
C_12004_Anlage

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	3
2 Änderung in gemSpec_Krypt.....	4
2.1.1 Anpassung für diesen Absatz und AFO in 3.3.2 "TLS-Verbindungen".....	5
3 Änderungen in Steckbriefen.....	6
3.1 Änderungen in gemProdT_PoPP_Service_PTV.....	6

1 Änderungsbeschreibung

~~Der PoPP-Service wird vorübergehend unter Ersatzvornahme für einen VSDM1-Betreiber die Prüfziffer im Kontext der TI 2.0 erstellen. Dazu wird er als weiterer Betreiber einen HMAC-Schlüssel generieren. Sobald der Anbieter des PoPP-Service diese Funktionalität bereitstellt, gelten für ihn ebenfalls die Anforderungen zur sicheren Aufbewahrung, Übermittlung und Verarbeitung des HMAC-Schlüssels. Die Anforderungen im Kapitel 3.18 "HMAC-Sicherung der Prüfziffer VSDM" werden für den Anbieter des PoPP-Services angepasst.~~

Aufgrund der Einführung der VSDM Prüfziffer Version 2 entfällt der ursprünglich geplante Migrationspfad, der den VSDM-PN als optionalen Teil der Token Response vorsah. Die entsprechenden Anforderungen werden daher aus den Spezifikationen entfernt. Es verbleibt lediglich eine Ergänzung im Kapitel 3.3.2 „TLS-Verbindungen“, die die TLS-Strecken zwischen dem PoPP-Service und dem PoPP-Client bzw. PoPP-Modul betrifft.

2 Änderung in gemSpec_Krypt

Im Kapitel 3.1.8 werden die Anforderungen [A_23460], [A_23461], [A_23463] durch die neuen Anforderungen [A_23460-01], [A_23461-01], [A_23463-01] ersetzt.

storniert: A_23460-01

A_23460-01 -VSDM- und PoPP-Service-Betreiber: HMAC-Schlüsselerzeugung

Ein Betreiber eines VSDM-Dienstes oder des PoPP-Services MUSS den HMAC-Sicherungsschlüssel für die kryptographische Sicherung der VSDM-Prüfziffern zufällig mit einer Länge von 256 Bit (= 32 Byte) und einer Mindestentropie von 120 Bit erzeugen. [\leq ,,]

storniert: A_23461-01

A_23461-01 -VSDM- und PoPP-Service-Betreiber: HMAC-Verfahren

Ein Betreiber eines VSDM-Dienstes oder des PoPP-Services MUSS für die HMAC-Sicherung der VSDM-Prüfziffern das HMAC-Verfahren aus [RFC2104] mit der Hashfunktion [SHA-256] (also nicht wie im RFC beschrieben mittels SHA-1) verwenden. Für das dabei zu verwendende geheime Schlüsselmaterial gilt [A_23460-*]. [\leq ,,]

storniert: A_23463-01

A_23463-01 -VSDM- und PoPP-Service-Betreiber: verschlüsselter Export des HMAC-Schlüssels für die E-Rezept-VAU

Ein Betreiber eines VSDM-Dienstes oder des PoPP-Services MUSS den HMAC-Sicherungsschlüssel mittels des ECIES-Verfahrens [SEC1-2009] für den Export an den E-Rezept-FD oder ein ePA-Aktensystem verschlüsseln und dabei folgende Vorgaben umsetzen

1. Er MUSS ein ephemeres ECDH-Schlüsselpaar erzeugen und mit diesem und dem VAU-Schlüssel aus [A_20160-*] ein ECDH gemäß [NIST-800-56-A] durchführen. Das somit erzeugte gemeinsame Geheimnis ist Grundlage für die folgende Schlüsselableitung.
2. Als Schlüsselableitungsfunktion MUSS er die HKDF nach [RFC5869] auf Basis von SHA-256 verwenden.
3. Dabei MUSS er den Ableitungsvektor "ecies-vau-transport" verwenden, d. h. in der Formulierung von [RFC5869] info="ecies-vau-transport" .
4. Er MUSS mit dieser Schlüsselableitung einen AES-128-Bit Content-Encryption-Key für die Verwendung von AES/GCM ableiten.
5. Er MUSS für Verschlüsselung mittels AES/GCM einen 96 Bit langen IV zufällig erzeugen.
6. Er MUSS mit dem CEK und dem IV mittels AES/GCM den HMAC-Sicherungsschlüssel verschlüsseln, wobei dabei ein 128 Bit langer Authentication-Tag zu verwenden ist.
7. Er MUSS das Ergebnis wie folgt kodieren: chr(0x01) || <32 Byte X-Koordinate von öffentlichen Schlüssel aus (a) > || <32 Byte Y-Koordinate> || <12 Byte IV> || <AES-GCM-Chiffre> || <16 Byte AuthenticationTag> (vgl. auch Tab_KRYPT_ERP und folgende die Beispielschlüsselung).
Die Koordinaten sind (wie üblich) vorne mit chr(0) zu paden solange bis sie eine Kodierungslänge von 32 Byte erreichen.

[\leq ,,]

2.1.1 Anpassung für diesen Absatz und AFO in 3.3.2 "TLS-Verbindungen"

Gleiches gilt für die Verwendung von TLS für die Anbindung von Leistungserbringernetzen an das TI-Gateway, da bei dieser VPN-Anbindung Client und Server Teil desselben Produkttyps sind (TI-Gateway-Zugangsmodul), sowie für die TLS-Verbindungen zwischen PoPP-Client bzw. -Modul zum PoPP-Service.

A_24779-02 -PoPP, TI-Gateway-Zugangsmodul und eHealth-CardLink - TLS-Cipher-Suiten

Die im Folgenden genannten Komponenten MÜSSEN ausschließlich TLS-Cipher-Suiten aus [TR-02102-2, Abschnitt 3.3.1 Tabelle 1] mit den dort vorgegebenen Domainparametern (Schlüssellänge, ECC-Kurven-Parameter etc.) verwenden bzw. bei Verwendung von TLS 1.3 die Vorgaben aus [TR-02102-2, Abschnitt 3.4] befolgen:

1. TI-Gateway Zugangsmodul, falls das TLS-Protokoll für die Sicherung der Datenübertragung aus dem Nutzernetzwerk zum Zugangsmodul des TI-Gateway verwendet wird,
2. PoPP-Service,
3. PoPP-Client,
4. PoPP-Modul,
5. eHealth-Cardlink, für die Verbindung der Clients eines Nutzers zum eHealth-Cardlink

[<=,PoPP_Client, PoPP_Modul, eHealth-CardLink, PoPP_Service, TI_GW_Zugangsmodul,Sich.techn. Eignung: Produktgutachten, Sich.techn. Eignung: Herstellererklärung]

3 Änderungen in Steckbriefen

3.1 Änderungen in gemProdT_PoPP_Service_PTV

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

Die geänderten Anforderungen der geSpec_Krypt wirken auf den neue Produkttyp PoPP_Service.

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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_24779-02	PoPP, TI-Gateway-Zugangsmodul und eHealth-CardLink - TLS-Cipher-Suiten	gemSpec_Krypt; Kap. 3.3.2