Inhaltsverzeichnis

1 Änderung in gemSpec_Kon

1.1 Kapitel 3.2.1 - Erneuerung der Zertifikate der gSMC-K

A_21744 wird durch A_21744-1 ersetzt:

- Der Konnektor soll eine Laufzeitverlängerung für alle gSM-K-basierten X.509-Zertifikate (C.NK.VPN, C.AK.AUT, C.SAK.AUT, C.SAK.AUTD_CVC, C.CA_SAK.CS) durchführen, unabhängig davon, ob sie auf der gSMC-K gespeichert oder im sicheren Speicher des Konnektors abgelegt sind.
- Für eine ECC-Laufzeitverlängerung ist es nicht ausreichend, nur das verwendete (d.h. am VPN-ZugD registrierte) C.NK.VPN Zertifikat zu verlängern, weil u.U. noch gar kein ECC-basiertes C.NK.VPN am VPN-ZugD registriert ist. Es müssen vielmehr alle vorhandenen Zertifikate versucht werden zu verlängern. So kann sichergestellt werden, dass immer ein nicht abgelaufenes ECC-basiertes C.NK.VPN-Zertifikat vorliegt.
- Hinweis: Diese Änderung bedeutet nicht, dass auch für jedes auf dem Konnektor vorhandene Zertifikat der Zertifikatserneuerungsprozess bis hin zur Erneuerung vollständig durchgeführt werden muss. Welche Zertifikate tatsächlich erneuert werden, wird dadurch festgelegt, welche erneuerten Zertifikate am Downloadpunkt zur Verfügung stehen.

A_21744-01 - Zertifikate regelmäßig erneuern
Der Konnektor MUSS die Zertifikate C.NK.VPN, C.AK.AUT, C.SAK.AUT, C.SAK.AUTD_CVC und C.CA_SAK.CS regelmäßig erneuern. Wenn im Konnektor kein C.NK.VPN-Zertifikat vorhanden ist, das länger als 180 Tage gültig ist,
~~Der Konnektor~~ MUSS er ~~180 Tage vor Ablauf des aktuell verwendeten C.NK.VPN-Zertifikats~~ den Zertifikatserneuerungsprozess anstoßen. Solange die Zertifikate noch nicht vollständig erfolgreich erneuert wurden, MUSS der Konnektor genau einmal täglich durch Aufruf von TUC_KON_410 neue Zertifikate beziehen.
[<=, Konnektor Option LZV, Konnektor PTV6, funkt. Eignung: Test Produkt/FA**]**

A_21745-02 - 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 einem erneuerten ~~dem~~

~~neuen~~ C.NK.VPN-Zertifikat beim Registrierungsdienst des VPN-Zugangsdienstes durchführen. Der Konnektor MUSS für die Re-Registrierung ein erneuertes ECC-Zertifikat verwenden, sofern vorhanden.
Solange nach einer vollständigen erfolgreichen automatischen Zertifikatserneuerung ~~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.
[<=, Konnektor Option LZV, Konnektor PTV6, funkt. Eignung: Test Produkt/FA**]**

A_21749-04 - 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: • Zertifikate am Downloadpunkt vorhanden • 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.
	a. Prüfung auf vollständiges Vorhandensein der Zertifikate (C.NK.VPN, C.AK.AUT, C.SAK.AUT, C.SAK.AUTD_CVC, C.CA_SAK.CS) für jedes bereitgestellte Kryptoverfahren (RSA und/oder ECC)
	i. Prüfung, dass C.SAK.AUTD_CVC dem Profil CHAT.51 entspricht ([gemSpec_PKI#Tab_PKI_918-01])
	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 im neuen Zertifikat zum privaten Schlüssel auf der gSMC-K passt
	d. Für C.NK.VPN-Zertifikat: OCSP-Abfrage (gemäß TUC_PKI_006)
	e. Für (C.NK.VPN, C.AK.AUT, C.SAK.AUT): Ermitteln des passenden CA-Zertifikats in der TSL und Prüfung der Signatur des neuen Zertifikats dagegen
	f. Für (C.SAK.AUTD_CVC, C.CA_SAK.CS):
	i. Prüfung der Signatur von C.SAK.AUTD_CVC gegen C.CA_SAK.CS
	ii. Ermittlung des passenden CVC-Root-Zertifikats im Truststore und Prüfung von C.CA_SAK.CS dagegen
	4. Wenn alle Zertifikate erfolgreich erneuert wurden: TUC_KON_256 {
	topic = „SMC_K/UPDATE/SUCCESS“;
	eventType = Op;
	severity = Info;
	parameters = „$Parameters“;
	doLog = true;
	doDisp = true }

Varianten/Alternativen	(->3d,e) Es kann auch eine vollständige Zertifikatsprüfung gemäß
	TUC_KON_037 „Zertifikat prüfen“{
	certificate = Zertifikatsreferenz;

	qualifiedCheck = not_required;
	offlineAllowNoCheck = true;
	validationMode = OCSP}
	
	erfolgen.
	
	Manuelle Aktualisierung:
	(->1) Die Files mit den neuen Zertifikaten werden vom Administrator in den Konnektor importiert.
	(->2) Herstellerspezifisch, je nach Dateiformat
	(->3d) Die OCSP-Abfrage erfolgt nur wenn
	• MGM_LU_ONLINE=Enabled und
	• Verbindung zum VPN-Konzentrator TI ist aufgebaut.

Fehlerfälle	(->1) Fehler beim Download:
	TUC_KON_256 {
	topic = „SMC_K/DOWNLOAD/ERROR“;
	eventType = Op;
	severity = Error;
	parameters = „$Parameters“;
	doLog = true;
	doDisp = true }
	
	(->2a) Wenn nicht alle erwarteten Zertifikate in der zip-Datei vorhanden sind oder ein Zertifikat nicht dekodiert werden kann: Fail=Incomplete
	Wenn eine der folgenden Prüfungen fehlschlägt, wird das bezogene Zertifikat verworfen und mit dem nächsten fortgesetzt:
	(->2a.i) Wenn C.SAK.AUTD_CVC nicht dem Profil CHAT.51 entspricht: Fail=Profile
	(->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
	(->3d) Zertifikat gesperrt oder unknown: Fail=Ocsp
	(->3e,f) Signaturprüfung fehlgeschlagen: Fail=Signature
	
	Bei automatischer Aktualisierung ab Schritt 2 bei jedem gefundenen Fehler:
	TUC_KON_256 {
	topic = „SMC_K/UPDATE/ERROR“;
	eventType = Op;
	severity = Error;
	parameters = „$Parameters“;
	doLog = true;
	doDisp = true }

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			

[<=, Konnektor Option LZV, Konnektor PTV6, funkt. Eignung: Test Produkt/FA**]**

1.2 4.3.7 Online-Anbindung verwalten

Die Anforderung A_23122 wird für Konnektor PTV6 entfernt.

A_23122 - Konfigurationsschalter für automatische Re-Registrierung (ECC-Migration)
Der Konnektor MUSS dem Administrator ermöglichen, die automatische Re-Registrierung mit dem ECC-NK-Zertifikat ein- und auszuschalten. Im Auslieferungszustand muss die automatische Re-Registrierung eingeschaltet sein.**[**<=, Konnektor PTV5, Konnektor PTV5Plus, Konnektor PTV6, funkt. Eignung: Test Produkt/FA**]**