

---

C\_12598\_Anlage\_FedMaster

---

Inhaltsverzeichnis

1 Änderungsbeschreibung.....2

2 Änderung in gemSpec\_IDP\_FedMaster.....3

3 Änderungen in Steckbriefen.....35

    3.1 Änderungen in gemProdT\_IDP\_FedMaster.....35

    3.2 Änderungen in gemAnbT\_IDP\_FedMaster.....37

---

## 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-Federation 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\_FedMaster.

---

## 2 Änderung in gemSpec\_IDP\_FedMaster

---

Es wird Kapitel "1.1 Zielsetzung" wie folgt angepasst:

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb des Produkttyps Superior Federation Master. Der Produkttyp TI-Föderation Superior Federation Master basiert auf dem Standard [OpenID Federation] und unter Berücksichtigung weiterer Standards wie OpenID Connect (OIDC), Open Authorization 2.0 (OAuth 2) und JSON Web Token (JWT). Superior Entities nach [OpenID Federation] sind entweder die Vertrauensanker (Trust Anchor) oder bestimmte Knotenpunkte (Intermediate). Der Federation Master ist einerseits der Anker des Vertrauensbereichs der TI-Föderation. Superior Entities stellen Schnittstellen bereit, andererseits stellt der Federation Master Schnittstellen bereit, welche Auskunft über die in der Föderation registrierten Teilnehmer geben. Ein sektoraler Identity Provider gibt. Die Kernaufgaben der Superior Entities des Federation Master sind:

- Verwaltung der öffentlichen Schlüssel aller in der Föderation registrierten Teilnehmer (OpenID Provider (OP), Relying Party (RP) und OAuth-Protected Resources (RS) gemäß Spezifikation [openid-connect-core])
- Validierung von Anfragen über Teilnehmer der Föderation
- Bereitstellung von Schnittstellen für:
  - die Auskunft zur Superior Entity zum Federation Master (Entity Statement)
  - die Auskunft über Teilnehmer der Föderation (Subordinate Statement)
  - die Auskunft über die Liste aller registrierten OpenID Provider (OP)
  - die Registrierung neuer Teilnehmer (Intermediate, OP, RP und RS)
  - das Löschen von nicht mehr benötigten Teilnehmern (Intermediate, OP, RP und RS)

Es wird Kapitel "1.4 Abgrenzungen" wie folgt angepasst:

Textuelle Anpassung: ... Als Umsetzungsleitlinie ist [OpenID Connect Core 1.0] und [OpenID Connect Federation 1.0] heranzuziehen. ...

Es wird Kapitel "2.1 Allgemeiner Überblick" wie folgt angepasst:

- Text und Abbildung werden entfernt, es wird auf gemKPT\_TI-Föderation verwiesen.

Es wird Kapitel "2.2 Detaillierter Überblick" wie folgt angepasst:

- Text und Abbildung werden entfernt, es wird auf gemKPT\_TI-Föderation verwiesen.

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

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

Es wird Kapitel "2.4 Attributbeschreibung" wie folgt angepasst:

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

Es wird Kapitel "3.1 Anwendungsfälle" wie folgt angepasst:

- Bis auf "Tabelle : Anwendungsfälle Federation Master" werden die Inhalte im Kapitel entfernt, es wird auf gemKPT\_TI-Föderation verwiesen.

**Tabelle 1: Anwendungsfälle Federation Master**

Typ	Anwendungsfall
Technisch	IDP-Liste bereitstellen
Technisch	Subordinate Entity Statement bereitstellen
Technisch	Schlüssel verwalten
Technisch / Organisatorisch	Schlüssel der TLS-Zertifikate abgleichen
Organisatorisch	Teilnehmer registrieren
Organisatorisch	Teilnehmer löschen

Die technischen Anwendungsfälle des Federation Master werden hier im Detail beschrieben. Details zu den organisatorischen Anwendungsfällen des Federation Master finden sich in Kapitel ["Organisatorische Prozesse am Federation Master"]. Die Ausprägung der Anwendungsfälle anderer Komponenten spielt im Rahmen dieser Spezifikation keine Rolle.

Kapitel 3.3 wird Kapitel "3.1 Anwendungsfall - Entity Statement bereitstellen" und wie folgt angepasst:

Anpassung der Abbildung

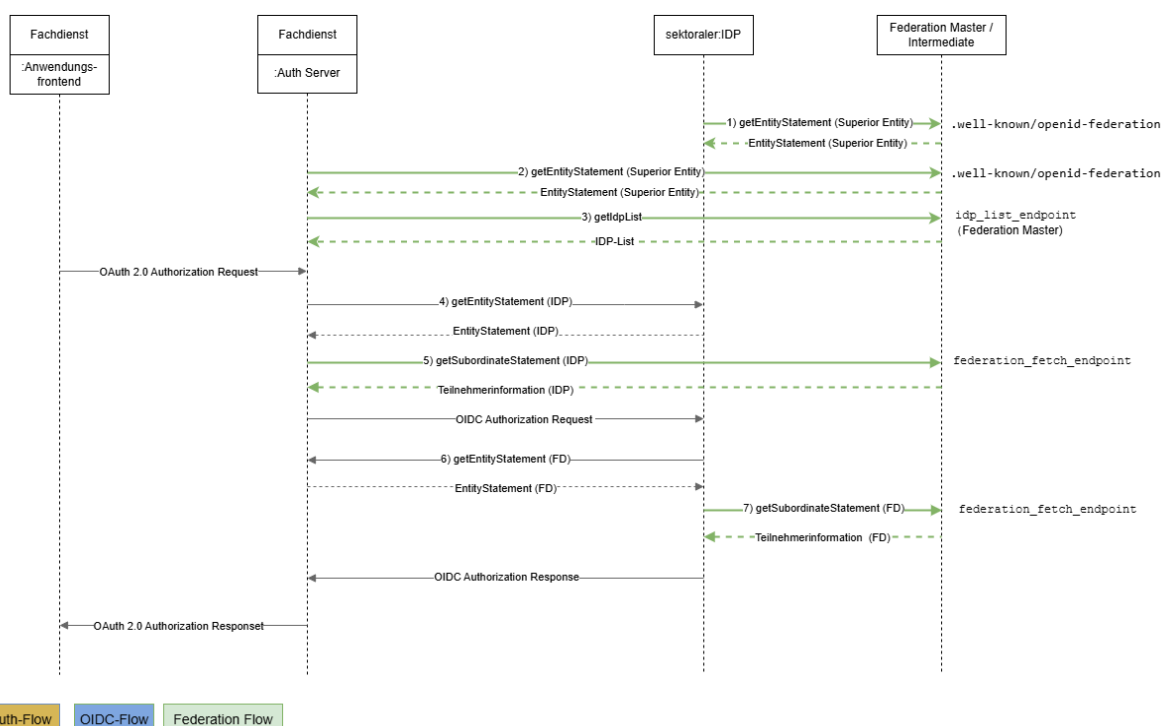


Abbildung 1 : Federation Master und Intermediate im Authorization-Flow

Tabelle 2: Federation Master und Intermediate im Authorization-Flow

Schritt	Beteiligte Parteien	Beschreibung
1 - getEntityStatement(FM Superior Entity)	sektoraler Identity Provider, Federation Master	Request zum Abholen des Entity Statement des Federation Master am Endpunkt  .well-known/openid-federation des Federation Master durch den sektoralen Identity Provider.
2 - getEntityStatement(FM Superior Entity)	Fachdienst Authorization Server, Federation Master/Intermediate	Request zum Abholen des Entity Statement der Superior Entity, bei welcher der Fachdienst Authorization Server registriert ist des Federation Master am Endpunkt  .well-known/openid-federation der Superior Entity des Federation Masters durch den Fachdienst Authorization Server.
3 - getIdpList	Fachdienst Authorization Server, Federation	Request zum Abholen der Liste der in der TI-Föderation registrierten sektoralen Identity

	Master	Provider vom Federation Master durch den Fachdienst <b>Authorization Server</b> amidp_list_endpoint Endpunkt des Federation Master.
4 - getEntityStatement(IDP)	Fachdienst <b>Authorization Server</b> , sektoraler Identity Provider	Request zum Abholen des Entity Statement vom sektoralen Identity Provider durch den Fachdienst <b>Authorization Server</b>
5 - <b>fetchEntityStatement(IDP)</b> <b>getSubordinateStatement(IDP)</b>	Fachdienst <b>Authorization Server</b> , Federation Master	Validieren des sektoralen Identity Provider als Teilnehmer der TI-Föderation beim Federation Master durch den Fachdienst <b>Authorization Server</b> am Endpunkt federation_fetch_endpoint des Federation Masters.
6 - getEntityStatement(FD)	sektoraler Identity Provider, Fachdienst <b>Authorization Server</b>	Request zum Abholen des Entity Statement des Fachdienstes vom Fachdienst <b>Authorization Server</b> durch den sektoralen Identity Provider.
7 - <b>fetchEntityStatement(FD)</b> <b>getSubordinateStatement(FD)</b>	sektoraler Identity Provider, Federation Master	Validieren des Fachdienstes <b>Authorization Server</b> als Teilnehmer der TI-Föderation beider Superior Entity, bei welcher der Fachdienst <b>Authorization Server</b> registriert ist <del>beim Federation Master</del> durch den sektoralen Identity Provider am Endpunkt federation_fetch_endpoint <del>der Superior Entity</del> <del>des Federation Masters</del> .

Hinweis: Eine detaillierte Beschreibung der Verwendung des OAuth- und OIDC-Standards ist nicht Teil dieser Spezifikation. Die diesbezüglichen Schritte im Flow werden nicht weiter erläutert.

**redaktionell**




geändert:

## **AF\_10101-01 -Bereitstellung von Informationen zu Teilnehmern der Föderation durch den Federation Master**

**Tabelle 3: Anwendungsfall "Bereitstellung von Informationen zu Teilnehmern der Föderation durch den Federation Master"**

Attribute	Bemerkung
-----------	-----------

Beschreibung	Der Nutzer einer Anwendung der Föderation muss durch die Anwendung autorisiert werden. Im Zuge des Autorisierungsablaufs wird der Nutzer über einen sektoralen Identity Provider authentifiziert. Im Ablauf dieses Authorization-Flow einer Anwendung wird der Federation Master zur Validierung der teilnehmenden Parteien einbezogen. Die Abbildung "Federation Master im Authorization-Flow" zeigt die Schritte im Flow, bei denen eine Kommunikation mit dem Federation Master stattfindet.
Akteur	Anwender der Fachanwendung
Auslöser	Ein Anwender möchte eine Gesundheitsanwendung der TI (Fachdienst) nutzen und muss dafür gegen einen sektoralen Identity Provider der TI authentifiziert werden.
Komponente	<ul style="list-style-type: none"> <li>• Federation Master</li> <li>• Fachdienst der TI</li> <li>• sektoraler Identity Provider</li> </ul>
Vorbedingung	<ul style="list-style-type: none"> <li>• Der Fachdienst ist in der TI-Föderation registriert und sein öffentlicher Schlüssel und sein Entity Statement sind beim Federation Master hinterlegt.</li> <li>• Der sektorale Identity Provider ist in der TI-Föderation registriert und sein öffentlicher Schlüssel und sein Entity Statement sind beim Federation Master hinterlegt.</li> <li>• Das Entity Statement des Federation Master steht zur Verfügung und die unter dem Attribut <code>federation_fetch_endpoint</code> benannte URL MUSS aus dem Internet erreichbar sein.</li> </ul>
Ablauf	<ul style="list-style-type: none"> <li>• Im Ablauf der Nutzung eines Fachdienstes (siehe Abbildung - Flow-Diagramm "Federation Master im Authorization-Flow") findet eine Verzweigung zum Federation Master in dem Fall statt, wenn der Fachdienst das Entity Statement des sektoralen Identity Provider oder wenn der sektorale Identity Provider das Entity Statement des Fachdienstes nicht kennt.</li> <li>• Die unter <code>federation_fetch_endpoint</code> im Entity Statement des Federation Master festgelegte URL MUSS aus dem Internet erreichbar sein.</li> <li>• Für die Abfrage von Informationen zu einem Teilnehmer der Föderation beim Federation Master sendet der anfragende Teilnehmer einen Request an die unter <code>federation_fetch_endpoint</code> im Entity Statement des Federation Master festgelegte URL. Der Request MUSS die in Tabelle "Teilnehmer Validierung Abfrage - Request Parameter" Parameter umfassen.</li> <li>• Der Federation Master MUSS als Response auf die Anfrage des Fachdienstes ein signiertes JSON Web Token senden. Die Header- und Payload-Attribute des JWS MÜSSEN mindestens die in den Tabellen "Teilnehmer Validierung Abfrage - Response-Payload-Attribute des signierten JSON-Web-Token" und</li> </ul>

	"Teilnehmer Validierung Abfrage - Response-Header-Attribute des signierten JSON-Web-Token" aufgeführten Attribute enthalten.
Ergebnis	Der anfragende Teilnehmer hat Informationen über den angefragten Teilnehmer erhalten, kann diese entschlüsseln und verwenden.
Akzeptanzkriterien	 <a href="#">ML-128451 - AF_10101 - Unter federation_fetch_endpoint benannte URL ist erreichbar und liefert signiertes JWS als Response</a> ,  <a href="#">ML-136402 - AF_10101 - Request von Teilnehmern an die federation_fetch_endpoint benannte URL des Federation Master</a> , <a href="#">ML-152179 - AF_10101 - Payload des JWS-Token enthält Informationen zum angefragten Teilnehmer der Föderation</a> 
Alternativen	Der Anwendungsfall entfällt, wenn die Teilnehmer sich kennen, eine gegenseitige Validierung bereits früher erfolgt ist und eine erneute Validierung (noch) nicht notwendig ist.

104 **Tabelle 4: Teilnehmer Validierung Abfrage - Request-Parameter**

Attribut	Werte / Typ	Beispiel	Anmerkung
iss	URL	"https://master0815.de"	URL des Federation Master
sub	URL	"https://idp4711.de" bzw. "https://Fachdienst007.de"	URL des angefragten Teilnehmer (sektoraler Identity Provider bzw. Fachdienst)
aud	URL	"https://Fachdienst007.de"	Identifiziert den anfragenden Teilnehmer. Wird dieser claim nicht gesetzt, so kann alternativ die bei der Registrierung des Fachdienstes/IDP vergebene Member-ID im UserAgent gesetzt werden.

105 **Tabelle 5: Teilnehmer Validierung Abfrage - Response-Payload-Attribute des signierten JSON-Web-Token**  
106  
107

Attribut	Werte / Typ	Beispiel	Anmerkungen
iss	URL	"https://master0815.de"	URL des Federation Master
sub	URL	"https://idp4711.de" bzw. "https://Fachdienst007.de"	URL des angefragten Teilnehmers (sektoraler Identity Provider bzw.



			Fachdienst)
iat	Alle time Werte in Sekunden seit 1970, <a href="#">[RFC7519#section-2]</a>	1645398001 = 2022-02-21 00:00:01	Ausstellungszeitpunkt des Abrufs
exp	Alle time Werte in Sekunden seit 1970, <a href="#">[RFC7519#section-2]</a>	1645484400 = 2022-02-22 00:00:00 entspricht einer Gültigkeit von 24 Stunden in Bezug auf den Wert in iat	Ablaufzeitpunkt der Gültigkeit der Liste (maximal iat + 24 Stunden)
jwtks	JWKS-Objekt		öffentlicher Schlüssel des angefragten Teilnehmers (sektoraler Identity Provider bzw. Fachdienst

Folgende Werte müssen Bestandteil des Headers der vom Federation Master signierten Informationen zu Teilnehmern der Föderation sein:

**Tabelle 6: Teilnehmer Validierung - Response-Header-Attribute des signierten JSON-Web-Token**

Name	Werte	Beispiel	Anmerkungen
alg	ES256	<-	
kid	wie aus jwtks im Body des Entity Statement		Identifiziert den verwendeten Schlüssel aus dem jwtks im Body des Statement
typ	entity-statement+jwt	<-	




[<=,IDP\_FedMaster,funkt. Eignung: Test Produkt/FA]

Neu:

## AF\_10101-02 -Bereitstellung von Informationen zu Teilnehmern der Föderation (Subordinate Statement)

119  
120**Tabelle 7: Anwendungsfall "Bereitstellung von Informationen zu Teilnehmern der Föderation durch eine Superior Entity"**

Attribute	Bemerkung
Beschreibung	Der Nutzer einer Anwendung der Föderation muss durch die Anwendung autorisiert werden. Im Zuge des Autorisierungsablaufs wird der Nutzer über einen sektoralen Identity Provider authentifiziert. Im Ablauf dieses Authorization-Flow einer Anwendung wird die Superior Entity (der Federation Master oder Intermediate), bei welcher der Fachdienst Authorization Server registriert ist, zur Validierung der teilnehmenden Parteien einbezogen. Die Abbildung "Federation Master und Intermediate im Authorization-Flow" zeigt die Schritte im Flow, bei denen eine Kommunikation mit der Superior Entity dem Federation Master stattfindet.
Akteur	Anwender der Fachanwendung
Auslöser	Ein Anwender möchte eine Gesundheitsanwendung der TI (Fachdienst) nutzen und muss dafür gegen einen sektoralen Identity Provider der TI authentifiziert werden.
Komponente	<ul style="list-style-type: none"> <li>• Superior Entity (Federation Master oder Intermediate)</li> <li>• Fachdienst Authorization Server eines Fachdienstes der TI</li> <li>• sektoraler Identity Provider</li> </ul>
Vorbedingung	<ul style="list-style-type: none"> <li>• Der Fachdienst Authorization Server ist bei einer Superior Entity in der TI-Föderation registriert und sein öffentlicher Schlüssel und sein Entity Statement sind bei der Superior Entity beim Federation Master hinterlegt.</li> <li>• Der sektorale Identity Provider ist beim Federation Master in der TI-Föderation registriert und sein öffentlicher Schlüssel und sein Entity Statement sind beim Federation Master hinterlegt.</li> <li>• Das Entity Statement der Superior Entity des Federation-Master steht zur Verfügung und die unter dem Attribut federation_fetch_endpoint benannte URL ist MUSS aus dem Internet erreichbar sein.</li> </ul>
Ablauf	<ul style="list-style-type: none"> <li>• Im Ablauf der Nutzung eines Fachdienstes (siehe Abbildung - Flow-Diagramm "Federation Master und Intermediate im Authorization-Flow") findet eine Verzweigung zu einer Superior Entity (zum Federation Master oder Intermediate) in dem Fall statt, wenn der Fachdienst Authorization Server das Entity Statement des sektoralen Identity Provider oder wenn der sektorale Identity Provider das Entity Statement des Fachdienstes Authorization Server nicht kennt.</li> <li>• Für die Abfrage von Informationen zu einem Teilnehmer der TI-Föderation bei einer Superior Entity beim Federation-Master sendet der anfragende Teilnehmer einen Request an die unter federation_fetch_endpoint im Entity Statement</li> </ul>

	<p>der Superior Entity des Federation Master festgelegte URL. Der Request MUSS die in Tabelle "Teilnehmer Validierung Abfrage - Request Parameter" Parameter umfassen.</p> <ul style="list-style-type: none"> <li>Die Superior Entity des Federation Master MUSS als Response auf die Anfrage des Fachdienstes ein signiertes JSON Web Token senden (Subordinate Statement). Die Header- und Payload-Attribute des JWS MÜSSEN mindestens die in den Tabellen "Teilnehmer Validierung Abfrage - Response-Payload-Attribute des signierten JSON-Web-Token" und "Teilnehmer Validierung Abfrage - Response-Header-Attribute des signierten JSON-Web-Token" aufgeführten Attribute enthalten.</li> </ul>
Ergebnis	Der anfragende Teilnehmer hat Informationen über den angefragten Teilnehmer erhalten, kann diese entschlüsseln und verwenden.
Akzeptanzkriterien	<p> <a href="#">ML-190119 - AF_10101 - Request von Teilnehmern an die im federation_fetch_endpoint benannte URL der Superior Entity</a></p> <p> <a href="#">ML-190120 - AF_10101 - Unter federation_fetch_endpoint benannte URL ist erreichbar und liefert signiertes JWS als Response</a></p> <p> <a href="#">ML-190121 - AF_10101 - Payload des JWS-Token enthält Informationen zum angefragten Teilnehmer der TI-Föderation</a></p>
Alternativen	Der Anwendungsfall entfällt, wenn die Teilnehmer sich kennen, eine gegenseitige Validierung bereits früher erfolgt ist und eine erneute Validierung (noch) nicht notwendig ist.

**Tabelle 8: Subordinate Statement - Request-Parameter (Subordinate Statement) gemäß [OpenID Federation 1.1] - "Fetch Subordinate Statement Request"**

Attribut	Werte / Typ	Anmerkung
iss (deprecated)*	string, URL nach [RFC1738]	Identifiziert (iss) des Federation Master aus dessen Entity Statement
sub	string, URL nach [RFC1738]	Identifiziert (iss) des angefragten Teilnehmers aus dessen Entity Statement
aud (deprecated)*	string, URL nach [RFC1738]	Identifiziert (iss) des angefragten Teilnehmers aus dessen Entity Statement Wird dieser claim nicht gesetzt, so kann alternativ die bei der Registrierung des Fachdienstes/IDP vergebene Member-ID im UserAgent gesetzt werden.

(\*) Nach finaler Version [OpenID Federation 1.1] sind die Parameter "iss" und "aud" nicht mehr notwendig. Subordinate Entities müssen die Schnittstelle mit und ohne die deprecated-Parameter unterstützen, bis alle Teilnehmer ihre Requests konform zum aktuellen Standard erstellen.

**Tabelle 9: Subordinate Statement - Response-Payload-Attribute des signierten JSON-Web-Token**

Attribut	Werte / Typ	Anmerkungen
iss	string, URL nach [RFC1738]	Identifiziert (iss) des Federation Master aus dessen Entity Statement
sub	string, URL nach [RFC1738]	Identifiziert (iss) des angefragten Teilnehmers aus dessen Entity Statement
iat	Alle time Werte in Sekunden seit 1970, [RFC7519#section-2]	Ausstellungszeitpunkt des Subordinate Statement
exp	Alle time Werte in Sekunden seit 1970, [RFC7519#section-2]	Ablaufzeitpunkt der Gültigkeit des Subordinate Statement
jwks	Set von JWK [RFC7517] zulässige Werte sind, gemäß [OpenID Federation 1.1] - jwks, nur die öffentlichen Schlüssel zu Schlüsseln, mit denen das Entity Statement signiert ist (Federation Entity signing key).	Öffentlicher Schlüssel, mit dem der angefragte Teilnehmer sein Entity Statement signiert (Federation Entity signing key).

Folgende Werte müssen Bestandteil des Header der vom Federation Master signierten Informationen zu Teilnehmern der TI-Föderation sein:

**Tabelle 10: 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]	Identifiziert des verwendeten Schlüssels aus dem jwks im Body des Statement
typ	entity-statement+jwt	

【<=,IDP\_FedMaster,funkt. Eignung: Test Produkt/FA】

Kapitel 3.3.1 wird Kapitel "3.1.1 Akzeptanzkriterien - Entity Statement bereitstellen" und wie folgt angepasst:

Alt:

**ML-136402 -AF\_10101 - Request von Teilnehmern an die federation\_fetch\_endpoint benannte URL des Federation Master**

Der Request eines in der Föderation registrierten Teilnehmers an die im Entity Statement des Federation Master unter dem Claim federation\_fetch\_endpoint benannte URL SOLL die in der Tabelle "Teilnehmer Validierung Abfrage - Request-Parameter" aufgeführten Claims enthalten. Ist der aud-Parameter im Fetch Entity-Statement-Request des anfragenden Teilnehmers nicht gesetzt, so SOLL die Member-ID als User-Agent im Request Header gesetzt sein. Ist weder der aud-Parameter noch der user-agent gesetzt MUSS trotzdem ein Entity Statement zum angefragten Teilnehmer vom Federation Master zurück geliefert werden. [≤]

**ML-128451 -AF\_10101 - Unter federation\_fetch\_endpoint benannte URL ist erreichbar und liefert signiertes JWS als Response**

Der Request eines Teilnehmers der Föderation an die URL, welche im Entity Statement des Federation Master unter dem Attribut federation\_fetch\_endpoint benannt ist, wird entgegengenommen und gibt als Response ein signiertes JWS zurück. Das Token ist mit dem privaten Schlüssel des Federation Master signiert und kann vom Fachdienst mit dem öffentlichen Schlüssel des Federation Master verifiziert werden. [≤]

**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 - Identifiziert Federation Master
- sub= URL - Identifiziert 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 -Identifiziert 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

[≤]

Neu:

**ML-190119 -AF\_10101 - Request von Teilnehmern an die im federation\_fetch\_endpoint benannte URL der Superior Entity**

Der Request eines in der TI-Föderation registrierten Teilnehmers an die im Entity Statement der Superior Entity, bei welcher der Teilnehmer registriert ist (Federation Master oder Intermediate), unter dem Claim federation\_fetch\_endpoint benannte URL SOLL die in der Tabelle "Teilnehmer Validierung Abfrage - Request-Parameter" aufgeführten Claims enthalten. Ist der aud-Parameter im Subordinate-Statement-Request des anfragenden Teilnehmers nicht gesetzt, so SOLL die Member-ID als User Agent im Request Header gesetzt sein. Ist weder der aud-Parameter noch der User Agent gesetzt, MUSS trotzdem ein Subordinate Statement zum angefragten Teilnehmer vom Federation Master zurückgeliefert werden. [ <= ]

**ML-190120 -AF\_10101 - Unter federation\_fetch\_endpoint benannte URL ist erreichbar und liefert signiertes JWS als Response**

Der Request eines Teilnehmers der TI-Föderation an die URL, welche im Entity Statement der Superior Entity, bei welcher der Teilnehmer registriert ist (Federation Master oder Intermediate), unter dem Attribut federation\_fetch\_endpoint benannt ist, wird entgegen genommen und gibt als Response ein signiertes JWS (Subordinate Statement) zurück. Das Token ist mit dem privaten Schlüssel der Superior Entity signiert und kann vom Teilnehmer der TI-Föderation mit dem öffentlichen Schlüssel der Superior Entity verifiziert werden. [ <= ]

**ML-190121 -AF\_10101 - Payload des JWS-Token enthält Informationen zum angefragten Teilnehmer der TI-Föderation**

Der Payload des JWS-Token (Subordinate Statement) enthält diese Informationen bezüglich des angefragten Teilnehmers der TI-Föderation:

- 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 federation entity signing key des angefragten Teilnehmers
- metadata= JSON Object mit den Metadaten, die der Teilnehmer in seinem Entity Statement ausweist

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

- scope = Scope, die bei der Registrierung der Relying Party bei der Superior Entity angegeben wurden
- claims = Claims, die bei der Registrierung der Relying Party der Superior Entity angegeben wurden
- redirect\_uris = redirect\_uris, die bei der Registrierung der Relying Party der Superior Entity angegeben wurden

[ <= ]

**Implementierung**

Neu:

## A\_28912 -Gefilterte Suche nach entity\_type

Federation Master und Intermediates MÜSSEN die gefilterte Suche nach entity\_type gemäß [\[OpenID Federation 1.1\]](#) unterstützen.

[<=,IDP\_FedMaster,funkt. Eignung: Test Produkt/FA]

## Kapitel 3.2 wird neues Kapitel "3.2 Federation Master"

- konkrete Anwendungsfälle Federation Master (siehe Tabelle "Übersicht über die Anwendungsfälle im Gesamtkontext Federation Master")
- (neu anordnen) Kapitel 3.2.1 Anwendungsfall - IDP-Liste bereitstellen (ehemals Kapitel 3.2)
- (neu anordnen) Kapitel 3.2.2 Anwendungsfall - Schlüssel verwalten (ehemals Kapitel 3.4)

## Kapitel 3.3 wird neues Kapitel "3.3 ZETA TI-Authorization Servers Intermediate" eingefügt

Der ZETA-TI-Authorization Server Intermediate, ist eine Superior-Entity, bei welcher alle ZETA-Authorization Server für TI-Fachdienste registriert sind. Die Einführung dieses Intermediate (gemäß [\[OpenID Federation 1.1\]](#)) wird bedingt durch Anforderungen an ZETA-Authorization Server, welche für den übrigen Teil der TI-Föderation nicht oder noch nicht gelten:

- Das Entity Statement von ZETA-Authorization Servern wird von einer großen Anzahl ZETA-Client aufgerufen. ZETA-Clients ermitteln über das Entity Statement die Adresse der Ressource, auf die nach erfolgreicher Authentifizierung zugegriffen wird. Die ZETA-Clients sind nicht Teil der TI-Föderation. Zur Herstellung des Vertrauensverhältnisses zwischen ZETA-Client und einem ZETA-Authorization Server muss jeder ZETA-Authorization Server in seinem Entity Statement eine Trust Mark [\[OpenID Federation 1.0 Kapitel "Trust Marks"\]](#) ausgestellt und signiert von einer Superior Entity enthalten. Ein beliebiger ZETA-Client kann die Trust Mark validieren.
- Die Umstellung von TI-Fachdiensten auf ZETA hat zur Folge, dass temporär sowohl die herkömmlichen Fachdienst Authorization Server als auch die Fachdienst ZETA-Authorization Server für einen Fachdienst in der TI-Föderation registriert sind. Es ist sicherzustellen, dass Clients den richtigen Authorization Server eines Fachdienstes zur Authentifizierung aufrufen.

Der ZETA-TI-Authorization Server Intermediate kann sowohl Trust Marks ausstellen, als auch das Auffinden der richtigen Authorization Server erleichtern. Der ZETA-TI-Authorization Server Intermediate ist Subordinate-Entity des Federation Master.

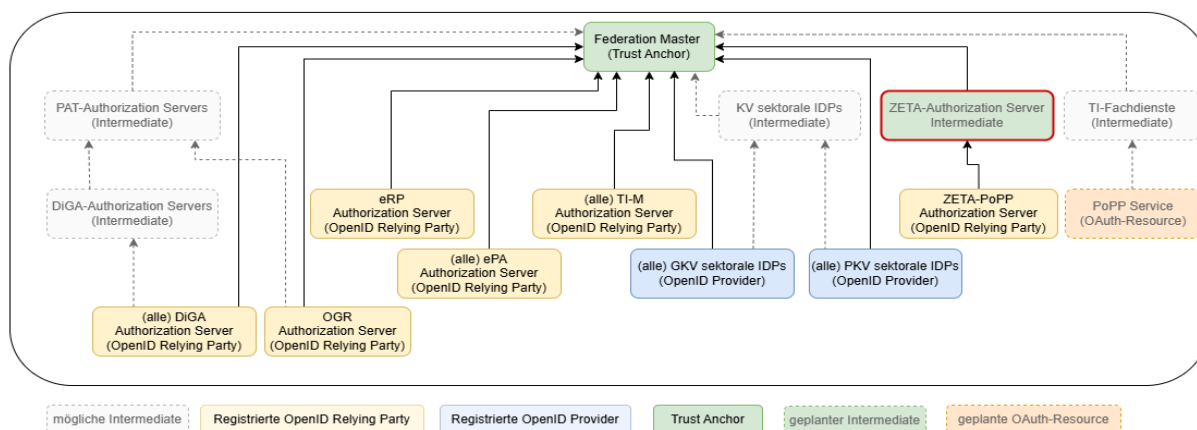


Abbildung 2 : ZETA-Authorization Server Intermediate in der TI-Föderation



### **A\_28985 -Ausstellen einer Trust Mark als Nachweis der Teilnehmer-Registrierung**

Der ZETA-TI-Authorization Server Intermediate MUSS für jeden bei ihm registrierten Teilnehmer eine Trust Mark gemäß [\[OpenID Federation 1.1\]](#) -"Trust Marks" ausstellen. Die ausgestellte Trust Mark entspricht dem Subordinate Statement des ZETA-TI-Authorization Server Intermediate zu diesem Teilnehmer. [≤, IDP\_FedMaster, funkt. Eignung: Test Produkt/FA]

### **A\_28986 -Teilnehmer-Registrierung ausschließlich ZETA-TI-Authorization Server**

Der ZETA-TI-Authorization Server Intermediate MUSS sicherstellen, dass ausschließlich ZETA-TI-Authorization Server als Subordinate Entities am ZETA-TI-Authorization Server Intermediate registriert werden. [≤, IDP\_FedMaster, funkt. Eignung: Herstellererklärung]

### **Anforderungen an ZETA-TI-Authorization Server --> Muss dann in ZETA-Spec**

- ZETA-TI-Authorization Server MÜSSEN sich über einen organisatorischen Prozess (A\_22675\* - Teilnehmerregistrierung am Federation Master und Intermediate) am ZETA-TI-Authorization Server Intermediate registrieren.
- ZETA-TI-Authorization Server MÜSSEN die vom ZETA-TI-Authorization Server Intermediate signierte Trust Mark nach [\[OpenID Federation 1.1\]](#) -"Trust Marks" in ihr Entity Statement integrieren.
- Zweisung A\_28848, A\_28857, A\_28879

### **Kapitel 3.4 wird neues Kapitel "3.4 TI-Trust Chain Resolver" eingefügt**

Der TI-Trust Chain Resolver erfüllt die Funktionalität zur Auflösung einer Vertrauenskette ausgehend von der Entity Configuration eines Teilnehmers bis zu TI-Trust Anchor [\[OpenID Federation 1.1\]](#) -"Resolve Entity". Ein Teilnehmer der TI-Föderation kann die Validierung der Trust Chain durch den TI-Trust Chain Resolver durchführen lassen und das Ergebnis der Prüfung speichern.

### **A\_28987 -TI-Trust Chain Resolver**

Der Federation Master MUSS die Funktionalität eines TI-Trust Chain Resolver gemäß [\[OpenID Federation 1.1\]](#) implementieren. Der Endpunkt, unter dem die Funktionalität von einem TI-Föderationsteilnehmer aufgerufen werden kann, MUSS in der Entity Configuration allen TI-Teilnehmern mit dem Entity Typ federation\_entity im claim\_federation\_resolve\_endpoint angegeben werden. [≤, IDP\_FedMaster, funkt. Eignung: Test Produkt/FA]

### **Es wird Kapitel "4.1 Aufbau und Inhalt des Federation Master Entity Statement" wie folgt angepasst:**

- Text anpassen (Federation = Trust Anchor, Intermediate weitere Superior Entities in der Vertrauenskette)

Superior Entities sind gemäß [\[OpenID Federation 1.1\]](#) Entitäten in der Hierarchie der TI-Föderation, bei der andere Entitäten (Subordinate Entity) registriert sind. Dabei kann es sich bei den Subordinate Entities um Intermediate oder Leaf Entities (OpenID Provider, OpenID Relying Party, OAuth Resource) handeln.



Der Federation Master ist bei keiner weiteren Superior Entity registriert. Er bildet den Vertrauensanker der TI-Föderation. Intermediate Entities sind Entitäten, welche Auskunft zu bei ihnen direkt registrierten Teilnehmern geben können (Subordinate Statement). Die Funktionen des Federation Master und der Intermediates sind in der TI-Föderation nahezu gleich. Der Funktionsumfang des Federation Master ist spezifisch für die TI-Föderation erweitert.

Gemäß den verwendeten Standards OpenID Federation, OpenID Connect und mit OAuth 2.0 kommen JSON Web Token (JWT), JSON Web Encryption (JWE), JSON Web Signature (JWS) und JSON Web Key (JWK) zum Einsatz.

Um den nutzenden Anwendungen eine einheitliche Bezugsquelle für die Adressierung von Schnittstellen zu schaffen, werden die für alle Akteure grundlegenden Schnittstellen in der Entity Configuration zusammengefasst. Jeder Teilnehmer veröffentlicht seine Entity Configuration als Entity Statement unter <Teilnehmer URL> \ und dort unter der ".well-known/openid-federation ([OpenID Federation Kapitel "Entity Statement"])" gemäß [OpenID Connect Federation 1.0] veröffentlicht.

Alle Akteure der TI-Föderation sind angehalten, das Entity Statement herunterzuladen und den Inhalt in den geplanten Betrieb einzubeziehen. Die Teilnehmer der TI-Föderation benötigen die Entity Configuration der Superior Entity des Federation Master zur:

- Validierung der Vertrauenskette in der Kommunikation zwischen Fachdiensten, Authorization Servern, Intermediates und sektoralen Identity Providern
- Validierung anderer Kommunikationsteilnehmer in der TI-Föderation
- Ermittlung des API-Endpunktes der Superior Entities und außerdem bei Bedarf die Entity Configuration des Federation Master zur
- Ermittlung der Liste aller in der TI-Föderation registrierten sektoralen Identity Provider.

Alt:

#### **A\_22949 -Aktualisierungszyklen der Entity Statements zu Teilnehmern der Föderation**

Der Federation Master MUSS seine Entity Statements zu den Teilnehmern der Föderation täglich aktualisieren. Darüber hinaus MUSS der Federation Master sein Entity Statement zu einem Teilnehmern bei jeder Änderung, welche sich auf das Entity Statement zum Teilnehmer auswirkt, aktualisieren. [≤, IDP\_FedMaster, Sich.techn. Eignung: Herstellererklärung, funkt. Eignung: Test Produkt/FA]

**redaktionell**

Neu:

#### **A\_22949-01 -Aktualisierungszyklen der Subordinate Statements zu Teilnehmern der TI-Föderation**

Federation Master und Intermediates MÜSSEN die Subordinate Statements zu den Teilnehmern der Föderation täglich aktualisieren. Darüber hinaus MÜSSEN Federation Master und Intermediates Subordinate Statement zu einem Teilnehmer bei jeder Änderung aktualisieren, welche sich auf das Subordinate Statement zum Teilnehmer auswirkt. [≤, IDP\_FedMaster, Sich.techn. Eignung: Herstellererklärung]

**redaktionell**

**A\_28857 ersetzt A\_22948**Alt:**A\_22948 -Aktualisierungszyklen der Entity Statements Federation Master**

Der Federation Master MUSS sein Entity Statement täglich aktualisieren. Darüber hinaus MUSS der Federation Master sein Entity Statement bei jeder Änderung, welche sich auf das Entity Statement auswirkt, aktualisieren. [≤, IDP\_FedMaster, Sich.techn. Eignung: Herstellererklärung, funkt. Eignung: Test Produkt/FA]

Neu:**A\_28857 -Maximale Gültigkeitsdauer und regelmäßige Erneuerung des Entity Statement eines TI-Föderation-Teilnehmers**

Teilnehmer der TI-Föderation MÜSSEN ihr Entity Statement bei Änderungen oder vor dem zeitlichen Ablauf neu ausstellen. Die maximale Gültigkeitsdauer - gegeben durch die Differenz der Attributwerte exp-iat - darf 24 Stunden nicht überschreiten.

[≤, Aktensystem\_ePA, Anw\_DiGA, extNutz\_GID, IDP-D, digi\_ID\_OGR, IDP-Sek, IDP\_FedMaster, funkt. Eignung: Herstellererklärung, funkt. Eignung: Anbietererklärung]

**Implementierung****Zuweisung A\_28848, A\_28857, A\_28879**Neu:**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 (wg. API-Änderung bis zur Umsetzung AF\_10101-02 im Federation Master):

**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 11: Teilnehmer Validierung Abfrage - Request-Parameter**

Attribut	Werte / Typ	Anmerkung
iss	string, URL nach [ <a href="#">RFC1738</a> ]	Identifiziert (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]*

#### Neu:

#### **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]

#### Alt:

#### **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 12 : Prüfung der Entity Statements von Fachdiensten**

Attribut	Abweichung	Auswirkung	Maßnahme
jwtks	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
authority_hints	Die	Als	Einstelle

	Vertrauenskette hat sich geändert.	Vertrauensanker ist nicht mehr der Federation Master eingetragen. Vertrauensraum ist ggf. gefährdet.	n eines Incident
metadata.openid_relying_party.client_name	Der Name des Fachdienstes hat sich geändert.	Nach <a href="#">[OpenID Federation 1.0#section-5.1.2]</a> wird der in [OpenID Connect Registration 1.0] definierte client_name zur Darstellung der RP im Consent-Dialog verwendet. Die Änderung kann zu Anzeigeproblemen bei den Nutzern führen.	Einstellen eines Incident
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 Incident

430 **[<=,Anb\_IDP\_FedMaster,Sich.techn. Eignung: Anbietererklärung]**

## 432 Implementierung

### 433 Neu:

- 434 • Die Prüfung von "authority\_hints" entfällt - Da die Anforderung A\_28848 dem Federation Master zugewiesen wird, ist diese separate Prüfung überflüssig. Durch  
435 Prüfung der Vertrauenskette bis zum Trust Anchor wird der Vertrauensraum über  
436 authority\_hints überprüft.
- 437 • Die Prüfung von "metadata.openid\_relying\_party.client\_name" entfällt -  
438 Risikoabwägung zugunsten des Verzichts auf die Prüfung. Das Risiko aus einer  
439 Manipulation von client\_name und organization\_name ist sehr überschaubar, das  
440 Angriffsszenario sehr konstruiert. Prüfung ist verzichtbar.

## 442 A\_25414-02 -Prüfung der Entity Statements von Fachdiensten

443 Anbieter des Federation Master und von Intermediates MÜSSEN nach Abfrage der Entity  
444 Statements von Fachdienst Authorization Servern die Werte der in Tabelle "Prüfung der  
445

Entity Statements von Fachdienst Authorization Servern" aufgeführten Attribute hinsichtlich der bei der Registrierung hinterlegten Werte prüfen. Stimmen die Werte nicht überein, so MUSS der Anbieter die in der Tabelle aufgeführten Maßnahmen treffen.

**Tabelle 13 : Prüfung der Entity Statements von Fachdienst Authorization Servern**

Attribut	Abweichung	Auswirkung	Maßnahme
iss	Die Client-ID hat sich geändert.	Der Teilnehmer ist in der TI-Föderation nicht mehr zu finden.	Einstellen eines Incident
jwtks	Schlüssel, mit dem der Fachdienst sein Entity Statement signiert (federation entity signing key), hat sich unabhängig vom Key-Rollover nach A_28859* geändert.	Die bei der Superior Entity hinterlegten Schlüssel sind nicht mehr korrekt, der Vertrauensraum ist ggf. gefährdet.	Einstellen eines Incident

【<=,Anb\_IDP\_FedMaster,Sich.techn. Eignung: Anbietererklärung】

*Hinweis 1: Zur Sicherung der Kompatibilität werden für folgende Abweichung erst nach initialer Anpassung aller registrierten Relying Parties Incidents eingestellt:*

- metadata.openid\_relying\_party.client\_name
- metadata.federation\_entity.organization\_name.

*Hinweis 2: Das Sperren eines Fachdienstes bedeutet technisch den Ausschluss aus der Föderation. Fragt ein sektoraler IDP die Teilnehmersauskunft zu einem gesperrten Fachdienst beim Federation Master ab, so antwortet dieser gemäß [OpenID Connect Federation 1.0#error\_response] mit Error Code HTTP-404 not\_found.*

*Hinweis 3: Zum Entsperren muss der Fachdienst die Abweichungen in seinem Entity-Statement korrigieren oder im Fall gewollter Änderungen zur Aktualisierung den organisatorischen Registrierungsprozess erneut durchlaufen.*

**A\_25415 entfällt, da nach A\_25414 keine Sperrmaßnahme vorgesehen ist**

**A\_25415 -Entsperren eines gesperrten Fachdienstes in der TI-Föderation**

Hat der Anbieter des Federation Master aufgrund von A\_25414 einen Fachdienst in der TI-Föderation gesperrt, so SOLL der Anbieter des Federation Master den Fachdienst ohne weitere Maßnahmen wieder zulassen, wenn dieser die Abweichungen im Entity Statement korrigiert hat.【<=,Anb\_IDP\_FedMaster,Sich.techn. Eignung: Anbietererklärung】

**A\_22604, A\_22605, A\_22608 - entfallen, Inhalte sind Teil von A\_22607-01 - Entity Configuration des Federation Master oder Intermediate**

**A\_22604 -Verwendung eindeutiger URI**

Der Federation Master MUSS alle verwendeten Adressen in Form von URL gemäß [RFC1738 ] angeben und in einem Entity Statement gemäß [OpenID Federation 1.0] im Internet veröffentlichen. [≤, IDP\_FedMaster, funkt. Eignung: Test Produkt/FA]

#### A\_22605 -Entity Statement Veröffentlichung

Der Federation Master MUSS sein Entity Statement im Internet gemäß [OpenID Connect Federation 1.0] unter ".well-known/openid-federation" veröffentlichen. [≤, IDP\_FedMaster, funkt. Eignung: Test Produkt/FA]

#### A\_22608 -Inhalte des Metadata Federation API-Endpunkt im Federation Master Entity Statement

Der Federation Master MUSS im Entity Statement gemäß [OpenID Federation 1.0] mindestens die folgenden Attribute als metadata/federation\_entity angeben:

**Tabelle 14: Attribut "Federation API Endpoint"**

Attribut	Typ	Beschreibung	Beispiel
federation_fetch_endpoint	URL	Adresse des Endpunktes zum Abrufen einzelner Statements zu sektoralen Identity Provider und Fachdiensten beim Federation Master	"https://master0815.de/federation_fetch"
federation_list_endpoint	URL	Adresse des Endpunktes zum Abrufen der Liste aller bekannten Entity Identifier	"https://master0815.de/federation_list"

[≤, IDP\_FedMaster, funkt. Eignung: Test Produkt/FA]

Alt:

#### A\_22607 -Inhalte des Federation Master Entity Statement

Der Federation Master MUSS im Entity Statement gemäß [OpenID Federation 1.0] mindestens die folgenden Attribute angeben:

**Tabelle 15: Attribute Entity Statement Federation Master**

Attribut	Typ	Beschreibung	Beispiel
iss	URL	URL des Federation Master	"https://master0815.de"
sub	URL	URL des Federation Master (=iss)	"https://master0815.de"
iat	long	Alle time-Werte in Sekunden seit 1970, <a href="#">RFC 7519 Sect.2</a>	1645398001 = 2022-02-21 00:00:01

jwks	JWKS	Schlüssel für die Signatur des Entity Statement	"master0815-1"
exp	long	Alle time-Werte in Sekunden seit 1970, <a href="#">RFC 7519 Sect.2</a>	1645484400 = Gültigkeit von 24 Stunden in Bezug auf den Wert in iat

495 [ $\leq$ , IDP\_FedMaster, funkt. Eignung: Test Produkt/FA]

## 496 Implementierung

### 497 Neu:

498 Im Rahmen der Kommentierung soll mit geklärt werden

- 500 • soll ein **display\_name** als MUSS im Entity Statement gefordert werden, wenn ja,  
501 welche anforderungen müssen daran gestellt werden
- 502 • welche Informationen können/sollen bei **contacts** hinterlegt werden können (e-Mail,  
503 Telefonnummern, Web-Page). Einschränken dazu seitens gematik oder keine  
504 normativen Festlegungen (über den OpenID Federation Standard hinaus - "JSON array  
505 with one or more strings representing contact persons at the Entity. These MAY  
506 contain names, e-mail addresses, descriptions, phone numbers, etc.")

507  
508 Anmerkung: Die Verwendung von "display\_name" ist aktuell in Klärung.

## 509 A\_22607-01 -Entity Configuration Inhalte des Federation Master oder 510 Intermediate

511 Federation Master und Intermediates MÜSSEN ihre Entity Configuration in einem selbst-  
512 signierten Entity Statement gemäß [OpenID Federation 1.1] ("Entity Statement")  
513 bereitstellen und im Internet verfügbar machen. Das Entity Statement MUSS mindestens  
514 die in der folgenden Tabelle aufgeführten Metadaten enthalten:

516 **Tabelle 16: Header des Entity Statement der Superior Entity**

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"

517 **Tabelle 17 :Allgemeine Attribute im well-known-Dokument der Superior Entity**

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 den das Entity Statement, ein Subordinate Statement und Trust Marks signiert ist (federation entity signing key)
authority_hints	[string] zulässige Werte gemäß <a href="#">OpenID Federation 1.1</a> ("Claims that MUST or MAY appear in both Entity Configurations and Subordinate Statements") - authority_hints
metadata	object, erforderlicher Wert: "federation_entity"

**Tabelle 18 :Attribute des Metadatenblocks federation\_entity im well-known-Dokument der Superior Entity**

Name	Werte
federation_fetch_endpoint	string (gemäß <a href="#">OpenID-Federation "Federation Entity"</a> - federation_fetch_endpoint) URL nach <a href="#">RFC1738</a>
federation_list_endpoint	string (gemäß <a href="#">OpenID-Federation "Federation Entity"</a> - federation_list_endpoint) URL nach <a href="#">RFC1738</a>
federation_historical_keys_endpoint	string (gemäß <a href="#">OpenID-Federation "Federation Entity"</a> - federation_historical_keys_endpoint) URL nach <a href="#">RFC1738</a>
organization_name	string (gemäß <a href="#">OpenID-Federation "Informational Metadata Extensions"</a> ] - organization_name) Wertebereich: <code>^[à-üÄ-Üß\w\ \-\.\+\*\V/]{1,128}\$</code>
display_name	string (gemäß <a href="#">OpenID-Federation "Informational Metadata Extensions"</a> ] - display_name)



	Wertebereich: ^[à-üÄ-Üß\w\  \.\ + \*V]{1,128}\$
keywords	[string] (gemäß [OpenID-Federation "Informational Metadata Extensions" ] - keywords) erforderlicher Werte: "product_type_version:<von der gematik zugelassene Produkttyp-Version>" "product_type:<von der gematik zugelassener Produkttyp>"
contacts	[string] (gemäß [OpenID-Federation "Informational Metadata Extensions" ] - contacts) erforderlicher Wert: "<E-Mail-Adresse für Supportanfragen>"

520 [ $\leq$ ,IDP\_FedMaster,funkt. Eignung: Test Produkt/FA]

521  
522 Alt:

### 523 A\_22606 -Entity Statement - Prüfung der angebotenen URL

524 Der Anbieter des Federation Master MUSS alle von ihm im Entity Statement angebotenen  
525 URL ständig auf bloße Erreichbarkeit prüfen.[ $\leq$ ,Anb\_IDP\_FedMaster,organ./betriebl.  
526 Eignung: Anbietererklärung]

527  
528 **redaktionell**

529 Neu:

### 530 A\_22606-01 -Entity Statement - Prüfung der angebotenen URL

531 Anbieter des Federation Master oder von Intermediates MÜSSEN alle von ihm im Entity  
532 Statement angebotenen URL ständig auf bloße Erreichbarkeit prüfen.  
533 [ $\leq$ ,Anb\_IDP\_FedMaster,organ./betriebl. Eignung: Anbietererklärung]

534  
535 Alt:

### 536 A\_23087 -Entity Statements gelöschter Teilnehmer

537 Der Federation Master MUSS sicherstellen, dass der Abruf des Entity Statement  
538 gelöschter Teilnehmer über das Federation Master API zu einer Fehlermeldung unter  
539 Berücksichtigung des Standards [OpenID Federation 1.0] führt.[ $\leq$ ,IDP\_FedMaster,funkt.  
540 Eignung: Test Produkt/FA]

541  
542 **redaktionell**

543 Neu:

### 544 A\_23087-01 -Entity Statements gelöschter Teilnehmer

545 Der Federation Master oder ein Intermediate MUSS sicherstellen, dass der Abruf des  
546 Subordinate Statement gelöschter Teilnehmer über das Federation EntityAPI zu einer  
547 Fehlermeldung unter Berücksichtigung des Standards [OpenID Federation 1.1] führt.  
548 [ $\leq$ ,IDP\_FedMaster,funkt. Eignung: Test Produkt/FA]

Es wird Kapitel "4.2 Organisatorische Prozesse am Federation Master und Intermediate" wie folgt angepasst:

Alt:

#### **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 Scope 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 Scope und Claims erhält. [ $\leq$ ,Anb\_IDP\_FedMaster,organ./betriebl. Eignung: Anbietererklärung, Sich.techn. Eignung: Gutachten (Anbieter)]

### **Implementierung**

Neu:

#### **A\_22675-03 -Teilnehmerregistrierung am Federation Master und Intermediate**

Anbieter des Federation Master und von Intermediates MÜSSEN einen organisatorischen Prozess für die Registrierung von Teilnehmern an der TI-Föderation etablieren. Alle Teilnehmer der TI-Föderation MÜSSEN über diesen Prozess ihre öffentlichen Schlüssel beim übergeordneten Intermediate oder beim Federation Master, wenn es keinen übergeordneten Intermediate gibt, hinterlegen. Fachdienste MÜSSEN zusätzlich die für ihre Anwendungsfälle notwendigen Scopes bzw. Claims hinterlegen. Der Anbieter des Federation Master oder Intermediate MUSS vorsehen, dass die gematik in den organisatorischen Ablauf eingebunden ist und die Möglichkeit der Prüfung der vom Fachdienst eingereichten Scopes und Claims erhält. Nach Abschluss des Registrierungsprozesses MUSS der Anbieter des Federation Master oder von Intermediates den öffentlichen Schlüssel, mit dem der Federation Master (Trust Anchor) sein Entity Statement signiert (Federation Entity Signing Key), dem registrierten Teilnehmer mitteilen.

*Hinweis 1: Der Registrierungsprozess muss die Registrierung der Entity-Typen openid\_provider, openid\_relying\_party, oauth\_resource und federation\_entity nach [OpenID Federation 1.1] ("Entity Type Identifiers") unterstützen.*

*Hinweis 2: Der Aufbau und die Verwendung der hierarchischen Vertrauensbeziehung (Trust Chain) ist im Standard [OpenID Federation 1.1] festgelegt und wird darüber hinaus hier nicht weiter spezifiziert.*

*Hinweise 3: Die Mitteilung des öffentlichen Schlüssel des Federation Entity Signing Key muss unabhängig vom eigentlichen Entity Statement erfolgen, der Verweis auf den jwks-claim im Entity Statement ist nicht ausreichend. Bei Registrierung der Teilnehmer über den Registrierungsprozess der gematik kann die Zustellung im Rahmen dieses Prozesses erfolgen.*

[ $\leq$ ,Anb\_IDP\_FedMaster,Sich.techn. Eignung: Anbietererklärung]

Alt:

#### **A\_22677 -Teilnehmer am Federation Master löschen**

Der Anbieter des Federation Master MUSS einen organisatorischen Prozess mit 4-Augen-Prinzip zur Erteilung von Löschaufträgen und einen technischen Prozess zum eigentlichen Löschen von Teilnehmern aus der Föderation etablieren.

601 [ $\leq$ ,Anb\_IDP\_FedMaster,organ./betriebl. Eignung: Anbietererklärung, Sich.techn.  
602 Eignung: Gutachten (Anbieter)]

603  
604 **redaktionell**

605 Neu:

606 **A\_22677-01 -Teilnehmer am Federation Master oder Intermediate löschen**

607 Der Anbieter des Federation Master oder eines Intermediate MUSS einen  
608 organisatorischen Prozess mit 4-Augen-Prinzip zur Erteilung von Löschaufträgen und  
609 einen technischen Prozess zum eigentlichen Löschen von Teilnehmern aus der TI-  
610 Föderation etablieren.[ $\leq$ ,Anb\_IDP\_FedMaster,Sich.techn. Eignung: Anbietererklärung]

611  
612 Neu:

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

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

623  
624 *Hinweis:* Nicht betroffen von dieser Anforderung sind kurzfristig notwendige  
625 Schlüsselwechsel, z. B. aufgrund von Sicherheitsvorfällen. Diese Maßnahmen sind  
626 beispielsweise über Security Incidents abzuwickeln. Die Bearbeitung solcher kurzfristigen  
627 Schlüsselwechsel muss die Aktualisierung beim Federation Master bzw. Intermediate mit  
628 berücksichtigen, da es ansonsten zu Verarbeitungsfehlern wegen ungültiger Schlüssel  
629 kommen kann.[ $\leq$ ,Anw\_DiGA, Anb\_IDP-D, Anb\_IDP-Sek\_KTR, digi\_ID\_OGR,  
630 Anb\_Aktensystem\_ePA, Anb\_IDP\_FedMaster,organ./betriebl. Eignung: Anbietererklärung]

631  
632 **Es wird Kapitel "4.2.1 Organisatorische Prozesse am Federation Master" neu erstellt:**

633 Folgende Anforderungen werden dem Kapitel zugeordnet

- 634 • A\_22945 - Schlüssel für Certificate Transparency TLS-Zertifikate übergeben
- 635 • A\_22968 - Maßnahmen bei nicht erfolgreicher TLS-Zertifikatsprüfung durch den
- 636 Federation Master

637 **Es wird Kapitel "4.3 Allgemeine Sicherheitsanforderungen" neu erstellt:**

638 Alt:

639 **A\_22678 -Schützenswerte Objekte**

640 Der Anbieter des Federation Master MUSS die folgenden kryptographischen Objekte als  
641 schützenswerte Objekte in seinem Sicherheitskonzept berücksichtigen:

- 642 • Privater Schlüssel und öffentlicher Schlüssel des Federation Master
- 643 • Öffentliche Schlüssel von registrierten Clients
- 644 • Authentisierungsinformationen von Löschberechtigten
- 645 • Dokumentation über beauftragte und durchgeführte Löschungen
- 646 • Statusinformationen

- Authentisierungsinformationen zur Authentisierung von internen Akteuren bzw. Rollen
- Protokolldaten
- Konfigurationsdaten.

【<=,Anb\_IDP\_FedMaster,Sich.techn. Eignung: Gutachten (Anbieter)】

## redaktionell

### Neu:

#### **A\_22678-01 -Schützenswerte Objekte**

Anbieter des Federation Master **oder von Intermediates MÜSSEN** die folgenden kryptographischen Objekte als schützenswerte Objekte in seinem Sicherheitskonzept berücksichtigen:

- Privater Schlüssel und öffentlicher Schlüssel des Federation Master **oder Intermediate**
- Öffentliche Schlüssel von registrierten Clients
- Authentisierungsinformationen von Löschberechtigten
- Dokumentation über beauftragte und durchgeführte Löschungen
- Statusinformationen
- Authentisierungsinformationen zur Authentisierung von internen Akteuren bzw. Rollen
- Protokolldaten
- Konfigurationsdaten

【<=,Anb\_IDP\_FedMaster,Sich.techn. Eignung: Gutachten (Anbieter)】

### Alt:

#### **A\_22601 -Federation Master - Berücksichtigung OWASP-Top-10-Risiken**

Der Anbieter des Federation Master MUSS Maßnahmen zum Schutz sowohl vor den zum Zulassungszeitpunkt aktuellen OWASP-Top-10-Risiken umsetzen, als auch die nach dem Zulassungszeitpunkt jeweils aktuellen OWASP-Top-10-Risiken berücksichtigen.

【<=,Anb\_IDP\_FedMaster,Sich.techn. Eignung: Gutachten (Anbieter)】

## redaktionell

### Neu:

#### **A\_22601-01 -Berücksichtigung OWASP-Top-10-Risiken**

Anbieter des Federation Master **oder von Intermediates MÜSSEN** Maßnahmen zum Schutz sowohl vor den zum Zulassungszeitpunkt aktuellen OWASP-Top-10-Risiken umsetzen, als auch die nach dem Zulassungszeitpunkt jeweils aktuellen OWASP-Top-10-Risiken berücksichtigen.【<=,Anb\_IDP\_FedMaster,Sich.techn. Eignung: Gutachten (Anbieter)】

Es wird Kapitel "4.4 Sicherheit der Netzübergänge" neu erstellt:

### Alt:

#### **A\_22591 -Federation Master - Sicherung zum Transportnetz Internet durch Paketfilter**

Der Anbieter des Federation Master MUSS dafür sorgen, dass das Transportnetz Internet durch einen Paketfilter (ACL) gesichert wird und ausschließlich die erforderlichen

Protokolle weiterleitet. Der Anbieter des Federation Master MUSS dafür sorgen, dass der Paketfilter des Federation Master frei konfigurierbar auf der Grundlage von Informationen aus OSI-Layer 3 und 4 ist (Quell- und Zieladresse, IP-Protokoll sowie Quell- und Zielport).  
[<=,Anb\_IDP\_FedMaster,Sich.techn. Eignung: Gutachten (Anbieter)]

## redaktionell

### Neu:

#### **A\_22591-01 -Sicherung zum Transportnetz Internet durch Paketfilter**

Anbieter des Federation Master **oder von Intermediates MÜSSEN** dafür sorgen, dass das Transportnetz Internet durch einen Paketfilter (ACL) gesichert wird und ausschließlich die erforderlichen Protokolle weiterleitet. Der Anbieter des Federation Master MUSS dafür sorgen, dass der Paketfilter des Federation Master frei konfigurierbar auf der Grundlage von Informationen aus OSI-Layer 3 und 4 ist (Quell- und Zieladresse, IP-Protokoll sowie Quell- und Zielport). [ <=,Anb\_IDP\_FedMaster,Sich.techn. Eignung: Gutachten (Anbieter)]

### Alt:

#### **A\_22592 -Federation Master - Platzierung des Paketfilters Internet**

Der Anbieter des Federation Master DARF den Paketfilter des Federation Master zum Schutz in Richtung Transportnetz Internet NICHT physisch auf dem vorgeschalteten TLS-terminierenden Load Balancer implementieren. [ <=,Anb\_IDP\_FedMaster,Sich.techn. Eignung: Gutachten (Anbieter)]

## redaktionell

### Neu:

#### **A\_22592-01 -Platzierung des Paketfilters Internet**

Anbieter des Federation Master **oder von Intermediates DÜRFEN** den Paketfilter des Federation Master zum Schutz in Richtung Transportnetz Internet NICHT physisch auf dem vorgeschalteten TLS-terminierenden Load Balancer implementieren.  
[ <=,Anb\_IDP\_FedMaster,Sich.techn. Eignung: Gutachten (Anbieter)]

### Alt:

#### **A\_22593 -Federation Master-Anbieter - Richtlinien für den Paketfilter zum Internet**

Der Anbieter des Federation Master MUSS beim Paketfilter die Weiterleitung von IP-Paketen an der Schnittstelle zum Internet auf das HTTPS-Protokoll beschränken.  
[ <=,Anb\_IDP\_FedMaster,Sich.techn. Eignung: Gutachten (Anbieter)]

## redaktionell

### Neu:

#### **A\_22593-01 -Richtlinien für den Paketfilter zum Internet**

Anbieter des Federation Master **oder von Intermediates MÜSSEN** beim Paketfilter die Weiterleitung von IP-Paketen an der Schnittstelle zum Internet auf das HTTPS-Protokoll beschränken. [ <=,Anb\_IDP\_FedMaster,Sich.techn. Eignung: Gutachten (Anbieter)]

### Alt:

**A\_22594 -Federation Master - Verhalten bei Vollauslastung**

Der Anbieter des Federation Master MUSS den Paketfilter des Federation Master so konfigurieren, dass bei Vollauslastung der Systemressourcen im Federation Master keine weiteren Verbindungen angenommen werden. [≤,Anb\_IDP\_FedMaster,Sich.techn. Eignung: Anbietererklärung]

**redaktionell**

Neu:

**A\_22594-01 -Verhalten bei Vollauslastung**

Anbieter des Federation Master **oder von Intermediates MÜSSEN** den Paketfilter des Federation Master so konfigurieren, dass bei Vollauslastung der Systemressourcen im Federation Master keine weiteren Verbindungen angenommen werden.  
[≤,Anb\_IDP\_FedMaster,Sich.techn. Eignung: Anbietererklärung]

Alt:

**A\_22589 -Richtlinien zum TLS-Verbindungsaufbau**

Der Anbieter des Federation Master MUSS dafür sorgen, dass der Eingangspunkt des Federation Master sich beim TLS-Verbindungsaufbau über das Transportnetz gegenüber dem Client mit einem TLS-Zertifikat eines Herausgebers gemäß [CAB-Forum] authentisiert.

Der Anbieter des Federation Master MUSS die TLS-Zertifikate aus einer CA beziehen, welche Certificate Transparency gemäß RFC 6962 / RFC 9162 unterstützt und täglich prüfen und sicherstellen, dass für seine Domänen keine unbekannten Zertifikate im Certificate Transparency Log gelistet werden.

Der Anbieter des Federation Master MUSS für seine TLS-Zertifikate Certification Authority Authorization (CAA) DNS Resource Records nach RFC 6844 bereitstellen, welche die Validität der ausstellenden CA verifizieren. [≤,Anb\_IDP\_FedMaster,Sich.techn. Eignung: Gutachten (Anbieter)]

**redaktionell**

Neu:

**A\_22589-01 -Richtlinien zum TLS-Verbindungsaufbau**

Anbieter des Federation Master **oder von Intermediates MÜSSEN** dafür sorgen, dass der Eingangspunkt des Federation Masteroder Intermediate sich beim TLS-Verbindungsaufbau über das Transportnetz gegenüber dem Client mit einem TLS-Zertifikat eines Herausgebers gemäß [CAB-Forum] authentisiert.

Anbieter des Federation Master **oder von Intermediates MÜSSEN** die TLS-Zertifikate aus einer CA beziehen, welche Certificate Transparency gemäß RFC 6962 / RFC 9162 unterstützt und täglich prüfen und sicherstellen, dass für seine Domänen keine unbekannten Zertifikate im Certificate Transparency Log gelistet werden.

Anbieter des Federation Master **oder von Intermediates MÜSSEN** für seine TLS-Zertifikate Certification Authority Authorization (CAA) DNS Resource Records nach RFC 6844 bereitstellen, welche die Validität der ausstellenden CA verifizieren.  
[≤,Anb\_IDP\_FedMaster,Sich.techn. Eignung: Gutachten (Anbieter)]

Es wird Kapitel "4.5 Fehlermeldungen" neu erstellt:

Alt:

**A\_22595 -Format der Fehlermeldungen**



Der Federation Master MUSS für die verschiedenen Teilfunktionen geeignete Fehlermeldungen erzeugen und diese an den jeweiligen Aufrufer übergeben. Die Festlegungen im Standard [OpenID Federation 1.0] MÜSSEN bei der Definition der Meldungsinhalte berücksichtigt werden. [≤, IDP\_FedMaster, funkt. Eignung: Herstellererklärung, Sich.techn. Eignung: Herstellererklärung]

#### **redaktionell**

##### Neu:

#### **A\_22595-01 -Format der Fehlermeldungen**

Federation Master und Intermediate MÜSSEN für die verschiedenen Teilfunktionen geeignete Fehlermeldungen erzeugen und diese an den jeweiligen Aufrufer übergeben. Die Festlegungen im Standard [OpenID Federation 1.1] MÜSSEN bei der Definition der Meldungsinhalte berücksichtigt werden. [≤, IDP\_FedMaster, Sich.techn. Eignung: Herstellererklärung]

##### Alt:

#### **A\_22596 -Nutzung von eindeutigen Error-Codes bei der Erstellung von Fehlermeldungen**

Der Federation Master MUSS Fehler durch eine eindeutige Nummer erkennbar machen und der gematik eine Liste der Error-Codes zur Verfügung stellen, damit die Ursachenklärung vereinfacht möglich wird. Die Festlegungen im Standard [OpenID Connect Federation 1.0] MÜSSEN bei der Definition der Fehlercodes berücksichtigt werden. [≤, IDP\_FedMaster, funkt. Eignung: Herstellererklärung, Sich.techn. Eignung: Herstellererklärung]

#### **redaktionell**

##### Neu:

#### **A\_22596-01 -Nutzung von eindeutigen Error-Codes bei der Erstellung von Fehlermeldungen**

Federation Master und Intermediate MÜSSEN Fehler durch eine eindeutige Nummer erkennbar machen und der gematik eine Liste der Error-Codes zur Verfügung stellen, damit die Ursachenklärung vereinfacht möglich wird. Die Festlegungen im Standard [OpenID Federation 1.1] MÜSSEN bei der Definition der Fehlercodes berücksichtigt werden. [≤, IDP\_FedMaster, Sich.techn. Eignung: Herstellererklärung]

##### Alt:

#### **A\_22597 -Verwendung eines einheitlichen Schemas für die Aufbereitung von Fehlermeldungen**

Der Federation Master MUSS alle ausgeworfenen Fehlermeldungen zur Weiterverarbeitung in einem einheitlichen Schema aufbereiten und bereitstellen. Zeitstempel MÜSSEN auf der UTC basieren. [≤, IDP\_FedMaster, funkt. Eignung: Herstellererklärung, Sich.techn. Eignung: Herstellererklärung]

#### **redaktionell**

##### Neu:

#### **A\_22597-01 -Verwendung eines einheitlichen Schemas für die Aufbereitung von Fehlermeldungen**

Federation Master und Intermediate MÜSSEN alle ausgeworfenen Fehlermeldungen zur Weiterverarbeitung in einem einheitlichen Schema aufbereiten und bereitstellen.

Zeitstempel MÜSSEN auf der UTC basieren.  
[<=,IDP\_FedMaster,Sich.techn. Eignung: Herstellererklärung]

Alt:

#### **A\_22598 -Formulierung der Fehlermeldungen**

Der Federation Master MUSS Fehlermeldungen, welche dem Nutzer angezeigt werden, in der Art ausformulieren, dass es dem Nutzer möglich ist, eigenes Fehlverhalten anhand der Fehlermeldung abzustellen. [<=,IDP\_FedMaster,funkt. Eignung: Herstellererklärung, Sich.techn. Eignung: Herstellererklärung]

**redaktionell**

Neu:

#### **A\_22598-01 -Formulierung der Fehlermeldungen**

Federation Master **und Intermediate MÜSSEN** Fehlermeldungen, welche dem Nutzer angezeigt werden, in der Art ausformulieren, dass es dem Nutzer möglich ist, eigenes Fehlverhalten anhand der Fehlermeldung abzustellen. [<=,IDP\_FedMaster,Sich.techn. Eignung: Herstellererklärung]

Alt:

#### **A\_22599 -Nutzung einer eindeutigen Beschreibung beim Aufbau von Fehlermeldungen**

Der Federation Master MUSS jedem Fehler eine eindeutige eigene Beschreibung zukommen lassen, sodass eine Fehlermeldung nicht für unterschiedliche Fehlerursachen zur Anwendung kommt. [<=,IDP\_FedMaster,funkt. Eignung: Herstellererklärung, Sich.techn. Eignung: Herstellererklärung]

**redaktionell**

Neu:

#### **A\_22599-01 -Nutzung einer eindeutigen Beschreibung beim Aufbau von Fehlermeldungen**

Federation Master **und Intermediate MÜSSEN** jedem Fehler eine eindeutige eigene Beschreibung zukommen lassen, sodass eine Fehlermeldung nicht für unterschiedliche Fehlerursachen zur Anwendung kommt. [<=,IDP\_FedMaster,Sich.techn. Eignung: Herstellererklärung]

Alt:

#### **A\_22600 -Ausgabe der Fehlermeldungen in umgekehrter Reihenfolge des Auftretens**

Der Federation Master MUSS aufeinander aufbauende Fehlermeldungen in der umgekehrten Reihenfolge ihres Auftretens "Traceback (most recent call last)" ausgeben. [<=,IDP\_FedMaster,funkt. Eignung: Herstellererklärung, Sich.techn. Eignung: Herstellererklärung]

**redaktionell**

Neu:



**A\_22600-01 -Ausgabe der Fehlermeldungen in umgekehrter Reihenfolge des Auftretens**

Federation Master und Intermediate MÜSSEN aufeinander aufbauende Fehlermeldungen in der umgekehrten Reihenfolge ihres Auftretens "Traceback (most recent call last)" ausgeben. [≤, IDP\_FedMaster, Sich. techn. Eignung: Herstellererklärung]

## 3 Änderungen in Steckbriefen

### 3.1 Änderungen in gemProdT\_IDP\_FedMaster

**Tabelle 19: Anforderungen zur funktionalen Eignung  
"Produkttest/Produktübergreifender Test"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
AF_10101-01	Bereitstellung von Informationen zu Teilnehmern der Föderation durch den Federation Master	gemSpec_IDP_FedMaster
AF_10101-02	Bereitstellung von Informationen zu Teilnehmern der Föderation durch den Federation Master	gemSpec_IDP_FedMaster
A_22604	Verwendung eindeutiger URI	gemSpec_IDP_FedMaster
A_22605	Entity Statement Veröffentlichung	gemSpec_IDP_FedMaster
A_22607	Inhalte des Federation Master Entity Statement	gemSpec_IDP_FedMaster
A_22607-01	Entity Configuration Inhalte des Federation Master oder Intermediate	gemSpec_IDP_FedMaster
A_22608	Inhalte des Metadata Federation API-Endpunkt im Federation Master Entity Statement	gemSpec_IDP_FedMaster
A_22948	Aktualisierungszyklen der Entity Statements Federation Master	gemSpec_IDP_FedMaster
A_22949	Aktualisierungszyklen der Entity Statements zu Teilnehmern der Föderation	gemSpec_IDP_FedMaster
A_23087	Entity Statements gelöschter Teilnehmer	gemSpec_IDP_FedMaster
A_23087-01	Entity Statements gelöschter Teilnehmer	gemSpec_IDP_FedMaster
A_28912	Gefilterte Suche nach entity_type	gemSpec_IDP_FedMaster
A_28985	Ausstellen einer Trust Mark als Nachweis der Teilnehmer Registrierung	gemSpec_IDP_FedMaster
A_28987	TI-Trust Chain Resolver	gemSpec_IDP_FedMaster

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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_28848	Validierung der Vertrauenskette eines TI-Föderation Teilnehmers	gemSpec_IDP_FedMaster

**Tabelle 21: Anforderungen zur funktionale Eignung "Herstellererklärung"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_28857	Maximale Gültigkeitsdauer und Regelmäßige Erneuerung des Entity Statement eines TI-Föderation Teilnehmers	gemSpec_IDP_FedMaster
A_28986	Teilnehmer Registrierung ausschließlich ZETA-TI-Authorization Server	gemSpec_IDP_FedMaster
A_29019	Abruf eines Subordinate Statements abweichend von OpenID Federation 1.1 (befristet)	gemSpec_IDP_FedMaster

**Tabelle 22: Anforderungen zur sicherheitstechnische Eignung "Herstellererklärung"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_22595	Format der Fehlermeldungen	gemSpec_IDP_FedMaster
A_22595-01	Format der Fehlermeldungen	gemSpec_IDP_FedMaster
A_22596	Nutzung von eindeutigen Error-Codes bei der Erstellung von Fehlermeldungen	gemSpec_IDP_FedMaster
A_22596-01	Nutzung von eindeutigen Error-Codes bei der Erstellung von Fehlermeldungen	gemSpec_IDP_FedMaster
A_22597	Verwendung eines einheitlichen Schemas für die Aufbereitung von Fehlermeldungen	gemSpec_IDP_FedMaster
A_22597-01	Verwendung eines einheitlichen Schemas für die Aufbereitung von Fehlermeldungen	gemSpec_IDP_FedMaster
A_22598	Formulierung der Fehlermeldungen	gemSpec_IDP_FedMaster
A_22598-01	Formulierung der Fehlermeldungen	gemSpec_IDP_FedMaster
A_22599	Nutzung einer eindeutigen Beschreibung beim Aufbau von Fehlermeldungen	gemSpec_IDP_FedMaster

A_22599-01	Nutzung einer eindeutigen Beschreibung beim Aufbau von Fehlermeldungen	gemSpec_IDP_FedMaster
A_22600	Ausgabe der Fehlermeldungen in umgekehrter Reihenfolge des Auftretens	gemSpec_IDP_FedMaster
A_22600-01	Ausgabe der Fehlermeldungen in umgekehrter Reihenfolge des Auftretens	gemSpec_IDP_FedMaster
A_22949-01	Aktualisierungszyklen der Subordinate Statements zu Teilnehmern der Föderation	gemSpec_IDP_FedMaster

### 3.2 Änderungen in gemAnbT\_IDP\_FedMaster

**Tabelle 23: Anforderungen zur betrieblichen Eignung "Anbietererklärung"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_22606	Entity Statement - Prüfung der angebotenen URL	gemSpec_IDP_FedMaster
A_22606-01	Entity Statement - Prüfung der angebotenen URL	gemSpec_IDP_FedMaster
A_22675-02	Teilnehmerregistrierung am Federation Master	gemSpec_IDP_FedMaster
A_22677	Teilnehmer am Federation Master löschen	gemSpec_IDP_FedMaster
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

**Tabelle 24: Anforderungen zur sicherheitstechnische Eignung "Anbietererklärung"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_22594-01	Verhalten bei Vollauslastung	gemSpec_IDP_FedMaster
A_22675-03	Teilnehmerregistrierung am Federation Master und Intermediate	gemSpec_IDP_FedMaster
A_22677-01	Teilnehmer am Federation Master oder Intermediate löschen	gemSpec_IDP_FedMaster
A_25414-	Prüfung der Entity Statements von Fachdiensten	gemSpec_IDP_FedMaster

01		
A_25414-02	Prüfung der Entity Statements von Fachdiensten	gemSpec_IDP_FedMaster
A_25415	Entsperren eines gesperrten Fachdienstes in der TI-Föderation	gemSpec_IDP_FedMaster
A_22594	Federation Master - Verhalten bei Vollauslastung	gemSpec_IDP_FedMaster

**Tabelle 25: Anforderungen zur sicherheitstechnische Eignung "Gutachten (Anbieter)"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_22591	Federation Master - Sicherung zum Transportnetz Internet durch Paketfilter	gemSpec_IDP_FedMaster
A_22591-01	Federation Master - Sicherung zum Transportnetz Internet durch Paketfilter	gemSpec_IDP_FedMaster
A_22592	Federation Master - Platzierung des Paketfilters Internet	gemSpec_IDP_FedMaster
A_22592-01	Platzierung des Paketfilters Internet	gemSpec_IDP_FedMaster
A_22593	Federation Master-Anbieter - Richtlinien für den Paketfilter zum Internet	gemSpec_IDP_FedMaster
A_22593-01	Richtlinien für den Paketfilter zum Internet	gemSpec_IDP_FedMaster
A_22598	Richtlinien zum TLS-Verbindungsaufbau	gemSpec_IDP_FedMaster
A_22598-01	Richtlinien zum TLS-Verbindungsaufbau	gemSpec_IDP_FedMaster
A_22601	Federation Master - Berücksichtigung OWASP-Top-10-Risiken	gemSpec_IDP_FedMaster
A_22601-01	Federation Master - Berücksichtigung OWASP-Top-10-Risiken	gemSpec_IDP_FedMaster
A_22678	Schützenswerte Objekte	gemSpec_IDP_FedMaster
A_22678-01	Schützenswerte Objekte	gemSpec_IDP_FedMaster