

---

## **C\_12791\_Anlage: Übergeordnete PKI-Ergänzungen: Prüfung von TI-Zertifikaten im Internet**

---

# **Inhaltsverzeichnis**

|          |                                                                                               |          |
|----------|-----------------------------------------------------------------------------------------------|----------|
| <b>1</b> | <b>Änderungsbeschreibung.....</b>                                                             | <b>2</b> |
| <b>2</b> | <b>Änderung in gemSpec_PKI.....</b>                                                           | <b>3</b> |
| 2.1      | NEUES Unterkapitel 8.2.6 - Besonderheiten bei der TSL-Prüfung im Internet.....                | 3        |
| 2.2      | NEUES Unterkapitel 8.3.5 - Vorgaben zur Prüfung von TI-Zertifikaten (nonQES) im Internet..... | 5        |
| 2.3      | NEUES Unterkapitel 8.5.3 - Vorgaben zur Prüfung von QES-Zertifikaten der TI im Internet.....  | 6        |
| <b>3</b> | <b>Änderung in gemSpec_Krypt.....</b>                                                         | <b>8</b> |
| <b>4</b> | <b>Änderungen in Steckbriefen.....</b>                                                        | <b>9</b> |
| 4.1      | Änderungen in gemProdT_...PTVx.y.z-n.....                                                     | 9        |

---

## 1 Änderungsbeschreibung

---

Das Kapitel 8.3 der gemSpec\_PKI beschreibt die Vorgaben, Schritte und Anforderungen, die für die Prüfung von X.509-Zertifikaten der TI-PKI notwendig sind. Da die TI (1.0) in der Vergangenheit ein geschlossenes Netz darstellte, wurden diese vornehmlich ohne Berücksichtigung von Prüfungen über das Internet betrachtet.

Neuere Anwendungen in der TI und vor allem TI 2.0-Anwendungen haben nur begrenzten oder keinen Zugang zu TI 1.0 Systemen mehr. Daher müssen sie zur Prüfung von TI-PKI\_Zertifikaten Komponenten im Internet (TSL-Downloadpunkte, OCSP-Responder) verwenden. Die Rahmenbedingungen zur Nutzung dieser Internet-Komponenten zur Prüfung von TI-Zertifikaten werden in diesem Änderungseintrag beschrieben und übergeordnete, strukturierte Vorgaben definiert.

Daher wird im Unterkapitel 8.3.5 ergänzend auf Prüf-Methodiken für nonQES-Zertifikate der TI-PKI eingegangen, die sich von der Prüfung über die TI (1.0) unterscheiden. Zusätzlich dazu werden entsprechende Unterkapitel 8.2.6 zur TSL-Prüfung im Internet und 8.5.3 zur Prüfung von QES-Zertifikaten im Internet bereitgestellt.

---

## 2 Änderung in gemSpec\_PKI

---

### 2.1 NEUES Unterkapitel 8.2.6 - Besonderheiten bei der TSL-Prüfung im Internet

Das Kapitel 8.2 beschreibt die Vorgaben, Regelungen und Anforderungen, die für die Verwendung der TSL notwendig sind. Diese ist für die Prüfung von X.509-Zertifikaten der TI-PKI eine Voraussetzung ist und berücksichtigte bisher keine Vorgaben zur Prüfung aus dem Internet. Neuere Anwendungen in der TI und vor allem TI 2.0-Anwendungen haben nur begrenzten oder keinen Zugang zu TI 1.0 Systemen mehr. Daher müssen sie zur Prüfung von TI-PKI Zertifikaten Komponenten im Internet (TSL-Downloadpunkte, OSCP-Responder) verwenden. Die folgenden Ergänzungen beschreiben Vorgaben, die bei der Nutzung der TSL aus dem Internet zu berücksichtigen sind.

Das Kapitel 8.2.1.1 beschreibt die Lokalisierung der TSL-Download-Adressen und bezieht sich dabei aber ausschließlich auf den Download über das geschlossene Netz der TI (1.0). Die URLs, die in der TSL selbst zu finden sind (unter PointersToOtherTSL) sind keine URLs, die über das Internet erreichbar sind. Die zum Download über das Internet relevanten URLs befinden sich in gemSpec\_TSL in Kap. 6.3.1 bzw. in der Anforderung A\_17680-\* und werden hier nochmal aufgeführt:

- Für die Produktivumgebung (PU)
  - TSL: [https://download.tsl.ti-dienste.de/ECC/ECC-RSA\\_TSL.xml](https://download.tsl.ti-dienste.de/ECC/ECC-RSA_TSL.xml)
  - Hash: [https://download.tsl.ti-dienste.de/ECC/ECC-RSA\\_TSL.sha2](https://download.tsl.ti-dienste.de/ECC/ECC-RSA_TSL.sha2)
- Für die Referenzumgebung (RU)
  - TSL: [https://download-ref.tsl.ti-dienste.de/ECC/ECC-RSA\\_TSL-ref.xml](https://download-ref.tsl.ti-dienste.de/ECC/ECC-RSA_TSL-ref.xml)
  - Hash: [https://download-ref.tsl.ti-dienste.de/ECC/ECC-RSA\\_TSL-ref.sha2](https://download-ref.tsl.ti-dienste.de/ECC/ECC-RSA_TSL-ref.sha2)
- Für die Testumgebung (TU)
  - TSL: [https://download-test.tsl.ti-dienste.de/ECC/ECC-RSA\\_TSL-test.xml](https://download-test.tsl.ti-dienste.de/ECC/ECC-RSA_TSL-test.xml)
  - Hash: [https://download-test.tsl.ti-dienste.de/ECC/ECC-RSA\\_TSL-test.sha2](https://download-test.tsl.ti-dienste.de/ECC/ECC-RSA_TSL-test.sha2)

Entsprechend wird zum Download der Vertrauensliste der Bundesnetzagentur (BNetzA\_VL) auch nicht die in der TSL konfigurierte Download-URL, sondern die offiziellen von der Bundesnetzagentur bereitgestellten URLs verwendet:

- URL der BNetzA\_VL die Produktivumgebung (PU)
  - BNetzA\_VL: <https://tl.bundesnetzagentur.de/TL-DE.xml>
  - Hash: <https://tl.bundesnetzagentur.de/TL-DE.sha2>
- URL der Pseudo-BNetzA\_VL zu Testzwecken in RU und TU
  - Pseudo-BNetzA-VL: <https://download-testref.tsl.ti-dienste.de/P-BNetzA/Pseudo-BNetzA-VL.xml>
  - Hash: <https://download-testref.tsl.ti-dienste.de/P-BNetzA/Pseudo-BNetzA-VL.sha2>

Bei Verwendung der TSL im Internet muss folgende Anforderung mit ergänzenden Abweichungen von „GS-A\_4642-\* - TUC\_PKI\_001: Periodische Aktualisierung TI-Vertrauensraum“ berücksichtigt werden:

#### **A\_30044 -TSL-Aktualisierung im Internet gemäß TUC\_PKI\_001**

Die Produkttypen und Komponenten der TI, die nonQES-Zertifikate der TI über das Internet prüfen MÜSSEN die Anforderungen aus TUC\_PKI\_001 umsetzen. Dabei gelten folgende Konkretisierungen und Abweichungen:

1. Abweichend von TUC\_PKI\_017 („Lokalisierung der TSL-Downloadadressen“) MUSS das System die jeweilige Betriebsumgebung (PU/RU/TU) konfigurierten TSL-Downloadadressen im Internet verwenden. Eine Ermittlung oder Verwendung von Backup-Downloadadressen DARF NICHT erfolgen.
2. Vor dem Download einer Trust-service Status List (TSL) MUSS das System den Hashwert der aktuell im System gespeicherten TSL mit dem Hashwert der am Downloadpunkt verfügbaren TSL vergleichen. Ein Download der TSL DARF nur erfolgen, wenn die Hashwerte voneinander abweichen oder noch keine TSL im System vorhanden ist.
3. Abweichend von TUC\_PKI\_005 („Ermittlung der OCSP-Adresse“) MUSS für das extrahierte TSL-Signer-Zertifikat die OCSP-Responder-Adresse aus der Erweiterung AuthorityInfoAccess (AIA) des Zertifikats ermittelt werden. Die Ermittlung der OCSP-Adresse gemäß TUC\_PKI\_005 DARF hierfür NICHT angewendet werden.
4. Tritt bei einer OCSP-Abfrage ein OCSP-Status-Fehler auf, MUSS das System die Abfrage zunächst bis zu drei Mal wiederholen. Besteht der Fehler auch nach dem dritten Wiederholungsversuch fort, DARF eine erneute OCSP-Abfrage erst nach Ablauf von fünf Minuten erfolgen.

[<=,TSP X.509 nonQES - SMC-B,funkt. Eignung: Test Produkt/FA]

Es ist zu beachten, dass zur Initialisierung des TI-Vertrauensankers die Hinweise und Anforderungen aus Kapitel 8.1.2 der gemSpec\_PKI zu berücksichtigen sind.

Bei Verwendung der Vertrauensliste der Bundesnetzagentur im Internet (BNetzA\_VL) muss folgende Anforderung mit ergänzenden Abweichungen von „GS-A\_5484-\* - TUC\_PKI\_036 „BNetzA-VL-Aktualisierung“ berücksichtigt werden:

#### **A\_30045 -Bezug der BNetzA-Vertrauensliste im Internet gemäß TUC\_PKI\_036**

Die Produkttypen und Komponenten der TI, die QES-Zertifikate über das Internet prüfen, MÜSSEN die Anforderungen aus TUC\_PKI\_036 umsetzen. Dabei gilt folgende Abweichung bzw. Konkretisierung:

Abweichend von TUC\_PKI\_036 DÜRFEN die Downloadadressen der BNetzA-Vertrauensliste (BNetzA-VL) NICHT aus der Trust-service Status List (TSL) ermittelt werden. Stattdessen MÜSSEN die für den Betrieb konfigurierten Downloadadressen im Internet verwendet werden. Eine Ermittlung oder Verwendung von Backup-Downloadadressen DARF NICHT erfolgen.

[<=,,]

## **2.2 NEUES Unterkapitel 8.3.5 - Vorgaben zur Prüfung von TI-Zertifikaten (nonQES) im Internet**

Das Kapitel 8.3 beschreibt die Vorgaben, Regelungen und Anforderungen, die für die Prüfung von X.509-Zertifikaten der TI-PKI notwendig sind und berücksichtigte bisher keine Vorgaben zur Prüfung aus dem Internet. Neuere Anwendungen in der TI und vor allem TI 2.0-Anwendungen haben nur begrenzten oder keinen Zugang zu TI 1.0 Systemen mehr. Daher müssen sie zur Prüfung von TI-PKI Zertifikaten Komponenten im Internet (TSL-Downloadpunkte, OCSP-Responder) verwenden. Die folgenden Ergänzungen beschreiben Vorgaben, die bei der Zertifikatsprüfung aus dem Internet zu berücksichtigen sind.

Das Kapitel 8.3.1 beschreibt die „Zertifikatsprüfung in der TI“ (von nonQES-TI-Zertifikaten) und bezieht sich dabei vornehmlich auf die Prüfung über das geschlossene Netz der TI (1.0). Viele neuere Produkttypen der TI prüfen nonQES-TI-Zertifikate ohne Zugang zum geschlossenen Netz der TI 1.0 (z.B. über den Konnektor). Dazu müssen die folgenden ergänzenden Abweichungen zu „GS-A\_4652-\* TUC\_PKI\_018: Zertifikatsprüfung in der TI“ zur Prüfung über das Internet berücksichtigt werden:

### **A\_30046 -Prüfung von nonQES-Zertifikaten der TI im Internet gemäß TUC\_PKI\_018**

Die Produkttypen und Komponenten der TI, die nonQES-Zertifikate der TI über das Internet prüfen, MÜSSEN die Anforderungen aus TUC\_PKI\_018 umsetzen. Dabei gelten folgende Abweichungen und Konkretisierungen:

1. Abweichend von TUC\_PKI\_005 („Ermittlung der OCSP-Adresse“) MUSS die OCSP-Responder-Adresse für das zu prüfende Zertifikat aus der Erweiterung AuthorityInfoAccess (AIA) des Zertifikats ermittelt werden. Die Ermittlung der OCSP-Adresse gemäß TUC\_PKI\_005 DARF hierfür NICHT angewendet werden.
2. Liefert die OCSP-Response den Zertifikatsstatus „unknown“, MUSS die Prüfung des certHash entfallen. Der Zertifikatsstatus „unknown“ MUSS in diesem Fall übernommen werden.
3. Tritt bei einer OCSP-Abfrage ein OCSP-Status-Fehler auf, MUSS das System die Abfrage zunächst bis zu drei Mal wiederholen. Besteht der Fehler auch nach dem dritten Wiederholungsversuch fort, DARF eine erneute OCSP-Abfrage erst nach Ablauf von fünf Minuten erfolgen.
4. Eine optionale Prüfung zurückgelieferter Rollen-OIDs DARF erst nach erfolgreichem Abschluss der Zertifikatsprüfung durchgeführt werden.
5. Enthält das zu prüfende Zertifikat im Attribut commonName einen Fully Qualified Domain Name (FQDN), MUSS dieser mit dem erwarteten FQDN übereinstimmen.
6. Ein lokales Caching von OCSP-Antworten MUSS entsprechend der Anforderung A\_23225 erfolgen.
7. Im Falle einer beigefügten OCSP-Response (z.B. eingebettet in Signatur) MÜSSEN mindestens die folgenden Prüfungen durchgeführt werden, wobei die Prüfung von zeitlichen Toleranzen gemäß GS-A\_5215-\* dabei immer entfällt:
  - a. Gültigkeitsprüfung der OCSP-Response zum Referenzzeitpunkt,
  - b. Prüfung, dass das OCSP-Signer-Zertifikat in der Trust-service Status List (TSL) enthalten ist,
  - c. Signaturprüfung der OCSP-Response gegen das anhand der TSL ermittelten OCSP-Signer-Zertifikats,
  - d. Vergleich des in der OCSP-Response enthaltenen certHash mit dem certHash des zu prüfenden Zertifikats (außer bei eGK-Zertifikaten)

**[<=,TSP X.509 nonQES - SMC-B, ZT\_Cluster,funkt. Eignung: Test Produkt/FA]**

## 2.3 NEUES Unterkapitel 8.5.3 - Vorgaben zur Prüfung von QES-Zertifikaten der TI im Internet

Das Kapitel 8.5 beschreibt die Vorgaben, Regelungen und Anforderungen, die für die Prüfung von X.509-QES-Zertifikaten der TI-PKI notwendig sind und berücksichtigte bisher keine Vorgaben zur Prüfung aus dem Internet. Neuere Anwendungen in der TI und vor allem TI 2.0-Anwendungen haben nur begrenzten oder keinen Zugang zu TI 1.0 Systemen mehr. Daher müssen sie zur Prüfung von TI-PKI Zertifikaten Komponenten im Internet (BNetzA-VL-Downloadpunkte, OCSP-Responder) verwenden. Die folgenden Ergänzungen beschreiben Vorgaben, die bei der Zertifikatsprüfung aus dem Internet zu berücksichtigen sind.

Das Kapitel 8.5.1 beschreibt die „QES-Zertifikatsprüfung“ und bezieht sich dabei vornehmlich auf die Prüfung über das geschlossene Netz der TI (1.0). Viele neuere Produkttypen der TI prüfen QES-TI-Zertifikate ohne Zugang zum geschlossenen Netz der TI 1.0 (z.B. über den Konnektor). Dazu müssen die folgenden ergänzenden Abweichungen zu „GS-A\_4750-\* TUC\_PKI\_030 QES-Zertifikatsprüfung“ berücksichtigt werden:

### **A\_30047 -Prüfung von QES-Zertifikaten der TI im Internet gemäß TUC\_PKI\_030**

Die Produkttypen und Komponenten der TI, die QES-Zertifikate der TI über das Internet prüfen, MÜSSEN die Anforderungen aus TUC\_PKI\_030 umsetzen. Dabei gelten folgende Abweichungen und Konkretisierungen:

1. Für die Durchführung einer OCSP-Abfrage MUSS die OCSP-Responder-Adresse unmittelbar aus der Erweiterung AuthorityInfoAccess (AIA) des zu prüfenden Zertifikats verwendet werden. Die Nutzung oder Ersetzung der OCSP-Adresse durch eine in der TSL enthaltene TI-Adresse DARF NICHT erfolgen.
2. Die OCSP-Abfrage für ein QES-Zertifikat MUSS stets unter Verwendung des Parameters Nonce erfolgen.
3. Liefert die OCSP-Response den Zertifikatsstatus „unknown“, MUSS die Prüfung des certHash entfallen. Der Zertifikatsstatus „unknown“ MUSS in diesem Fall übernommen werden.
4. Eine OCSP-Response MUSS auch dann als gültig akzeptiert werden, wenn das geprüfte QES-Zertifikat und das OCSP-Signer-Zertifikat von unterschiedlichen Certification Authorities (CAs) stammen, sofern die Signaturprüfung des geprüften QES-Zertifikats gegen das zugehörige QES-CA-Zertifikat aus der BNetzA-Vertrauensliste (BNetzA-VL) sowie die Signaturprüfung des OCSP-Signer-Zertifikats gegen das jeweils zugehörige QES-CA-Zertifikat aus der BNetzA-VL erfolgreich sind.
5. Tritt bei einer OCSP-Abfrage ein OCSP-Status-Fehler auf, MUSS das System die Abfrage zunächst bis zu drei Mal wiederholen. Besteht der Fehler auch nach dem dritten Wiederholungsversuch fort, DARF eine erneute OCSP-Abfrage erst nach Ablauf von fünf Minuten erfolgen.
6. Eine optionale Prüfung zurückgelieferter Rollen-OIDs DARF erst nach erfolgreichem Abschluss der Zertifikatsprüfung durchgeführt werden.
7. Wird eine OCSP-Response gemeinsam mit dem zu prüfenden Objekt bereitgestellt, beispielsweise eingebettet in einer elektronischen Signatur, MÜSSEN mindestens die folgenden Prüfungen durchgeführt werden, wobei die Prüfung von zeitlichen Toleranzen gemäß GS-A\_5215-\* dabei immer entfällt:

- 212 a. Gültigkeitsprüfung der OCSP-Response zum Referenzzeitpunkt,  
213 b. Signaturprüfung der OCSP-Response gegen das in der OCSP-Response enthaltene  
214 OCSP-Signer-Zertifikat,  
215 c. Signaturprüfung des OCSP-Signer-Zertifikats gegen das zugehörige Aussteller-CA-  
216 Zertifikat aus der BNetzA-VL.  
217 **[<=,,]**  
218

---

### 3 Änderung in gemSpec\_Krypt

---

Im informativen Text nach [gemSpec\_Krypt#GS-A\_5581] wird <https://download.tsl.ti-dienste.de> zu <https://download.tsl.ti-dienste.de/ECC/> aktualisiert. Analog in Abschnitt [gemSpec\_Krypt#4.1].



---

## 4 Änderungen in Steckbriefen

---

### 4.1 Änderungen in gemProdT\_...\_PTVx.y.z-n

*Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT\_...]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.*

**Tabelle 1: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"**

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|--------|-----------------|-------------------|
|        | [...]           |                   |