

1
2
3
4
5
6
7
8
9
10

11 **Elektronische Gesundheitskarte und Telematikinfrastruktur**

12
13
14
15
16
17
18
19

20 **Spezifikation**
21 **Federation Master**

22
23
24
25
26
27

Version: [1.1.0-0-CC2](#)
Revision: [477811495733](#)
Stand: [11.0730.09.2022](#)
Status: zur Abstimmung freigegeben
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemSpec_IDP_FedMaster

28
29

30

Dokumentinformationen

Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

34

35

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0 CC	11.07.22		initiale Erstellung des Dokuments	gematik
1.1.0 CC2	30.09.22		Kommentierung und Stellungnahmen	gematik

37

38

39

40

Inhaltsverzeichnis

41	1 Einordnung des Dokuments	6
42	1.1 Zielsetzung	6
43	1.2 Zielgruppe	6
44	1.3 Geltungsbereich	6
45	1.4 Abgrenzungen	7
46	1.5 Methodik	7
47	1.5.1 Anforderungen	7
48	1.5.2 Anwendungsfälle und Akzeptanzkriterien	8
49	1.5.3 Hinweise	8
50	2 Systemüberblick	9
51	2.1 Allgemeiner Überblick	9
52	2.2 Detaillierter Überblick	11
53	2.3 Akteure und Rollen	15
54	2.4 Begriffsdefinition	17
55	3 Funktionsmerkmale	19
56	3.1 Anwendungsfälle	19
57	3.2 Anwendungsfall – IDP-Liste bereitstellen	23
58	3.2.1 Akzeptanzkriterien – IDP-Liste bereitstellen	28
59	3.3 Anwendungsfall – Entity Statement bereitstellen	28
60	3.3.1 Akzeptanzkriterien – Entity Statement bereitstellen	34
61	3.4 Anwendungsfall – Schlüssel verwalten	35
62	3.4.1 Akzeptanzkriterien – Schlüssel verwalten	38
63	4 Anforderungen an den Produkttyp	39
64	4.1 Aufbau und Inhalt des Federation Master Entity Statement	39
65	4.2 Organisatorische Prozesse am Federation Master	41
66	4.3 Betrieblichen Anforderungen	43
67	4.4 Allgemeine Sicherheitsanforderungen	43
68	4.5 Sicherheit der Netzübergänge	44
69	4.6 Fehlermeldungen	45
70	5 Anhang – Verzeichnisse	46
71	5.1 Abkürzungen	46
72	5.2 Glossar	46
73	5.3 Abbildungsverzeichnis	49
74	5.4 Tabellenverzeichnis	49

75	5.5 Referenzierte Dokumente	51
76	5.5.1 Dokumente der gematik.....	51
77	5.5.2 Weitere Dokumente.....	52
78	1 Einordnung des Dokuments	6
79	1.1 Zielsetzung	6
80	1.2 Zielgruppe	6
81	1.3 Geltungsbereich	6
82	1.4 Abgrenzungen	7
83	1.5 Methodik	7
84	1.5.1 Anforderungen.....	7
85	1.5.2 Anwendungsfälle und Akzeptanzkriterien.....	8
86	1.5.3 Hinweise	8
87	2 Systemüberblick	9
88	2.1 Allgemeiner Überblick	9
89	2.2 Detaillierter Überblick	11
90	2.3 Akteure und Rollen	15
91	2.4 Attributbeschreibung	17
92	3 Funktionsmerkmale	19
93	3.1 Anwendungsfälle	19
94	3.2 Anwendungsfall - IDP-Liste bereitstellen	23
95	3.2.1 Akzeptanzkriterien - IDP-Liste bereitstellen	28
96	3.3 Anwendungsfall - Entity Statement bereitstellen	28
97	3.3.1 Akzeptanzkriterien - Entity Statement bereitstellen	34
98	3.4 Anwendungsfall - Schlüssel verwalten	35
99	3.4.1 Akzeptanzkriterien - Schlüssel verwalten.....	38
100	4 Anforderungen an den Produkttyp	39
101	4.1 Aufbau und Inhalt des Federation Master Entity Statement	39
102	4.2 Organisatorische Prozesse am Federation Master	41
103	4.3 Allgemeine Sicherheitsanforderungen	43
104	4.4 Sicherheit der Netzübergänge	44
105	4.5 Fehlermeldungen	45
106	5 Anhang – Verzeichnisse	46
107	5.1 Abkürzungen	46
108	5.2 Glossar	46
109	5.3 Abbildungsverzeichnis	49
110	5.4 Tabellenverzeichnis	49
111	5.5 Referenzierte Dokumente	51

112	5.5.1 Dokumente der gematik.....	51
113	5.5.2 Weitere Dokumente.....	52
114		
115		

116

1 Einordnung des Dokuments

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb des Produkttyps Federation Master. Der Federation Master basiert auf den Standards OpenID Connect (OIDC), Open Authorization 2.0 (OAuth 2) und JSON Web Token (JWT). Der Federation Master ist einerseits der Anker des Vertrauensbereichs der Föderation. Andererseits stellt der Federation Master Schnittstellen bereit, welche Auskunft über die in der Föderation registrierten sektoralen Identity Provider gibt. Die Kernaufgaben des Federation Master sind:

- Verwaltung der öffentlichen Schlüssel aller in der Föderation registrierten Teilnehmer (OpenID Provider-(OP) und Relying Party-(RP) gemäß Spezifikation [openid-connect-core])
- Validierung von Anfragen zu Teilnehmern über Teilnehmer der Föderation
- Bereitstellung von Schnittstellen für:
 - die Auskunft zum Federation Master (Entity Statement)
 - die Auskunft zu Teilnehmern über Teilnehmer der Föderation
 - die Auskunft über die Liste aller registrierten OpenID Provider (OP)
 - die Registrierung neuer OP und RP
 - ~~Sperrung unsicherer OP und RP~~
 - das Löschen von nicht mehr benötigten OP und RP.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter, welche die Funktionen des Produkttyps Produkttyps **Federation Master** der gematik realisieren wollen.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur (TI) des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu

151 tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder
152 Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen
153 Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik
154 GmbH übernimmt insofern keinerlei Gewährleistungen.

155 1.4 Abgrenzungen

156 Nicht Bestandteil des vorliegenden Dokumentes sind die Verfahrensschritte zur Erstellung
157 des notwendigen Schlüsselmaterials. Für die Signatur des Entity Statement wird
158 angenommen, dass die OpenID Provider (OP) und Relying Parties (RP) der Föderation
159 ihre innerhalb der TI zu verwendenden Zertifikate für die Transport Layer Security (TLS)-
160 Sicherung über zentrale Plattformdienste der TI beziehen und diese dort auch geprüft
161 werden können.

162 Als Umsetzungsleitlinie ist [OpenID Connect Core 1.0] und [OpenID Connect
163 Federation1.0] heranzuziehen. Die TI-weit übergreifenden Festlegungen – insbesondere
164 aus Dokumenten wie beispielsweise [gemSpec_Krypt] bezüglich Algorithmen und
165 Schlüsselstärken sowie [gemSpec_PKI] bezüglich zu verwendender Zertifikatstypen und
166 deren Attributausprägungen – haben Bestand, sind ebenso bindend und werden nicht in
167 diesem Dokument beschrieben.

168 Für weitere Komponenten der TI-Föderation gelten eigene Spezifikationsdokumente:

- 169 • sektorale Identity Provider - [gemSpec_IDP_Sek]
- 170 • Fachdienste - [gemSpec_IDP_FD]
- 171 • Anwendungsfrontend der Fachdienste - [gemSpec_IDP_Frontend-].

172 1.5 Methodik

173 ~~Die Spezifikation ist im Stil einer RFC Spezifikation verfasst. Dies bedeutet:-~~

- 174 • ~~Der gesamte Text in der Spezifikation ist sowohl für den Hersteller des~~
175 ~~Produktes Federation Master als auch für den betreibenden Anbieter~~
176 ~~entsprechend [gemKPT_Betr] verbindlich zu betrachten und gilt als~~
177 ~~Zulassungskriterium beim Produkt und Anbieter.~~
- 178 • ~~Die Verbindlichkeit SOLL durch die dem RFC 2119 [RFC2119] entsprechenden, in~~
179 ~~Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT,~~
180 ~~SOLL, SOLL NICHT, KANN gekennzeichnet werden.~~
- 181 • ~~Da in dem Beispielsatz „Eine leere Liste DARF NICHT ein Element besitzen.“ die~~
182 ~~Phrase „DARF NICHT“ semantisch irreführend wäre (wenn nicht ein, dann~~
183 ~~vielleicht zwei?), wird in diesem Dokument stattdessen „Eine leere Liste DARF~~
184 ~~KEIN Element besitzen.“ verwendet.~~
- 185 • ~~Die Schlüsselworte KÖNNEN außerdem um Pronomen in Großbuchstaben ergänzt~~
186 ~~werden, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.~~

187 1.5.1 Anforderungen

188 Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID in
189 eckigen Klammern sowie die dem RFC 2119 [RFC2119] entsprechenden, in

190 Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL,
191 SOLL NICHT, KANN gekennzeichnet.

192 Sie werden im Dokument wie folgt dargestellt:

193 **<AFO-ID> - <Titel der Afo>**

194 Text / Beschreibung

195 [**<=**]

196 Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und der Textmarke [**<=**]
197 angeführten Inhalte.

198

199 1.5.2 Anwendungsfälle und Akzeptanzkriterien

200 Anwendungsfälle und Akzeptanzkriterien als Ausdruck normativer Festlegungen werden
201 als Grundlage für Erlangung der Zulassung durch Tests geprüft und nachgewiesen. Sie
202 besitzen eine eindeutige, permanente ID, welche als Referenz verwendet werden SOLL.
203 Die Tests werden gegen eine von der gematik gestellte Referenz-Implementierung
204 durchgeführt.

205

206 Anwendungsfälle und Akzeptanzkriterien werden im Dokument wie folgt dargestellt:

207 **<ID> - <Titel des Anwendungsfalles / Akzeptanzkriteriums>**

208 Text / Beschreibung

209 [**<=**]

210 Die einzelnen Elemente beschreiben:

- 211 • **ID**: einen eindeutigen Identifier.
 - 212 • Bei einem Anwendungsfall besteht der Identifier aus der Zeichenfolge 'AF_'
 - 213 gefolgt von einer Zahl,
 - 214 • Der Identifier eines Akzeptanzkriteriums wird von System vergeben, z.B. die
 - 215 Zeichenfolge 'ML_' gefolgt von einer Zahl
- 216 • **Titel des Anwendungsfalles / Akzeptanzkriteriums**: Ein Titel, welcher
- 217 zusammenfassend den Inhalt beschreibt
- 218 • **Text / Beschreibung**: Ausführliche Beschreibung des Inhalts. Kann neben Text
- 219 Tabellen, Abbildungen und Modelle enthalten

220 Dabei umfasst der Anwendungsfall bzw. das Akzeptanzkriterium sämtliche zwischen ID
221 und Textmarke [**<=**] angeführten Inhalte.

222 Der für die Erlangung einer Zulassung notwendige Nachweis der Erfüllung des
223 Anwendungsfalles wird in den jeweiligen Steckbriefen festgelegt, in denen jeweils der
224 Anwendungsfall gelistet ist. Akzeptanzkriterien werden in der Regel nicht im Steckbrief
225 gelistet.

226

227 1.5.3 Hinweise

228 Hinweis auf offene Punkte

Offener Punkt: Das Kapitel wird in einer späteren Version des Dokumentes ergänzt.

229

2 Systemüberblick

230 2.1 Allgemeiner Überblick

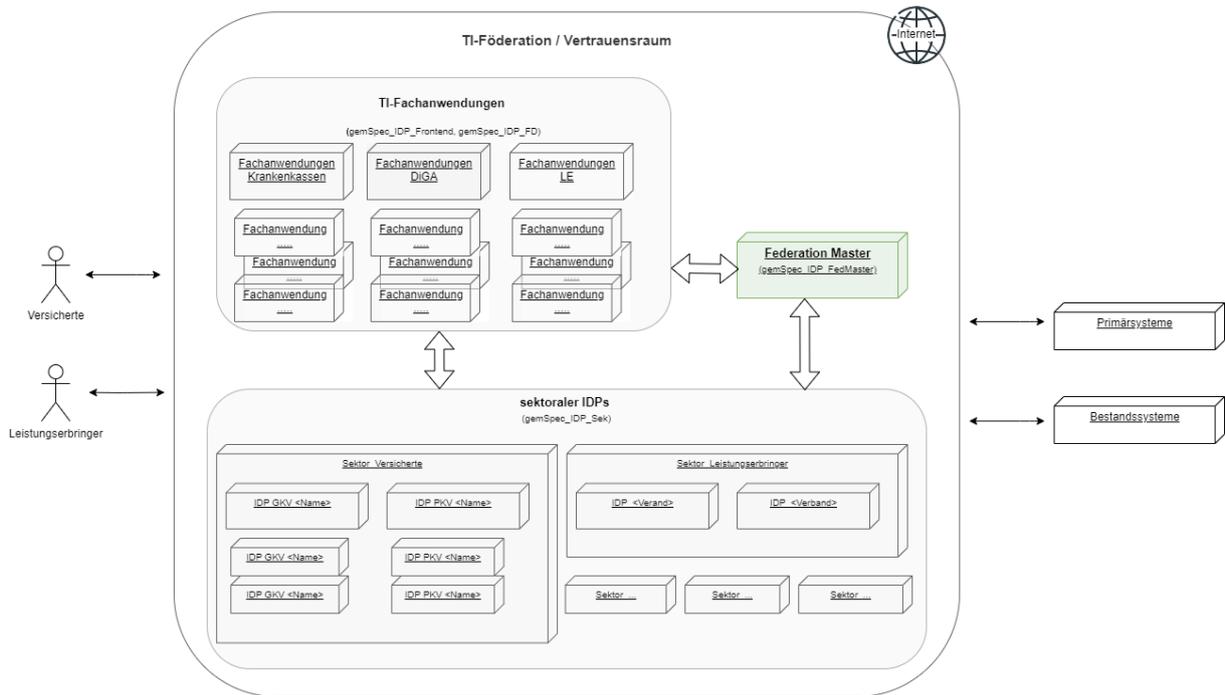
231 Zentrales Merkmal des zukünftigen Identity Management der Telematikinfrastruktur ist
232 das Prinzip der Föderation. Die Identitäten werden nicht von einem einzigen zentralen
233 Dienst bereitgestellt, sondern „kollektiv“ durch eine Menge von Identity Providern, für die
234 jeweils die entsprechenden identitätsbestätigenden Institutionen verantwortlich sind,
235 welche auch für die jeweiligen Nutzergruppen zuständig sind.

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

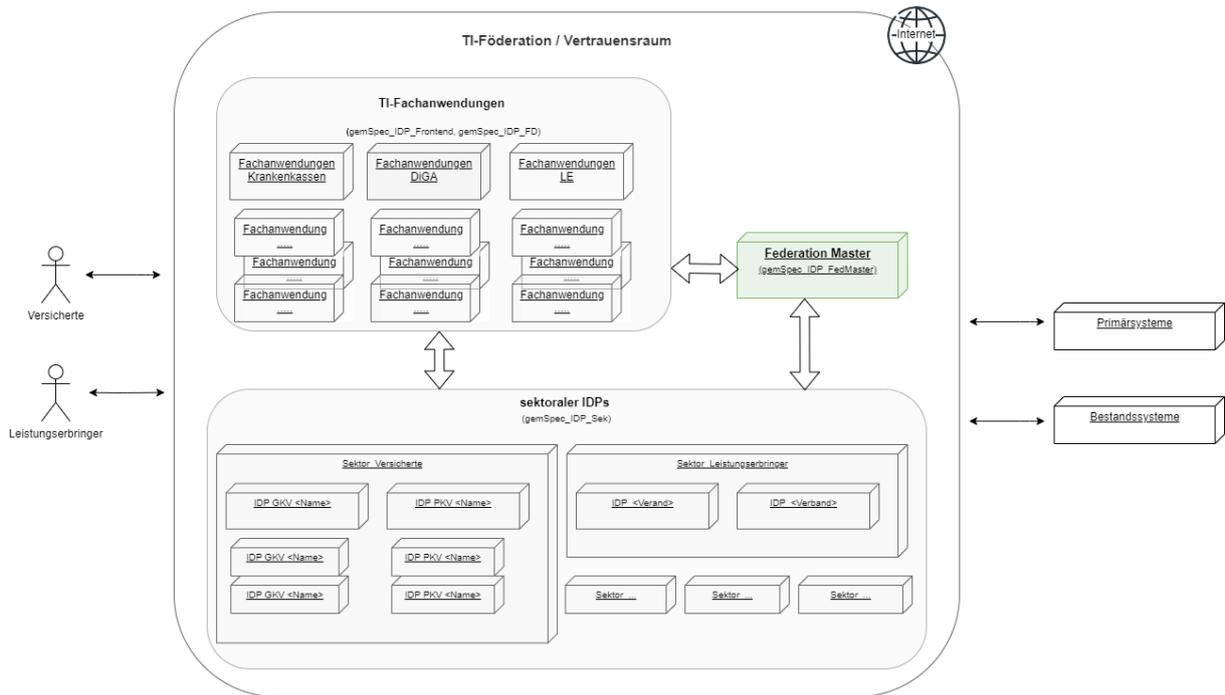
- 240 • Einheitliche Identitätsattribute für die Nutzergruppen (Minimal `claim Sets`,
241 `scopes`)
- 242 • Grundstruktur der Vertrauensbeziehungen der Föderierung (IDP Federation/Trust
243 Chains)
- 244 • Einheitliche Verfahren zum Auffinden von sektoralen Identity Providern (IDP
245 Discovery)
- 246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

247 Die Grundidee der Föderation ist die Erstellung eines Vertrauensraums, in dem
248 verschiedene Anwendungen und Identity Provider abgesichert über Vertrauensketten
249 (Trust chain) miteinander kommunizieren, ohne zuvor über organisatorische Prozesse
250 miteinander verknüpft zu werden. [Diese Anwendungen und Identity Provider werden im](#)
251 [Folgenden als Teilnehmer der Föderation bezeichnet](#). Die TI-Föderation baut auf dem
252 Standard [OpenID Connect Federation 1.0] auf. Die Autorisierung und Authentisierung
253 von Anwendungen und Nutzern orientiert sich an den Standards zu OAuth 2.0 und
254 OpenID Connect. Die für die TI zwingend notwendige Identifikation der Nutzer ist nicht
255 Teil der Spezifikation.

256



257



258

259

260

261

Abbildung 1-4: Überblick TI-Föderation

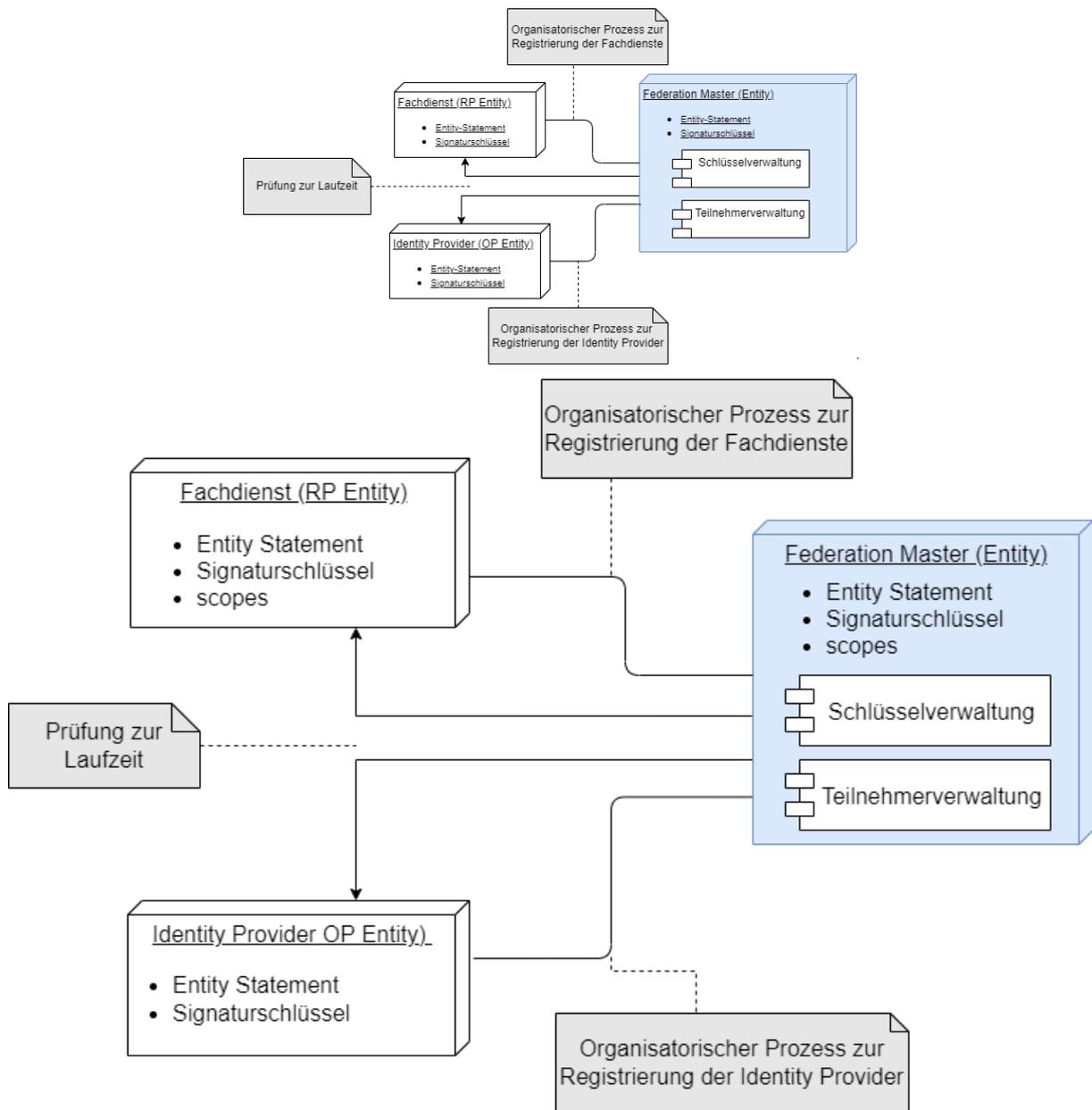
262 2.2 Detaillierter Überblick

263 Die untere Abbildung beschreibt den Systemkontext aus Sicht des Federation Master. Alle
264 sektoralen Identity Provider der Föderation müssen beim Federation Master registriert
265 sein. Ebenso müssen alle Fachanwendungen, welche die bei den Identity -Providern
266 hinterlegten digitalen Identitäten nutzen möchten, beim Federation Master registriert
267 sein. Jede teilnehmende Partei inklusive des Federation Master muss ein OpenID -
268 Connect spezifikationskonformes Entity Statement bereitstellen.

269 Die Identity -Provider der Föderation stellen sicher, dass Nutzer anfragender Fachdienste
270 identifiziert sind. Ebenso wird sichergestellt, dass die Nutzer den Anwendungen Zugriff
271 auf eine Teilmenge ihrer Daten gewähren (Consent).

272 Die in der Föderation registrierten Fachdienste nutzen die sektoralen Identity Provider,
273 um Nutzer ihrer Anwendungen über die Verfahren der sektoralen Identity
274 Provider eindeutig zu authentifizieren und die Zustimmung der Datennutzung von den
275 Nutzern einzuholen.

276



277

278

279

Abbildung 2-4: Systemkontext

280 Im Prozess der Autorisierung eines Nutzers für eine Anwendung ist der Federation Master
 281 als Vertrauensstelle eingebunden. Die Voraussetzung für die Kommunikation zwischen
 282 Fachdiensten und sektoralen Identity Providern ist deren Registrierung im
 283 Vertrauensbereich der Föderation. Diese initiale Registrierung erfolgt organisatorisch und
 284 unabhängig vom späteren Ablauf.

285 Voraussetzungen für die Prüfung der beteiligten Komponenten im Kontext eines
 286 Nutzungsflows:

- 287 • Die aktuellen Signaturschlüssel der beteiligten sektoralen Identity Provider und
 288 Fachdienste wurden über einen vom Anbieter [bereit-gestellten-bereitgestellten](#)
 289 organisatorischen Prozess beim Federation Master hinterlegt.

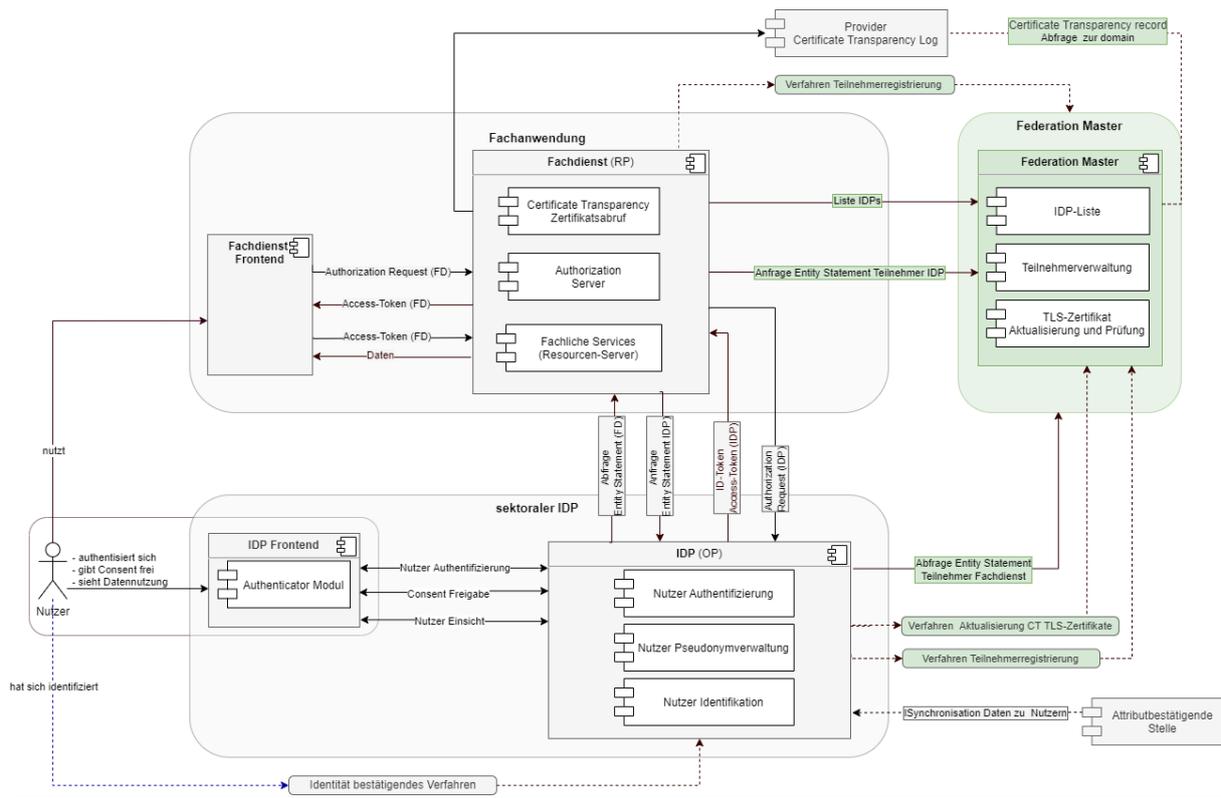


Abbildung 3: Übersichtsschaubild OIDC Federation

Erläuterungen zur obigen Abbildung:

Die grün dargestellten Komponenten und Schnittstellen sind Gegenstand der vorliegenden Spezifikation. Komponenten und Schnittstellen, welche in der Abbildung grau hinterlegt sind, werden in der vorliegenden Spezifikation nicht weiter betrachtet.

Hinter den gestrichelt dargestellten Schnittstellen verbergen sich organisatorische Prozesse und Verfahren, die anderen Schnittstellen sind Bestandteil der Abläufe zur Autorisierung und Authentifizierung eines Anwenders im Kontext einer Fachanwendung.

Die organisatorischen Prozesse dienen der Registrierung, Sperrung und Löschung von Teilnehmern der Föderation sowie der Aktualisierung der beim Federation Master hinterlegten TLS-Schlüssel der sektoralen Identity Provider.

Im Ablauf der Autorisierung und Authentifizierung eines Anwenders im Vertrauensraum der Föderation, müssen der beteiligte Fachdienst und der beteiligte sektorale Identity Provider sicherstellen, dass der jeweilige Kommunikationspartner ebenfalls ein Mitglied der Föderation ist. Diese Teilschritte sind in der Abbildung als Federation-Flow gekennzeichnet und grün hinterlegt.

Beide Komponenten laden sich dazu das Entity Statement des Federation Master zur jeweils anderen Komponente herunter unter:

GET /.well-known/openid-federation HTTP/1.1

Host: <host Teilnehmer>

Zur Verifizierung müssen die Komponenten prüfen, ob der jeweils andere Teilnehmer Teil der Föderation ist. Das Entity Statement des Federation Master (HTTP-GET <federation master>/.well-known/openid-federation HTTP/1.1) enthält die URL der API-Schnittstelle

332 des Federation Master. Die Information zu einem Teilnehmer der Föderation kann dann
 333 über die API-Schnittstelle des Federation Master geladen werden. Dabei müssen sowohl
 334 der Entity Identifier (URL) des Federation Master als auch der des Teilnehmers als
 335 Parameter übergeben werden. Der Federation Master liefert ein ~~von~~ ihm signiertes
 336 Entity Statement zum angefragten Teilnehmer zurück.

337

338 **Tabelle 1: Request zur Teilnehmerabfrage an den Federation Master**

Parameter	Beschreibung
iss (issuer)	Entity Identifier (URL) der Entity, welche angefragt wird - Federation Master
sub (subject)	Entity Identifier (URL) der Entity, nach welchewelcher gefragt wird - Teilnehmer

339

340 Jeder Teilnehmer stellt zusätzlich ein selbst signiertes Entity Statement bereit, dessen
 341 Schlüssel gegen das durch den Federation Master signierte Statement verifiziert werden.

342 2.3 Akteure und Rollen

343 **Tabelle 2: Akteure und Rollen**

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

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

2.4 Begriffsdefinition

2.4 Attributbeschreibung

Die folgende Tabelle enthält ~~die Abkürzungen welche~~ [eine Erläuterung zu den Attributen, die](#) in den Entity Statements des Federation Master verwendet werden. Die ~~Abkürzungen~~ [Attribute](#) entsprechen dem [OIDC Standard für Entity-Statements](#).

Tabelle 3: ~~Begriffsklärung~~ Attributbeschreibung

Bezeichnung	Beschreibung	Wertebereich	Beispiel
iss	issuer = URL des Federation Master	URL	"http://master0815.de"
sub	subject = Name des beauskundschaf teten DienstURL der Entity, nach welcher gefragt wird	URL	"http://master0815.de"
iat	Ausstellungszeitpunkt des Entity Statement	Alle time-Werte in Sekunden seit 1970, RFC 7519 Sect.2	1645398001 (2022-02-21 00:00:01)
exp	Ablaufzeitpunkt des Entity Statement	Alle time-Werte in Sekunden seit 1970, RFC 7519 Sect.2	1646002800 (2022-02-28 00:00:00)
jwks	Schlüssel für die Signatur des Entity Statement. Gemäß [OpenID Connect Federation 1.0#rfc.section.9.2] werden hier auch Schlüssel für einen Key-Rollover transportiert.		
authority_hints	Ausgehend von einer Entität die Liste der IDs von Identitäten in der Trust Chain bis hin zum Trust - Anchor (Federation Master). Die Liste darf nicht leer sein.		["http://idp4711.de", "http://master0815.de"]

<p><i>metadata</i></p>	<p>Metadaten zu Entities werden in Metadattentypen unterteilt. Dabei ist jeder Metadattentyp ein JSON-Objekt und hält eine Reihe von key/value-Paaren, den eigentlichen Metadaten. Wenn das <i>iss</i> einer Entity-Anweisung auf dieselbe Entität wie das <i>sub</i> verweist (z.B. beim Federation Master),^{1,2} muss die Entity-Anweisung einen Metadaten-<i>claim</i> enthalten.</p>		<pre>metadata { federation_entity { <key>:<value>, <key>:<value> } }</pre>
------------------------	---	--	--

351
 352 Anforderungen an die konkrete Belegung der Attribute im Entity Statement des
 353 Federation Master sind in [ML-127207 - Aufbau und Inhalt des Federation Master Entity](#)
 354 [Statement](#) beschrieben .

355

3 Funktionsmerkmale

3.1 Anwendungsfälle

Der Federation Master ist eine Komponente, welche in den Kommunikationsfluss bei der Nutzung von Fachdiensten der TI eingebunden ist. Zudem ist der Federation Master an notwendigen organisatorischen Prozesse beteiligt. Folgende Anwendungsfälle dienen der Beschreibung der Anforderungen an den Federation Master:

361

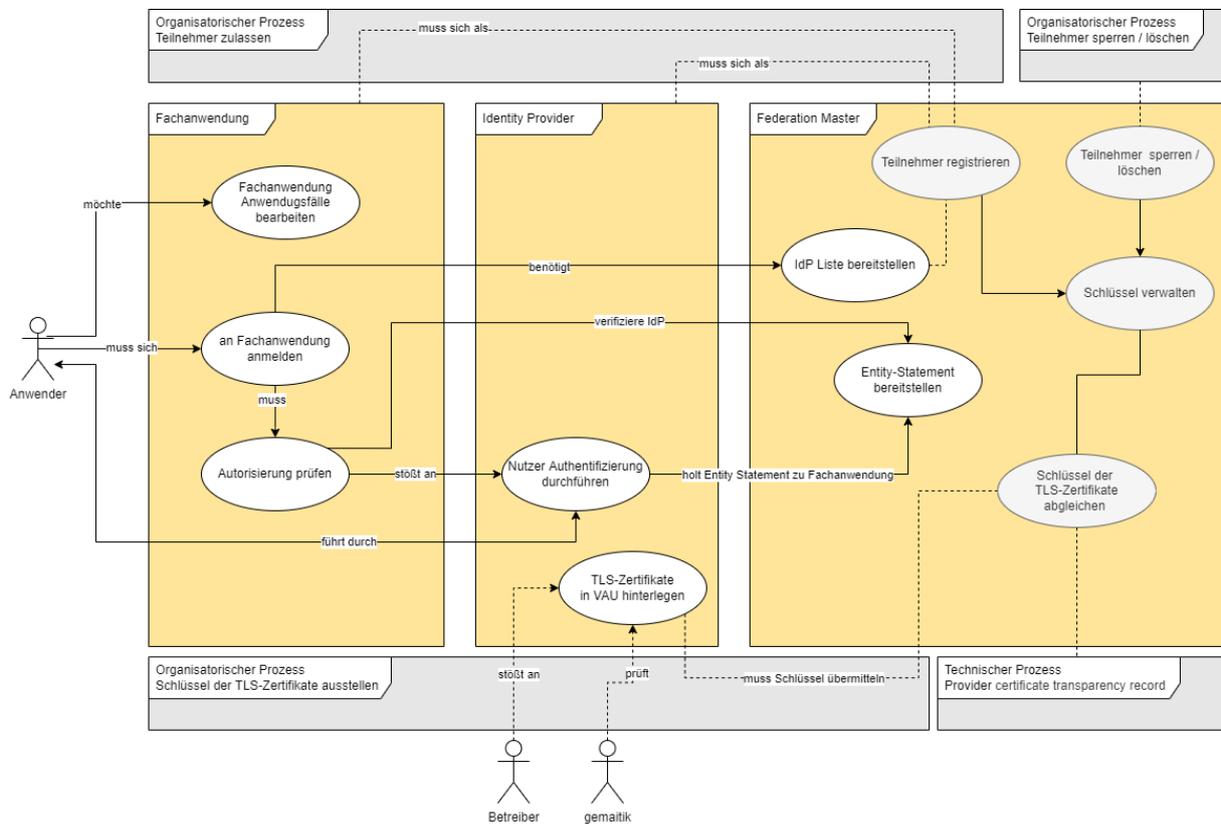
362 **Tabelle 4: Übersicht über die Anwendungsfälle im Gesamtkontext Federation Master**

Use -Case	Komponente	Kurzbeschreibung
Teilnehmer registrieren	Federation Master	Jede Fachanwendung und jeder Identity Provider muss sich als Teilnehmer beim Federation Master registrieren. Im Zuge der Registrierung wird der öffentliche Teil des Schlüssels, mit dem der Teilnehmer sein Entity Statement signiert, beim Federation Master hinterlegt. Für jede Fachanwendung wird zusätzlich hinterlegt, welche Informationen zum Nutzer (<u>scopes</u>) diese beim Identity Provider erfragen dürfen. Für jeden Identity Provider werden die Schlüssel der TLS-Verbindungen in die VAU hinterlegt.
an Fachanwendung anmelden	Fachanwendung	Der Nutzer meldet sich an einer Fachanwendung an. Fachanwendungen können z.B. Anwendungen von Krankenkassen, TI-Anwendungen –(wie <u>bspw.</u> E-Rezept, ePA oder <u>DiGAsDiGA</u>) sein. Die Anmeldung <u>soll zentral</u> für alle Anwendungen <u>erfolgt über einengenau den</u> Identity Provider <u>laufen</u> , bei dem <u>die</u> elektronische Identität <u>des</u> Nutzers hinterlegt ist. Zur Ermittlung des richtigen Identity <u>ProvidersProvider</u> wird die Liste aller in der Föderation registrierten Identity Provider vom Federation Master abgefragt. Die Auswahl trifft dann der Nutzer im Kontext der Anmeldung.
IDP-Liste bereitstellen	Federation Master	Zu allen in der Föderation registrierten Identity Providern werden die Informationen <u>Organisationsname, Logo'Organisationsname', 'Logo'</u> und <u>Zieladresse'Zieladresse</u> (URL) ermittelt und als Liste bereitgestellt.

<p>Autorisierung prüfen</p>	<p>Fachanwendung</p>	<p>Der Anwendungsfall <i>Autorisierung prüfen</i> ist ein Anwendungsfall der Fachanwendung ohne Nutzer Interaktion<i>Nutzerinteraktion</i>. In dem Anwendungsfall wird geprüft, welche fachlichen Aktionen der Nutzer in der Fachanwendung ausführen darf und welche Informationen für diese Entscheidung vom Nutzer benötigt und vom Identity Provider bezogen werden müssen.</p>
<p>Entity Statement bereitstellen</p>	<p>Federation Master</p>	<p>Der Federation Master stellt zu jedem registrierten Teilnehmer ein Entity Statement aus.</p>
<p>Nutzer authentifizieren</p>	<p>Identity Provider</p>	<p>Vor der eigentlichen Authentifizierung des Nutzers wird in diesem Anwendungsfall geprüft, ob die anfragenden<i>anfragende</i> Fachanwendung Teil der TI-Föderation ist und sie berechtigt ist, die geforderten Information<i>Informationen</i> zum Nutzer (<i>scopes, claims</i>) einzuholen. Dazu wird das Entity Statement des Fachdienstes vom Federation Master abgeholt. Die eigentliche Authentifikation des Nutzers erfolgt durch Interaktion mit dem Nutzer über das Authenticator-Modul des Identity Provider. Das Authenticator-Modul steht dem Nutzer z.B. als Funktion einer App zur Verfügung.</p>
<p>Fachanwendung_ Anwendungsfälle bearbeiten</p>	<p>Fachanwendung</p>	<p>Nach erfolgreicher Nutzer<i>Nutzerauthentifizierung</i> kann der Nutzer die Anwendungsfälle der Fachanwendung bearbeiten, für die er autorisiert ist.</p>
<p>TLS-Zertifikate in VAU hinterlegen</p>	<p>Identity Provider</p>	<p>Im Zuge der Erzeugung von TLS-Zertifikaten zu Domänen des Identity Provider wird geprüft, ob TLS-Zertifikate betroffen sind, deren Schlüssel in der VAU hinterlegt sind. Ist das der Fall, wird der Prozess von einer Prüfinstanz (z.B. gematik) überwacht. In diesem Kontext muss auch eine Aktualisierung des Schlüsselmaterials beim Federation Master erfolgen.</p>
<p>Schlüssel der TLS-Zertifikate abgleichen</p>	<p>Federation Master</p>	<p>In regelmäßigen Abständen und bei Zertifikaterstellung prüft der Federation Master die TLS-Zertifikate der in der VAU mündenden TLS-Verbindungen in der Weise, ob die öffentlichen Schlüssel der Zertifikate im Federation Master hinterlegt sind. Zur Ermittlung aller in Frage kommender TLS-Zertifikate nutzt der Federation Master öffentlich zugängliche Certificate Transparency Provider.</p>

<p>Schlüssel verwalten</p>	<p>Federation Master</p>	<p>Der Federation Master verwaltet die Schlüssel <u>und Adressen</u> der Teilnehmer <u>in einer sicheren Umgebung</u> (z.B. HSM). Der Zugriff auf die Schlüssel erfolgt ausschließlich über eine <u>vertrauenswürdige Ausführungsumgebung und beglaubigt sie gegenüber anderen Diensten</u>. Das Einbringen der <u>SchlüsselDaten</u> neuer Teilnehmer bzw. das Löschen der <u>SchlüsselDaten</u> auszuschließender Teilnehmer erfolgt über organisatorische Prozesse (Teilnehmer registrieren, Teilnehmer sperren/löschen).</p>
--------------------------------	--------------------------	--

363
364



365
366
367

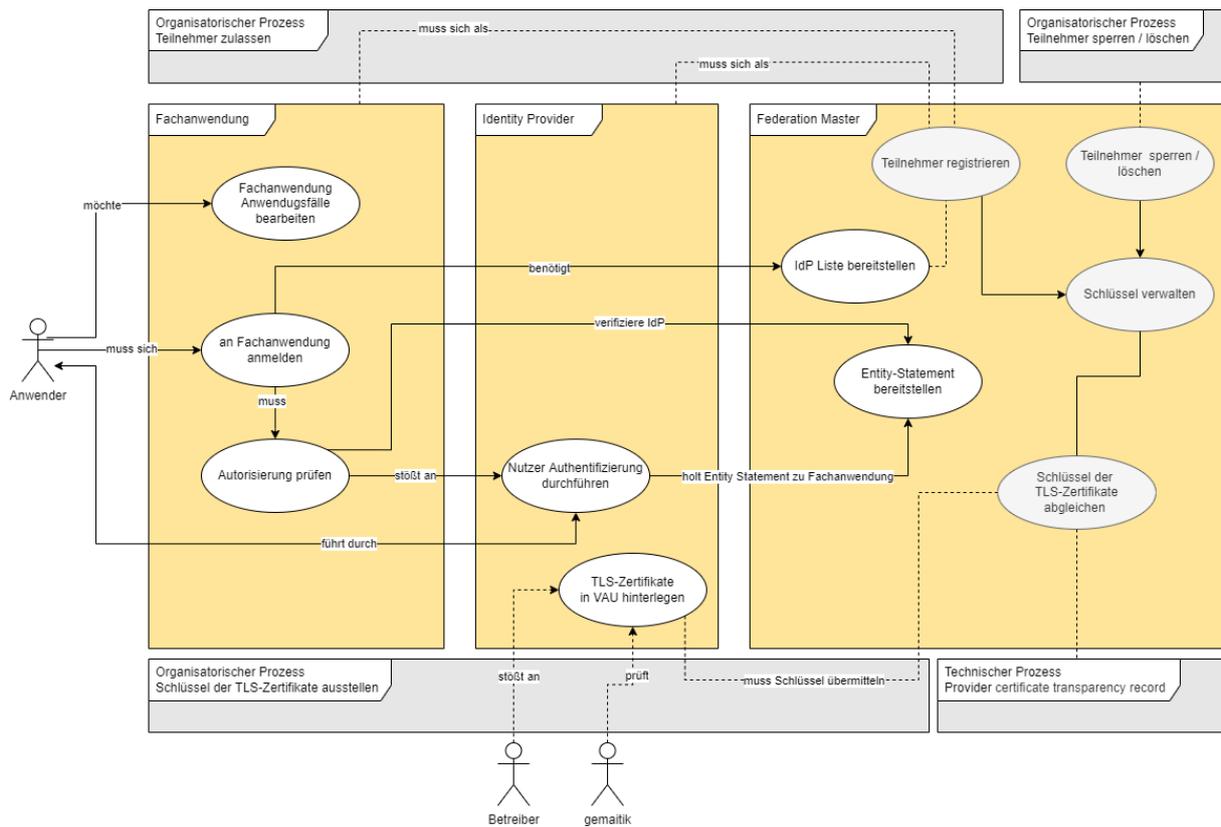


Abbildung 4-3: Anwendungsfälle Federation Master

Tabelle 5: Anwendungsfälle Federation Master

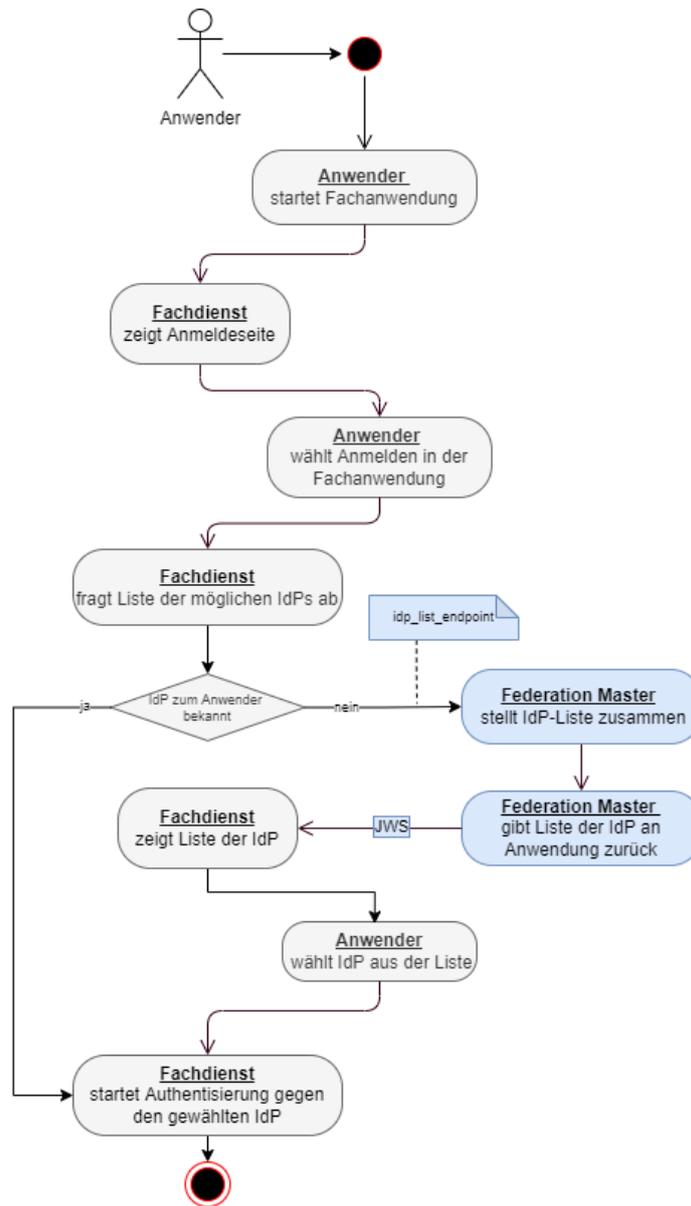
Typ	Anwendungsfall
Technisch	IDP-Liste bereitstellen
Technisch	Entity Statement bereitstellen
Technisch	Schlüssel verwalten
Technisch / Organisatorisch	Schlüssel der TLS-Zertifikate abgleichen
Organisatorisch	Teilnehmer registrieren
Organisatorisch	Teilnehmer sperren/löschen

Die technischen Anwendungsfälle des Federation Master werden hier im Detail beschrieben. Details zu den organisatorischen Anwendungsfällen des Federation Master finden sich in Kapitel 4.2: Organisatorische Prozesse am Federation Master. Die

377 Ausprägung der Anwendungsfälle anderer Komponenten spielt im Rahmen dieser
 378 Spezifikation keine Rolle.

379 **3.2 Anwendungsfall - IDP-Liste bereitstellen**

380



381

382

383

Abbildung 5-1: Aktivitätsdiagramm "Auswahl sektorale Identity Provider"

384 AF_10100 - ~~Bereitstellung Liste registrierte Identity Provider~~ Bereitstellung Liste
 385 registrierter Identity Provider

386 **Tabelle 6: Anwendungsfall "Bereitstellung Liste ~~registrierter~~ registrierter Identity**
 387 **Provider"**

Attribute	Bemerkung
Beschreibung	<p>Ein Anwender möchte einen in der TI registrierte <u>registrierten</u> Fachdienst nutzen. Der Fachdienst muss sicherstellen, dass der Anwender zur Nutzung des Dienstes berechtigt ist. Um die Berechtigung sicherzustellen, MUSS der Fachdienst die Authentifizierung des Anwenders gegenüber einem <u>seinem</u> sektoralen Identity Provider veranlassen. Dazu benötigt der Fachdienst die Information vom Anwender, gegen welchen sektoralen Identity Provider er sich identifiziert hat.</p> <p>Der Fachdienst MUSS in seinem Frontend dem Anwender eine Liste der in der TI registrierten sektoralen Identity Provider anzeigen. Diese Liste MUSS sich der Fachdienst vom Federation Master erfragen.</p> <p>Der Federation Master MUSS eine API-Schnittstelle bereitstellen, über die ein Fachdienst die Liste der in der TI registrierten sektoralen Identity Provider abfragen kann.</p> <p>Jeder Listeneintrag MUSS mindestens diese Informationen enthalten:</p> <ul style="list-style-type: none"> • eindeutige issuer-id des sektoralen Identity Provider in der TI-Föderation • Name des sektoralen Identity Provider in lesbarer Form • Logo des sektoralen Identity Provider (wenn vorhanden). <p>Der Anwender des Fachdienstes MUSS genau einen sektoralen Identity Provider aus der Liste auswählen. Der Fachdienst kann sich die Zuordnung eines Anwenders zu seinem sektoralen Identity Provider speichern, so dass die Abfrage der Liste beim Federation Master nicht bei jeder Anmeldung des Anwenders wiederholt werden muss.</p>
Akteur	Anwender der Fachanwendung
Auslöser	Ein Anwender möchte eine Gesundheitsanwendung der TI (Fachdienst) nutzen. Als Voraussetzung für die Authentifizierung des Anwenders muss dieser auswählen, bei welchem Identity Provider er registriert ist (bei Versicherten - Auswahl der Krankenkasse).
Komponenten	<ul style="list-style-type: none"> • Fachdienst der TI • Federation Master

<p>Vorbedingung</p>	<ol style="list-style-type: none"> 1. Der Fachdienst ist in der TI-Föderation registriert, sein Schlüssel ist dem Federation Master bekannt. 2. Es gibt eine Liste in der TI-Föderation registrierter (sektoraler) Identity Provider, deren Schlüssel sind dem Federation Master bekannt. 3. Der Anwender ist durch einen der (sektoraler) Identity Provider identifiziert worden. 4. Das Entity Statement des Federation Master steht zur Verfügung und die unter dem Attribut <code>idp_list_endpoint</code> benannte URL ist MUSS aus dem Internet erreichbar sein.
<p>Ablauf</p>	<ol style="list-style-type: none"> 1. Im Ablauf der Nutzung eines Fachdienstes (siehe Abbildung - Aktivitätsdiagramm "Auswahl sektoraler Identity Provider") findet eine Verzweigung zum Federation Master in dem Fall statt, wenn der Fachdienst die Zuordnung des Anwenders zu seinem IDP nicht kennt. 2. Der Fachdienst sendet einen Request an die URL, welche im Entity Statement des Federation Master unter dem Attribut <code>idp_list_endpoint</code> benannt ist. Der Federation Master nimmt den Request entgegen. 3. Der Federation Master erstellt eine Liste aller registrierten sektoralen Identity Provider. Die Liste MUSS zu jedem sektoralen Identity Provider diesen Attributen diese Attribute enthalten: <ol style="list-style-type: none"> a. Name der Organisation b. URI (client_id bzw. iss) des sektoralen Identity Provider c. Logo der Organisation d. Unterstützte Unterstützte Anwendertypen 4. 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 "<i>Liste sektorale Identity Provider - Payload-Attribute des signierten JSON-Web-Token</i>" und "<i>Liste sektorale Identity Provider - Headerattribute des signierten JSON-Web-Token</i>" aufgeführten Attribute enthalten.
<p>Ergebnis</p>	<ol style="list-style-type: none"> 1. Der Anwender hat aus der Liste der in der TI registrierten (sektoralen) Identity Provider denjenigen ausgewählt, gegenüber dem er sich zuvor identifiziert hat. 2. Der Fachdienst hat alle Informationen, um die Authentifizierung und Autorisierung durchzuführen.
<p>Akzeptanzkriterien</p>	<p> ML-128409 ,  ML-128411</p>

Alternativen	Die Fachanwendung kennt (z.B. aus früheren Sitzungen) den sektoralen Identity Provider des Anwenders. In diesem Fall KANN der Anwendungsfall ausgeführt werden.
--------------	---

388 **Tabelle 7: Liste sektorale Identity Provider - Payload-Attribute des signierten JSON-Web-**
389 **Token**

Attribut	Werte / Typ	Beispiel	Anmerkungen
iss	URL	"http://master0815.de"	URL des Federation Master
iat	Alle time-Werte in Sekunden seit 1970, RFC 7519 Sect.2	1645398001 = 2022-02-21 00:00:01	Ausstellungszeitpunkt der Liste
exp	Alle time-Werte in Sekunden seit 1970, RFC 7519 Sect.2	1645484400 = 2022-02-22 00:00:00 entspricht einer Gültigkeit von 24 Stunden in Bezug auf den Wert in iat	Ablaufzeitpunkt der Gültigkeit des Liste (maximal iat + 24 Stunden)
<i>idp_entity</i>			Der Block <i>idp_entity</i> enthält die Liste der sektoralen Identity Provider und einige Metadaten.
organization_name	String (max. 128 Zeichen)	"IDP 4711"	Der Name des sektoralen Identity Provider zur Anzeige für den Benutzer aus der Definition von "organization_name" im Entity Statement des sektoralen Identity Provider wird bei der Registrierung des sektoralen IDP dem Federation Master bekanntgegeben. Der Wert des Parameters organization_name wird bei der täglichen Abfrage des Entity Statement überprüft und ggf. geändert.
iss	URI	"https://idp4711.de"	issuer-Wert des jeweiligen sektoralen Identity Provider (URL) - sollte nach Vorgaben der Föderation der Adresse für die Authentisierung

			entsprechen und wird bei der Registrierung des sektoralen IDP dem Federation Master bekanntgegeben.
logo_uri	URI	"https://idp4711.de/logo.png"	Der Parameter "logo_uri" aus dem Entity Statement des sektoralen Identity Provider wird bei der Registrierung des sektoralen IDP dem Federation Master bekanntgegeben. Der Wert des Parameters logo_uri wird bei der täglichen Abfrage des Entity Statement überprüft und ggf. geändert.
user_type_supported	[HCI = Health Care Institution, HP = Health Professional, IP = Insured Person]	"IP"	Der Parameter "user_type_supported" aus dem Entity Statement des sektoralen Identity Provider wird bei der Registrierung des sektoralen IDP dem Federation Master bekanntgegeben. Eine tägliche Aktualisierung über das Entity Statement des IDP ist nicht notwendig.

390
391 Folgende Werte müssen Bestandteil des Header der vom Federation Master signierten
392 IDP-Liste sein:
393

394 **Tabelle 8: Liste sektorale Identity Provider - Headerattribute des signierten JSON-Web-**
395 **Token**

Name	Werte	Beispiel	Anmerkungen
alg	ES256		
kid	wie aus jwks im Body des Entity Statement		Identifiziert den verwendeten Schlüssel aus dem jwks im Body des Entity Statement des Federation Master
typ	JWT		

396 [**<=**]

397 3.2.1 Akzeptanzkriterien - IDP-Liste bereitstellen

398 ML-128409 - ~~AF_10100~~ ~~Unter idp_list_endpoint benannte URL ist erreichbar~~
399 ~~und liefert signiertes JWS als Response~~

400 Der Request vom Fachdienst an URL, welche im Entity Statement des Federation Master
401 unter dem Attribut `idp_list_endpoint` benannt ist, wird entgegengenommen und gibt
402 als Response ein signiertes JWS zurück. Das Token ist mit dem privaten Schlüssel des
403 Federation Master signiert und kann vom Fachdienst mit dem öffentlichen Schlüssel des
404 Federation Master ~~entschlüsselt~~ verifiziert werden. [~~=~~]

405

406

407

408 ML-128411 - ~~AF_10100~~ ~~Payload des JWS-Token enthält Informationen zu~~
409 ~~jedem registrierten sektoralen Identity Provider der Föderation~~

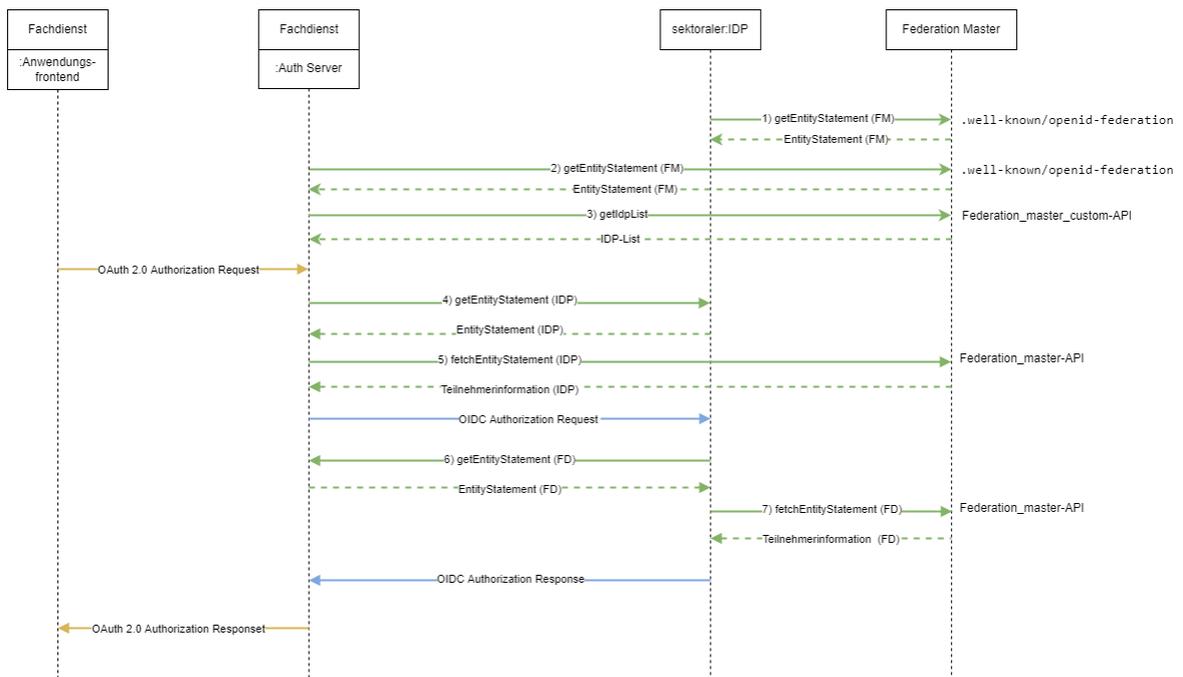
410 Der Payload des JWS-Token enthält zu jedem in der Föderation registrierten sektoralen
411 Identity Provider die Informationen

- 412 • Organisationsname
- 413 • URL, unter welcher das Logo der Organisation abrufbar ist
- 414 • URI des sektoralen Identity Provider, welcher dem Identifier (iss) des sektoralen
415 Identity Provider entspricht
- 416 • Liste der supporteten Usertypen Usertype

417 [~~=~~]

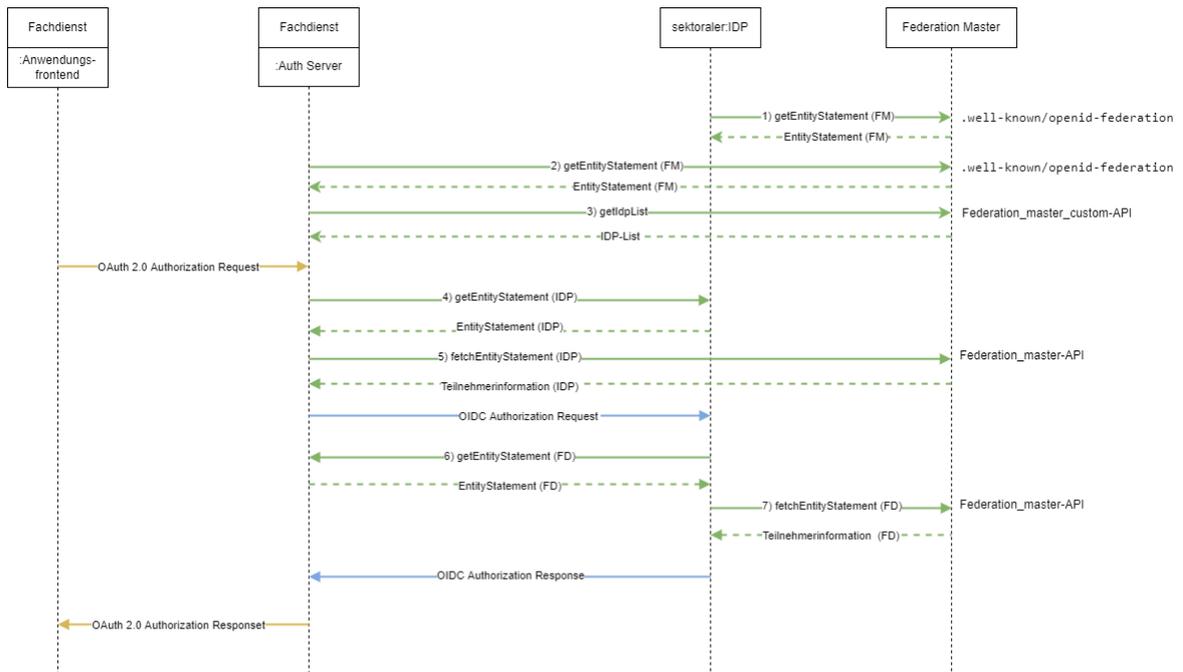
418 3.3 Anwendungsfall - Entity Statement bereitstellen

419



420

OAuth-Flow OIDC-Flow Federation Flow



421

OAuth-Flow OIDC-Flow Federation Flow

Abbildung 6: Federation Master im Authorization-Flow

422

423

424

425

Tabelle 9: Federation Master im Authorization-Flow

Schritt	Beteiligte Parteien	Beschreibung
---------	---------------------	--------------

1 - getEntityStatement(FM)	sektoraler Identity Provider, Federation Master	ladenRequest zum Abholen des Entity Statement des Federation Master durch den sektoralen Identity Provider
2 - getEntityStatement(FM)	Fachdienst, Federation Master	ladenRequest zum Abholen des Entity Statement des Federation Master durch den Fachdienst
3 - getIdpListe	Fachdienst, Federation Master	ladenRequest zum Abholen der Liste der in der Föderation registrierten sektoralen Identity Provider vom Federation Master durch den Fachdienst
4 - getEntityStatement(IDP)	Fachdienst, sektoraler Identity Provider	ladenRequest zum Abholen des Entity Statement des sektoralen Identity Provider vom sektoralen Identity Provider durch den Fachdienst
5 - fetchEntityStatement(IDP)	Fachdienst, Federation Master	validieren des sektoralen Identity Provider als Teilnehmer der Föderation beim Federation Master durch den Fachdienst
6 - getEntityStatement(FD)	sektoraler Identity Provider, Fachdienst	ladenRequest zum Abholen des Entity Statement des FachdienstFachdienstes vom Fachdienst durch den sektoralen Identity Provider
7 - fetchEntityStatement(FD)	sektoraler Identity Provider, Federation Master	validieren des FachdienstFachdienstes als Teilnehmer der Föderation beim Federation Master durch den sektoralen Identity Provider

426

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

430

431 **AF_10101 - Bereitstellung von Informationen zu Teilnehmern der Föderation**
 432 **durch den Federation Master**

433 **Tabelle 10: Anwendungsfall "Bereitstellung von Informationen zu Teilnehmern der**
 434 **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"> • Federation Master • Fachdienst der TI • sektoraler Identity Provider
Vorbedingung	<ul style="list-style-type: none"> • Der Fachdienst ist in der TI-Föderation registriert, <u>und</u> sein öffentlicher Schlüssel und sein Entity Statement sind beim Federation Master hinterlegt. • Der sektorale Identity Provider ist in der TI-Föderation registriert, <u>und</u> sein öffentlicher Schlüssel und sein Entity Statement sind beim Federation Master hinterlegt. • Das Entity Statement des Federation Master steht zur Verfügung und die unter dem Attribut <code>federation_api_fetch_endpoint</code> benannte URL MUSS aus dem Internet erreichbar sein.

<p>Ablauf</p>	<ul style="list-style-type: none"> • 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. • Die unter <code>federation_apis_fetch_endpoint</code> im Entity Statement des Federation Master festgelegte URL MUSS aus dem Internet erreichbar sein. • Für die Abfrage von Informationen zu einem Teilnehmer der Föderation beim Federation Master sendet der anfragende Teilnehmer einen Request an die unter <code>federation_apis_fetch_endpoint</code> im Entity Statement des Federation Master festgelegte URL. Der Request MUSS die in Tabelle "Teilnehmer Validierung Abfrage - Request Parameter" Parameter umfassen. • 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 "Teilnehmer Validierung Abfrage - Response-Headerattribute-Header-Attribute des signierten JSON-Web-Token" aufgeführten Attribute enthalten.
<p>Ergebnis</p>	<p>Der anfragende Teilnehmer <u>hat</u> Informationen <u>über</u> den angefragten Teilnehmer erhalten, kann diese entschlüsseln und verwenden.</p>
<p>Akzeptanzkriterien</p>	<p> ML-128451 ,  ML-128452</p>
<p>Alternativen</p>	<p>Der Anwendungsfall entfällt, wenn die Teilnehmer sich kennen, eine gegenseitige Validierung bereits früher erfolgt ist und eine erneute Validierung (noch) nicht notwendig ist.</p>

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

Attribut	Werte / Typ	Beispiel	Anmerkung
iss	URL	"http://master0815.de"	URL des Federation Master
sub	URL	"https://idp4711.de" bzw. "https://Fachdienst007.de"	URL des angefragten Teilnehmer (sektoraler Identity Provider bzw. Fachdienst)

436
437
438

Tabelle 12: Teilnehmer Validierung Abfrage - Response-Payload-Attribute des signierten JSON-Web-Token

Attribut	Werte / Typ	Beispiel	Anmerkungen
iss	URL	"http://master0815.de"	URL des Federation Master
sub	URL	"https://idp4711.de" bzw. "https://Fachdienst007.de"	URL des angefragten Teilnehmer (sektoraler Identity Provider bzw. Fachdienst)
iat	Alle time Werte in Sekunden seit 1970, RFC 7519 Sect.2	1645398001 = 2022-02-21 00:00:01	Ausstellungszeitpunkt des Abrufs
exp	Alle time Werte in Sekunden seit 1970, RFC 7519 Sect.2	1645484400 = 2022-02-22 00:00:00 entspricht einer Gültigkeit von 24 Stunden in Bezug auf den Wert in iat	Ablaufzeitpunkt der Gültigkeit des AbrufsListe (maximal iat + 24 Stunden)
jwks	JWKS Objekt		öffentlicher Schlüssel des angefragten Teilnehmer (sektoraler Identity Provider bzw. Fachdienst)

439
440
441
442

Folgende Werte müssen Bestandteil des Header der vom Federation Master signierten IDP-Liste sein:

443
444

Tabelle 13: Teilnehmer Validierung - Response-Headerattribute-Header-Attribute des signierten JSON-Web-Token

Name	Werte	Beispiel	Anmerkungen
alg	ES256	<-	Brainpool nicht zwingend (überhaupt erlaubt zu unterstützen?) zu Diskutieren // OIDC Fed: Entities MUST support signing Entity Statements with the RSA-SHA-256 algorithm (an alg value of RS256) – Wir wollen aber ECC überall, ggf ein Problem

kid	wie aus jwks im Body des Entity Statement		Identifizier des verwendeten Schlüssels aus dem jwks im Body des Statement
typ	JWT		

445 [**<=**]446 **3.3.1 Akzeptanzkriterien - Entity Statement bereitstellen**

447 ML-128451 - ~~AF_10101~~ ~~Unter federation_api_endpoint benannte URL ist~~
 448 ~~erreichbar und liefert signiertes JWS als Response~~

449 Der Request eines Teilnehmers der Föderation an die URL, welche im Entity Statement
 450 des Federation Master unter dem Attribut `federation_api_fetch_endpoint` benannt ist,
 451 wird entgegengenommen und gibt als Response ein signiertes JWS zurück. Das Token ist
 452 mit dem privaten Schlüssel des Federation Master signiert und kann vom Fachdienst mit
 453 dem öffentlichen Schlüssel des Federation Master ~~entschlüsselt~~verifiziert werden. [**<=**]

454 [Hinweis: Für den Fetch Entity Request gelten die Festlegung im Standard \[OpenID](#)
 455 [Connect Federation 1.0\] Kapitel 7.1.1.](#)

456 ML-128452 - ~~AF_10101~~ ~~Payload des JWS Token enthält Informationen zum~~
 457 ~~angefragten Teilnehmer der Föderation~~

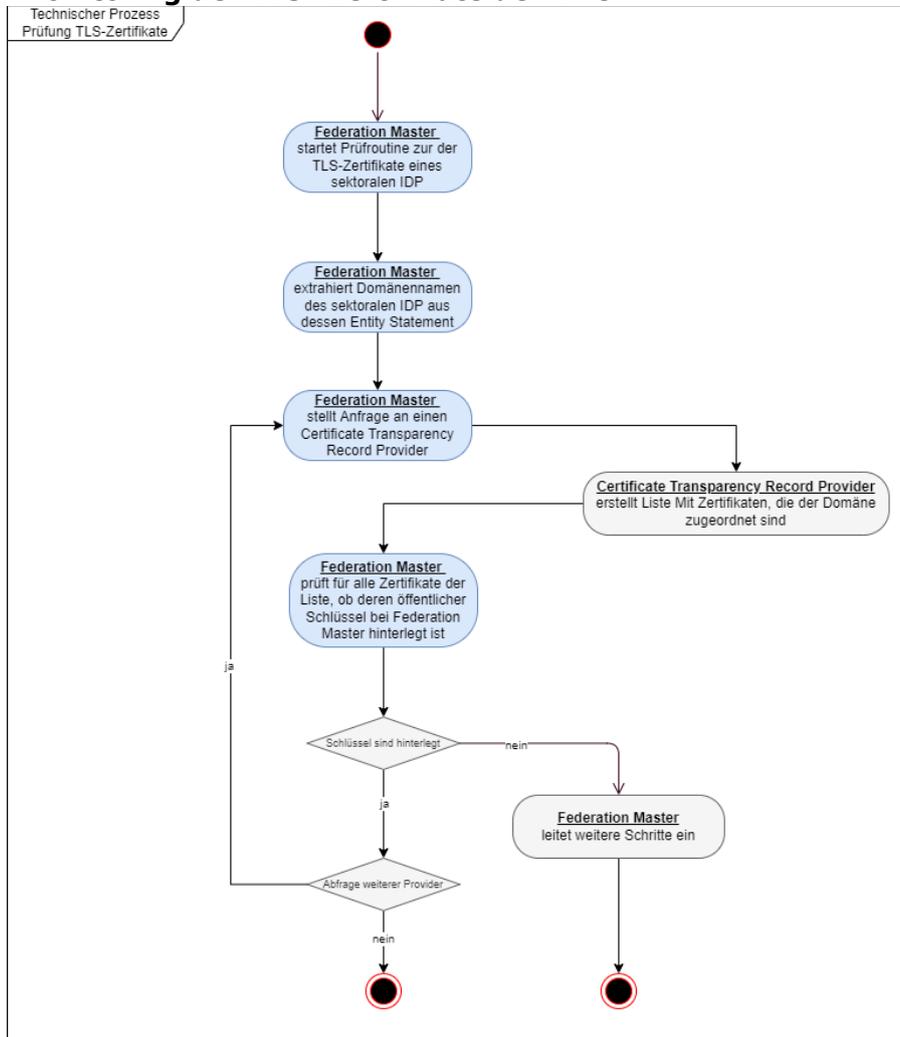
458 Der Payload des JWS-Token enthält diese Informationen bezüglich des angefragten
 459 ~~Teilnehmer~~Teilnehmers der Föderation (siehe auch [gemSpec IDP Sek - Anhang B -](#)
 460 [Abläufe](#)):

- 461 • `iss` = URL - Identifizier Federation Master
- 462 • `sub` = URL - Identifizier des angefragten Teilnehmers
- 463 • `iat` = long Wert - Ausstellungszeitpunkt des Abrufs (Alle `time_`-Werte in Sekunden
 464 seit 1970)
- 465 • `exp` = long Wert - Ablaufzeitpunkt der Gültigkeit des Abrufs (Alle `time_`-Werte in
 466 Sekunden seit 1970)
- 467 • `jwtks` = JWKS Objekt - öffentlicher Schlüssel des angefragten Teilnehmers.
- 468 • [aud](#) = URL - Identifizier des anfragenden Teilnehmers. Wenn der `aud`-Parameter im
 469 [Fetch Entity-Statement-Request des anfragenden Teilnehmers vorhanden ist,](#)
 470 [SOLLTE der `aud` Parameter in der Fetch Entity-Statement-Response vorhanden](#)
 471 [sein und genau diesen Wert annehmen.](#)

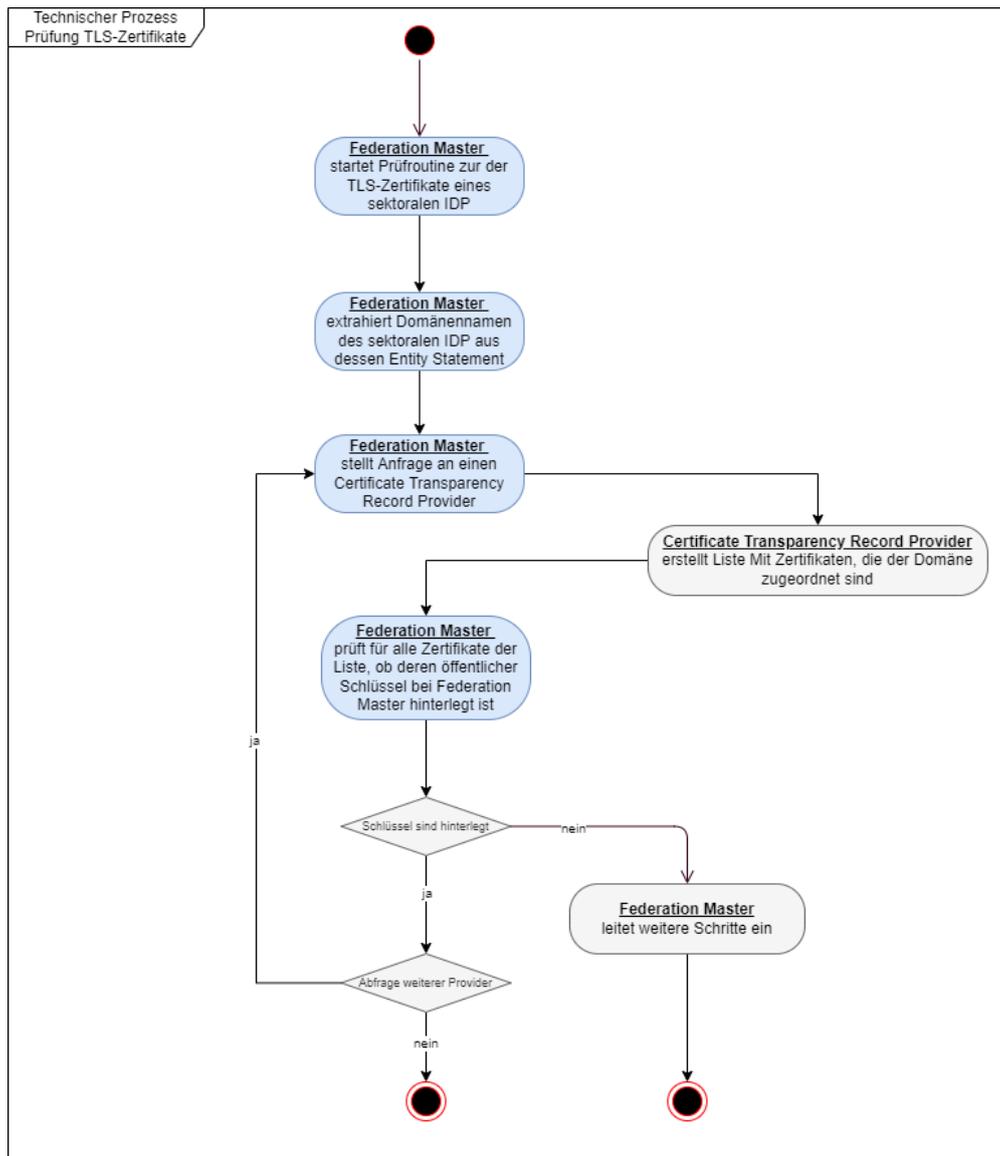
472 [**<=**]

473 **3.4 Anwendungsfall - Schlüssel verwalten**

474 **AF_10110 - Monitoring der TLS- Zertifikate der VAU**



475



476

477

478

479

Abbildung 7-4: Prüfung der TLS-Zertifikate eines sektoralen Identity Provider am Federation Master

Tabelle 14: Anwendungsfall "Monitoring der TLS-Zertifikate der VAU"

Attribute	Bemerkung
Beschreibung	Certificate Transparency Monitor für die TLS-Zertifikate
Akteur	Federation Master
Auslöser	<ul style="list-style-type: none"> Ein TLS-Zertifikat für eine Domäne, welche in der VAU des jeweiligen sektoralen IDP Dienst mündet, wird erstellt. Regelmäßige Prüfung der veröffentlichten TLS-Zertifikate
Komponente	<ul style="list-style-type: none"> Federation Master

	<ul style="list-style-type: none"> • sektoraler Identity Provider
Vorbedingung	<p>Der sektorale Identity Provider ist in der TI-Föderation registriert. Bei neu erstellten TLS-Zertifikaten wurde der Prozess <u>Certificate Transparency</u> TLS-Zertifikate der sektoralen Identity Provider prüfen erfolgreich durchlaufen. Die öffentlichen Schlüssel des <u>sektoralen Identity Provider und</u> seine öffentliche TLS-Schlüssel des sektoralen Identity Provider sind beim Federation Master hinterlegt.</p>
Ablauf	<p>Der Federation Master MUSS einen Certificate Transparency Monitor für die TLS-Zertifikate der Domains der sektoralen Identity Provider betreiben, die in der VAU des jeweiligen sektoralen IDP-Dienst münden. In diesem Certificate Transparency Monitor findet der Abgleich der Zertifikate gegen die bekannten Schlüssel der sektoralen Identity Provider statt (RFC9162). Dazu MUSS der Federation Master einmal täglich die TLS-Zertifikate der registrierten sektoralen Identity Provider prüfen. Zu diesem Zweck extrahiert er <u>aus den Domänennamen im Entity Statement</u> des sektoralen Identity Provider <u>aus dessen Entity Statement (z.B. aus den hinterlegten</u> Adressen zum Token- <u>oder, PAR- und</u> Authorization-Endpunkt).</p> <p><i>Hinweis: Alternativ kann das Hinterlegen des Domänennamen schon im Rahmen der Registrierungsprozess einmalig erfolgen, die Domänennamen.</i></p> <p>Der Federation Master fragt mit <u>den ermittelten</u> Domänennamen die Schnittstelle <u>eines oder mehrerer mindestens zweier unterschiedlicher öffentlich zugänglicher</u> Provider für Certificate Transparency Records ab (z.B. https://sslmate.com/ct_search_api/).</p> <p>Der Die Provider <u>liefern</u> alle registrierten Zertifikate zum Domänennamen.</p> <p>Der Federation Master MUSS jedes Zertifikat <u>dahin gehend</u> prüfen, ob der zugehörige öffentliche Schlüssel beim Federation Master bekannt und damit im HSM der VAU hinterlegt ist.</p>
Ergebnis	<p>Bei erfolgreicher Prüfung ist keine Maßnahme seitens Federation Master notwendig. Ist <u>die mindestens eine</u> Prüfung negativ, MUSS der Federation Master weitere Schritte hinsichtlich des negativ geprüften sektoralen Identity Provider einleiten und einen "Security Incident" (gemäß 3.4 <u>aus [gemRL_Betr_TI]</u>) erstellen.</p>
Akzeptanzkriterien	<p> ML-132625 ,  ML-132627</p>
Alternativen	-

480 [**<=**]

481 **3.4.1 Akzeptanzkriterien - Schlüssel verwalten**482 ML-132625 - ~~AF10110AF~~ [10110](#) - **Ablage der TLS-Schlüssel im Federation Master**

483 Wurde ein sektoraler Identity Provider erstmalig beim Federation Master registriert, so
484 MÜSSEN die öffentlichen Schlüssel aller TLS-Zertifikate zu den second-level, third-level
485 bzw. higher-level domain des ~~sektoraler~~sektoralen Identity Provider ~~welche~~die in der
486 VAU terminieren beim Federation Master zum sektoraler Identity Provider hinterlegt
487 sein.

488 Wurde eine TLS-Zertifikat zu einer second-level, third-level bzw. higher-level domain
489 eines ~~sektoraler~~sektoralen Identity Provider ~~das, welcher~~ in der VAU terminiert,
490 hinzugefügt oder aktualisiert, so MUSS der öffentliche Schlüssel des hinzugefügten oder
491 aktualisierten TLS-~~Zertifikat~~Zertifikats zur Domäne des ~~sektoraler~~sektoralen Identity
492 Provider beim Federation Master zum ~~sektoraler~~sektoralen Identity Provider hinterlegt
493 sein. [<=]

494

495

496 ML-132627 - ~~AF10110AF~~ [10110](#) - **TLS-Schlüsselprüfung durch den Federation
497 Master nicht erfolgreich**

498 Gibt es mindestens ein TLS-~~Zertifikate~~Zertifikat zu einer second-level, third-level bzw.
499 higher-level domain eines ~~sektoraler~~sektoralen Identity Provider ~~das in~~ der in der VAU
500 terminiert, und dessen öffentlicher Schlüssel nicht oder falsch beim Federation Master
501 registriert ist, so ist die Prüfung nicht erfolgreich. Der Betreiber des Federation Master
502 hat Schritte zur Problemlösung (gemäß  [ML-132673 - Maßnahmen bei negativer TLS-
503 Zertifikatsprüfung durch den Federation Master](#)) eingeleitet. [<=]

504

505

4 Anforderungen an den Produkttyp

506

4.1 Aufbau und Inhalt des Federation Master Entity Statement

508 Der Federation Master bildet den Vertrauensanker der Föderation. Ebenso ist der
509 Federation Master eine Entität innerhalb der ~~der~~-Föderation. Gemäß dem verwendeten
510 Standard OpenID Connect mit OAuth 2.0 kommen JSON Web Token (JWT), JSON Web
511 Encryption (JWE), JSON Web Signature (JWS) und JSON Web Key (JWK) zum Einsatz.

512 Um nutzenden Anwendungen eine einheitliche Bezugsquelle für die Adressierung von
513 Schnittstellen zu schaffen, werden die für alle Akteure grundlegenden Schnittstellen im
514 sogenannten Entity Statement zusammengefasst und dort unter der ".well-known/openid-
515 federation" gemäß [[OpenID Connect Federation 1.0#rfc.section.6](#)] veröffentlicht.

516 Alle Akteure der Föderation sind angehalten, das Entity Statement herunterzuladen und
517 den Inhalt in den geplanten Betrieb einzubeziehen. Die Teilnehmer der Föderation
518 benötigen das Entity Statement des Federation Master zur:

- 519 • Validierung der Vertrauenskette in der Kommunikation zwischen Fachdiensten und
520 sektoralen Identity Provider
- 521 • Validierung anderer Kommunikationsteilnehmer in der Föderation
- 522 • Ermittlung des API-Endpunktes des Federation Master
- 523 • Ermittlung der Liste aller in der Föderation registrierten sektoralen Identity
524 Provider.

525

526 **A_22947 - Aktualisierungszyklen für die Liste der registrierten sektoralen** 527 **Identity Provider**

528 Der Federation Master MUSS die Liste der registrierten sektoralen Identity Provider
529 täglich aktualisieren. Darüber hinaus MUSS der Federation Master die Liste bei
530 Neuregistrierung, ~~Sperrung~~ oder Löschung von sektoralen Identity Providern
531 aktualisieren. [[zur Kommentierung freigegeben,](#)
532 **f<=]**

533 **A_22948 - Aktualisierungszyklen der Entity Statements Federation Master**

534 Der Federation Master MUSS sein Entity Statement täglich aktualisieren. Darüber hinaus
535 MUSS der Federation Master sein Entity Statement bei jeder Änderung, welche sich auf
536 das Entity Statement auswirkt, aktualisieren. [[zur Kommentierung freigegeben,](#) **<=f<=]**

537 **A_22949 - Aktualisierungszyklen der Entity Statements zu Teilnehmern der** 538 **Föderation**

539 Der Federation Master MUSS seine Entity Statements zu den Teilnehmern der
540 Föderation täglich aktualisieren. Darüber hinaus MUSS der Federation Master sein Entity
541 Statement zu einem Teilnehmern bei jeder Änderung, welche sich auf das Entity
542 Statement zum Teilnehmer auswirkt, aktualisieren. [[zur Kommentierung freigegeben,](#) **<=f<=]**
543

544 **A_22604 - Verwendung eindeutiger URI**

545 Der Federation Master MUSS alle verwendeten Adressen in Form von URL gemäß
546 [RFC1738] angeben und in einem Entity Statement gemäß [[OpenID Connect Federation](#)

547 [1.0#rfc.section.3.1](#)] im Internet veröffentlichen. [\[zur Kommentierung](#)
 548 [freigegeben, <=f<=\\]](#)

549 **A_22605 - Entity Statement Veröffentlichung**

550 Der Federation Master MUSS sein Entity Statement im Internet gemäß [[OpenID Connect](#)
 551 [Federation 1.0#rfc.section.6](#)] unter ".well-known/openid-federation" veröffentlichen. [\[zur](#)
 552 [Kommentierung freigegeben, <=f<=\\]](#)

553 **A_22606 - Entity Statement - Prüfung der angebotenen URL**

554 Der Anbieter des Federation Master MUSS alle von ihm im Entity Statement angebotenen
 555 URL ständig auf bloße Erreichbarkeit prüfen. [\[zur Kommentierung freigegeben, <=f<=\\]](#)

556 **A_22607 - Inhalte des Federation Master Entity Statement**

557 Der Federation Master MUSS im Entity Statement gemäß [[OpenID Connect Federation](#)
 558 [1.0#rfc.section.6.2](#)] mindestens die folgenden Attribute angeben:

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

Attribut	Typ	Beschreibung	Beispiel
iss	URL	URL des Federation Master	"http://master0815.de"
sub	URL	URL des Federation Master (=iss)	"http://master0815.de"
iat	long	Alle time_Werte in Sekunden seit 1970, RFC 7519 Sect.2	1645398001 = 2022-02-21 00:00:01
jwt	JWKS	Schlüssel für die Signatur des Entity Statement	"master0815-1"
exp	long	Alle time_Werte in Sekunden seit 1970, RFC 7519 Sect.2	1646002800 1645484400 = Gültigkeit von 7 Tagen24 Stunden in Bezug auf den Wert in iat

560 [f<=\\]](#)[\[zur Kommentierung freigegeben, <=\]](#)

561 **A_22608 - Inhalte des Metadata Federation API-Endpoint im Federation**
 562 **Master Entity Statement**

563 Der Federation Master MUSS im Entity Statement gemäß [[OpenID Connect Federation](#)
 564 [1.0#rfc.section.6.2](#)[OpenID Connect Federation 1.0#rfc.section.4.6](#)] mindestens
 565 ~~das folgende Attribut~~die folgenden Attribute als metadata/federation_entity angeben:

567 **Tabelle 16: Attribut "Federation API Endpoint"**

Attribut	Typ	Beschreibung	Beispiel
federation_apis_fetch_endpoint	URL	Adresse des Endpunktes zum Abrufen einzelner oder aller Statements des Masters über	"http://master0815.de/federation_apis_fetch_endpoint"

		sektoralezu sektoralen Identity Provider und FachdiensteFachdiensten beim Federation Master	
federation_list_end_point	U RL	Adresse des Endpunktes zum Abrufen der Liste aller bekannten Entity Identifier	"http://master0815.de/federation_list"

568 [\[<=>\]](#) [zur Kommentierung freigegeben, <=]

569 **A_22609 - Inhalte des Federation Master Entity Statement Metadata IDP-Liste**

570 Der Federation Master MUSS im Entity Statement mindestens das folgende Attribut
571 als metadata/federation_entity angeben:

572

573 **Tabelle 17: Attribut "IDP List Endpoint"**

Attribut	Typ	Beschreibung	Beispiel
idp_list_endpoint	URL	Adresse des Endpunktes zum Abrufen einer Liste aller sektoraler Identity Provider mit deren Namen, Logo und Identifier und Nutzergruppe	"http://master0815.de/idp_list.jws"

574 [\[<=>\]](#) [zur Kommentierung freigegeben, <=]

575 **A_23087 - ~~Entity Statements gesperrter oder gelöschter Teilnehmer~~ Entity Statements gelöschter Teilnehmer**

576
577 Der Federation Master MUSS sicherstellen, dass der Abruf des Entity Statement
578 ~~gesperrter oder~~ gelöschter Teilnehmer über das Federation Master API zu einer
579 Fehlermeldung unter Berücksichtigung des [Standards \[OpenID Connect Federation 1.0#rfc.section.7.5\]](#) führt. [\[zur Kommentierung freigegeben, <=Standard \[OpenID Connect Federation 1.0#rfc.section.7.4 \] führt.](#)

581 [\[<=>\]](#)

582
583

584 **4.2 Organisatorische Prozesse am Federation Master**

585 **A_22675 - Teilnehmerregistrierung am Federation Master**

586 Der Anbieter des Federation Master MUSS einen organisatorischen Prozess für die
587 Registrierung von Teilnehmern an der Föderation etablieren. Alle Teilnehmer der
588 Föderation MÜSSEN über diesen Prozess ihre öffentlichen Schlüssel beim Federation
589 Master hinterlegen. Fachdienste MÜSSEN zusätzlich die für ihre Anwendungsfälle

590 notwendigen scopes hinterlegen. Der Anbieter des Federation Master MUSS vorsehen,
591 dass die gematik in den organisatorischen Ablauf eingebunden ist und die Möglichkeit der
592 Prüfung der vom Fachdienst eingereichten scopes erhält. [\[zur Kommentierung](#)
593 [freigegeben, <= \[<= \]](#)

594 *Hinweis: Der Aufbau und die Verwendung der hierarchischen Vertrauensbeziehung*
595 *(Trust Chain) ist im Standard [[OpenID Connect Federation 1.0](#)] festgelegt und wird*
596 *darüber hinaus hier nicht weiter spezifiziert.*

597 *Fachdienste sollten nur genau die scopes beanspruchen, die für die Ausführung ihrer*
598 *Anwendungsfälle unbedingt notwendig sind.*

599 ~~A_22676—Teilnehmer am Federation Master sperren~~

600 ~~Der Anbieter des Federation Master MUSS einen organisatorischen Prozess für das~~
601 ~~Sperren von Teilnehmern durch die gematik an der Föderation etablieren. Der Anbieter~~
602 ~~des Federation Master MUSS sicherstellen, dass der Abruf des Entity Statement~~
603 ~~gesperrter Teilnehmer über das Federation Master API zu einer entsprechenden~~
604 ~~Fehlermeldung führt. [<=]~~

605

606

607 **A_22741 - Prüfung "scope" von Fachdiensten**

608 Der Anbieter des Federation Master MUSS einen Prozess etablieren, in dem der Anbieter
609 des Federation Master [regelmäßig mindestens täglich die](#) Entity Statements ~~des~~
610 [Fachdienstes der Fachdienste](#) abfragt und die dort aufgeführten scopes hinsichtlich der
611 bei der Registrierung hinterlegten scopes prüft. ~~Stimmen abfragte scopes nicht mit den~~
612 ~~bei der Registrierung hinterlegten scopes überein, so ist die Prüfung negativ,~~ MUSS der
613 Anbieter des Federation Master [organisatorische und/oder technische Prozesse mit](#)
614 [geeigneten Maßnahmen zur Problembeseitigung etablieren.](#) [\[zur Kommentierung](#)
615 [freigegeben, den Fachdienst unverzüglich sperren. \[<= \]](#)

616 [Hinweis: Geeignete Maßnahmen können je nach Analyseergebnis z.B. das Einstellen von](#)
617 [Security-Bugs beim Betreiber des Fachdienstes, die Einstellung eines](#)
618 [sicherheitsrelevanten Notfalls gegen den Anbieter des entsprechenden Fachdienstes](#)
619 [durch den Federation Master im TI-ITSM \(für TI-ITSM Teilnehmer\), aber auch das](#)
620 [Löschen des betroffenen Fachdienstes sein.](#)

621 **A_22677 - Teilnehmer am Federation Master löschen**

622 Der Anbieter des Federation Master MUSS einen organisatorischen Prozess ~~für das~~ [mit 4-](#)
623 [Augen-Prinzip zur Erteilung von Löschaufträgen und einen technischen Prozess zum](#)
624 [eigentlichen](#) Löschen von Teilnehmern ~~aus~~ der Föderation etablieren. [\[zur](#)
625 [Kommentierung freigegeben, <= \[<= \]](#)

626 [Hinweise: Die Abwicklung kann über Service Request durch gematik. oder durch](#)
627 [definierte Trigger im Rahmen eines Sicherheitsvorfalls erfolgen.](#)

628 **A_22945 - Schlüssel für Certificate Transparency TLS-Zertifikate übergeben**

629 Der Anbieter des Federation Master MUSS einen organisatorischen Prozess etablieren,
630 über den die Übergabe der öffentlichen Schlüssel von TLS-Zertifikaten zu Domänen eines
631 sektoraler Identity Provider, welche in der VAU terminieren, erfolgt. [\[zur Kommentierung](#)
632 [freigegeben, <= \[<= \]](#)

633 *Hinweis: Für den Ablauf der Schlüsselprüfungen siehe [3.4-1- Monitoring der TLS-](#)*
634 *[Zertifikate der VAU](#)*

A_22968 - Maßnahmen bei negativer TLS-Zertifikatsprüfung durch den Federation Master

Gibt es mindestens ein TLS-Zertifikate-zurZertifikat der Domäne/Unterdomäne eines sektoraler Identity Provider, das in der VAU terminiert, und dessen öffentlicher Schlüssel nicht oder falsch beim Federation Master registriert ist, so ist die Prüfung nicht erfolgreich. Für diesen Fall MUSS der Anbieter des Federation Master organisatorische und technische Prozesse mit geeignetegeeigneten Maßnahmen zur Analyse und Problembeseitigung etablieren. [zur Kommentierung freigegeben,

{<=}

~~Hinweis: Geeignete Maßnahmen können je nach Analyseergebnis z.B. Hinweis: Geeignete Maßnahmen können je nach Analyseergebnis z.B. das Einstellen von Security-Bugs beim Betreiber des sektoralen Identity Provider, die Einstellung eineneines sicherheitsrelevanten NotfallNotfalls gegen den Anbieter des entsprechenden sektoralen IDP Dienstes durch den Federation Master im ITSM, aber auch das SperrenLöschen des betroffenen betroffenen sektoralen Identity ProviderIDP sein.~~

4.3 Betrieblichen Anforderungen

-

~~A_22958 — Georedundanz des Federation Master~~

~~Der Anbieter des Federation Master MUSS die aktuellen Empfehlungen des BSI bei der Standortwahl seiner Rechenzentren vollumfänglich umsetzt. Der Anbieter des Federation Master MUSS seinen Dienst an zwei Standorten betreiben. Der Anbieter des Federation Master MUSS Unterschreitungen der Empfehlungen des BSI begründen und die Abmilderung der Risiken begründet nachweisen, wobei eine Unterschreitung des Abstandes von 100 km gemäß aktuellen Empfehlungen des BSI nicht zulässig ist.~~

{<=}

~~Hinweis: Weiterführende Informationen sind unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/RZ_Sicherheit/Standort-Kriterien_Rechenzentren.pdf zu finden.~~

4.4.3 Allgemeine Sicherheitsanforderungen

A_22678 - Schützenswerte Objekte

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

- PrivatePrivater Schlüssel und öffentlicher Schlüssel des Federation Master
- Öffentliche Schlüssel von registrierten Clients
- Authentisierungsinformationen von SperrberechtigtenLöschberechtigten
- Dokumentation über beauftragte und durchgeführte SperrungenLöschungen
- Statusinformationen
- Authentisierungsinformationen zur Authentisierung von internen Akteuren bzw. Rollen

- 677 • Protokolldaten
- 678 • Konfigurationsdaten.

679 [\[<=>\]zur Kommentierung freigegeben, <=>\]](#)

680 **A_22601 - Federation Master - Berücksichtigung OWASP-Top-10-Risiken**

681 Der Anbieter des Federation Master MUSS Maßnahmen zum Schutz sowohl vor den zum
682 Zulassungszeitpunkt aktuellen OWASP-Top-10-Risiken umsetzen, als auch ~~nach~~ die nach
683 dem Zulassungszeitpunkt jeweils aktuellen OWASP-Top-10-Risiken berücksichtigen. [\[zur](#)
684 [Kommentierung freigegeben, <=>\]](#)

685 **4.54.4 Sicherheit der Netzübergänge**

686 **A_22591 - Federation Master – Sicherung zum Transportnetz Internet durch** 687 **Paketfilter**

688 Der Anbieter des Federation Master MUSS dafür sorgen, dass das Transportnetz Internet
689 durch einen Paketfilter (ACL) gesichert wird und ausschließlich die erforderlichen
690 Protokolle weiterleitet. Der Anbieter des Federation Master MUSS dafür sorgen, dass der
691 Paketfilter des Federation Master frei konfigurierbar auf der Grundlage von Informationen
692 aus OSI-Layer 3 und 4 ist, ~~das heißt~~ (Quell- und Zieladresse, IP-Protokoll sowie Quell-
693 und Zielport). [\[zur Kommentierung freigegeben, <=>\]](#)

694 **A_22592 - Federation Master – Platzierung des Paketfilters Internet**

695 Der Anbieter des Federation Master DARF den Paketfilter des Federation Master zum
696 Schutz in Richtung Transportnetz Internet NICHT physisch auf dem vorgeschalteten TLS-
697 terminierenden Load Balancer implementieren. [\[zur Kommentierung](#)
698 [freigegeben, <=>\]](#)

699 **A_22593 - Federation Master-Anbieter – Richtlinien für den Paketfilter zum** 700 **Internet**

701 Der Anbieter des Federation Master MUSS beim Paketfilter die Weiterleitung von IP-
702 Paketen an der Schnittstelle zum Internet auf das HTTPS-Protokoll beschränken. [\[zur](#)
703 [Kommentierung freigegeben, <=>\]](#)

704 **A_22594 - Federation Master – Verhalten bei Volllauslastung**

705 Der Anbieter des Federation Master MUSS den Paketfilter des Federation Master so
706 konfigurieren, dass bei Volllauslastung der Systemressourcen im Federation Master keine
707 weiteren Verbindungen angenommen werden. [\[zur Kommentierung freigegeben, <=>\]](#)

708 *Hinweis: Durch die Zurückweisung von Verbindungen wird sichergestellt, dass Clients*
709 *einen Verbindungsaufbau mit einer anderen Instanz des Fachdienstes versuchen, bei*
710 *dem die erforderlichen Ressourcen zur Verfügung stehen.*

711 **A_22589 - Richtlinien zum TLS-Verbindungsaufbau**

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

716 Der Anbieter ~~des Federation Master~~ MUSS ~~dafür sorgen, dass das Zertifikat sich an die~~
717 ~~jeweilige Schnittstelle des Eingangspunkts bindet, damit Clientsysteme beim TLS-~~
718 ~~Verbindungsaufbau eine vereinfachte Zertifikatsprüfung mit Zertifikate aus einer CA~~
719 ~~beziehen, welche Certificate Transparency gemäß RFC 6962 / RFC 9162 unterstützt und~~
720 ~~täglich prüfen und sicherstellen, dass für seine Domänen keine unbekanntes Zertifikate~~
721 ~~im Certificate Transparency Log gelistet werden.~~

722 ~~Der Anbieter des Federation Master MUSS für seine TLS-Zertifikate Certification Authority~~
723 ~~Authorization (CAA) DNS Resource Records nach RFC 6844 bereitstellen, welche die~~

724 [Validität der ausstellenden CA verifizieren. \[zur Kommentierung](#)
725 [freigegeben, Standardbibliotheken durchführen können.](#)
726 [f<=\]](#)

727

728 **4.64.5 Fehlermeldungen**

729 **A_22595 - Format der Fehlermeldungen**

730 Der Federation Master MUSS für die verschiedenen Teilfunktionen geeignete
731 Fehlermeldungen erzeugen und diese an den jeweiligen Aufrufer übergeben. Die
732 Festlegungen im Standard [[OpenID Connect Federation 1.0#rfc.section.7.4](#) }[OpenID](#)
733 [Connect Federation 1.0#rfc.section.7.5](#)] MÜSSEN bei der Definition der Meldungsinhalte
734 berücksichtigt werden. [<=\[zur Kommentierung freigegeben, <=f<=\]](#)

735 **A_22596 - Nutzung von eindeutigen Error-Codes bei der Erstellung von** 736 **Fehlermeldungen**

737 Der Federation Master MUSS Fehler durch eine eindeutige Nummer erkennbar machen
738 und der gematik eine Liste der Error-Codes zur Verfügung stellen, damit die
739 Ursachenklärung vereinfacht möglich wird. Die Festlegungen im Standard [[OpenID](#)
740 [Connect Federation 1.0#rfc.section.7.4](#) }[OpenID Connect Federation 1.0#rfc.section.7.5](#)]
741 MÜSSEN bei der Definition der Fehlercodes berücksichtigt werden. [\[zur Kommentierung](#)
742 [freigegeben, f<=\]](#)

743 **A_22597 - Verwendung eines einheitlichen Schemas für die Aufbereitung von** 744 **Fehlermeldungen**

745 Der Federation Master MUSS alle ausgeworfenen Fehlermeldungen zur
746 Weiterverarbeitung in einem einheitlichen Schema aufbereiten und bereitstellen.
747 Zeitstempel MÜSSEN auf der UTC basieren. [\[zur Kommentierung freigegeben, <=f<=\]](#)

748 **A_22598 - Formulierung der Fehlermeldungen**

749 Der Federation Master MUSS Fehlermeldungen, welche dem Nutzer angezeigt werden, in
750 der Art ausformulieren, dass es dem Nutzer möglich ist, eigenes Fehlverhalten anhand
751 der Fehlermeldung abzustellen. [\[zur Kommentierung freigegeben, <=f<=\]](#)

752 **A_22599 - Nutzung einer eindeutigen Beschreibung beim Aufbau von** 753 **Fehlermeldungen**

754 Der Federation Master MUSS jedem Fehler eine eindeutige eigene Beschreibung
755 zukommen lassen, sodass eine Fehlermeldung nicht für unterschiedliche Fehlerursachen
756 zur Anwendung kommt. [\[zur Kommentierung freigegeben, <=f<=\]](#)

757 **A_22600 - Ausgabe der Fehlermeldungen in umgekehrter Reihenfolge des** 758 **Auftretens**

759 Der Federation Master MUSS aufeinander aufbauende Fehlermeldungen in der
760 umgekehrten Reihenfolge ihres Auftretens "Traceback (most recent call last)"
761 ausgeben. [\[zur Kommentierung freigegeben, <=f<=\]](#)

762

763

5 Anhang – Verzeichnisse

764 5.1 Abkürzungen

765 **Tabelle 18: Abkürzungen**

Kürzel	Erläuterung
CT	Certificate Transparency
JWE	JSON Web Encryption
JWK	JSON Web Key
JWS	JSON Web Signature
JWT	JSON Web Token
OIDC	OpenID Connect
OP	OpenID Provider
OSI	Open Systems Interconnection model
RP	Relying Party
TLS	Transport Layer Security
URL	Uniform Resource Locator

766

767 5.2 Glossar

768 **Tabelle 19: Glossar**

Begriff	Erläuterung
Anwendungsfrontend	Die Applikation durch welche ein Nutzer die Dienste einer Anwendung der Telematikinfrastruktur wie etwa das E-Rezept nutzt.
Authentifizierung	Prüfung eines Identitätsnachweis des Nutzers am Gerät mit bestimmten Authentifizierungsmittel.
Claim	Ein Key/Value-Paar im Payload eines JSON Web Token.

Client	OAuth2-Rolle (siehe [RFC6749 # section-1.1]): Eine Anwendung (Relying Party), die auf geschützte Ressourcen des Resource Owners zugreifen möchte, die vom Resource Server bereitgestellt werden. Der Client kann auf einem Server (Webanwendung), Desktop-PC, mobilen Gerät etc. ausgeführt werden. Im Fokus der aktuellen Spezifikationen liegt jedoch allein die Kommunikation mit dem E-Rezept-FdV.
Consent	Zustimmung des Nutzers zur Verarbeitung der angezeigten Daten. Der Consent umfasst die Attribute, welche vom sektoralen Identity Provider bezogen auf die im <code>claim</code> des jeweiligen Fachdienstes eingeforderten Attribute zusammenfasst. Es besteht Einigkeit zwischen dem, was gefordert wird, und welche Attribute im Token bestätigt werden.
DiGA	Digitale Gesundheitsanwendung(en)
Entity Statement	Ein Entity Statement [OpenID Connect Federation 1.0#entity-statement] —(Entitätsaussage—) wird von einer Entität ausgegeben, die sich auf eine Subjekt-Entität und Blatt-Entitäten bezieht. Ein Entitätsstatement ist immer ein signiertes JWT.
Fachanwendungen / Relying Party	Fachanwendungen sind Relying Party (RP) im Kontext der OIDC-Spezifikation. Nach erfolgreicher Authentifizierung des Nutzers und dessen Zustimmung zur Datennutzung (Consent Freigabe) bekommt die Fachanwendung Zugang zu einem definierten Teil der Identifikationsattribute des Nutzers. Die Fachanwendung nutzt diese Informationen zur Autorisierung des Nutzers zur die Durchführung definierter Anwendungsfälle der Fachanwendung.
Federation Master	Der Federation Master basiert auf den Standards OpenID Connect (OIDC), Open Authorization 2.0 (OAuth 2) und JSON Web Token (JWT). Der Federation Master ist einerseits der Trust Anchor des Vertrauensbereichs der Föderation. Andererseits stellt der Federation Master Schnittstellen bereit, welche Auskunft über die in der Föderation registrierten sektoralen Identity Provider gibt.
Gerät	Alle Arten von mobilen oder stationären Endgeräten.
Identitätsattribute	Daten, welche eine natürliche Person eindeutig identifizieren (Name, Vorname, Geburtsdatum, Anschrift, KVNR)
identitätsbestätigenden Institutionen	Institutionen, welche die Identität einer natürlichen Person geprüft haben und bestätigen können. Solche Institutionen sind beispielsweise die Krankenkassen, welche die Identität der bei ihnen versicherten Personen bestätigen können.

JSON Web Token	Ein auf JSON basiertes und nach [RFC7519] (JWT) genormtes <code>ACCESS_TOKEN</code> . Das JWT ermöglicht den Austausch von verifizierbaren <code>claims</code> innerhalb seines Payloads.
Nutzergruppen	Nutzergruppen sind Personengruppen mit bestimmten Rollen im Kontext der TI-Anwendungslandschaft. Nutzergruppen sind beispielsweise Versicherte und Leistungserbringer (ggf. weiter differenziert - Ärzte, Zahnärzte, etc.)
Open Authorization 2.0	Ein Protokoll zur Autorisierung für Web-, Desktop und Mobile Anwendungen. Dabei wird es einem Endbenutzer (Resource Owner) ermöglicht, einer Anwendung (Client) den Zugriff auf Daten oder Dienste (Resources) zu ermöglichen, die von einem Dritten (Resource Server) bereitgestellt werden.
OpenID Connect	OpenID Connect (OIDC) ist eine Authentifizierungsschicht, die auf dem Autorisierungsframework OAuth 2.0 basiert. Es ermöglicht Clients, die Identität des Nutzers anhand der Authentifizierung durch einen Authorization-Server zu überprüfen (siehe [OpenID Connect Core 1.0]).
Pushed Authorization Request (PAR)	Der Pushed Authorization Request (PAR) ermöglicht es Clients, eine OAuth 2.0-Autorisierungsanforderung direkt an den Authorization-Server des sektoralen Identity Provider zu senden. Die übergebenen <code>redirect-URI</code> ist Autorisierungsendpunkt und wird im weiteren Flow verwendet. https://datatracker.ietf.org/doc/html/rfc9126
Resource Owner	OAuth2-Rolle (siehe [RFC6749 # section-1.1]): Eine Entität (Nutzer), die einem Dritten den Zugriff auf ihre geschützten Ressourcen gewähren kann. Diese Ressourcen werden durch den Resource Server bereitgestellt. Ist der Resource Owner eine Person, wird dieser als Nutzer bezeichnet.
Resource Server	OAuth2 Rolle (siehe [RFC6749 # section-1.1]): Der Server (Dienst), auf dem die geschützten Ressourcen (Protected Resources) liegen. Er ist in der Lage, auf Basis von Access Tokens darauf Zugriff zu gewähren. Ein solcher Token repräsentiert die delegierte Autorisierung des Resource Owners.
Scope	<code>scopes</code> definieren ein festgelegtes Set an <code>claims</code> . Mit <code>scopes</code> lässt sich steuern, dass Anwendungen oder Anwendungsgruppen nur genau die Informationen einer Identität bekommen, die für die Anwendungsfälle der Anwendung(en) notwendig sind. Im Kontext OIDC gibt es vordefinierte <code>scopes</code> wie <code>openid</code> , <code>profile</code> und <code>email</code> , die verwendet werden können (siehe auch OpenID Connect Basic)

	<p>Client Implementer's Guide 1.0#Scopes). In der Föderation wird es darüber hinaus weitere scopes geben.</p>
<p>sektoraler Identity Provider / OpenID Provider</p>	<p>Als sektoraler Identity Provider bzw. OpenID Provider (OP) wird ein Dienst bezeichnet, welcher nach vorheriger Authentifizierung Identitätsinformationen für eine bestimmte Gruppe von Nutzern innerhalb der Telematikinfrastruktur des Gesundheitswesens bereitstellt. Diese Informationen werden anschließend von Fachdiensten verwendet, um auf Fachdaten und -prozesse zuzugreifen.</p>

769 Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung
 770 gestellt.

771 **5.3 Abbildungsverzeichnis**

772 [Abbildung 1 :Überblick TI-Föderation](#)10
 773 [Abbildung 2 : Systemkontext](#)12
 774 [Abbildung 3: Übersichtsschaubild OIDC Federation](#)14
 775 [Abbildung 4 : Anwendungsfälle Federation Master](#)22
 776 [Abbildung 5 : Aktivitätsdiagramm "Auswahl sektorale Identity Provider"](#)23
 777 [Abbildung 6 : Federation Master im Authorization-Flow](#)29
 778 [Abbildung 7 : Prüfung der TLS-Zertifikate eines sektoralen Identity Provider am](#)
 779 [Federation Master](#)36
 780 [Abbildung 1: Überblick TI-Föderation](#)10
 781 [Abbildung 2: Systemkontext](#)12
 782 [Abbildung 3: Übersichtsschaubild OIDC Federation](#)14
 783 [Abbildung 4: Anwendungsfälle Federation Master](#)22
 784 [Abbildung 5: Aktivitätsdiagramm "Auswahl sektorale Identity Provider"](#)23
 785 [Abbildung 6: Federation Master im Authorization-Flow](#)29
 786 [Abbildung 7: Prüfung der TLS-Zertifikate eines sektoralen Identity Provider am](#)
 787 [Federation Master](#)36
 788 |

789 **5.4 Tabellenverzeichnis**

790 [Tabelle 1: Request zur Teilnehmerabfrage an den Federation Master](#)15
 791 [Tabelle 2: Akteure und Rollen](#)15

792	Tabelle 3: Begriffsklärung	17
793	Tabelle 4: Übersicht über die Anwendungsfälle im Gesamtkontext Federation Master	19
794	Tabelle 5: Anwendungsfälle Federation Master	22
795	Tabelle 6: Anwendungsfall "Bereitstellung Liste registrierte Identity Provider"	24
796	Tabelle 7: Liste sektorale Identity Provider — Payload Attribute des signierten JSON-Web-Token	26
797		
798	Tabelle 8: Liste sektorale Identity Provider — Headerattribute des signierten JSON-Web-Token	27
799		
800	Tabelle 9: Federation Master im Authorization-Flow	29
801	Tabelle 10: Anwendungsfall "Bereitstellung von Informationen zu Teilnehmern der Föderation durch den Federation Master"	30
802		
803	Tabelle 11: Teilnehmer Validierung Abfrage — Request-Parameter	32
804	Tabelle 12: Teilnehmer Validierung Abfrage — Response Payload Attribute des signierten JSON-Web-Token	33
805		
806	Tabelle 13: Teilnehmer Validierung — Response Headerattribute des signierten JSON-Web-Token	33
807		
808	Tabelle 14: Anwendungsfall "Monitoring der TLS-Zertifikate der VAU"	36
809	Tabelle 15: Attribute Entity Statement Federation Master	40
810	Tabelle 16: Attribut "Federation API Endpoint"	40
811	Tabelle 17: Attribut "IDP List Endpoint"	41
812	Tabelle 18: Abkürzungen	46
813	Tabelle 19: Glossar	46
814	Tabelle 20: Quellen	51
815	Tabelle 21: Weitere Dokumente	52
816	Tabelle 1: Request zur Teilnehmerabfrage an den Federation Master	15
817	Tabelle 2: Akteure und Rollen	15
818	Tabelle 3: Attributbeschreibung	17
819	Tabelle 4: Übersicht über die Anwendungsfälle im Gesamtkontext Federation Master	19
820	Tabelle 5: Anwendungsfälle Federation Master	22
821	Tabelle 6: Anwendungsfall "Bereitstellung Liste registrierter Identity Provider"	24
822	Tabelle 7: Liste sektorale Identity Provider - Payload-Attribute des signierten JSON-Web-Token	26
823		
824	Tabelle 8: Liste sektorale Identity Provider - Headerattribute des signierten JSON-Web-Token	27
825		
826	Tabelle 9: Federation Master im Authorization-Flow	29
827	Tabelle 10: Anwendungsfall "Bereitstellung von Informationen zu Teilnehmern der Föderation durch den Federation Master"	30
828		
829	Tabelle 11: Teilnehmer Validierung Abfrage - Request-Parameter	32

830 [Tabelle 12: Teilnehmer Validierung Abfrage - Response-Payload-Attribute des signierten](#)
 831 [JSON-Web-Token33](#)

832 [Tabelle 13: Teilnehmer Validierung - Response-Header-Attribute des signierten JSON-](#)
 833 [Web-Token33](#)

834 [Tabelle 14: Anwendungsfall "Monitoring der TLS-Zertifikate der VAU"36](#)

835 [Tabelle 15: Attribute Entity Statement Federation Master40](#)

836 [Tabelle 16: Attribut "Federation API Endpoint"40](#)

837 [Tabelle 17: Attribut "IDP List Endpoint"41](#)

838 [Tabelle 18: Abkürzungen46](#)

839 [Tabelle 19: Glossar46](#)

840 [Tabelle 20: Quellen51](#)

841 [Tabelle 21: Weitere Dokumente52](#)

842 |

843 **5.5 Referenzierte Dokumente**

844 **5.5.1 Dokumente der gematik**

845 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument
 846 referenzierten Dokumente der gematik zur Telematikinfrastruktur. ~~Der mit der~~
 847 ~~vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und~~
 848 ~~Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und~~
 849 ~~Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht~~
 850 ~~aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der~~
 851 ~~aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die~~
 852 ~~vorliegende Version aufgeführt wird.~~

853
 854 **Tabelle 20: Quellen**

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte – Glossar
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation zur Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_PKI]	gematik: Übergreifende Spezifikation PKI
[gemSpec_IDP_Sek]	gematik: Spezifikation der sektoralen Identity Provider der TI-Föderation
[gemSpec_IDP_Frontend]	gematik: Spezifikation der Frontendkomponenten von Fachdiensten in der TI-Föderation
[gemSpec_IDP_FD]	gematik: Spezifikation der Fachdienste in der TI-Föderation

855 **5.5.2 Weitere Dokumente**

856 Tabelle 21: Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
JWT [RFC7519]	JSON Web Token (JWT) (Mai 2015) https://datatracker.ietf.org/doc/html/rfc7519
OAuth 2.0 Spezifikation ([RFC6749])	The OAuth 2.0 Authorization Framework (Oktober 2012) https://datatracker.ietf.org/doc/html/rfc6749
[openid-connect-core]	OpenID Connect Core 1.0 (incorporating errata set 1 , November 2014) https://openid.net/specs/openid-connect-core-1_0.html
[OpenID Connect Basic Client Implementer's Guide 1.0]	OpenID Connect Basic Client Implementer's Guide 1.0 (draft 40 , Juli 2020) https://openid.net/specs/openid-connect-basic-1_0.html)
[OpenID Connect Federation1.0]	OpenID Connect Federation1.0 (September 2021 Draft 22 , Juni 2022) https://openid.net/specs/openid-connect-federation-1_0.html
[Pushed Authorization Request]	OAuth 2.0 Pushed Authorization Requests (März September 2021) https://datatracker.ietf.org/doc/html/rfc9126
PKCE ([RFC7636])	Proof Key for Code Exchange by OAuth Public Clients (September 2015) https://datatracker.ietf.org/doc/html/rfc7636
CAB-Forum	https://cabforum.org/
OWASP	Open Web Application Security Project https://owasp.org/
Certificate Transparency (CT)	Certificate Transparency Version 2.0 (Dezember 2021) https://datatracker.ietf.org/doc/html/rfc9162

857