
C_12693_Anlage

Inhaltsverzeichnis

1 Änderungsbeschreibung.....2

1.1 Personalisierungsanpassung.....2

1.2 Entfernen der Optionalität des HSM.....2

2 Änderung in gemF_Highspeed-Konnektor.....3

2.1 Personalisierungsanpassung.....3

2.2 Entfernen der Optionalität des HSM.....3

1 Änderungsbeschreibung

1.1 Personalisierungsanpassung

Im Zuge der RSA2ECC Migration dürfen RSA2048 basierte Zertifikate auf HSMs nicht mehr personalisiert werden. Zum einen dürfen keine entsprechenden CSR-Requests mit solchen Zertifikaten an einen TSP gestellt werden. Zum anderen werden die TSPen CSRs, welche RSA2048 Zertifikate beinhalten entweder ablehnen oder nur die ECC-Anteile signieren.

Dies gilt ebenfalls für die virtuellen Geräteidentitäten von Highspeed-Konnektoren (AKA gSM-K).

Dieser Änderungseintrag befasst sich mit den notwendigen Änderungen, um gSM-K Identitäten weiterhin ohne Probleme auf HSMs der HSK personalisieren zu können.

1.2 Entfernen der Optionalität des HSM

Weiterhin werden in demselben Zuge noch verbleibende Überreste aus den Zeiten, als das HSM beim HSK optional war aus den Anforderungen entfernt.

2 Änderung in gemF_Highspeed-Konnektor

2.1 Personalisierungsanpassung

Neue Anforderung wird in Kapitel 5.2.1.3 nach TIP1-A_4503-04 eingefügt:

A_29018 - Personalisierung der Konnektoridentitäten im HSM

Für den HSK MÜSSEN genau die Geräteidentitäten mit genau den Schlüssel-/Zertifikatstypen personalisiert werden wie in TAB_KON_xxx vorgegeben. Bei der Personalisierung sind die entsprechenden Vorgaben aus gemSpec_Krypt zu erfüllen.

TAB_KON_xxx: Zuordnung der Konnektoridentitäten eines HSK-HSMs auf die kryptographischen Schlüssel-/Zertifikatstypen

Geräteidentität	zu Personalisierende Schlüsseltypen und darauf signierte Zertifikatstypen
ID.AK.AUT	ausschließlich 1x ECC NIST auf der Kurve P-256
ID.SAK.AUT	ausschließlich 1x ECC Brainpool auf der Kurve brainpoolP256r1
ID.SAK.AUTD_CV C	ausschließlich 1x ECC Brainpool auf der Kurve brainpoolP256r1
ID.HSK.ENC	ausschließlich 1x ECC Brainpool auf der Kurve brainpoolP256r1
ID.HSK.SIG	ausschließlich 1x ECC Brainpool auf der Kurve brainpoolP256r1

[<=]

Prüfverfahren: Anbietererklärung

AFO A_26378 entfällt, weil in o.g. A_29018 integriert

AFO A_22590 entfällt, weil in o.g. A_29018 integriert

2.2 Entfernen der Optionalität des HSM

Ersetzen des Freitext in Kapitel 4:

...

Die gSMC-K kann wird durch zertifizierte (z. B. [FIPS](#) 140-1 und 140-2 oder CC) HSM oder TPM-Lösungen ersetzt werden. Die Anforderungen an die Personalisierung der gSMC-K gelten analog für die Personalisierung des HSM.

...

TIP1-A_4701-06 wird durch TIP1-A_4701-07 ersetzt:

TIP1-A_4701-07 -TUC KON_035 „Zertifikatsdienst initialisieren“

In der Bootup-Phase MUSS der Konnektor den Zertifikatsdienst durch Aufruf des TUC_KON_035 „Zertifikatsdienst initialisieren“ initialisieren.

Tabelle 1: TAB_KON_772 TUC_KON_035 „Zertifikatsdienst initialisieren“

Element	Beschreibung
Name	TUC_KON_035 „Zertifikatsdienst initialisieren“
Beschreibung	Der TUC beschreibt den gesamten Ablauf der Initialisierung des TrustStore im Rahmen der betrieblichen Prozesse: Prüfung der Aktualität, Integrität und Authentizität der Einträge im TrustStore.
Auslöser	<ul style="list-style-type: none"> • Bootup des Konnektors
Vorbedingungen	keine
Eingangsdaten	keine
Komponenten	Konnektor
Ausgangsdaten	<ul style="list-style-type: none"> • Status der Initialisierung des TrustStore
Nachbedingunge n	Keine
Standardablauf	<p>Für den übergebenen Status der Initialisierung des TrustStore werden folgende Schritte durchgeführt:</p> <ol style="list-style-type: none"> 1. Aktualisierung der TSL mit Hashwertprüfung (A_17572* und TUC_KON_032). Wenn der HSK ein zentrales Modul zum TSL-Download besitzt, muss dieses die TSL beim Bootup des HSK aktualisieren und virtuelle Instanzen beziehen, wenn sie neu gestartet werden, die TSL von diesem zentralen Modul. 2. Falls im Zeitraum von CERT_BNETZA_VL_UPDATE_INTERVAL keine Aktualisierung der BNetza VL stattgefunden hat, aktualisiert der Konnektor die BNetza VL durch den Aufruf von TUC_KON_031 „BNetza-VL aktualisieren“. 3. Der Konnektor prüft die Gültigkeitsdauer der Zertifikate aller gesteckten Karten entsprechend TIP1-A_4691* 4. Der Konnektor liest von der gSMC-K bzw. vom HSM den öffentlichen Schlüssel des CVC-Root-Zertifikats und speichert diesen im TrustStore [gemSpec_gSMC-K_ObjSys#5.3.10].
Varianten/ Alternativen	Keine
Fehlerfälle	Keine
Nichtfunktionale Anforderungen	Keine
Zugehörige	Keine

Diagramme	
-----------	--

Tabelle 2: TAB_KON_605 Fehlercodes TUC_KON_035 „Zertifikatsdienst initialisieren“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können keine weiteren Fehlercodes auftreten.			

【<=,Konnektor Highspeed,Sich.techn. Eignung: Herstellererklärung, funkt. Eignung: Test Produkt/FA】

Ersetzen des Freitext in Kapitel 5.2.1.2 unter A_22336:

Wenn keine gSMC-K verwendet wird, muss dDer initiale Anker für den Vertrauensraum muss im sicheren Speicher des HSK oder im HSM personalisiert werden.

A_21885 wird durch A_21885-01 ersetzt:

A_21885-01 -Personalisierung des HSM mit Konnektoridentitäten durch Hersteller

Der Hersteller des Konnektors MUSS, wenn er ein HSM für die Speicherung der Konnektoridentitäten verwendet, das HSM mittels sicherer Prozesse und in seiner gesicherten Produktionsumgebung personalisieren.【<=,Konnektor Highspeed,Sich.techn. Eignung: Gutachten】

A_21886 wird durch A_21886-01 ersetzt:

A_21886-01 -Feste Kopplung von Konnektor und HSM

Der Konnektor MUSS, wenn ein HSM verwendet wird, fest kryptographisch mit dem HSM gekoppelt sein, sodass eine hinsichtlich Vertraulichkeit und Integrität geschützte, beidseitig authentifizierte Verbindung zwischen Konnektor und HSM besteht und ausschließlich der Konnektor die auf dem HSM gespeicherten Identitäten nutzen kann.【<=,Konnektor Highspeed,Sich.techn. Eignung: Produktgutachten】