

## Änderung in gemSpec\_PKI, C\_11581\_Anlage

Es wird in Kapitel "5.13.1" nur der gelb-markierte Text aufgenommen....

### 1.1.1 Kapitel 5.13.1 Definition der OCSP-Signer-Identität

(...)

#### **A\_23142 - TSP-X.509nonQES: OCSP-Responder-Zertifikate nach RFC-6960#4.2.2.2**

Ein TSP-X.509 nonQES MUSS sicherstellen, dass die von ihm neu erzeugten OCSP-Responder-Zertifikate den Vorgaben aus [RFC-6960#4.2.2.2 (Option 2)] genügen. Die OCSP-Responder-Zertifikate MÜSSEN von der CA, über die sie bezüglich der Sperrinformationen auskunftsberechtigt sein sollen, direkt ausgestellt (signiert) werden. [ $\leq$ ]

*Hinweis: Neue OCSP-Signer-Zertifikate sollten gemäß [RFC6960#4.2.2.2] signiert werden. Zu beachten ist, dass OCSP-Signer-Zertifikate zur Verwendung in der TI in die TSL eingebracht werden müssen. (vgl. [gemSpec\_TSL#TIP1-A\_4084] sowie TUC\_PKI\_006 „OCSP-Abfrage“, Schritt 5.)*

*Ziel ist es in Bezug auf die Verknüpfung Root-CA-Zertifikate -> CA-Zertifikate -> OCSP-Responder-Zertifikate einen klassischen gerichteten PKI-Graphen zu erhalten. D. h., ein Zertifikat im Graph und seine Zertifikatssignatur ist durch den öffentlichen Schlüssel des direkten Vorgängerknotens prüfbar*

#### **A\_24172 - TSP-X.509nonQES: Gültigkeitsdauer OCSP-Responder-Zertifikat und EE-Zertifikate, Vorhalten von OCSP-Antworten**

Ein TSP-X.509 nonQES SMC-B und HBA MUSS sicherstellen, dass

1. es einen Zeitraum D mit Länge(D) > 1 Stunde gibt (bspw. einen Tag, siehe Anwendungshinweis in [gemSpec\_PKI#A\_24172-Anwendungshinweis-1]), so dass für alle von einer CA bestätigten EE-Zertifikate, die keine OCSP-Responder-Zertifikate sind, gilt: Ende-der-Gültigkeitsdauer-EE-Zertifikat-nicht-OCSP + Länge(D) < Ende-der-Gültigkeitsdauer-bestätigende-CA.
2. nach Ablauf der Gültigkeitsdauer eines EE-Zertifikat-nicht-OCSP und vor Ablauf der CA-Gültigkeitsdauer und des korrespondierenden OCSP-Responder-Zertifikats die CA eine OCSP-Antwort für dieses Zertifikat erzeugt, was aufgrund von Punkt 1 immer möglich ist. Die erzeugten OCSP-Antworten MÜSSEN lokal gespeichert werden (vorhalten). Die OCSP-Antworten enthalten dann je nach Sperrstatus des EE-Zertifikats entweder "good" oder "revoked" als Sperrstatus. Die dabei erzeugten OCSP-Antworten MÜSSEN im "nextUpdate"-Feld das Datum "9999-12-31T23:59:59" enthalten.
3. OCSP-Anfragen über abgelaufene EE-Zertifikate-nicht-OCSP aus dem Speicher von Punkt 2. beantwortet werden, d. h. die dort enthaltenen statischen OCSP-Antworten als Antwort gesendet werden.

[ $\leq$ ]

#### **A\_24172-Anwendungshinweis-1:**

Bei der klassischen PKI-Zertifikatsprüfung muss das zulässige/auskunftsberechtigte OCSP-Responder-Zertifikat direkt von der CA bestätigt (signiert) sein (vgl. A\_23142). Abgelaufene EE-Zertifikate können ihren Sperrstatus nicht mehr verändern, d. h. sie sind nach Ablauf entweder gesperrt oder nicht. Nach Ablauf von EE-Zertifikaten wird von der CA selbstständig eine Sperrinformation erzeugt, die A\_23142 genügt. Wegen A\_24172-Punkt-1 ist dies für jedes EE-Zertifikat-nicht-OCSP möglich. Diese Sperrinformation (OCSP-Antwort) wird lokal gespeichert. Die OCSP-Antworten aus diesem Speicher sind die Antworten auf zukünftige OCSP-Anfragen. Die Länge des Zeitraums D kann der TSP selbst bestimmen und sie ist abhängig von der Gestaltung der internen Abläufe innerhalb des TSPs.

Der TSP kann entscheiden, ob der direkt nach Ablauf eines EE-Zertifikats-nicht-OCSP die OCSP-Antworten nach A\_24172#Punkt 2 erzeugt oder, ob er innerhalb des Zeitraums D für alle von der entsprechenden CA erzeugten EE-Zertifikat-nicht-OCSP die OCSP-Antworten nach A\_24172#Punkt 2 erzeugt.

#### **Hinweis zur OCSP-Prüfung von abgelaufenen Signatur-Zertifikaten (beim Client):**

Eine OCSP-Antwort mit einem nextUpdate "9999-12-31T23:59:59" wird nicht mehr erneuert werden.

Die Prüfung der Zeitangabe in producedAt gegen die OCSP-Graceperiod ((TUC\_PKI\_006 Varianten 1a2 und 1a3) bzw. gegen die Gültigkeitsdauer beim lokalen Caching (A\_23235) muss daher immer als zeitlich gültig bewertet werden.

(....)

Es wird in Kapitel "9.1.2.2" nur der gelb-markierte Text aufgenommen....

#### **1.1.1.1 Kapitel 9.1.2.2 OCSP-Response - Zeiten**

##### **GS-A\_4688 - Statusprüfdienst – Angabe von Zeitpunkten**

Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES MÜSSEN sicherstellen, dass die Angabe zu den Zeitpunkten `producedAt`, `thisUpdate` und `nextUpdate` spezifikationskonform gemäß Tab\_PKI\_292 erfolgt.

**Tabelle 1: Tab\_PKI\_292 Zeiten in einer OCSP-Response**

Zeiten	Bedeutung
<b>thisUpdate</b>	„thisUpdate“ enthält den Zeitpunkt, für den die gemachte Aussage gültig ist. Es gibt den Zeitpunkt an zu der die Statusinformation als korrekt angesehen wurde.
<b>nextUpdate</b>	„nextUpdate“ enthält die Zeit, wann neue Informationen über das angefragte Zertifikat verfügbar sein werden. OCSP-Antworten, die keinen „nextUpdate“ Zeitpunkt enthalten, zeigen an, dass jederzeit neuere Statusinformationen zu Zertifikaten vorhanden sein können.
<b>producedAt</b>	Der Zeitpunkt der Signierung einer OCSP-Response.

[<=]

Der Zeitpunkt `nextUpdate` ist nur für OCSP-Antworten sinnvoll, die auf CRLs basieren.

Eine OCSP-Antwort mit einem nextUpdate "9999-12-31T23:59:59" wird nicht mehr erneuert werden und zeigt an, dass es keine neueren Statusinformationen mehr geben wird, weil z.B. die herausgebende CA zeitlich abgelaufen ist.

## Änderungen in Steckbriefen

- gemProdT\_X509\_TSP\_nonQES\_SMC-B
- gemProdT\_X509\_TSP\_nonQES\_HBA

**Tabelle 2: Anforderungen zur funktionalen Eignung "Sicherheitstechnische Eignung, Herstellererklärung"**

Afo-ID	Afo-Bezeichnung	Zuweisung
A_24172	TSP-X.509nonQES: Gültigkeitsdauer OCSP-Responder-Zertifikat und EE-Zertifikate, Vorhalten von OCSP-Antworten	<p>TSP-X.509 nonQES SMC-B Prüfnachweis: Sicherheitstechnische Eignung: Herstellererklärung</p> <p>TSP-X.509 nonQES HBA Prüfnachweis: Sicherheitstechnische Eignung: Herstellererklärung</p>