Änderung in gemSpec_IDP_Sek

Es wird in Kapitel "4.3.2 Authentifizierungsverfahren" neu aufgenommen:

Neu:

A_22867 - Signalisierung der Verwendung von Authentisierungsverfahren "gematik-ehealth-loa-substantial" beim Zugriff auf Daten mit hohem Schutzbedarf

Der sektorale IDP MUSS den claim `amr` auf den Wert "urn:telematik:auth:mEW" setzen, wenn der Fachdienst eine Authentifizierung des Nutzers auf dem Niveau "gematik-ehealth-loa-high" angefragt hat, der Nutzer jedoch ein Authentisierungsverfahren auf dem Niveau "gematik-ehealth-loa-substantial" verwendet hat. Die Einwilligung des Anwenders zur Nutzung dieses Verfahrens zum Zugriff auf Daten mit hohem Schutzbedarf MUSS vorliegen. **[<=]**

[WI1][AH2] [ES3][AH4] [KJ5][AH6][ES7]

Neu:

A_23103 - Einwilligung zur Verwendung von Authentisierungsverfahren "gematik-ehealth-loa-substantial" beim Zugriff auf Daten mit hohem Schutzbedarf

Vor der Aktivierung der Einwilligungssignalisierung nach A_22867 MUSS der sektorale IDP sicherstellen, dass die Einwilligung des Nutzers vollständig freiwillig erfolgt. Dabei müssen sicherere Verfahren hervorgehoben und die Möglichkeit des Widerrufs der Einwilligung aufgezeigt werden. Der Nutzer muss insbesondere über die Risiken einer Absenkung des Vertrauensniveaus aufgeklärt werden und der Verwendung der gewählten Authentifizierungsverfahren zum Zugriff auf Daten mit hohem Schutzbedarf aktiv zustimmen.**[<=]**

[WI8][AH9] [OB10][AH11] [KJ12][AH13]

Hinweis: Die Hersteller der sektoralen IDP werden zusammen mit der gematik einen Text [OB14][AH15] abstimmen, welcher für alle Identity Provider gilt.

Neu:

A_25248 - Protokollierung der Einwilligung zur Verwendung von Authentisierungsverfahren "gematik-ehealth-loa-substantial"

Der sektorale IDP MUSS die Einwilligung des Nutzers zur Verwendung des Authentisierungsverfahrens "gematik-ehealth-loa-substantial" protokollieren.**[<=]**

Hinweis: Das Protokoll wird ggf. für Audits verwendet.

Alt:

A_22236 - Auskunft an Versicherten

Neu:

A_22236-01 - Auskunft an Versicherten

Der Anbieter des sektoralen Identity Provider MUSS dem Versicherten auf dessen Verlangen Auskunft geben über:

- erfolgte Zugriffe auf das elektronische Authentisierungsmittel ~~Identifizierungsmittel~~ des Versicherten ~~und~~
- Änderungen der Authentifizierungsfaktoren des Versicherten~~.~~
- Einwilligungzur Verwendung des Authentisierungsverfahrens "gematik-ehealth-loa-substantial"

[<=]

Alt:

A_23129-01- Identifikation des Authentifizierungsverfahren

Neu:

A_23129-03 - Identifikation des Authentifizierungsverfahren
Der sektorale Identity Provider MUSS den claim `amr` im `ID_TOKEN` entsprechend dem durchgeführten Authentisierungsverfahren nach folgender Tabelle belegen.

Tabelle 1: Codierung der Authentisierungsverfahren

Authentifizierungsverfahren	**Wert des `amr` Claim**	**zulässiges Niveau `(acr)`**
Authentifizierung mittels eGK und PIN	urn:telematik:auth:eGK	gematik-ehealth-loa-high
Authentifizierung mittels elektronischem Identitätsnachweis (Online-Ausweisfunktion)	urn:telematik:auth:eID	gematik-ehealth-loa-high
Authentisierungsverfahren mit Einwilligung für ein Single-Sign-On (SSO)	urn:telematik:auth:sso	gematik-ehealth-loa-high
Authentisierungsverfahren mit Einwilligung zum Zugriff auf Daten mit hohem Schutzbedarf	urn:telematik:auth:mEW	gematik-ehealth-loa-substantial
Anderes Authentisierungsverfahren	urn:telematik:auth:other	gematik-ehealth-loa-high und gematik-ehealth-loa-substantial

[<=]

[ES16][AH17]

Es wird in Kapitel "4.3.2.1 Gerätenutzung" geändert:

Die unterschiedliche Ausstattung der mobilen Geräte erfordert unterschiedliche Anforderung hinsichtlich der Authentifizierungsverfahren. Unterschieden werden:

- ~~Geräte ohne Hardware Keystore~~
- ~~Geräte mit Hardware Keystore~~
- ~~Geräte mit zertifiziertem Secure Element.~~
- Geräte mit Software Keystore
- Gerät mit Trusted Execution Environment (TEE) Keystore
- Gerät mit Tamper-Resistant Hardware (TRH) Keystore
- Gerät mit zertifizierter Tamper-Resistant (TRH) Keystore

Das Vorhandensein einer TEE / ~~eines Hardware Keystore~~ TRH wird hierbei wie folgt definiert:

- Apple (TRH) - Entscheidend ist das Vorhandensein eines "Secure Enclave" [support.apple.com/guide/security]. Diese ist Bestandteil der A7 und neueren Chips von Apple. Die A7 Serie wurde erstmals 2013 mit dem iPhone 5s eingeführt.
- Android (TEE/TRH) - Ab Android 9 gibt es den Systemaufruf [KeyInfo#getSecurityLevel()], um die Speicherung eines Schlüssels ~~im Hardware Keystore abzufragen. Die Rückgabewerte~~ in TEE/TRH abzufragen. Folgende Rückgabewerte sind zulässig:
  - `KeyProperties.SECURITY_LEVEL_TRUSTED_ENVIRONMENT`~~,~~ für TEE
  - `KeyProperties.SECURITY_LEVEL_UNKNOWN_`~~SECURE oder~~ `SECURE` für TEE
  - `KeyProperties.SECURITY_LEVEL_STRONGBOX` ~~sind zulässig.~~ für TRH
- Ältere Systeme bieten die Schnittstelle [KeyInfo#isInsideSecureHardware()] an. Hier ist der Rückgabewert `true` für TEE zulässig. Eine TRH lässt sich hiermit nicht eindeutig nachweisen.

Alt:

A_22750 - Gerätebindung und Authentisierung für gematik-ehealth-loa-high

Abhängig von der Geräteausstattung des Nutzers ist eine Gerätebindung für einen festgelegten Zeitraum ohne Erneuerung gültig. Der Anbieter des sektoralen IDP MUSS, wenn er eine Gerätebindung im Rahmen eines Authentisierungsverfahren nutzt, die Zeitrahmen der Gültigkeit für die Gerätebindung gemäß Tabelle "*Übersicht Gerätebindung*" berücksichtigen. Die Gerätebindung MUSS durch den Nutzer nach Ablauf dieser Frist dementsprechend erneuert werden.
Der Anbieter des sektoralen IDP MUSS, mit den zur Verfügung stehende Plattformmechanismen, einen kryptographischen Nachweis der Gerätebindung auf dem Endgerät erzeugen und auf Serverseite prüfen (z.B. Android: Key & ID Attestation; iOS: DCAppAttestService).
Das Vertrauensniveau einer Gerätebindung als Authentisierungsfaktor entspricht dem für die Einrichtung verwendeten Verfahren.

Tabelle 2: Übersicht Gerätebindung für gematik-ehealth-loa-high

Gerätenutzung	Authentisierung
ohne Hardware Keystore	Die Gerätebindung kann a) durch Identifikation, welche dem Niveau "gematik-ehealth-loa-high" entspricht oder b) mit einer 2FA, welche dem Niveau "gematik-ehealth-loa-high" entspricht, angelegt werden. Die Gerätebindung kann für 24 Stunden zusammen mit einem Faktor aus den Bereichen Wissen oder Inhärenz auf dem Niveau "gematik-ehealth-loa-high" genutzt werden.
mit Hardware Keystore	Die Gerätebindung kann a) durch Identifikation, welche dem Niveau "gematik-ehealth-loa-high" entspricht oder b) mit einer 2FA, welche dem Niveau "gematik-ehealth-loa-high" entspricht, angelegt werden. Die Gerätebindung kann für 6 Monate zusammen mit einem Faktor aus den Bereichen Wissen oder Inhärenz auf dem Niveau "gematik-ehealth-loa-high" genutzt werden.
mit zertifiziertem Secure Element	Die Gerätebindung kann a) durch Identifikation, welche dem Niveau "gematik-ehealth-loa-high" entspricht oder b) mit einer 2FA, welche dem Niveau "gematik-ehealth-loa-high" entspricht, angelegt werden. Die Gerätebindung kann unbegrenzt zusammen mit einem Faktor aus den Bereichen Wissen oder Inhärenz auf dem Niveau "gematik-ehealth-loa-high" genutzt werden.

[<=]

Neu:

A_22750-01 - Schlüsselspeicher und Gerätebindung

Abhängig von der Ausstattung des Geräts des Nutzers ist eine Gerätebindung für einen festgelegten Zeitraum ohne Erneuerung gültig. Der Anbieter des sektoralen IDP MUSS die Zeitrahmen der Gültigkeit für die Gerätebindung gemäß Tabelle *"Übersicht Gerätebindung"* einhalten, wenn er eine Gerätebindung im Rahmen eines Authentisierungsverfahrens nutzt. Der Anbieter des sektoralen IDP MUSS sicherstellen, dass nach Ablauf dieser Frist die Gerätebindung durch den Nutzer erneuert wird.

Der Anbieter des sektoralen IDP MUSS mit den verfügbaren Plattformmechanismen einen kryptographischen Nachweis der Gerätebindung auf dem Endgerät erzeugen und auf Serverseite prüfen (z.B. Android: Key & ID Attestation; iOS: DCAppAttestService).
Die Gerätebindung wird als Authentisierungsfaktor genutzt und ihr Vertrauensniveau entspricht dem für die Einrichtung verwendeten Verfahren.

Tabelle 3: Schlüsselspeicher und Gerätebindung

Schlüsselspeicher	**Gültigkeit der Gerätebindung**
Software Keystore	"gematik-ehealth-loa-high" - 24 Stunden "gematik-ehealth-loa-substantial" - 24 Stunden
Trusted Execution Environment (TEE) Key Store	"gematik-ehealth-loa-high" - 12 Monate "gematik-ehealth-loa-substantial" - 24 Monate
Tamper-Resistant Hardware (TRH) Keystore	"gematik-ehealth-loa-high"- 24 Monate "gematik-ehealth-loa-substantial" - unbegrenzt
zertifizierter Tamper-Resistant Hardware (TRH) Keystore	"gematik-ehealth-loa-high"- unbegrenzt "gematik-ehealth-loa-substantial" - unbegrenzt

[<=]

[KJ18][AH19] [KJ20][AH21]~~[KJ22][AH23]~~ [KJ24][AH25][ES26][AH27]

~~*Hinweis: Die Überprüfung, zu welcher der in der Tabelle aufgeführten Kategorien das Gerät mit dem Authenticator-Modul gehört, kann im Authenticator-Modul selbst erfolgen oder alternativ beim sektoralen IDP durch Übermittlung der notwendigen Informationen vom Authenticator-Modul an den sektoralen IDP. Die Überprüfung der in der Tabelle je Kategorie genannten Gültigkeitszeiträume für eine Gerätebindung erfolgt beim sektoralen IDP.*~~

~~*Hinweis: In der Praxis erlaubt dieses Vorgehen primär die Nutzung von nicht zertifizierten Hardware-Keystores für eine Authentisierung auf dem formalen Sicherheitsniveau "gematik-ehealth-loa-high".*~~

~~*Hinweis: Die Tabelle "Übersicht Gerätebindung für gematik-ehealth-loa-high" weicht ab von der Anforderung A_23025. Die Kriterien für die in der Tabelle angegebene Gerätebindung genügen der Verwendung als Authentisierungsfaktor für "gematik-ehealth-loa-high" und der in A_23025 geforderten Angriffswiderstand muss nicht nachgewiesen werden.*~~

Hinweis 1: Eine Tamper-Resistant Hardware (TRH) ist ein spezialisierter Chip bzw. ein spezialisierter Bereich eines Chips, der durch physische Schutzmaßnahmen gehärtet und isoliert ist, um die Kompromittierung von in ihm gespeicherten kryptographischen Schlüsselmaterials zu verhindern bzw. stark zu erschweren.

Unter diese [KJ28][AH29]Definition einer TRH fallen u.a. (embedded) Secure Elements ((e)SE), Trusted Platform Modules (TPM), Hardware-Sicherheitsmodule (HSM), (embedded) Universal Integrated Circuit Card ((e)UICC), Apple Secure Enclave und Android Strongbox.

Hinweis 2: Als zertifiziert gilt ein TRH, wenn Hard- und Firmware über eine der folgenden Zertifizierungen verfügen:

- *die eine Resistenz gegen ein moderates Angriffspotential nachweißt (z.B. Common Criteria EAL4 mit AVA_VAN.4)*
- *FIPS 140-2 Level 3 oder FIPS 140-3 mit Physical Security Level >= 3*
- *FIDO Authenticator Certification >= Level 2 (L2)*

Hinweis 3: Der Nachweis über eine Zertifizierung der TRH eines Gerätes mit einem definierten Android-OS bzw. Apple-iOS kann in Form einer Herstellererklärung des Geräteherstellers oder durch geeignete technische Nachweise (z.B. "Google Play Protection Zertifizierung" als Nachweis der Einhaltung der Android CDD) erfolgen.

Neu:

A_23699 - Erstellung oder Erneuerung einer Gerätebindung an eine Nutzeridentität
Der Anbieter des sektoralen IDP MUSS zur Erstellung oder Erneuerung der Gerätebindung eine Identifizierung oder Authentifizierung des Nutzers auf dem Vertrauensniveau "gematik-ehealth-loa-high" durchführen. Die Nutzung einer bestehenden Gerätebindung zur Erneuerung einer Gerätebindung an eine Nutzeridentität ist gemäß A_25138 ausgeschlossen.**[<=]**

[KJ30][AH31] [ES32][AH33] [WI34][KK35]

Hinweis 1: Eine Liste der zugelassenen Identifikationsverfahren ist von der gematik im Fachportal [Zulässigkeit von Identifikationsverfahren] veröffentlicht und wird regelmäßig aktualisiert.

Hinweis 2: Zulässige Authentifizierungsverfahren sind eGK+PIN sowie die Online-Ausweisfunktion.

Neu:

A_23701 - Verwendung von Biometrie als Faktor zur Nutzerauthentifizierung
Der Anbieter des sektoralen IDP MUSS für die Nutzung von Biometrie-Sensoren zur Nutzerauthentifizierung, die in der Tabelle "Biometrie" aufgeführten Einschränkungen berücksichtigen. Für die Nutzung eines biometrischen Faktors MUSS die Einwilligung des Nutzers gemäß A_23103 vorliegen.

Tabelle 4: Biometrie

Nutzung der biometrischen Sensoren der mobilen Plattformen als biometrischer Faktor
Biometrie iOS (FaceID, TouchID) - uneingeschränkt nutzbar

Nutzung der biometrischen Sensoren der mobilen Plattformen als biometrischer Faktor
Biometrie Android - Nutzung eingeschränkt auf die Erfüllung Biometric.STRONG oder Class-3

[<=]

[KJ36][AH37] [ES38][AH39] [ES40][AH41] [WI42][KK43][AH44]

Hinweis: Biometrie Android Definitionen -
siehe https://source.android.com/docs/security/features/biometric?hl=de

Änderung in gemSpec_IDP_FD

Es wird das Kapitel 4.2 Übergreifende Festlegungen erweitert

Neu:

A_23202-01 - Akzeptanz der Einwilligung zur Verwendung von Authentisierungsverfahren "gematik-ehealth-loa-substantial" beim Zugriff auf Daten mit hohem Schutzbedarf
Fachdienste der TI-Föderation MÜSSEN auch bei Authentisierung auf dem Niveau "gematik-ehealth-loa-substancial" den Zugriff auf Daten mit hohem Schutzbedarf gewähren, wenn der`amr` des ID_TOKEN auf "urn:telematik:auth:mEW" gesetzt ist und der Nutzer somit der Verwendung dieses Verfahrens für den Zugriff auf Daten mit hohem Schutzbedarf zugestimmt hat.**[<=]**

[WI45][AH46]

Neu:

A_23030 - Erzwingen einer Authentisierung des Nutzers
Fachdienste der TI-Föderation KÖNNEN eine Benutzerauthentifizierung auch dann erzwingen, wenn mögliche Single-Sign-On-Mechanismen durch den sektoralen IDP unterstützt werden, indem gemäß https://openid.net/specs/openid-connect-core-1_0.html#AuthorizationRequest entsprechende Parameter im Pushed Authorization-Request gesetzt werden.**[<=]**

[ES47][AH48][WI49][AH50][WI51]

Hinweis: Beispielsweise kann die Relying Party über den Parameter prompt=login oder über den Parameter max_age=0 signalisieren, dass der Nutzer sich erneut authentifizieren muss. Verpflichtende Parameter, die sich daraus ergeben (z.B. auth_time), müssen gemäß https://openid.net/specs/openid-connect-core-1_0.html berücksichtigt werden.