In gemSpec_Krypt#A_25192 wird geändert:

Ein Aktensystem MUSS sicherstellen, dass in einer VAU-Instanz bei jeder Nutzer-Authentisierung (i. S. v. egal ob über A_24568-* oder A_25055-*) eines ePA-Nutzers, bei der der Nutzer die Telematik-ID ~~"9-E_Rezept_Fachdienst"~~ "9-E-Rezept-Fachdienst" besitzt, [...]

In gemSpec_Krypt wird im Literaturverzeichnis hinzugefügt:

[RFC-CBOR]	**RFC-8949: Concise Binary Object Representation (CBOR), C. Bormann, P. Hoffman, December 2020** **https://datatracker.ietf.org/doc/html/rfc8949**

In gemSpec_Krypt#3.15.3 wird ein informativer Hinweis, der ab ePA 3.0 nicht mehr gilt, gestrichen:

~~Es gibt ePA-Aktensysteme deren Access Gateway [gemSpec_Aktensystem_ePAfuerAlle] die Verwendung von TLS-Session-Resumption per Session-ID von einem ePA-FdV verlangen. Ebenfalls gibt es ePA-Aktensysteme deren Access Gateway die Verwendung von TLS-Session-Resumption per Session-Tickets von einem ePA-FdV verlangen. Nach einem TLS-Verbindungsende muss ein ePA-FdV eine TLS-Session-Resumption verwenden, ansonsten muss der Versicherte sich neu authentisieren (erneuter Login).~~

~~Ein ePA-FdV muss, um die beiden Anwendungsfälle (1) Aktensystemwechsel und (2) Versicherten-Vertreter über ein ePA-FdV eines anderen Aktensystemherstellers zu ermöglichen, beide Varianten der TLS-Session-Resumption unterstützen. Die meisten TLS-Bibliotheken unterstützen beide Varianten per Defaul~~t.

In gemSpec_Krypt#A_24624 wird geändert zu

A_24624-01 VAU-Protokoll: VAU-Client: Prüfung der "signierten öffentlichen VAU-Schlüssel"
Ein VAU-Client MUSS die "signierten öffentlichen VAU-Schlüssel" (vgl. A_24425-*) bei der Verarbeitung von Nachricht 3 (vgl. A_24623-*) wie folgt prüfen. Hat er bei einem der folgenden Prüfpunkte kein positives Prüfergebnis, MUSS er die Verarbeitung (Handshake) abbrechen.

1. Prüfung des TI-Zertifikats ~~aus dem "cert"-Feld~~, das den Hashwert aus dem "cert_hash"-Datenfeld besitzt (Bezug des Zertifikats vgl. A_24957-*), u. a. unter der Verwendung der OCSP-Response aus "ocsp_response" für die Prüfung des Sperrstatus (Prüfung ob "good"). Die OCSP-Response darf dabei nicht älter als 24 Stunden sein.
2. Das VAU/TI-Zertifikat MUSS zeitlich gültig sein. Es MUSS kryptographisch in einer Zertifikats-/Signaturprüfungskette rückführbar auf eine X.509-Root-Version der TI-PKI sein.
3. Das TI-Zertifikat MUSS aus der ~~aus der~~ Komponenten-PKI der TI stammen und die Rollen-OID "oid_epa_vau" besitzen.
4. Die Signatur im "signature-ES256"-Datenfeld MUSS eine valide Signatur für die Daten im Datenfeld "signed_pub_keys" (Signaturprüfung ergibt "valid/accept") sein, unter Verwendung des öffentlichen Signatur-Schlüssels aus dem VAU/TI-Zertifikats bei der Signaturprüfung.

5. Der ECC-Schlüssel in signed_pub_keys (vgl. Erzeugung bei A_24425) MUSS ein gültiger Punkt der Kurve P-256 [FIPS-186-5] sein. Der öffentliche Schlüssel in "Kyber768_PK"-Datenfeld MUSS ein gültiger Kyber-768-Schlüssel [IEFT-Kyber] sein.
6. Die Zeit in "signed_pub_keys.exp" MUSS größer als die aktuelle Systemzeit (Seconds since epoch) sein, d. h. die beiden Schlüssel (ECDH_PK und Kyber768_PK) sind noch zeitlich gültig.

[<=]

In gemSpec_PKI wird in Kapitel 5.9.3.4. unterhalb des Afo A_15591-01 der folgende Hinweis-Text angepasst:

**Hinweis zur Telematik-ID: Für den eRezept-Fachdienst wird eine Telematik-ID verwendet, die die gematik vorgibt in der Form (Beispiel): "9-E-Rezept-Fachdienst"*

© gematik – öffentlich_Entwurf