

---

## Inhaltsverzeichnis

---

|  |          |
|--|----------|
| <b>1 Änderung in gemSpec_Kon .....</b>                                 | <b>2</b> |
| <b>1.1 Kapitel 3.2.1 - Erneuerung der Zertifikate der gSMC-K .....</b> | <b>2</b> |
| <b>1.2 4.3.7 Online-Anbindung verwalten .....</b>                      | <b>7</b> |

---

## 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.

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.

Der Konnektor MUSS einmal täglich den Zertifikatserneuerungsprozess durch Aufruf von TUC\_KON\_410 auslösen, wenn

- die C.NK.VPN (RSA) oder C.NK.VPN (ECC) der gSMC-K in den nächsten 180 Tagen ablaufen

und

- für mindestens eines der C.NK.VPN Zertifikate der gSMC-K kein Verlängerungszertifikat installiert wurde.

[<=, 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: <ul style="list-style-type: none"><li>• Zertifikate am Downloadpunkt vorhanden</li><li>• MGM_LU_ONLINE=Enabled</li><li>• Verbindung zum VPN-Konzentrator TI ist aufgebaut</li></ul> |
| Eingangsdaten  | Manuelle Aktualisierung: <ul style="list-style-type: none"><li>• Zertifikate</li></ul>   |
| Komponenten    | Konnektor, TSP Komponenten   |
| Ausgangsdaten  | Keine  |

| Element        | Beschreibung   |
|----------------|--|
| Standardablauf | <p>Automatische Aktualisierung:</p> <ol style="list-style-type: none"> <li>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]).</li> <li>Die zip-Dateien werden entpackt. <ol style="list-style-type: none"> <li>Prüfung auf vollständiges Vorhandensein der Zertifikate(i und iii ; ii und iii ; i, ii und iii): <ol style="list-style-type: none"> <li>C.NK.VPN, C.AK.AUT, C.SAK.AUT mit RSA-Kryptographie</li> <li>C.NK.VPN, C.AK.AUT, C.SAK.AUT mit ECC-Kryptographie</li> <li>C.SAK.AUTD_CVC, C.CA_SAK.CS</li> </ol> </li> <li>Prüfung, dass C.SAK.AUTD_CVC dem Profil CHAT.51 entspricht ([gemSpec_PKI#Tab_PKI_918-01])</li> </ol> </li> <li>Für jedes bezogene Zertifikat führt der Konnektor folgende Prüfungen durch: <ol style="list-style-type: none"> <li>ICCSN des neuen und alten Zertifikats sind gleich</li> <li>Ablaufdatum des neuen Zertifikats liegt nach Ablaufdatum des alten Zertifikats</li> <li>Kryptografische Prüfung, dass öffentlicher Schlüssel im neuen Zertifikat zum privaten Schlüssel auf der gSMC-K passt</li> <li>Für C.NK.VPN-Zertifikat: OCSP-Abfrage (gemäß TUC_PKI_006)</li> <li>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</li> <li>Für (C.SAK.AUTD_CVC, C.CA_SAK.CS): <ol style="list-style-type: none"> <li>Prüfung der Signatur von C.SAK.AUTD_CVC gegen C.CA_SAK.CS</li> <li>Ermittlung des passenden CVC-Root-Zertifikats im Truststore und Prüfung von C.CA_SAK.CS dagegen</li> </ol> </li> </ol> </li> <li>Wenn alle Zertifikate erfolgreich erneuert wurden: <pre> TUC_KON_256 {   topic = „SMC_K/UPDATE/SUCCESS“;   eventType = Op;   severity = Info;   parameters = „\$Parameters“;   doLog = true;   doDisp = true } </pre> </li> </ol> |

| Element                | Beschreibung  |
|------------------------|---|
| Varianten/Alternativen | <p>(-&gt;3d,e) Es kann auch eine vollständige Zertifikatsprüfung gemäß</p> <pre>TUC_KON_037 „Zertifikat prüfen“{<br/>  certificate = Zertifikatsreferenz;<br/>  qualifiedCheck = not_required;<br/>  offlineAllowNoCheck = true;<br/>  validationMode = OCSP}</pre> <p>erfolgen.</p> <p>Manuelle Aktualisierung:<br/>(-&gt;1) Die Files mit den neuen Zertifikaten werden vom Administrator in den Konnektor importiert.<br/>(-&gt;2) Herstellerspezifisch, je nach Dateiformat<br/>(-&gt;3d) Die OCSP-Abfrage erfolgt nur wenn</p> <ul style="list-style-type: none"><li>• MGM_LU_ONLINE=Enabled und</li><li>• Verbindung zum VPN-Konzentrator TI ist aufgebaut.</li></ul> |

| Element                        | Beschreibung   |
|--------------------------------|--|
| Fehlerfälle                    | <p>(-&gt;1) Fehler beim Download:<br/> TUC_KON_256 {<br/>   topic = „SMC_K/DOWNLOAD/ERROR“;<br/>   eventType = Op;<br/>   severity = Error;<br/>   parameters = „\$Parameters“;<br/>   doLog = true;<br/>   doDisp = true }<br/> <br/> (-&gt;2a) Wenn nicht alle erwarteten Zertifikate in der zip-Datei vorhanden sind oder ein Zertifikat nicht dekodiert werden kann:<br/> Fail=Incomplete<br/> Wenn eine der folgenden Prüfungen fehlschlägt, wird das bezogene Zertifikat verworfen und mit dem nächsten fortgesetzt:<br/> (-&gt;2a.i) Wenn C.SAK.AUTD_CVC nicht dem Profil CHAT.51 entspricht: Fail=Profile<br/> (-&gt;3a) ICCSN nicht gleich: Fail=Iccsn<br/> (-&gt;3b) Neues Ablaufdatum nicht später als altes Ablaufdatum:<br/> Fail=Date<br/> (-&gt;3c) Öffentlicher Schlüssel passt nicht zum privaten Schlüssel:<br/> Fail=Crypt<br/> (-&gt;3d) Zertifikat gesperrt oder unknown: Fail=Ocsp<br/> (-&gt;3e,f) Signaturprüfung fehlgeschlagen: Fail=Signature<br/> <br/> Bei automatischer Aktualisierung ab Schritt 2 bei jedem gefundenen Fehler:<br/> TUC_KON_256 {<br/>   topic = „SMC_K/UPDATE/ERROR“;<br/>   eventType = Op;<br/>   severity = Error;<br/>   parameters = „\$Parameters“;<br/>   doLog = true;<br/>   doDisp = true }<br/> </p> |
| 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]