C_12922_Anlage - Sekt. IDP - Weitere Anforderungen an Integration der EUDI-Wallet

Inhaltsverzeichnis

1 Änderungsbeschreibung....2

2 Änderung in gemSpec_IDP_Sek....3

3 Änderungen in Steckbriefen....7

3.1 Änderungen in gemProdT_IDP-Sek_KTR_PTV....7

3.2 Änderungen in gemAnbT_IDP-Sek_ATV....7

1 Änderungsbeschreibung

Aus den Ergebnissen des PoC und aus dem Fortschritt der Entwicklung der deutschen EUDI Wallet sind normative Anforderungen an die sekt. IDPs abzuleiten.
Die Anforderungen sind zu formulieren und abzustimmen. Die neuen Anforderungen sollen mit Release IDP_26_2 veröffentlicht werden.

2 Änderung in gemSpec_IDP_Sek

Es wird Kapitel "4.4.1 Identifikation des Nutzers" wie folgt angepasst:

Alt:

A_22865-01 - Verpflichtende Verfahren zur Identifikation von Nutzern
Der Anbieter des sektoralen IDP MUSS einen Prozess zur Identifikation von Nutzern mit mindestens diesen Identifikationsverfahren zur Nutzeridentifikation anbieten:

- Identifikation mittels elektronischen Identitätsnachweises (online Ausweisfunktion)
- Identifikation mittels eGK und PIN
- Identifikation mittels PID aus einer zertifizierten EUDI-Wallet

Neu:

A_22865-02 - Verpflichtende Verfahren zur Identifikation von Nutzern
Der Anbieter des sektoralen IDP MUSS einen Prozess zur Identifikation von Nutzern mit mindestens diesen Identifikationsverfahren zur Nutzeridentifikation anbieten:

- Identifikation mittels elektronischen Identitätsnachweis (online Ausweisfunktion)
- Identifikation mittels eGK und PIN
- Identifikation mittels PID aus einer ~~zertifizierten~~ EUDI-Wallet gemäß A_30614*

Allgemeine Anforderungen zur Unterstützung der EUDI-Wallet durch sektorale IDPs

Neu:

A_30615 - Verifier-Komponente - Umsetzung einer Verifier-Komponenten nach [OID4VP]-Protokoll
Der sektorale IDP MUSS über eine Verifier-Komponente verfügen, die das [OID4VP]-Protokoll unter Berücksichtigung des [HAIP]-Profils und der weiteren Profilierung gemäß [ETSI TS 119 472-2] unterstützt, um die Personenidentifizierungsdaten (PID) für natürliche Personen gemäß des Anhangs von (EU) 2024/2977 aus der EUDI-Wallet entgegennehmen und validieren zu können.

Hinweis: Informationen zur Umsetzung der Integration der deutschen PID für Relying Parties finden sich im Developer Guide https://bmi.usercontent.opencode.de/eudi-wallet/developer-guide/resources/pid_reference/.

Neu:

A_30616 - Verifier-Komponente - Anforderungen an die Unterstützung gemäß [HAIP]-Spezifikation
Die Verifier-Komponente des sektoralen IDP MUSS die [HAIP]-Variante mit Redirects gemäß Abschnitt 5.1 der [HAIP]-Spezifikation oder die [HAIP]-Variante mit W3C Digital Credentials API gemäß Abschnitt 5.2 der [HAIP]-Spezifikation unterstützen.

Neu:

A_30613 - Verifier-Komponente - Unterstützung der fakultativen PID gemäß des deutschen „PID-Rulebooks“
Die Verifier-Komponente des sektoralen IDP MUSS neben der obligatorischen PID aus Tabelle 1 des Anhangs von (EU) 2024/2977 auch die fakultativen PID aus Tabelle 2 des Anhangs und zumindest die zusätzlichen fakultativen PID gemäß des deutschen „PID-Rulebooks“ unterstützen.

Hinweis: Das deutsche „PID-Rulebooks“ ist unter https://bmi.usercontent.opencode.de/eudi-wallet/eidas-2.0-architekturkonzept/content/features/PID/german-pid-rulebook/ veröffentlicht.

Neu:

A_30614 - Vertrauensanker aus der entsprechenden „List of Trusted Entities“
Die Verifier-Komponente des sektoralen IDP MUSS die Validierung der präsentierten PID unter Verwendung der hierfür vorgesehenen Vertrauensanker aus der entsprechenden „List of Trusted Entities“ im Format [ETSI TS 119 602], die im „eIDAS Dashboard“ der Europäischen Kommission im Bereich „Wallet“ verfügbar sind, durchführen.

Hinweis: Die Zertifizierung der deutschen EUDI-Wallet nach TR-03189 wird zu einem späteren Zeitpunkt, wenn diese alle eIDAS-2.0-Funktionen enthält, erfolgen. Solange die deutsche Wallet nicht zertifiziert ist, muss diese gegenüber der nationalen Trust-List https://trustlists.eudihub.de/ validiert werden.

Es wird Kapitel "4.4.2 Authentifizierungsverfahren" wie folgt angepasst:

Alt:

A_28990 - Unterstützung der EUDI-Wallet
Der Hersteller eines sektoralen IDP MUSS ein Authentifizierungsverfahren mittels PID aus einer zertifizierten EUDI-Wallet unterstützen.

Neu:

A_28990-01 - Unterstützung der EUDI-Wallet
Der Hersteller eines sektoralen IDP MUSS ein Authentifizierungsverfahren mittels PID aus einer ~~zertifizierten~~ EUDI-Wallet gemäß A_30614* unterstützen.

Alt:

A_23129-06 - Identifikation des Authentisierungsverfahren
Der sektorale IDP MUSS den Claim`amr` im ID_TOKENentsprechend dem durchgeführten Authentisierungsverfahren nach folgender Tabelle befüllen.

Tabelle 1: Codierung der Authentisierungsverfahren

Authentisierungsverfahren	**Wert des`amr` Claim**	**zulässiges Niveau (`acr`)**
Authentisierung mittels eGK und PIN	urn:telematik:auth:eGK	gematik-ehealth-loa-high

Authentisierung mittels elektronischem Identitätsnachweis (Online-Ausweisfunktion)	urn:telematik:auth:eID	gematik-ehealth-loa-high
Authentisierung mittels eGK und PIN ohne Prüfung Gerätebindung (Gastzugang)	urn:telematik:auth:guest:eGK	gematik-ehealth-loa-high
Authentisierung mittels PID einer zertifizierten EUDI-Wallet	urn:telematik:auth:eudiWallet	gematik-ehealth-loa-high
Anderes Authentisierungsverfahren	urn:telematik:auth:other	gematik-ehealth-loa-high und gematik-ehealth-loa-substantial
Authentisierungsverfahren mit Einwilligung für ein Single Sign-On (SSO) (deprecated)	urn:telematik:auth:sso	gematik-ehealth-loa-high gematik-ehealth-loa-substantial
Authentisierungsverfahren mit Einwilligung zum Zugriff auf Daten mit hohem Schutzbedarf (deprecated)	urn:telematik:auth:mEW	gematik-ehealth-loa-substantial

Hinweis: Die Authentisierungsverfahren "urn:telematik:auth:sso" und "urn:telematik:auth:mEW" werden nach vollständiger Umsetzung der Anforderungen A_27591, A_27592 und A_27593 durch alle Teilnehmer der TI-Föderation aus der Anforderung entfernt.

Neu:

A_23129-07 - Identifikation des Authentisierungsverfahren
Der sektorale IDP MUSS den Claim`amr` im ID_TOKENentsprechend dem durchgeführten Authentisierungsverfahren nach folgender Tabelle befüllen.

Tabelle 2: Codierung der Authentisierungsverfahren

Authentisierungsverfahren	**Wert des`amr` Claim**	**zulässiges Niveau (`acr`)**
Authentisierung mittels eGK und PIN	urn:telematik:auth:eGK	gematik-ehealth-loa-high
Authentisierung mittels elektronischem Identitätsnachweis (Online-Ausweisfunktion)	urn:telematik:auth:eID	gematik-ehealth-loa-high

Authentisierung mittels eGK und PIN ohne Prüfung Gerätebindung (Gastzugang)	urn:telematik:auth:guest:eGK	gematik-ehealth-loa-high
Authentisierung mittels PID einer ~~zertifizierten~~ EUDI-Wallet gemäß A_30614*	urn:telematik:auth:eudiWallet	gematik-ehealth-loa-high
Anderes Authentisierungsverfahren	urn:telematik:auth:other	gematik-ehealth-loa-high und gematik-ehealth-loa-substantial
Authentisierungsverfahren mit Einwilligung für ein Single Sign-On (SSO) (deprecated)	urn:telematik:auth:sso	gematik-ehealth-loa-high gematik-ehealth-loa-substantial
Authentisierungsverfahren mit Einwilligung zum Zugriff auf Daten mit hohem Schutzbedarf (deprecated)	urn:telematik:auth:mEW	gematik-ehealth-loa-substantial

Hinweis: Die Authentisierungsverfahren "urn:telematik:auth:sso" und "urn:telematik:auth:mEW" werden nach vollständiger Umsetzung der Anforderungen A_27591, A_27592 und A_27593 durch alle Teilnehmer der TI-Föderation aus der Anforderung entfernt.

3 Änderungen in Steckbriefen

3.1 Änderungen in gemProdT_IDP-Sek_KTR_PTV

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

Tabelle 3: Anforderungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_28990~~	Unterstützung der EUDI-Wallet	gemSpec_IDP_Sek
A_28990-01	Unterstützung der EUDI-Wallet	gemSpec_IDP_Sek

Tabelle 4: Anforderungen zur Sich.techn. Eignung "Produktgutachten"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_23129-06~~	Identifikation des Authentisierungsverfahren	gemSpec_IDP_Sek
A_23129-07	Identifikation des Authentisierungsverfahren	gemSpec_IDP_Sek
A_30613	Verifier-Komponente - Unterstützung der fakultativen PID gemäß des deutschen „PID-Rulebooks“	gemSpec_IDP_Sek
A_30614	Vertrauensanker aus der entsprechenden „List of Trusted Entities“	gemSpec_IDP_Sek
A_30615	Verifier-Komponente - Umsetzung einer Verifier-Komponenten nach [OID4VP]-Protokoll	gemSpec_IDP_Sek
A_30616	Verifier-Komponente - Anforderungen an die Unterstützung gemäß [HAIP]-Spezifikation	gemSpec_IDP_Sek

3.2 Änderungen in gemAnbT_IDP-Sek_ATV

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemAnbT_IDP-

Sek_ATV]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 5: Anforderungen zur Sich.techn. Eignung "Gutachten (Anbieter)"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_22865-01~~	Verpflichtende Verfahren zur Identifikation von Nutzern	gemSpec_IDP_Sek
A_22865-02	Verpflichtende Verfahren zur Identifikation von Nutzern	gemSpec_IDP_Sek