*Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.*

# Änderungen in gemSpec_PKI

Kap. 8.1.1.1 wird wie folgt angepasst

**⌦ GS-A_5612 TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“ – überholte Variante**

Die Produkttypen der TI, die Zertifikate prüfen, KÖNNEN im Zuge der Aktualisierung des TI-Vertrauensraums gemäß TUC_PKI_001 folgende Abweichungen umsetzen:

- im Schritt 6 kann eine inhaltliche Überprüfung der Datenfelder eines Zertifikats beim Speichern des Zertifikats im system-eigenen Truststore erfolgen,
- im Schritt 6 können auch Zertifikate, die für den Produkttypen nicht relevant sind, in seinen Truststore übernommen werden.⌫

*Hinweis: Die Anforderung GS-A_5612 stellt eine überholte, weniger robuste Ablaufvariante von TUC_PKI_001 dar und wird perspektivisch entfallen. Eine Umsetzung ist demzufolge nicht empfohlen.*

**Tabelle 80: TUC_PKI_001 "Periodische Aktualisierung TI-Vertrauensraum"**

| Element | Beschreibung |
|---|---|
| Name | TUC_PKI_001 "Periodische Aktualisierung TI-Vertrauensraum" |
| Beschreibung | Dieser Use Case beschreibt den gesamten Ablauf zur periodischen Aktualisierung des TI-Vertrauensraumes mittels einer TSL-Datei. Dabei verwendet er weitere TUCs, die im Laufe des Kapitels detailliert spezifiziert werden<br>Ein Offline-Modus ist zu berücksichtigen für<br>a) das Mobile-Kartenterminal<br>b) Konnektor ohne Anbindung an die TI<br>Beide verfügen nicht über die automatischen Online-Möglichkeiten zum Bezug von Statusinformationen oder TSL-Aktualisierungen aus der TI. |
| Anwendungsumfeld | System, das die TSL auswertet |
| Auslöser | Produkttypspezifischer Trigger<br>Zeitpunkt MUSS durch Facharchitekturen vorgegeben werden.<br>(Standardmäßig ist eine tägliche Prüfung der Aktualität vorzusehen.) |
| Eingangsdaten | • TSL im System<br>• Neu eingebrachte TSL-Datei (optional)<br>• OCSP-Graceperiod (legt bei der Verwendung von gecachten OCSP-Antworten den maximal zulässigen Zeitraum fest, den die Systemzeit der prüfenden Komponente noch nach dem Zeitpunkt der OCSP-Antwort liegen darf)<br>• Flag für Offline-Modus (Im Offline-Fall kann keine Sperrstatusprüfung des TSL-Signer-Zertifikates durchgeführt werden.) |


© gematik – öffentlich_Entwurf

| Element | Beschreibung |
|---|---|
| Komponenten | System, TSL-Download-Punkt, OCSP-Responder |
| Ausgangsdaten | Status der Initialisierung |
| Referenzen | [ETSI_TS_102_231] |
| Standardablauf | 1.<br>[System:] System startet die Initialisierung des TI-Vertrauensraums.<br>2.<br>[System:] Die TSL im System wird auf Aktualität geprüft (TUC_PKI_019 „Prüfung der Aktualität der TSL"). Diese Prüfung erfolgt gegen die neu eingebrachte TSL-Datei als Eingangsparameter. (Ansonsten wird die aktuelle TSL-Datei bei diesem Schritt heruntergeladen.) Die Prüfung ergibt, dass die im System abgelegten TSL-Informationen erneuert werden müssen.<br>3.<br>[System:] Das verwendete TSL-Signer-Zertifikat wird aus der TSL-Datei extrahiert.<br>4.<br>[System:] OCSP-Abfrage für das extrahierte TSL-Signer-Zertifikat durch das System (TUC_PKI_006 "OCSP-Abfrage")<br>(Sämtliche anderen Schritte einer Prüfung des Zertifikates und der XML-Signatur sind im TUC_PKI_019 „Prüfung der Aktualität der TSL" referenziert, vgl. im Schritt 2.)<br>5.<br>[System:] Es wird ermittelt, ob in der neuen TSL ein neuer TI-Vertrauensanker vorliegt (TUC_PKI_013 „Import TI-Vertrauensanker aus TSL“).<br>6.<br>[System:] Aus den CA-Zertifikaten aus der neuen TSL wird der neue TI-Vertrauensraum gebildet. Dazu werden sie aus der TSL-Datei extrahiert, z. B. in einen system-eigenen Truststore gespeichert und dem System bereitgestellt. Bei der Extraktion der Zertifikate aus der TSL darf keine inhaltliche Überprüfung der Datenfelder oder eine Signaturprüfung des Zertifikats erfolgen.<br>Falls ein solcher Truststore nur den Vertrauensraum der TI enthält, wird er vor der Neubefüllung geleert, so dass anschließend nur die Zertifikate aus der aktuellen TSL dem System zur Verfügung stehen.<br>Falls der Truststore auch für die sichere Speicherung von Zertifikaten benutzt wird, die nicht in der TSL stehen, muss keine komplette Leerung des Truststores erfolgen. Das System muss aber sicherstellen, dass im Truststore nur diejenigen Zertifikate der TI enthalten sind, die den aktuellen Vertrauensraum der TI aufspannen bzw. in der aktuellen TSL-Datei enthalten sind.<br>Die Form des Truststore wird nicht näher spezifiziert, dieser muss nur den gestellten Anforderungen (z. B. bezüglich Sicherheit oder Performance) genügen.<br>Das System muss den TI-Vertrauensraum mit den in der TSL als vertrauenswürdig bezeichneten und für den Produkttyp relevanten CA-Zertifikaten gemäß Tab_PKI_271 „Erlaubte Inhalte des TSL-Elements ServiceStatus“ befüllen.<br>7.<br>[System:] Der Truststore wird für Zertifikatsprüfung (wieder) bereitgestellt.<br>8.<br>[System:] Ende des Use Case |
| Varianten/Alternativen | Der Standardablauf stellt die Prüfungen dar, die vollzogen werden müssen. Eine Trennung in zwei Prozesse oder eine Umstrukturierung, bei |


© gematik – öffentlich_Entwurf

| Element | Beschreibung |
|---|---|
| | der alle notwendigen Prüfungen erfolgen, ist zulässig.<br><br>Im Falle einer aktuellen TSL im System endet der Ablauf nach Schritt 2:<br>2a.<br>[System:] TSL aus Download ist gleich TSL im System; und TSL ist noch gültig.<br>2a.1<br>[System:] Ende des Use Case<br>3a.<br>[System:] Wenn das Offline-Flag gesetzt ist (offline==true), dann wird mit Schritt 5 weitergefahren.<br>(Im Offline-Fall kann keine OCSP-Abfrage stattfinden.) |
| Fehlerfälle/Warnung | Ein Fehlerfall ist, dass dem System keine gültige TSL vorliegt :<br>1a.<br>[System:] Es ist keine TSL im System vorhanden. Abbruch mit Fehlermeldung (TSL_INIT_ERROR)<br>2b.<br>[System:] Der TUC_PKI_019 wirft eine VALIDITY_WARNING_2. VALIDITY_WARNING_2 wird als Fehlermeldung ausgegeben.<br>Die weitere Fehlerbehandlung erfolgt unter Beachtung von [GS-A_5336].<br>3b.<br>[System:] Das TSL-Signer-Zertifikat lässt sich nicht aus der TSL-Datei extrahieren (TSL_CERT_EXTRACTION_ERROR).<br>6a. [System:] Abbruch mit Fehlermeldung (TSL_CERT_EXTRACTION_ERROR)<br><br>Weitere Fehlerfälle sind in den jeweiligen referenzierten TUCs beschrieben. |
| Technische Fehlermeldung | Es ist keine TSL im System vorhanden.<br>Zertifikat(e) lässt/lassen sich nicht extrahieren.<br><br>Weitere technische Fehlermeldungen sind in den jeweiligen referenzierten TUCs beschrieben |
| Sicherheitsanforde-rungen | Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen. |
| Anmerkungen | Die Angaben zur Prüfung einer neuen TSL-Datei müssen als vertrauenswürdige Informationen im System schon vorhanden sein. Deshalb muss die OCSP-Adresse zur Prüfung des Signers der neuen TSL-Datei aus der TSL im System ausgelesen werden.<br><br>Für die Prüfung der ersten TSL-Datei nach einem Vertrauensankerwechsel (entsprechend TUC_PKI_013 „Import TI-Vertrauensanker aus TSL“ und angekündigt mit ServiceTypeIdentifier „http://uri.etsi.org/TrstSvc/Svctype/TSLServ iceCertChange“) bedeutet dies, dass die OCSP-Adresse aus dem „TSLServiceCertChange“ Eintrag aus der TSL im System genommen werden muss. |
| Zugehörige Diagramme | Aktivitätsdiagramm TUC_PKI_001 "Periodische Aktualisierung TI-Vertrauensraum" |


© gematik – öffentlich_Entwurf

# Änderungen in gemProdT_OCSP_Proxy, gemProdT_gematik-Root-CA, gemProdT_X.509_TSP_nonQES_eGK, gemProdT_X.509_TSP_nonQES_HBA, gemProdT_X.509_TSP_nonQES_SMC-B, gemProdT_X.509_TSP_nonQES_Komp, gemProdT_X.509_TSP_QES, gemProdT_TSL, gemProdT_NamD, gemProdT_KSR, gemProdT_SG_BestNetze, gemProdT_VPN_ZugD, gemProdT_ZeitD, gemProdT_ZentrNetz, gemProdT_Intermediaer_VSDM, gemProdT_VZD, gemProdT_FD_VSDM

Es wird Kap. 3.1.1 wie folgt ergänzt

## 3.1.1 Produkttest / Produktübergreifender Test

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Anforderungen an den technischen Teil des Produkttyps verzeichnet, deren Umsetzung im Zuge von Zulassungstests durch die gematik geprüft wird.

**Tabelle 2: Anforderungen zur funktionalen Eignung "Produkttest / Produktübergreifender Test"**

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|---|---|---|
| … | | |
| GS-A_5612 | TUC_PKI_001 „Periodische Aktualisierung TI-Vertrauensraum“ -– überholte Variante | gemSpec_PKI |
| … | | |


© gematik – öffentlich_Entwurf