Änderung in gemSpec_Krypt

In Abschnitt 3.3.1 wird geändert:

GS-A_4382-01 - IPsec-Kontext - Schlüsselvereinbarung
Alle Produkttypen, die die Authentifizierung, den Schlüsselaustausch und die verschlüsselte Kommunikation im IPsec-Kontext durchführen, MÜSSEN die Schlüsselvereinbarung mittels IKEv2 [RFC-7296] gemäß den folgenden Vorgaben durchführen:

- Zur Authentisierung MUSS eine Identität mit einem X.509-Zertifikat gemäß [gemSpec_Krypt#GS-A_4360] verwendet werden.
- Für „Hash und URL" MUSS SHA-1 verwendet werden.
- Die Diffie-Hellman-Gruppe Gruppe 14 (definiert in [RFC-3526], verwendbar bis Ende 2023) MUSS für den Schlüsselaustausch unterstützt werden. Zusätzlich KÖNNEN Gruppen aus [BSI-TR-02102-3, Abschnitt 3.2.4, Tabelle 5], bei denen der Verwendungszeitraum ein „+" enthält, verwendet werden.
- Der private DH-Exponent für den Schlüsselaustausch MUSS eine Länge von mindestens 256 Bit haben.
- Die Authentisierung der ephemeren (EC)DH-Parameter erfolgt durch eine Signatur der Parameter durch den jeweiligen Protokollteilnehmer. Bei dieser Signatur MUSS SHA-256 als Hashfunktion verwendet werden. Es SOLL die Authentisierungsmethode „Digital Signature" nach [RFC-7427] dabei verwendet werden.
- Bei den symmetrische Verschlüsselungsalgorithmen MUSS AES mit 256 Bit Schlüssellänge im CBC-Modus unterstützt werden (sowohl für IKE-Nachrichten als auch später für die Verschlüsselung von ESP-Paketen). Es KÖNNEN weitere Verfahren nach [BSI-TR-02102-3, Abschnitt 3.2.1, Tabelle 2] bzw. [BSI-TR-02102-3, Abschnitt 3.3.1, Tabelle 7] verwendet werden.
- Für den Integritätsschutz (sowohl innerhalb von IKEv2 als auch anschließend für ESP-Pakete) MUSS HMAC mittels ~~SHA-1 und~~ SHA-256 (vgl. [gemSpec_Krypt#Hinweis-4382-1]) unterstützt werden. Es KÖNNEN weitere Verfahren nach [BSI-TR-02102-3, Abschnitt 3.2.3, Tabelle 4] bzw. [BSI-TR-02102-3, Abschnitt 3.3.1, Tabelle 8] verwendet werden,andere Verfahren dürfen nicht verwendet werden.
- Als PRF MUSS ~~MÜSSEN PRF_HMAC_SHA1 und~~ PRF_HMAC_SHA2_256 (vgl. [gemSpec_Krypt#Hinweis-4382-1]) unterstützt werden. Es KÖNNEN weitere Verfahren nach [BSI-TR-02102-3, Abschnitt 3.2.2, Tabelle 3] verwendet werden.
- Schlüsselaktualisierung: die IKE-Lifetime darf maximal 24*7 Stunden betragen (Reauthentication). Die IPsec-SA-Lifetime darf maximal 24 Stunden betragen (Rekeying). Der Initiator soll nach Möglichkeit vor Ablauf der Lifetime das Rekeying anstoßen. Ansonsten muss der Responder bei Ablauf der Lifetime das Rekeying von sich aus sicherstellen, bzw. falls dies nicht möglich ist, die Verbindung beenden.
- Für die Schlüsselberechnung muss Forward Secrecy [BSI-TR-02102-1, S.ix] (in [RFC-7296] „Perfect Forward Secrecy" genannt) gewährleistet werden. Meint die Wiederverwendung von zuvor schon verwendeten (EC-)Diffie-Hellman-Schlüsseln ([RFC-7296, Abschnitt 2.12]) ist nicht erlaubt.

<=

~~Hinweis 4382-1: In [NK-PP] wird mit FCS_COP.1/NK.HMAC und FCS_COP.1/NK.Hash die Unterstützung von SHA-1 und SHA-256 gefordert. Da für den Einsatz innerhalb einer HMAC-Funktion und innerhalb einer PRF die Einwegeigenschaft der Hashfunktion im Vordergrund steht und nicht die allgemeine Kollisionsresistenz, ist dort der Einsatz von SHA-1 noch zulässig (vgl. auch [BSI-TR-02102-3, Abschnitt 3.2.2, Tabelle 3, 4 und 8]). Es ist davon auszugehen, dass die Zulässigkeit von SHA-1 bei diesen beiden Einsatzzwecken zukünftig nicht mehr gegeben sein kann, und sowohl im NK als auch im VPN-Zugangsdienst, bspw. per Konfiguration, deaktiviert werden muss.~~

In Abschnitt 3.3.2 wird geändert:

GS-A_4384-01 - TLS-Verbindungen
Alle Produkttypen, die Übertragungen mittels TLS durchführen, MÜSSEN die folgenden Vorgaben erfüllen:

- Zur Authentifizierung MUSS eine X.509-Identität gemäß [gemSpec_Krypt#GS-A_4359] verwendet werden.
- ~~Als Cipher Suite MUSS TLS_DHE_RSA_WITH_AES_128_CBC_SHA oder TLS_DHE_RSA_WITH_AES_256_CBC_SHA verwendet werden.~~
- ~~Es MUSS für die Schlüsselaushandlung Gruppe 14 (definiert in [RFC-3526], verwendbar bis Ende 2023) verwendet werden.~~
- ~~Der private DH-Exponent für den Schlüsselaustausch MUSS eine Länge von mindestens 256 Bit haben.~~
- Als Cipher-Suite MÜSSEN TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 und TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 unterstützt werden.
- Beim ephemeren Elliptic-Curve-Diffie-Hellman-Schlüsselaustausch (vgl. "ECDHE" im Namen der Cipher-Suites) MÜSSEN die Kurven P-256 oder P-384 [FIPS-186-4] unterstützt werden. Es SOLLEN die Kurven brainpoolP256r1 und brainpoolP384r1 (vgl. [RFC-5639] und [RFC-7027]) unterstützt werden. Andere Kurven als in GS-A_4384-* aufgeführt SOLLEN NICHT verwendet werden.
- Es KÖNNEN weitere Cipher-Suiten aus [TR-02102-2, Abschnitt 3.3.1 Tabelle 1] unterstützen.

<=

Erläuterung zu GS-A_4384-*:

In einigen Konstellationen (ePA-FdV auf iOS-Geräten) ist die Verwendung von brainpool-Kurven nur schwer möglich. Dort bedeutet die SOLL-Bestimmung aus GS-A_4384-*, dass es zulässig ist auf die brainpool-Kurven-Unterstützung dort zu verzichten.

A_23226 - TLS-Verbindung, Konnektor: Legacy-KT-Unterstützung
Der Konnektor MUSS für die Unterstützung von alten eHealth-KT folgende TLS-Vorgaben ebenfalls unterstützen:

- Als Cipher Suite MUSS TLS_DHE_RSA_WITH_AES_128_CBC_SHA oder TLS_DHE_RSA_WITH_AES_256_CBC_SHA unterstützt werden.
- Dabei MUSS für die Schlüsselaushandlung Gruppe 14 (definiert in [RFC-3526], verwendbar bis Ende 2023) verwendet werden.
- Der private DH-Exponent für den Schlüsselaustausch MUSS eine Länge von mindestens 256 Bit haben.

[<=]

Die Anforderungen GS-A_5339 und GS-A_5482 werden gestrichen und anstatt GS-A_4384-01 zugewiesen.

GS-A_5345-01 - TLS-Verbindungen Konnektor
Der Konnektor MUSS für die TLS gesicherten Verbindungen neben den in [gemSpec_Krypt#GS-A_4384] aufgeführten Ciphersuiten folgende Vorgaben umsetzen:

1. Der Konnektor MUSS zusätzlich folgende Ciphersuiten unterstützen:
   - ~~TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC0, 0x13),~~
   - ~~TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC0, 0x14),~~
   - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC0, 0x27),
   - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC0, 0x28),
   - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2f) und
   - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x30).
1. Der Konnektor KANN weitere Ciphersuiten aus [TR-02102-2, Abschnitt 3.3.1 Tabelle 1] unterstützen.
2. Falls Ciphersuiten aus Spiegelstrich (1) oder (2) unterstützt werden,
   a. MÜSSEN bei dem ephemeren Elliptic-Curve-Diffie-Hellman-Schlüsselaustausch die Kurven P-256 oder P-384 [FIPS-186-4] unterstützt werden,
   b. MÜSSEN die Kurven brainpoolP256r1 und brainpoolP384r1 (vgl. [RFC-5639] und [RFC-7027]) unterstützt werden.

Andere Kurven SOLLEN NICHT verwendet werden.

1. Falls Ciphersuiten aus (1) oder (2) unterstützt werden, so MÜSSEN diese im CC-Zertifizierungsverfahren berücksichtigt werden.

<=

In Abschnitt 5.4 wird geändert:

A_17124-01 - TLS-Verbindungen (ECC-Migration)
Alle Produkttypen, die Übertragungen mittels TLS durchführen, MÜSSEN die folgenden Vorgaben erfüllen:

1. Zur Authentifizierung MUSS eine X.509-Identität gemäß [gemSpec_Krypt#GS-A_4359] verwendet werden.
2. Als Ciphersuiten MÜSSEN TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xC0,0x2B) und TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xC0,0x2C) unterstützt werden.
3. Falls der Produkttyp in der Rolle als TLS-Client agiert, so MUSS er die eben genannten Ciphersuiten gegenüber evtl. ebenfalls von ihm unterstützen RSA-basierte Ciphersuiten (vgl. GS-A_4384) bevorzugen (in der Liste "cipher_suites" beim ClientHello vorne an stellen, vgl. [RFC-5246#7.4.1.2 Client Hello]).

4. Beim ephemeren Elliptic-Curve-Diffie-Hellman-Schlüsselaustausch (vgl. "ECDHE" im Namen der Cipher-Suites) MÜSSEN die Kurven P-256 oder P-384 [FIPS-186-4] unterstützt werden. Es SOLLEN die Kurven brainpoolP256r1 und brainpoolP384r1 (vgl. [RFC-5639] und [RFC-7027]) unterstützt werden. Andere Kurven als in A_17124-* aufgeführt SOLLEN NICHT verwendet werden.
5. ~~Als Basis für den ephemeren ECDH MÜSSEN die Kurven brainpoolP256r1 und brainpoolP384r1 (vgl. [RFC-5639] und [RFC-7027]) unterstützt und verwendet werden.~~

<=

In Abschnitt 5.8 wird geändert:

A_17089-01 - eHealth-Kartenterminals: TLS-Verbindungen (ECC-Migration)
Ein eHealth-Kartenterminal MUSS prüfen, ob die in ihm gesteckte SMC-KT für die TLS-Verbindung zum Konnektor eine RSA-basierte Identität (AUT) und/oder eine ECDSA-basierte Identität besitzt (vgl. [gemSpec_gSMC-KT_ObjSys_G2.1], bspw. jeweils EFs mit ShortFileIdentifier 1 und 4 prüfen).
Falls eine RSA-basierte Identität dort vorhanden ist, so MUSS das eHealth-Kartenterminal folgende TLS-folgende Vorgaben erfüllen:

1. Als Cipher-Suite MÜSSEN TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 und TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 unterstützt werden.
2. Beim ephemeren Elliptic-Curve-Diffie-Hellman-Schlüsselaustausch (vgl. "ECDHE" im Namen der Cipher-Suites) MÜSSEN die Kurven P-256 oder P-384 [FIPS-186-4] unterstützt werden. Es SOLLEN die Kurven brainpoolP256r1 und brainpoolP384r1 (vgl. [RFC-5639] und [RFC-7027]) unterstützt werden. Andere Kurven als in A_17089-* aufgeführt SOLLEN NICHT verwendet werden.
3. Es KÖNNEN weitere Cipher-Suiten aus [TR-02102-2, Abschnitt 3.3.1 Tabelle 1] unterstützen.
4. ~~Als Ciphersuiten MÜSSEN TLS_DHE_RSA_WITH_AES_128_CBC_SHA und TLS_DHE_RSA_WITH_AES_256_CBC_SHA unterstützt werden.~~
5. ~~Es MUSS dabei für die Schlüsselaushandlung Gruppe 14 (definiert in [RFC-3526], verwendbar bis Ende 2023) unterstützt und verwendet werden.~~
6. ~~Der private ephemere DH-Exponent für den Schlüsselaustausch MUSS eine Länge von mindestens 256 Bit haben.~~

Falls eine ECDSA-basierte Identität vorhanden ist, so MUSS das eHealth-Kartenterminal zusätzlich folgende Vorgaben erfüllen:

1. Als Ciphersuiten MÜSSEN TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xC0,0x2B) und TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xC0,0x2C) unterstützt werden.
2. Beim ephemeren Elliptic-Curve-Diffie-Hellman-Schlüsselaustausch (vgl. "ECDHE" im Namen der Cipher-Suites) MÜSSEN die Kurven P-256 oder P-384 [FIPS-186-4] unterstützt werden. Es SOLLEN die Kurven brainpoolP256r1 und brainpoolP384r1 (vgl. [RFC-5639] und [RFC-7027]) unterstützt werden. Andere Kurven als in GS-A_17089-* aufgeführt SOLLEN NICHT verwendet werden.
3. ~~Als Basis für den ephemeren ECDH MUSS die Kurve brainpoolP256r1 und brainpoolP384r1 (vgl. [RFC-5639] und [RFC-7027]) unterstützt und verwendet werden.~~

Dies bedeutet, falls beide Identitäten auf der SMC-KT vorhanden sind (wie bei [gemSpec_gSMC-KT_ObjSys_G2.1]), so MÜSSEN alle vier oben genannten Ciphersuiten unterstützt werden.
<=

In Abschnitt 3.16 wird der informative Text wie folgt geändert:

Hinweis: GS-A_4384-01 ~~(TLS_DHE_RSA_WITH_AES_128_CBC_SHA etc.)~~ ist absichtlich nicht den Produkttypen der E-Rezept-Anwendung zugewiesen. Die Interoperabilität zu den Konnektoren ist mindestens über die ersten beiden Cipher-Suiten aus A_21332 (1) sichergestellt, ebenfalls über A_17094-*.

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: Anforderungszuweisungen

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_5339		Die Anforderungen GS-A_5339 und GS-A_5482 werden gestrichen und anstatt GS-A_4384-01 zugewiesen.
GS-A_5482		Die Anforderungen GS-A_5339 und GS-A_5482 werden gestrichen und anstatt GS-A_4384-01 zugewiesen.
A_23226		wird dem PTV5-Konnektor zugewiesen. (Herstellererklärung: funktionale Eignung, Common Criteria Sicherheitszertifizierung)

Abbildung 1: xxx