
C_12406_Anlage

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	2
2 Änderung in gemSpec_Kon.....	3

1 Änderungsbeschreibung

Da Zertifikatspakete für die Laufzeitverlängerung ab 2027 nur ECC-Zertifikate und keine RSA-Zertifikate mehr enthalten sollen, muss ein dual-personalisierter Konnektor auch eine ECC-only-Laufzeitverlängerung durchführen können. Die Konnektoren müssen sich bei unterschiedlichen Laufzeiten von RSA- und ECC-Zertifikaten robust verhalten. RSA-only Aspekte der LZV werden in der Spezifikation nicht mehr benötigt.

Die Anzahl versuchter Laufzeitverlängerungen und Re-Registrierungen wird auf maximal viermal pro Tag erhöht.

Die Verwendung des laufzeitverlängerten AK.AUT-Zertifikats soll tagesgenau am Tag des Ablaufs des alten Zertifikats automatisch aktiviert werden.

2 Änderung in gemSpec_Kon

A_28504 -ECC-only Laufzeitverlängerung

Ein dual-personalisierter Konnektor MUSS auch eine ECC-only Laufzeitverlängerung durchführen können. [<=, „]

A_21744-03 -Zertifikate regelmäßig erneuern

Der Konnektor MUSS bei dual-personalisierten Konnektoren in folgenden Fällen mindestens einmal täglich und höchstens viermal täglich den Zertifikatserneuerungsprozess durch Aufruf von TUC_KON_410 auslösen:

Bei single-personalisierten Konnektoren

- wenn das C.NK.VPN (RSA) der gSMC-K in den nächsten 180 Tagen abläuft und noch kein Verlängerungszertifikat dafür im Konnektor vorhanden ist
- wenn das im Konnektor vorhandene Verlängerungszertifikat C.NK.VPN (RSA) in den nächsten 180 Tagen abläuft

Bei dual-personalisierten Konnektoren

- wenn das C.NK.VPN (RSA) oder das C.NK.VPN (ECC) der gSMC-K in den nächsten 180 Tagen abläuft und noch kein Verlängerungszertifikat für C.NK.VPN (ECC) im Konnektor vorhanden ist
- wenn das im Konnektor vorhandene Verlängerungszertifikat C.NK.VPN (ECC) in den nächsten 180 Tagen abläuft

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

A_21749-05 -TUC_KON_410 „gSMC-K-Zertifikate aktualisieren“

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

Tabelle1: 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: <ul style="list-style-type: none">• Zertifikate am Downloadpunkt vorhanden• MGM_LU_ONLINE=Enabled• Verbindung zum VPN-Konzentrator TI ist aufgebaut
Eingangsdaten	Manuelle Aktualisierung: <ul style="list-style-type: none">• Zertifikate

Komponenten	Konnektor, TSP Komponenten
Ausgangsdaten	Keine
Standardablauf	<p>Automatische Aktualisierung:</p> <ol style="list-style-type: none"> 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. <ol style="list-style-type: none"> a. Prüfung auf vollständiges Vorhandensein der Zertifikate (i und iii; ii und iii; i, ii und iii): <ol style="list-style-type: none"> i. C.NK.VPN, C.AK.AUT, C.SAK.AUT mit RSA-Kryptographie ii. C.NK.VPN, C.AK.AUT, C.SAK.AUT mit ECC-Kryptographie iii. C.SAK.AUTD_CVC, C.CA_SAK.CS b. 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: <ol style="list-style-type: none"> 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): <ol style="list-style-type: none"> 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 { <ol style="list-style-type: none"> topic = „SMC_K/UPDATE/SUCCESS“; eventType = Op; severity = Info; parameters = „\$Parameters“; doLog = true; doDisp = true }
Varianten/ Alternativen	<p>(->3d,e) Es kann auch eine vollständige Zertifikatsprüfung gemäß</p> <p>TUC_KON_037 „Zertifikat prüfen“{</p>

	<p>certificate = Zertifikatsreferenz; qualifiedCheck = not_required; offlineAllowNoCheck = true; validationMode = OCSP} erfolgen.</p> <p>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</p> <ul style="list-style-type: none"> • MGM_LU_ONLINE=Enabled und • Verbindung zum VPN-Konzentrator TI ist aufgebaut.
Fehlerfälle	<p>(->1) Fehler beim Download: TUC_KON_256 { topic = „SMC_K/DOWNLOAD/ERROR“; eventType = Op; severity = Error; parameters = „\$Parameters“; doLog = true; doDisp = true }</p> <p>(->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</p> <p>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 }</p>
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle2: 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】

A_21745-03 -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 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 noch keine erfolgreiche Re-Registrierung durchgeführt wurde, MUSS der Konnektor **genaumindestens** einmal täglich **und höchstens viermal täglich** TUC_KON_411 aufrufen.

【<=,Konnektor Option LZV, Konnektor PTV6,funkt. Eignung: Test Produkt/FA】