1 Überblick

Das Feature "Laufzeitverlängerung gSMC-K" soll erweitert werden, damit ein Admin manuell neue gSMC-K-Zertifikate einbringen kann, auch nach Ablauf der ursprünglichen Zertifikate.
Es kann vorkommen, dass Konnektoren dauerhaft offline sind (z.B. Reserve insbesondere in Krankenhäusern). Für diese Konnektoren ist die skizzierte automatisierte Lösung zur Laufzeitverlängerung nur geeignet, wenn sie rechtzeitig vor Ablauf der Zertifikate online genommen werden.
Weiterhin kann es vorkommen, dass die automatische Zertifikatsaktualisierung fehlschlägt und ein Konnektor sich nicht mehr mit der TI verbinden kann.

Folgende Aktionen werden ermöglicht:

- Admin importiert alle Zertifikate manuell
- Manueller Aufruf von TUC_KON_410 (Trigger Administrator)
- Manueller Aufruf von TUC_KON_411 (Trigger Administrator)

Die Konnektor-Hersteller können in ihrer Rolle als berechtigte Zertifikatsantragsteller die notwendigen Zertifikate über das PMS-Tools des TSP-Komponenten (Arvato) abrufen.
Das gilt sowohl für die EE-Zertifikate, als auch für das C.CA_SAK.CS.
C.CA_SAK.CS kann darüber hinaus auch vom Internet Downloadpunkt der TSL bezogen werden.

2 Änderung in gemSpec_Kon

2.1 Es wird in Kapitel 3.1.1 "Erneuerung der Zertifikate der gSMC-K" neu aufgenommen, bzw. geändert:

A_21879 - Erneuerte Zertifikate der gSMC-K manuell importieren
Der Konnektor MUSS es dem Administrator ermöglichen, erneuerte Zertifikate C.NK.VPN, C.AK.AUT, C.SAK.AUT, C.SAK.AUTD_CVC und C.CA_SAK.CS manuell von lokaler Datenquelle einzuspielen.
Der Konnektor MUSS dies auch im kritischen Betriebszustand `EC_NK_Certificate_Expired` ermöglichen.**[<=]**

A_21749-01 - TUC_KON_410 „gSMC-K-Zertifikate aktualisieren"
Der Konnektor MUSS den technischen Use Case TUC_KON_410 „gSMC-K-Zertifikate aktualisieren" umsetzen.

Tabelle 1: TAB_KON_930 – TUC_KON_410 „Zertifikate aktualisieren"

Element	Beschreibung
Name	TUC_KON_410 "gSMC-K-Zertifikate aktualisieren"
Beschreibung	Dieser TUC bezieht neue gSMC-K-Zertifikate vom Downloadpunkt des TSP X.509 nonQES für Komponenten, oder diese werden vom Administrator übergeben.
Auslöser	A_21744, Administrator
Vorbedingungen	Automatische Aktualisierung: • MGM_LU_ONLINE=Enabled • Verbindung zum VPN-Konzentrator TI ist aufgebaut
Eingangsdaten	Manuelle Aktualisierung: • Zertifikate
Komponenten	Konnektor, TSP Komponenten
Ausgangsdaten	Keine

Standardablauf	Automatische Aktualisierung:
	1. Für jede verbaute gSMC-K wird die zip-Datei mit neuen Zertifikaten per HTTP vom Downloadpunkt TSP Komponenten bezogen ([gemSpec_X.509_TSP#A_21770]).
	2. Die zip-Dateien werden entpackt.
	3. Für jedes bezogene Zertifikat führt der Konnektor folgende Prüfungen durch:
	a. ICCSN des neuen und alten Zertifikats sind gleich
	b. Ablaufdatum des neuen Zertifikats liegt nach Ablaufdatum des alten Zertifikats
	c. Kryptografische Prüfung, dass öffentlicher Schlüssel zum privaten Schlüssel passt
	d. Neue Zertifikatsseriennummer ungleich alter Zertifikatsseriennummer
	e. Für C.NK.VPN-Zertifikat: OCSP-Abfrage gemäß GS-A_4657-03
	4. Erfolgreich geprüfte Zertifikate werden im sicheren Speicher abgelegt und zur Verwendung vorgemerkt.
	5. TUC_KON_256 {
	topic = „SMC_K/UPDATE/SUCCESS“;
	eventType = Op;
	severity = Info;
	parameters = „$Parameters“;
	doLog = true;
	doDisp = true }

Varianten/Alternativen	Manuelle Aktualisierung: 1. Die Files mit den neuen Zertifikaten werden vom Administrator in den Konnektor importiert. 2. Herstellerspezifisch, je nach Dateiformat

Fehlerfälle	(->1) Fehler beim Download:
	TUC_KON_256 {
	topic = „SMC_K/DOWNLOAD/ERROR“;
	eventType = Op;
	severity = Error;
	parameters = „$Parameters“;
	doLog = true;
	doDisp = true }
	(->3) Wenn eine der folgenden Prüfungen fehlschlägt, wird das bezogene Zertifikat verworfen und mit dem nächsten fortgesetzt:
	(-> 3a) ICCSN nicht gleich: Fail=Iccsn
	(-> 3b) Neues Ablaufdatum nicht später als altes Ablaufdatum: Fail=Date
	(-> 3c) Öffentlicher Schlüssel passt nicht zum privaten Schlüssel: Fail=Crypt
	(-> 3e) Zertifikat gesperrt oder unknown: Fail=Ocsp
	Automatische Aktualisierung: TUC_KON_256 {
	topic = „SMC_K/UPDATE/ERROR“;
	eventType = Op;
	severity = Error;
	parameters = „$Parameters“;
	doLog = true;
	doDisp = true }
	(->3) Wenn eine der folgenden Prüfungen fehlschlägt, wird das bezogene Zertifikat trotzdem zur Verwendung vorgemerkt:
	(-> 3d) Zertifikatsseriennummer identisch: Fail=Serial
	Warnung wird protokolliert

Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 2: Tab_Kon_931 Fehlercodes TUC_KON_410 „gSMC-K-Zertifikate aktualisieren“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
herstellerspezifisch			

[<=]

2.2 Es wird in Kapitel 4.3.8 "Re-Registrierung des Konnektors mit neuem NK-Zertifikat " neu aufgenommen, bzw. geändert

A_21745-01 - Re-Registrierung mit neuem NK-Zertifikat automatisch durchführen
Nach einer vollständigen erfolgreichen automatischen Zertifikatserneuerung über TUC_KON_410 MUSS der Konnektor eine Re-Registrierung mit dem neuen Zertifikat beim Registrierungsdienst des VPN-Zugangsdienstes durchführen. Solange nach Bezug eines neuen C.NK.VPN-Zertifikats noch keine erfolgreiche Re-Registrierung durchgeführt wurde, MUSS der Konnektor genau einmal täglich TUC_KON_411 aufrufen.
[<=]

A_21881 - Re-Registrierung mit neuem NK-Zertifikat manuell durchführen
Der Konnektor MUSS die manuelle Re-Registrierung mittels TUC_KON_411 durch den Administrator auch im kritischen Betriebszustand `EC_NK_Certificate_Expired` ermöglichen.**[<=]**

A_21758-01 - TUC_KON_411 „Konnektor mit neuem NK-Zertifikat registrieren"
Der Konnektor MUSS den technischen Use Case TUC_KON_411 "Konnektor mit neuem NK-Zertifikat registrieren" umsetzen.

Tabelle 3: TAB_KON_932 – TUC_KON_411 „Konnektor mit neuem NK-Zertifikat registrieren"

Element	Beschreibung
Name	TUC_KON_411 "Konnektor mit neuem NK-Zertifikat registrieren"
Beschreibung	Dieser TUC führt eine Deregistrierung mit dem alten und eine Neuregistrierung mit dem neuen NK-Zertifikat durch.
Auslöser	A_21745, Administrator
Vorbedingungen	Keine
Eingangsdaten	Keine
Komponenten	Konnektor, VPN-ZugD
Ausgangsdaten	Keine

Standardablauf	1. Der Konnektor ermittelt die URI des Registrierungsservers (MGM_ZGDP_REGSERVER) durch eine DNS-Anfrage nach dem SRV und TXT Resource Record „_regserver._tcp.<DNS_DOMAIN_VPN_ZUGD_INT>".
	2. Der Konnektor MUSS eine deRegisterKonnektorRequest-Struktur gemäß [gemSpec_VPN_ZugD] erstellen und mit den entsprechenden Parametern befüllen (aktuelles Datum/Uhrzeit, bei der letzten erfolgreichen Registrierung verwendetes C.NK.VPN-Zertifikat, MGM_ ZGDP_CONTRACTID).
	Der Konnektor MUSS die Request-Nachricht mittels einer verfügbaren SM-B (ID.HCI.OSIG) im Element deRegisterKonnektorRequest/Signature signieren. (MGM_ ZGDP_SMCB ist zu bevorzugen, es kann aber auch eine andere SM-B verwendet werden).
	3. Der Konnektor ruft unter Verwendung der erzeugten Request-Nachricht die in [gemSpec_VPN_ZugD#Tab_ZD_deregisterKonnektor] definierte Operation I_Registration_Service::deRegisterKonnektor mit der Zieladresse MGM_ZGDP_REGSERVER auf.
	Der Response der Operation wird verarbeitet:
	a. Setze MGM_TI_ACCESS_GRANTED auf
	- Enabled, wenn /RegistrationStatus = „Registriert"
	- Disabled, wenn /RegistrationStatus = „Nicht registriert"
	b. Persistiere diese Zustandsinformation zusammen mit dem Zeitpunkt
	c. Verteile das folgende Ereignis über TUC_KON_256: {
	topic = "MGM/TI_ACCESS_GRANTED";
	eventType = Op;
	severity = Info;
	parameters = „Active=$MGM_TI_ACCESS_GRANTED";
	doLog = true;
	doDisp=true }
	4. Der Konnektor MUSS eine registerKonnektorRequest-Struktur gemäß ProvisioningService.xsd [gemSpec_VPN_ZugD] erstellen und mit den entsprechenden Parametern befüllen (aktuelles Datum/Uhrzeit, erneuertes C.NK.VPN-Zertifikat, MGM_ ZGDP_CONTRACTID). Der Konnektor MUSS die Request-Nachricht mittels der ausgewählten SM-B (ID.HCI.OSIG) im Element registerKonnektorRequest/Signature signieren und das SM-B-Zertifikat im Element X509Data ablegen.

	5. Der Konnektor ruft unter Verwendung der erzeugten Request-Nachricht die in [gemSpec_VPN_ZugD#Tab_ZD_registerKonnektor] definierte Operation I_Registration_Service::registerKonnektor mit der Zieladresse MGM_ZGDP_REGSERVER auf.
	Der Response der Operation wird verarbeitet:
	a. Setze MGM_TI_ACCESS_GRANTED auf
	- Enabled, wenn /RegistrationStatus = „Registriert“
	- Disabled, wenn /RegistrationStatus = „Nicht registriert“
	b. Persistiere diese Zustandsinformation zusammen mit dem VPN:ContractStatus
	c. Verteile das folgende Ereignis über TUC_KON_256
	{
	topic = ”MGM/TI_ACCESS_GRANTED“;
	eventType = Op;
	severity = Info;
	parameters = „Active=$MGM_TI_ACCESS_GRANTED“;
	doLog = true;
	doDisp = true }

Varianten/Alternativen	Automatische Registrierung: (->5) Wenn der Konnektor nicht mit dem neuen C.NK.VPN-Zertifikat registriert werden konnte, dann muss sich der Konnektor, beginnend mit Schritt 4, erneut mit dem alten C.NK.VPN-Zertifikat registrieren. Manuelle Registrierung: (->2) Der Administrator soll die zu verwendende SM-B auswählen können.

Fehlerfälle	(→ 2,4) Es konnte keine freigeschaltete SM-B ausgewählt werden:
	Fail=No_Smcb
	(->4,5) Im Fehlerfall
	TUC_KON_256 {
	topic = „SMC_K/REGISTER/ERROR";
	eventType = Op;
	severity = Error;
	parameters = „$Parameters";
	doLog = true;
	doDisp = true }
	Die Registrierung soll herstellerspezifisch erneut mehrmals versucht werden.
	Bei allen Fehlerfällen, die zum Abbruch führen:
	TUC_KON_256 {
	topic = „SMC_K/REGISTER/ERROR";
	eventType = Op;
	severity = Error;
	parameters = „$Parameters";
	doLog = true;
	doDisp = true }

Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 4: Tab_Kon_933 Fehlercodes TUC_KON_411 „Zertifikate aktualisieren"

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
herstellerspezifisch			

[<=]

2.3 Es wird in Kapitel 3.3 "Betriebszustand " geändert

Tabelle 5: TAB_KON_504 Ausführungserlaubnis für Dienste in kritischen Fehlerzuständen

	EC_Software_Integrity_Check_Failed	EC_Random_Generator_Not_Reliable	EC_Security_Log_Not_Writable	EC_Time_Sync_Pending_Critical	EC_Time_Difference_Intolerable	EC_CRL_Out_Of_Date	EC_TSL_Out_Of_Date_Beyond_Grace_Period	EC_TSL_Trust_Anchor_Out_Of_Date	EC_Secure_Key_Store_Not_Available	EC_FW_Not_Valid_Status_Blocked	EC_NK_Certificate_Expired
Technische Use Cases (TUCs) der Basisdienste relevant für Fachanwendung und die Kommunikation mit Weiteren Anwendungen und SIS											
Zugriffsberechtigungsdienst											
TUC_KON_000 Prüfe Zugriffsberechtigung	-	x	x	x	x	x	x	x	x	x	x
Dienstverzeichnisdienst											
TUC_KON_041 Einbringen der Endpunktinformationen während der Bootup-Phase	-	-	-	x	x	x	x	x	x	x	x
Kartenterminaldienst											
TUC_KON_051 Mit Anwender über Kartenterminal interagieren	-	-	-	-	-	x	x	x	-	x	-
Kartendienst											
TUC_KON_005 Card-to-Card authentisieren	-	-	-	-	-	x	x	x	-	x	-
TUC_KON_006 Datenzugriffsaudit eGK schreiben	-	-	-	-	-	x	x	x	-	x	-

TUC_KON_018 eGK-Sperrung prüfen	-	-	-	-	-	x	x	x	-	x	-
TUC_KON_024 Karte zurücksetzen	-	-	-	-	-	x	x	x	-	x	-
TUC_kON_026 Liefere CardSession	-	-	-	-	-	x	-	x	-	-	-
TUC_KON_200 SendeAPDU	-	-	-	-	-	x	x	x	-	x	-
TUC_KON_202 LeseDatei	-	-	-	-	-	x	x	x	-	x	-
TUC_KON_203 SchreibeDatei	-	-	-	-	-	x	x	x	-	x	-
TUC_KON_209 LeseRecord	-	-	-	-	-	x	x	x	-	x	-
Systeminformationsdienst											
TUC_KON_256 Systemereignis absetzen	-	x	x	x	x	x	x	x	x	x	x
Verschlüsselungsdienst											
TUC_KON_072 Daten symmetrisch verschlüsseln	-	-	-	x	x	x	x	x	-	x	-
TUC_KON_073 Daten symmetrisch entschlüsseln	-	-	-	x	x	x	x	x	-	x	-
Zertifikatsdienst											
TUC_KON_034 Zertifikatsinformationen extrahieren	-	-	-	x	x	x	x	x	-	x	x
Protokollierungsdienst											
TUC_KON_271 Schreibe Protokolleintrag	-	x	x	x	x	x	x	x	x	x	x
TLS-Dienst											

TUC_KON_110 Kartenbasierte TLS-Verbindung aufbauen	-	-	-	-	-	-	-	-	-	-	-
Verbindung zum VPN-Konzentrator											
TUC_VPN-ZD_0001 „IPsec Tunnel TI aufbauen”	-	-	-	-	-	-	-	-	-	-	-
TUC_VPN-ZD_0002 „IPsec Tunnel SIS aufbauen”	-	-	-	-	-	-	-	-	-	-	-
Feature Laufzeitverlängerung gSMC-K)											
TUC_KON_410 „gSMC-K-Zertifikate aktualisieren (automatisch)	-	-	-	-	-	-	-	-	-	-	-
TUC_KON_410 „gSMC-K-Zertifikate aktualisieren (manuell)	-	-	-	-	-	-	-	-	-	-	x
TUC_KON_411 „Konnektor mit neuem NK-Zertifikat registrieren (automatisch)	-	-	-	-	-	-	-	-	-	-	-
TUC_KON_411 „Konnektor mit neuem NK-Zertifikat registrieren (manuell)	-	-	-	-	-	-	-	-	-	-	x
Operationen der Basisdienste											
Kartendienst											
VerifyPin	-	-	-	-	-	x	x	x	-	x	-
UnblockPin	-	-	-	-	-	x	x	x	-	x	-
ChangePin	-	-	-	-	-	x	x	x	-	x	-
GetPinStatus	-	-	-	-	-	x	x	x	-	x	-

Systeminformationsdienst											
Schnittstelle der Ereignissenke	-	x	x	x	x	x	x	x	x	x	x
GetCardTerminals	-	x	x	x	x	x	x	x	x	x	-
GetCards	-	x	x	x	x	x	x	x	x	x	-
GetResourceInformation	-	x	x	x	x	x	x	x	x	x	-
Subscribe	-	x	x	x	x	x	x	x	x	x	-
RenewSubscription	-	x	x	x	x	x	x	x	x	x	-
Unsubscribe	-	x	x	x	x	x	x	x	x	x	-
GetSubscription	-	x	x	x	x	x	x	x	x	x	-
Verschlüsselungsdienst											
EncryptDocument	-	-	-	-	-	x	x	x	-	x	-
DecryptDocument	-	-	-	-	-	x	x	x	-	x	-
Signaturdienst											
SignDocument	-	-	-	-	-	x	x	x	-	x	-
VerifyDocument	-	-	-	-	-	x	x	x	-	x	-
GetJobNumber	-	-	-	-	-	x	x	x	-	x	-
StopSignature	-	-	-	-	-	x	x	x	-	x	-
ActivateComfortSignature	-	-	-	-	-	x	x	x	-	x	-
DeactivateComfortSignature	-	-	-	-	-	x	x	x	-	x	-
GetSignatureMode	-	-	-	-	-	x	x	x	-	x	-
Authentifizierungsdienst											
ExternalAuthenticate	-	-	-	-	-	x	x	x	-	x	-

Zertifikatsdienst											
	ReadCardCertificate	-	-	-	-	-	x	x	x	x	x	-
	CheckCertificateExpiration	-	-	-	-	-	x	x	x	x	x	-
	VerifyCertificate	-	-	-	-	-	x	-	x	x	x	-
Zeitdienst												
	I_NTP_Time_Information	-	-	-	-	-	x	x	x	x	-	-
Konnektormanagement												
	Softwareaktualisierung	x	x	x	x	x	x	x	x	x	x	x
	Protokolleinsicht	x	x	x	x	x	x	x	x	x	x	x
	Werksreset	x	x	x	x	x	x	x	x	x	x	x
	Sonstiges	-	x	x	x	x	x	x	x	x	x	x

3 Änderungen in gemProdT_Kon_PTV5

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_Kon_PTV5]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 6: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

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