
C_12213_Anlage

Inhaltsverzeichnis

1 Änderung in gemSpec_Kon.....	2
---------------------------------------	----------

1 Änderung in gemSpec_Kon

A_23614-04 - SMC-B Prüfung bei Steckvorgang

Wenn der Konnektor einen Steckvorgang für eine SMC-B erkennt, MUSS der Konnektor - im Anschluss an die in TUC_KON_001 geforderten Aktionen - das ECC-Signaturzertifikat der SMC-B wie folgt prüfen. Wenn kein ECC-Zertifikat vorhanden ist, MUSS das RSA-Zertifikat geprüft werden:

- Wenn MGM_LU_ONLINE= "Enabled"

```
TUC_KON_037 „Zertifikat prüfen“{
  certificate = C.HCI.OSIG;
  qualifiedCheck = not_required;
  offlineAllowNoCheck = true;
  validationMode = OCSP;
  getOCSPResponses = includeRevocationInfo}
```

- Ist das Ergebnis der Statusprüfung "good", MUSS die OCSP-Response im Konnektor gespeichert werden.
Die maximale Dauer der Speicherung von SMC-B-Informationen im Konnektor ist in TIP1-A_4558 festgelegt.
- Ist das Ergebnis der Statusprüfung nicht "good" bzw. das Zertifikat ungültig MUSS der Konnektor ein Event auslösen: ("SMC-B Status not good")
TUC_KON_256 „Systemereignis absetzen“ {

```
  topic = „CERT/CARD/STATUS“;
  eventType = Op;
  severity = Warning;
  parameters = („CARD_TYPE=$Type,
    ICCSN=$ICCSN,
    CARD_HANDLE=$CardHandle,
    CardHolderName=$CardHolderName,
    CertName=$Name von certificate,
    ExpirationDate=$validity“,
```

```
  CARD_CERTSTATUS (Belegung gemäß TAB_KON_285= $CARD.CERTSTATUS))
```

```
  doLog=false;
  doDisp = true }
```

- Wenn MGM_LU_ONLINE= "Disabled",

```
TUC_KON_037 „Zertifikat prüfen“{
  certificate = C.HCI.OSIG;
  qualifiedCheck = not_required;
  offlineAllowNoCheck = true;
  validationMode = NONE }
```

Ist das Zertifikat ungültig MUSS der Konnektor ein Event auslösen: Systemereignis-senden ("SMC-B Status ungültig not available") TUC_KON_256 „Systemereignis absetzen“ {

```
  topic = „CERT/CARD/STATUS“;
  eventType = Op;
  severity = Warning;
```

```

parameters = („CARD_TYPE=$Type,
              ICCSN=$ICCSN,
              CARD_HANDLE=$CardHandle,
              CardHolderName=$CardHolderName,
              CertName=$Name von certificate,
              ExpirationDate=$validity“,
CARD_CERTSTATUS= (Belegung gemäß TAB_KON_285 "NotAvailable")
doLog=false;
doDisp = true }

```

Außerdem MUSS der Konnektor für das ECC-AUT-Zertifikat der SMC-B (C.HCI.AUT) den Zertifikatsablauf wie folgt prüfen. Wenn kein ECC-Zertifikat vorhanden ist, MUSS das RSA-Zertifikat geprüft werden:

```

TUC_KON_033 „Zertifikatsablauf prüfen“ {
    cardSession;
    doInformClients = true }

```

Tabelle 1 TAB_KON_285 Wertebereich Parameter CARD_CERTSTATUS

Bedingung	CARD_CERTSTATUS
MGM_LU_ONLINE= "Enabled"	
Zertifikat ungültig	Invalid
Zertifikat gültig, keine OCSP-Antwort	Inconclusive
Zertifikat gültig, OCSP liefert unknown	Unknown
Zertifikat gültig, OCSP liefert revoked	Revoked
MGM_LU_ONLINE= "Disabled"	
Zertifikat ungültig	Invalid

[<=, Konnektor Highspeed, Konnektor PTV6, Sich.techn. Eignung: CC-Evaluierung, funkt. Eignung: Test Produkt/FA, Sich.techn. Eignung: Prüfung durch CC-Prüfstelle]

A_23311-02 - HBA Prüfung bei Steckvorgang

Wenn der Konnektor einen Steckvorgang für einen HBAX erkennt, MUSS der Konnektor - im Anschluss an die in TUC_KON_001 geforderten Aktionen - das ECC-Signaturzertifikat des HBAX wie folgt prüfen. Wenn kein ECC-Zertifikat vorhanden ist, MUSS das RSA-Zertifikat geprüft werden:

- Wenn MGM_LU_ONLINE= "Enabled" und die Verbindung zum VPN-Konzentrator TI aufgebaut ist

```

TUC_KON_037 „Zertifikat prüfen“ {

```

```
certificate = C.HP.QES;
qualifiedCheck = required;
offlineAllowNoCheck = true;
validationMode = OCSP;
getOCSPResponses = includeRevocationInfo}
```

- Ist das Ergebnis der Statusprüfung "good", MUSS die OCSP-Response im Konnektor gespeichert werden.
Die maximale Dauer der Speicherung von HBA-Informationen im Konnektor ist in TIP1-A_4558 festgelegt.

- Ist das Ergebnis der Statusprüfung nicht "good" bzw. das Zertifikat ungültig MUSS der Konnektor ein Event auslösen: ("HBA Status not good")
TUC_KON_256 „Systemereignis absetzen“ {

```
topic = „CERT/CARD/STATUS“;
eventType = Op;
severity = Warning;
parameters = („CARD_TYPE=$Type,
ICCSN=$ICCSN,
CARD_HANDLE=$CardHandle,
CardHolderName=$CardHolderName,
CertName=$Name von certificate,
ExpirationDate=$validity“
```

```
CARD_CERTSTATUS= (Belegung gemäß TAB_KON_285 in A_23614* =
$CARD.CERTSTATUS))
```

```
doLog=false;
doDisp = true }
```

- Wenn MGM_LU_ONLINE= "Disabled",

```
TUC_KON_037 „Zertifikat prüfen“{
certificate = C.HP.QES;
qualifiedCheck = required;
offlineAllowNoCheck = true;
validationMode = NONE }
```

Ist das Zertifikat ungültig MUSS der Konnektor ein Event auslösen: ~~und~~
Systemereignis senden

```
("HBAungültig Status not available") TUC_KON_256 „Systemereignis absetzen“ {
```

```
topic = „CERT/CARD/STATUS“;
eventType = Op;
severity = Warning;
parameters = („CARD_TYPE=$Type,
ICCSN=$ICCSN,
CARD_HANDLE=$CardHandle,
CardHolderName=$CardHolderName,
CertName=$Name von certificate,
ExpirationDate=$validity“,
```

```
CARD_CERTSTATUS (Belegung gemäß TAB_KON_285 in A_23614* =
"NotAvailable")
```

```
doLog=false;
doDisp = true }
```

Außerdem MUSS der Konnektor für das ECC-AUT-Zertifikat des HBAX (C.HP.AUT) den

Zertifikatsablauf wie folgt prüfen. Wenn kein ECC-Zertifikat vorhanden ist, MUSS das RSA-Zertifikat geprüft werden:

TUC_KON_033 „Zertifikatsablauf prüfen“ {

 cardSession;

 doInformClients = true }

【<=, Konnektor Highspeed, Konnektor PTV5Plus, Konnektor PTV6, Sich.techn. Eignung: CC-Evaluierung, funkt. Eignung: Test Produkt/FA, Sich.techn. Eignung: Prüfung durch CC-Prüfstelle】