

---

## C\_12598\_Anlage\_IDP\_FD

---

# Inhaltsverzeichnis

<b>1</b>	<b>Änderungsbeschreibung.....</b>	<b>2</b>
<b>2</b>	<b>Änderung in gemSpec_IDP_FD.....</b>	<b>3</b>
2.1	Es wird Kapitel "2 Systemüberblick" wie folgt angepasst:.....	3
2.2	Es wird Kapitel "3 Systemkontext" wie folgt angepasst:.....	3
2.3	Es wird Kapitel "3.1 Akteure und Rollen" wie folgt angepasst:.....	3
2.4	Es wird Kapitel "4.1 Registrierung des Fachdienstes beim Federation Master" wie folgt angepasst:.....	3
2.5	Es wird Kapitel "4.2 Übergreifende Festlegungen" wie folgt angepasst:...	4
2.6	Es wird Kapitel "4.3 Entity Configuration und Entity Statements" wie folgt angepasst:.....	5
2.7	Es wird neues Kapitel "5 Anbindung eines Fachdienstes als OAuth-Resources in die TI-Föderation", Bisheriges Kapitel 5 wird Kapitel 6, Bisheriges Kapitel 6 wird Kapitel 7.....	15
<b>3</b>	<b>Änderung in gemSpec_PoPP_Service.....</b>	<b>17</b>
<b>4</b>	<b>Änderungen in Steckbriefen.....</b>	<b>18</b>
4.1	Änderungen in gemAnw_DiGA, digi_ID_OGR,.....	18
4.2	Änderungen in gemAnbT_Aktensystem_ePA.....	19
4.3	Änderungen in gemProdT_Aktensystem_ePA.....	19
4.4	Änderungen in gemAnbT_IDP-Dienst.....	20
4.5	Änderungen in gemProdT_IDP-Dienst.....	21

---

## 1 Änderungsbeschreibung

---

Die Spezifikationen gemSpec\_IDP\_Sek, gemSpec\_IDP\_FedMaster, gemSpec\_IDP\_FD setzen auf den Standard OpenID-Federation 1.0 - Draft 21 ([https://openid.net/specs/openid-connect-federation-1\\_0-21.html](https://openid.net/specs/openid-connect-federation-1_0-21.html)) auf. Der Standard hat sich weiterentwickelt und ist seit 02/2026 final ([https://openid.net/specs/openid-federation-1\\_0.html](https://openid.net/specs/openid-federation-1_0.html)). Der OpenID Federation Standard wird dahin gehend weiter entwickelt, dass

- "OpenID Federation 1.1" alle Technologie unabhängigen Aspekte enthält ([https://openid.net/specs/openid-federation-1\\_1.html](https://openid.net/specs/openid-federation-1_1.html))
- "OpenID Federation for OpenID Connect 1.1" aufsetzend auf "OpenID Federation 1.1" alle Aspekte für OIDC Architekturen enthält ([https://openid.net/specs/openid-federation-connect-1\\_1.html](https://openid.net/specs/openid-federation-connect-1_1.html))
- "OpenID Federation for Wallet Architectures 1.0" aufsetzend auf "OpenID Federation 1.1" alle Aspekte für Wallet Architekturen enthält ([https://openid.net/specs/openid-federation-wallet-1\\_0.html](https://openid.net/specs/openid-federation-wallet-1_0.html))

Es ist zwingend notwendig, die Spezifikationen an den aktuellen Standard anzupassen, da sich wesentliche Bestandteile geändert haben.

Im Zuge dessen werden alle grundlegenden Informationen zur TI-Föderation in ein eigenes Dokument gemKPT\_TI-Föderation ausgelagert, die eigentlichen Spezifikationen werden um die allgemeinen Informationen bereinigt. Damit wird gesichert, dass der allgemeine Blick nicht widersprüchlich in den den Spezifikation sondern zentral in einem Dokument gepflegt und weiterentwickelt werden.

Die Anlage enthält alle geplanten Anpassungen in gemSpec\_IDP\_FD.

---

## 2 Änderung in gemSpec\_IDP\_FD

---

### 2.1 Es wird Kapitel "2 Systemüberblick" wie folgt angepasst:

- Text und Abbildung werden entfernt, es wird auf gemKPT\_TI-Föderation verwiesen. Aufbau und Funktionsweise der TI-Föderation ist in [gemKPT\_TI-Föderation] dargestellt und beschrieben.

### 2.2 Es wird Kapitel "3 Systemkontext" wie folgt angepasst:

- Kapitel wird entfernt, es wird auf gemKPT\_TI-Föderation verwiesen.

### 2.3 Es wird Kapitel "3.1 Akteure und Rollen" wie folgt angepasst:

- Kapitel wird entfernt, es wird auf gemKPT\_TI-Föderation verwiesen.

### 2.4 Es wird Kapitel "4.1 Registrierung des Fachdienstes beim Federation Master" wie folgt angepasst:

- Textuelle Beschreibung verallgemeinern auf Superior Entities (Federation Master/Intermediates)

Fachdienstbetreiber müssen ihren Authorization Server bei einer Superior Entity der TI-Föderation (beim Federation Master oder Intermediate) registrieren. Die Registrierung erfolgt als organisatorischer Prozess, bevor ein Fachdienst Authorization Server 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 Scope und Claims angegeben wurden, können sektorale Identity Provider ID\_TOKEN für den Fachdienst Authorization Server ausstellen.

#### Alt:

#### **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 Scope bzw. Claims beschreiben und dem Federation Master zur Verfügung stellen. Die Registrierung MUSS ebenso die absolute URI des Fachdienstes im Internetumfassen (seine Client-ID) sowie dessen Signaturschlüssel für das Entity\_Statement.

[<=, Anw\_DiGA, extNutz\_GID, Anb\_IDP-D, digi\_ID\_OGR, Anb\_Aktensystem\_ePA, organ./betriebl. Eignung: Anbietererklärung]

**A\_23046 -öffentlicher Schlüssel des Federation Master**

Anbieter von Fachdiensten MÜSSEN den öffentlichen Signaturschlüssel des Federation Master durch einen sicheren Registrierungsprozess im Authorization-Server einbringen und initial zur Signaturprüfung verwenden. [≤, Anw\_DiGA, extNutz\_GID, Anb\_IDP-D, digi\_ID\_OGR, Anb\_Aktensystem\_ePA, Sich.techn. Eignung: Anbietererklärung, organ./betriebl. Eignung: Anbietererklärung]

**A\_23045-02, A\_23046 entfallen durch die Zuordnung von A\_28879 zum Fachdienst Authorization Server**

Neu: Zuweisung A\_28879

**A\_28879 -Registrierung von Teilnehmern in der TI-Föderation durch organisatorischen Prozess**

Ein Teilnehmer der TI-Föderation MUSS seinen öffentlichen Schlüssel für die Signatur des selbst-signierten Entity Statement (federation entity signing key) über einen organisatorischen Prozess bei der Superior Entity (Federation Master oder Intermediate) bekannt machen, bei welcher der Teilnehmer als Subordinate Entity registriert werden soll. Nach erfolgreicher Registrierung wird dem Teilnehmer der öffentliche Schlüssel übermittelt, mit dem das Entity Statement des Federation Master signiert ist (federation entity signing key). Der Teilnehmer MUSS diesen Schlüssel speichern und zur Validierung einer Vertrauenskette gemäß A\_28848\* verwenden. [≤, Anw\_DiGA, extNutz\_GID, Anb\_IDP-D, Anb\_IDP-Sek\_KTR, digi\_ID\_OGR, Anb\_Aktensystem\_ePA, Anb\_IDP\_FedMaster, organ./betriebl. Eignung: Anbietererklärung]

**2.5 Es wird Kapitel "4.2 Übergreifende Festlegungen" wie folgt angepasst:**

- Textuelle Beschreibung verallgemeinern auf Superior Entities (Federation Master/Intermediates)

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 im Verlauf des Registrierungsprozesses in der TI-Föderation geprüft und abgestimmt. ~~(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.html#IDToken](#)]) erwarten Fachdienste in der Regel weitere Informationen, wie zum Beispiel Vorname, Name, Rolle und KVR des Nutzers. Siehe hierzu auch [gemSpec\_IDP\_Sek#Kapitel: Token-Endpunkt Ausgangsdaten].

**redaktionell**

Alt:

**A\_23004 -Anforderung eines Vertrauensniveaus**

Fachdienste MÜSSEN eine Authentisierung auf dem für den Zugriff auf ihre Fachdaten notwendigen Vertrauensniveau im Parameteracr\_values des Pushed Authorization-Request anfragen oder, wenn nur ein Wert infrage kommt diesen im Felddefault\_acr\_values ihres Entity Statements nennen. [≤, Aktensystem\_ePA, Anw\_DiGA, TI-M\_FD\_ePA, extNutz\_GID, IDP-D, digi\_ID\_OGR, funkt. Eignung: Herstellererklärung, funkt. Eignung: Anbietererklärung, funkt. Eignung: Test Produkt/FA]

Neu:

#### **A\_23004-01 -Anforderung eines Vertrauensniveaus**

Fachdienste **Authorization Server** MÜSSEN eine Authentisierung auf dem für den Zugriff auf ihre Fachdaten notwendigen Vertrauensniveau im Parameteracr\_values des Pushed Authorization-Request anfragen oder, wenn nur ein Wert infrage kommt diesen im Felddefault\_acr\_values ihrer Entity **Configuration Statements** nennen. [≤, Aktensystem\_ePA, Anw\_DiGA, TI-M\_FD\_ePA, extNutz\_GID, IDP-D, digi\_ID\_OGR, funkt. Eignung: Herstellererklärung, funkt. Eignung: Anbietererklärung, funkt. Eignung: Test Produkt/FA]

## **2.6 Es wird Kapitel "4.3 Entity Configuration und Entity Statements" wie folgt angepasst:**

Alt:

#### **A\_23034-01 -Entity Statement veröffentlichen**

Authorization Server MÜSSEN unter „well-known/openid-federation“ ein über sich Auskunft gebendes, mit ES256 signiertes Entity Statement gemäß [OpenID Federation 1.0#name-obtaining-federation-entity] veröffentlichen. Dieses Entity Statement muss die Metadaten openid\_relying\_party und federation\_entity als Relying Party der TI-Föderation enthalten. Das Entity Statement ist maximal 24 Stunden gültig. Es MUSS mindestens die in der folgenden Tabelle aufgeführten Metadaten enthalten:

**Tabelle 1: Header des Entity Statement des Fachdienstes**

Name	Werte / Wertebereich
alg	string, zulässiger Wert: "ES256"
kid	string Es wird empfohlen, den JWK Thumbprint gemäß [RFC7638] als kid zu verwenden.
typ	string zulässiger Wert: "entity-statement+jwt"

**Tabelle 2 :Allgemeine Attribute im well-known-Dokument des Authorization Server des Fachdienstes**

Name	Werte / Wertebereich
------	----------------------

iss	string, URL nach [ <a href="#">RFC1738</a> ]
sub	string, URL nach [ <a href="#">RFC1738</a> ]
iat	number, Alle time-Werte in Sekunden seit 1970,[ <a href="#">RFC7519#section-2</a> ]
exp	number, Alle time-Werte in Sekunden seit 1970,[ <a href="#">RFC7519#section-2</a> ]
jwks	Set von JWK [ <a href="#">RFC7517</a> ]
authority_hints	[string] zulässiger Wert: iss aus dem Entity Statement des Federation Master
metadata	string, zulässiger Wert: "openid_relying_party"

159  
160

**Tabelle 3 :Attribute des Metadatenblocks openid\_relying\_party im well-known-Dokument des Authorization Server des Fachdienstes**

Name	Werte
signed_jwks_uri (*)	string, URL nach <a href="#">[RFC1738]</a>
jwks (*)	Set von JWK <a href="#">[RFC7517]</a>
client_name	string, Wertebereich: ^[ÄÖÜäöüß\w\ \-\.\&\+\\*\V/]{1,128}\$
redirect_uris	[string], Wertebereich: Bei der Registrierung des Fachdienstes hinterlegte redirect_uris
response_types	[string] zulässiger Wert: "code"
client_registration_types	[string] zulässiger Wert: "automatic"
grant_types	[string] zulässiger Wert: "authorization_code"
require_pushed_authorization_requests	boolean zulässiger Wert: true
token_endpoint_auth_method	string, zulässiger Wert: "self_signed_tls_client_auth"
default_acr_values	[string] zulässiger Wertebereich: "gematik-ehealth-loa-high", "gematik- ehealth-loa-substantial"
id_token_signed_response_alg	string, zulässiger Wert: "ES256"
id_token_encrypted_response_alg	string, zulässiger Wert: "ECDH-ES"
id_token_encrypted_response_enc	string, zulässiger Wert: "A256GCM"
scope	string
ti_features_supported {	
id_token_version_supported	[string] zulässige Werte in Liste:



	"1.0.0", "2.0.0"
--	------------------

(\*) - gemäß [OpenID Federation 1.0] darf der Metadatenblock nur  
entweder `signed_jwks_uri` oder `jwks` enthalten.

**Tabelle 4 :Attribute des Metadatenblocks `federation_entity` im well-known-Dokument des Fachdienstes Authorization Server**

Name	Werte / Wertebereich
organization_name	String (max. 128 Zeichen) Wertebereich: <code>^[ÄÖÜäöüß\w\ \-\.\&amp;\+\\*\V]{1,128}\$</code>

[<=, Aktensystem\_ePA, Anw\_DiGA, TI-M\_FD\_ePA, extNutz\_GID, IDP-D, digi\_ID\_OGR, funkt. Eignung: Herstellererklärung, funkt. Eignung: Anbietererklärung, funkt. Eignung: Test Produkt/FA]

## Implementierung

Neu:

### A 23034-02 -Entity Statement veröffentlichen

Ein Fachdienst Authorization Server 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 Statement MUSS mindestens die in der folgenden Tabelle aufgeführten Metadaten enthalten:

**Tabelle 5: Header des Entity Statement des Fachdienstes Authorization Server**

Name	Werte / Wertebereich
alg	string, zulässiger Wert: "ES256"
kid	string, UUID7-Format [RFC9562#name-uuid-version-7] Es wird empfohlen, den JWK Thumbprint gemäß [RFC7638] als kid zu verwenden.
typ	string, zulässiger Wert: "entity-statement+jwt"

**Tabelle 6 :Allgemeine Attribute der Entity Configuration im .well-known-Dokument des Authorization Server des Fachdienstes**

Name	Werte / Wertebereich
iss	string, URL nach [RFC1738]

sub	string, URL nach <a href="#">RFC1738</a>
iat	number, Alle time-Werte in Sekunden seit 1970, <a href="#">[RFC7519#section-2]</a>
exp	number, Alle time-Werte in Sekunden seit 1970, <a href="#">[RFC7519#section-2]</a>
jwks	Set von JWK <a href="#">[RFC7517]</a> , zulässige Werte sind, gemäß <a href="#">[OpenID Federation "Claims that MUST or MAY Appear in both Entity Configurations and Subordinate Statements"]</a> - jwks, nur die öffentlichen Schlüssel zu Schlüsseln, mit den das Entity Statement signiert ist.
authority_hints	[string], zulässige Werte gemäß <a href="#">[OpenID Federation "Claims that MUST or MAY Appear in Entity Configurations but Not in Subordinate Statements"]</a> - authority_hints
trust_marks	[JSON Object], Optional, wenn Trust Marks für die Relying Party ausgestellt wurden, werden sie hier propagiert. zulässige Werte gemäß <a href="#">[OpenID Federation "Claims that MUST or MAY Appear in Entity Configurations but Not in Subordinate Statements"]</a> - trust_marks
metadata	JSON Object, erforderlicher Wert: "openid_relying_party"

183  
184

**Tabelle 7 :Attribute des Metadatenblocks openid\_relying\_partyder Entity Configuration im .well-known-Dokument des Authorization Server des Fachdienstes**

Name	Werte
signed_jwks_uri (*)	string, URL nach <a href="#">[RFC1738]</a>
jwks (*)	Set von JWK <a href="#">[RFC7517]</a>
client_name	string, Wertebereich: <code>^[a-zA-Üßw\ \-\. \&amp; \+ \*V]{1,128}\$</code>
organization_name	string (gemäß <a href="#">[OpenID-Federation "Informational Metadata Extensions"]</a> - organization_name) Wertebereich: <code>^[a-zA-Üßw\ \-\. \+ \*V]{1,128}\$</code>
display_name	string (gemäß <a href="#">[OpenID-Federation "Informational Metadata Extensions"]</a> - display_name) Wertebereich: <code>^[a-zA-Üßw\ \-\. \+ \*V]{1,128}\$</code>
keywords	<a href="#">[string]</a> (gemäß <a href="#">[OpenID-Federation "Informational Metadata Extensions"]</a> - keywords) erforderliche Werte: "product_type_version:<von der gematik zugelassene Produkttyp-Version>" "product_type:<von der gematik zugelassener Produkttyp>"
contacts	<a href="#">[string]</a> (gemäß <a href="#">[OpenID-Federation "Informational Metadata Extensions"]</a> - contacts) erforderlicher Wert: "<E-Mail-Adresse für Supportanfragen>"
redirect_uris	<a href="#">[string]</a> , Wertebereich: Bei der Registrierung des Fachdienstes hinterlegte redirect_uris
response_types	<a href="#">[string]</a> , zulässiger Wert: "code"
client_registration_types	<a href="#">[string]</a> , zulässiger Wert: "automatic"
grant_types	<a href="#">[string]</a> ,

	zulässiger Wert: "authorization_code"
require_pushed_authorization_requests	boolean, zulässiger Wert: true
token_endpoint_auth_method	string, zulässiger Wert: "self_signed_tls_client_auth"
default_acr_values	[string], zulässiger Wertebereich: "gematik-ehealth-loa-high", " <del>gematik-ehealth-loa-substantial</del> "
id_token_signed_response_alg	string, zulässiger Wert: "ES256"
id_token_encrypted_response_alg	string, zulässiger Wert: "ECDH-ES"
id_token_encrypted_response_enc	string, zulässiger Wert: "A256GCM"
scope	string
<i>ti_features_supported</i> {	
id_token_version_supported	[string] zulässige Werte in Liste: "1.0.0", "2.0.0"
}	

(\*) - gemäß [OpenID Federation 1.1] darf der Metadatenblock nur  
entweder signed\_jwks\_uri oder jwks enthalten.

[<=, Aktensystem\_ePA, Anw\_DiGA, TI-M\_FD\_ePA, extNutz\_GID, IDP-D, digi\_ID\_OGR, funkt.  
Eignung: Herstellererklärung, funkt. Eignung: Anbietererklärung, funkt. Eignung: Test  
Produkt/FA]

Alt:

#### **A\_27504 - Informationspflicht bei Änderungen der benötigten Werte "scope" und "redirect\_uris"**

Anbieter von Fachdiensten DÜRFEN die Claimsredirect\_uris und scope in ihrem Entity Statement NICHT verändern, bevor diese über den von der gematik kommunizierten organisatorischen Prozess dem Federation Master bekannt gegeben wurden. Erst nach positiver Rückmeldung dürfen diese gemeldeten Veränderungen im Entity Statement des Fachdienstes veröffentlicht werden. [<=, Aktensystem\_ePA, Anw\_DiGA, TI-M\_FD\_ePA, extNutz\_GID, IDP-D, digi\_ID\_OGR, funkt. Eignung: Herstellererklärung, funkt. Eignung: Anbietererklärung]

Neu:

**A\_27504-01 -Informationspflicht bei Änderungen der benötigten Werte "scope" und "redirect\_uris"**

Anbieter von Fachdiensten ~~ten~~Authorization Servern DÜRFEN die Claimsredirect\_uris und scope in ihrer Entity Configuration Statement NICHT verändern, bevor diese über den von der gematik kommunizierten organisatorischen Prozess dem direkt übergeordneten Superior (Federation Master oder Intermediate) bekannt gegeben wurden. Erst nach positiver Rückmeldung dürfen diese gemeldeten Veränderungen in der Entity Configuration im Entity Statement des Fachdienstes veröffentlicht werden.

Die Änderung der Client-ID in der Entity Configuration (iss) ist generell unzulässig.

*Hinweis: Soll z.B. bedingt durch einen Domänenwechsel die iss-URL geändert werden, so ist eine Deregistrierung des alten und die Neuregistrierung des neuen Clients in der TI-Föderation erforderlich. [≤, Aktensystem\_ePA, Anw\_DiGA, TI-M\_FD\_ePA, extNutz\_GID, IDP-D, digi\_ID\_OGR, funkt. Eignung: Herstellererklärung, funkt. Eignung: Anbietererklärung]*

**A\_24607 entfällt nach Abstimmung mit SI, Key-Rollver erfolgt automatisiert nach A\_28859**

Alt:

**A\_24607 -Schlüsselwechsel Signaturschlüssel für Entity Statement**

Anbieter von Fachdiensten MÜSSEN im Rahmen eines geplanten Schlüsselwechsels der Signaturschlüssel, mit dem der Fachdienst sein Entity Statement signiert, den öffentlichen Signaturschlüssel mindestens 24 Stunden vor der Verwendung über einen organisatorischen Prozess beim Federation Master hinterlegen.

[≤, Anb\_Aktensystem\_ePA, organ./betriebl. Eignung: Anbietererklärung]

Neu: Zuweisung A\_28859

**A\_28859 -Vorlaufzeit bei geplantem Schlüsselwechsel Signaturschlüssel für Entity Statements**

Im Rahmen eines geplanten Schlüsselwechsels der Signaturschlüssel MÜSSEN Teilnehmer der TI-Föderation den neuen öffentlichen Signaturschlüssel mindestens 24 Stunden vor der Verwendung im jwks-Schlüsselsatz im Entity Statement zusätzlich zum aktuell gültigen Signaturschlüssel veröffentlichen. Dieser Signaturschlüssel ist der neue Schlüssel, mit dem der Teilnehmer sein Entity Statement (federation entity signing key) frühestens 24 Stunden nach dieser Veröffentlichung signiert. Der Schlüsselwechsel sollte entsprechend [[OpenID Federation 1.1](#)] ("Updating Metadata, Key Rollover, and Revocation") erfolgen.

*Hinweis:* Nicht betroffen von dieser Anforderung sind kurzfristig notwendige Schlüsselwechsel, z. B. aufgrund von Sicherheitsvorfällen. Diese Maßnahmen sind beispielsweise über Security Incidents abzuwickeln. Die Bearbeitung solcher kurzfristigen Schlüsselwechsel muss die Aktualisierung beim Federation Master bzw. Intermediate mit berücksichtigen, da es ansonsten zu Verarbeitungsfehlern wegen ungültiger Schlüssel kommen kann. [≤, Anw\_DiGA, Anb\_IDP-D, Anb\_IDP-Sek\_KTR, digi\_ID\_OGR, Anb\_Aktensystem\_ePA, Anb\_IDP\_FedMaster, organ./betriebl. Eignung: Anbietererklärung]

Alt:

#### A\_23038 -Entity Statement abrufen

Authorization-Server MÜSSEN benötigte Schlüssel und Endpunkte des Federation Master und verwendeter sektoraler Identity Provider durch Abfrage ihrer Entity Statements entsprechend [gemSpec\_IDP\_FedMaster]#AF\_10101 einholen. [≤, Aktensystem\_ePA, Anw\_DiGA, extNutz\_GID, IDP-D, digi\_ID\_OGR, funkt. Eignung: Herstellererklärung, funkt. Eignung: Anbietererklärung]

#### A\_23039 -Entity Statement vorhalten

Authorization-Server KÖNNEN einmal heruntergeladene fremde Entity Statements zwischenspeichern. Diese SOLLEN nach 12 Stunden erneut heruntergeladen werden und MÜSSEN nach maximal 24 Stunden verworfen werden. [≤, Aktensystem\_ePA, Anw\_DiGA, extNutz\_GID, IDP-D, digi\_ID\_OGR, funkt. Eignung: Herstellererklärung, organ./betriebl. Eignung: Anbietererklärung, funkt. Eignung: Anbietererklärung]

#### A\_23040 -Fachdienst: Prüfung der Signatur des Entity Statements

Authorization-Server MÜSSEN die Signatur der heruntergeladenen Entity Statement prüfen und auf einen zeitlich gültigen Signaturschlüssel zurückführen, welcher von dem ihm bekannten Federation Master oder von einem durch den Federation Master beglaubigten sektoralen Identity Provider ausgestellt sein MUSS. Vor der weiteren Verwendung MUSS die Prüfung der Entity Statements erfolgreich abgeschlossen sein. [≤, Aktensystem\_ePA, Anw\_DiGA, extNutz\_GID, IDP-D, digi\_ID\_OGR, Sich.techn. Eignung: Anbietererklärung, Sich.techn. Eignung: Produktgutachten]

**A\_23038, A\_23039, A\_23040 entfallen durch die Zuordnung von A\_28848 zum Fachdienst Authorization Server**

### Implementierung

Neu:Zuweisung - A\_28848

#### A\_28848 -Validierung der Vertrauensketten eines TI-Föderation-Teilnehmers

Teilnehmer der TI-Föderation, welche mit anderen Teilnehmern der TI-Föderation kommunizieren wollen, MÜSSEN das Entity Statement des anderen TI-Föderation-Teilnehmers abrufen und gemäß der Regeln [[OpenID Federation 1.1](#)] ("Entity Statement Validation") validieren, sowie die Vertrauenskette gemäß [[OpenID Federation 1.1](#)] ("Resolving the Trust Chain and Metadata") prüfen. Der Abruf des Entity Statement sollte alle 12h und MUSS innerhalb von 24h erfolgen. [≤, Aktensystem\_ePA, Anw\_DiGA, TI-M\_FD\_ePA, extNutz\_GID, IDP-D, digi\_ID\_OGR, IDP-Sek, IDP\_FedMaster, Sich.techn. Eignung: Anbietererklärung, Sich.techn. Eignung: Produktgutachten, Sich.techn. Eignung: Herstellererklärung]

Neu:Zuweisung - A\_29019

#### A\_29019 -Abruf eines Subordinate Statement abweichend von OpenID Federation 1.1 (befristet)

Der Abruf eines Subordinate Statement eines Teilnehmers zu einem anderen Teilnehmer bei dessen Superior Entity MUSS abweichend zu [[OpenID Federation 1.1](#)] ("Fetch Subordinate Statement Request") ein HTTP-GET Request mit folgenden Parametern an den federation\_fetch\_endpoint der Superior Entity sein:

**Tabelle 8: Teilnehmer Validierung Abfrage - Request-Parameter**

Attribut	Werte / Typ	Anmerkung
----------	-------------	-----------

iss	string, URL nach <a href="#">RFC1738</a>	Identifizier (iss) der Subordinate Entity (Federation Master oder Intermediate-Entity), bei welcher der Teilnehmer (sub) registriert ist.
sub	string, URL nach <a href="#">RFC1738</a>	Identifizier (iss) des angefragten Teilnehmers aus dessen Entity Statement

*Hinweis: Eine Umstellung auf den aktuellen Standard entsprechend [\[OpenID Federation 1.1\]](#) ("Fetch Subordinate Statement Request") kann erst erfolgen, wenn die API des Federation Master angepasst wurde. [≤, Aktensystem\_ePA, Anw\_DiGA, TI-M\_FD\_ePA, extNutz\_GID, IDP-D, digi\_ID\_OGR, IDP-Sek, IDP\_FedMaster, funkt. Eignung: Herstellererklärung, funkt. Eignung: Anbietererklärung]*

**A\_27989 entfällt, der Inhalt ist bereits in A\_27504-01 enthalten.**

Alt:

### **A\_27989 -Bekanntgabe von Änderungen im Entity Statement einer Relying Party der TI-Föderation**

Anbieter eines Authorization Server in der TI-Föderation MÜSSEN geplante Änderungen folgender claims im Entity Statement vor Veröffentlichung dem Federation Master über einen organisatorischen Prozess beantragen:

- Änderungen des Schlüsselsets, mit dem das Entity Statement signiert wird - jwks,
- Änderungen des in der TI-Föderation propagierten Organisationsnamens - federation\_entity.organization\_name,
- Änderungen des Namens der Anwendung - openid\_relying\_party.client\_name.

[≤, Anw\_DiGA, Anb\_IDP-D, Anb\_TI-M\_ePA, digi\_ID\_OGR, Anb\_Aktensystem\_ePA, extNutz\_TI-Dienste\_allg, organ./betriebl. Eignung: Anbietererklärung]

## **2.7 Es wird neues Kapitel "5 Anbindung eines Fachdienstes als OAuth-Resources in die TI-Föderation", Bisheriges Kapitel 5 wird Kapitel 6, Bisheriges Kapitel 6 wird Kapitel 7**

Die TI-Föderation bietet die Möglichkeit TI-Fachdienste in den Vertrauensraum der TI-Föderation zu integrieren. Die Fachdienste sind i.d.R. "Protected Resources", auf die nur berechnete Clients zugreifen dürfen. Die Registrierung in der TI-Föderation erfolgt als Entity-type "oauth\_resource" gemäß [\[OpenID Federation 1.1\]](#).

### **A\_28911 -Entity Statement eines TI-Fachdienstes als Protected Resource**

TI-Fachdienste, die sich als Protected 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 9: Header des Entity Statement des TI-Fachdienstes als Protected Resource**

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

**Tabelle 10 : Allgemeine Attribute im well-known-Dokument des TI-Fachdienstes als Protected Resource**

Name	Werte / Wertebereich
iss	string, URL nach [ <a href="#">RFC1738</a> ]
sub	string, URL nach [ <a href="#">RFC1738</a> ]
iat	number, Alle time-Werte in Sekunden seit 1970,[ <a href="#">RFC7519#section-2</a> ]
exp	number, Alle time-Werte in Sekunden seit 1970,[ <a href="#">RFC7519#section-2</a> ]
jwks	Set von JWK [ <a href="#">RFC7517</a> ] zulässige Werte sind, gemäß [ <a href="#">OpenID Federation "Claims that MUST or MAY Appear in both Entity Configurations and Subordinate Statements"</a> ] - jwks, nur die öffentlichen Schlüssel zu Schlüsseln, mit denen das Entity Statement signiert ist (federation entity signing key)
authority_hints	[string] zulässige Werte gemäß [ <a href="#">OpenID Federation "Claims that MUST or MAY Appear in Entity Configurations but Not in Subordinate Statements"</a> ] - authority_hints
metadata	JSON Object, erforderlicher Wert: "oauth_resource"

**Tabelle 11 : Attribute des Metadatenblocks oauth\_resource im well-known-Dokument des TI-Fachdienstes als Protected Resource**

Name	Werte
------	-------



signed_jwks_uri(*)	string, URL nach <a href="#">RFC1738</a>
organization_name	string (gemäß <a href="#">[OpenID-Federation "Informational Metadata Extensions" ]</a> - organization_name) Wertebereich: ^[à-üÀ-Üß\w\ \-\.+\\*V]{1,128}\$
display_name	string (gemäß <a href="#">[OpenID-Federation "Informational Metadata Extensions" ]</a> - display_name) Wertebereich: ^[à-üÀ-Üß\w\ \-\.+\\*V]{1,128}\$
keywords	[string] (gemäß <a href="#">[OpenID-Federation "Informational Metadata Extensions" ]</a> - keywords) erforderliche Werte: "product_type_version:<VERSION>" "product_type:<von der gematik zugelassener Produkttyp>"
contacts	[string] (gemäß <a href="#">[OpenID-Federation "Informational Metadata Extensions" ]</a> - contacts) erforderlicher Wert in Liste: "<E-Mail-Adresse für Supportanfragen>"

【<=, PoPP\_Service, funkt. Eignung: Herstellererklärung】

---

### 3 Änderung in gemSpec\_PoPP\_Service

---

- **A\_27294, A\_27295, A\_27296 entfallen durch die Zuordnung von A\_28911 zum PoPP-Service**
- **Zweisung A\_28848, A\_28857, A\_28879**

## 4 Änderungen in Steckbriefen

### 4.1 Änderungen in gemAnw\_DiGA, digi\_ID\_OGR,

**Tabelle 12: Anforderungen zur sicherheitstechnischen Eignung "Anbietererklärung"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_23040	Fachdienst: Prüfung der Signatur des Entity Statements	gemSpec_IDP_FD
A_28848	Validierung der Vertrauenskette eines TI-Föderation Teilnehmers	gemSpec_IDP_FedMaster

**Tabelle 13: Anforderungen zur funktionale Eignung "Anbietererklärung"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_23004	Anforderung eines Vertrauensniveaus	gemSpec_IDP_FD
A_23004-01	Anforderung eines Vertrauensniveaus	gemSpec_IDP_FD
A_23034-01	Entity Statement veröffentlichen	gemSpec_IDP_FD
A_23034-02	Entity Statement veröffentlichen	gemSpec_IDP_FD
A_23038	Entity Statement abrufen	gemSpec_IDP_FD
A_23039	Entity Statement vorhalten	gemSpec_IDP_FD
A_23046	öffentlicher Schlüssel des Federation Master	gemSpec_IDP_FD
A_27504	Informationspflicht bei Änderungen der benötigten Werte "scope" und "redirect_uris"	gemSpec_IDP_FD
A_27504-01	Informationspflicht bei Änderungen der benötigten Werte "scope" und "redirect_uris"	gemSpec_IDP_FD
A_28911	Entity Statement eines TI-Fachdienstes als Protected Resource	gemSpec_IDP_FD
A_29019	Abruf eines Subordinate Statements abweichend von OpenID Federation 1.1 (befristet)	gemSpec_IDP_FedMaster

**Tabelle 14: Anforderungen zur betriebliche Eignung "Anbietererklärung"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_23045-02	Registrierung des Fachdienstes	gemSpec_IDP_FD
A_27989	Bekanntgabe von Änderungen im Entity Statement einer Relying Party der TI-Föderation	gemSpec_IDP_FD
A_28859	Vorlaufzeit bei geplantem Schlüsselwechsel Signaturschlüssel für Entity Statements	gemSpec_IDP_FedMaster
A_28879	Registrierung von Teilnehmer in der TI-Föderation durch organisatorischen Prozess	gemSpec_IDP_FedMaster

## 4.2 Änderungen in gemAnbT\_Aktensystem\_ePA

**Tabelle 15: Anforderungen zur betriebliche Eignung "Anbietererklärung"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_23045-02	Registrierung des Fachdienstes	gemSpec_IDP_FD
A_23046	öffentlicher Schlüssel des Federation Master	gemSpec_IDP_FD
A_24607	Schlüsselwechsel Signaturschlüssel für Entity Statement	gemSpec_IDP_FD
A_27989	Bekanntgabe von Änderungen im Entity Statement einer Relying Party der TI-Föderation	gemSpec_IDP_FD
A_28859	Vorlaufzeit bei geplantem Schlüsselwechsel Signaturschlüssel für Entity Statements	gemSpec_IDP_FedMaster
A_28879	Registrierung von Teilnehmer in der TI-Föderation durch organisatorischen Prozess	gemSpec_IDP_FedMaster

## 4.3 Änderungen in gemProdT\_Aktensystem\_ePA

**Tabelle 16: Anforderungen zur funktionale Eignung "Herstellererklärung"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_23004	Anforderung eines Vertrauensniveaus	gemSpec_IDP_FD

A_23004-01	Anforderung eines Vertrauensniveaus	
A_23034-01	Entity Statement veröffentlichen	gemSpec_IDP_FD
A_23034-02	Entity Statement veröffentlichen	gemSpec_IDP_FD
A_23038	Entity Statement abrufen	gemSpec_IDP_FD
A_23039	Entity Statement vorhalten	gemSpec_IDP_FD
A_27504	Informationspflicht bei Änderungen der benötigten Werte "scope" und "redirect_uris"	gemSpec_IDP_FD
A_27504-01	Informationspflicht bei Änderungen der benötigten Werte "scope" und "redirect_uris"	gemSpec_IDP_FD
A_29019	Abruf eines Subordinate Statements abweichend von OpenID Federation 1.1 (befristet)	gemSpec_IDP_FedMaster

**Tabelle 17: Anforderungen zur sicherheitstechnische Eignung "Produktgutachten"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_23040	Fachdienst: Prüfung der Signatur des Entity Statements	gemSpec_IDP_FD
A_28848	Validierung der Vertrauenskette eines TI-Föderation Teilnehmers	gemSpec_IDP_FedMaster

## 4.4 Änderungen in gemAnbT\_IDP-Dienst

**Tabelle 18: Anforderungen zur betriebliche Eignung "Anbietererklärung"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_23040	Fachdienst: Prüfung der Signatur des Entity Statements	gemSpec_IDP_FD
A_23045-02	Registrierung des Fachdienstes	gemSpec_IDP_FD
A_23046	öffentlicher Schlüssel des Federation Master	gemSpec_IDP_FD
A_27989	Bekanntgabe von Änderungen im Entity Statement einer Relying Party der TI-Föderation	gemSpec_IDP_FD
A_28859	Vorlaufzeit bei geplantem Schlüsselwechsel	gemSpec_IDP_FedMaster

	Signaturschlüssel für Entity Statements	
A_28879	Registrierung von Teilnehmer in der TI-Föderation durch organisatorischen Prozess	gemSpec_IDP_FedMaster

## 4.5 Änderungen in gemProdT\_IDP-Dienst

**Tabelle 19: Anforderungen zur funktionale Eignung "Herstellererklärung"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_23004	Anforderung eines Vertrauensniveaus	gemSpec_IDP_FD
A_23004-01	Anforderung eines Vertrauensniveaus	gemSpec_IDP_FD
A_23034-01	Entity Statement veröffentlichen	gemSpec_IDP_FD
A_23034-02	Entity Statement veröffentlichen	gemSpec_IDP_FD
A_23038	Entity Statement abrufen	gemSpec_IDP_FD
A_23039	Entity Statement vorhalten	gemSpec_IDP_FD
A_27504	Informationspflicht bei Änderungen der benötigten Werte "scope" und "redirect_uris"	gemSpec_IDP_FD
A_27504-01	Informationspflicht bei Änderungen der benötigten Werte "scope" und "redirect_uris"	gemSpec_IDP_FD
A_29019	Abruf eines Subordinate Statements abweichend von OpenID Federation 1.1 (befristet)	gemSpec_IDP_FedMaster

**Tabelle 20: Anforderungen zur sicherheitstechnische Eignung "Produktgutachten"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_23040	Fachdienst: Prüfung der Signatur des Entity Statements	gemSpec_IDP_FD
A_28848	Validierung der Vertrauenskette eines TI-Föderation Teilnehmers	gemSpec_IDP_FedMaster