Änderung in gemSpec_Krypt

in Kapitel 5.9 ECC-Migration Konnektor

1.1 ECC-Migration Konnektor

~~Die Verpflichtung der Implementierung bestimmter (s. u.) für die ECC-Migration notwendiger Funktionalitäten wird für den PTV4-Konnektor mit Hinblick auf die fristgerechte Umsetzung der ePA zunächst ausgesetzt:~~

- ~~Für die TLS-Schnittstellen, die bereits mit dem PTV3-Konnektor zertifiziert wurden (Schnittstellen zu Kartenterminals, Clientsystemen, Intermediär, zentralen Diensten), wird in PTV4 auf eine verpflichtende ECC-Unterstützung zunächst verzichtet.~~
- ~~Ebenso wird auf die verpflichtende Umsetzung der ECC-Unterstützung an der IPsec/IKE-Schnittstelle zum VPN-Konzentrator zunächst verzichtet.~~

~~Unverändert verpflichtend gefordert wird die ECC-Unterstützung an der Schnittstelle zum ePA-Aktensystem, bei den Karten und für KOM-LE. Insbesondere bedeutet dies, dass ein PTV4-Konnektor auch weiterhin~~

- ~~die TSL(ECC-RSA) prüfen und verwenden muss (vgl. ☐*ML-92906 - Missing cross-reference*),~~
- ~~die Signaturerstellung und -prüfungen auf ECDSA-Basis beherrschen muss (vgl. ☐*ML-92908 - Missing cross-reference*, ☐*ML-93560 - Missing cross-reference*, ☐*ML-92909 - Missing cross-reference*, ☐*ML-93559 - Missing cross-reference*, ☐*ML-92910 - Missing cross-reference* und die VAU-Protokoll und die SGD-Protokoll relevanten Operationen) und~~
- ~~die Ver- und Entschlüsselung über das ECIES-Verfahren (vgl. ☐*ML-92933 - Missing cross-reference* , ☐*ML-92934 - Missing cross-reference* und die Transport-Verschlüsselung innerhalb des SGD-Protokolls mit ☐*ML-94672 - Missing cross-reference*)~~

~~unterstützen muss.~~

~~Werden die SOLL-Anforderungen ☐*ML-92603 - Missing cross-reference* und ☐*ML-100520 - Missing cross-reference* nicht umgesetzt, so ist dies mit einem Firmwareupdate im Jahre 2021 nachzuholen.~~

[A_17094 wird abgelöst durch die Afo A_17094_01, Prüfverfahren: Herstellererklärung und CC-Evaluierung]

A_17094-01 - TLS-Verbindungen Konnektor (ECC-Migration)
Der Konnektor MUSS zusätzlich zu den RSA-basierten TLS-Ciphersuiten (vgl. GS-A_4385 und GS-A_5345) die TLS-Ciphersuiten

1. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 und

2. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

unterstützen. Dabei MÜSSEN bei dem ephemeren Elliptic-Curve-Diffie-Hellman-Schlüsselaustausch die Kurven P-256 und P-384 [FIPS-186-4] und die Kurven brainpoolP256r1 und brainpoolP384r1 (vgl. [RFC-5639] und [RFC-7027]) unterstützt werden. Andere Kurven SOLLEN NICHT verwendet werden.
Falls der Konnektor in der Rolle TLS-Client agiert, so MUSS er die eben genannten Ciphersuiten gegenüber RSA-basierten Ciphersuiten (vgl. GS-A_4384) bevorzugen (in der Liste "cipher_suites" beim ClientHello vorne an stellen, vgl. [RFC-5256#7.4.1.2 Client Hello]).

Kommentiert [DS1]: C_10062

.....

*[**A_18624 wird ganz gestrichen**]*

.....

Hinweis: für den Konnektor gelten die IPsec-Anforderungen A_17125 und A_17126.

A_17209 - Signaturverfahren für externe Authentisierung (ECC-Migration)
Der Konnektor MUSS an der Schnittstelle für die externe Authentisierung die Signaturverfahren RSASSA-PKCS1-v1_5 [PKCS#1], RSASSA-PSS [PKCS#1] und ECDSA [BSI-TR-03111] anbieten.

Änderung in gemILF_PS

Ergänzung in Kapitel 4.1.1.1 Client-Authentisierung (Letzter Absatz)

1.1.1.1 Client-Authentisierung

.....

<PTV4> Ein Konnektor KANN für den Aufbau der TLS-Verbindung zum Primärsystem Verfahren auf Basis von ECC verwenden. Bei Verwendung geeigneter Standardimplementierungen kann der Entwicklungsaufwand für die Unterstützung elliptischer Kurven (Elliptic Curve Cryptography, im Folgenden kurz "ECC") relativ gering sein und womöglich sogar ausschließlich durch Konfigurationsänderungen in Standardimplementierungen ohne Anpassungen am Primärsystem umsetzbar sein. Standardimplementierungen sehen insbesondere eine parallele Unterstützung von RSA-2048 und ECC-256 gemäß [gemSpec_Krypt#5.4 und 5.5] vor, wobei NIST-Kurven verwendet werden dürfen. </PTV4>

<PTV5> Ein Konnektor MUSS für den Aufbau der TLS-Verbindung zum Primärsystem Verfahren auf Basis von ECC verwenden. Bei Verwendung geeigneter Standardimplementierungen kann der Entwicklungsaufwand für die Unterstützung elliptischer Kurven (Elliptic Curve Cryptography, im Folgenden kurz "ECC") relativ gering sein und womöglich sogar ausschließlich durch Konfigurationsänderungen in Standardimplementierungen ohne Anpassungen am Primärsystem umsetzbar sein. Standardimplementierungen sehen insbesondere eine parallele Unterstützung von

RSA-2048 und ECC-256 gemäß [gemSpec_Krypt#5.4 und 5.5] vor, wobei NIST-Kurven verwendet werden dürfen. </PTV5>

Änderungen in gemProdT_Kon_PTV5

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_Kon_PTV5]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehen.

Tabelle 1: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_17124	TLS-Verbindungen (ECC-Migration)	gemSpec_Krypt
A_17125	IKE-Schlüsselaushandlung für IPsec (ECC-Migration)	gemSpec_Krypt
A_17126	IPsec-Kontext -- Verschlüsselte Kommunikation (ECC-Migration)	gemSpec_Krypt
~~A_18624~~	~~Konnektor, IPsec/IKE: optionale ECC-Unterstützung~~	~~gemSpec_Krypt~~

Tabelle 2: Anforderungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_18624~~	~~Konnektor, IPsec/IKE: optionale ECC-Unterstützung~~	~~gemSpec_Krypt~~
A_17094_01	TLS-Verbindungen Konnektor (ECC-Migration)	gemSpec_Krypt
~~A_17094~~		

Tabelle 3: Anforderungen zur funktionalen Eignung "CC-Evaluierung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)

A_17094_01	TLS-Verbindungen Konnektor (ECC-Migration)	gemSpec_Krypt
~~A_17094~~		
A_17124	TLS-Verbindungen (ECC-Migration)	gemSpec_Krypt
A_17125	IKE-Schlüsselaushandlung für IPsec (ECC-Migration)	gemSpec_Krypt
A_17126	IPsec-Kontext -- Verschlüsselte Kommunikation (ECC-Migration)	gemSpec_Krypt
~~A_18624~~	~~Konnektor, IPsec/IKE: optionale ECC-Unterstützung~~	~~gemSpec_Krypt~~

[Hinweis: die Zuordnung von A_17124, A_17125 und A_17126 zu den Prüfverfahren Test und CC-Evaluierung muss noch durchgeführt werden.]