Änderung in gemSpec_PKI

Nach GS-A_5215 und der Erläuterung zu der Anforderung wird folgendes hinzugefügt:

A_23225 - lokales Caching von Sperrinformationen und Toleranzzeiten
Alle Produkttypen der TI, die im Rahmen von Zertifikatsprüfung Sperrinformation für nonQES-Zertifikate einholen, MÜSSEN folgende Vorgaben umsetzen:

1. Die Sperrinformationen (bspw. OCSP-Responses) müssen lokal gespeichert werden (caching), solange sie noch zeitlich gültig sind.
2. Definition zeitliche Gültigkeit: Sei p die Zeit zu der die Sperrinformation vom TSP erzeugt wurde. Im Fall von OCSP-Responses ist diese Zeit die productedAt-Angabe [RFC-6960]. Sei s die lokale Systemzeit des prüfenden Systems. Eine Sperrinformation ist zeitlich gültig, wenn gilt s - D <= p <= s + 5 Minuten, wobei D im default-Fall eine Stunde beträgt.
   (Es gibt anwendungsspezifische Verlängerungen der Gültigkeitsdauer D, die dann explizit in den entsprechenden Spezifikationen definiert werden.
   D. h. die Sperrinformation können im default-Fall maximal eine Stunde alt sein und maximal für fünf Minuten "aus der Zukunft kommen". (Da nicht alle Produkttypen ihre Systemzeit in der TI synchronisieren, erlauben wir hier eine fünfminutige fehlerhafte Abweichung der lokalen Zeit.)
3. Das prüfende System muss, bevor es Sperrinformationen (bspw. für ein Zertifikat) einholt, prüfen, ob im Cache (vgl. Punkt 1) zeitlich gültige Sperrinformationen schon vorliegen. Falls ja muss es diese Informationen verwenden und darf diese nicht neu beziehen.
4. Bei der einer evtl. Abarbeitung von TUC_PKI_006 muss der optionale Eingabeparameter "OCSP-Graceperiod" ignoriert werden und für die zeitliche Gültigkeit ist Punkt 2 maßgeblich. Bei OCSP-Antworten ist in diesem Kontext die Konsistenzprüfung wie in TUC_PKI_006 in Schritt 6 aufgeführt fachlich unnötig und deshalb nicht durchzuführen.
5. Zeitlich ungültige Sperrinformation im Cache dürfen nicht für Zertifikatsprüfvorgänge verwendet werden und müssen mindestens alle 24h aus dem Cache aktiv entfernt werden.

[<=]

Erläuterung zu A_23225:

Falls A_23225-* einem Produkttypen zugwiesen ist, so gilt GS-A_5215 nicht und ist daher diesem Produkttypen nicht zugewiesen.

Kontext OCSP: die aufgrund der historischen Entwicklung von OCSP als Abfragemechanismus einer CRL-Abfrage bei einem TSP stammenden Werte thisUpdate und nextUpdate sind für A_23225-* irrelevant. Was zählt ist, dass der bestmögliche Informationsstand eines TSP zum Zeitpunkt producedAt in der Antwort dokumentiert ist. Dieser Informationsstand wird im Cache für die in A_23225 aufgeführte Zeit als maßgeblich betrachtet und im prüfenden System verwendet.

Falls Sperrinformationen grundsätzlich vom zu authentifizierenden System mit gesendet werden (bspw. TLS-OCSP-stapling, VAUServerHello), so holt der Client diese nicht aktiv ein, d. h., A_23225 greift in Bezug auf das Caching nicht als MUSS-Bestimmung.

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: Anforderungszuweisung

Afo-ID	Afo-Bezeichnung	Zuweisung
A_23225	lokales Caching von Sperrinformationen und Toleranzzeiten	Aktensystem_ePA (Herstellererklärung sicherheitstechnische Eignung) Verzeichnisdienst (Herstellererklärung sicherheitstechnische Eignung) E-Rezept Fachdienst (Herstellererklärung sicherheitstechnische Eignung) IDP-D (Herstellererklärung sicherheitstechnische Eignung) Zugangsdienst (Herstellererklärung sicherheitstechnische Eignung)
GS-A_5215	Festlegung der zeitlichen Toleranzen in einer OCSP-Response	Die Zuweisung wird bei allen Produkttypen entfernt bei denen A_23225 zugewiesen wurde.