
C_12715_Anlage

Inhaltsverzeichnis

1 Änderungsbeschreibung.....2

2 Änderung in gemF_Personalisierung_HSM-B.....3

3 Änderungen in Steckbriefen.....8

3.1 Änderungen in gemProdT_..._PTVx.y.z-n.....8

1 Änderungsbeschreibung

Um eine HSM-B Personalisierung auch für HSK im Eigenbetrieb sicherzustellen, soll den Anbietern TI-Gateway ermöglicht werden, Schlüsselverwalten eines HSK im Eigenbetrieb die Nutzung des SMB-Service zu ermöglichen. Dadurch entfällt für TSP-X509 die Notwendigkeit, einen separaten Prozess für HSK im Eigenbetrieb umzusetzen und zuzulassen. Ein Zugangsmodul TI-Gateway realisiert das Interface zum Schlüsselverwalter anstelle des TSP. Wegen der geringen Verbreitung des HSK-Eigenbetriebs und der Marktsituation, kann dieses Feature des Zugangsmoduls optional sein.

2 Änderung in gemF_Personalisierung_HSM-B

Kapitel 3.2.2.1 wird angepasst:

3.2.2.1 HSK-Eigenbetrieb

Beteiligte Rollen: gematik, Anbieter SMCB, Anbieter TI-Gateway, Anbieter HSK, Schlüsselvehalter

Im Falle des HSK-Eigenbetriebs muss der Schlüsselvehalter registriert werden. Die Schlüsselvehalter von zugelassenen Anbietern HSK werden der gematik von diesem Anbieter HSK benannt. Die gematik gibt diese Information (Schlüsselvehalter als Person und zugehörige Organisation, also Anbieter HSK) weiter an den benannten Anbieter TI-Gateway. Die potentiellen Schlüsselvehalter werden als Nutzer mit der Rolle "Schlüsselvehalter" im TI-Gateway angelegt. 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 Schlüsselvehalter. Der Antragsteller des HSK im Eigenbetrieb wählt im Antragsprozess beim Anbieter SMCB das benannte TI-Gateway aus und authentifiziert sich mit den Credentials des Schlüsselvehalters. Antragsteller und Schlüsselvehalter müssen dazu eng kooperieren, idealerweise werden beide Rollen von einer Person ausgeführt. Damit kann Danach empfängt der Schlüsselvehalter Aufträge zur Schlüsselgenerierung erhalten über das TI-Gateway, lädt CSR-Pakete hochladen und Zertifikatspakete herunterladen. Schlüsselvehalter wenden sich zur Registrierung an die Anbieter SMC-B. Anbieter SMC-B sind verpflichtet alle Schlüsselvehalter 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

3.3.2.2 CSR-Erzeugung im HSK

Beteiligte Rollen: HSK, Schlüsselvehalter, 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 3.2.1 Personalisierung von HSK-Identitäten durch Hersteller HSK). 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 (Schlüsselvehalter oder Zugangsmodul) zurückgegeben und von diesen über das Zugangsmodul zum Anbieter SMC-B übertragen.

Anpassungen im Kapitel 3.3

3.3 Herausgabe von Institutionsidentitäten

...

Fall HSK-Eigenbetrieb

Im Fall des HSK-Eigenbetriebs vermittelt der Schlüsselverwalter zwischen den Systemen des Anbieters SMB TI-GW und dem HSK. Antragsteller und Schlüsselverwalter kommen aus der gleichen Organisation und müssen eng kooperieren, idealerweise werden beide Rollen von einer Person ausgeführt.

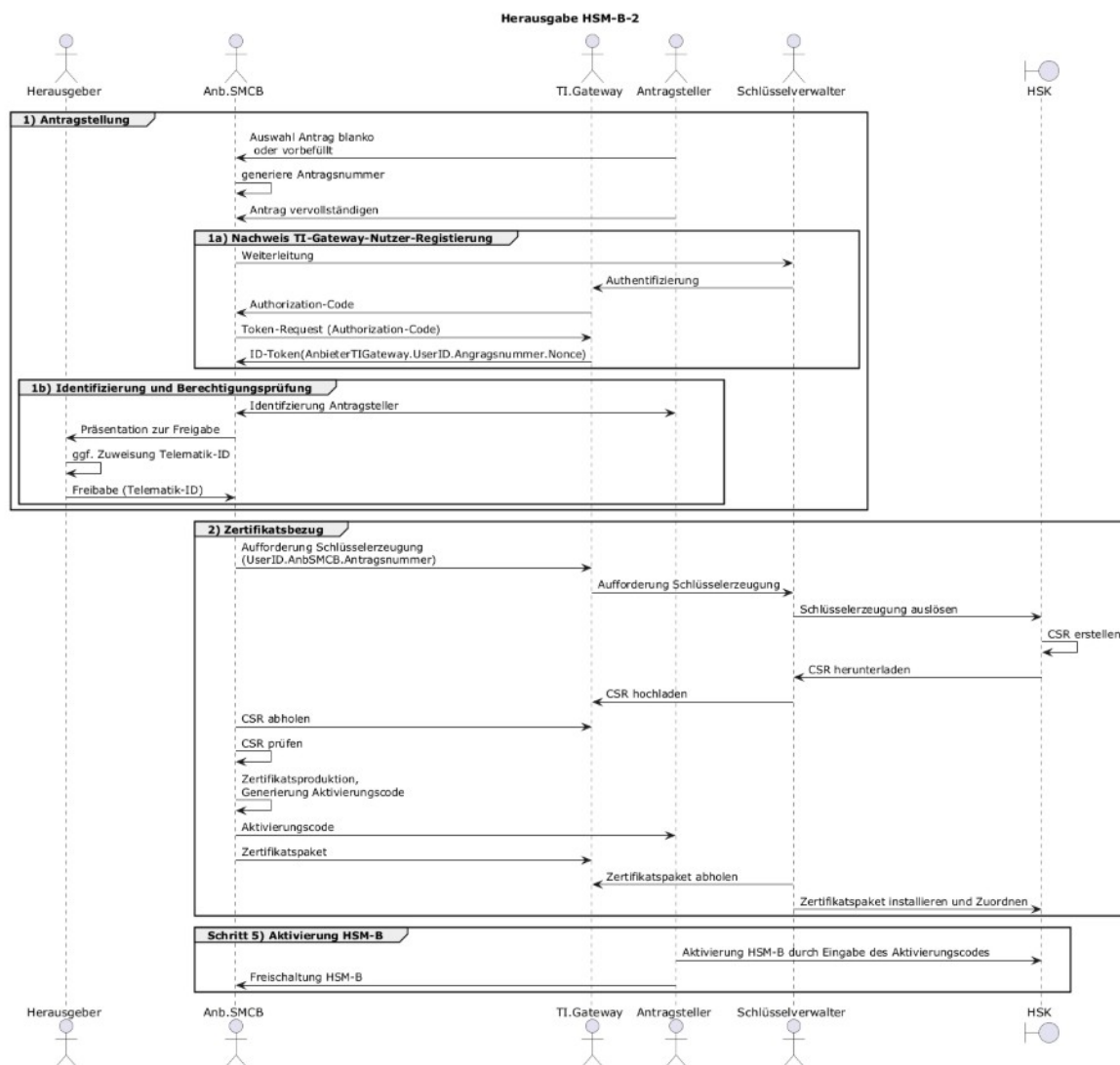


Abbildung 1: Übersicht HSM-B-Personalisierung HSK-Eigenbetrieb

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-Eigenbetriebs) bzw. Anbieter TI-Gateway (wenn das TI-Gateway genutzt wird) auswählt. Es werden alle zugelassenen Anbieter TI-Gateway Typ I und alle zugelassenen Anbieter HSK, deren Schlüsselverwalter bereits beim Anbieter SMC-B registriert wurden, gelistet. Die Anbieter Typ II/III müssen ihre Kunden darüber informieren, welchen Anbieter sie hier auswählen müssen. Der Anbieter SMC-B muss alle Schlüsselverwalter von zugelassenen Anbietern HSK registrieren, wenn diese sich dahingehend bei ihm melden (vgl. 3.2.2.1 HSK-Eigenbetrieb).

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 3.2.2 Vertrauensbeziehungen herstellen).

Nach der vollständigen Befüllung des Antrags sendet der Antragsteller diesen ab. Wurde ein TI-Gateway gewählt, Es erfolgt direkt die Verifikation des Antragstellerkontos beim Anbieter TI-Gateway (siehe 3.3.1.3 TI-Gateway: Verifikation des Antragstellerkontos beim TI-Gateway)

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-Basisystems erzeugt der Schlüsselverwalter ebenfalls unter Angabe der Antragsnummer alle notwendigen Schlüsselpaare und exportiert das signierte CSR-Paket (siehe 3.3.2.2 CSR-Erzeugung im HSK). Dieses Paket lädt der Schlüsselverwalter im Portal des Anbieter SMC-B hoch.

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, prüft die Rolle des zur UserID gehörenden Accounts, stellt fest dass die Rolle "Schlüsselverwalter" ist und benachrichtigt den Schlüsselverwalter unter Angabe von Antragsnummer und Anbieternamen. Der Schlüsselverwalter löst mit diesen Daten die Erstellung des CSR-Pakets im HSK aus (siehe 3.3.2.2 CSR-Erzeugung im HSK). Der Schlüsselverwalter lädt das CSR-Paket in das TI-Gateway hoch, von wo es der Anbieter SMC-B über den mTLS-Kanal abholt.

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~~ Der Anbieter SMC-B liefert das verschlüsselte Zertifikatspaket zusammen mit den Auftragsdaten (inkl. GatewayUserID) der Antragstellung (siehe 3.3.1.3 TI-Gateway: Verifikation des Antragstellerkontos beim TI-Gateway) an das Zugangsmodul des Anbieter TI-Gateway aus (über technische Schnittstelle mittels mTLS-Kanal).

Im Falle des HSK Eigenbetriebs holt der Schlüsselverwalter das Zertifikatspaket vom TI-Gateway ab.

4.1.1.2.3 Ermitteln von Schlüsselverwaltern

A_29015 - Optionale Rolle Schlüsselverwalter

Das TI-Gateway-Zugangsmodul KANN für ihre Nutzer die Rolle Schlüsselverwalter umsetzen. <=

A_29016 - Vorgaben für optionale Nutzerrolle Schlüsselverwalter

Das TI-Gateway-Zugangsmodul MUSS, wenn es die Nutzerrolle Schlüsselverwalter umsetzt, durchsetzen, dass ausschließlich Nutzer mit der Rolle Schlüsselverwalter

- Aufforderungen zur Schlüsselgenerierung erhalten,
- CSR-Pakete hochladen können,
- Zertifikatspakete herunterladen können und

Nutzer der Rolle Schlüsselverwaltung keine virtuellen Instanzen anlegen können. <=

A_29017 - CSR prüfung durch Zugangsmodule

Das TI-Gateway-Zugangsmodul MUSS vom Schlüsselverwalter hochgeladene CSR-Pakete entsprechend A_23758* prüfen und verwerfen, wenn die Prüfung nicht vollständig positiv durchlaufen wird.

A_25091-01 - Onboarding von

Schlüsselverwaltern https://gemspec.gematik.de/docs/gemF/gemF_Personalisierung_HS_M-B/latest/#A_25091

Der Anbieter SMC-B TI-Gateway MUSS, wenn er die Rolle Schlüsselverwalter umsetzt, durchsetzen, dass es allen ausschließlich von der gematik gemeldete Schlüsselverwalter die Rolle Schlüsselverwalter zugewiesen bekommen; der zugelassenen Anbieter HSK ermöglichen, eine Vertrauensbeziehung für den hinsichtlich Integrität geschützten Austausch von Schlüsselgenerierungsaufforderungen, CSR-Paketen und Zertifikatspaketen herzustellen und dabei geprüft wird, dass die Personen- und Kontaktdaten der Schlüsselverwalter genau mit den von der gematik gemeldeten Daten übereinstimmen. [<=]

4.1.1.4.1 Aufforderung zur Schlüsselerzeugung

A_25100 – Aufforderung zur Schlüsselerzeugung Anbieter

HSK https://gemspec.gematik.de/docs/gemF/gemF_Personalisierung_HSM-B/latest/#A_25100

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. [\leq]

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]

4.1.1.4.3 Zertifikatsproduktion

...

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 Schlüsselverwalter der ausgewählten Unternehmensgruppe zum Download des Zertifikatspakets auffordern.

4.1.3 Anforderungen an den Anbieter HSK**A_23635-01 - Registrierung der Schlüsselverwalter**

Der Anbieter Highspeed-Konnektor MUSS sicherstellen, dass Schlüsselverwalter (dedizierte Personen) sich für den Zugang zum ausgewählten TI-GatewayTrust-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-BTI-Gateway diese Personen im Betrieb zum Zwecke des Uploads von im HSK erzeugten CSR-Paketen und des Downloads von Zertifikatspaketen authentifizieren kann. [\leq]

Der Schlüsselverwalter führt dann Schlüsselerzeugung, Zertifikatsbeantragung und Zertifikatsbezug entsprechend den Vorgaben des Anbieters SMC-Bim HSK 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.

3 Änderungen in Steckbriefen

3.1 Änderungen in gemProdT_..._PTVx.y.z-n

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)
	[...]	