1 Änderung in gemSpec_Kon

TUC_KON_035 wird folgendermaßen angepasst (Änderungen mit C_11676 werden zusammengeführt):

TIP1-A_4701-05 - 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	• Bootup des Konnektors
Vorbedingungen	keine
Eingangsdaten	keine
Komponenten	Konnektor
Ausgangsdaten	• Status der Initialisierung des TrustStore
Nachbedingungen	Keine
Standardablauf	Für den übergebenen Status der Initialisierung des TrustStore werden folgende Schritte durchgeführt: 1. Durch eine DNS-Anfrage an den DNS-Forwarder zur Auflösung der SRV-RR mit dem Bezeichner "_ocsp._tcp.<DOMAIN_SRVZONE_TI>„ erhält der Konnektor Adressen des http-Forwarders des VPN-Zugangsdienststandortes. 2. Aktualisierung der TSL mit Hashwertprüfung (A_17572* und TUC_KON_032) 3. Falls in den letzten 24 Stunden keine Aktualisierung der ~~TSL und~~ CRL im Truststore stattgefunden hat, aktualisiert der Konnektor ~~die TSL durch den Aufruf von TUC_KON_032 „TSL aktualisieren" und~~ die CRL durch den Aufruf von TUC_KON_040 „CRL aktualisieren". 4. 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".

	5. Der Konnektor prüft die Gültigkeitsdauer der Zertifikate aller gesteckten Karten (inkl. gSMC-K) mittels Aufruf von: für gSMC-K TUC_KON_033{checkSMCK; doInformClients=Ja; crypt = ECC} TUC_KON_033{checkSMCK; doInformClients=Ja; crypt = RSA} für jede gesteckte G2.0 Karte TUC_KON_033{cardSession; doInformClients=Ja; crypt = RSA} für jede gesteckte ab G2.1 Karte TUC_KON_033{cardSession; doInformClients=Ja; crypt = ECC} TUC_KON_033{cardSession; doInformClients=Ja; crypt = RSA} 6. Der Konnektor liest von der gSMC-K 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 Diagramme	Keine

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 PTV4, Konnektor PTV5, Konnektor PTV5Plus, Konnektor PTV6, Konnektor PTV4Plus, Konnektor eHealth, Sich.techn. Eignung: CC-Evaluierung, funkt. Eignung: Test Produkt/FA**]**

TIP1-A_4685-01 wird durch folgende AFO ersetzt:

TIP1-A_4685-02 - Vermeidung von Spitzenlasten bei TSL- und CRL-Download
Der Konnektor MUSS Spitzenlasten durch paralleles Herunterladen der TSL und der CRL vermeiden. Dazu MÜSSEN die im Einsatz befindlichen Konnektoren eines Herstellers ihre Download-Versuche gleichmäßig über den Tag verteilen. Die Festlegung des Downloadzeitpunktes MUSS unabhängig von dem Zeitpunkt des Bootup des Konnektors sein.
[<=, Konnektor Highspeed, Konnektor PTV4, Konnektor PTV5, Konnektor PTV5Plus, Konnektor PTV6, Konnektor PTV4Plus, Konnektor eHealth, funkt. Eignung: Herstellererklärung, funkt. Eignung: Test Produkt/FA**]**