschlüsselte Zertifikatspaket an den Schlüsselverwalter-HSK aus.
- CV-Zertifikate einer SM-B Identität beinhalten die pseudo-ICCSN, X.509-Zertifikate beinhalten die Telematik-ID als Identitätsmerkmal.

- Der Schlüsselverwalter lädt das Zertifikatspaket in den HSK, wo es mit dem dort verfügbaren privaten C.HSK.ENC-Schlüssel entschlüsselt wird. Der Schlüsselverwalter ordnet dann das so erzeugten HSM-B auf Ebene des Basissystems HSK-Instanzen zu.
- Der Instanz-Admin kann dann die in der Instanz verfügbaren HSM-Bs im Infomodell einem Mandanten zuordnen (wie SMC-Bs).
- Um ein HSM-B nutzbar zu machen muss der Instanz-Admin den Aktivierungscode eingeben, der ihm vom Antragsteller übergeben wurde. Die Funktion des Aktivierungscodes ist vergleichbar mit einer Transport-PIN, die Zustellung kann z.B. über das Antragsportal des Anbieter SM-B an den authentifizierten Antragsteller erfolgen. Der HSK prüft den Aktivierungscode gegen den mit den Zertifikaten importierten Hashwert des Aktivierungscodes.
- Der HSK stellt sicher, dass nur HSM-Bs verwendet werden können, deren private Schlüssel im HSM geschützt sind.
- Durch die genannten organisatorischen Prozesse und Rollenausschlüsse, die Zuordnung von Schlüsseln zu einer LEI über die Auftragsnummer im CSR sowie die zwingend notwendige Aktivierung des HSM-B durch den Aktivierungscode den nur der Antragsteller über das Antragsportal des Anbieter SM-B erhalten hat, ist gewährleistet, dass nur die berechtigte LEI ihre HSM-B-Identität nutzen kann.



1.2 Anforderungen

Im Folgenden werden die neuen Anforderungen für alle Beteiligten definiert.

1.2.1 Anforderungen an den Anbieter SM-B (gemF_HighSpeed-Konnektor)

A_23731 - HSM-B Aktivierungscode
Der Anbieter SM-B MUSS bei der Zertifikatsproduktion für ein HSM-B einen individuellen, zufälligen Aktivierungscode aus zwölf (12) alphanummerischen Zeichen (Kleinbuchstaben [a..z] und Zahlen [0..9]) in der Form XXXX-XXXX-XXXX generieren.
Der Anbieter SM-B MUSS genau nur den SHA-256-Hashwert des Aktivierungscodes in einer Datei mit dem Namen <Auftragsnummer>_Aktivierungscode.txt dem Zertifikatspaket hinzufügen.
Der Anbieter SM-B MUSS genau nur dem Antragsteller den Aktivierungscode zugängig machen.**[**<=**]**

Sicherheitsgutachten

A_23759 - HSM-B-Identitäten - Prüfgrundlage für CSRs
Der Anbieter SM-B MUSS für die Zertifikatsproduktion für ein HSM-B als Prüfgrundlage täglich die TSL aus der TI beziehen, diese prüfen und im Erfolgsfall abspeichern und er SOLL zusätzlich die für die Prüfung von HSMs erbrachten Attestierungen notwendigen Prüfgrundlagen Authentizität und Integrität beziehen.**[**<=**]**

Sicherheitsgutachten

Als Abweichung von dem per "SOLL" geforderten Teil der Anforderung A_23759* gilt lediglich die Nicht-Verfügbarkeit solcher Attestierungsfunktionalität in HSMs und somit entsprechend die Nicht-Verfügbarkeit der genannten Prüfgrundlage. Perspektivisch wird auch dieser Anforderungsteil per "MUSS" gefordert werden und dann ggf. detailliert.

A_23758 - HSM-B-Identitäten - Signaturprüfung CSR-Paket und Verschlüsselung Zertifikatspaket
Der Anbieter SM-B MUSS bei der Zertifikatsproduktion für ein HSM-B

- die Signatur des empfangenen CSR-Pakets wie folgt prüfen:
  - mathematische Korrektheit der Signatur,
  - C.HSK.SIG-Zertifikat
    - zeitliche Gültigkeit
    - Prüfung gegen die TSL
    - Prüfung OCSP-Status
- prüfen, dass das im Request enthaltene C.HSK.ENC-Zertifikat die gleiche pseudo-ICCSN beinhaltet, wie das zuvor geprüfte C.HSK.SIG-Zertifikat
- Als Zertifikatspaket ein tar-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 Hash des Aktivierungscodes als Aktivierungscode.txt bilden. 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.
- das fertige Zertifikatspaket mit dem öffentlichen Schlüssel aus dem zuvor geprüften C.HSK.ENC hybrid mittels AES-GCM verschlüsseln und dabei die Vorgaben aus gemSpec_Krypt umsetzen (GS-A_4368*, GS-A_4389*, A_17220*).

Das Signaturformat für das CSR-Paket entspricht dem für die detached Signatur einer TSL entsprechend A_21185* mit der Beschränkung auf den Fall ECDSA.

Darüber hinaus SOLL der Anbieter SM-B die HSM-Attestierung der CSRs bzw. öffentlichen Schlüssel aus den CSR gegen die zuvor bezogene Prüfgrundlage verifizieren und Zertifikate auf die geprüften öffentlichen Schlüssel ausschließlich im Erfolgsfall ausstellen.**[<=]**

Sicherheitsgutachten

Als Abweichung von dem per "SOLL" geforderten Teil der Anforderung A_23758* gilt lediglich die Nicht-Verfügbarkeit solcher Attestierungsfunktionalität in HSMs und somit entsprechend die Nicht-Verfügbarkeit der genannten Prüfgrundlage. Perspektivisch wird auch dieser Anforderungsteil per "MUSS" gefordert werden und ggf. detailliert.

1.2.2 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.
Falls der Hersteller Highspeed-Konnektoren, die bereits im Feld in Betrieb sind, mit der Funktion Institutsidentitäten 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 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

1.2.3 Anforderungen an den Anbieter HSK

A_23634 - Benennung von Schlüsselverwaltern
Der Anbieter eines Highspeed-Konnektors MUSS Mitarbeiter benennen, welche die Rolle Schlüsselverwalter übernehmen, diese Mitarbeiter mit Name, Geburtsort, Geburtsdatum, Anschrift, E-Mail-Adresse an die gematik melden und die gematik über Änderungen der Schlüsselverwalter informieren.
[<=]

Sicherheitsgutachten

Die benannten Mitarbeiter werden von der gematik nach Zulassung an den Anbieter SM-B gemeldet.

A_23635 - Registrierung der Schlüsselverwalter
Der Anbieters Highspeed-Konnektor MUSS sicherstellen, dass Schlüsselverwalter sich für den Zugang zum Trust-Management-System (TMS) des Anbieter SM-B gegenüber diesem identifizieren und die Prozesse des Anbieters SM-B für die Zertifikatsbeantragung einhalten.
[<=**]**

Sicherheitsgutachten

Nach erfolgreicher Registrierung des/der Schlüsselverwalter können Antragsteller-Institutsidentität diese Schlüsselverwalter für die Verwaltung ihrer Identitäten im Antragsportal auswählen. Der Schlüsselverwalter führt dann Schlüsselerzeugung, Zertifikatsbeantragung und Zertifikatsbezug entsprechend den Vorgaben des Anbieters SM-B durch.

Nach erfolgreicher Zuordnung und Aktivierung der HSM-B in einer HSK-Instanz aktiviert der Antragsteller-Institutsidentität seine HSM-B im TMS der Anbieter SM-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 MUSS sicherstellen, dass Schlüsselverwalter für jeden verwalteten HSK am jeweiligen HSK die Zertifikate C.HSK.SIG und C.HSK.ENC hinsichtlich ihrer Laufzeit überwachen und spätestens 3 Monate vor Ablauf der aktuellen Zertifikate eine Ausstellung neuer Schlüssel und Zertifikate beim Hersteller des HSK beauftragen.**[**<=**]**

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

1.2.4 Produkteigenschaften des HSK

A_23654 - HSK - Optionales Feature virtuelle Institutsidentitäten (HSM-B)
Der Highspeed-Konnektor KANN die Speicherung und Nutzung von Institutsidentitäten im HSM unterstützen**[**<=**]**

fkt. Eig. Test, CC-Prüfstelle

A_24016 - HSM-B - Kein Zugriff des Betreibers auf das HSM
Der Highspeed-Konnektor mit virtuellen Institutsidentitäten 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-Zugangsmodul (A_23473*) aus. Lediglich ein Zugriff durch der Hersteller des HSK KANN ermöglicht werden.**[**<=**]**

CC-Prüfstelle, Produktgutachten

A_23628 - HSM-B - Schlüsselerzeugung für Institutsidentitäten
Ein Highspeed-Konnektor mit virtuellen Institutsidentitäten MUSS die Erzeugung von Schlüsselpaaren für Institutsidentitäten durch den Schlüsselverwalter 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. 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 Institutsidentitäten 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 Institutsidentitäten MUSS bei der Erzeugung von CSRs die Antragsnummer vom Schlüsselverwalter abfragen.
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 SM-B vergebene Antragsnummer), die Schlüsselverwendungen (siehe Tabelle) 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 Auftragsnummer im CN und der öffentlicher Schlüssel übergeben werden.
Dem CN muss bei CSRs in der Test- und Referenzumgebung ein „TEST-ONLY“ angefügt

sein.
Die Signatur eines CSRs muss mit dem zu zertifizierenden öffentlichen Schlüssel prüfbar sein.
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 nach dem Muster [Antragsnummer]_SMB.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 erzeugten Schlüssel für die SM-B-Identitäten SOLLEN im HSM durch das HSM so attestiert werden, dass für den TSP prüfbar ist, dass die Schlüssel im HSM erzeugt wurden.

Zertifikatstyp	**Schlüsselverwendung (Key Usage)**
Aut (RSA)	digitalSignature keyEncipherment
Aut (ECC)	digitalSignature
Enc (RSA)	keyEncipherment dataEncipherment
Enc (ECC)	keyAgreement
OSig (RSA)	nonRepudiation
OSig (ECC)	nonRepudiation

[<=]

CC-Prüfstelle, fkt. Eig Test

Als Abweichung von dem per "SOLL" geforderten Teil der Anforderung A_23655* gilt lediglich die Nicht-Verfügbarkeit solcher Attestierungsfunktionalität in HSMs. Perspektivisch wird auch dieser Anforderungsteil per "MUSS" gefordert werden.

A_23629 - HSM-B - Import von Zertifikaten zu Institutsidentitäten
Ein Highspeed-Konnektor mit virtuellen Institutsidentitäten MUSS dem Schlüsselverwalter ermöglichen Zertifikatspakete von Institutsidentitäten 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 die Gültigkeit der Zertifikate im Vertrauensraum der TI prüfen. Der HSK MUSS zu jeder Institutsidentität den mit der Identität zusammen importierten Hash des Aktivierungscodes speichern. **[<=]**

CC-Prüfstelle

A_23630 - HSM-B - Handhabung von Institutsidentitäten als HSM-B
Der Highspeed-Konnektor muss die Zertifikate (AUT, ENC, SIG, CVC) einer Institutsidentität 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 Highspeed-Konnektor muss für eine HSM-B die Parameter CardHandle und InsertTime füllen. **[**<=**]**

fkt. Eig. Test

A_23631 - HSM-B - Zuordnung von Institutsidentitäten zu HSK-Instanzen
Der Highspeed-Konnektor MUSS dem Schlüsselverwalter ermöglichen eine HSM-B-Identität einer oder mehreren HSK-Instanzen zuzuordnen und MUSS gewährleisten, dass die Identität auch nur von diesen HSK-Instanzen verwendet werden kann. **[**<=**]**

fkt. EIg Test, CC-Prüfstelle

A_23632 - HSM-B - Mandantenzuordnung mit Aktivierungscode
Der Highspeed-Konnektor MUSS einem Instanz-Administrator ermöglichen eine HSM-B einem Mandanten als SM-B_Verwaltet zuzuordnen. Der Highspeed-Konnektor MUSS dabei zur Eingabe eines Aktivierungscodes auffordern. Die Zuordnung darf nur gespeichert werden, wenn der SHA-256-Hashwert des eingegebenen Aktivierungscode dem mit den Zertifikaten Importierten Aktivierungscode-Hashwert entspricht.**[**<=**]**

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_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.
- Anzeige in der Liste der gesteckten Karte (Admingui) anzeigen.
- 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

A_23359-01 - 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 HSK-Instanzen
  - 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 und C.HSK.ENC erzeugen und CSRs exportieren
  - Zertifikate C.HSK.SIG und C.HSK.ENC importieren.
- Basissystem-Administrator
  - Verwaltung der instanzenübergreifenden HSK-Konfigurationen inkl. Einspielen Updates
  - Ressourcenkonfiguration von HSK-Instanzen
  - Leserechte auf das Logging des Basissystems ohne die Logs der HSK-Instanzen
  - Backup/Restore von HSK-Instanzen (Snapshots)
  - Löschen von HSK-Instanzen
  - 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 Institutsidentitäten 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 Institutsidentitäten
  - Zuordnen von Institutsidentitäten zu HSK-Instanzen
  - Zertifikate C.HSK.SIG und C.HSK.ENC importieren
  - Institutionsidentitäten löschen
- Zugangsmodul (technischer user)
  - Erzeugen und löschen von HSK-Instanzen
  - Zuordnen von IP-Adressen zu Konnektor-Instanzen

- Backup/Restore von HSK-Instanzen
- Ressourcenkonfiguration von HSK-Instanzen

[<=]

CC-Prüfstelle, fkt. Eig Test

Änderungen in gemProdT_Highspeed-Konnektor_PTV1.3.0

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 1: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

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

Änderungen in gemAnbT_Highspeed-Konnektor_ATV1.3.0

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 2: 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 SM-B	

Änderungen in gemAnbT_SMC-B_ATV1.7.4

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 3: 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	