Inhaltsverzeichnis

1 Änderungsbeschreibung....2
2 Änderung in gemSpec_IDP_FedMaster....3
3 Änderung in gemSpec_IDP_Sek....7
4 Änderung in gemSpec_IDP_FD....15
5 Änderungen in Steckbriefen....26
5.1 Änderungen in gemProdT_IDP_FedMaster_PTV....26
5.2 Änderungen in gemAnbT_IDP_FedMaster_ATV....26
5.3 Änderungen in gemProdT_IDP-Sek_PTV....27
5.4 Änderungen in gemAnbT_IDP-Sek_KTR_ATV....28
5.5 Änderungen in gemAnbT_IDP-Dienst....29
5.6 Änderungen in gemProdT_SigD....29
5.7 Änderungen in gemAnbT_Aktensystem_ePA....30
5.8 Änderungen in gemProdT_Aktensystem_ePA....30
5.9 Änderungen in gemAnbT_PoPP_Service....30
5.10 Änderungen in gemAnw_DiGA....31
5.11 Änderungen in gemAnw_OGR....32

1 Änderungsbeschreibung

In den aktuell veröffentlichten Spezifikationen gibt es Anforderungen, die nicht präzise genug formuliert oder falsch sind. Die Fehler sind zu korrigieren.
Im Detail handelt es sich um:

- Korrektur ML-133237 - AF_10118
- ID-Token V1 + V2
  - In gemKPT_TI-Foderation Tabelle "Attribute des ID-Token" sind die claims des ID-Token aufgezählt.
  - gemSpec_IDP_FD - "ML-133237 - AF_10118" verweist auf Tabellen der gemSpec_IDP_Sek
  - gemSpec_IDP_Sek - es gibt keine Anforderungen zur konkreten vollständigen Ausgestaltung ID-Token V1/V2
  - Ausführliche Beschreibung ID-Token V1 und ID-Token V2 - siehe auch https://service.gematik.de/browse/ANFIM-73
  - gemKPT_TI-Foderation - Beispiel ID-Token V1 +V2
- Afo(s) schärfen urn:telematik:auth:consentTyp String (ggf. Format für alle spezifischen claims festlegen)
- A_27593 und A_23202-02 SigD zuweisen
- Zuweisung sekt. IDP A_28886 und A_28866 aus gemSpec_Krypt und entfernen A_23006 dann.
- gemSpec_IDP_FD Doppeltes Kapitel 4 in gemSpec_IDP_FD
- gemSpec_IDP_Sek fehlerhafte Referenzen auf z.B A_22651
- gemSpec_IDP_FedMaster, gemSpec_IDP_Sek, gemSpec_IDP_FD redaktionelle Korrektur -claim "kid" Format soll UUID7 sein
  - neue verallgemeinerte Anforderung UUID7 A_28208-01 ersetzt A_28195 (sekt. IDPs) und A_28208 (Relying Parties)
    A_28208-01 wird in der Spezifiation FedMaster ergänzt und (analog der anderen allgemeinen Afos) den Releying Parties und sekt. IDPs zugewiesen. A_28195 und A_28208 werden storniert.
  - Angaben zum kid-Format UUID7 aus allen anderen Anforderungen entfernen
- amr für die Authentifizierung in der Geschäftsstelle - Hinweis ergänzen (siehe https://service.gematik.de/projects/ANFIM/queues/custom/339/ANFIM-62)
- AF_10116 - Der AF ist allen Relying Parties der TI-Föderation zuzuordnen, die kein 1:1 Bezug zum KTR haben. Die Zuordnung zum ePA-Aktensystem muss entfernt werden.

2 Änderung in gemSpec_IDP_FedMaster

Es wird in Kapitel "3.1 Anwendungsfall - Subordinate Statement bereitstellen" geändert redaktionell - die Formatangabe für "kid" entfällt, dafür gibt es eine entsprechende Afo A_28208-01

Alt:

AF_10101-02 - Bereitstellung von Informationen zu Teilnehmern der Föderation (Subordinate Statement)

Tabelle 1: Subordinate Statement - Response-Header-Attribute des signierten JSON-Web-Token

Name	Werte	Anmerkungen
`alg`	string, zulässiger Wert: "ES256"	
`kid`	string UUID7-Format [RFC9562#name-uuid-version-7]	Identifier des verwendeten Schlüssels aus dem jwks im Body des Statement
`typ`	entity-statement+jwt	

...

Neu:

AF_10101-03 - Bereitstellung von Informationen zu Teilnehmern der Föderation (Subordinate Statement)

Tabelle 2: Subordinate Statement - Response-Header-Attribute des signierten JSON-Web-Token

Name	Werte	Anmerkungen
`alg`	string, zulässiger Wert: "ES256"	
`kid`	string ~~UUID7-Format [RFC9562#name-uuid-version-7]~~	Identifier des verwendeten Schlüssels aus dem jwks im Body des Statement
`typ`	entity-statement+jwt	

...

Es wird in Kapitel "3.2.1 Anwendungsfall - IDP-Liste bereitstellen" geändert redaktionell - die Formatangabe für "kid" entfällt, dafür gibt es eine entsprechende Afo A_28208-01

Alt:

AF_10100-02 - Bereitstellung Liste registrierter Identity Provider

...

Tabelle 3: Liste sektorale Identity Provider - Headerattribute des signierten JSON-Web-Token

Name	Werte	Anmerkungen
`alg`	string, zulässiger Wert "ES256"	
kid	string UUID7-Format [RFC9562#name-uuid-version-7]	Identifier des federation_entity_signing_key des Federation Master. Der Schlüssel kann aus dem jwks im Body des Entity Statement des Federation Master ermittelt werden.
`typ`	idp-list+jwt	

Neu:

AF_10100-03 - Bereitstellung Liste registrierter Identity Provider

...

Tabelle 4: Liste sektorale Identity Provider - Headerattribute des signierten JSON-Web-Token

Name	Werte	Anmerkungen
`alg`	string, zulässiger Wert "ES256"	
kid	string ~~UUID7-Format [~~RFC9562#name-uuid-version-7~~]~~	Identifier des federation_entity_signing_key des Federation Master. Der Schlüssel kann aus dem jwks im Body des Entity Statement des Federation Master ermittelt werden.
`typ`	idp-list+jwt	

Es wird in Kapitel "4.1 Allgemeine Anforderungen an Teilnehmer der TI-Föderation" geändert

redaktionell - neue verallgemeinerte Anforderung UUID7 A_28208-01 ersetzt A_28195 (sekt. IDPs) und A_28208 (Relying Parties)

A_28208-01 wir in der Spezifiation FedMaster ergänzt und (analog der anderen allgemeinen Afos) den Releying Parties und sekt. IDPs zugewiesen. A_28195 und A_28208 werden storniert.

Neu:

A_28208-01 - Schlüssel-Identifier im JWK-Format

~~Der Anbieter des Fachdienstes als Relying Party~~ Ein Teilnehmer der TI-Föderation MUSS sicherstellen, dass bei der Bereitstellung neuer Schlüssel im JSON Web Key Set (JWKS) Format die Key Identifier der Schlüssel im UUID7-Format [RFC9562#name-uuid-version-7] vorliegen, die den Zeitpunkt der Schlüsselerzeugung widerspiegeln.

redaktionell - die Formatangabe für "kid" entfällt, dafür gibt es eine entsprechende Afo A_28208-01

Alt:

A_22607-01 - Entity Configuration Inhalte des Federation Master oder Intermediate
Federation Master und Intermediates MÜSSEN ihre Entity Configuration in einem selbst-signierten Entity Statement gemäß [OpenID Federation 1.1] ("Entity Statement") bereitstellen und im Internet verfügbar machen. Das Entity Statement MUSS mindestens die in der folgenden Tabelle aufgeführten Metadaten enthalten:

Tabelle 5: Header des Entity Statement der Superior Entity

Name	Werte / Wertebereich
`alg`	string, zulässiger Wert "ES256"
`kid`	string, UUID7-Format [RFC9562#name-uuid-version-7]
`typ`	string, zulässiger Wert "entity-statement+jwt"

....

Neu:

A_22607-02 - Entity Configuration Inhalte des Federation Master oder Intermediate
Federation Master und Intermediates MÜSSEN ihre Entity Configuration in einem selbst-signierten Entity Statement gemäß [OpenID Federation 1.1] ("Entity Statement") bereitstellen und im Internet verfügbar machen. Das Entity Statement MUSS mindestens die in der folgenden Tabelle aufgeführten Metadaten enthalten:

Tabelle 6: Header des Entity Statement der Superior Entity

Name	Werte / Wertebereich
`alg`	string, zulässiger Wert "ES256"
`kid`	string, ~~UUID7-Format [RFC9562#name-uuid-version-7]~~
`typ`	string, zulässiger Wert "entity-statement+jwt"

....

3 Änderung in gemSpec_IDP_Sek

Es wird in Kapitel "3.1 Sicherheitsanforderungen für den operativen Betrieb" geändert

redaktionell - Verweis auf Tabelle wird geändert

Alt:

A_23023 - Sicherung externen Schnittstellen gegen bösartige Eingaben
Der sektorale IDP MUSS sicherstellen, dass alle Eingabewerte, welche vom sektoralen IDP über externe Schnittstellen (siehe Tabelle "Schnittstellenübersicht") entgegengenommen und verarbeitet werden, auf schadhafte Werte geprüft werden.

Neu:

A_23023-01- Sicherung externen Schnittstellen gegen bösartige Eingaben
Der sektorale IDP MUSS sicherstellen, dass alle Eingabewerte, welche vom sektoralen IDP über externe Schnittstellen (siehe ~~Tabelle "Schnittstellenübersicht"~~ [gemKPT_TI-Föderation] "Schnittstellen zu Umsystemen") entgegengenommen und verarbeitet werden, auf schadhafte Werte geprüft werden.

Es wird in Kapitel "3.2.2 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld" geändert

Die Anforderungen aus A__23006 werden inhaltlich durch A_28886 und A_28866 der [gemSpec_Krypt] abgebildet. A_28886 und A_28866 werden den sekt. IDP zugewiesen, A_23006 und der Hinweis zu A_23006 entfallen.

~~**A_23006 - Subdomäne für Webservice-Endpunkte in der VAU**~~
~~Der Verarbeitungskontext des sektoralen IDP MUSS diese Endpunkte anbieten:~~

- ~~Endpunkt für Authorization Requests~~
- ~~Endpunkt für Pushed Authorization Requests~~
- ~~Token-Endpunkt~~

~~Für die Endpunkte der VAU MUSS eine eigene Subdomäne, welche keine Wildcard-Domäne ist, erstellt werden~~

~~*Hinweis: Die Erstellung einer eigenen Subdomäne für die VAU eines sektoralen IDP ist notwendig, um die Certificate Transparency TLS-Zertifikate im Federation Master effektiv prüfen zu können.*~~

Es wird in Kapitel "4.2 Entity Statement des sektoralen IDP" geändert

redaktionell - neue verallgemeinerte Anforderung UUID7 A_28208-01 ersetzt A_28195 (sekt. IDPs). A_28208-01 wird in der Spezifikation FedMaster ergänzt und (analog der anderen allgemeinen Afos) und sekt. IDPs zugewiesen. A_28195 wird storniert.

Alt:

A_28195 - Anbieter sektoraler IDP - Schlüssel-Identifier im JWK-Format
Der Anbieter des sektoralen IDP MUSS sicherstellen, dass bei der Bereitstellung neuer Schlüssel im JSON Web Key Set (JWKS) Format die Key Identifier der Schlüssel im UUID7-Format [RFC9562#name-uuid-version-7] vorliegen, die den Zeitpunkt der Schlüsselerzeugung widerspiegeln.

Neu (gemSpec_IDP_FedMaster):

A_28208-01 - Schlüssel-Identifier im JWK-Format

~~Der Anbieter des Fachdienstes als Relying Party~~ Ein Teilnehmer der TI-Föderation MUSS sicherstellen, dass bei der Bereitstellung neuer Schlüssel im JSON Web Key Set (JWKS) Format die Key Identifier der Schlüssel im UUID7-Format [RFC9562#name-uuid-version-7] vorliegen, die den Zeitpunkt der Schlüsselerzeugung widerspiegeln.

redaktionell - die Formatangabe für "kid" entfällt, dafür gibt es eine entsprechende Afo A_28208-01

Alt:

A_22643-02 - Entity Statement des sektoralen IDP

Der sektorale IDP MUSS ein selbst signiertes Entity Statement gemäß[OpenID Federation 1.1] ("Entity Statement") bereitstellen und im Internet verfügbar machen. Das Entity Statement MUSS mindestens die in der folgenden Tabelle aufgeführten Metadaten enthalten:

Tabelle 7: Header des Entity Statement des sektoralen IDP

Name	Werte / Wertebereich
`alg`	string, zulässiger Wert "ES256"
`kid`	string, UUID7-Format [RFC9562#name-uuid-version-7]
`typ`	string, zulässiger Wert "entity-statement+jwt"

...

Neu:

A_22643-03 - Entity Statement des sektoralen IDP

Der sektorale IDP MUSS ein selbst signiertes Entity Statement gemäß[OpenID Federation 1.1] ("Entity Statement") bereitstellen und im Internet verfügbar machen. Das Entity Statement MUSS mindestens die in der folgenden Tabelle aufgeführten Metadaten enthalten:

Tabelle 8: Header des Entity Statement des sektoralen IDP

Name	Werte / Wertebereich
`alg`	string, zulässiger Wert "ES256"
`kid`	string, ~~UUID7-Format [RFC9562#name-uuid-version-7]~~
`typ`	string, zulässiger Wert "entity-statement+jwt"

...

Es wird in Kapitel "4.3.2.1 PAR-Endpunkt Eingangsdaten" geändert

redaktionell - Verweis auf Tabelle wird entfernt.

Alt:

A_22651 - Parameter des Pushed Authorization Request durch den sektoralen IDP
Der sektorale IDP MUSS die Annahme von Pushed Authorization Request gemäß [OAuth 2.0 Pushed Authorization Requests#section-2] unterstützen und den Endpoint für Pushed Authorization Request im Entity Statement des sektoralen IDP`pushed_authorization_request_endpoint` bekanntgeben.
Der sektorale IDP MUSS mindestens die in der ML-132850 - Missing cross-referenceTabelle *Parameter Pushed Authorization Request* dargestellten Parameter im Pushed Authorization Request des Authorization Server eines Fachdienstes annehmen.

Neu:

A_22651-01 - Parameter des Pushed Authorization Request durch den sektoralen IDP
Der sektorale IDP MUSS die Annahme von Pushed Authorization Request gemäß [OAuth 2.0 Pushed Authorization Requests#section-2] unterstützen und den Endpoint für Pushed Authorization Request im Entity Statement des sektoralen IDP`pushed_authorization_request_endpoint` bekanntgeben.
~~Der sektorale IDP MUSS mindestens die in der ML-132850 - Missing cross-referenceTabelle *Parameter Pushed Authorization Request* dargestellten Parameter im Pushed Authorization Request des Authorization Server eines Fachdienstes annehmen.~~

redaktionell - Hinweis zur Berücksichtigung Postels Gesetz unter A_22966-02 ergänzt

Neu:

A_22966-02 -Prüfung eingehender Pushed Authorization Request durch den sektoralen IDP

Der sektorale IDP MUSS eingehende Pushed Authorization Requests validieren und invalide Requests gemäß [OAuth 2.0 Pushed Authorization Requests#section-2.3] mit einer Fehlermeldung ablehnen. Die Validierung eines eingegangenen Pushed Authorization Request MUSS die Prüfung der im Request enthaltenen Werte für redirect_uri, scope und claims beinhalten. Dabei müssen redirect_uri, scope und claims aus dem Pushed Authorization Request eine Teilmenge der Werte sein, die der Federation Master für diesen Fachdienst in der Teilnehmerauskunft liefert. [<=]

Hinweis: Entsprechend des Postels Gesetz prüft der sektorale IDP das Vorhandensein aller für den PAR notwendigen Parameter. Er prüft jedoch nicht, ob die Parameter selbst den Vorgaben gemSpec_IDP_FD entsprechen, wenn dies für die weitere fehlerfreie Bearbeitung nicht notwendig ist.

Es wird ein Kapitel "4.3.4.2.1 Beispiele für ID-Token V1 und V2" eingefügt

redaktionell - Beispiele für ID-Token V1 und V2 eingefügt

Fallbeispiel 1:

- Die Relying Party hat in ihrem Entity Statement den claim default_acr_values = ["gematik-ehealth-loa-high"] oder im PAR acr_values="gematik-ehealth-loa-high" gesetzt.
- Der Versicherte authentifiziert sich mit Biometrie nachdem er der Absenkung des Vertrauensniveau (A_23103*) zugestimmt hat

Tabelle 9: Authentifizierung mit Biometrie

ID-Token V1	ID-Token V2
acr=gematik-ehealth-loa-substantial	acr=gematik-ehealth-loa-substantial
amr=urn:telematik:auth:mEW	amr=urn:telematik:auth:other
urn:telematik:auth:interactive nicht vorhanden	urn:telematik:auth:interactive nicht vorhanden
urn:telematik:auth:consent nicht vorhanden	urn:telematik:auth:consent = [loa-substantial]

Fallbeispiel 2:

- Die Relying Party hat in ihrem Entity Statement den claim default_acr_values = ["gematik-ehealth-loa-high"] oder im PAR acr_values="gematik-ehealth-loa-high" gesetzt.
- Der Versicherte authentifiziert sich über SSO auf Basis einer Authentifizierung mit Gerätebindung (juenger als 6 Monate) und PIN Eingabe

Tabelle 10: Authentifizierung mit SSO nach Erstauthenifizierung mit System-PIN

ID-Token V1	ID-Token V2
acr=gematik-ehealth-loa-high	acr=gematik-ehealth-loa-high
amr=urn:telematik:auth:sso (+ urn:telematik:auth:mEW)	amr=urn:telematik:auth:other
urn:telematik:auth:interactive nicht vorhanden	urn:telematik:auth:interactive = "silent"
urn:telematik:auth:consent nicht vorhanden	urn:telematik:auth:consent nicht vorhanden

Fallbeispiel 3:

- Die Relying Party hat in ihrem Entity Statement den claim default_acr_values = ["gematik-ehealth-loa-high"] oder im PAR acr_values="gematik-ehealth-loa-high" gesetzt.
- Der Versicherte authentifiziert sich über SSO auf Basis Biometrie nachdem er der Absenkung des Vertrauensniveau (A_23103*) zugestimmt hat.

Tabelle 11: Authentifizierung mit SSO nach Erstauthenifizierung mit Biometrie

ID-Token V1	ID-Token V2

acr=gematik-ehealth-loa-substantial,	acr=gematik-ehealth-loa-substantial,
amr=urn:telematik:auth:sso (+ urn:telematik:auth:mEW)	amr=urn:telematik:auth:other
urn:telematik:auth:interactive nicht vorhanden	urn:telematik:auth:interactive = "silent"
urn:telematik:auth:consent nicht vorhanden	urn:telematik:auth:consent = [loa-substantial]

Es wird in Kapitel "4.4.2 Authentifizierungsverfahren" geändert

redaktionell - Präzisierung für den Fall der Authentifizierung in der Geschäftsstelle mit hoheitlichem Dokument (Personalausweis, Pass).

Alt:

A_23129-06 - Identifikation des Authentisierungsverfahren

Der sektorale IDP MUSS den Claim amr im ID_TOKEN entsprechend dem durchgeführten Authentisierungsverfahren nach folgender Tabelle befüllen.

Tabelle 12: Codierung der Authentisierungsverfahren

Authentisierungsverfahren	**Wert des`amr` Claim**	**zulässiges Niveau (`acr`)**
Authentisierung mittels eGK und PIN	urn:telematik:auth:eGK	gematik-ehealth-loa-high
Authentisierung mittels elektronischem Identitätsnachweis (Online-Ausweisfunktion)	urn:telematik:auth:eID	gematik-ehealth-loa-high
Authentisierung mittels eGK und PIN ohne Prüfung Gerätebindung (Gastzugang)	urn:telematik:auth:guest:eGK	gematik-ehealth-loa-high
Authentisierung mittels PID einer zertifizierten EUDI-Wallet	urn:telematik:auth:eudiWallet	gematik-ehealth-loa-high
Anderes Authentisierungsverfahren	urn:telematik:auth:other	gematik-ehealth-loa-high und gematik-ehealth-loa-substantial
Authentisierungsverfahren mit Einwilligung für ein Single Sign-On (SSO) (deprecated)	urn:telematik:auth:sso	gematik-ehealth-loa-high gematik-ehealth-loa-substantial

Authentisierungsverfahren mit Einwilligung zum Zugriff auf Daten mit hohem Schutzbedarf (deprecated)	urn:telematik:auth:mEW	gematik-ehealth-loa-substantial

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

Neu:

A_23129-07 - Identifikation des Authentisierungsverfahren

Der sektorale IDP MUSS den Claim amr im ID_TOKEN entsprechend dem durchgeführten Authentisierungsverfahren nach folgender Tabelle befüllen.

Tabelle 13: Codierung der Authentisierungsverfahren

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

Hinweis: Findet im Rahmen der Identifizierung einer Person mit einem hoheitlichen Dokument (Personalausweis, Pass) in der Geschäftsstelle des Kostenträgers auch eine

Authentifizierung statt, so ist dafür im ID-Token amr=urn:telematik:auth:eID zu belegen.
Hinweis: Die Authentisierungsverfahren "urn:telematik:auth:sso" und "urn:telematik:auth:mEW"werden nach vollständiger Umsetzung der Anforderungen A_27591, A_27592 und A_27593 durch alle Teilnehmer der TI-Föderation aus der Anforderung entfernt.

redaktionell - Eindeutige Markierung "loa-substantial" als String

Alt:

A_27591 - Signalisierung der Einwilligung durch den Nutzer in "gematik-ehealth-loa-substantial" beim Zugriff auf Daten mit hohem Schutzbedarf

Der sektorale IDP MUSS in den Custom Claim urn:telematik:auth:consent den Wert loa-substantial ergänzen, wenn der Fachdienst eine Authentisierung des Nutzers auf dem Niveau gematik-ehealth-loa-high angefragt, der Nutzer jedoch ein Authentisierungsverfahren auf dem Niveau gematik-ehealth-loa-substantial verwendet hat und die Einwilligung des Anwenders zur Nutzung dieses Verfahrens zum Zugriff auf Daten mit hohem Schutzbedarf vorliegt.<=

Neu:

A_27591-01 - Signalisierung der Einwilligung durch den Nutzer in "gematik-ehealth-loa-substantial" beim Zugriff auf Daten mit hohem Schutzbedarf

Der sektorale IDP MUSS in den Custom Claim urn:telematik:auth:consent den ~~Wert~~ String "loa-substantial" ergänzen, wenn der Fachdienst eine Authentisierung des Nutzers auf dem Niveau gematik-ehealth-loa-high angefragt, der Nutzer jedoch ein Authentisierungsverfahren auf dem Niveau gematik-ehealth-loa-substantial verwendet hat und die Einwilligung des Anwenders zur Nutzung dieses Verfahrens zum Zugriff auf Daten mit hohem Schutzbedarf vorliegt.<=

Es wird in Kapitel "5.2.2 Rahmenbedingungen" geändert

redaktionell - Verweis auf [gemSpec_IDP_Sek#Tabelle Ablaufbeschreibung App-App-Flow] korrigiert

Alt:

A_24748-01 - SSO-Unterstützung auf Anwendungsebene innerhalb einer APP
Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS in seinem Authenticator-Modul eine Schnittstelle anbieten, der das Client-Modul bzw. Frontend eines TI-Fachdienstes die vom sektoralen IDP als Ergebnis des Pushed Authorization Request ausgestellte URI-PAR übergeben kann (siehe [gemSpec_IDP_Sek#Tabelle Ablaufbeschreibung App-App-Flow] Schritt 5). Die Schnittstelle MUSS als Ergebnis des Aufrufs den vom sektoralen IDP nach erfolgreicher Nutzerauthentisierung ausgestellten AUTH_CODE an das aufrufende Client-Modul zurückgeben.

Neu:

A_24748-02 - SSO-Unterstützung auf Anwendungsebene innerhalb einer APP
Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS in seinem Authenticator-Modul eine Schnittstelle anbieten, der das Client-Modul bzw. Frontend eines TI-Fachdienstes die vom sektoralen IDP als Ergebnis des Pushed Authorization Request ausgestellte URI-PAR übergeben kann (siehe~~[gemSpec_IDP_Sek#Tabelle Ablaufbeschreibung App-App-Flow] Schritt 5~~ [gemKPT-TI-Föderation] Kapitel "Ablaufbeschreibung App2App-Flow"). Die Schnittstelle MUSS als Ergebnis des Aufrufs den vom sektoralen IDP nach erfolgreicher Nutzerauthentisierung ausgestellten AUTH_CODE an das aufrufende Client-Modul zurückgeben.

324

325

4 Änderung in gemSpec_IDP_FD

Es wird in Kapitel "3.4 Entity Statements" geändert

redaktionell - neue verallgemeinerte Anforderung UUID7 A_28208-01 ersetzt A_28208 (Relying Parties)

A_28208-01 wir in der Spezifikation FedMaster ergänzt und (analog der anderen allgemeinen Afos) den Releying Parties zugewiesen. A_28208 wird storniert.

Alt:

A_28208 - Schlüssel-Identifier im JWK-Format

Der Anbieter des Fachdienstes als Relying Party der TI-Föderation MUSS sicherstellen, dass bei der Bereitstellung neuer Schlüssel im JSON Web Key Set (JWKS) Format die Key Identifier der Schlüssel im UUID7-Format [RFC9562#name-uuid-version-7] vorliegen, die den Zeitpunkt der Schlüsselerzeugung widerspiegeln.

Neu (gemSpec_IDP_FedMaster):

A_28208-01 - Schlüssel-Identifier im JWK-Format

~~Der Anbieter des Fachdienstes als Relying Party~~ Ein Teilnehmer der TI-Föderation MUSS sicherstellen, dass bei der Bereitstellung neuer Schlüssel im JSON Web Key Set (JWKS) Format die Key Identifier der Schlüssel im UUID7-Format [RFC9562#name-uuid-version-7] vorliegen, die den Zeitpunkt der Schlüsselerzeugung widerspiegeln.

Es wird in Kapitel "3.5 Anfrage von ID_TOKEN beim sektoralen Identity Provider" geändert

- AF_10117 wird präzisiert.
  - Nicht mehr vorhandene Links und Referenzen werden entfernt. Die Tabelle mit den Parametern eines PAR wird in den AF mit aufgenommen (stett Referenz auf anderes Dokument).
  - In einem Hinweis sind best practices für die Ausgestaltung "nonce" und "state" formuliert
- ML-133233 wird präzisiert
- ML-133234 ist in ML-133233 enthalten und kann deshalb entfallen
- AF_10118 wird präzisiert. Nicht mehr vorhandene Links und Referenzen werden entfernt. Die Tabelle mit den Parametern eines PAR wird in den AF mit aufgenommen (stett Referenz auf anderes Dokument).
- ML-133236 wird präzisiert
- ML-133237 ist in ML-133236 enthalten und kann deshalb entfallen

Alt:

AF_10117 - OAuth 2.0 Pushed Authorization Request

Tabelle 14: Anwendungsfall "OAuth 2.0 Pushed Authorization Request"

Attribute	Bemerkung

Beschreibung	Ein Anwender möchte einen in der TI registrierten Fachdienst nutzen. Der Fachdienst muss sicherstellen, dass der Anwender zur Nutzung des Dienstes berechtigt ist. Hierzu authentisiert sich der Anwender gegenüber einem sektoralen Identity Provider, bei dem er registriert ist. Der Fachdienst als Relying Party der TI-Föderation MUSS bei Erhalt eines Autorisierung Requests vom Anwendungsfrontend oder vom Web-Backend eine entsprechende Anfrage (Pushed Authorization Request) an den angegebenen sektoralen Identity Provider senden. Anschließend sendet die Relying Party die vom sektoralen Identity Provider erhaltene URI zurück an die aufrufende Instanz.
Akteur	Anwender der Fachanwendung
Auslöser	Ein Anwender möchte eine Gesundheitsanwendung der TI (Fachdienst) nutzen. Als Voraussetzung muss er sich bei einem sektoralen Identity Provider authentifizieren, bei welchem er registriert ist.
Komponenten	• Anwendungsfrontend oder Web-Backend • Fachdienstes als Relying Party der TI-Föderation • sektoraler Identity Provider
Vorbedingung	1. Der Anwender ist durch einen der (sektoralen) Identity Provider identifiziert worden 2. Das Entity Statement des Federation Master steht zur Verfügung. 3. Der involvierte sektorale Identity Provider ist beim Federation Master registriert.
Ablauf	1. Das Anwendungsfrontend oder Web-Backend schickt einen Authorization Request unter Angabe des zu verwendenden sektoralen Identity Providers an die Komponente des Fachdienstes, der als Relying Party der TI-Föderation registriert ist. 2. Die Relying Party prüft, ob er das Entity Statement des angegebenen sektoralen Identity Provider kennt und ob dieses nicht älter als 24h ist. Ist das Entity Statement des angegebenen sektoralen Identity Provider unbekannt oder älter als 24h, lädt die Relying Party das Entity Statement vom angegebenen sektoralen Identity Provider entsprechend [gemSpec_IDP_Sek#Kapitel: Entity Statement des sektoralen IDP]. 3. Die Relying Party sendet seinerseits einen Pushed Authentication Request an den Pushed Authorization Endpoint des angegebenen sektoralen Identity Providers ([gemSpec_IDP_Sek#Tabelle: Parameter Pushed Authorization Request]). In diesem Request sind zufällige "state" und "nonce" Parameter enthalten, welche die Relying Party nutzt, um

	spätere Antworten zuzuordnen und zu validieren. 4. (Falls nötig, lädt der sektorale Identity Provider das Entity Statement der Relying Party entsprechend A_23034*.) 5. Der sektorale Identity Provider antwortet mit einer URI auf den Pushed Authorization Request ([gemSpec_IDP_Sek#Tabelle: Parameter der HTTP-Response]) ([https://www.rfc-editor.org/rfc/rfc9126.html]). 6. Die Relying Party sendet die URI zurück an die aufrufende Instanz. ([gemSpec_IDP_Sek#Tabelle: Request Parameter des Fachdienstes zum sektoralen IDP])
Ergebnis	Das Anwendungsfrontend oder Web-Backend hat die PAR URI erhalten, mittels derer er die Benutzerauthentifizierung initiieren kann.
Akzeptanzkriterien	ML-133233 - AF_10117 - Antwort auf den Pushed Authorization Request, ML-133234 - AF_10117 - PAR URI
Alternativen	keine

Neu:

AF_10117-01 - OAuth 2.0 Pushed Authorization Request

Tabelle 15: Anwendungsfall "OAuth 2.0 Pushed Authorization Request"

Attribute	**Bemerkung**
Beschreibung	Ein Anwender möchte einen in der TI registrierten Fachdienst nutzen. Der Fachdienst muss sicherstellen, dass der Anwender zur Nutzung des Dienstes berechtigt ist. Hierzu authentisiert sich der Anwender gegenüber einem sektoralen Identity Provider, bei dem er registriert ist. Der Fachdienst als Relying Party der TI-Föderation MUSS bei Erhalt eines Autorisierung Requests vom Anwendungsfrontend oder vom Web-Backend eine entsprechende Anfrage (Pushed Authorization Request) an den angegebenen sektoralen Identity Provider senden. Anschließend sendet die Relying Party die vom sektoralen Identity Provider erhaltene URI zurück an die aufrufende Instanz.
Akteur	Anwender der Fachanwendung
Auslöser	Ein Anwender möchte eine Gesundheitsanwendung der TI (Fachdienst) nutzen. Als Voraussetzung muss er sich bei einem sektoralen Identity Provider authentifizieren, bei welchem er registriert ist.
Komponenten	• Anwendungsfrontend oder Web-Backend • Fachdienstes als Relying Party der TI-Föderation • sektoraler Identity Provider
Vorbedingung	1. Der Anwender ist durch einen der (sektoralen) Identity Provider identifiziert worden

	2. Das Entity Statement des Federation Master steht zur Verfügung. 3. Der Fachdienst Authorization Server ist in der TI-Föderation registriert. 4. Der involvierte sektorale Identity Provider ist ~~beim Federation Master~~ in der TI-Föderation registriert.
Ablauf	1. Das Anwendungsfrontend oder Web-Backend schickt einen Authorization Request unter Angabe des zu verwendenden sektoralen Identity Providers an die Komponente des Fachdienstes, der als Relying Party der TI-Föderation registriert ist. 2. Die Relying Party prüft, ob er das Entity Statement des angegebenen sektoralen Identity Provider kennt und ob dieses nicht älter als 24h ist. Ist das Entity Statement des angegebenen sektoralen Identity Provider unbekannt oder älter als 24h, lädt die Relying Party das Entity Statement vom angegebenen sektoralen Identity Provider~~entsprechend [gemSpec_IDP_Sek#Kapitel: Entity Statement des sektoralen IDP]~~. 3. Die Relying Party sendet ihrerseits einen Pushed Authentication Request (PAR) an den aus dem Entity Statement des sektoralen Identity Providers ermittelten Pushed Authorization Endpoint ~~des angegebenen sektoralen Identity Providers ([gemSpec_IDP_Sek#Tabelle: Parameter Pushed Authorization Request])~~. Die Tabelle "Inhalte eines Pushed Authorization Request" listet die Parameter eines PAR. In diesem Request sind zufällige "state" und "nonce" Parameter enthalten, welche die Relying Party nutzt, um spätere Antworten zuzuordnen und zu validieren. 4. Falls nötig, lädt der sektorale Identity Provider das Entity Statement der Relying Party entsprechend A_23034*. 5. Der sektorale Identity Provider antwortet ~~mit einer URI auf den Pushed Authorization Request ([gemSpec_IDP_Sek#Tabelle: Parameter der HTTP-Response]) ([https://www.rfc-editor.org/rfc/rfc9126.html])~~ auf den Pushed Authorization Request gemäß A_22992* [gemSpec_IDP_Sek] und [RFC9126#section-2.2] mit einer URI-PAR. 6. Die Relying Party sendet die URI-PAR zurück an ~~die aufrufende Instanz. ([gemSpec_IDP_Sek#Tabelle: Request Parameter des Fachdienstes zum sektoralen IDP])~~ das aufrufende Anwendungsfrontend oder Web-Backend.
Ergebnis	Das Anwendungsfrontend oder Web-Backend hat die PAR URI erhalten, mittels derer er die Benutzerauthentifizierung initiieren kann.
Akzeptanzkriterien	ML-133233 - AF_10117 - Antwort auf den Pushed Authorization Request

368 **Tabelle 16: Inhalte eines Pushed Authorization Request**

Name	Anmerkungen
client_id	Die client_id ist die ID des als OpenID-Relying-Party in der TI-Föderation registrierten Fachdienstes in der TI-Föderation, welcher den Pushed Authorization Request an den s IDP stellt. Die client_id entspricht dem claim "iss" in dessen Entity Statement.
state	Vom Fachdienst (OpenID-Relying-Party) erstellter Zufallswert, der in der weiteren Kommunikation mit dem sektoralen IDP zur Prüfung der Integrität verwendet wird.
redirect_uri	Adresse, an welche der vom sektoralen IDP ausgestellte Authorization Code zugestellt soll. I.d.R. ist dies der als OpenID-Relying-Party in der TI-Föderation registrierte Fachdie

code_challenge	Hash über einen vom Fachdienst (OpenID-Relying-Party) erzeugten "code_verifier".
code_challenge_method	Methode, mit welcher der Hashwert "code_challenge" aus dem "code_verifier" erzeugt
response_type	Für den Authorization Code Flow ist "response_type"="code".
nonce	Die nonce ist ein vom Fachdienst (OpenID-Relying-Party) ausgesteller Zufallswert.
scope	Im claim "scope" sind die Informationen (scopes) aufgeführt, die der Fachdienst (Openl Relying-Party) im vom sektoralen IDP ausgestellten ID-Token erwartet.
acr_values	Der claim "acr_values" gibt an, welche Vertrauensniveaus bei der Nutzerauthentifizieru eingehalten werden müssen, damit der Fachdienst der Authentifizierung vertrauen kan Wert hat Einfluss darauf, welche Authentisierungsmittel dem Nutzer angeoten werden. Für alle TI-Fachdienst und Anwendungen, die Gesundheitsdaten verarbeiten muss acr_values="gematik-ehealth-loa-high" sein.

Hinweis: Der Pushed Authorization Request kann weitere oder z.T. andere claims enthalten (z.B. "essential" claims nach A_24932).*

Hinweis: Für die "nonce" ist A_24833 zu beachten. Es wird empfohlen die Vorgaben für die "nonce" auch für den state-Parameter einzuhalten. Des weiteren sollten "state" und "nonce" nur einmalig verwendet werden. Die Erzeugung der Werte sollte zufällig (z.B. über Zufallszahlen-Generatoren oder UUID-Generatoren) erfolgen.*

Alt:

ML-133233 - AF_10117 - Antwort auf den Pushed Authorization Request

Das Anwendungsfrontend oder Web-Backend hat die Antwort auf den Pushed Authorization Request von der Relying Party erhalten.

Neu:

ML-133233 - AF_10117 - Antwort auf den Pushed Authorization Request

Das Anwendungsfrontend oder Web-Backend hat ~~die~~ als Antwort auf den Pushed Authorization Request von der Relying Party erhalten:

- entwerder HTTP-201 und die URI-PAR
- oder einen HTTP-Error Code

~~**ML-133234-AF_10117 - PAR URI**~~

~~Die gelieferte Antwort enthält die PAR URI, mittels derer das Anwendungsfrontend oder Web-Backend die Benutzerauthentifizierung initiieren kann.~~

Alt:

AF_10118 - Benutzerauthentifizierung und Erhalt des ID_TOKEN

394 **Tabelle 17: Anwendungsfall "Benutzerauthentifizierung und Erhalt des`ID_TOKEN`"**

Attribute	Bemerkung
Beschreibung	Ein Anwender möchte einen in der TI registrierten Fachdienst nutzen. Der Fachdienst muss sicherstellen, dass der Anwender zur Nutzung des Dienstes berechtigt ist. Hierzu authentisiert sich der Anwender gegenüber einem sektoralen Identity Provider, bei dem er registriert ist. Nach Abschluss der Authentifizierung des Nutzers gegenüber dem sektoralen Identity Provider, erhält der Fachdienst als Relying Party der TI-Föderation den `AUTHORIZATION_CODE` mit dem er das `ID_TOKEN` abrufen kann.
Akteur	Anwender der Fachanwendung
Auslöser	Ein Anwender möchte eine Gesundheitsanwendung der TI (Fachdienst) nutzen. Als Voraussetzung muss er sich bei einem sektoralen Identity Provider authentifizieren, bei welchem er registriert ist. Das Anwendungsfrontend erhält von der Relying Party die Pushed Authorization Requests URI zurück ([gemSpec_IDP_Sek#Kapitel: PAR-Endpunkt Ausgangsdaten]).
Komponenten	• Anwendungsfrontend oder Web-Backend • Fachdienst als Relying Party der TI-Föderation • sektoraler Identity Provider
Vorbedingung	1. Der Anwender ist durch einen der (sektoraler) Identity Provider identifiziert worden 2. Das Entity Statement des Federation Master steht zur Verfügung. 3. Der involvierte sektorale Identity Provider ist beim Federation Master registriert. 4. Der Fachdienst ist als Relying Party in der TI-Föderation registriert 5. Eine OAuth 2.0 Pushed Authorization Request URI wurde entsprechend [gemSpec_IDP_Sek#Kapitel: PAR-Endpunkt Ausgangsdaten] zurück geliefert.
Ablauf	1. Das Anwendungsfrontend oder Web-Backend ruft den Authorization-Endpunkt des sektoralen Identity Providers auf und übergibt die OAuth 2.0 Pushed Authorization Requests URI. Diese leitet weiter auf das Web-Frontend des sektoralen Identity Providers oder direkt auf dessen Authenticator-Modul. (Die eigentliche Authentifizierung erfolgt Implementations-spezifisch und wird hier nicht weiter definiert.) 2. Nach erfolgreichem Abschluss der Authentisierung sendet der sektorale Identity Provider einen `AUTHORIZATION_CODE` an das aufrufende Anwendungsfrontend oder Web-Backend. 3. Das Anwendungsfrontend oder Web-Backend sendet den `AUTHORIZATION_CODE` an den als Relying Party in der TI-

	Föderation registrierten Fachdienst. 4. Dier Releying Party sendet den AUTHORIZATION_CODE an den involvierten sektoralen Identity Provider [gemSpec_IDP_Sek#Kapitel: Detailinformationen zum App-App-Flow - Schritt 10] und authentisiert sich dabei als Client der TLS Verbindung mit einem Zertifikat das über sein Entity Statement validierbar ist. 5. Der sektorale Identity Provider überprüft die Gültigkeit des AUTHORIZATION_CODE entsprechend [https://datatracker.ietf.org/doc/html/rfc7636#section-4.6] 6. Der sektorale Identity Provider antwortet dem Fachdienst als Relying Party der TI-Föderation nach erfolgreicher Überprüfung des AUTHORIZATION_CODE mit dem zugehörigen ID_TOKEN. ([gemSpec_IDP_Sek#Kapitel: Detailinformationen zum App-App-Flow - Schritt 11])
Ergebnis	Der Nutzer ist authentifiziert und der Fachdienst als Relying Party der TI-Föderation hat den ID_TOKEN mit dem es den ACCESS_TOKEN zum Zugriff auf die Fachdienst API abrufen kann.
Akzeptanzkriterien	ML-133236 - AF_10118 - ID_TOKEN erhalten, ~~ML-133237 – AF_10118 - ID_TOKEN entspricht Vorgaben~~

Neu:

AF_10118-01 - Benutzerauthentifizierung und Erhalt des ID_TOKEN

Tabelle 18: Anwendungsfall "Benutzerauthentifizierung und Erhalt des ID_TOKEN"

Attribute	Bemerkung
Beschreibung	Ein Anwender möchte einen in der TI registrierten Fachdienst nutzen. Der Fachdienst muss sicherstellen, dass der Anwender zur Nutzung des Dienstes berechtigt ist. Hierzu authentisiert sich der Anwender gegenüber einem sektoralen Identity Provider, bei dem er registriert ist. Nach Abschluss der Authentifizierung des Nutzers gegenüber dem sektoralen Identity Provider, erhält der Fachdienst als Relying Party der TI-Föderation den AUTHORIZATION_CODE mit dem er das ID_TOKEN abrufen kann.
Akteur	Anwender der Fachanwendung
Auslöser	Ein Anwender möchte eine Gesundheitsanwendung der TI (Fachdienst) nutzen. Als Voraussetzung muss er sich bei einem sektoralen Identity Provider authentifizieren, bei welchem er registriert ist. Das Anwendungsfrontend erhält von der Relying Party die Pushed Authorization Requests URI (URI-PAR) zurück (AF_10117*) ~~([gemSpec_IDP_Sek#Kapitel: PAR-Endpunkt Ausgangsdaten])~~.
Komponenten	• Anwendungsfrontend oder Web-Backend • Fachdienst als Relying Party der TI-Föderation • sektoraler Identity Provider
Vorbedingung	1. Der Anwender ist durch einen der (sektoraler) Identity Provider identifiziert worden

	2. Das Entity Statement des Federation Master steht zur Verfügung. 3. Der involvierte sektorale Identity Provider ist beim Federation Master registriert. 4. Der Fachdienst ist als Relying Party in der TI-Föderation registriert 5. Eine ~~OAuth 2.0 Pushed Authorization Request URI wurde entsprechend [gemSpec_IDP_Sek#Kapitel: PAR-Endpunkt Ausgangsdaten]~~ URI-PAR wurde entsprechend AF_10117* zurück geliefert.
Ablauf	1. Das Anwendungsfrontend oder Web-Backend ruft den Authorization-Endpunkt des sektoralen Identity Providers auf und übergibt die~~OAuth 2.0 Pushed Authorization Requests URI~~ URI-PAR. Diese leitet weiter auf das Web-Frontend des sektoralen Identity Providers oder direkt auf dessen Authenticator-Modul. (Die eigentliche Authentifizierung erfolgt Implementations-spezifisch und wird hier nicht weiter definiert.) 2. Nach erfolgreichem Abschluss der Authentisierung sendet der sektorale Identity Provider einen `AUTHORIZATION_CODE` an das aufrufende Anwendungsfrontend oder Web-Backend. 3. Das Anwendungsfrontend oder Web-Backend sendet den `AUTHORIZATION_CODE` an den als Relying Party in der TI-Föderation registrierten Fachdienst. 4. Die Releying Party sendet den `AUTHORIZATION_CODE` an den involvierten sektoralen Identity Provider ~~[gemSpec_IDP_Sek#Kapitel: Detailinformationen zum App-App-Flow - Schritt 10]~~ und authentisiert sich dabei als Client der TLS Verbindung mit einem Zertifikat das über sein Entity Statement validierbar ist. 5. Der sektorale Identity Provider überprüft die Gültigkeit des `AUTHORIZATION_CODE` entsprechend [https://datatracker.ietf.org/doc/html/rfc7636#section-4.6] 6. Der sektorale Identity Provider antwortet dem Fachdienst als Relying Party der TI-Föderation nach erfolgreicher Überprüfung des `AUTHORIZATION_CODE` mit dem zugehörigen `ID_TOKEN`gemäß [gemSpec_IDP_Sek] ~~([gemSpec_IDP_Sek#Kapitel: Detailinformationen zum App-App-Flow - Schritt 11])~~.
Ergebnis	Der Nutzer ist authentifiziert und ~~der~~ demFachdienst als Relying Party der TI-Föderationwurde vom sektoralen IDP das `ID_TOKEN` zugestellt ~~hat den `ID_TOKEN` mit dem es den `ACCESS_TOKEN` zum Zugriff auf die Fachdienst API abrufen kann~~.
Akzeptanzkriterien	ML-133236 - AF_10118 - ID_TOKEN erhalten, ~~ML-133237 - AF_10118 - ID_TOKEN entspricht Vorgaben~~

Alt:

ML-133236 - AF_10118 - ID_TOKEN erhalten
Der Fachdienste als Relying Party der TI-Föderation hat einen ID_TOKEN vom sektoralen Identity Provider erhalten.

Neu:

ML-133236 - AF_10118 - ID_TOKEN erhalten
Der Fachdienste als Relying Party der TI-Föderation hat einen `ID_TOKEN` vom sektoralen Identity Provider erhalten. Das erhaltene `ID_TOKEN` entspricht den Vorgaben [gemSpec_IDP_Sek].

~~**ML-133237 - AF_10118 - ID_TOKEN entspricht Vorgaben**~~

~~Der erhaltene ID_TOKEN entspricht den Vorgaben in [gemSpec_IDP_Sek] Tabellen: "Header-Claims des ID_TOKEN des sektoralen IDP", "Signature Header-Claims des ID_TOKEN des sektoralen IDP" und "Body-Claims für den ID_TOKEN des sektoralen IDP".~~

Es wird in Kapitel "3.4 Entity Statements" geändert

redaktionell - die Formatangabe für "kid" entfällt, dafür gibt es eine entsprechende Afo A_28208-01

Alt:

A_23034-02 - Entity Statement veröffentlichen

Ein Fachdienst als Relying Party der TI-Föderation MUSS seine Entity Configuration in einem selbst-signierten Entity Statement gemäß [OpenID Federation 1.1] ("Entity Statement") bereitstellen und im Internet verfügbar machen. Die Entity Configuration MUSS mindestens die in der folgenden Tabelle aufgeführten Metadaten enthalten:

Tabelle 19: *Header des Entity Statement der Relying Party der TI-Föderation*

Name	Werte / Wertebereich
`alg`	string, zulässiger Wert: "ES256"
`kid`	string, UUID7-Format [RFC9562#name-uuid-version-7]
`typ`	string, zulässiger Wert: "entity-statement+jwt"

...

Neu:

A_23034-03 - Entity Statement veröffentlichen

Ein Fachdienst als Relying Party der TI-Föderation MUSS seine Entity Configuration in einem selbst-signierten Entity Statement gemäß [OpenID Federation 1.1] ("Entity Statement") bereitstellen und im Internet verfügbar machen. Die Entity Configuration MUSS mindestens die in der folgenden Tabelle aufgeführten Metadaten enthalten:

Tabelle 20: *Header des Entity Statement der Relying Party der TI-Föderation*

Name	Werte / Wertebereich
`alg`	string, zulässiger Wert: "ES256"
`kid`	string, ~~UUID7-Format [RFC9562#name-uuid-version-7]~~
`typ`	string, zulässiger Wert: "entity-statement+jwt"

...

Es wird in Kapitel "4 Anbindung eines Fachdienste als OAuth-Resources in die TI-Föderation" geändert

redaktionell - die Formatangabe für "kid" entfällt, dafür gibt es eine entsprechende Afo A_28208-01

Alt:

A_28911 - Entity Statement eines TI-Fachdienstes als Proteced Resource

TI-Fachdienste, die sich als Proteced Resource in der TI-Föderation registrieren, MÜSSEN ein selbst-signiertes Entity Statement gemäß[OpenID Federation 1.1] ("Entity Statement") bereitstellen und im Internet verfügbar machen. Das Entity Statement MUSS mindestens die in der folgenden Tabelle aufgeführten Metadaten enthalten:

Tabelle 21: Header des Entity Statement des TI-Fachdienstes als Proteced Resource

Name	Werte / Wertebereich
`alg`	string, zulässiger Wert "ES256"
`kid`	string, UUID7-Format [RFC9562#name-uuid-version-7]
`typ`	string, zulässiger Wert "entity-statement+jwt"

...

Neu:

A_28911-01 - Entity Statement eines TI-Fachdienstes als Proteced Resource

TI-Fachdienste, die sich als Proteced Resource in der TI-Föderation registrieren, MÜSSEN ein selbst-signiertes Entity Statement gemäß[OpenID Federation 1.1] ("Entity Statement") bereitstellen und im Internet verfügbar machen. Das Entity Statement MUSS mindestens die in der folgenden Tabelle aufgeführten Metadaten enthalten:

Tabelle 22: Header des Entity Statement des TI-Fachdienstes als Proteced Resource

Name	Werte / Wertebereich
`alg`	string, zulässiger Wert "ES256"
`kid`	string, ~~UUID7-Format [RFC9562#name-uuid-version-7]~~
`typ`	string, zulässiger Wert "entity-statement+jwt"

...

5 Änderungen in Steckbriefen

5.1 Änderungen in gemProdT_IDP_FedMaster_PTV

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

Tabelle 23: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~AF_10101-02~~	Bereitstellung von Informationen zu Teilnehmern der Föderation (Subordinate Statement)	gemSpec_IDP_FedMaster
AF_10101-03	Bereitstellung von Informationen zu Teilnehmern der Föderation (Subordinate Statement)	gemSpec_IDP_FedMaster
~~AF_10100-02~~	Bereitstellung Liste registrierter Identity Provider	gemSpec_IDP_FedMaster
AF_10100-03	Bereitstellung Liste registrierter Identity Provider	gemSpec_IDP_FedMaster
~~A_22607-01~~	Entity Configuration Inhalte des Federation Master oder Intermediate	gemSpec_IDP_FedMaster
A_22607-02	Entity Configuration Inhalte des Federation Master oder Intermediate	gemSpec_IDP_FedMaster

5.2 Änderungen in gemAnbT_IDP_FedMaster_ATV

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

Tabelle 24: Anforderungen zur Sich.techn. Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_28208-01	Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FedMaster

Tabelle 25: Anforderungen zur organ./betriebl. Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_28208-01	A_28208-01 - Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FedMaster

5.3 Änderungen in gemProdT_IDP-Sek_PTV

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

Tabelle 26: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_22643-02~~	Entity Statement des sektoralen IDP	gemSpec_IDP_Sek
A_22643-03	Entity Statement des sektoralen IDP	gemSpec_IDP_Sek
~~A_22651~~	Parameter des Pushed Authorization Request durch den sektoralen IDP	gemSpec_IDP_Sek
A_22651-01	Parameter des Pushed Authorization Request durch den sektoralen IDP	gemSpec_IDP_Sek
~~A_24748-01~~	SSO-Unterstützung auf Anwendungsebene innerhalb einer APP	gemSpec_IDP_Sek
A_24748-02	SSO-Unterstützung auf Anwendungsebene innerhalb einer APP	gemSpec_IDP_Sek

Tabelle 27: Anforderungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_27591~~	Signalisierung der Einwilligung durch den Nutzer in "gematik-ehealth-loa-substantial" beim Zugriff auf Daten mit hohem Schutzbedarf	gemSpec_IDP_Sek
A_27591-01	Signalisierung der Einwilligung durch den Nutzer in "gematik-ehealth-loa-substantial" beim Zugriff auf Daten mit hohem Schutzbedarf	gemSpec_IDP_Sek

Tabelle 28: Anforderungen zur sicherheitstechnische Eignung "Produktgutachten"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)

~~A_23129-06~~	Identifikation des Authentisierungsverfahren	gemSpec_IDP_Sek
A_23129-07	Identifikation des Authentisierungsverfahren	gemSpec_IDP_Sek

5.4 Änderungen in gemAnbT_IDP-Sek_KTR_ATV

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

Tabelle 29: Anforderungen zur sicherheittechnische Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_28208-01	Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FedMaster
~~A_28195~~	A_28195 - Anbieter sektoraler IDP - Schlüssel-Identifier im JWK-Format	gemSpec_IDP_Sek
~~A_23006~~	Subdomäne für Webservice-Endpunkte in der VAU	gemSpec_IDP_Sek

Tabelle 30: Anforderungen zur organ./betriebl. Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_28208-01	Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FedMaster
~~A_28195~~	A_28195 - Anbieter sektoraler IDP - Schlüssel-Identifier im JWK-Format	gemSpec_IDP_Sek
A_28886	Verbot von wildcard-Namenseinträgen für TLS-terminierte VAU Endpunkte	gemSpec_Krypt
A_28866	Auswahl der Domain für TLS-terminierte Vertrauenswürdige Ausführungsumgebungen (VAU)	gemSpec_Krypt

Tabelle 31: Anforderungen zur sicherheittechnische Eignung "Gutachten (Anbieter)"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_23023~~	Sicherung externen Schnittstellen gegen bösartige Eingaben	gemSpec_IDP_Sek
A_23023-01	Sicherung externen Schnittstellen gegen bösartige Eingaben	gemSpec_IDP_Sek

5.5 Änderungen in gemAnbT_IDP-Dienst

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

Tabelle 32: Anforderungen zur Sich.techn. Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_28208~~	Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FD
A_28208-01	Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FedMaster

Tabelle 33: Anforderungen zur organ./betriebl. Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_28208~~	A_28208 - Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FD
A_28208-01	A_28208-01 - Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FedMaster

5.6 Änderungen in gemProdT_SigD

Tabelle 34: Anforderungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_27593	Akzeptanz der Einwilligung zur Authentisierung auf "gematik-ehealth-loa-substantial" beim Zugriff auf Daten mit hohem Schutzbedarf	gemSpec_IDP_FD

Tabelle 35: Anforderungen zur sicherheitstechnische Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_23202-02	Akzeptanz der Einwilligung zur Verwendung von Authentisierungsverfahren "gematik-ehealth-loa-substantial" beim Zugriff auf Daten mit hohem Schutzbedarf (befristet)	gemSpec_IDP_FD

5.7 Änderungen in gemAnbT_Aktensystem_ePA

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

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

Tabelle 36: Anforderungen zur Sich.techn. Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_28208~~	Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FD
A_28208-01	Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FedMaster

Tabelle 37: Anforderungen zur organ./betriebl. Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_28208~~	A_28208 - Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FD
A_28208-01	A_28208-01 - Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FedMaster

5.8 Änderungen in gemProdT_Aktensystem_ePA

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

Tabelle 38: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~AF_10116~~	Bereitstellung Liste registrierte Identity Provider	gemSpec_IDP_FD

5.9 Änderungen in gemAnbT_PoPP_Service

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

Tabelle 39: Anforderungen zur Sich.techn. Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)

~~A_28208~~	Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FD
A_28208-01	Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FedMaster

Tabelle 40: Anforderungen zur organ./betriebl. Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_28208~~	A_28208 - Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FD
A_28208-01	A_28208-01 - Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FedMaster

5.10 Änderungen in gemAnw_DiGA

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

Tabelle 41: Anforderungen zur Sich.techn. Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_28208~~	Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FD
A_28208-01	Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FedMaster

Tabelle 42: Anforderungen zur organ./betriebl. Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_28208~~	A_28208 - Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FD
A_28208-01	A_28208-01 - Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FedMaster

5.11 Änderungen in gemAnw_OGR

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

Tabelle 43: Anforderungen zur Sich.techn. Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)

~~A_28208~~	Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FD
A_28208-01	Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FedMaster

Tabelle 44: Anforderungen zur organ./betriebl. Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_28208~~	A_28208 - Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FD
A_28208-01	A_28208-01 - Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FedMaster

Tabelle 45: Anforderungen zur Sich.techn. Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_28208~~	Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FD
A_28208-01	Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FedMaster

Tabelle 46: Anforderungen zur organ./betriebl. Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_28208~~	A_28208 - Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FD
A_28208-01	A_28208-01 - Schlüssel-Identifier im JWK-Format	gemSpec_IDP_FedMaster