Änderung in gemSpec_PKI

Kurz vor Ende von Abschnitt "5.13 OCSP - Statusauskunftsdienst" wird hinzugefügt:

A_23142 - TSP-X.509nonQES: OCSP-Responder-Zertifikate nach RFC-6960#4.2.2.2
Ein TSP-X.509 nonQES MUSS sicherstellen, dass von ihm neu erzeugte OCSP-Responder-Zertifikate die 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.**[**<=**]**

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.

Änderung in gemSpec_Krypt

Am Ende von Abschnitt "2.4.1 Prüfung auf angreifbare (schwache) Schlüssel" wird hinzugefügt:

Unter https://security.googleblog.com/2022/08/announcing-open-sourcing-of-paranoids.html ist eine Vielzahl von Schlüsseltests als OpenSource verfügbar.

In Abschnitt "3.7 KOM-LE-spezifische Vorgaben" wird eine Korrektur in informativen Erläuterungstext vorgenommen:

Bei KOM-LE werden E-Mail-Anhänge, deren Gesamtgröße ~~die konnektorschnittstellenbedingte Maximalgröße (vgl. [gemSpec_KON]) von etwas weniger als 25~~ 15 MiB überschreitet, separat symmetrisch verschlüsselt und das Chiffrat auf dem "Fachdienst Download-Server (KAS)" abgelegt.

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: Zuweisung der Anforderungen

Afo-ID	Afo-Bezeichnung	Zuweisung
A_23142	TSP-X.509nonQES: OCSP-Responder-Zertifikate nach RFC-6960#4.2.2.2	TSP X.509 nonQES - HBA, TSP X.509 nonQES - eGK, TSP X.509 QES, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC funkt. Eignung: Herstellererklärung, Sich.techn. Eignung: Herstellererklärung