Änderungen in gemSpec_TSL

NEUES Unterkapitel in gemSpec_TSL:

6.3.1.3 „Automatisierbarer TSL-Download aus dem Internet"

Neben der Bereitstellung der TSL in der TI und im Internet zum manuellen Download wird die Möglichkeit geschaffen, im Internet die TSL nebst relevanter Prüf-Dateien zum automatisierbaren Download bereitzustellen. Damit haben Konnektoren die Möglichkeit, im Falle der Nichterreichbarkeit der TI durch eine fehlende oder ungültige TSL, eine gültige TSL aus dem Internet als Fallback-Mechanismus automatisiert einlesen und verifizieren zu können.

A_21175 - Automatisierbarer TSL-Download im Internet – nur per HTTP
Der TSL-Dienst MUSS zusätzliche Internet-Downloadpunkte für den automatisierbaren Download als Fallback-Verfahren für Konnektoren bereitstellen. Dazu MUSS der TSL-Dienst die Schnittstelle I_TSL_Download im Internet gemäß HTTP-Version 1.1 [RFC2616] implementieren.**[**<=**]**

A_21176 - Automatisierbarer TSL-Download im Internet - Gleicher Host wie CRL
Der TSL-Dienst MUSS für die zusätzliche in A_21175 definierte Schnittstelle den gleichen Server (Host) verwenden, an dem auch die CRL zum Download bereitgestellt wird (siehe [gemSpec_X.509_TSP#TIP1-A_4248]).**[**<=**]**

A_21177 - Automatisierbarer TSL-Download im Internet – Bereitstellung von 3 Dateien
Der TSL-Dienst MUSS auf den in A_21175 definierten zusätzlichen Internet-Downloadpunkten für den automatisierbaren TSL-Download je Umgebung jeweils drei verschiedene Dateien bereitstellen:

1. Die TSL-Datei mit der Datei-Endung „.xml", die auch innerhalb der TI bereitgestellt wird.
2. Eine Detached-Signatur-Datei mit der Datei-Endung „.sig" als Signatur der gesamten TSL-XML-Datei.
3. Eine OCSP-Antwort-Datei mit der Datei-Endung „.ocsp", zur Statusprüfung des für die Detached-Signatur unter Punkt 2. verwendeten TSL-Signers.

Der TSL-Dienst MUSS die TSL-Datei und die Detached-Signatur-Datei immer konsistent zueinander halten und gleichzeitig bereitstellen und aktualisieren.**[**<=**]**

A_21178 - Automatisierbarer TSL-Download im Internet – TSL-Datei
Der TSL-Dienst MUSS die TSL-Datei jeweils unmittelbar nach Bereitstellung in der TI, spätestens nach einer Stunde, auch auf dem zusätzlichen Internet-Downloadpunkte für den automatisierbaren Download (siehe A_21175) bereitstellen.**[**<=**]**

A_21179 - Automatisierbarer TSL-Download im Internet – Detached-Signatur-Datei

Der TSL-Dienst MUSS mit dem TSL-Signer, der auch die XML-Datei der TSL signiert hat, eine Detached-Signatur der gesamten TSL-Datei (*.xml) erzeugen und als Signatur-Datei mit der Endung „.sig" bereitstellen. Dabei MUSS der TSL-Dienst je Signaturtyp der TSL (RSA oder ECC) den jeweiligen aktuellen TSL-Signer (RSA oder ECC) verwenden. Die erzeugte Signatur muss als ASN1-Struktur mit den folgenden 3 Elementen bestehen:

1. **OID für den Signaturtyp**
   a. im Falle ECDSA:
   ```
   SEQUENCE {OBJECT IDENTIFIER ecdsaWithSHA256 (1 2 840 10045 4 3
   2)}
   ```
   b. im Falle RSASSA-PSS:
   ```
   SEQUENCE {OBJECT IDENTIFIER rsaPSS (1 2 840 113549 1 1 10)
       SEQUENCE {
         [0] {SEQUENCE {OBJECT IDENTIFIER sha-256 (2 16 840 1 101 3
   4 2 1)}}
         [1] {SEQUENCE {
                   OBJECT IDENTIFIER pkcs1-MGF (1 2 840 113549 1 1
   8)
                   SEQUENCE {OBJECT IDENTIFIER sha-256 (2 16 840 1
   101 3 4 2 1)}}}
         [2] {INTEGER 32}}}
   ```
2. **Kryptografische Signatur**
   a. im Falle ECDSA:
   eine ECDSA-Signatur nach [BSI-TR-03111#5.2.2.]
   b. im Falle RSASSA-PSS:
   eine RSASSA-PSS-Signatur nach [RFC-8017] (reiner ASN.1-kodierter Signaturwert – die OID ist schon in Teil 1.b aufgeführt)
3. **Signatur-Zertifikat (TSL-Signer)**

[<=]

Hinweis: Eine erweiterte Übersicht zum Aufbau der Detached Signatur Datei inkl. Beispiel finden sie unter

https://github.com/gematik/examples-TelematikInterfaces/tslService/detachedSignature.

A_21181 - Automatisierbarer TSL-Download im Internet – OCSP-Antwort-Datei
Der TSL-Dienst MUSS für den aktuell verwendeten TSL-Signer eine OCSP-Antwort erzeugen, stündlich erneuern und als Antwort-Datei mit der Endung „.ocsp" bereitstellen. Dabei MUSS der TSL-Dienst zum Signieren der OCSP-Antwort je Signaturtyp der TSL (RSA oder ECC) wie bei regulären OCSP-Antworten den jeweiligen aktuellen OCSP-Signer (RSA oder ECC) verwenden.**[<=]**

A_21182 - Automatisierbarer TSL-Download im Internet – URIs für TSL-Downloads
Der TSL-Dienst MUSS für die zusätzliche, in A_21175 definierte Schnittstelle die folgenden URIs realisieren (aufgeteilt je nach Umgebung):

Für die Produktivumgebung (PU):
TSL (RSA):

TSL-Datei: http://download.crl.ti-dienste.de/TSL-RSA/TSL.xml
Signatur-Datei: http://download.crl.ti-dienste.de/TSL-RSA/TSL.sig
OCSP-Antwort-Datei: http://download.crl.ti-dienste.de/TSL-RSA/TSL.ocsp

TSL (ECC-RSA):

TSL-Datei: http://download.crl.ti-dienste.de/TSL-ECC/ECC-RSA_TSL.xml
Signatur-Datei: http://download.crl.ti-dienste.de/TSL-ECC/ECC-RSA_TSL.sig
OCSP-Antwort-Datei: http://download.crl.ti-dienste.de/TSL-ECC/ECC-RSA_TSL.ocsp

Für die Referenzumgebung (RU):
TSL (RSA):

TSL Datei: http://download-testref.crl.ti-dienste.de/TSL-RSA-ref/TSL-ref.xml
Signatur Datei: http://download-testref.crl.ti-dienste.de/TSL-RSA-ref/TSL-ref.sig
OCSP-Antwort Datei: http://download-testref.crl.ti-dienste.de/TSL-RSA-ref/TSL-ref.ocsp

TSL (ECC-RSA):

TSL-Datei: http://download-testref.crl.ti-dienste.de/TSL-ECC-ref/ECC-RSA_TSL-ref.xml
Signatur-Datei: http://download-testref.crl.ti-dienste.de/TSL-ECC-ref/ECC-RSA_TSL-ref.sig
OCSP-Antwort-Datei: http://download-testref.crl.ti-dienste.de/TSL-ECC-ref/ECC-RSA_TSL-ref.ocsp

Für die Testumgebung (TU):
TSL (RSA):

TSL-Datei: http://download-testref.crl.ti-dienste.de/TSL-RSA-test/TSL-test.xml
Signatur-Datei: http://download-testref.crl.ti-dienste.de/TSL-RSA-test/TSL-test.sig
OCSP-Antwort-Datei: http://download-testref.crl.ti-dienste.de/TSL-RSA-test/TSL-test.ocsp

TSL (ECC-RSA):

TSL-Datei: http://download-testref.crl.ti-dienste.de/TSL-ECC-test/ECC-RSA_TSL-test.xml
Signatur-Datei: http://download-testref.crl.ti-dienste.de/TSL-ECC-test/ECC-RSA_TSL-test.sig
OCSP-Antwort-Datei: http://download-testref.crl.ti-dienste.de/TSL-ECC-test/ECC-RSA_TSL-test.ocsp

[<=]

TIP1-A_4076-01 - Erreichbarkeit OCSP-Responder
Der TSL-Dienst MUSS sicherstellen, dass der Validierungsdienst in Form eines OCSP-Responders über das Netzwerk der Telematikinfrastruktur wie auch im Internet erreichbar ist.
[<=]

Änderungen in gemSpec_Kon ==> (V5.x.y PTV5)

4.1.9 Zertifikatsdienst

TIP1-A_4693-02 - TUC_KON_032 „TSL aktualisieren"
Der Konnektor MUSS den technischen Use Case TUC_KON_032 „TSL aktualisieren" umsetzen.

Tabelle 1: TAB_KON_766 TUC_KON_032 „TSL aktualisieren"

Element	Beschreibung
Name	TUC_KON_032 „TSL aktualisieren"
Beschreibung	Dieser TUC prüft die Aktualität der TSL und initialisiert ggf. den TSL-spezifischen Bereich des TrustStores neu. Zusätzlich wird bei einem Wechsel des TI-Vertrauensankers das neue TSL-Signer-CA-Zertifikat in einem sicheren Speicherort im Konnektor hinterlegt. Im Fall der Veröffentlichung eines CVC-Root-CA-Zertifikats werden das CVC-Root-CA-Zertifikat und die Cross-CV-Zertifikate aus der TSL in den Truststore eingestellt.
Auslöser	• Aufruf durch andere TUCs
Vorbedingungen	• Ein gültiger TI-Vertrauensanker ist vorhanden • Das XML-Schema der TSL-Datei liegt vor
Eingangsdaten	• importedTSL – *optional* (TSL aus aus manuellem Import) (Optional) • baseTime – *optional; default: aktuelles Datum* (Referenzzeitpunkt) () • onlineMode [ENABLED | DISABLED] (Flag „MGM_LU_ONLINE" für Offline/Online-Modus) • hashTSL - *optional* (Hashwert-Datei der TSL im System; gilt nur für TSL(ECC-RSA))
Komponenten	Konnektor
Ausgangsdaten	• result (Status der Prüfung) • newHashTSL - *optional; verpflichtend für TSL(ECC-RSA)* (Hashwert-Datei der TSL im System; gilt nur für TSL(ECC-RSA))
Nachbedingungen	• Aktuelle TSL-Informationen inkl. des Vertrauensankers der BNetzA VL und sämtlicher CVC-Root-CA- und Cross-CV-Zertifikate liegen im Truststore vor. • Ein ggf. gelieferter neuer Vertrauensanker der TI ist in einem sicheren Speicherort gespeichert

Standardablauf	1. Der Konnektor prüft und aktualisiert ggf. die TSL durch Aufruf von TUC_PKI_001. Der Konnektor verwendet bei der Aktualisierung der TSL standardmäßig die Download-Punkte in der TI.
	Der durch den dort aufgerufenen TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates" benötigte aktuelle TI-Vertrauensanker befindet sich auf der gSMC-K in der Datei EF.C.TSL_CA_1 oder in einem sicheren Speicherort im Konnektor. Es ist dasjenige Zertifikat zu verwenden, welches zum Referenzzeitpunkt gültig ist und ab dem Aktivierungsdatum (`StatusStartingTime` des neuen TSL-Signer-CA-Zertifikats) aktiviert ist.
	2. Ggf. vorhandene CVC-Root-CA-Zertifikat und Cross-CV-Zertifikate werden genauso wie und zusammen mit den anderen CA-Zertifikaten aus der TSL extrahiert.
	3. Alle Informationen aus der TSL werden im TSL-spezifischen Bereich des TrustStores gespeichert
	4. Der Konnektor löst TUC_KON_256 {
	topic = „CERT/TSL/UPDATED";
	eventType = Op;
	severity = Info;
	doLog = true;
	doDisp = false }
	aus.
	5. CERT_CRL_DOWNLOAD_ADDRESS wird mit den CRL-Download-Adressen aus der TSL überschrieben.

Varianten/ Alternativen	(-> 1) Wenn der Download der TSL aus der TI fehlschlägt oder wenn der Konnektor im Fall*onlineMode* = ENABLED keine Verbindung zur TI hat, muss der Konnektor die TSL vom Download-Punkt im Internet (CERT_TSL_DOWNLOAD_ADDRESS_INTERNET) gemäß [gemSpec_TSL#A_21182] beziehen. Im Fall onlineMode = DISABLED wird abgebrochen. Wenn die Namensauflösung für CERT_TSL_DOWNLOAD_ADDRESS_INTERNET fehlschlägt, muss der Konnektor die TSL über CERT_TSL_IP_ADDRESS_INTERNET beziehen. Wenn keiner der vorigen Downloadversuche erfolgreich war, muss der Konnektor die TSL von der konfigurierbaren Adresse CERT_TSL_DOWNLOAD_ADDRESS_INTERNET_BU beziehen. Wenn die Namensauflösung für CERT_TSL_DOWNLOAD_ADDRESS_INTERNET_BU fehlschlägt, muss der Konnektor die TSL über CERT_TSL_IP_ADDRESS_INTERNET_BU beziehen. Für eine aus dem Internet bezogene TSL muss der Konnektor auch die vom TSL-Dienst gemäß [gemSpec_TSL#A_21182] bereitgestellte detached-Signatur der TSL herunterladen. Der Konnektor muss dann immer zunächst die detached-Signatur der TSL prüfen, einschließlich vollständiger Prüfung der Zertifikatskette bis zum TI-Vertrauensanker. Die

	kryptographische Prüfung der Signatur muss entsprechend A_21185 durchgeführt werden. Bezüglich der Prüfung des Sperrstatus des TSL-Signer-Zertifikats muss der Konnektor eines der folgenden Verfahren umsetzen: 1. Der Konnektor lädt die vorgefertigte OCSP-Response für das TSL-Signer Zertifikat aus dem Internet herunter (vgl. [gemSpec_TSL#A_21182]). Bei der Prüfung dieser OCSP-Response entfällt die Auswertung gegen die im System konfigurierte OCSP-Graceperiod. Der Konnektor prüft, dass die vorgefertigte OCSP-Response nicht älter als 61 Minuten ist. Die OCSP-Abfrage für das TSL-Signer Zertifikat in TUC_PKI_001, Schritt 4 entfällt. oder 2. Standard OCSP-Abfrage für das TSL-Signer Zertifikat in TUC_PKI_001, Schritt 4, jedoch unter Verwendung des im Internet verfügbaren OCSP-Responders entsprechend [gemSpec_TSL#TIP1-A_4076-01]. (→1) Wird die *importedTSL* manuell übergeben (in den Eingangsdaten), so wird diese statt des Downloads verwendet und an TUC_PKI_001 übergeben. Innerhalb der PKI TUCs findet dann kein Download der TSL statt. (→1) Falls *onlineMode* = DISABLED, kann der Sperrstatus des TSL-Signer-Zertifikats nicht überprüft werden. In diesem Fall wird die Aktivierung der *importedTSL* auch ohne Prüfung des Sperrstatus durchgeführt. (→1) Wird durch den von TUC_PKI_001 aufgerufenen TUC_PKI_013 „Import neuer Vertrauensanker" ein neuer TI-Vertrauensanker (ein neues TSL-Signer-CA-Zertifikat) in der *importedTSL* gefunden, so wird dieser, wie dort beschrieben, extrahiert und in einem sicheren Speicherort gespeichert. Vor Erreichen des Aktivierungsdatums werden die TSLs ausschließlich mit dem alten TSL-Signer-Zertifikat signiert. Ab dem Aktivierungsdatum werden die TSLs mit einem TSL-Signer-Zertifikat signiert, das von der neuen TSL-Signer-CA ausgestellt wurde.

Fehlerfälle	(→1) Tritt beim manuellen Import der Datei ein Fehler auf, wird TUC_KON_256 {
	topic = „CERT/TSL/IMPORT";
	eventType = Op;
	severity = Error;
	parameters = „$Fehlerbeschreibung";
	doLog = true;
	doDisp = false }
	ausgelöst. Fehlercode 4128.
	(→1) Tritt beim periodischen Update der TSL beim Aufruf des TUC_PKI_001 oder eines durch ihn aufgerufenen TUCs ein Fehler auf, geht der Konnektor in den Betriebszustand EC_TSL_Update_Not_Successful. Der Konnektor geht erst in den Betriebszustand EC_TSL_Update_Not_Successful, wenn weder der Downloadversuch aus der TI noch der

	Downloadversuch aus dem Internet erfolgreich war. Die vorhandenen TSL-Vertrauensanker werden weiter verwendet. Fehlercode 4127.
Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

Tabelle 2: TAB_KON_598 Fehlercodes TUC_KON_032 „TSL aktualisieren"

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4127	Security	Error	Import der TSL-Datei fehlgeschlagen
4128	Technical	Error	der manuelle Import der TSL-Datei schlägt fehl

[<=]

[neue Afo inkl. informativem Teil - motiviert durch Prüfung der "simplen" detached Signatur der TSL]

Für den Download der TSL über einen HTTP-Server im Internet wird zusätzlich zu der bereits mit einer XML-Signatur versehenen TSL eine detached-Signatur als separate Datei auf dem Download-Punkt zur Verfügung gestellt. Diese detached-Signatur umfasst die TSL in ihrerer Gänze, das heißt die TSL-XML-Datei wird inkl. der dort bereits enthaltenen XML-Signatur nochmal durch den TSL-Signer signiert. Ein Konnektor verwendet dann bei der Signaturprüfung einer TSL, die über das Internet bezogen wurde, die detached-Signatur für die Signaturprüfung. Hintergrund ist die aus Sicherheitsperspektive einfachere, im Sinne von sicherer prüfbare detached-Signatur. Das heißt, die TSL muss nicht als XML-File verarbeitet und die relativ komplexe XML-Signatur - die potentiell von einem Angreifer modifiziert sein könnte - nicht ausgewertet werden. Deshalb wird der Weg gewählt, der auch für die Signatur von X.509-Zertifikaten und OCSP-Responses verwendet wird.

A_21185 - Prüfung der detached Signatur der TSL bei Download aus dem Internet

Der Konnektor MUSS beim Download der TSL aus dem Internet ebenfalls deren detached-Signatur (vgl. [gemSpec_TSL#A_21182]) mit herunterladen und immer zunächst folgende Prüfungen durchführen:

1. Prüfung, dass die heruntergeladene detached-Signatur-Datei den folgenden Aufbau aufweist:
   Sequence aus drei Elementen:
   ```
   SEQUENCE {
     a
     b
     c}
   ```
   Mit *a*, *b* und *c* wie folgt:

a. OID für den Signaturtyp, bestehend aus
   i. im Falle ECDSA:
   ```
   SEQUENCE {OBJECT IDENTIFIER ecdsaWithSHA256 (1 2 840 10045 4
   3 2)}
   ```
   ii. im Falle RSASSA-PSS:
   ```
   SEQUENCE {OBJECT IDENTIFIER rsaPSS (1 2 840 113549 1 1 10)
       SEQUENCE {
         [0] {SEQUENCE {OBJECT IDENTIFIER sha-256 (2 16 840 1
   101 3 4 2 1)}}
         [1] {SEQUENCE {
                   OBJECT IDENTIFIER pkcs1-MGF (1 2 840 113549 1
   1 8)
                   SEQUENCE {OBJECT IDENTIFIER sha-256 (2 16 840
   1 101 3 4 2 1)}}}
         [2] {INTEGER 32}}}
   ```

b. Kryptographische Signatur
   i. im Falle ECDSA:
   einer ECDSA-Signatur nach [BSI-TR-03111#5.2.2.]
   ii. im Falle RSASSA-PSS:
   eine RSASSA-PSS-Signatur nach [RFC-8017] (reiner ASN.1-kodierter Signaturwert – die OID ist schon in Teil a.ii. aufgeführt)

c. Zertifikat des Signierenden (TSL-Signer)
   i. im Falle ECDSA:
   genau nur das ECC-TSL-Signer-Zertifikat
   ii. im Falle RSASSA-PSS:
   genau nur das RSA-TSL-Signer-Zertifikat

2. Prüfung der Signatur (1b) gegen das TSL-Signer-Zertifikat (1c).

Schlägt eine der Prüfungen fehl, MUSS der Import abgebrochen werden.
Ist die Prüfung erfolgreich, KANN die Prüfung der XML-Signatur der TSL im weiteren fachlichen Ablauf der TSL-Aktualisierung entfallen.
[<=]

Eine erweiterte Übersicht zum Aufbau der detached-Signatur-Datei inkl. Beispiel finden sie unter

https://github.com/gematik/examples-TelematikInterfaces/tslService/detachedSignature.

[neue Afo - motiviert durch Kommentar BSI-03 aus Kommentierung R3.1.3 HF3]

A_20750 - Hinweis auf Betreiber-Verantwortung bei automatischer TSL-Aktualisierung
Der Hersteller des Konnektors MUSS den Betreiber des Konnektors in geeigneter Weise (mindestens per Handbuch-Eintrag und per Hinweis innerhalb der UpdateInformation eines FirmwareUpdates am KSR) darüber informieren, dass im Fall, dass eine TSL-Aktualisierung innerhalb der TI fehlschlägt, automatisch versucht wird, eine TSL-Aktualisierung aus dem Internet vorzunehmen.**[<=]**

...

Kapitel 4.1.9.6 Betriebliche Aspekte

[Afo A_20469 kommt mit HF3:C_10202 rein. Muss durch -01 aktualisiert werden]

A_20469-01 - Automatisierte Etablierung des ECC-RSA-Vertrauensraums (ECC-Migration)
In der BootUp-Phase MUSS ein Konnektor, der den RSA-Vertrauensraum (RSA) verwendet, überprüfen, ob die TSL(ECC-RSA) und die entsprechenden TSL-Signer-CA Cross-Zertifikate sowie TSL-Signer-CA-Zertifikate verfügbar sind und MUSS sie im positiven Fall automatisiert herunterladen, nach erfolgreicher Prüfung verwenden und dadurch den ECC-Vertrauensraum (ECC-RSA) etablieren.
Der Konnektor MUSS hierzu die Downloadpunkte, die mit A_17680-02 in [gemSpec_TSL#6.3.1.2] definiert sind, verwenden. Dabei MUSS der Konnektor zunächst die Downloadpunkte innerhalb der TI verwenden. Wenn der Download aus der TI fehlschlägt, MUSS der Konnektor einen der definierten Downloadpunkte im Internet verwenden.
Falls beim Wechsel auf den ECC-RSA Vertrauensraum ein Fehler auftritt, MUSS der Konnektor weiterhin den RSA-Vertrauensraum (RSA) verwenden.

[<=]

...

[nach Afo TIP1-A_4705 folgende neue Afo einfügen und Text]:

Auch im Fall des automatischen Imports der TSL muss dies im kritischen Betriebszustand `EC_TSL_Out_Of_Date_Beyond_Grace_Period` unterstützt werden.

A_20536 - TSL im kritischen Betriebszustand
Der Konnektor MUSS den automatischen Import einer TSL auch ermöglichen, wenn er sich im kritischen Betriebszustand `EC_TSL_Out_Of_Date_Beyond_Grace_Period` befindet. **[<=]**

[motiviert durch Kommentierung GKV-SV_04. bewusst keine Abwandlung der Vorbedingung von TUC_KON_032 (gültige TSL im System)]

A_20748 - Automatischer TSL Download im kritischen Zustand
Falls der Konnektor im kritischen Betriebszustand EC_TSL_Out_Of_Date_Beyond_Grace_Period ist, und falls *onlineMode* = ENABLED ist, MUSS der Konnektor periodisch und in der BootUp Phase die TSL aktualisieren.**[<=]**

[geänderte Afo TIP1-A_4702-03 ; hier ist ggf ein Merge mit TIP1-A_4020-02 notwendig, die mit R3.1.3 HF 3 zur Freigabe geführt wird!!)]:

TIP1-A_4702-03 - Konfigurierbarkeit des Zertifikatsdienstes
Der Administrator MUSS die in TAB_KON_606 aufgelisteten Parameter über die Managementschnittstelle konfigurieren und die in TAB_KON_733 aufgelisteten Parameter ausschließlich einsehen können.

Tabelle 3: TAB_KON_606 Konfiguration des Zertifikatsdienstes

ReferenzID	Belegung	Bedeutung
CERT_TSL_DEFAULT_GRACE_PERIOD_DAYS	X Tage	Default Grace Period TSL in Tagen Gibt an, wie viele Tage der Konnektor mit einer zeitlich abgelaufenen TSL weiter betrieben werden kann. Der Wert MUSS zwischen 1 und 30 Tagen liegen. Default-Wert = 30 Tage *Hinweis: Vor dem zeitlichen Ablauf einer TSL wird mit ausreichendem Vorlauf eine neue TSL verteilt. Sollte die TSL dennoch ablaufen und der Konfigurationswert überschritten werden, kann eine neue TSL immer noch lokal geladen werden (TIP1-A_4705 „TSL manuell importieren").*
CERT_OCSP_DEFAULT_GRACE_PERIOD_NONQES	X Minuten	Default Grace Period OCSP für nonQES in Minuten. Der Wert MUSS zwischen 0 und 20 Minuten liegen. Default-Wert = 10 Minuten
CERT_OCSP_TIMEOUT_NONQES	X Sekunden	Timeout für OCSP-Abfragen bei der Prüfung von nonQES-Zertifikaten. Der Wert MUSS zwischen 1 und 120 Sekunden liegen. Default-Wert = 10 Sekunden
CERT_OCSP_TIMEOUT_QES	X Sekunden	Timeout für OCSP-Abfragen bei der Prüfung von QES-Zertifikaten. Der Wert muss zwischen 1 und 120 Sekunden liegen. Default-Wert = 10 Sekunden
CERT_EXPIRATION_WARN_DAYS	X Tag(e)	Warnung X Tage vor Ablauf von Zertifikaten im Managementinterface und per Ereignis. Der Wert muss zwischen 0 und 180 Tagen (0=keine Warnung) liegen. Default-Wert = 90 Tage

CERT_EXPIRATION_ CARD_CHECK_DAYS	X Tag(e)	Alle X Tage wird der Ablauf aller gesteckten Karten überprüft. Der Wert muss zwischen 0 und 365 liegen (0=kein Check). Default-Wert = 1 Tag
CERT_IMPORTED_ CA_LIST	Liste von manuell importierten CA-Zertifikaten	Der Administrator MUSS CA-Zertifikate importieren, anzeigen und löschen können. Der Konnektor DARF CA-Zertifikate zur Ableitung von QES-Zertifikaten NICHT importieren. Default-Wert = leere Liste
CERT_BNETZA_VL_ UPDATE_INTERVAL	X Stunden	Intervall, in dem die BNetzA VL auf Aktualität geprüft werden muss. Der Wert MUSS zwischen 1 Stunde und 168 Stunden (7 Tage) liegen. Default-Wert = 24 Stunden
CERT_TSL_DOWNLOAD_ADDRESS_INTERNET_BU	1 URI	Konfigurierbare Backup Adresse der TSL im Internet
CERT_ECC_RSA_TSL_SIGNER_CA_CERTIFICATE_INTERNET_BU	1 URI	Konfigurierbare Backup Adresse der TSL-Signer-CA Zertifikate im Internet (gemäß gemSpec_TSL#A_17680-02 und gemSpec_PKI#(5.15.3 X.509 Zertifikatsprofil der TSL-Signer-CA)
CERT_ECC_RSA_TSL_SIGNER_CA_CROSS_CERTIFICATE_INTERNET_BU	1 URI	Konfigurierbare Backup Adresse der TSL-Signer-CA-Cross Zertifikate im Internet (gemäß gemSpec_TSL#A_17680-02 und gemSpec_PKI#(5.15.3 X.509 Zertifikatsprofil der TSL-Signer-CA)
CERT_TSL_IP_ADDRESS_INTERNET_BU	1 URI	Konfigurierbare Backup Adresse der TSL im Internet (enthält IP-Adresse des Hosts statt FQDN). Wird verwendet, falls Auflösen der FQDN mittels DNS bei CERT_TSL_DOWNLOAD_ADDRESS_INTERNET_BU fehlschlägt.

Tabelle 4: TAB_KON_733 Einsehbare Konfigurationsparameter des Zertifikatsdienstes

ReferenzID	Belegung	Bedeutung
CERT_CRL_DOWNLOAD_ADDRESS	2 URIs	Download-Adressen für die CRL
CERT_OCSP_FORWARDER_ADDRESS	2 FQDNs	Adressen der OCSP-Forwarder (HTTPS-Proxy) beim Zugangsdienstprovider Der Administrator muss in geeigneter Weise einen Test auslösen können, ob einer der Server per ICMP-Echo (ping) erreichbar ist und ob ein (beliebiger) OCSP-Request zu einer erhaltenen OCSP-Antwort führt.
CERT_OCSP_FORWARDER_PORT	TCP-Port	TCP-Port des OCSP-Forwarders (HTTPS-Proxy) beim Zugangsdienstprovider
CERT_TSL_DOWNLOAD_ADDRESS_INTERNET	1 URI	Adresse der TSL im Internet gemäß gemSpec_TSL
CERT_ECC_RSA_TSL_SIGNER_CA_CERTIFICATE_INTERNET	URIs	Adresse der TSL-Signer-CA Zertifikate im Internet (gemäß gemSpec_TSL#A_17680-02 und gemSpec_PKI#(5.15.3 X.509 Zertifikatsprofil der TSL-Signer-CA)
CERT_ECC_RSA_TSL_SIGNER_CA_CROSS_CERTIFICATE_INTERNET	URIs	Adresse der TSL-Signer-CA-Cross Zertifikate im Internet (gemäß gemSpec_TSL#A_17680-02 und gemSpec_PKI#(5.15.3 X.509 Zertifikatsprofil der TSL-Signer-CA)
CERT_TSL_IP_ADDRESS_INTERNET	1 URI	Adresse der TSL im Internet gemäß gemSpec_TSL (enthält IP-Adresse des Hosts statt FQDN). Wird verwendet, falls Auflösen der FQDN mittels DNS bei CERT_TSL_DOWNLOAD_ADDRESS_INTERNET fehlschlägt.

[<=]

4.2.1 Anbindung LAN/WAN

TIP1-A_4736-02 - Kommunikation mit dem Internet (via IAG)
Der Konnektor MUSS sicherstellen, dass eingehende IP-Pakete von der Kommunikation mit dem Internet mit der Empfängeradresse ungleich (ANLW_LAN_IP_ADDRESS oder aus einem der Netzwerksegmente in ANLW_LEKTR_INTRANET_ROUTES wenn ANLW_WAN_ADAPTER_MODUS=DISABLED) oder (ANLW_WAN_IP_ADDRESS wenn ANLW_WAN_ADAPTER_MODUS=ENABLED) verworfen werden.
Der Konnektor MUSS sicherstellen, dass ausgehende IP-Pakete für die Kommunikation mit dem Internet mit der Absenderadresse ungleich (ANLW_LAN_IP_ADDRESS oder aus einem der Netzwerksegmente in ANLW_LEKTR_INTRANET_ROUTES wenn ANLW_WAN_ADAPTER_MODUS=DISABLED) oder (ANLW_WAN_IP_ADDRESS wenn ANLW_WAN_ADAPTER_MODUS=ENABLED) verworfen werden.
Der Konnektor MUSS die Kommunikation mit Systemen des Netzwerksegments Internet (via IAG) für folgende Fälle unterstützen:

- [19] vom Konnektor kommend zu den folgenden Systemen für das Protokoll IPsec
  - VPN_KONZENTRATOR_TI_IP_ADDRESS
  - VPN_KONZENTRATOR_SIS_IP_ADDRESS
- [19] vom Konnektor kommend zu den folgenden Systemen für HTTP und HTTPS
  - CERT_CRL_DOWNLOAD_ADDRESS
  - TSL-Download-Punkt des TSL-Dienstes
  - hash&URL-Server
  - Registrierungsserver
  - Remote-Managementserver
  - DNS_ROOT_ANCHOR_URL (benötigte IP-Adressen um den DNSSEC Trust Anchor im Namensraum Internet zu verifizieren)
- [19] vom Konnektor kommend zu den folgenden Systemen für das Protokoll DNS
  - beliebige Hosts

Der Konnektor MUSS insbesondere die Kommunikation an seinen Außenschnittstellen mit Internet (via IAG) für folgende Fälle blockieren oder umleiten:

- [20a] blockieren, wenn (ANLW_INTERNET_MODUS=KEINER oder MGM_LU_ONLINE=Disabled) von „Aktive Komponenten“ kommend
- [20b] mittels ICMP Redirect gemäß [RFC792] zum Default Gateway umleiten, wenn die Zieladresse des IP-Pakets nicht innerhalb der Adressbereiche (NET_TI_ZENTRAL, NET_TI_OFFENE_FD, NET_TI_GESICHERTE_FD und ANLW_AKTIVE_BESTANDSNETZE) ist und ANLW_INTERNET_MODUS=IAG und von „Aktive Komponenten“ kommend.
- [21] blockieren, wenn von IAG kommend in Richtung Konnektor (und die dahinterliegenden „Aktive Komponenten“)

[<=]

Änderungen in gemProdT_Kon_PTV4 und gemProdT_Kon_PTV5 und gemProdT_TSL-Dienst

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle der Originaldokumentr [gemProdT_Kon_PTV4] , [gemProdT_Kon_PTV5] und [gemProdT_TSL_Dienst] Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehen.

Tabelle 5: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_4693-02	TUC_KON_032 „TSL aktualisieren”	gemSpec_Kon (PTV4 + PTV5)
~~TIP1-A_4693~~	~~TUC_KON_032 „TSL aktualisieren”~~	gemSpec_Kon (PTV4 + PTV5)
A_20750	Hinweis auf Betreiber-Verantwortung bei automatischer TSL-Aktualisierung	gemSpec_Kon (PTV4 + PTV5)
A_20469-01	Automatisierte Etablierung des ECC-RSA-Vertrauensraums (ECC-Migration)	gemSpec_Kon (PTV4 + PTV5)
~~A_20469~~	~~Automatisierte Etablierung des ECC-RSA-Vertrauensraums (ECC-Migration)~~	gemSpec_Kon (PTV4 + PTV5)
A_20536	TSL im kritischen Betriebszustand	gemSpec_Kon (PTV4 + PTV5)
A_20748	Automatischer TSL Download im kritischen Zustand	gemSpec_Kon (PTV4 + PTV5)
TIP1-A_4702-03	Konfigurierbarkeit des Zertifikatsdienstes	gemSpec_Kon (PTV4 + PTV5)
~~TIP1-A_4702-02~~	~~Konfigurierbarkeit des Zertifikatsdienstes~~	gemSpec_Kon (PTV4 + PTV5)
TIP1-A_4736-02	Kommunikation mit dem Internet (via IAG)	gemSpec_Kon (PTV4 + PTV5)

~~TIP1-A_4736~~	~~Kommunikation mit dem Internet (via IAG)~~	gemSpec_Kon (PTV4 + PTV5)
A_21185	Prüfung der detached Signatur der TSL bei Download aus dem Internet	gemSpec_Kon (PTV4 + PTV5)

Tabelle 6: Anforderungen zur funktionalen Eignung "CC-Evaluierung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_4693-02	TUC_KON_032 „TSL aktualisieren”	gemSpec_Kon (PTV4 + PTV5)
~~TIP1-A_4693~~	~~TUC_KON_032 „TSL aktualisieren”~~	gemSpec_Kon (PTV4 + PTV5)
TIP1-A_4736-02	Kommunikation mit dem Internet (via IAG)	gemSpec_Kon (PTV4 + PTV5)
~~TIP1-A_4736~~	~~Kommunikation mit dem Internet (via IAG)~~	gemSpec_Kon (PTV4 + PTV5)
A_21185	Prüfung der detached Signatur der TSL bei Download aus dem Internet	gemSpec_Kon (PTV4 + PTV5)