
C_11897_Anlage

Inhaltsverzeichnis

| | |
|--|-----------|
| 1 Änderungsbeschreibung | 3 |
| 2 Änderungen in gemSpec_IDP_Sek..... | 4 |
| 3 Änderungen in gemSpec_IDP_FedMaster | 66 |
| 4 Änderungen in gemSpec_IDP_FD | 88 |

1 Änderungsbeschreibung

- Aktualisierung HSM-Anforderung
- SSO auch für Authentisierungen mit Biometrie ermöglichen
- Einwilligungen für starke biometrische Sensoren konkretisiert
- Generalisierung der Anforderung zum Schutz vor Replay-Attacken
- Änderung von Prüfzuordnungen, deren Anforderungen produkt- statt anbieterspezifisch sind
- Abweichende Regelungen Gastanmeldung (eGK+PIN)
- Korrektur von `scope` und `claims`
- Ergänzung `epk`
- Konkretisierung der Signalisierung angeforderter und verwendeter `amr` und `acr`
- Konkretisierung der Signalisierung der Einwilligung
- Korrektur OpenID Federation Metadaten
- Korrektur dokumenteninterner Verweise und aktualisierter externer Spezifikationen (OpenID Connect Federation)
- Korrektur redaktioneller Fehler
- Korrektur Mediatype `signed_jwks_uri`
- Korrektur `x5c` Attribut Typ

2 Änderungen in gemSpec_IDP_Sek

Änderungen in Kapitel 3.2.2 "Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld"

Alt:

A_22829 - Anbieter sektoraler IDP Speicherung Schlüsselmaterial in HSM

Der Anbieter des sektoralen IDP MUSS das private Schlüsselmaterial für kryptografische Verfahren in einem HSM speichern, dessen Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde. Als Evaluierungsschemata kommen dabei Common Criteria oder Federal Information Processing Standard (FIPS) in Frage.

Die Prüftiefe MUSS mindestens:

1. FIPS 140-2 Level 3 oder
2. Common Criteria EAL 4+ erweitert um AVA_VAN.5 entsprechen.

[<=]

Neu:

A_22829-01 - Anbieter sektoraler IDP Speicherung Schlüsselmaterial in HSM

Der Anbieter des sektoralen IDP MUSS das private Schlüsselmaterial für kryptografische Verfahren in einem HSM speichern, dessen Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde. Als Evaluierungsschemata kommen dabei Common Criteria oder Federal Information Processing Standard (FIPS) in Frage.

Die Prüftiefe MUSS mindestens:

1. FIPS 140-2 Level 3 oder
2. **FIPS 140-3 Level 3 oder**
3. Common Criteria EAL 4+ erweitert um AVA_VAN.5

entsprechen.

[<=]

Änderungen in Kapitel 4.2.4.2 "Token-Endpunkt Ausgangsdaten"

Alt:

A_22706-01 - "ID_TOKEN" des sektoralen IDP

Der sektorale IDP MUSS nach erfolgreicher Prüfung des erhaltenen `AUTHORIZATION_CODE` dem aufrufenden Authorization-Server des Fachdienstes ein `ID_TOKEN` gemäß OIDC Standard OpenID Connect Core 1.0 (section-2) mit den angefragten `scopes` und `claims` zurückgeben.

[<=]

Neu:

A_22706-02 - "ID_TOKEN" des sektoralen IDP

Der sektorale IDP MUSS nach erfolgreicher Prüfung des erhaltenen `AUTHORIZATION_CODE` dem aufrufenden Authorization-Server des Fachdienstes ein `ID_TOKEN` gemäß OIDC Standard [OpenID Connect Core 1.0#IDToken] mit den

angefragten scopes und claims zurückgeben.
[<=]

Alt:

A_22989-01 - "scopes" und "claims" des sektoralen IDP für Versicherte

Ein sektoraler IDP, welcher die Identitäten für Versicherte verwaltet, MUSS mindestens die folgenden scopes und claims unterstützen:

Tabelle 5: scopes und claims

| Scope | Claim | Wert | Beschreibung |
|----------------------------|-----------|--------|--|
| urn:telematik:geburtsdatum | birthdate | string | <p>Die Angaben des Geburtsdatums des Nutzers erfolgt im Format ISO 8601:2004 [ISO8601-2004] YYYY-MM-DD.</p> <p>Ist das Geburtsdatum nicht bekannt, so wird es (analog einer Festlegung für diesen Fall bei Ausstellung einer eGK) durch folgende Regeln definiert. (dabei wird davon ausgegangen, dass das Geburtsjahr immer vorhanden ist):</p> <ul style="list-style-type: none">• Ist der Monat aber nicht der Tag des Geburtsdatums bekannt, so wird der 15. des Monat als Geburtsdatum festgelegt (TT.03.1975 - >15.03.1975)• Sind Tag und Monat des Geburtsdatums nicht bekannt, so wird der 01.07. des Jahres als Geburtsdatum festgelegt (TT.MM.1975 - >01.07.1975) |

| | | | |
|----------------------------|-----------------------------------|--------|--|
| urn:telematik:alter | urn:telematik:claims:alter | string | Alter der Person in Jahren zum Zeitpunkt der Erstellung des Tokens |
| urn:telematik:display_name | urn:telematik:claims:display_name | string | Analog zu name gemäß [OpenID Connect Core 1.0] Vollständiger Name des Versicherten in anzeigbarer Form inklusive aller Namensbestandteile und ggf. vorhandener Titel oder Namenszusätze. |
| urn:telematik:family_name | urn:telematik:claims:family_name | string | Nachname des Versicherten kodiert als UTF8 String [RFC3629] |
| urn:telematik:given_name | urn:telematik:claims:given_name | string | Vorname des Versicherten, kodiert als UTF8 String [RFC3629] |
| urn:telematik:geschlecht | urn:telematik:claims:geschlecht | string | Geschlecht des Nutzers. Kodierung analog VSDM M = männlich, W = weiblich, X = unbestimmt, D = divers |
| urn:telematik:email | urn:telematik:claims:email | string | E-Mail-Adresse des Versicherten, wenn bekannt |
| urn:telematik:versicherter | urn:telematik:claims:profession | string | Für Versicherte 1.2.276.0.76.4.49 |
| | urn:telematik:claims:id | string | Für Versicherte der unveränderliche Anteil der KVNR |
| | urn:telematik:claims:organization | string | ID oder Name der attributsbestätigenden Stelle (IK-Nummer der Kasse) |

< =

Neu:**A_22989-02 - "scope" und "claims" Werte des sektoralen IDP für Versicherte**

Ein sektoraler IDP, welcher die Identitäten für Versicherte verwaltet, MUSS mindestens die folgenden scope und claims Werte unterstützen:

Tabelle 5: scopes und claims

| Scope | Claim | Wert | Beschreibung |
|----------------------------|-----------------------------------|--------|---|
| urn:telematik:geburtsdatum | birthdate | string | <p>Die Angaben des Geburtsdatums des Nutzers erfolgt im Format ISO 8601:2004 [ISO8601-2004] YYYY-MM-DD.</p> <p>Ist das Geburtsdatum nicht bekannt, so wird es (analog einer Festlegung für diesen Fall bei Ausstellung einer eGK) durch folgende Regeln definiert. (dabei wird davon ausgegangen, dass das Geburtsjahr immer vorhanden ist):</p> <ul style="list-style-type: none"> Ist der Monat aber nicht der Tag des Geburtsdatums bekannt, so wird der 15. des Monat als Geburtsdatum festgelegt (TT.03.1975 - >15.03.1975) Sind Tag und Monat des Geburtsdatums nicht bekannt, so wird der 01.07. des Jahres als Geburtsdatum festgelegt (TT.MM.1975 - >01.07.1975) |
| urn:telematik:alter | urn:telematik:claims:alter | string | Alter der Person in Jahren zum Zeitpunkt der Erstellung des Tokens |
| urn:telematik:display_name | urn:telematik:claims:display_name | string | Analog zu name gemäß [OpenID Connect Core 1.0] Vollständiger Name des Versicherten in anzeigbarer Form inklusive aller Namensbestandteile und ggf. vorhandener Titel oder |

| | | | |
|----------------------------|-----------------------------------|--------|--|
| | | | Namenszusätze. |
| urn:telematik:family_name | urn:telematik:claims:family_name | string | Nachname des Versicherten kodiert als UTF8 String [RFC3629] |
| urn:telematik:given_name | urn:telematik:claims:given_name | string | Vorname des Versicherten, kodiert als UTF8 String [RFC3629] |
| urn:telematik:geschlecht | urn:telematik:claims:geschlecht | string | Geschlecht des Nutzers. Kodierung analog VSDM M = männlich, W = weiblich, X = unbestimmt, D = divers |
| urn:telematik:email | urn:telematik:claims:email | string | E-Mail-Adresse des Versicherten, wenn bekannt |
| urn:telematik:versicherter | urn:telematik:claims:profession | string | Für Versicherte 1.2.276.0.76.4.49 |
| | urn:telematik:claims:id | string | Für Versicherte der unveränderliche Anteil der KVN |
| | urn:telematik:claims:organization | string | ID oder Name der attributsbestätigenden Stelle (IK-Nummer der Kasse) |

<=

Alt:**A_23197 - Nutzung eines pairwise Subject als Pseudonym des Versicherten**

Der sektorale IDP MUSS das Attribut "sub" gemäß [[OpenID Connect Core 1.0 \(sektion-8.1\)](#)] als pairwise Subject Identifiers bilden. Dieses wird als pseudonyme ID des Versicherten verwendet:

- Der Subject Identifier MUSS je Versichertem und Fachdienst fest und eineindeutig sein
- Der Subject Identifier MUSS sich für einen Versicherten gegenüber jedem Fachdienst unterscheiden.

[<=]

Neu:**A_23197-01 - Nutzung eines pairwise Subject als Pseudonym des Versicherten**

Der sektorale IDP MUSS das Attribut "sub" gemäß [[OpenID Connect Core 1.0#PairwiseAlg](#)] als pairwise Subject Identifiers bilden. Dieses wird als pseudonyme ID des Versicherten verwendet:

- Der Subject Identifier MUSS je Versichertem und Fachdienst fest und eindeutig sein.
- Der Subject Identifier MUSS sich für einen Versicherten gegenüber jedem Fachdienst unterscheiden.

Abweichend hiervon MUSS der sektorale IDP das Attribut "sub" bei jeder Gastanmeldung mittels eGK+PIN nach A_25239 mit einem zufälligen, nicht rückverfolgaren Wert belegen. Dieser Zufallswert DARF NICHT gespeichert werden und MUSS für jeden Anmeldevorgang neu berechnet werden.

[<=]

Änderungen in Kapitel 4.3.2 "Authentifizierungsverfahren"

Alt:

A_24547 - Anfrage spezifischer Authentisierungsmittel (amr) durch Relying Parties

Ein sektoraler IDP MUSS die Anfrage von Relying Parties zum Einsatz bestimmter Authentisierungsmittel im claims Parameter des Authorization Request durch Verwendung des Claims *authentication_method_reference* (amr) unterstützen.[<=]

Neu:

A_24547-01 - Anfrage spezifischer Authentisierungsmittel (amr) durch Relying Parties

Ein sektoraler IDP MUSS die Anfrage von Relying Parties zum Einsatz bestimmter Authentisierungsmittel im claims-Parameter des Authorization Requests durch Verwendung des amr (*authentication_method_reference*) Claims (gemäß [\[OpenID Connect Core 1.0#IDToken\]](#) ein JSON Array) unterstützen.

- Signalisiert eine Relying Party im Authorization Request die amr-Präferenz ohne das Attribut *essential* oder mit dem Attribut *essential* und dem Wert *false*, so SOLL der sektorale IDP diese Authentisierungsmittel in absteigender Reihenfolge der Auflistung bei der Authentisierung des Nutzers berücksichtigen. Wurde ein aufgelistetes Authentisierungsmittel erfolgreich verwendet, so ist auf die Prüfung weiterer Authentisierungsmittel zu verzichten. Konnte kein angefordertes Authentisierungsmittel erfolgreich verwendet werden, so liegt es im Ermessen des sektoralen IDP, unter Berücksichtigung der Nutzerpräferenzen, welches Authentisierungsmittel zur Erfüllung des Authorization Request erforderlich ist.
- Signalisiert eine Relying Party im Authorization Request die amr-Präferenz mit dem Attribut *essential* und dem Wert *true*, so MUSS der sektorale IDP diese Authentisierungsmittel in absteigender Reihenfolge der Auflistung bei der Authentisierung des Nutzers berücksichtigen. Wurde ein aufgelistetes Authentisierungsmittel erfolgreich verwendet, so ist auf die Prüfung weiterer Authentisierungsmittel zu verzichten. Konnte kein angefordertes Authentisierungsmittel erfolgreich verwendet werden, so ist die Authentisierung mit einem Fehler (siehe [\[OpenID Connect Core 1.0#AuthError\]](#)) abzubrechen.

Bei der Auswahl des zu verwendenden Authentisierungsmittels MUSS der sektorale IDP sicherstellen, dass dieses für das im Authorization Request angeforderte *acr* nach A_23129-* zulässig ist. Angeforderte amr, die dem *acr* nicht genügen, MÜSSEN ignoriert

werden.

[<=]

Hinweis: ein Beispiel für den Aufbau der amr Präferenz ist der Tabelle "Parameter Pushed Authorization Request" in der Zeile "Claims" zu entnehmen

Alt:

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 6: Codierung der Authentisierungsverfahren

| Authentifizierungsverfahren | Wert des <code>amr</code> Claim | zulässiges Niveau (<code>acr</code>) |
|---|---------------------------------|--|
| 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 |
| Authentifizierung mittels eGK und PIN ohne Prüfung Gerätebindung (Gastzugang) | urn:telematik:auth:guest:eGK | gematik-ehealth-loa-high |
| Anderes Authentisierungsverfahren | urn:telematik:auth:other | gematik-ehealth-loa-high und gematik-ehealth-loa-substantial |

<=, Anb_IDP-Sek_KTR, Sich.techn. Eignung: Gutachten (Anbieter)

Hinweis: Das `amr` Claim wird generell von sektoralen IDPs im `ID_TOKEN` gemäß der Anforderung A_23129-03 mitgeliefert. Um ein bestimmtes Authentisierungsmittel bei der Nutzerauthentifizierung durch den sektoralen IDP zu erzwingen, fordert die Relying Party dies im Authorization Request mittels Claims Parameter an.

Beispiel: Claims Parameter (URL encoded) zum Anfordern der Nutzerauthentifizierung mit eGK
`claims%3D%7B%22id_token%22%3A%7B%22amr%22%3A%7B%22values%22%3A%5B%22urn%3Atelematik%3Aauth%3AeGK%22%5D%7D%7D%7D`

Neu:

A_23129-04 Identifikation des Authentifizierungsverfahren

Der sektorale IDP MUSS den claim `amr` im `ID_TOKEN` entsprechend dem durchgeführten Authentisierungsverfahren nach folgender Tabelle **belegenbefüllen**.

Tabelle 6: Codierung der Authentisierungsverfahren

| Authentifizierungsverfahren | Wert des <code>amr</code> Claim | zulässiges Niveau (<code>acr</code>) |
|---|---------------------------------|--|
| 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 gematik-ehealth-loa-substantial |
| Authentisierungsverfahren mit Einwilligung zum Zugriff auf Daten mit hohem Schutzbedarf | urn:telematik:auth:mEW | gematik-ehealth-loa-substantial |
| Authentifizierung mittels eGK und PIN ohne Prüfung Gerätebindung (Gastzugang) | urn:telematik:auth:guest:eGK | gematik-ehealth-loa-high |
| Anderes Authentisierungsverfahren | urn:telematik:auth:other | gematik-ehealth-loa-high und gematik-ehealth-loa-substantial |

<=, **Anb_IDP-Sek_KTR**, Sich.techn. Eignung: **Gutachten (Anbieter)Produktgutachten**

Hinweis: Das Claim `amr` wird generell von sektoralen IDP im `ID_TOKEN` gemäß der Anforderung A_23129-03* mitgeliefert. Bei dem Claim handelt es sich gemäß [\[OpenID Connect Core 1.0#IDToken\]](#) um ein JSON Array.

Hinweis 2: Um ein bestimmtes Authentisierungsmittel bei der Nutzerauthentifizierung durch den sektoralen IDP zu erzwingen, fordert die Relying Party dies im Authorization Request mittels Claims Parameter an. Ein Beispiel kann der Tabelle "Parameter Pushed Authorization Request" in der Zeile zu Claims entnommen werden.

Beispiel: Claims Parameter (URL encoded) zum Anfordern der Nutzerauthentifizierung mit eGK: `claims%3D%7B%22id_token%22%3A%7B%22amr%22%3A%7B%22values%22%3A%5B%22urn%3Atelematik%3Aauth%3AeGK%22%5D%7D%7D%7D`

Alt:

A_22867 - Signalisierung der Verwendung des Authentisierungsverfahrens "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. [`<=`]

Neu:

A_22867-01 - Signalisierung der Verwendung des Authentisierungsverfahrens "gematik-ehealth-loa-substantial" beim Zugriff auf Daten mit hohem Schutzbedarf

Der sektorale IDP MUSS den claim `amr` **aufum** den Wert "urn:telematik:auth:mEW" **setzenerweitern**, 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. [`<=`]

Alt:

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

Vor der Nutzung von Authentisierungsverfahren mit substantiellem Schutzniveau beim Zugriff auf Daten mit hohem Schutzbedarf nach A_22867 MUSS der sektorale IDP sicherstellen, dass die Einwilligung des Nutzers vollständig freiwillig erfolgt. Dabei müssen alternative Verfahren mit Sicherheitsniveau "gematik-loa-high" hervorgehoben und die Möglichkeit des Widerrufs der Einwilligungserklärung aufgezeigt werden. Der Nutzer muss insbesondere über die Risiken einer Absenkung des Vertrauensniveaus informiert werden und der Verwendung eines Verfahrens mit einem anderen angemessenen Sicherheitsniveau zum Zugriff auf Daten mit hohem Schutzbedarf aktiv zustimmen.[`<=`]

Neu:

A_23103-01 - Einwilligung zur Verwendung des Authentisierungsverfahrens "gematik-ehealth-loa-substantial" beim Zugriff auf Daten mit hohem Schutzbedarf

Vor der Nutzung von Authentisierungsverfahren mit substantiellem Schutzniveau beim Zugriff auf Daten mit hohem Schutzbedarf nach A_22867 MUSS der sektorale IDP sicherstellen, dass die Einwilligung des Nutzers vollständig freiwillig erfolgt. Dabei müssen alternative Verfahren mit Sicherheitsniveau "gematik-**ehealth**-loa-high" hervorgehoben und die Möglichkeit des Widerrufs der Einwilligungserklärung aufgezeigt werden. Der Nutzer muss insbesondere über die Risiken einer Absenkung des Vertrauensniveaus informiert werden und der Verwendung eines Verfahrens mit einem anderen angemessenen Sicherheitsniveau zum Zugriff auf

Daten mit hohem Schutzbedarf aktiv zustimmen.
[<=]

Änderungen in Kapitel 4.3.2.1 "Gerätenutzung"

Alt:

A_22750-01 - Gerätebindung und Authentisierung für "gematik-ehealth-loa-high" und "gematik-ehealth-loa-substantial"

Abhängig von der Geräteausrüstung 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 Authentisierungsverfahrens nutzt, die Zeitrahmen der Gültigkeit für die Gerätebindung gemäß Tabelle "Übersicht Gerätebindung" berücksichtigen. Beim Zugriff auf Daten mit hohem Schutzbedarf gelten die Zeiträume der maximalen Gerätebindung gematik-ehealth-loa-high in der Tabelle. Nach Einwilligung des Nutzers gemäß A_23103* gelten beim Zugriff auf Daten mit hohem Schutzbedarf, unter Verwendung von Authentisierungsverfahrens gematik-ehealth-loa-substantial die Zeiträume der maximalen Gerätebindung gematik-ehealth-loa-substantial in Tabelle "Übersicht Gerätebindung".

Die Gerätebindung MUSS durch den Nutzer nach Ablauf dieser Frist dementsprechend erneuert werden.

Der Anbieter des sektoralen IDP MUSS mit den zur Verfügung stehenden Plattformmechanismen, einen kryptographischen Nachweis der Gerätebindung auf dem Endgerät erzeugen und auf Serverseite prüfen (z.B. Android: Key & ID Attestation; iOS: DCAppAttestService).

Die Gerätebindung kann:

1. durch Identifikation, welche dem Niveau gematik-ehealth-loa-high entspricht oder
2. mit einer 2FA, welche dem Niveau gematik-ehealth-loa-high entspricht,

angelegt werden.

Tabelle 7: Übersicht Gerätebindung

| Schlüsselspeicher | Gültigkeit der Gerätebindung |
|------------------------|---|
| ohne Hardware Keystore | Die Gerätebindung kann mit einem Faktor aus den Bereichen Wissen oder Inhärenz genutzt werden: <ul style="list-style-type: none">• 24h auf dem Niveau "gematik-ehealth-loa-high"• 48h auf dem Niveau "gematik-ehealth-loa-substantial" |
| mit Hardware Keystore | Die Gerätebindung kann mit einem Faktor aus den Bereichen Wissen oder Inhärenz genutzt werden: <ul style="list-style-type: none">• 6 Monate auf dem Niveau "gematik-ehealth-loa-high"• 12 Monate auf dem Niveau "gematik-ehealth-loa- |

| | |
|-----------------------------------|---|
| | substantial" |
| mit zertifiziertem Secure Element | <p>Die Gerätebindung kann mit einem Faktor aus den Bereichen Wissen oder Inhärenz genutzt werden:</p> <ul style="list-style-type: none"> • unbegrenzt auf dem Niveau "gematik-ehealth-loa-high" • unbegrenzt auf dem Niveau "gematik-ehealth-loa-substantial" |

<=, Anb_IDP-Sek_KTR,Sich.techn. Eignung: Gutachten (Anbieter)

Geänderte Zuordnung:

A_22750-01 - Gerätebindung und Authentisierung für "gematik-ehealth-loa-high" und "gematik-ehealth-loa-substantial"

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 Authentisierungsverfahrens nutzt, die Zeitrahmen der Gültigkeit für die Gerätebindung gemäß Tabelle "Übersicht Gerätebindung" berücksichtigen. Beim Zugriff auf Daten mit hohem Schutzbedarf gelten die Zeiträume der maximalen Gerätebindung gematik-ehealth-loa-high in der Tabelle. Nach Einwilligung des Nutzers gemäß A_23103* gelten beim Zugriff auf Daten mit hohem Schutzbedarf, unter Verwendung des Authentisierungsverfahrens gematik-ehealth-loa-substantial die Zeiträume der maximalen Gerätebindung gematik-ehealth-loa-substantial in Tabelle "Übersicht Gerätebindung".

Die Gerätebindung MUSS durch den Nutzer nach Ablauf dieser Frist dementsprechend erneuert werden.

Der Anbieter des sektoralen IDP MUSS mit den zur Verfügung stehenden Plattformmechanismen, einen kryptographischen Nachweis der Gerätebindung auf dem Endgerät erzeugen und auf Serverseite prüfen (z.B. Android: Key & ID Attestation; iOS: DCAppAttestService).

Die Gerätebindung kann:

1. durch Identifikation, welche dem Niveau gematik-ehealth-loa-high entspricht oder
2. mit einer 2FA, welche dem Niveau gematik-ehealth-loa-high entspricht,

angelegt werden.

Tabelle 7: Übersicht Gerätebindung

| Schlüsselspeicher | Gültigkeit der Gerätebindung |
|-------------------|------------------------------|
|-------------------|------------------------------|

| | |
|-----------------------------------|--|
| ohne Hardware Keystore | Die Gerätebindung kann mit einem Faktor aus den Bereichen Wissen oder Inhärenz genutzt werden: <ul style="list-style-type: none"> • 24h auf dem Niveau "gematik-ehealth-loa-high" • 48h auf dem Niveau "gematik-ehealth-loa-substantial" |
| mit Hardware Keystore | Die Gerätebindung kann mit einem Faktor aus den Bereichen Wissen oder Inhärenz genutzt werden: <ul style="list-style-type: none"> • 6 Monate auf dem Niveau "gematik-ehealth-loa-high" • 12 Monate auf dem Niveau "gematik-ehealth-loa-substantial" |
| mit zertifiziertem Secure Element | Die Gerätebindung kann mit einem Faktor aus den Bereichen Wissen oder Inhärenz genutzt werden: <ul style="list-style-type: none"> • unbegrenzt auf dem Niveau "gematik-ehealth-loa-high" • unbegrenzt auf dem Niveau "gematik-ehealth-loa-substantial" |

<=, Anb_IDP-Sek_KTR, Sich.techn. Eignung: Gutachten (Anbieter)Produktgutachten

Alt:

A_25138-01 - Erneuerung der Gerätebindung für "gematik-ehealth-loa-high"

Nach Ablauf der Gültigkeitsdauer einer Gerätebindung DARF die bestehende Gerätebindung NICHT als Authentisierungsfaktor für die Erneuerung der Gerätebindung für gematik-ehealth-loa-high verwendet werden.

<=, IDP-Sek,Sich.techn. Eignung: Gutachten

Geänderte Zuordnung:

A_25138-01 - Erneuerung der Gerätebindung für "gematik-ehealth-loa-high"

Nach Ablauf der Gültigkeitsdauer einer Gerätebindung DARF die bestehende Gerätebindung NICHT als Authentisierungsfaktor für die Erneuerung der Gerätebindung für gematik-ehealth-loa-high verwendet werden.

<=, IDP-Sek,Sich.techn. Eignung: Produktgutachten

Alt:

A_25969 - Keine Nutzung einer Gerätebindung zur Einrichtung einer Gerätebindung

Eine Gerätebindung DARF NICHT mittels einer bestehenden Gerätebindung neu eingerichtet werden.

<=, IDP-Sek,Sich.techn. Eignung: Gutachten

Geänderte Zuordnung:**A_25969 - Keine Nutzung einer Gerätebindung zur Einrichtung einer Gerätebindung**

Eine Gerätebindung DARF NICHT mittels einer bestehenden Gerätebindung neu eingerichtet werden.

<=, IDP-Sek,Sich.techn. Eignung: **Produktgutachten**

Änderungen in Kapitel 4.3.2.2 "Nutzung von Biometrie"Alt:**A_23701 - Verwendung von Biometrie als Faktor zur Nutzerauthentifizierung**

Der Anbieter der sektoralen TI MUSS die in der Tabelle "Biometrie" aufgeführten Einschränkungen für die Nutzung biometrischer Sensoren zur Authentifizierung des Nutzers berücksichtigen. Für die Nutzung eines biometrischen Faktors MUSS, wenn damit eine Herabstufung des Vertrauensniveaus verbunden ist, die Einwilligung des Nutzers zur Verwendung des Authentisierungsverfahrens "gematik-ehealth-loa-substantial" beim Zugriff auf Daten mit hohem Schutzbedarf ([A_23103]) vorliegen.

Tabelle 8: Biometrie

| LoA | Nutzung der biometrischen Sensoren der mobilen Plattformen als biometrischer Faktor | Einschränkungen |
|---------------------------------|---|--|
| gematik-ehealth-loa-high | <ul style="list-style-type: none"> Biometrische Sensoren, welche den Anforderungen mit BAL/LoA high (vgl. BSI TR-03107-1, TR-03166) genügen | keine |
| gematik-ehealth-loa-substantial | <ul style="list-style-type: none"> Biometrische Sensoren, welche den Anforderungen mit BAL/LoA high (vgl. BSI TR-03107-1, TR-03166) genügen Biometrische Sensoren, welche den Anforderungen mit BAL/LoA substantial (vgl. BSI TR-03107-1, TR-03166) genügen | keine |
| | <ul style="list-style-type: none"> Biometrie Android - Nutzung eingeschränkt auf die Erfüllung Biometric.STRONG oder Class-3 Apple-TouchID | Als Voraussetzung zur Verwendung dieser Übergangslösung ist es erforderlich, dass der Risikoträger im Rahmen einer „Risiko-Meldung“ angemessen über die in Teilen leichte Überwindbarkeit dieser |

| | | |
|--|--|--|
| | | biometrischen Verfahren in leicht verständlicher Sprache und barrierearm informiert wird. Nach Einwilligung in die Übernahme des Risikos durch den Risikoträger, dürfen die entsprechenden Verfahren angeboten werden. |
|--|--|--|

<=, Anb_IDP-Sek_KTR,Sich.techn. Eignung: Gutachten (Anbieter)

Neu:

Hinweis: Durch einen redaktionellen Fehler wurde ein anderer Text der [A_23701] veröffentlicht, als in der Kommentierung freigegeben. Mit [A_23701-01] wird der ursprünglich freigegebene Inhalt wiederhergestellt.

A_23701-01 - Verwendung von Biometrie als Faktor zur Nutzerauthentifizierung

Der Anbieter des sektoralen IDP MUSS die in der Tabelle "Biometrie" aufgeführten Einschränkungen für die Nutzung von biometrischen Sensoren zur Nutzerauthentifizierung des Nutzers die in der Tabelle "Biometrie" aufgeführten Einschränkungen berücksichtigen. Für die Nutzung eines biometrischen Faktors MUSS, wenn damit eine Herabstufung des Vertrauensniveaus verbunden ist, die Einwilligung des Nutzers zur Verwendung des Authentisierungsverfahrens gematik-ehealth-loa-substantial beim Zugriff auf Daten mit hohem Schutzbedarf (A_23103) vorliegen.

Tabelle 8: Biometrie

| LoA | Nutzung der biometrischen Sensoren der mobilen Plattformen als biometrischer Faktor | Einschränkungen |
|---------------------------------|---|-----------------|
| gematik-ehealth-loa-high | <ul style="list-style-type: none"> Biometrische Sensoren, welche den Anforderungen mit BAL/LoA high (vgl. BSI TR-03107-1, TR-03166) genügen | keine |
| gematik-ehealth-loa-substantial | <ul style="list-style-type: none"> Biometrische Sensoren, welche den Anforderungen mit BAL/LoA high (vgl. BSI TR-03107-1, TR-03166) genügen Biometrische Sensoren, welche den Anforderungen mit BAL/LoA substantial (vgl. BSI TR-03107-1, TR-03166) genügen | keine |

| | | |
|--|--|--|
| | <ul style="list-style-type: none"> • Biometrie Android - Nutzung eingeschränkt auf die Erfüllung Biometric.STRONG oder Class-3 • Apple-TouchID | <p>Als Voraussetzung zur Verwendung dieser Übergangslösung ist es erforderlich, dass der Risikoträger im Rahmen einer „Risiko-Meldung“ angemessen über die in Teilen leichte Überwindbarkeit dieser biometrischen Verfahren in leicht verständlicher Sprache und barrierearm informiert wird. Nach Einwilligung in die Übernahme des Risikos durch den Risikoträger, dürfen die entsprechenden Verfahren angeboten werden.</p> |
|--|--|--|

<=, **Anb_IDP-Sek_KTR**, Sich.techn. Eignung: **Gutachten (Anbieter)Produktgutachten**

Am Ende des Kapitels wird hinzugefügt

Neu:

A_26591 - Einwilligung zur Verwendung biometrischer Sensoren

Der sektorale IDP MUSS die explizite Einwilligung zur Verwendung der in Tabelle "Biometrie" zugelassenen biometrischen Sensoren einholen, wenn diese Sensoren nicht die erforderliche Güte für die uneingeschränkte Nutzung auf dem Vertrauensniveau **gematik-ehealth-loa-substantial beziehungsweise gematik-ehealth-loa-high** erfüllen. Dabei MUSS der sektorale IDP sicherstellen, dass der Nutzer über die damit verbundenen Risiken hinreichend informiert wurde, die Einwilligung des Nutzers vollständig freiwillig erfolgt und die Einwilligung kryptografisch abgesichert ist. Diese Einwilligung MUSS durch den sektoralen IDP für jedes zu verwendende Endgerät eingeholt werden, unabhängig von bereits erfolgten Einwilligungen auf anderen Endgeräten. Der sektorale IDP MUSS sicherstellen, dass erteilte Einwilligungen auf den jeweiligen Geräten durch den Nutzer widerrufen werden können.

<=, IDP-Sek, Sich.techn. Eignung: **Produktgutachten**

Änderungen in Kapitel 4.3.2.3 "Unterstützung Single-Sign-On (SSO) auf Anwendungsebene"

Alt:

A_23207-01 - Single Sign-On (SSO) als Authentifizierungsverfahren

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS im Claim `acr` das Niveau beauskunften, welches dem der vorhergehenden Authentisierung entspricht. Der Claim `amr` MUSS auf den Wert `urn:telematik:auth:sso` gemäß der Tabelle "Codierung der Authentisierungsverfahren" gesetzt werden.

<=, IDP-Sek,Sich.techn. Eignung: Gutachten

Neu:

A_23207-02 - Single Sign-On (SSO) als Authentifizierungsverfahren

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS im claim `acr` das Niveau beauskunften, welches dem der vorhergehenden Authentisierung entspricht. Der claim `amr` MUSS **aufum** den Wert `urn:telematik:auth:sso` gemäß der Tabelle "Codierung der Authentisierungsverfahren" **gesetzterweitert** werden.

<=, IDP-Sek,Sich.techn. Eignung: **Produktg**Gutachten

Alt:

A_23208-01 - Zustimmung des Nutzer für SSO

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS vor der Aktivierung eines Single Sign-On (SSO) nach [A_23207] sicherstellen, dass die Einwilligung des Nutzers hierzu insbesondere aufgeklärt, vollständig freiwillig, unter Hervorhebung sichererer Verfahren und widerrufbar erfolgt. Der Nutzer MUSS über die Risiken des SSO ausreichend aufgeklärt werden und der Verwendung für jeden einzelnen Fachdienst aktiv zustimmen.

<=, Anb_IDP-Sek_KTR,Sich.techn. Eignung: Gutachten (Anbieter)

Geänderte Zuordnung:

A_23208-01 - Zustimmung des Nutzer für SSO

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS vor der Aktivierung eines Single Sign-On (SSO) nach A_23207 sicherstellen, dass die Einwilligung des Nutzers hierzu insbesondere aufgeklärt, vollständig freiwillig, unter Hervorhebung sichererer Verfahren und widerrufbar erfolgt. Der Nutzer MUSS über die Risiken des SSO ausreichend aufgeklärt werden und der Verwendung für jeden einzelnen Fachdienst aktiv zustimmen.

<=, **Anb_IDP-Sek_KTR**, Sich.techn. Eignung: **Gutachten (Anbieter)Produktgutachten**

Alt:

A_24721-01 - Ausstellen einer SessionID zu einem Anwendungskontext

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS zur Absicherung des SSO nach der ersten erfolgreichen Nutzerauthentisierung eine SessionID zum laufenden Anwendungskontext generieren und dem Authenticator-Modul des Anwendungskontextes übertragen. Der Hersteller von sektoralen IDP MUSS sicherstellen, dass eine zu einem Anwendungskontext ausgestellte SessionID ausschließlich für diesen verwendet werden kann und nach dem Schließen des Anwendungskontext gelöscht wird.

<=, IDP-Sek,Sich.techn. Eignung: Gutachten

Neu:**A_24721-02 Ausstellen einer SessionID zu einem Anwendungskontext**

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS zur Absicherung des SSO **im Ablauf** der ersten erfolgreichen Nutzerauthentisierung eine SessionID zum laufenden **Nutzer**kontext generieren und diese an das Authenticator-Modul des Anwendungskontextes übertragen. Der Hersteller MUSS sicherstellen, dass eine ausgestellte SessionID **nur nach erfolgreicher Authentisierung und** ausschließlich für **den jeweiligen Nutzerkontext** verwendet werden kann und **spätestens nach der in A_23212 festgelegten Zeitspanne nach der letzten Nutzerinteraktion am Authenticator-Modul oder durch explizite Signalisierung der Beendigung des Anwendungskontextes durch die Anwendung** gelöscht wird.

<=, IDP-Sek,Sich.techn. Eignung: **Produktg**Gutachten

Hinweis: Unter Nutzerkontext sind die Informationen zu einem Nutzer zu verstehen, die mit der SessionID nach erfolgreicher Nutzerauthentifizierung mittels Authenticator durch den IDP assoziiert sind. Deshalb spricht man auch von einer Subject-Session, die durch die SessionID identifiziert ist. Der Anwendungskontext hingegen erstreckt sich über die Anwendung, also alle Komponenten und Dienste, die funktional für diese Anwendung benötigt werden.

Alt:**A_24725-01 - Prüfung der SessionID zu einem Anwendungskontext**

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS zur Absicherung des SSO jede Nutzerauthentisierung ohne Nutzerinteraktion die Gültigkeit, der vom Authenticator-Modul übertragenen SessionID überprüfen indem:

- die Signatur der SessionID mit dem zum Nutzer und zur SessionID gespeicherten public Key validiert wird,
- die SessionID mit der zum Nutzer gespeicherten SessionID verglichen wird,
- der Gültigkeitszeitraum der SessionID überprüft wird.

Ist die Prüfung nicht erfolgreich, so MUSS der sektorale IDP eine Nutzerauthentisierung mit Nutzerinteraktion durchführen.

<=, IDP-Sek,Sich.techn. Eignung: Gutachten

Geänderte Zuordnung:

A_24725-01 - Prüfung der SessionID zu einem Anwendungskontext

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS zur Absicherung des SSO jede Nutzerauthentisierung ohne Nutzerinteraktion die Gültigkeit, der vom Authenticator-Modul übertragenen SessionID überprüfen indem:

- die Signatur der SessionID mit dem zum Nutzer und zur SessionID gespeicherten public Key validiert wird,
- die SessionID mit der zum Nutzer gespeicherten SessionID verglichen wird,
- der Gültigkeitszeitraum der SessionID überprüft wird.

Ist die Prüfung nicht erfolgreich, so MUSS der sektorale IDP eine Nutzerauthentisierung mit Nutzerinteraktion durchführen.

<=, IDP-Sek,Sich.techn. Eignung: Produktgutachten

Alt:

A_23212-02 - Gültigkeitsdauer einer SessionID

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS sicherstellen, dass die vom sektoralen IDP zu einem Anwendungskontext ausgestellte SessionID ungültig wird und gelöscht werden muss, wenn:

- der Anwendungskontext, zu dem die SessionID erstellt wurde, beendet wurde
- der Nutzer bei offenem Anwendungskontext mindestens 10 Minuten inaktiv war
- die SessionID die maximale Gültigkeitsdauer von 1h überschreitet

In diesen Fällen ist eine erneute Nutzerauthentisierung mit aktiver Nutzerinteraktion notwendig.

<=, Anb_IDP-Sek_KTR,Sich.techn. Eignung: Gutachten (Anbieter)

Geänderte Zuordnung:

A_23212-02 - Gültigkeitsdauer einer SessionID

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS sicherstellen, dass die vom sektoralen IDP zu einem Anwendungskontext ausgestellte SessionID ungültig wird und gelöscht werden muss, wenn:

- Der Anwendungskontext, zu dem die SessionID erstellt wurde, beendet wurde.
- Der Nutzer bei offenem Anwendungskontext mindestens 10 Minuten inaktiv war.
- Die SessionID die maximale Gültigkeitsdauer von 1 Stunde überschreitet.

In diesen Fällen ist eine erneute Nutzerauthentisierung mit aktiver Nutzerinteraktion notwendig.

<=, Anb_IDP-Sek_KTR, Sich.techn. Eignung: Gutachten (Anbieter)Produktgutachten

Änderungen in Kapitel 5.2.2 "Rahmenbedingungen"

Alt:

Die Anforderungen in diesem Kapitel und die zusätzlichen Informationen im Kapitel 7.4 betreffen nur Hersteller, die ein SSO auf Anwendungsebene implementieren. Für Hersteller, die kein SSO auf Anwendungsebene umsetzen, gelten die Anforderungen dieses Kapitels nicht.

Neu:

Die Anforderungen in diesem Kapitel und die zusätzlichen Informationen im Kapitel 7.4 "Unterstützung Single-Sign-On auf Anwendungsebene" betreffen nur Hersteller, die ein SSO auf Anwendungsebene implementieren. Für Hersteller, die kein SSO auf Anwendungsebene umsetzen, gelten die Anforderungen dieses Kapitels nicht.

Alt:

A_24722-01 - Ausstellen eines Schlüssels zu einem Anwendungskontext

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS zur Absicherung des SSO nach der ersten erfolgreichen Nutzerauthentisierung im Schlüsselspeicher des Nutzergerätes ein Schlüsselpaar generieren und an den laufenden Anwendungskontext sowie an die vom sektoralen IDP erhaltenen SessionID binden. Das Authenticator-Modul MUSS nach der ersten erfolgreichen Nutzerauthentisierung den öffentlichen Schlüssel und die mit dem privaten Schlüssel signierte SessionID zum Anwendungskontext an den sektoralen IDP übertragen. Der Hersteller von sektoralen IDP MUSS sicherstellen, dass das zu einem Anwendungskontext generierte Schlüsselpaar und SessionID nach dem Schließen des Anwendungskontextes aus dem Schlüsselspeicher des Geräts gelöscht werden.

<=, IDP-Sek,Sich.techn. Eignung: Gutachten

Geänderte Zuordnung:

A_24722-01 - Ausstellen eines Schlüssels zu einem Anwendungskontext

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS zur Absicherung des SSO nach der ersten erfolgreichen Nutzerauthentisierung im Schlüsselspeicher des Nutzergerätes ein Schlüsselpaar generieren und an den laufenden Anwendungskontext sowie an die vom sektoralen IDP erhaltenen SessionID binden. Das Authenticator-Modul MUSS nach der ersten erfolgreichen Nutzerauthentisierung den öffentlichen Schlüssel und die mit dem privaten Schlüssel signierte SessionID zum Anwendungskontext an den sektoralen IDP übertragen. Der Hersteller von sektoralen IDP MUSS sicherstellen, dass das zu einem Anwendungskontext generierte Schlüsselpaar und SessionID nach dem Schließen des Anwendungskontextes aus dem Schlüsselspeicher des Geräts gelöscht werden.

<=, IDP-Sek,Sich.techn. Eignung: **Produktgutachten**

Alt:

A_24768-01 Wechsel des Schlüssels zu einem Anwendungskontext

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS zur Absicherung des SSO das im Authenticator-Modul zum laufenden Anwendungskontext generierte Schlüsselpaar nach spätestens 3 Minuten erneuern.

<=, IDP-Sek,Sich.techn. Eignung: Gutachten

Neu:

A_24768-02 - Schutz vor Replay-Attacken innerhalb eines Anwendungskontextes

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS ein geeignetes Verfahren zum Schutz vor Replay-Attacken implementieren.

<=, IDP-Sek,Sich.techn. Eignung: Produktgutachten

Hinweis 1: Ein solches Verfahren kann beispielsweise durch eine Erneuerung des im Authenticator-Modul zum laufenden Anwendungskontext generierten Schlüsselpaars nach spätestens 3 Minuten und eine geschützte Übertragung des öffentlichen Schlüssels zum IDP umgesetzt werden.

Hinweis 2: Die beispielhaften Ablaufsequenzen (Key-Rotation und Server-Nonce) sind informativ im Anhang dargestellt.

Alt:

A_24723-01 - Signieren der SessionID zu einem Anwendungskontext

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS zur Absicherung des SSO bei jeder Nutzerauthentisierung ohne Nutzerinteraktion im Authenticator-Modul die vom sektoralen IDP übertragene SessionID zur laufenden Anwendungsinstanz mit dem zur SessionID auf dem Gerät des Versicherten gespeicherten Schlüssel signieren und an den sektoralen IDP übertragen.

<=, IDP-Sek,Sich.techn. Eignung: Gutachten

Geänderte Zuordnung:

A_24723-01 - Signieren der SessionID zu einem Anwendungskontext

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS zur Absicherung des SSO bei jeder Nutzerauthentisierung ohne Nutzerinteraktion im Authenticator-Modul die vom sektoralen IDP übertragene SessionID zur laufenden Anwendungsinstanz mit dem zur SessionID auf dem Gerät des Versicherten gespeicherten Schlüssel signieren und an den sektoralen IDP übertragen.

<=, IDP-Sek,Sich.techn. Eignung: Produktgutachten

Unter A_24748-01

Alt:

Hinweis 2: Ein Beispielablauf für SSO Unterstützung auf Anwendungsebene innerhalb einer APP ist in Kapitele 7.4.1 dargestellt.

Neu:

Hinweis 2: Ein Beispielablauf für SSO Unterstützung auf Anwendungsebene innerhalb einer APP ist im Kapitel e-7.4.1 "SSO-Unterstützung auf Anwendungsebene innerhalb einer APP" dargestellt.

Alt:

A_25870 - SSO-Unterstützung auf Anwendungsebene bei separater Authenticator-APP

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS in seinem Authenticator-Modul sicherstellen, dass ein Authorization Request mit SSO-Anforderung von einem Anwendungsfrontend kommt, bei dem der Versicherte sich bereits authentifiziert hat, um SSO-Anforderungen von nicht berechtigten Anwendungen erkennen und ablehnen zu können.

<=, IDP-Sek,Sich.techn. Eignung: Gutachten

Hinweis: Ein Beispielablauf für SSO-Unterstützung auf Anwendungsebene bei separater Authenticator-APP ist im Kapitel 7.4.2 dargestellt.

Geänderte Zuordnung:

A_25870 - SSO-Unterstützung auf Anwendungsebene bei separater Authenticator-APP

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS in seinem Authenticator-Modul sicherstellen, dass ein Authorization Request mit SSO-Anforderung von einem Anwendungsfrontend kommt, bei dem der Versicherte sich bereits authentifiziert hat, um SSO-Anforderungen von nicht berechtigten Anwendungen erkennen und ablehnen zu können.

<=, IDP-Sek,Sich.techn. Eignung: **Produktg**Gutachten

*Hinweis: Ein Beispielablauf für SSO-Unterstützung auf Anwendungsebene bei separater Authenticator-APP ist im Kapitel **7.4.2 "SSO-Unterstützung auf Anwendungsebene bei separater Authenticator-APP"** dargestellt.*

Alt:

A_24749-01 - Validierung gegen Nutzerzustimmung

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS vor einer Nutzerauthentisierung ohne Nutzerinteraktion prüfen, ob für den Fachdienst, welcher die Nutzerauthentisierung angefordert hat, die Zustimmung zum SSO-Verfahren durch den Nutzer vorliegt. Eine Nutzerauthentisierung ohne Nutzerinteraktion darf nur bei Zustimmung durchgeführt werden.

<=, IDP-Sek,Sich.techn. Eignung: Gutachten

Geänderte Zuordnung:

A_24749-01 - Validierung gegen Nutzerzustimmung

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS vor einer Nutzerauthentisierung ohne Nutzerinteraktion prüfen, ob für den Fachdienst, welcher die Nutzerauthentisierung angefordert hat, die Zustimmung zum SSO-Verfahren durch den Nutzer vorliegt. Eine Nutzerauthentisierung ohne Nutzerinteraktion darf nur bei Zustimmung durchgeführt werden.

<=, IDP-Sek,Sich.techn. Eignung: **Produktg**Gutachten

Alt:

A_25875 - Aktive Nutzerauthentifizierung im Anwendungskontext

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert,

MUSS vor einer Nutzerauthentisierung ohne Nutzerinteraktion prüfen, ob der Nutzer sich im laufenden Anwendungskontext bereits aktiv auf `gematik-loa-high` authentifiziert hat.

<=, IDP-Sek,Sich.techn. Eignung: Gutachten

Neu:

A_25875-01 - Aktive Nutzerauthentifizierung im Anwendungskontext

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS vor einer Nutzerauthentisierung ohne Nutzerinteraktion prüfen, ob der Nutzer sich im laufenden Anwendungskontext bereits aktiv auf dem Vertrauensniveau `gematik-ehealth-loa-high` oder auf dem Vertrauensniveau `gematik-ehealth-loa-substantial` - zu welcher eine Einwilligung des Anwenders zur Nutzung dieses Verfahrens zum Zugriff auf Daten mit hohem Schutzbedarf vorliegt - authentifiziert hat.

<=, IDP-Sek,Sich.techn. Eignung: ProduktgGutachten

Änderungen in Kapitel 5.3.1 "PIN der eGK ändern"

Alt:

A_15497-03 - Authenticator-Modul: PIN der eGK ändern

Das Authenticator-Modul von sektoralen IdPs gesetzlicher Krankenkassen KANN den Anwendungsfall "PIN der eGK ändern" gemäß TAB_FdV_156 umsetzen.

Tabelle 10: TAB_FdV_156 – PIN der eGK ändern

| | |
|----------------|---|
| Name | PIN der eGK ändern |
| Auslöser | Auswahl des Anwendungsfalls in der GUI |
| Akteur | Versicherter oder berechtigter Vertreter |
| Vorbedingung | Die eGK des Nutzers ist im Kartenleser gesteckt. |
| Nachbedingung | PIN wurde geändert |
| Standardablauf | Die Umsetzung ist in TAB_FdV_157 beschrieben <ul style="list-style-type: none"> 1. PL_TUC_CARD_CHANGE_PIN nutzen 2. PL_TUC_CARD_CHANGE_PIN Ergebnis verarbeiten 3. Ergebnis anzeigen |

Tabelle 11: TAB_FdV_157 – Ablaufaktivitäten – PIN der eGK ändern

| | |
|---|------------------------|
| 1. PL_TUC_CARD_CHANGE_PIN nutzen | |
| Plattformoperation | PL_TUC_CARD_CHANGE_PIN |

| | |
|---|---|
| <i>Eingangsdaten</i> | |
| Identifikator | MRPIN.home |
| Benutzerhinweis am Kartenterminaldisplay (Sicherheitsklasse 3) bzw. im FdV-Benutzerinterface bei Aufruf der Umgebungsoperation ENV_TUC_SECRET_INPUT | Alte PIN: "Eingabe alte PIN: " bzw. Neue PIN: "Eingabe neue PIN: " |
| <i>Beschreibung</i> | Der Plattformbaustein wird zur Änderung den PIN genutzt. |
| 2. Rückgabewert von PL_TUC_CARD_CHANGE_PIN verarbeiten | |
| <i>Rückgabedaten</i> | |
| OK | PIN erfolgreich geändert |
| Fehlerfälle | Siehe Beschreibung PL_TUC_CARD_CHANGE_PIN |
| <i>Beschreibung</i> | <p>Das Ändern einer PIN auf der eGK basiert auf der parametrisierten Plattformbaustein PL_TUC_CARD_CHANGE_PIN. Diese liefert ein Ergebnis zurück. Zur Änderung muss zwingend die Eingabe der alten PIN erfolgen.</p> <p>Wird durch den Versicherten ein falsches altes PIN-Geheimnis eingegeben, wird die verbleibende Anzahl der Eingabeversuche bis zur Sperrung der PINs zurückgemeldet. Im Fehlerfall wird eine Fehlermeldung entsprechenden Details zurückgegeben.</p> |
| 3. Ergebnis anzeigen | |
| <i>Hinweis an den Versicherten</i> | <p>Die Rückgabedaten des Plattformbausteins enthalten Informationen über den Erfolg der Operation auf der eGK des Versicherten. Im Fehlerfall wird der Versicherte in verständlicher Form über den Fehler informiert. Im Erfolgsfall ist dem Versicherten eine Bestätigung zur Anzeige zu bringen.</p> <p>Falls eine Warnung aufgetreten ist, wird diese dem Versicherten in verständlicher Form angezeigt. Bei einer Fehleingabe der PIN des Versicherten wird dem Versicherten die verbleibende Anzahl der Eingabeversuche bis zur Sperrung der PIN zurückgemeldet.</p> |

Neu:

A_15497-04 - Authenticator-Modul: PIN der eGK ändern

Das Authenticator-Modul von sektoralen IDP gesetzlicher Krankenkassen KANN den Anwendungsfall "PIN der eGK ändern" gemäß TAB_FdV_156 umsetzen.

Tabelle 10: TAB_FdV_156 – PIN der eGK ändern

| | |
|----------------|---|
| Name | PIN der eGK ändern |
| Auslöser | <ul style="list-style-type: none">• Auswahl des Anwendungsfalls in der GUI |
| Akteur | Versicherter oder berechtigter Vertreter |
| Vorbedingung | Die eGK des Nutzers ist im Kartenleser gesteckt mit dem Kartenlesegerät verbunden . |
| Nachbedingung | PIN wurde geändert |
| Standardablauf | Die Umsetzung ist in TAB_FdV_157 beschrieben <ol style="list-style-type: none">1. PL_TUC_CARD_CHANGE_PIN nutzen2. PL_TUC_CARD_CHANGE_PIN Ergebnis verarbeiten3. Ergebnis anzeigen |

Tabelle 11: TAB_FdV_157 – Ablaufaktivitäten – PIN der eGK ändern

| | |
|---|---|
| 1. PL_TUC_CARD_CHANGE_PIN nutzen | |
| Plattformoperation | PL_TUC_CARD_CHANGE_PIN |
| <i>Eingangsdaten</i> | |
| Identifikator | MRPIN.home |
| Benutzerhinweis am Kartenterminaldisplay (Sicherheitsklasse 3) bzw. im FdV-Benutzerinterface bei Aufruf der Umgebungsoperation ENV_TUC_SECRET_INPUT | Alte PIN: "Eingabe alte PIN: " bzw. Neue PIN: "Eingabe neue PIN: " |
| <i>Beschreibung</i> | Der Plattformbaustein wird zur Änderung den PIN genutzt. |

| | |
|---|---|
| 2. Rückgabewert von PL_TUC_CARD_CHANGE_PIN verarbeiten | |
| <i>Rückgabedaten</i> | |
| OK | PIN erfolgreich geändert |
| Fehlerfälle | Siehe Beschreibung PL_TUC_CARD_CHANGE_PIN |
| <i>Beschreibung</i> | <p>Das Ändern einer PIN auf der eGK basiert auf dem parametrisierten Plattformbaustein PL_TUC_CARD_CHANGE_PIN. Dieser liefert ein Ergebnis zurück. Zur Änderung muss zwingend die Eingabe der alten PIN erfolgen.</p> <p>Wird durch den Versicherten ein falsches altes PIN-Geheimnis eingegeben, wird die verbleibende Anzahl der Eingabeversuche bis zur Sperrung der PIN zurückgemeldet. Im Fehlerfall wird eine Fehlermeldung mit entsprechenden Details zurückgegeben.</p> |
| 3. Ergebnis anzeigen | |
| <i>Hinweis an den Versicherten</i> | <p>Die Rückgabedaten des Plattformbausteins enthalten Informationen über den Erfolg der Operation auf der eGK des Versicherten. Im Fehlerfall wird der Versicherte in verständlicher Form über den Fehler informiert. Im Erfolgsfall ist dem Versicherten eine Bestätigung zur Anzeige zu bringen.</p> <p>Falls eine Warnung aufgetreten ist, wird diese dem Versicherten in verständlicher Form angezeigt. Bei einer Fehleingabe der PIN des Versicherten wird dem Versicherten die verbleibende Anzahl der Eingabeversuche bis zur Sperrung der PIN zurückgemeldet.</p> |

< =

Änderungen in Kapitel 5.3.2 "PIN der eGK entsperren"

Alt:

A_15498-03 - Authenticator-Modul: PIN der eGK entsperren

Das Authenticator-Modul von sektoralen IdPs gesetzlicher Krankenkassen KANN den Anwendungsfall "PIN der eGK entsperren" gemäß TAB_FdV_158 umsetzen.

Tabelle 12: TAB_FdV_158 – PIN der eGK entsperren

| | |
|----------------|--|
| Name | PIN der eGK entsperren |
| Auslöser | Auswahl des Anwendungsfalls in der GUI |
| Akteur | Versicherter oder berechtigter Vertreter |
| Vorbedingung | Die eGK des Nutzers ist im Kartenleser gesteckt. Die PIN der eGK (MRPIN.home) ist gesperrt. |
| Nachbedingung | PIN des Versicherten wurde entsperrt. |
| Standardablauf | Die Umsetzung ist in TAB_FdV_159 beschrieben: <ol style="list-style-type: none"> 1. PL_TUC_CARD_UNBLOCK_PIN nutzen 2. PL_TUC_CARD_UNBLOCK_PIN Ergebnis verarbeiten 3. Ergebnis anzeigen. |

Tabelle 13: TAB_FdV_159 – Ablaufaktivitäten – PIN der eGK entsperren

| | |
|---|--|
| 1. PL_TUC_CARD_UNBLOCK_PIN aufrufen | |
| Plattformbaustein | PL_TUC_CARD_UNBLOCK_PIN |
| <i>Eingangsdaten</i> | |
| Identifikator | MRPIN.home |
| Benutzerhinweis am Kartenterminaldisplay (Sicherheitsklasse 3) bzw. im FdV-Benutzerinterface bei Aufruf der Umgebungsoperation ENV_TUC_SECRET_INPUT | PUK: "Eingabe PUK: " bzw. Neue PIN: "Eingabe neue PIN: " |
| Beschreibung | Für das Entsperren der PIN wird ein Plattformbaustein genutzt. |
| 2. PL_TUC_CARD_UNBLOCK_PIN Ergebnis verarbeiten | |
| <i>Rückgabedaten</i> | |
| OK | PIN wurde entsperrt. |

| | |
|------------------------------------|--|
| PasswordBlocked | Die PUK wurde wegen zu häufiger Nutzung gesperrt. Der Versicherte muss darüber in verständlicher Form informiert und auf die Notwendigkeit einer neuen eGK hingewiesen werden. |
| Weitere Fehlerfälle | Siehe Beschreibung PL_TUC_CARD_UNBLOCK_PIN |
| <i>Beschreibung</i> | Das Entsperren einer PIN auf der eGK basiert auf dem parametrisierten Plattformbaustein PL_TUC_CARD_UNBLOCK_PIN. Zum Entsperren muss zwingend die Eingabe einer PUK erfolgen. Wird durch den Versicherten ein falsches PUK-Geheimnis eingegeben, wird die verbleibende Anzahl der Eingabeversuche bis zur Sperrung des PUKs zurückgemeldet. Im Fehlerfall wird eine Fehlermeldung mit entsprechenden Details zurückgegeben. |
| 3. Ergebnis anzeigen | |
| <i>Hinweis an den Versicherten</i> | Die Rückgabedaten des Plattformbausteins enthalten Informationen über den Erfolg der Operation auf der eGK des Versicherten. Im Fehlerfall wird der Versicherte in verständlicher Form über den Fehler informiert. Im Erfolgsfall ist dem Versicherten eine Bestätigung zur Anzeige zu bringen. Falls eine Warnung aufgetreten ist, wird diese dem Versicherten in verständlicher Form angezeigt. |

<=

Neu:**A_15498-04 - Authenticator-Modul: PIN der eGK entsperren**

Das Authenticator-Modul von sektoralen IdPs gesetzlicher Krankenkassen KANN den Anwendungsfall "PIN der eGK entsperren" gemäß TAB_FdV_158 umsetzen.

Tabelle 12: TAB_FdV_158 – PIN der eGK entsperren

| | |
|--------------|---|
| Name | PIN der eGK entsperren |
| Auslöser | <ul style="list-style-type: none"> Auswahl des Anwendungsfalls in der GUI |
| Akteur | Versicherter oder berechtigter Vertreter |
| Vorbedingung | Die eGK des Nutzers ist im Kartenleser gesteckt mit dem Kartenlesegerät verbunden. |

| | |
|----------------|--|
| | Die PIN der eGK (MRPIN.home) ist gesperrt. |
| Nachbedingung | PIN des Versicherten wurde entsperrt. |
| Standardablauf | <p>Die Umsetzung ist in TAB_FdV_159 beschrieben</p> <ol style="list-style-type: none"> 1. PL_TUC_CARD_UNBLOCK_PIN nutzen 2. PL_TUC_CARD_UNBLOCK_PIN Ergebnis verarbeiten 3. Ergebnis anzeigen |

Tabelle 13: TAB_FdV_159 – Ablaufaktivitäten – PIN der eGK entsperren

| | |
|---|---|
| 1. PL_TUC_CARD_UNBLOCK_PIN aufrufen | |
| Plattformbaustein | PL_TUC_CARD_UNBLOCK_PIN |
| <i>Eingangsdaten</i> | |
| Identifikator | MRPIN.home |
| Benutzerhinweis am Kartenterminaldisplay (Sicherheitsklasse 3) bzw. im FdV-Benutzerinterface bei Aufruf der Umgebungsoperation ENV_TUC_SECRET_INPUT | PUK: "Eingabe PUK: " bzw. Neue PIN: "Eingabe neue PIN: " |
| Beschreibung | Für das Entsperren der PIN wird ein Plattformbaustein genutzt. |
| 2. PL_TUC_CARD_UNBLOCK_PIN Ergebnis verarbeiten | |
| <i>Rückgabedaten</i> | |
| OK | PIN wurde entsperrt. |
| PasswordBlocked | Die PUK wurde wegen zu häufiger Nutzung gesperrt. Der Versicherte muss darüber in verständlicher Form informiert und auf die Notwendigkeit einer neuen eGK hingewiesen werden. |
| Weitere Fehlerfälle | Siehe Beschreibung PL_TUC_CARD_UNBLOCK_PIN |

| | |
|------------------------------------|--|
| <i>Beschreibung</i> | <p>Das Entsperren einer PIN auf der eGK basiert auf dem parametrierten Plattformbaustein PL_TUC_CARD_UNBLOCK_PIN. Zum Entsperren muss zwingend die Eingabe einer PUK erfolgen.</p> <p>Wird durch den Versicherten ein falsches PUK-Geheimnis eingegeben, wird die verbleibende Anzahl der Eingabeversuche bis zur Sperrung der PUK zurückgemeldet. Im Fehlerfall wird eine Fehlermeldung mit entsprechenden Details zurückgegeben.</p> |
| 3. Ergebnis anzeigen | |
| <i>Hinweis an den Versicherten</i> | <p>Die Rückgabedaten des Plattformbausteins enthalten Informationen über den Erfolg der Operation auf der eGK des Versicherten. Im Fehlerfall wird der Versicherte in verständlicher Form über den Fehler informiert. Im Erfolgsfall ist dem Versicherten eine Bestätigung zur Anzeige zu bringen.</p> <p>Falls eine Warnung aufgetreten ist, wird diese dem Versicherten in verständlicher Form angezeigt.</p> |

<=

Änderungen in Kapitel 6.5.2 "Weitere Dokumente"

Neu:

| [Quelle] | Herausgeber (Erscheinungsdatum): Titel |
|--|--|
| [ANDROIDAPPLINKS] | https://developer.android.com/studio/write/app-link-indexing |
| [APPLEUNIVERSAL] | https://developer.apple.com/ios/universal-links/ |
| Verordnung (EU) Nr. 910/2014 auch eIDAS Verordnung genannt | VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG |
| Durchführungsverordnung (EU) 2015/1502 | DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1502 DER KOMMISSION vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt |

| | |
|--|--|
| [GKV-SV Richtlinie "Kontakt mit Versicherten"] | Richtlinie des GKV-Spitzenverbandes zu Maßnahmen zum Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme nach § 217f Absatz 4b SGB V (GKV-SV Richtlinie Kontakt mit Versicherten) vom 14.12.2018 |
| [Uniform Resource Identifier (URI)] [RFC3986] | Uniform Resource Identifier (URI): Generic Syntax (Januar 2005) https://datatracker.ietf.org/doc/html/rfc3986 |
| [The OAuth 2.0 Authorization Framework] [RFC6749] | The OAuth 2.0 Authorization Framework (Oktober 2012) https://datatracker.ietf.org/doc/html/rfc6749 |
| [Hypertext Transfer Protocol (HTTP/1.1)] [RFC7231] | Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content (Juni 2014) https://datatracker.ietf.org/doc/html/rfc7231 |
| [JSON Web Key (JWK)] [RFC7517] | JSON Web Key (JWK) (Mai 2015) https://www.rfc-editor.org/rfc/rfc7517 |
| [JSON Web Token (JWT)] [RFC7519] | JSON Web Token (JWT) (Mai 2015) https://datatracker.ietf.org/doc/html/rfc7519 |
| [Proof Key for Code Exchange by OAuth Public Clients] [RFC7636] | Proof Key for Code Exchange by OAuth Public Clients (September 2015) https://datatracker.ietf.org/doc/html/rfc7636 |
| [OAuth 2.0 for Native Apps] [RFC8252] | Auth 2.0 for Native Apps (Oktober 2017) https://datatracker.ietf.org/doc/html/rfc8252 |
| [OpenID Connect Core 1.0] | OpenID Connect Core 1.0 (incorporating errata set 1, November 2014) https://openid.net/specs/openid-connect-core-1_0.html |
| [OpenID Connect Federation 1.0] [OpenID Federation 1.0] | OpenID Connect Federation 1.0 (Draft 2140, 24. Oktober 20242022) https://openid.net/specs/openid-connect-federation-1_0-21.html https://openid.net/specs/openid-federation-1_0.html |
| [OpenID Connect Discovery 1.0] | OpenID Connect Discovery 1.0 (incorporating errata set 2, . Dezember 2023) https://openid.net/specs/openid-connect-discovery-1_0.html |
| [OAuth 2.0 Pushed Authorization] | OAuth 2.0 Pushed Authorization Requests (September 2021) https://datatracker.ietf.org/doc/html/rfc9126 |

| | |
|--|---|
| Requests] [RFC9126] | |
| [ISO18045] | Publicly Available Standards (iso.org) |
| [TR-03107-1] | Technische Richtlinie TR-03107-1 Version 1.1.1, 07.05.2019 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.pdf;jsessionid=FFBC05B6EE23EE8461127AC755D621FC.internet461?__blob=publicationFile&v=1 |
| [KeyInfo#getSecurityLevel()] | https://developer.android.com/reference/android/security/keystore/KeyInfo#getSecurityLevel() |
| [KeyInfo#isInsideSecureHardware()] | https://developer.android.com/reference/android/security/keystore/KeyInfo#isInsideSecureHardware() |
| [support.apple.com/guide/security] | https://support.apple.com/de-de/guide/security/sec59b0b31ff/web |
| [OpenID Connect Native SSO for Mobile Apps 1.0] | OpenID Connect Native SSO for Mobile Apps 1.0 - draft 03 (Juli 2019) https://openid.net/specs/openid-connect-native-sso-1_0.html |
| [DiGA-Kriterien] | Datenschutzkriterien nach § 139e Absatz 11 SGB V und § 78a Absatz 8 SGB XI https://www.bfarm.de/DE/Medizinprodukte/Aufgaben/DiGA-und-DiPA/Datenschutzkriterien/_node.html |

Änderungen in Kapitel 7.1.4 "Detailinformationen zum App-App-Flow"

Alt:

Tabelle 16 : Body Entity Statement des Federation Master

| iss | URL | "http://master0815.de" | iss anstelle issuer ist hier Spec konform = URL des Federation Master (wird definiert) |
|-----|-----|------------------------|--|
| sub | URL | "http://master0815.de" | URL des Federation Master (wird definiert) = iss |

| | | | |
|----------------------------|--|--|--|
| iat | Alle time Werte in Sekunden seit 1970, [RFC 7519 Sect.2] | 1645398001 | 2022-02-21 00:00:01 |
| exp | Alle time Werte in Sekunden seit 1970, RFC 7519 Sect.2 [] | 1646002800 | Beispielhafte Gültigkeit von 7 Tagen |
| jwks | JWKS Objekt | unter anderem "master0815-1" | Schlüssel für die Signatur des Entity Statement. Gemäß [OpenID Federation 1.0 - draft 41] werden hier auch Schlüssel für einen Key-Rollover transportiert. |
| <i>metadata {</i> | | | |
| <i>federation_entity {</i> | | | |
| federation_fetch_endpoint | URL | "http://master0815.de/federation_fetch_endpoint" | Adresse des Endpunktes zum Abrufen einzelner oder aller Statements des Masters über IDPs und Fachdienste |
| federation_list_endpoint | URL | Adresse des Endpunktes zum Abrufen der Liste aller bekannten Entity Identifier | "http://master0815.de/federation_list" |
| idp_list_endpoint | URL | "http://master0815.de/idp_list.jws" | non-Standard Claim - ggf. auch als reine Konfiguration machbar z. B. /.well- |

| | | | |
|----|--|--|----------------------|
| | | | known/entity_listing |
| }} | | | |

Neu:

Tabelle 16 : Body Entity Statement des Federation Master

| iss | URL | "http://master0815.de" | iss anstelle issuer ist hier Spec konform = URL des Federation Master (wird definiert) |
|---------------------|--|------------------------------|---|
| sub | URL | "http://master0815.de" | URL des Federation Master (wird definiert) = iss |
| iat | Alle time Werte in Sekunden seit 1970, [RFC7519#section-2] | 1645398001 | 2022-02-21 00:00:01 |
| exp | Alle time Werte in Sekunden seit 1970, [RFC7519#section-2] | 1646002800 | Beispielhafte Gültigkeit von 7 Tagen |
| jwks | JWKS-Objekt | unter anderem "master0815-1" | Schlüssel für die Signatur des Entity Statement. Gemäß [OpenID Federation 1.0 - draft 41] werden hier auch Schlüssel für einen Key-Rollover transportiert. |
| metadata { | | | |
| federation_entity { | | | |

| | | | |
|---------------------------|--|--|--|
| federation_fetch_endpoint | URL | "http://master0815.de/federation_fetch_endpoint" | Adresse des Endpunktes zum Abrufen einzelner oder aller Statements des Masters über IDPs und Fachdienste |
| federation_list_endpoint | URL | Adresse des Endpunktes zum Abrufen der Liste aller bekannten Entity Identifier | "http://master0815.de/federation_list" |
| idp_list_endpoint | URL | "http://master0815.de/idp_list.jws" | non Standard Claim - ggf. auch als reine Konfiguration machbar z. B. /.well-known/entity_listing |
| organization_name | String (max. 128 Zeichen) Wertebereich: h: ^[ÄÖÜäöüß \\w\\ \\- \\.\\&\\+*\\V] {1,128} | | |
| }} | | | |

Alt:

Tabelle 21 : Body Entity Statement des sektoralen IDP

| Name | Werte | Beispiel | Anmerkungen |
|------|-------|----------------------|---|
| iss | URL | "https://idp4711.de" | iss anstelle issuer ist hier Spec konform = URL des IDP (variabel je Mandant/Kasse) |
| sub | URL | "https://idp4711.de" | URL des IDP (variabel je Mandant/Kasse) = iss |

| | | | |
|-------------------|--|-------------------------------|---|
| iat | Alle time Werte in Sekunden seit 1970, RFC 7519 Sect.2 | 1645484401 | 2022-02-22 00:00:01 |
| exp | Alle time Werte in Sekunden seit 1970, RFC 7519 Sect.2 | 1645570800 | Gültigkeit von 24 Stunden |
| jwks | JWKS Objekt | unter anderem "idp4711-3" | Schlüssel für die Signatur des Entity Statement |
| authority_hints | [string] | "http://master0815.de" | iss Bezeichnung des Federation Master |
| metadata { | | | |
| openid_provider { | | | |
| issuer | URL | "https://idp4711.de" | URL des IDP (variabel je Mandant/Kasse) |
| signed_jwks_uri | URL | "https://idp4711.de/jws.json" | Ablageort für weitere Schlüssel des IDP etwa die zur Signatur seiner Token Wenn eine signed_jwks_uri im Entity Statement angegeben ist müssen diese Schlüssel importiert werden. |
| organization_name | | | Name des IDP - wird genutzt in der Auswahlliste für den Benutzer (Alternativ name im Feld federation_entity) |

| | | | |
|---------------------------------------|--|-------------------------------|--|
| | | | nutzen) |
| logo_uri | URL | „https://idp4711.de/logo.png“ | Attribut ist nicht im Standard, ist nach OpenID Connect Discovery 1.0 - aber in Federation Spec auch für ein OP gelistet |
| authorization_endpoint | URL | „https://idp4711.de/Auth“ | Adresse des IDP-Endpunkt (im Internet) |
| token_endpoint | URL | „https://idp4711.de/Token“ | Adresse des IDP-Endpunkt (im Internet) |
| pushed_authorization_request_endpoint | URL | „https://idp4711.de/PAR_Auth“ | Adresse des IDP-Endpunkt (im Internet) nach OAuth 2.0 Pushed Authorization Requests (section-5) |
| client_registration_types_supported | [<i>automatic</i>] | - | gemäß OpenID Connect Federation 1.0 (section-4.2) |
| subject_types_supported | [<i>pairwise</i>] | - | |
| response_types_supported | [<i>code</i>] | - | Weitere Werte sind möglich, aber nicht innerhalb der Föderation vorgesehen. |
| scopes_supported | [<i>openid</i> <i>urn:telematik:geburtsdatum</i> <i>urn:telematik:alter</i> <i>urn:telematik:display_name</i> <i>urn:telematik:given_name</i>] | - | Weitere Werte sind möglich - The OAuth 2.0 Authorization Framework (section-3.3) |

| | | | |
|---------------------------------------|---|---|--|
| | <code>urn:telematik:geschlecht</code> <code>urn:telematik:email</code> <code>urn:telematik:versicherter</code> <code>urn:telematik:family_name</code> <code>]</code> | | |
| claims_supported | <code>[birthdate,</code> <code>urn:telematik:claims:alter,</code> <code>urn:telematik:claims:display_name,</code> <code>urn:telematik:claims:given_name,</code> <code>urn:telematik:claims:geschlecht,</code> <code>urn:telematik:claims:email,</code> <code>urn:telematik:claims:profession,</code> <code>urn:telematik:claims:id,</code> <code>urn:telematik:claims:organization</code> <code>]</code> | - | Weitere Werte sind möglich - The OAuth 2.0 Authorization Framework (section-3.3) |
| claims_parameter_supported | true | | |
| response_modes_supported | <code>[query]</code> | - | |
| grant_types_supported | <code>[authorization_code]</code> | - | |
| require_pushed_authorization_requests | true | - | OAuth 2.0 Pushed Authorization Requests (section-5) |
| token_endpoint_auth_methods_supported | <code>[self_signed_tls_client_auth]</code> | - | Weitere Werte sind möglich, aber nicht innerhalb der Föderation vorgesehen. |

| | | | |
|--|---|---|--|
| request_authentication_methods_supported | { " ": ["none"], " ": ["self_signed_tls_client_auth"] } | - | |
| id_token_signing_alg_values_supported | [ES256] | - | Weitere Werte sind möglich, aber nicht innerhalb der Föderation vorgesehen. |
| id_token_encryption_alg_values_supported | [ECDH-ES] | - | Weitere Werte sind möglich, aber nicht innerhalb der Föderation vorgesehen. |
| id_token_encryption_enc_values_supported | [A256GCM] | - | Weitere Werte sind möglich, aber nicht innerhalb der Föderation vorgesehen. |
| user_type_supported | [IP = Insured Person] | ["IP"] | Bei sektoralen IDP für Versicherte muss der Wert immer "IP" sein. |
| } | | | |
| federation_entity { | | | |
| name | String | "IDP 4711" | Name des IDP - wird genutzt in der Auswahlliste für den Benutzer (alternativ <code>organization_name</code> aus Metadata nutzen) |
| contacts | [string] | ["support@idp4711.de", "info@idp4711.de"] | optional |
| homepage_uri | URL | "https://idp4711." | optional |

| | | | |
|----|--|-----|--|
| | | de" | |
| }} | | | |

Neu:

Tabelle 21 : Body Entity Statement des sektoralen IDP

| Name | Werte | Beispiel | Anmerkungen |
|-------------------|--|---------------------------|---|
| iss | URL | "https://idp4711.de" | iss anstelle issuer ist hier Spec konform = URL des IDP (variabel je Mandant/Kasse) |
| sub | URL | "https://idp4711.de" | URL des IDP (variabel je Mandant/Kasse) = iss |
| iat | Alle time Werte in Sekunden seit 1970, [RFC7519#section-2] | 1645484401 | 2022-02-22 00:00:01 |
| exp | Alle time Werte in Sekunden seit 1970, [RFC7519#section-2] | 1645570800 | Gültigkeit von 24 Stunden |
| jwks | JWKS-Objekt | unter anderem "idp4711-3" | Schlüssel für die Signatur des Entity Statements |
| authority_hints | [string] | "http://master0815.de" | iss Bezeichnung des Federation Masters |
| metadata { | | | |
| openid_provider { | | | |
| issuer | URL | "https://idp4711.de" | URL des IDP (variabel je Mandant/Kasse) |

| | | | |
|-----------------------------------|-----|-------------------------------|---|
| signed_jwks_uri | URL | "https://idp4711.de/jws.json" | Ablageort für weitere Schlüssel des IDP, etwa die zur Signatur seiner Token Wenn eine signed_jwks_uri im Entity Statement angegeben ist, müssen diese Schlüssel importiert werden. |
| organization_name (deprecated) | | | Name des IDP wird genutzt in der Auswahlliste für den Benutzer (Alternativ name im Feld federation_entity nutzen) Der organization_name ist optional und muss nicht zwingend belegt sein. Der Claim wird aus der Tabelle entfernt. Für die Darstellung der Organisation in der TI-Föderation ist im metadata-Block "federation_entity/organization_name" zu belegen. |
| logo_uri | URL | „https://idp4711.de/logo.png“ | Attribut ist nicht im Standard, ist nach [OpenID Connect Discovery 1.0] https://openid.net/specs/openid-connect-discovery-1_0.html aber in Federation Spec auch für ein OP gelistet |
| authorization_endpoint | URL | „https://idp4711.de/Auth“ | Adresse des IDP-Endpunkt (im Internet) |
| token_endpoint | URL | „https://idp4711.de/Token“ | Adresse des IDP-Endpunkt (im Internet) |

| | | | |
|---------------------------------------|---|-------------------------------|---|
| pushed_authorization_request_endpoint | URL | „https://idp4711.de/PAR_Auth“ | Adresse des IDP-Endpunktes (im Internet) nach [OAuth 2.0 Pushed Authorization Requests#section-5] |
| client_registration_types_supported | [<i>automatic</i>] | - | gemäß OpenID Connect Federation 1.0 (section-4.2) [OpenID Federation 1.0#section-5.1.2] |
| subject_types_supported | [<i>pairwise</i>] | - | |
| response_types_supported | [<i>code</i>] | - | Weitere Werte sind möglich, aber nicht innerhalb der Föderation vorgesehen. |
| scopes_supported | [<i>openid urn:telematik:geburtsdatum urn:telematik:alter urn:telematik:display_name urn:telematik:given_name urn:telematik:geschlecht urn:telematik:email urn:telematik:versicherter urn:telematik:familienname</i>] | - | Weitere Werte sind möglich - [The OAuth 2.0 Authorization Framework#section-3.3] |
| claims_supported | [birthdate, urn:telematik:claims:alter, urn:telematik:claims:display_name, urn:telematik:claims:given_name, urn:telematik:claims:geschlecht, urn:telematik:claims:email, urn:telematik:claims: | - | Weitere Werte sind möglich - [The OAuth 2.0 Authorization Framework#section-3.3] |

| | | | |
|--|---|---|---|
| | s:profession, urn:telematik:claim s:id, urn:telematik:claim s:organization] | | |
| claims_parameter_supported | true | | |
| response_modes_supported | [<i>query</i>] | - | |
| grant_types_supported | [<i>authorization_code</i>] | - | |
| require_pushed_authorization_requests | true | - | [OAuth 2.0 Pushed Authorization Requests#section-5] |
| token_endpoint_auth_methods_supported | [<i>self_signed_tls_client_auth</i>] | - | Weitere Werte sind möglich, aber nicht innerhalb der Föderation vorgesehen. |
| request_authentication_methods_supported | { " ": [<i>none</i>], " ": [<i>self_signed_tls_client_auth</i>] } | - | |
| id_token_signing_alg_values_supported | [<i>ES256</i>] | - | Weitere Werte sind möglich, aber nicht innerhalb der Föderation vorgesehen. |
| id_token_encryption_alg_values_supported | [<i>ECDH-ES</i>] | - | Weitere Werte sind möglich, aber nicht innerhalb der Föderation vorgesehen. |
| id_token_encryption_enc_values_supported | [<i>A256GCM</i>] | - | Weitere Werte sind möglich, aber nicht innerhalb der Föderation vorgesehen. |

| | | | |
|---------------------|---|---|---|
| user_type_supported | [IP = Insured Person] | ["IP"] | Bei sektoralen IDP für Versicherte muss der Wert immer "IP" sein. |
| } | | | |
| federation_entity { | | | |
| name (deprecated) | String | "IDP 4711" | Organisationsname des Teilnehmers der TI-Föderation, Name des IDP - wird genutzt in der Auswahlliste für den Benutzer |
| organization_name | String (max. 128 Zeichen) Wertebereich: ^[ÄÖÜäöüßw\ \- \. \& \+ * \V]{1,128} | "IDP 4711" | Organisationsname des Teilnehmers der TI-Föderation, Name des IDP - wird genutzt in der Auswahlliste für den Benutzer |
| contacts | [string] | ["support@idp4711.de", "info@idp4711.de"] | optional |
| homepage_uri | URL | "https://idp4711.de" | optional |
| }} | | | |

Alt:**signed_jwks_uri**

Ablageort für weitere Schlüssel des IDP etwa die zur Signatur seiner Token. Wenn eine `signed_jwks_uri` im Entity Statement angegeben ist, müssen auch diese Schlüssel importiert werden.

Die Auflösung der `signed_jwks_uri` erfolgt dabei mittels HTTP GET Request.

Response auf GET an die Adresse "https://idp4711.de/jws.json"

HTTP 200 mit Content-Type: application/jwk-set+json

Neu:**signed_jwks_uri**

Ablageort für weitere Schlüssel des IDP, etwa die zur Signatur seiner Token. Wenn eine `signed_jwks_uri` im Entity Statement angegeben ist, müssen auch diese Schlüssel importiert werden.

Die Auflösung der `signed_jwks_uri` erfolgt dabei mittels HTTP GET Request.

Response auf GET an die Adresse "`https://idp4711.de/jws.json`"

HTTP 200 mit Content-Type: `application/jwk-set+json`

Alt:

Tabelle 27 : Parameter Pushed Authorization Request

| Name | Werte | Beispiel | Anmerkungen |
|------------------------------------|---|---|---|
| <code>client_id</code> | URL | " <code>https://Fachdienst007.de</code> " | kein ";" und kein "†" (definiert gem. Unicode U+253C (9532)), kein Leerzeichen |
| <code>state</code> | VSCHAR (max. 512 Zeichen) | <code>bg1jgktnmelk</code> | Generierter Wert, ist ein anderer <code>state</code> als in dem OAUTH Request des Frontend an den Fachdienst |
| <code>redirect_uri</code> | URL | <code>https://Fachdienst007.de/AS</code> | Adresse des Fachdienstes Authorization Server |
| <code>code_challenge</code> | Hash über <code>CODE_VERIFIER</code> des Fachdienstes | K2- <code>mvd94bdd5i1d0x7FTD_sFNR</code> <code>K4cxx-vDIbpFL2u9W</code> | <code>CODE_VERIFIER</code> ist ein beliebiger Wert, über den der Hash gebildet wird. |
| <code>code_challenge_method</code> | <code>S256</code> | - | |
| <code>response_type</code> | <code>code</code> | - | |
| <code>nonce</code> | (max. 512 Zeichen) | <code>274312:dj83hs9s</code> | Beliebig generierter Wert, hier wird auch die <code>nonce</code> genutzt, die mit dem <code>ID_TOKEN</code> abgeglichen wird. |
| <code>scope</code> | [string] | " <code>openid</code> <code>urn:telematik:display_name</code> " | The OAuth 2.0 Authorization Framework (section- |

| | | | |
|------------|---|-----------------------------|----------------------|
| | | urn:telematik:versicherter" | 3.3) |
| acr_values | "gematik-ehealth-loa-high" oder "gematik-ehealth-loa-substantial" | "gematik-ehealth-loa-high" | |

Zu den Scopes und Claims bzgl. der Identitäten für Versicherte siehe A_22989-01 in Kapitel 4.2.4.2.

Neu:

Tabelle 27: Parameter Pushed Authorization Request

| Name | Werte | Beispiel | Anmerkungen |
|-----------------------|--|---|--|
| client_id | URL | "https://Fachdienst007.de" | kein ";" und kein "†" (definiert gem. Unicode U+253C (9 532)), kein Leerzeichen |
| state | VSCHAR (max. 512 Zeichen) | bg1jgktnelk | Generierter Wert, ist ein anderer state als in dem OAUTH Request des Frontends an den Fachdienst |
| redirect_uri | URL | https://Fachdienst007.de/AS | Adresse des Fachdiensts Authorization-Server |
| code_challenge | Hash über CODE_VERIFIER des Fachdienstes | K2-mvd94bdd5i1d0x7FTD_sFNRK4cxa-vDIbpfL2u9W | CODE_VERIFIER ist ein beliebiger Wert, über den der Hash gebildet wird |
| code_challenge_method | S256 | - | |
| response_type | code | - | |

| | | | |
|--------|--------------------|--|--|
| nonce | (max. 512 Zeichen) | 274312:dj83hs9s | Beliebig generierter Wert, hier wird auch die nonce genutzt, die mit dem ID-Token abgeglichen wird |
| scope | [string] | "openid urn:telematik:display_name urn:telematik:versicherter" | [The OAuth 2.0 Authorization Framework#section-3.3] |
| claims | URL-encoded String | Beispiel 1: AMR JSON Objekt: <pre>{ "id_token": { "amr": { "essential": true, "values": ["urn:telematik:auth:eGK"], "email": { "essential": true } } } }</pre> URL-Encoded: <pre>claims=%7B%22id_token%22%3A%7B%22amr%22%3A%7B%22essential%22%3Atrue,%22values%22%3A%5B%22urn%3Atelematik%3Aauth%3AeGK%22%5D%7D,%22email%22%3A%7B%22essential%22%3Atrue%7D%7D%7D</pre> | Der claims Parameter kann genutzt werden, um dem IDP zu signalisieren, welche der angeforderten Claims als "essentiell" und somit "nicht abwählbar" im Einwilligungsdialog für den Nutzer dargestellt werden sollen. Freiwillige Claims, wie auch alle Scopes können stets vom Nutzer ausgewählt werden. |
| | | Beispiel 2: ACR JSON Objekt: <pre>{ "id_token": { "acr": { "essential": true, "values": ["gematik-ehealth-loa-high"] } } }</pre> URL-Encoded: <pre>claims=%7B%22id_token%22%3A%7B%22acr%22%3A%7B%22essential%22%3Atrue,%22values%22%3A%5B%22gematik-ehealth-loa-high%22%5D%7D%7D</pre> | Wenn im claims Parameter das Authentisierungsniveau gematik-ehealth-loa-high gemeinsam mit dem "essential" Attribut mit dem Wert "true" angefordert wird, DARF der IDP NICHT Authentisierungsverfahren verwenden, die dieses Authentisierungsniveau |

| | | | |
|------------|---|---|---|
| | | B%22acr%22%3A%7B%22essential%22%3A%20true%2C%22values%22%3A%5B%22gematik-ehealth-loa-high%22%5D%7D%7D | <p>eaue unterbrechen. Wenn kein Authentisierungsverfahren für dieses Vertrauensniveau zur Verfügung steht, so MUSS er den Authorization Request mit einer Fehlermeldung ablehnen.</p> |
| acr_values | "gematik-ehealth-loa-high" oder "gematik-ehealth-loa-substantial" | "gematik-ehealth-loa-high" | Obligatorischer Parameter, wenn nicht alternativ als acr (siehe Beispiel 2 in claims) im claims Parameter explizit angefordert wird. |

Zu den Scopes und Claims bzgl. der Identitäten für Versicherte siehe A_22989-01* im Kapitel 4.2.4.2 "Token-Endpunkt Ausgangsdaten"

Alt:

Tabelle 29: Body des Entity Statement des Fachdienstes

| Name | Werte | Beispiel | Anmerkungen |
|------|--|---------------------------|--|
| iss | URL | "https://Fachdienst07.de" | iss anstelle issuer ist hier Spec konform = URL des Fachdienstes |
| sub | URL | "https://Fachdienst07.de" | URL des Fachdienstes (variabel je Mandant/Kasse) = iss |
| iat | Alle time Werte in Sekunden seit 1970, RFC 7519 Sect.2 , | 1645484401 | 2022-02-22 00:00:01 |

| | | | |
|------------------------|--|--|---|
| exp | Alle time Werte in Sekunden seit 1970, RFC 7519 Sect.2 , | 1645570800 | //Gültigkeit von 24 Stunden |
| jwt | JWKS Objekt | unter anderem "Fachdienst007-42" | Schlüssel für die Signatur des Entity Statement |
| authority_hints | [string] | "http://master0815.de" | iss Bezeichnung des Federation Master |
| metadata { | | | |
| openid_relying_party { | | | |
| signed_jwt_uri | URL | https://Fachdienst007.de/jws.json | enthält Schlüssel für die Signatur des Entity Statement, die TLS Client Schlüssel und Zertifikate (x5c, use = sig) und für die Verschlüsselung der ID_TOKEN (use = enc) Wenn eine signed_jwt_uri im Entity Statement angegeben ist müssen auch diese Schlüssel importiert werden |
| jwt | Liste von JWKS Objekten | unter anderem "Fachdienst007-69", wenn nicht im signed_jwt_uri transportiert | Optional - gemäß https://openid.net/specs/openid-connect-federation-1_0.html#name-openid-connect-and-oauth2-m für den Fall das ein Fachdienst signed_jwt_uri nicht anbieten kann. |
| organization_name | String | 007 GmbH | Optional: Name der Organisation die hinter dem |

| | | | |
|---------------------------------------|-----------------------------|-----------------------------------|---|
| | | | Fachdienst steht |
| client_name | String | Fachdienst007 | Name des Fachdienstes (redundant zum name in den "Federation Entity"claims) |
| logo_uri | URL | https://Fachdienst007.de/logo.jpg | Optional: Wenn vorhanden zur Darstellung der Anfrage durch den Authenticator/IDP zu verwendet |
| redirect_uris | [URLs] | https://Fachdienst007.de/client | One of these registered Redirection URI values MUST exactly match the redirect_uri parameter value used in each Authorization Request |
| response_types | [code] | - | |
| client_registration_types | [automatic] | - | gemäß OpenID Connect Federation 1.0 (section-4.1) |
| grant_types | [authorization_code] | - | OpenID Connect Dynamic Client Registration 1.0 (section-2) |
| require_pushed_authorization_requests | true | - | OAuth 2.0 Pushed Authorization Requests (section-6) |
| token_endpoint_auth_method | self_signed_tls_client_auth | - | |

| | | | |
|---------------------------------|---|--|--|
| default_acr_values | ["gematik-ehealth-loa-high" "gematik-ehealth-loa-substantial"] | ["gematik-ehealth-loa-high"] | OpenID Connect Dynamic Client Registration 1.0 (section-2) |
| id_token_signed_response_alg | ES256 | - | Weitere Werte sind möglich. |
| id_token_encrypted_response_alg | ECDH-ES | - | Weitere Werte sind möglich. |
| id_token_encrypted_response_enc | A256GCM | - | Weitere Werte sind möglich. |
| scope | [string] | "openid urn:telematik:display_name urn:telematik:versicherter" | String mit space-delimited scope values |
| } | | | |
| federation_entity{ | | | |
| name | string | "Fachdienst007" | Optional: Name des Fachdienstes - wird z. B., genutzt in der Consent-Freigabe des Benutzers (redundant zum client_name) |
| contacts | [strings] | ["Support@Fachdienst007.de", "info@Fachdienst007.de"] | Optional |
| homepage_uri | URL | "https://Fachdienst007.de" | Optional |
| }} | | | |

Neu:

Tabelle 29: Body des Entity Statement des Fachdienstes

| Name | Werte | Beispiel | Anmerkungen |
|-------------------------------|--|-------------------------------------|---|
| iss | URL | "https://Fachdienst07.de" | iss anstelle issuer ist hier Spec konform = URL des Fachdienstes |
| sub | URL | "https://Fachdienst07.de" | URL des Fachdienstes (variabel je Mandant/Kasse) = iss |
| iat | Alle time Werte in Sekunden seit 1970, RFC7519 #section-2[] | 1645484401 | 2022-02-22 00:00:01 |
| exp | Alle time Werte in Sekunden seit 1970, RFC7519 #section-2[] | 1645570800 | //Gültigkeit von 24 Stunden |
| jwks | JWKS-Objekt | unter anderem "Fachdienst007-42" | Schlüssel für die Signatur des Entity Statement |
| authority_hints | [string] | "http://master0815. de" | iss Bezeichnung des Federation Master |
| <i>metadata {</i> | | | |
| <i>openid_relying_party {</i> | | | |
| signed_jwks_uri | URL | https://Fachdienst007.de/jws.json | enthält Schlüssel für die Signatur des Entity Statement, die TLS Client Schlüssel und Zertifikate (x5c, use = sig) und für die Verschlüsselung der ID_TOKEN (use = enc) |

| | | | |
|-------------------|-------------------------|---|---|
| | | | Wenn ein signed_jwks_uri im Entity Statement angegeben ist, müssen auch diese Schlüssel importiert werden. |
| jwks | Liste von JWKS-Objekten | unter anderem "Fachdienst007-69", wenn nicht im signed_jwks_uri transportiert | Optional - gemäß https://openid.net/specs/openid-connect-federation-1-0.html#name-openid-connect-and-oauth2-m [OpenID Federation 1.0#section-5.2.1] für den Fall, dass ein Fachdienst signed_jwks_uri nicht anbieten kann. |
| organization_name | String | 007 GmbH | Optional: Name der Organisation die hinter dem Fachdienst steht |
| client_name | String | Fachdienst007 | Name des Fachdienste - wird in der Darstellung im Consent Dialog verwendet |
| logo_uri | URL | https://Fachdienst007.de/logo.jpg | Optional: Wenn vorhanden zur Darstellung der Anfrage durch den Authenticator/IDP zu verwendet |
| redirect_uris | [URLs] | https://Fachdienst007.de/client | One of these registered Redirection URI values MUST exactly match the redirect_uri parameter value used in each Authorization Request |

| | | | |
|---------------------------------------|---|--|---|
| response_types | [code] | - | |
| client_registration_types | [automatic] | - | gemäß OpenID Connect Federation 1.0 (section 4.1) [OpenID Federation 1.0#section-5.1.2] |
| grant_types | [authorization_code] | - | [OpenID Connect Dynamic Client Registration 1.0#ClientMetadata] |
| require_pushed_authorization_requests | true | - | [RFC9126#section-6] |
| token_endpoint_auth_method | self_signed_tls_client_auth | - | |
| default_acr_values | ["gematik-ehealth-loa-high" "gematik-ehealth-loa-substantial"] | ["gematik-ehealth-loa-high"] | [OpenID Connect Dynamic Client Registration 1.0#ClientMetadata] |
| id_token_signed_response_alg | ES256 | - | Weitere Werte sind möglich. |
| id_token_encrypted_response_alg | ECDH-ES | - | Weitere Werte sind möglich. |
| id_token_encrypted_response_enc | A256GCM | - | Weitere Werte sind möglich. |
| scope | string | "openid urn:telematik:display_name urn:telematik:versicherter" | Wenn mehr als ein Wert enthalten ist, so sind diese durch ein Leerzeichen separiert gemäß |

| | | | |
|----------------------------|---|--|---|
| | | | [RFC6749#section-3.3] in einem String zusammenzufassen. |
| } | | | |
| <i>federation_entity</i> { | | | |
| name (deprecated) | string | "Fachdienst007" | Der Claim name ist nicht [OpenID Federation 1.0] konform und wird entfernt. |
| organization_name | String (max. 128 Zeichen) Wertebereich: ^[ÄÖÜäöüß\w\-\.\&\+*\V]{1,128} | "Fachdienst007" | Organisationsname des Teilnehmers der TI-Föderation, Name des IDP - wird genutzt in der Auswahlliste für den Benutzer |
| contacts | [strings] | ["Support@Fachdienst007.de", "info@Fachdienst007.de"] | Optional |
| homepage_uri | URL | "https://Fachdienst007.de" | Optional |
| }} | | | |

Alt:**signed_jwks_uri**

Ablageort für weitere Schlüssel des Fachdienstes etwa die zur TLS Client Schlüssel und Zertifikate (x5c, use = sig) oder für die Verschlüsselung der ID-Token (use = "enc").

Wenn eine signed_jwks_uri im Entity Statement angegeben ist müssen auch diese Schlüssel importiert werden.

Die Auflösung der signed_jwks_uri erfolgt dabei mittels HTTP GET Request.

Response auf GET an die Adresse "https://idp4711.de/jws.json"

HTTP 200 mit Content-Type: [application/jwk-set+json](#)

Neu:

signed_jwks_uri

Ablageort für weitere Schlüssel des Fachdienstes etwa die zur TLS Client Schlüssel und Zertifikate (x5c, use = sig) oder für die Verschlüsselung der ID Token (use = "enc").

Wenn eine signed_jwks_uri im Entity Statement angegeben ist, müssen auch diese Schlüssel importiert werden.

Die Auflösung der signed_jwks_uri erfolgt dabei mittels HTTP GET Request.

Response auf GET an die Adresse "https://idp4711.de/jws.json"

HTTP 200 mit Content-Type: application/jwk-set+jsonjwt

Alt:**Tabelle 34 : Body zum Entity Statement des Federation Master über den Fachdienst**

| Name | Werte | Beispiel | Anmerkungen |
|------|--|----------------------------------|---|
| iss | URL | "http://master0815.de" | URL des Federation Master |
| sub | URL | "https://Fachdienst007.de" | URL des angefragten Fachdienstes |
| iat | Alle time Werte in Sekunden seit 1970, RFC 7519 Sect.2 , | 1645398001 | 2022-02-21 00:00:01 |
| exp | Alle time Werte in Sekunden seit 1970, RFC 7519 Sect.2 , | 1645480801 | Beispielhafte Gültigkeit von 1 Tag für Möglichkeit der Sperrung |
| jwks | JWKS Objekt | unter anderem "Fachdienst007-42" | Schlüssel für die Signatur des EntityStatement |

Neu:**Tabelle 34 : Body zum Entity Statement des Federation Master über den Fachdienst**

| Name | Werte | Beispiel | Anmerkungen |
|------|-------|------------------------|---------------------------|
| iss | URL | "http://master0815.de" | URL des Federation Master |

| | | | |
|-------|--|--|---|
| sub | URL | "https://Fachdienst007.de" | URL des angefragten Fachdienstes |
| iat | Alle time Werte in Sekunden seit 1970, RFC7519#section-2[] | 1645398001 | 2022-02-21 00:00:01 |
| exp | Alle time Werte in Sekunden seit 1970, RFC7519#section-2[] | 1645480801 | Beispielhafte Gültigkeit von 1 Tag für Möglichkeit der Sperrung |
| jwks | JWKS-Objekt | unter anderem "Fachdienst007-42" | Schlüssel für die Signatur des EntityStatement |
| scope | string | "openid urn:telematik:display_name urn:telematik:versicherter" | Wenn mehr als ein Wert enthalten ist, so sind diese durch ein Leerzeichen separiert gemäß RFC6749#section-3.3 in einem String zusammenzufassen. |

Alt:

Tabelle 39 : HTTP-POST Parameter für AUTHORIZATION_CODE und den CODE_VERIFIER

| Name | Werte | Beispiel | Anmerkungen |
|---------------|---|--------------------------|---------------------------------------|
| grant_type | <i>authorization_code</i> | - | |
| code | <AUTHORIZATION_CODE des sektoralen IDP base64-kodiert> - max. 2000 Zeichen | AUTHORIZATION_CODE_IDP | AUTHORIZATION_CODE des sektoralen IDP |
| code_verifier | <CODE_VERIFIER des Fachdienstes> | code_verifier_Fachdienst | |

| | | | |
|--------------|-----|-------------------------------|--|
| client_id | URL | "https://Fachdienst007.de" | URL des Fachdienstes = seine client_id |
| redirect_uri | URL | "https://Fachdienst007.de/AS" | |

Neu:**Tabelle 39 : HTTP-POST Parameter für AUTHORIZATION_CODE und den CODE_VERIFIER**

| Name | Werte | Beispiel | Anmerkungen |
|---------------|---|-------------------------------|--|
| grant_type | authorization_code | - | |
| code | <AUTHORIZATION_CODE des sektoralen IDP base64-kodiert> - max. 2000 Zeichen | AUTHORIZATION_CODE_IDP | AUTHORIZATION_CODE des sektoralen IDP |
| code_verifier | <CODE_VERIFIER des Fachdienstes> | code_verifier_Fachdienst | |
| client_id | URL | "https://Fachdienst007.de" | URL des Fachdienstes = seine client_id |
| redirect_uri | URL | "https://Fachdienst007.de/AS" | |

Alt:**Tabelle 40 : Header-claims des ID_TOKEN des sektoralen IDP**

| Name | Werte | Beispiel | Anmerkungen |
|------|-------------------------|--------------------|--|
| alg | <i>ECDH-ES</i> | - | |
| enc | <i>A256GCM</i> | - | |
| kid | wie aus signed_jwks_uri | "Fachdienst007-69" | Ein Schlüssel mit der use="enc" aus dem signed_jwks_uri des Fachdienstes |

| | | | |
|-----|-----|---|--|
| cty | JWT | - | |
|-----|-----|---|--|

Neu:**Tabelle 40 : Header-claims des ID_TOKEN des sektoralen IDP**

| Nam e | Werte | Beispiel | Anmerkungen |
|----------|---|--|--|
| alg | ECDH-ES | - | |
| enc | A256GCM | - | |
| kid | wie aus signed_jwks _uri | "Fachdienst007-69" | Ein Schlüssel mit der use="enc" aus dem signed_jwks_uri des Fachdienstes |
| cty | JWT | - | |
| epk | JWK- Repräsentati on des Ephemeral Public Key für den Key- Transfer | "epk": { "kty": "EC", "crv": "P-256", "x": "gI0GAILBdu7T53akrFmMyGcsF3n5dO7MmwNBHKW5SV0", "y": "SLW_xSffzIPWrHEVI30DHM_4egVwt3NQqeUD7nMFpps" } | |

Alt:**Tabelle 41: Signature HeaderClaims des ID_TOKEN des sektoralen IDP**

| N a m e | Wer te | Beispiel | Anmer kunge n |
|------------------|-----------|----------|--------------------------------|
| alg | ES256 | | P256 wird zugela ssen |

| | | | |
|------|---|---|--|
| typ | JWT | JWT | Belegung gemäß [RFC7517] |
| kind | wie aus jwks in Entity Statement des sektoralen IDP | | Für die Signatur des Token verwendeter Schlüssel |
| x5c | base64-encoded DER Zertifikat | MIIDQjCCAiqqAwIBAgIGATz/FuLiMA0GCSqGSIb3DQEBBQUAMGIXCzAJBgNVBAYTAIVTMQswCQYDVQQIEwJDTzEPMA0GA1UEBxMGRGVudmVYMRwwGgYDVQQKEwNQaW5nI | <p>Zertifikat aus der Komponenten-PKI mit P256 ECC Schlüssel, welcher für die Signatur des ID_Token verwendet wurde.</p> <p>Dienste können das Token auch anhand des</p> |

| | | | |
|--|--|--|--|
| | | | mittels der kid auffindbaren Schlüssel im Entity Statement prüfen. |
|--|--|--|--|

Neu:**Tabelle 41: Signature Header *Claims* des ID_TOKEN des sektoralen IDP**

| N a m e | Wer te | Beispiel | Anmer kunge n |
|------------------|---|---|--|
| alg | ES256 | | P256 wird zugelassen |
| typ | JWT | JWT | Belegung gemäß [RFC7517] |
| kid | wie aus jwks in Entity Statement des sektoralen IDP | | Für die Signatur des Token verwendeter Schlüssel |
| x | [bas | "x5c": ["MIIDQjCCAiqqAwIBAgIGATz/FuLiMA0GCSqGSIb3DQEBBQUAMGIXCzA | Zertifikat |

| | | | |
|----|---|--|--|
| 5c | e64 - enc ode d DER Zert ifika t] | JBgNVBAYTAIVTMQswCQYDVQQIEwJDTzEPMA0GA1UEBxMGRGVudmVyMRwwGgYDVQQKEExNQaW5nI"] | aus der Komp onent en-PKI mit P256 ECC Schlüs sel, welch er für die Signat ur des ID_To ken verwe ndet wurde . Dienst e könn en das Token auch anhan d des mittel s der kid auffin dbare n Schlüs sel im Entity State ment prüfen . |
|----|---|--|--|

Neu:

Nach Tabelle 42 wird A_22989 entfernt, da diese bereits im Kapitel 4.2.4.2 enthalten ist und durch folgenden Satz ersetzt:

Zu den Scopes und Claims bzgl. der Identitäten für Versicherte siehe A_22989-01 im Kapitel "Token-Endpunkt Ausgangsdaten".

3 Änderungen in gemSpec_IDP_FedMaster

Änderungen in Kapitel 2.1 "Allgemeiner Überblick"

Alt:

Um eine Gesamtlösung sicherzustellen, bei der Anwendungen in möglichst einfacher Weise die verschiedenen sektoralen Identity Provider nutzen können, sind in bestimmten Bereichen einheitliche Vorgaben für die technische und organisatorische Umsetzung zu erstellen:

- Einheitliche Identitätsattribute für die Nutzergruppen (Minimal `claim Sets`, `scopes`)
- Grundstruktur der Vertrauensbeziehungen der Föderierung (IDP Federation/Trust Chains)
- Einheitliche Verfahren zum Auffinden von sektoralen Identity Providern (IDP Discovery)
- Einheitliche Vertrauensniveaus (Trust Framework).

Neu:

Um eine Gesamtlösung sicherzustellen, bei der Anwendungen in möglichst einfacher Weise die verschiedenen sektoralen Identity Provider nutzen können, sind in bestimmten Bereichen einheitliche Vorgaben für die technische und organisatorische Umsetzung zu erstellen:

- Einheitliche Identitätsattribute für die Nutzergruppen (Minimal `claim Sets`, `scopes`),
- Grundstruktur der Vertrauensbeziehungen der Föderierung (IDP Federation/Trust Chains),
- Einheitliche Verfahren zum Auffinden von sektoralen Identity Providern (IDP Discovery),
- Einheitliche Vertrauensniveaus (Trust Framework).

Änderungen in Kapitel 2.3 "Akteure und Rollen"

Alt:

Tabelle 2: Akteure und Rollen

| Komponente | Beschreibung |
|------------|--------------|
|------------|--------------|

| | |
|------------------------------|---|
| Federation Master | <ul style="list-style-type: none">• Der Federation Master bildet den Vertrauensanker der Föderation gemäß [OpenID Connect Federation 1.0].• Der Federation Master ist eine Entität im Sinne von OIDC und muss ein Entity Statement (Entitätsaussage) mit den Eigenschaften der Entität ausgeben.• Alle Teilnehmer der Föderation müssen beim Federation Master registriert sein. Der Federation Master verwaltet die öffentlichen Schlüssel aller teilnehmenden Parteien.• Der Federation Master kennt die aktuellen TLS-Zertifikate der registrierten sektoralen Identity Provider. |
| sektoraler Identity Provider | <ul style="list-style-type: none">• sektorale Identity Provider sind OpenID Provider (OP) entsprechend der Spezifikation [OpenID Connect Core 1.0].• Jeder sektorale Identity Provider ist im Sinne von OIDC eine Entität und muss ein Entity Statement (Entitätsaussage) mit seinen Eigenschaften ausgeben.• Alle OpenID Provider der Föderation müssen beim Federation Master registriert sein. Auf einem organisatorischen Weg muss jeder OpenID Provider seinen öffentlichen Schlüssel beim Federation Master hinterlegen.• Jeder OpenID Provider hat eine über die gesamte Föderation eindeutige Issuer-ID.• Zur Verifikation der Sicherheitskette (trust chain) stehen den OpenID Providern Schnittstellen entsprechend der Spezifikation [OpenID Connect Federation 1.0] zur Verfügung• Im Sektor "Versicherte" tritt jede Krankenkasse als eigener sektoraler Identity Provider auf.• Anbieter können die sektoralen Identity Provider mehrerer Krankenkassen als Mandanten getrennt betreiben.• Sektorale Identity Provider sind Teilnehmer der Föderation. |

| | |
|------------|---|
| Fachdienst | <ul style="list-style-type: none"> Fachdienste sind Relying Partys (RP) entsprechend der Spezifikation [OpenID Connect Core 1.0]. Jeder Fachdienst ist im Sinne von OIDC eine Entität und muss ein Entity Statement (Entitätsaussage) mit seinen Eigenschaften ausgeben. Alle Relying Partys der Föderation müssen beim Federation Master registriert sein. Auf einem organisatorischen Weg muss jede Relying Party ihren öffentlichen Schlüssel beim Federation Master hinterlegen. Jede Relying Party hat eine über die gesamte Föderation eindeutige Client-ID. Jede Relying Party muss genau die <code>scopes</code> und <code>claims</code> beim Federation Master hinterlegen, welche sie für ihre fachlichen Anwendungsfälle benötigt. Der Nutzer muss der Verwendung der in den <code>scopes</code> und <code>claims</code> enthaltenen Daten durch den Fachdienst zustimmen (Consent-Freigabe). Fachdienste sind Teilnehmer der Föderation. |
|------------|---|

Neu:

Tabelle 2: Akteure und Rollen

| Komponente | Beschreibung |
|-------------------|--|
| Federation Master | <ul style="list-style-type: none"> Der Federation Master bildet den Vertrauensanker der Föderation gemäß [OpenID Federation 1.0] Der Federation Master ist eine Entität im Sinne von OIDC und muss ein Entity Statement (Entitätsaussage) mit den Eigenschaften der Entität ausgeben. Alle Teilnehmer der Föderation müssen beim Federation Master registriert sein. Der Federation Master verwaltet die öffentlichen Schlüssel aller teilnehmenden Parteien. Der Federation Master kennt die aktuellen TLS-Zertifikate der registrierten sektoralen Identity Provider. |

| | |
|------------------------------|---|
| sektoraler Identity Provider | <ul style="list-style-type: none"> • Sektorale Identity Provider sind OpenID Provider (OP) entsprechend der Spezifikation [OpenID Connect Core 1.0] • Jeder sektorale Identity Provider ist im Sinne von OIDC eine Entität und muss ein Entity Statement (Entitätsaussage) mit seinen Eigenschaften ausgeben. • Alle OpenID Provider der Föderation müssen beim Federation Master registriert sein. Auf einem organisatorischen Weg muss jeder OpenID Provider seinen öffentlichen Schlüssel beim Federation Master hinterlegen. • Jeder OpenID Provider hat eine über die gesamte Föderation eindeutige Issuer-ID. • Zur Verifikation der Sicherheitskette (trust chain) stehen den OpenID Providern Schnittstellen entsprechend der Spezifikation [OpenID Federation 1.0] zur Verfügung • Im Sektor "Versicherte" tritt jede Krankenkasse als eigener sektoraler Identity Provider auf. • Anbieter können die sektoralen Identity Provider mehrerer Krankenkassen als Mandanten getrennt betreiben. • Sektorale Identity Provider sind Teilnehmer der Föderation. |
| Fachdienst | <ul style="list-style-type: none"> • Fachdienste sind Relying Partys (RP) entsprechend der Spezifikation [OpenID Connect Core 1.0]. • Jeder Fachdienst ist im Sinne von OIDC eine Entität und muss ein Entity Statement (Entitätsaussage) mit seinen Eigenschaften ausgeben. • Alle Relying Partys der Föderation müssen beim Federation Master registriert sein. Auf einem organisatorischen Weg muss jede Relying Party ihren öffentlichen Schlüssel beim Federation Master hinterlegen. • Jede Relying Party hat eine über die gesamte Föderation eindeutige Client-ID. • Jede Relying Party muss genau die <code>scopes</code> und <code>claims</code> beim Federation Master hinterlegen, welche sie für ihre fachlichen Anwendungsfälle benötigt. Der Nutzer muss der Verwendung der in den <code>scopes</code> und <code>claims</code> enthaltenen Daten durch den Fachdienst zustimmen (Consent-Freigabe). • Fachdienste sind Teilnehmer der Föderation. |

Änderungen in Kapitel 3.1 "Anwendungsfälle"

Alt:

Tabelle 4: Übersicht über die Anwendungsfälle im Gesamtkontext Federation Master

| Use Case | Komponente | Kurzbeschreibung |
|----------|------------|------------------|
|----------|------------|------------------|

| | | |
|--------------------------------|-------------------|--|
| Teilnehmer registrieren | Federation Master | <p>Jede Fachanwendung und jeder Identity Provider muss sich als Teilnehmer beim Federation Master registrieren. Im Zuge der Registrierung wird der öffentliche Teil des Schlüssels, mit dem der Teilnehmer sein Entity Statement signiert, beim Federation Master hinterlegt.</p> <p>Für jede Fachanwendung wird zusätzlich hinterlegt, welche Informationen zum Nutzer (<i>scopes</i> bzw. <i>claims</i>) diese beim Identity Provider erfragen dürfen.</p> <p>Für jeden Identity Provider werden die Schlüssel der TLS-Verbindungen in die VAU hinterlegt.</p> |
| an Fachanwendung anmelden | Fachanwendung | <p>Der Nutzer meldet sich an einer Fachanwendung an. Fachanwendungen können z.B. Anwendungen von Krankenkassen, TI-Anwendungen (wie bspw. E-Rezept, ePA) oder DiGAs sein. Die Anmeldung für alle Anwendungen erfolgt über genau den Identity Provider, bei dem die elektronische Identität des Nutzers hinterlegt ist. Ist der richtigen Identity Provider nicht bekannt, so kann die Liste aller in der Föderation registrierten Identity Provider zur Ermittlung des richtigen Identity Provider vom Federation Master abgefragt werden. Die Auswahl kann dann durch den Nutzer im Kontext der Anmeldung getroffen werden.</p> |
| IDP-Liste bereitstellen | Federation Master | <p>Zu allen in der Föderation registrierten Identity Providern werden die Informationen 'Organisationsname', 'Logo' und 'Zieladresse (URL)' ermittelt und als Liste bereitgestellt.</p> |
| Autorisierung prüfen | Fachanwendung | <p>Der Anwendungsfall <i>Autorisierung prüfen</i> ist ein Anwendungsfall der Fachanwendung ohne Nutzerinteraktion. In dem Anwendungsfall wird geprüft, welche fachlichen Aktionen der Nutzer in der Fachanwendung ausführen darf und welche Informationen für diese Entscheidung vom Nutzer benötigt und vom Identity Provider bezogen werden müssen.</p> |
| Entity Statement bereitstellen | Federation Master | <p>Der Federation Master stellt zu jedem registrierten Teilnehmer ein Entity Statement aus.</p> |
| Nutzer authentifizieren | Identity Provider | <p>Vor der eigentlichen Authentifizierung des Nutzers wird in diesem Anwendungsfall geprüft, ob die anfragende Fachanwendung Teil der TI-</p> |

| | | |
|--|-------------------|--|
| | | <p>Föderation ist und sie berechtigt ist, die geforderten Informationen zum Nutzer (scopes, claims) einzuholen. Dazu wird das Entity Statement des Fachdienstes vom Federation Master abgeholt.</p> <p>Die eigentliche Authentifikation des Nutzers erfolgt durch Interaktion mit dem Nutzer über das Authenticator-Modul des Identity Provider. Das Authenticator-Modul steht dem Nutzer z.B. als Funktion einer App zur Verfügung.</p> |
| Fachanwendung-Anwendungsfälle bearbeiten | Fachanwendung | Nach erfolgreicher Nutzerauthentifizierung kann der Nutzer die Anwendungsfälle der Fachanwendung bearbeiten, für die er autorisiert ist. |
| TLS-Zertifikate in VAU hinterlegen | Identity Provider | Im Zuge der Erzeugung von TLS-Zertifikaten zu Domänen des Identity Provider wird geprüft, ob TLS-Zertifikate betroffen sind, deren Schlüssel in der VAU hinterlegt sind. Ist das der Fall, wird der Prozess von einer Prüfinstanz (z.B. gematik) überwacht. In diesem Kontext muss auch eine Aktualisierung des Schlüsselmaterials beim Federation Master erfolgen. |
| Schlüssel der TLS-Zertifikate abgleichen | Federation Master | In regelmäßigen Abständen und bei Zertifikaterstellung prüft der Federation Master die TLS-Zertifikate der in der VAU mündenden TLS-Verbindungen in der Weise, ob die öffentlichen Schlüssel der Zertifikate im Federation Master hinterlegt sind. Zur Ermittlung aller in Frage kommender TLS-Zertifikate nutzt der Federation Master öffentlich zugängliche Certificate Transparency Provider. |
| Schlüssel verwalten | Federation Master | Der Federation Master verwaltet die Schlüssel und Adressen der Teilnehmer und beglaubigt sie gegenüber anderen Diensten. Das Einbringen der Daten neuer Teilnehmer bzw. das Löschen der Daten auszuschließender Teilnehmer erfolgt über organisatorische Prozesse (Teilnehmer registrieren, Teilnehmer löschen). |

Neu:

Tabelle 4: Übersicht über die Anwendungsfälle im Gesamtkontext Federation Master

| Use Case | Komponente | Kurzbeschreibung |
|------------|-------------------|---------------------------------------|
| Teilnehmer | Federation Master | Jede Fachanwendung und jeder Identity |

| | | |
|--------------------------------|-------------------|--|
| registrieren | | <p>Provider muss sich als Teilnehmer beim Federation Master registrieren. Im Zuge der Registrierung wird der öffentliche Teil des Schlüssels, mit dem der Teilnehmer sein Entity Statement signiert, beim Federation Master hinterlegt.</p> <p>Für jede Fachanwendung wird zusätzlich hinterlegt, welche Informationen zum Nutzer (scopes bzw. claims) diese beim Identity Provider erfragen dürfen.</p> <p>Für jeden Identity Provider werden die Schlüssel der TLS-Verbindungen in die VAU hinterlegt.</p> |
| an Fachanwendung anmelden | Fachanwendung | <p>Der Nutzer meldet sich an einer Fachanwendung an. Fachanwendungen können z.B. Anwendungen von Krankenkassen, TI-Anwendungen (wie bspw. E-Rezept, ePA) oder DiGAs sein. Die Anmeldung für alle Anwendungen erfolgt über genau den Identity Provider, bei dem die elektronische Identität des Nutzers hinterlegt ist. Ist der richtigen Identity Provider nicht bekannt, so kann die Liste aller in der Föderation registrierten Identity Provider zur Ermittlung des richtigen Identity Provider vom Federation Master abgefragt werden. Die Auswahl kann dann durch den Nutzer im Kontext der Anmeldung getroffen werden.</p> |
| IDP-Liste bereitstellen | Federation Master | <p>Zu allen in der Föderation registrierten Identity Providern werden die Informationen 'Organisationsname', 'Logo' und 'Zieladresse (URL)' ermittelt und als Liste bereitgestellt.</p> |
| Autorisierung prüfen | Fachanwendung | <p>Der Anwendungsfall <i>Autorisierung prüfen</i> ist ein Anwendungsfall der Fachanwendung ohne Nutzerinteraktion. In dem Anwendungsfall wird geprüft, welche fachlichen Aktionen der Nutzer in der Fachanwendung ausführen darf und welche Informationen für diese Entscheidung vom Nutzer benötigt und vom Identity Provider bezogen werden müssen.</p> |
| Entity Statement bereitstellen | Federation Master | <p>Der Federation Master stellt zu jedem registrierten Teilnehmer ein Entity Statement aus.</p> |
| Nutzer authentifizieren | Identity Provider | <p>Vor der eigentlichen Authentifizierung des Nutzers wird in diesem Anwendungsfall geprüft, ob die anfragende Fachanwendung Teil der TI-Föderation ist und sie berechtigt ist, die</p> |

| | | |
|--|-------------------|--|
| | | <p>geforderten Informationen zum Nutzer (scopes, claims) einzuholen. Dazu wird das Entity Statement des Fachdienstes vom Federation Master abgeholt.</p> <p>Die eigentliche Authentifikation des Nutzers erfolgt durch Interaktion mit dem Nutzer über das Authenticator-Modul des Identity Provider. Das Authenticator-Modul steht dem Nutzer z.B. als Funktion einer App zur Verfügung.</p> |
| Fachanwendung-Anwendungsfälle bearbeiten | Fachanwendung | Nach erfolgreicher Nutzerauthentifizierung kann der Nutzer die Anwendungsfälle der Fachanwendung bearbeiten, für die er autorisiert ist. |
| TLS-Zertifikate in VAU hinterlegen | Identity Provider | Im Zuge der Erzeugung von TLS-Zertifikaten zu Domänen des Identity Provider wird geprüft, ob TLS-Zertifikate betroffen sind, deren Schlüssel in der VAU hinterlegt sind. Ist das der Fall, wird der Prozess von einer Prüfinstanz (z.B. gematik) überwacht. In diesem Kontext muss auch eine Aktualisierung des Schlüsselmaterials beim Federation Master erfolgen. |
| Schlüssel der TLS-Zertifikate abgleichen | Federation Master | In regelmäßigen Abständen und bei Zertifikaterstellung prüft der Federation Master die TLS-Zertifikate der in der VAU mündenden TLS-Verbindungen in der Weise, ob die öffentlichen Schlüssel der Zertifikate im Federation Master hinterlegt sind. Zur Ermittlung aller in Frage kommender TLS-Zertifikate nutzt der Federation Master öffentlich zugängliche Certificate Transparency Provider. |
| Schlüssel verwalten | Federation Master | Der Federation Master verwaltet die Schlüssel und Adressen der Teilnehmer und beglaubigt sie gegenüber anderen Diensten. Das Einbringen der Daten neuer Teilnehmer bzw. das Löschen der Daten auszuschließender Teilnehmer erfolgt über organisatorische Prozesse (Teilnehmer registrieren, Teilnehmer löschen). |

Änderungen in Kapitel 3.3.1 "Akzeptanzkriterien - Entity Statement bereitstellen"

Alt:

ML-152179 - AF_10101 - Payload des JWS-Token enthält Informationen zum angefragten Teilnehmer der Föderation

Der Payload des JWS-Token enthält diese Informationen bezüglich des angefragten Teilnehmers der Föderation (siehe auch [gemSpec IDP Sek - Anhang B - Abläufe](#)):

- `iss` = URL - Identifier Federation Master
- `sub` = URL - Identifier des angefragten Teilnehmers
- `iat` = long Wert - Ausstellungszeitpunkt des Abrufs (Alle time-Werte in Sekunden seit 1970)
- `exp` = long Wert - Ablaufzeitpunkt der Gültigkeit des Abrufs (Alle time-Werte in Sekunden seit 1970)
- `jwks` = JWKS Objekt - öffentlicher Schlüssel des angefragten Teilnehmers.
- `aud` = URL - Identifier des anfragenden Teilnehmers. Wenn der `aud`-Parameter im Fetch Entity-Statement-Request des anfragenden Teilnehmers vorhanden ist, MUSS der `aud` Parameter in der Fetch Entity-Statement-Response vorhanden sein und genau diesen Wert annehmen.

Für registrierte Relying Parties (Fachdienste) MÜSSEN zusätzlich diese Informationen im Payload des JWS-Token enthalten sein:

- `scope` = scope, die bei der Registrierung der Relying Party beim Federation Master angegeben wurden
- `claims` = claims, die bei der Registrierung der Relying Party beim Federation Master angegeben wurden
- `redirect_uris` = `redirect_uris`, die bei der Registrierung der Relying Party beim Federation Master angegeben wurden

<=

Hinweis: Will eine Relying Party den Umfang der vom sektoralen IDP anforderbaren scopes oder claims erweitern oder `redirect_uris` ändern, so müssen diese Änderungen über den organisatorischen Registrierungsprozess laufen.

Neu:**ML-152179 - AF_10101 - Payload des JWS-Token enthält Informationen zum angefragten Teilnehmer der Föderation**

Der Payload des JWS-Token enthält diese Informationen bezüglich des angefragten Teilnehmers der Föderation (siehe auch [\[gemSpec IDP Sek - Anhang B - Abläufe\]](#)):

- `iss` = URL - Identifier Federation Master
- `sub` = URL - Identifier des angefragten Teilnehmers
- `iat` = long Wert - Ausstellungszeitpunkt des Abrufs (Alle time-Werte in Sekunden seit 1970)
- `exp` = long Wert - Ablaufzeitpunkt der Gültigkeit des Abrufs (Alle time-Werte in Sekunden seit 1970)
- `jwks` = JWKS-Objekt - öffentlicher Schlüssel des angefragten Teilnehmers.
- `aud` = URL - Identifier des anfragenden Teilnehmers. Wenn der `aud`-Parameter im Fetch Entity-Statement-Request des anfragenden Teilnehmers vorhanden ist,

MUSS der `aud` Parameter in der Fetch Entity-Statement-Response vorhanden sein und genau diesen Wert annehmen.

Für registrierte Relying Parties (Fachdienste) MÜSSEN zusätzlich diese Informationen im Payload des JWS-Token enthalten sein:

- `scopes` = `scopes`, die bei der Registrierung der Relying Party beim Federation Master angegeben wurden
- `claims` = `claims`, die bei der Registrierung der Relying Party beim Federation Master angegeben wurden
- `redirect_uris` = `redirect_uris`, die bei der Registrierung der Relying Party beim Federation Master angegeben wurden

<=

Hinweis: Will eine Relying Party den Umfang der vom sektoralen IDP anforderbaren Scopes oder Claims erweitern oder `redirect_uris` ändern, so müssen diese Änderungen über den organisatorischen Registrierungsprozess laufen.

Änderungen in Kapitel 4.1 "Aufbau und Inhalt des Federation Master Entity Statement"

Alt:

A_25414 - Prüfung der Entity Statements von Fachdiensten

Der Anbieter des Federation Master MUSS einen Prozess etablieren, in dem der Anbieter des Federation Master mindestens täglich die Entity Statements der Fachdienste abfragt und die Werte der in Tabelle "Prüfung der Entity Statements von Fachdiensten" aufgeführten Attribute hinsichtlich der bei der Registrierung hinterlegten Werte prüft. Stimmen die Werte nicht überein, so MUSS der Federation Master die in der Tabelle aufgeführten Maßnahmen treffen.

Tabelle 15 : Prüfung der Entity Statements von Fachdiensten

| Attribut | Abweichung | Auswirkung | Maßnahme |
|------------------------------|--|---|---|
| <code>jwks</code> | Schlüssel, mit der Fachdienst sein Entity Statement signiert, hat sich geändert. | Der im Federation Master hinterlegte Schlüssel ist nicht mehr korrekt, der Vertrauensraum ist ggf. gefährdet. | Einstellen eines Incident und Sperren des Teilnehmers in der Föderation |
| <code>authority_hints</code> | Die Vertrauenskette hat sich geändert. | Als Vertrauensanker ist nicht mehr der | Einstellen eines Incident |

| | | | |
|---------------|---|--|--|
| | | Federation Master eingetragen. Vertrauensraum ist ggf. gefährdet. | t und Sperren des Teilnehmers in der Föderation |
| scopes | Der Umfang der vom Fachdienst anfragbaren scopes hat sich geändert. | Hat sich der Umfang, der anfragbaren scopes erweitert, so besteht die Gefahr des unberechtigten Zugriffs auf Identitätsdaten. Eine Verringerung des Umfangs der anfragbaren scopes hat keine negativen Auswirkungen. | Einstellen eines Incidents und Sperren des Teilnehmers in der Föderation |
| claims | Der Umfang der vom Fachdienst anfragbaren claims hat sich geändert. | Hat sich der Umfang, der anfragbaren claims erweitert, so besteht die Gefahr des unberechtigten Zugriffs auf Identitätsdaten. Eine Verringerung des Umfangs der anfragbaren claims hat keine negativen Auswirkungen. | Einstellen eines Incidents und Sperren des Teilnehmers in der Föderation |
| redirect_uris | Der Inhalt der Liste der URLs, an den die vom IDP ausgestellten Identitätsinformationen | Die vom IDP ausgestellten Identitätsinformationen | Einstellen eines Incidents |

| | | | |
|---|---|--|---|
| | geschickt werden, hat sich geändert. | können ggf. an unberechtigte Endpunkte verschickt werden, so besteht die Gefahr des unberechtigten Zugriffs auf Identitätsdaten. | t und Sperren des Teilnehmers in der Föderation |
| metadata.openid_relying_party.organization_name | Der Name der Organisation hat sich geändert. | Die Änderung kann zu Anzeigeproblemen bei den Nutzern führen. | Einstellen eines Incidents |
| metadata.openid_relying_party.client_name | Der Name des Fachdienstes (redundant zu metadata:federation_entity:name) hat sich geändert. | Die Änderung kann zu Anzeigeproblemen bei den Nutzern führen. | Einstellen eines Incidents |
| metadata.federation_entity.name | Der Name des Fachdienstes (redundant zu metadata:openid_relying_party:client_name) hat sich geändert. | Die Änderung kann zu Anzeigeproblemen bei den Nutzern führen. | Einstellen eines Incidents |

<=, IDP_FedMaster, Sich.techn. Eignung: Herstellererklärung

Hinweis 1: Das Sperren eines Fachdienstes bedeutet technisch den Ausschluss aus der Föderation. Fragt ein sektoraler IDP die Teilnehmers Auskunft zu einem gesperrten Fachdienst beim Federation Master ab, so antwortet dieser gemäß [https://openid.net/specs/openid-federation-1.0.html#error_response] mit Error Code HTTP-401 invalid_client.

Neu:

A_25414-01 - Prüfung der Entity Statements von Fachdiensten

Der Anbieter des Federation Master MUSS einen Prozess etablieren, in dem der Anbieter des Federation Master mindestens täglich die Entity Statements der Fachdienste abfragt und die Werte der in Tabelle "Prüfung der Entity Statements von Fachdiensten" aufgeführten Attribute hinsichtlich der bei der Registrierung hinterlegten Werte prüft. Stimmen die Werte nicht überein, so MUSS der Federation Master die in der Tabelle aufgeführten Maßnahmen treffen.

Tabelle 15 : Prüfung der Entity Statements von Fachdiensten

| Attribut | Abweichung | Auswirkung | Maßnahme |
|-----------------|--|--|---|
| jwks | Schlüssel, mit der Fachdienst sein Entity Statement signiert, hat sich geändert. | Der im Federation Master hinterlegte Schlüssel ist nicht mehr korrekt, der Vertrauensraum ist ggf. gefährdet. | Einstellen eines Incident und Sperren des Teilnehmers in der Föderation |
| authority_hints | Die Vertrauenskette hat sich geändert. | Als Vertrauensanker ist nicht mehr der Federation Master eingetragen. Vertrauensraum ist ggf. gefährdet. | Einstellen eines Incident und Sperren des Teilnehmers in der Föderation |
| scopes | Der Umfang der vom Fachdienst anfragbaren scopes hat sich erweitert . | Hat sich der Umfang, der anfragbaren scopes erweitert, so besteht die Gefahr des unberechtigten Zugriffs auf Identitätsdaten. Eine Verringerung des Umfangs der anfragbaren scopes hat keine negativen Auswirkungen. | Einstellen eines Incident und Sperren des Teilnehmers in der Föderation |
| claims | Der Umfang der vom Fachdienst anfragbaren Claims | Hat sich der Umfang, der anfragbar | Einstellen eines |

| | | | |
|--|--|--|--|
| | hat sich erweitert . | en claims erweitert, so besteht die Gefahr des unberechtigten Zugriffs auf Identitätsdaten. Eine Verringerung des Umfangs der anfragbaren claims hat keine negativen Auswirkungen. | Incident und Sperren des Teilnehmers in der Föderation |
| redirect_uris | Der Inhalt der Liste der URLs, an den die vom IDP ausgestellten Identitätsinformationen geschickt werden, hat sich geändert. | Die vom IDP ausgestellten Identitätsinformationen können ggf. an unberechtigte Endpunkte verschickt werden, so besteht die Gefahr des unberechtigten Zugriffs auf Identitätsdaten. | Einstellen eines Incident und Sperren des Teilnehmers in der Föderation |
| metadata.openid_relying_party.organization_name | Der Name der Organisation hat sich geändert. | Die Änderung kann zu Anzeigeproblemen bei den Nutzern führen. | Einstellen eines Incident |
| metadata.openid_relying_party.client_name | Der Name des Fachdienstes (redundant zu metadata:federation_entity_name) hat sich geändert. | Nach [OpenID Federation 1.0#section-5.1.2] wird der in [OpenID Connect Registration 1.0] definierte client_name | Einstellen eines Incident |

| | | | |
|--|---|---|----------------------------|
| | | zur Darstellung der RP im Consent-Dialog verwendet. Die Änderung kann zu Anzeigeproblemen bei den Nutzern führen. | |
| metadata.federation_entity.name | Der Name des Fachdienstes (redundant zu metadata:openid_relying_party:client_name) hat sich geändert. | Die Änderung kann zu Anzeigeproblemen bei den Nutzern führen. | Einstellen eines Incidents |
| metadata.federation_entity.organization_name | Der Organisationsname des Teilnehmers der TI-Föderation hat sich geändert. | Die Änderung kann zu Anzeigeproblemen bei den Nutzern führen. | Einstellen eines Incidents |

<=, Anb_IDP_FedMaster, Sich.techn. Eignung: HerstellerAnbietererklärung

Hinweis 1: Das Sperren eines Fachdienstes bedeutet technisch den Ausschluss aus der Föderation. Fragt ein sektoraler IDP die Teilnehmerauskunft zu einem gesperrten Fachdienst beim Federation Master ab, so antwortet dieser gemäß https://openid.net/specs/openid-federation-1.0.html#error_response [OpenID Federation 1.0#error_response] mit Error Code HTTP-401 invalid_client 404 not_found.

Änderungen in Kapitel 4.2 "Organisatorische Prozesse am Federation Master"

Alt:

A_22675-01 - Teilnehmerregistrierung am Federation Master

Der Anbieter des Federation Master MUSS einen organisatorischen Prozess für die Registrierung von Teilnehmern an der Föderation etablieren. Alle Teilnehmer der Föderation MÜSSEN über diesen Prozess ihre öffentlichen Schlüssel beim Federation Master hinterlegen. Fachdienste MÜSSEN zusätzlich die für ihre Anwendungsfälle notwendigen scopes bzw. claims hinterlegen. Der Anbieter des Federation Master MUSS vorsehen, dass die gematik in den organisatorischen Ablauf eingebunden ist und die Möglichkeit der Prüfung der vom Fachdienst eingereichten scopes und claims erhält.
[<=]

Neu:

A_22675-02 - Teilnehmerregistrierung am Federation Master

Der Anbieter des Federation Master MUSS einen organisatorischen Prozess für die Registrierung von Teilnehmern an der Föderation etablieren. Alle Teilnehmer der Föderation MÜSSEN über diesen Prozess ihre öffentlichen Schlüssel beim Federation Master hinterlegen. Fachdienste MÜSSEN zusätzlich die für ihre Anwendungsfälle notwendigen `scopes` bzw. `claims` hinterlegen. Der Anbieter des Federation Master MUSS vorsehen, dass die gematik in den organisatorischen Ablauf eingebunden ist und die Möglichkeit der Prüfung der vom Fachdienst eingereichten `scopes` und `claims` erhält.

[<=]

Alt:

Fachdienste sollten nur genau die `scopes` beanspruchen, die für die Ausführung ihrer Anwendungsfälle unbedingt notwendig sind. Eine differenziertere Unterscheidung in verpflichtenden Attribute (`essential claims`, ohne die eine Dienstleistung gar nicht möglich ist) und freiwillige Attribute (`voluntary claims`, ohne die eine Dienstleistung in eingeschränktem Umfang möglich ist) wird durch die Verwendung von `claims` ermöglicht.

Neu:

Fachdienste sollten nur genau die `scopes` Werte beanspruchen, die für die Ausführung ihrer Anwendungsfälle unbedingt notwendig sind. Eine differenziertere Unterscheidung in verpflichtenden Attribute (`essential claims`, ohne die eine Dienstleistung gar nicht möglich ist) und freiwillige Attribute (`voluntary claims`, ohne die eine Dienstleistung in eingeschränktem Umfang möglich ist) wird durch die Verwendung von `claims` ermöglicht.

Änderungen in Kapitel 5.2 "Glossar"

Alt:

Tabelle 1: Glossar

| Begriff | Erläuterung |
|--------------------|--|
| Anwendungsfrontend | Die Applikation durch welche ein Nutzer die Dienste einer Anwendung der Telematikinfrastruktur wie etwa das E-Rezept nutzt. |
| Authentifizierung | Prüfung eines Identitätsnachweis des Nutzers am Gerät mit bestimmten Authentifizierungsmittel. |
| Claim | Ein Key/Value-Paar im Payload eines JSON Web Token. |
| Client | OAuth2-Rolle (siehe [RFC6749 # section-1.1]): Eine Anwendung (Relying Party), die auf geschützte Ressourcen des Resource Owners zugreifen möchte, die vom Resource Server bereitgestellt werden. Der Client kann auf einem Server (Webanwendung), Desktop-PC, mobilen Gerät etc. ausgeführt werden. Im Fokus der aktuellen Spezifikationen liegt jedoch allein die Kommunikation mit dem E-Rezept-FdV. |

| | |
|---------------------------------------|---|
| Consent | Zustimmung des Nutzers zur Verarbeitung der angezeigten Daten. Der Consent umfasst die Attribute, welche vom sektoralen Identity Provider bezogen, auf die im <code>claim</code> des jeweiligen Fachdienstes eingeforderten Attribute zusammenfasst. Es besteht Einigkeit zwischen dem, was gefordert wird, und welche Attribute im Token bestätigt werden. |
| DiGA | Digitale Gesundheitsanwendung(en) |
| Entity Statement | Ein Entity Statement [OpenID Connect Federation 1.0#entity-statement] (Entitätsaussage) wird von einer Entität ausgegeben, die sich auf eine Subjekt-Entität und Blatt-Entitäten bezieht. Ein Entitätsstatement ist immer ein signiertes JWT. |
| Fachanwendungen / Relying Party | Fachanwendungen sind Relying Party (RP) im Kontext der OIDC-Spezifikation. Nach erfolgreicher Authentifizierung des Nutzers und dessen Zustimmung zur Datennutzung (Consent Freigabe) bekommt die Fachanwendung Zugang zu einem definierten Teil der Identifikationsattribute des Nutzers. Die Fachanwendung nutzt diese Informationen zur Autorisierung des Nutzers zu der Durchführung definierter Anwendungsfälle der Fachanwendung. |
| Federation Master | Der Federation Master basiert auf den Standards OpenID Connect (OIDC), Open Authorization 2.0 (OAuth 2) und JSON Web Token (JWT). Der Federation Master ist einerseits der Trust Anchor des Vertrauensbereichs der Föderation. Andererseits stellt der Federation Master Schnittstellen bereit, welche Auskunft, über die in der Föderation registrierten, sektoralen Identity Provider gibt. |
| Gerät | Alle Arten von mobilen oder stationären Endgeräten. |
| Identitätsattribute | Daten, welche eine natürliche Person eindeutig identifizieren (Name, Vorname, Geburtsdatum, Anschrift, KVN-R) |
| identitätsbestätigenden Institutionen | Institutionen, welche die Identität einer natürlichen Person geprüft haben und bestätigen können. Solche Institutionen sind beispielsweise die Krankenkassen, welche die Identität der bei ihnen versicherten Personen bestätigen können. |
| JSON Web Token | Ein auf JSON basiertes und nach [RFC7519] (JWT) genormtes <code>ACCESS_TOKEN</code> . Das JWT ermöglicht den Austausch von verifizierbaren <code>claims</code> innerhalb seines Payloads. |
| Nutzergruppen | Nutzergruppen sind Personengruppen mit bestimmten Rollen im Kontext der TI-Anwendungslandschaft. Nutzergruppen sind beispielsweise Versicherte und Leistungserbringer (ggf. weiter differenziert - Ärzte, Zahnärzte, etc.) |

| | |
|--|---|
| Open Authorization 2.0 | Ein Protokoll zur Autorisierung für Web-, Desktop und Mobile Anwendungen. Dabei wird es einem Endbenutzer (Resource Owner) ermöglicht, einer Anwendung (Client) den Zugriff auf Daten oder Dienste (Resources) zu ermöglichen, die von einem Dritten (Resource Server) bereitgestellt werden. |
| OpenID Connect | OpenID Connect (OIDC) ist eine Authentifizierungsschicht, die auf dem Autorisierungsframework OAuth 2.0 basiert. Es ermöglicht Clients, die Identität des Nutzers anhand der Authentifizierung durch einen Authorization-Server zu überprüfen (siehe [OpenID Connect Core 1.0]). |
| Pushed Authorization Request (PAR) | Der Pushed Authorization Request (PAR) ermöglicht es Clients, eine OAuth 2.0-Autorisierungsanforderung direkt an den Authorization-Server des sektoralen Identity Provider zu senden. Die übergeben redirect-URI ist Autorisierungsendpunkt und wird im weiteren Flow verwendet. https://datatracker.ietf.org/doc/html/rfc9126 |
| Resource Owner | OAuth2-Rolle (siehe [RFC6749 # section-1.1]): Eine Entität (Nutzer), die einem Dritten den Zugriff auf ihre geschützten Ressourcen gewähren kann. Diese Ressourcen werden durch den Resource Server bereitgestellt. Ist der Resource Owner eine Person, wird dieser als Nutzer bezeichnet. |
| Resource Server | OAuth2 Rolle (siehe [RFC6749 # section-1.1]): Der Server (Dienst), auf dem die geschützten Ressourcen (Protected Resources) liegen. Er ist in der Lage, auf Basis von Access Tokens darauf Zugriff zu gewähren. Ein solcher Token repräsentiert die delegierte Autorisierung des Resource Owners. |
| Scope | <code>scopes</code> definieren ein festgelegtes Set an <code>claims</code> . Mit <code>scopes</code> lässt sich steuern, dass Anwendungen oder Anwendungsgruppen nur genau die Informationen einer Identität bekommen, die für die Anwendungsfälle der Anwendung(en) notwendig sind. Im Kontext OIDC gibt es vordefinierte <code>scopes</code> wie <i>openid</i> , <i>profile</i> und <i>E-Mail</i> , die verwendet werden können (siehe auch OpenID Connect Basic Client Implementer's Guide 1.0#Scopes). In der Föderation wird es darüber hinaus weitere <code>scopes</code> geben. |
| sektoraler Identity Provider / OpenID Provider | Als sektoraler Identity Provider bzw. OpenID Provider (OP) wird ein Dienst bezeichnet, welcher nach vorheriger Authentifizierung Identitätsinformationen für eine bestimmte Gruppe von Nutzern innerhalb der Telematikinfrastruktur des Gesundheitswesens bereitstellt. Diese Informationen werden anschließend von Fachdiensten verwendet, um auf Fachdaten und -prozesse zuzugreifen. |

Neu:

Tabelle 2: Glossar

| Begriff | Erläuterung |
|---------------------------------|---|
| Anwendungsfrontend | Die Applikation durch welche ein Nutzer die Dienste einer Anwendung der Telematikinfrastruktur wie etwa das E-Rezept nutzt. |
| Authentifizierung | Prüfung eines Identitätsnachweis des Nutzers am Gerät mit bestimmten Authentifizierungsmittel. |
| Claim | Ein Key/Value-Paar im Payload eines JSON Web Token. |
| Client | OAuth2-Rolle (siehe [RFC6749 # section-1.1]): Eine Anwendung (Relying Party), die auf geschützte Ressourcen des Resource Owners zugreifen möchte, die vom Resource Server bereitgestellt werden. Der Client kann auf einem Server (Webanwendung), Desktop-PC, mobilen Gerät etc. ausgeführt werden. Im Fokus der aktuellen Spezifikationen liegt jedoch allein die Kommunikation mit dem E-Rezept-FdV. |
| Consent | Zustimmung des Nutzers zur Verarbeitung der angezeigten Daten. Der Consent umfasst die Attribute, welche vom sektoralen Identity Provider bezogen, auf die im <code>claim</code> des jeweiligen Fachdienstes eingeforderten Attribute zusammenfasst. Es besteht Einigkeit zwischen dem, was gefordert wird, und welche Attribute im Token bestätigt werden. |
| DiGA | Digitale Gesundheitsanwendung(en) |
| Entity Statement | Ein Entity Statement[OpenID Federation 1.0#entity statement] (Entitätsaussage) wird von einer Entität ausgegeben, die sich auf eine Subjekt-Entität und Blatt-Entitäten bezieht. Ein Entitätsstatement ist immer ein signiertes JWT. |
| Fachanwendungen / Relying Party | Fachanwendungen sind Relying Party (RP) im Kontext der OIDC-Spezifikation. Nach erfolgreicher Authentifizierung des Nutzers und dessen Zustimmung zur Datennutzung (Consent Freigabe) bekommt die Fachanwendung Zugang zu einem definierten Teil der Identifikationsattribute des Nutzers. Die Fachanwendung nutzt diese Informationen zur Autorisierung des Nutzers zu der Durchführung definierter Anwendungsfälle der Fachanwendung. |
| Federation Master | Der Federation Master basiert auf den Standards OpenID Connect (OIDC), Open Authorization 2.0 (OAuth 2) und JSON Web Token (JWT). Der Federation Master ist einerseits der Trust Anchor des Vertrauensbereichs der Föderation. Andererseits stellt der Federation Master Schnittstellen bereit, welche Auskunft, über die in der Föderation registrierten, |

| | |
|---------------------------------------|--|
| | sektoralen Identity Provider gibt. |
| Gerät | Alle Arten von mobilen oder stationären Endgeräten. |
| Identitätsattribute | Daten, welche eine natürliche Person eindeutig identifizieren (Name, Vorname, Geburtsdatum, Anschrift, KVNR) |
| identitätsbestätigenden Institutionen | Institutionen, welche die Identität einer natürlichen Person geprüft haben und bestätigen können. Solche Institutionen sind beispielsweise die Krankenkassen, welche die Identität der bei ihnen versicherten Personen bestätigen können. |
| JSON Web Token | Ein auf JSON basiertes und nach [RFC7519] (JWT) genormtes ACCESS_TOKEN. Das JWT ermöglicht den Austausch von verifizierbaren claims innerhalb seines Payloads. |
| Nutzergruppen | Nutzergruppen sind Personengruppen mit bestimmten Rollen im Kontext der TI-Anwendungslandschaft. Nutzergruppen sind beispielsweise Versicherte und Leistungserbringer (ggf. weiter differenziert - Ärzte, Zahnärzte, etc.) |
| Open Authorization 2.0 | Ein Protokoll zur Autorisierung für Web-, Desktop und Mobile Anwendungen. Dabei wird es einem Endbenutzer (Resource Owner) ermöglicht, einer Anwendung (Client) den Zugriff auf Daten oder Dienste (Resources) zu ermöglichen, die von einem Dritten (Resource Server) bereitgestellt werden. |
| OpenID Connect | OpenID Connect (OIDC) ist eine Authentifizierungsschicht, die auf dem Autorisierungsframework OAuth 2.0 basiert. Es ermöglicht Clients, die Identität des Nutzers anhand der Authentifizierung durch einen Authorization-Server zu überprüfen (siehe [OpenID Connect Core 1.0]). |
| Pushed Authorization Request (PAR) | Der Pushed Authorization Request (PAR) ermöglicht es Clients, eine OAuth 2.0-Autorisierungsanforderung direkt an den Authorization-Server des sektoralen Identity Provider zu senden. Die übergeben redirect-URI ist Autorisierungsendpunkt und wird im weiteren Flow verwendet. [https://datatracker.ietf.org/doc/html/rfc9126] |
| Resource Owner | OAuth2-Rolle (siehe [RFC6749 # section-1.1]): Eine Entität (Nutzer), die einem Dritten den Zugriff auf ihre geschützten Ressourcen gewähren kann. Diese Ressourcen werden durch den Resource Server bereitgestellt. Ist der Resource Owner eine Person, wird dieser als Nutzer bezeichnet. |

| | |
|--|--|
| Resource Server | OAuth2 Rolle (siehe [RFC6749 # section-1.1]): Der Server (Dienst), auf dem die geschützten Ressourcen (Protected Resources) liegen. Er ist in der Lage, auf Basis von Access Tokens darauf Zugriff zu gewähren. Ein solcher Token repräsentiert die delegierte Autorisierung des Resource Owners. |
| Scope | Ein scopes definiert ein festgelegtes Set an claims. Mit scopes lässt sich steuern, dass Anwendungen oder Anwendungsgruppen nur genau die Informationen einer Identität bekommen, die für die Anwendungsfälle der Anwendung(en) notwendig sind. Im Kontext OIDC gibt es vordefinierte scopes Werte wie openid, profile und E-Mail, die verwendet werden können (siehe auch [OpenID Connect Basic Client Implementer's Guide 1.0#Scopes]). In der Föderation wird es darüber hinaus weitere scopes geben. |
| sektoraler Identity Provider / OpenID Provider | Als sektoraler Identity Provider bzw. OpenID Provider (OP) wird ein Dienst bezeichnet, welcher nach vorheriger Authentifizierung Identitätsinformationen für eine bestimmte Gruppe von Nutzern innerhalb der Telematikinfrastruktur des Gesundheitswesens bereitstellt. Diese Informationen werden anschließend von Fachdiensten verwendet, um auf Fachdaten und -prozesse zuzugreifen. |

Änderungen in Kapitel 5.5.2 weitere Dokumente

Neu:

Tabelle 22: Weitere Dokumente

| [Quelle] | Herausgeber (Erscheinungsdatum): Titel |
|---|--|
| JWT [RFC7519] | JSON Web Token (JWT) (Mai 2015) https://datatracker.ietf.org/doc/html/rfc7519 |
| OAuth 2.0 Spezifikation ([RFC6749]) | The OAuth 2.0 Authorization Framework (Oktober 2012) https://datatracker.ietf.org/doc/html/rfc6749 |
| [openid-connect-core] | OpenID Connect Core 1.0 (incorporating errata set 1, November 2014) https://openid.net/specs/openid-connect-core-1_0.html |
| [OpenID Connect Basic Client Implementer's Guide 1.0] | OpenID Connect Basic Client Implementer's Guide 1.0 (draft 40, Juli 2020) https://openid.net/specs/openid-connect-basic-1_0.html |

| | |
|--|--|
| [OpenID Connect Federation 1.0] [OpenID Federation 1.0] | OpenID Connect Federation 1.0 (Draft 2140, 24. Oktober 20242022) https://openid.net/specs/openid-connect-federation-1-0-21.html https://openid.net/specs/openid-federation-1_0.html |
| [OpenID Connect Registration 1.0] | OpenID Connect Dynamic Client Registration 1.0 incorporating errata set 2 (15. Dezember 2023) https://openid.net/specs/openid-connect-registration-1_0.html |
| [Pushed Authorization Request] | OAuth 2.0 Pushed Authorization Requests (September 2021) https://datatracker.ietf.org/doc/html/rfc9126 |
| PKCE ([RFC7636]) | Proof Key for Code Exchange by OAuth Public Clients (September 2015) https://datatracker.ietf.org/doc/html/rfc7636 |
| CAB-Forum | https://cabforum.org/ |
| OWASP | Open Web Application Security Project https://owasp.org/ |
| Certificate Transparency (CT) | Certificate Transparency Version 2.0 (Dezember 2021) https://datatracker.ietf.org/doc/html/rfc9162 |

4 Änderungen in gemSpec_IDP_FD

Änderungen in Kapitel 2 "Systemüberblick"

Alt:

Fachdienste, welche sektorale IDPs der TI-Föderation zur Nutzer-Authentisierung nutzen möchten, müssen die folgenden Prozesse und Schnittstellen bedienen:

- Registrierung des Fachdienstes beim Federation Master (organisatorischer Prozess gemäß [gemSpec_IDP_FedMaster]), sowie der verwendeten öffentlichen Schlüssel für die Signatur von Entity Statements und Mitteilung der benötigten `scopes` bzw. `claims` (Key/Value-Paare im Payload eines JWT)
- Veröffentlichung ihres signierten Entity Statements (siehe 4.5).

Neu:

Fachdienste, welche sektorale IDPs der TI-Föderation zur Nutzer-Authentisierung nutzen möchten, müssen die folgenden Prozesse und Schnittstellen bedienen:

- Registrierung des Fachdienstes beim Federation Master (organisatorischer Prozess gemäß [gemSpec_IDP_FedMaster]), sowie der verwendeten öffentlichen Schlüssel für die Signatur von Entity Statements und Mitteilung der benötigten `scopes` bzw. `claims` (Key/Value-Paare im Payload eines JWT)
- Veröffentlichung ihres signierten Entity Statements (siehe 4.5).

Änderungen in Kapitel 4.1 "Registrierung des Fachdienstes beim Federation Master"

Alt:

Fachdienstbetreiber müssen ihren Authorization Server beim Federation Master registrieren. Die Registrierung erfolgt als organisatorischer Prozess, bevor ein Fachdienst an den vom föderierten Identitätsmanagement (IDM) angebotenen Authentifizierungsprozessen teilnehmen kann. Erst nach erfolgter Registrierung, bei der die Adresse des Fachdienstes bzw. seines Authorization Servers, seine öffentlichen Schlüssel sowie die verwendeten `scopes` und `claims` angegeben wurden, können sektorale Identity Provider `ID_TOKEN` für den Fachdienst ausstellen.

Neu:

Fachdienstbetreiber müssen ihren Authorization Server beim Federation Master registrieren. Die Registrierung erfolgt als organisatorischer Prozess, bevor ein Fachdienst an den vom föderierten Identitätsmanagement (IDM) angebotenen Authentifizierungsprozessen teilnehmen kann. Erst nach erfolgter Registrierung, bei der die Adresse des Fachdienstes bzw. seines Authorization Servers, seine öffentlichen Schlüssel sowie die verwendeten `scopes` und `claims` angegeben wurden, können sektorale Identity Provider `ID_TOKEN` für den Fachdienst ausstellen.

Alt:

A_23045-01 - Registrierung des Fachdienstes

Anbieter von Fachdiensten MÜSSEN bei der Registrierung ihrer Authorization-Server am Federation Master die von ihnen erwarteten Attribute in `scopes` bzw. `claims` beschreiben und dem Federation Master zur Verfügung stellen. Die Registrierung MUSS ebenso die absolute URI des Fachdienstes im Internet umfassen (seine Client-ID) sowie dessen Signaturschlüssel für das Entity_Statement.

[<=]

Neu:

A_23045-02 - Registrierung des Fachdienstes

Anbieter von Fachdiensten MÜSSEN bei der Registrierung ihrer Authorization-Server am Federation Master die von ihnen erwarteten Attribute in `scopes` bzw. `claims` beschreiben und dem Federation Master zur Verfügung stellen. Die Registrierung MUSS ebenso die absolute URI des Fachdienstes im Internet umfassen (seine Client-ID) sowie dessen Signaturschlüssel für das Entity_Statement.

[<=]

Alt:

Hinweis: `claims` definieren konkrete Key/Value-Paare, die als Payload eines JWT codiert werden. `Scopes` fassen ein oder mehrere `claims` als Gruppe im Authorization Request zusammen. Ein vereinbarter `scope` sagt aus, welche Key/Value-Paare im Payload erwartet werden. Die Vereinbarung wird zwischen dem Fachdienst und dem Federation Master während der Registrierung des Fachdienstes getroffen. Im Rahmen einer Authentifizierung fragen Authorization Server den jeweils benötigten `scope` bzw. `claims` an, die im Rahmen des `ID_TOKEN` vom sektoralen Identity Provider bestätigt werden.

Neu:

Hinweis: `claims` definieren konkrete Key/Value-Paare, die als Payload eines JWT codiert werden. Ein `scopes` fassten ein oder mehrere `claims` als Gruppe im Authorization Request zusammen. Ein vereinbarter `scope` sagt aus, welche Key/Value-Paare im Payload erwartet werden. Die Vereinbarung wird zwischen dem Fachdienst und dem Federation Master während der Registrierung des Fachdienstes getroffen. Im Rahmen einer Authentifizierung fragen Authorization Server den jeweils benötigten `scope` bzw. `claims` an, die im Rahmen des `ID_TOKEN` vom sektoralen Identity Provider bestätigt werden.

Änderungen in Kapitel 4.2 "Übergreifende Festlegungen"

Alt:

Der Payload eines JWT beinhaltet Key/Value-Paare, welche in einem oder mehreren `scopes` definiert werden. Inhalte eines `scopes` sind mehrere Attribute, welche der sektorale IDP auf Basis der vorgetragenen Identität bestätigen kann.

Die `scopes` beinhalten die für diesen Fachdienst abgestimmten Attribute (die `scopes` werden pro Fachdienst in einem organisatorischen Prozess gesoert vom

jeweiligen Fachdienst mit dem Federation Master abgestimmt) und den Wertebereich, welchen diese annehmen können.

Neben den im Standard vorgesehenen Attributen (siehe [openid-connect-core-1.0.html#IDToken](#)) erwarten Fachdienste in der Regel weitere Informationen, wie zum Beispiel Vorname, Name, Rolle und KVNR des Nutzers. Siehe hierzu auch [gemSpec_IDP_Sek] Kapitel: "Token-Endpunkt Ausgangsdaten".

Neu:

Der Payload eines JWT beinhaltet Key/Value-Paare, welche in einem oder mehreren **scopes** definiert werden. Inhalte eines **scopes** sind mehrere Attribute, welche der sektorale IDP auf Basis der vorgetragenen Identität bestätigen kann.

Die **scopes** beinhalten die für diesen Fachdienst abgestimmten Attribute (die **scopes** werden pro Fachdienst in einem organisatorischen Prozess gesondert vom jeweiligen Fachdienst mit dem Federation Master abgestimmt) und den Wertebereich, welchen diese annehmen können.

Neben den im Standard vorgesehenen Attributen (siehe [\[OpenID Connect Core 1.0#IDToken\]](#)) erwarten Fachdienste in der Regel weitere Informationen, wie zum Beispiel Vorname, Name, Rolle und KVNR des Nutzers. Siehe hierzu auch [gemSpec_IDP_Sek] Kapitel: "Token-Endpunkt Ausgangsdaten".

Alt:

A_23036-01 - Inhalte der "scopes" für Versicherte

Fachdienste MÜSSEN bei ihrer Registrierung am Federation Master sicherstellen, dass ausschließlich die fachlich benötigten Attribute aus der in [gemSpec_IDP_Sek] Kapitel: "Token-Endpunkt Ausgangsdaten" definierten Auswahl als **scopes** und **claims** beantragt werden.

[<=]

Neu:

A_23036-02 - Inhalte des "scopes" für Versicherte

Fachdienste MÜSSEN bei ihrer Registrierung am Federation Master sicherstellen, dass ausschließlich die fachlich benötigten Attribute aus der in [gemSpec_IDP_Sek] Kapitel: "Token-Endpunkt Ausgangsdaten" definierten Auswahl als **scopes** und **claims** beantragt werden.

<=

Alt:

A_23037 - Robustheit bei fehlenden Daten

Sind einzelne **claims** des angefragten **scopes** nicht im **ID_TOKEN** enthalten oder leer, weil beispielsweise der Nutzer die Herausgabe verweigert oder Daten nicht hinterlegt wurden, so MUSS der Fachdienst das **ID_TOKEN** trotzdem akzeptieren und innerhalb der Fachanwendung geeignet reagieren.[<=]

Neu:

A_23037-01 - Robustheit bei fehlenden Daten

Sind einzelne **claims** des angefragten **scopes** nicht im **ID_TOKEN** enthalten oder leer, weil beispielsweise der Nutzer die Herausgabe verweigert oder Daten nicht hinterlegt wurden,

so MUSS der Fachdienst das `ID_TOKEN` trotzdem akzeptieren und innerhalb der Fachanwendung geeignet reagieren.[<=]

Alt:

A_23202-01 - Akzeptanz der Einwilligung zur Verwendung von Authentisierungsverfahren "gematik-ehealth-loa-substantial" beim Zugriff auf Daten mit hohem Schutzbedarf

Die Fachdienste der TI-Föderation MÜSSEN den Zugriff auf Daten mit hohem Schutzbedarf auch bei einer Authentisierung auf dem Niveau `gematik-ehealth-loa-substantial` 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.[<=]

Neu:

A_23202-02 - Akzeptanz der Einwilligung zur Verwendung von Authentisierungsverfahren "gematik-ehealth-loa-substantial" beim Zugriff auf Daten mit hohem Schutzbedarf

Die Fachdienste der TI-Föderation MÜSSEN den Zugriff auf Daten mit hohem Schutzbedarf auch bei einer Authentisierung auf dem Niveau `gematik-ehealth-loa-substantial` gewähren, wenn der `Claim amr` des `ID_TOKEN` `urn:telematik:auth:mEW` oder `urn:telematik:auth:sso` enthält und der Nutzer somit der Verwendung dieses Verfahrens für den Zugriff auf Daten mit hohem Schutzbedarf zugestimmt hat.[<=]

Änderungen in Kapitel 4.5 "Verifikation des "ID_TOKEN""

Alt:

A_22860-01 - Prüfung benötigter "scopes" und "claims"

Fachdienste MÜSSEN erhaltene `ID_TOKEN` auf das Vorhandensein der benötigten `scopes` und `claims` überprüfen.
[<=]

Neu:

A_22860-02 - Prüfung benötigter "scopes" und "claims"

Fachdienste MÜSSEN erhaltene `ID_TOKEN` auf das Vorhandensein der benötigten `scopes` und `claims` überprüfen.