Änderung in gemSpec_Krypt

GS-A_4357-01 - X.509-Identitäten für die Erstellung und Prüfung digitaler nicht-qualifizierter elektronischer Signaturen
Alle Produkttypen, die X.509-Identitäten bei der Erstellung oder Prüfung digitaler nicht-qualifizierter elektronischer Signaturen verwenden, MÜSSEN die in Tab_KRYPT_002 aufgeführten Algorithmen unterstützen und die Tabellenvorgaben erfüllen.
Produkttypen, die Zertifikate (X.509-Identitäten) auf Basis der Schlüsselgeneration „ECDSA" ausstellen (vgl. Abschnitt 5.1) oder verwenden, MÜSSEN die in Tab_KRYPT_002a aufgeführten Algorithmen und die Tabellenvorgaben erfüllen.
<=

Die Tabelle Tab_KRYPT_002a wird wie folgt angepasst.

Tabelle 1: Tab_KRYPT_002a Algorithmen für X.509-Identitäten zur Erstellung nicht-qualifizierter Signaturen für die Schlüsselgeneration „ECDSA"

Anwendungsfall	Vorgabe
Art und Kodierung des öffentlichen Schlüssels	ecPublicKey {OID 1.2.840.10045.2.1} **Entweder** auf der Kurve brainpoolP256r1 [RFC-5639#3.4, brainpoolP256r1] zulässig bis Ende 2023+ **oder** auf der Kurve P-256 [FIPS-186-4] zulässig bis Ende 2023+ Verständnishinweis: vgl. auch A_23139 bezüglich der Entweder-Oder-Beziehung Die Kodierung des öffentlichen Punkt erfolgt nach [RFC5480, Abschnitt 2] (vgl. Beispiel in Abschnitt 5.2) Der privater Schlüssel muss zufällig und gleichverteilt aus {1, …, q-1} gewählt werden. (q ist die Ordnung des Basispunkts und ceil($\log_2$ q)=256).
Signatur eines Zertifikats Signatur einer OCSP-Response Signatur eines OCSP-Responder-Zertifikates Signatur einer CRL Signatur des Zertifikats das Basis der Signaturprüfung einer CRL ist	ecdsa-with-SHA256 [RFC-3279] {OID 1.2.840.10045.4.3.2} **Entweder** auf der Kurve brainpoolP256r1 [RFC-5639#3.4, brainpoolP256r1] zulässig bis Ende 2023+ **oder** auf der Kurve P-256 [FIPS-186-4] zulässig bis Ende 2023+ vgl. Beispiel in Abschnitt 5.2

	Der privater Schlüssel muss zufällig und gleichverteilt aus {1, …, q-1} gewählt werden. (q ist die Ordnung des Basispunkts und ceil($\log_2$ q)=256).

Am Ende von Abschnitt 2.1.1.1. wird hinzugefügt:

A_23139 - TSP-X.509-nonQES: ECC-Kurvenparameter, Komplexitätsreduktion
Ein TSP-X.509-nonQES, der nicht die X.509-Root-CA der TI ist, MUSS sicherstellen, dass

1. ein öffentlicher ECC-Schlüssel im CA-Zertifikat,
2. die öffentlichen ECC-Schlüssel der zum CA-Zertifikat aus (1) zugehörigen OCSP-Zertifikate (vgl. [RFC-6960#4.2.2.2] bzw. A_23142), und
3. die öffentlichen ECC-EE-Schlüssel in den EE-Zertifikate, die durch die CA mit dem Schlüssel aus (1) prüfbar sind,

die gleichen Kurvenparameter (brainpoolP256r1, P-256 etc. vgl. [gemSpec_Krypt#Tab_KRYPT_002a]) besitzen.
[<=]

Verständnishinweis:

Die Chipkarten der TI verwenden für ihre ECC-EE-Schlüssel alle die Kurvenparameter brainpoolP256r1. Dies ist in den Objektsystem-Spezifikationen (und damit auch den Objektsystemen) der Chipkarten fixiert. Die CA-en, die EE-Zertifikate für diese Chipkarten bestätigen, müssen nach A_23139-* ebenfalls ein ECC-Schlüsselpaar auf Basis von brainpoolP256r1 verwenden.

Die Komponenten-PKI der TI besitzt mehrere CA-Zertifikate. Es gibt mindestens ein CA-Zertifikat, das für die Prüfung der ECC-EE-Zertifikate von SMC-K, SMC-KT und der meisten Fachdienste verwendet wird. Dieses CA-Zertifikat verwendet ebenfalls als öffentlichen Prüfschlüssel ein Schlüssel auf brainpoolP256r1-Basis (A_23139-*).

Für bestimmte Fachdienste, die zukünftig direkt von einen Primärsystem per TLS erreichbar sein sollen, sollen TLS-Zertifikate in der Komponenten-PKI der TI erzeugt werden können, die anstatt brainpool-Kurvenpunkte (brainpoolP256r1) NIST-Kurvenpunkte (P-256) als öffentliche Schlüssel enthalten. Grund dafür ist die deutlich bessere Unterstützung der NIST-Kurvenparameter durch verschiedene Standard-Kryptographie-Softwarebibliotheken.

Es gibt in der Komponenten-PKI mindestens ein CA-Zertifikat, dessen öffentlicher ECC-Schlüssel NIST-kurvenbasiert ist. Falls ein Fachdienst einen CSR mit einen NIST-Kurvenpunkt als öffentlichen Schlüssel einreicht bei der Komponenten-PKI, dann wird dieser unter der CA bestätigt, die NIST-kurvenbasiert ist.

In der Regel werden X.509-Root-CA-Zertifikate (RCA7 etc.) NIST-kurvenbasiert sein. Damit kann ein PVS mit einer Kryptographie-Softwarebibliothek ohne brainpool-Kurvenunterstützung mit solch einem Root-CA-Zertifikat die komplette Zertifikatskette bis zum Fachdienst prüfen.

Für die X.509-Root-CA gilt A_23139 absichtlich nicht.

Anforderungszweisungen

Tabelle 2: Anforderungszuweisungen

Afo-ID	Afo-Bezeichnung	Zuweisung
A_23139	TSP-X.509-nonQES: ECC-Kurvenparameter, Komplexitätsreduktion	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