

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Federation Master

Version:	1. 23 .0
Revision:	86419279335
Stand:	30.01 05.04.2024
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_IDP_FedMaster

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	06.02.2023		Einarbeitung Release FedMaster	gematik
1.1.0	01.09.2023		Einarbeitung IdP_Maintenance_23.4	gematik
1.2.0	30.01.2024		Einarbeitung ePAfueralle	gematik
1.3.0	05.04.2024		Einarbeitung IDP_24_5	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments.....	5
1.1 Zielsetzung.....	5
1.2 Zielgruppe.....	5
1.3 Geltungsbereich.....	5
1.4 Abgrenzungen.....	6
1.5 Methodik.....	6
1.5.1 Anforderungen.....	6
1.5.2 Anwendungsfälle und Akzeptanzkriterien.....	6
1.5.3 Hinweise.....	7
2 Systemüberblick.....	8
2.1 Allgemeiner Überblick.....	8
2.2 Detaillierter Überblick.....	9
2.3 Akteure und Rollen.....	12
2.4 Attributbeschreibung.....	14
3 Funktionsmerkmale.....	16
3.1 Anwendungsfälle.....	16
3.2 Anwendungsfall – IDP-Liste bereitstellen.....	19
3.2.1 Akzeptanzkriterien – IDP-Liste bereitstellen.....	25
3.3 Anwendungsfall – Entity Statement bereitstellen.....	26
3.3.1 Akzeptanzkriterien – Entity Statement bereitstellen.....	31
3.4 Anwendungsfall – Schlüssel verwalten.....	32
3.4.1 Akzeptanzkriterien – Schlüssel verwalten.....	34
4 Anforderungen an den Produkttyp.....	36
4.1 Aufbau und Inhalt des Federation Master Entity Statement.....	36
4.2 Organisatorische Prozesse am Federation Master.....	38
4.3 Allgemeine Sicherheitsanforderungen.....	40
4.4 Sicherheit der Netzübergänge.....	41
4.5 Fehlermeldungen.....	41
5 Anhang – Verzeichnisse.....	43
5.1 Abkürzungen.....	43
5.2 Glossar.....	43
5.3 Abbildungsverzeichnis.....	46
5.4 Tabellenverzeichnis.....	46
5.5 Referenzierte Dokumente.....	47

5.5.1 Dokumente der gematik.....	47
5.5.2 Weitere Dokumente.....	48

1 Einordnung des Dokuments.....	6
1.1 Zielsetzung.....	6
1.2 Zielgruppe.....	6
1.3 Geltungsbereich.....	6
1.4 Abgrenzungen.....	7
1.5 Methodik.....	7
1.5.1 Anforderungen.....	7
1.5.2 Anwendungsfälle und Akzeptanzkriterien.....	7
1.5.3 Hinweise.....	8
2 Systemüberblick.....	9
2.1 Allgemeiner Überblick.....	9
2.2 Detaillierter Überblick.....	10
2.3 Akteure und Rollen.....	16
2.4 Attributbeschreibung.....	17
3 Funktionsmerkmale.....	20
3.1 Anwendungsfälle.....	20
3.2 Anwendungsfall - IDP-Liste bereitstellen.....	24
3.2.1 Akzeptanzkriterien - IDP-Liste bereitstellen.....	31
3.3 Anwendungsfall - Entity Statement bereitstellen.....	32
3.3.1 Akzeptanzkriterien - Entity Statement bereitstellen.....	38
3.4 Anwendungsfall - Schlüssel verwalten.....	39
3.4.1 Akzeptanzkriterien - Schlüssel verwalten.....	43
4 Anforderungen an den Produkttyp.....	44
4.1 Aufbau und Inhalt des Federation Master Entity Statement.....	44
4.2 Organisatorische Prozesse am Federation Master.....	49
4.3 Allgemeine Sicherheitsanforderungen.....	51
4.4 Sicherheit der Netzübergänge.....	51
4.5 Fehlermeldungen.....	52
5 Anhang - Verzeichnisse.....	54
5.1 Abkürzungen.....	54
5.2 Glossar.....	54
5.3 Abbildungsverzeichnis.....	57
5.4 Tabellenverzeichnis.....	58
5.5 Referenzierte Dokumente.....	59

5.5.1 Dokumente der gematik.....59
5.5.2 Weitere Dokumente.....60

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 über Teilnehmer der Föderation
- Bereitstellung von Schnittstellen für:
 - die Auskunft zum Federation Master (Entity Statement)
 - die Auskunft über Teilnehmer der Föderation
 - die Auskunft über die Liste aller registrierten OpenID Provider (OP)
 - die Registrierung neuer 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 **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 tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen

Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzungen

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

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

Für weitere Komponenten der TI-Föderation gelten eigene Spezifikationsdokumente:

- sektorale Identity Provider - [gemSpec_IDP_Sek]
- Fachdienste - [gemSpec_IDP_FD]
- Anwendungsfrontend der Fachdienste - [gemSpec_IDP_Frontend].

1.5 Methodik

1.5.1 Anforderungen

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID in eckigen Klammern sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Sie werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>

Text / Beschreibung

[<=]

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

1.5.2 Anwendungsfälle und Akzeptanzkriterien

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

Anwendungsfälle und Akzeptanzkriterien werden im Dokument wie folgt dargestellt:

<ID> - <Titel des Anwendungsfalles / Akzeptanzkriteriums>

Text / Beschreibung
[<=]

Die einzelnen Elemente beschreiben:

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

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

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

1.5.3 Hinweise

Hinweis auf offene Punkte

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

2 Systemüberblick

2.1 Allgemeiner Überblick

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

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

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

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

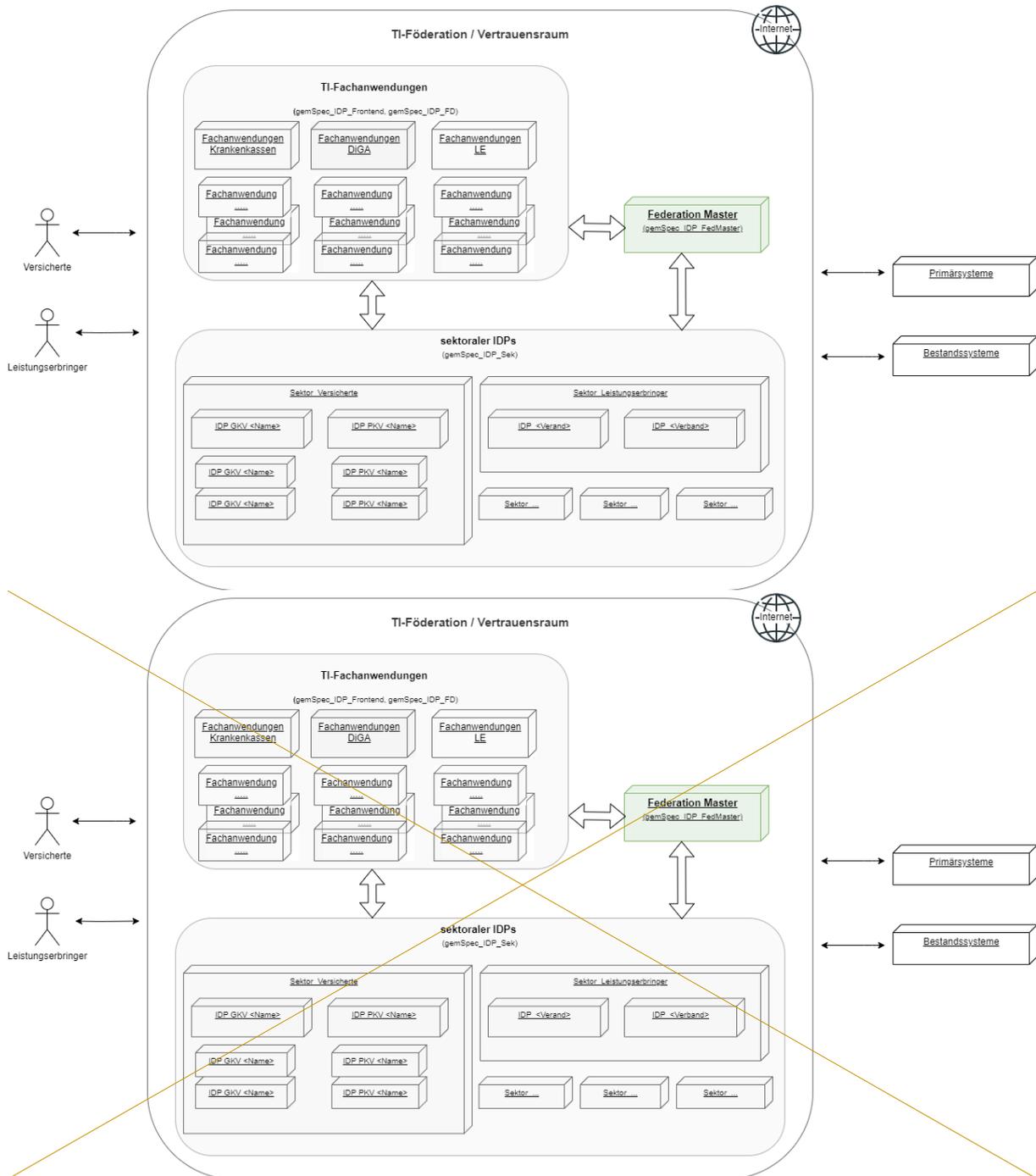


Abbildung 1: Überblick TI-Föderation

2.2 Detaillierter Überblick

Die untere Abbildung beschreibt den Systemkontext aus Sicht des Federation Master. Alle sektoralen Identity Provider der Föderation müssen beim Federation Master registriert sein. Ebenso müssen alle Fachanwendungen, welche die bei den Identity Providern hinterlegten digitalen Identitäten nutzen möchten, beim Federation Master registriert

sein. Jede teilnehmende Partei inklusive des Federation Master muss ein OpenID Connect spezifikationskonformes Entity Statement bereitstellen.

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

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

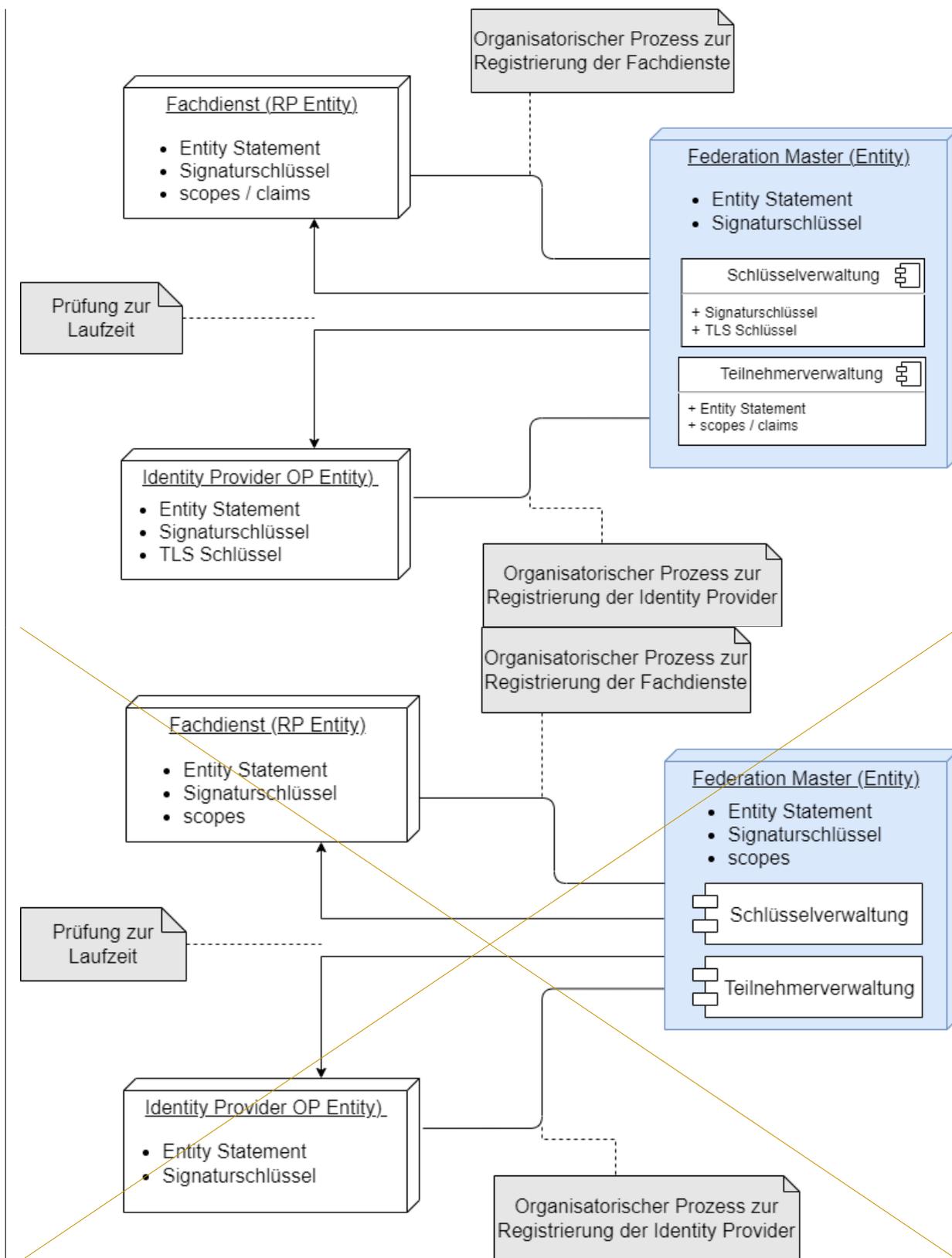


Abbildung 2: Systemkontext

Im Prozess der Autorisierung eines Nutzers für eine Anwendung ist der Federation Master als Vertrauensstelle eingebunden. Die Voraussetzung für die Kommunikation zwischen

Fachdiensten und sektoralen Identity Providern ist deren Registrierung im Vertrauensbereich der Föderation. Diese initiale Registrierung erfolgt organisatorisch und unabhängig vom späteren Ablauf.

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

- Die aktuellen Signaturschlüssel der beteiligten sektoralen Identity Provider und Fachdienste wurden über einen vom Anbieter bereitgestellten organisatorischen Prozess beim Federation Master hinterlegt.
- Die Entity Statements der beteiligten sektoralen Identity Provider und Fachdienste entsprechen den Vorgaben [OpenID Connect Federation1.0]
- Der Identifier des Federation Master wurde vom Anbieter des Federation Master veröffentlicht.

Das folgende Übersichtsschaubild gibt einen Überblick über das Zusammenspiel der unterschiedlichen Komponenten der Föderation. Grau hinterlegte Schritte sind nicht Bestandteil des Nutzungsflows.

Die Kommunikation des Anwenders über das Anwendungsfrendend mit dem Fachdienst entspricht der OAuth-2.0-Spezifikation ([\[RFC6749\]](#)) mit PKCE ([\[RFC7636\]](#)) und wird hier nicht detailliert beschrieben.

Die Kommunikation zwischen dem Fachdienst (Relying Party) und dem sektoralen Identity Provider (OpenID-Provider) entspricht den Spezifikationen zu OpenID Connect ([Final: OpenID Connect Core 1.0](#)) und Pushed Authorization Request (<https://datatracker.ietf.org/doc/html/rfc9126>) und wird hier nicht detailliert beschrieben.

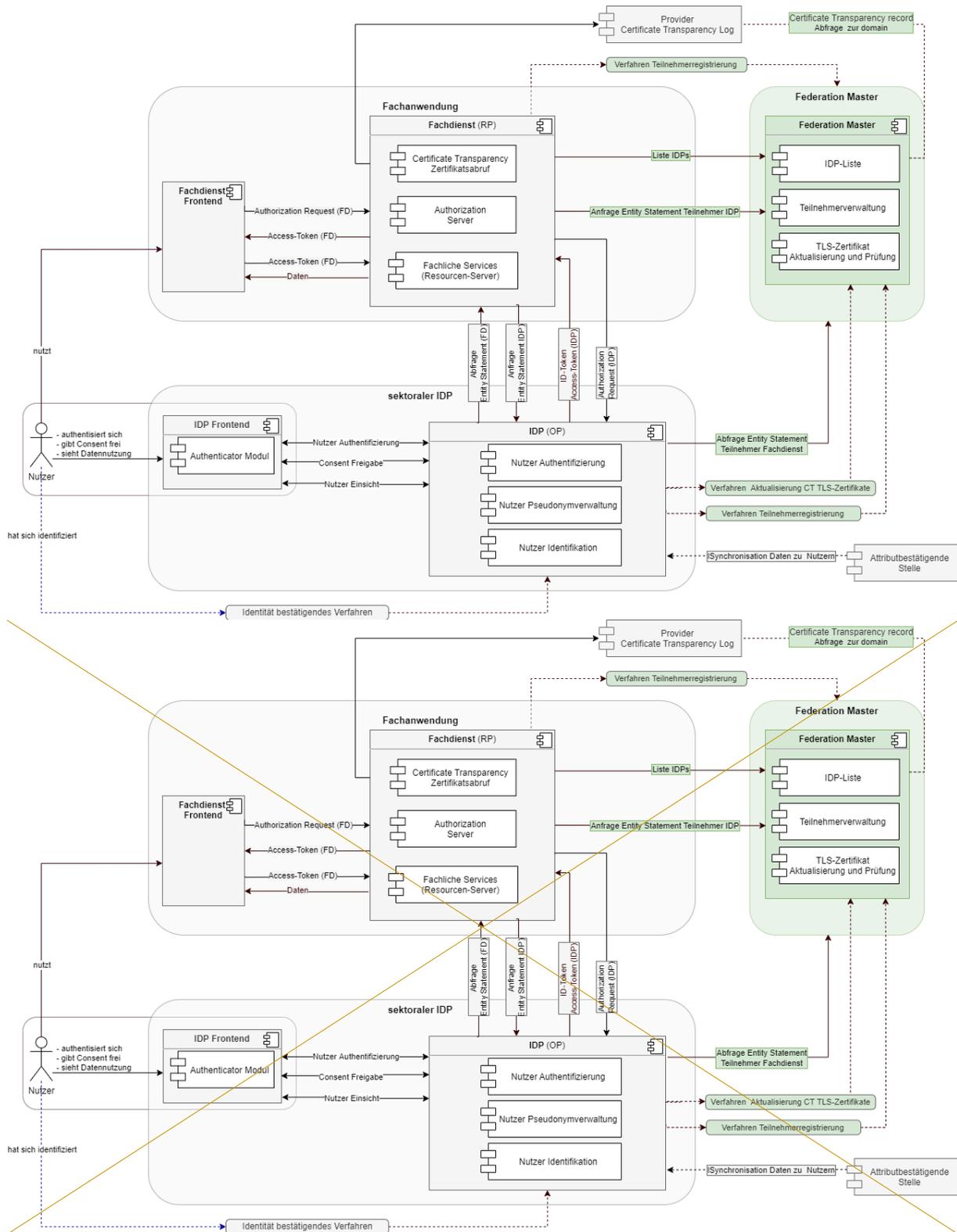


Abbildung 3: Übersichtsschaubild OIDC Federation

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

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 welcher gefragt wird - Teilnehmer

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

2.3 Akteure und Rollen

Tabelle 2: Akteure und Rollen

Komponente	Beschreibung
Federation Master	<ul style="list-style-type: none"> Der Federation Master bildet den Vertrauensanker der

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

2.4 Attributbeschreibung

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

Tabelle 3: Attributbeschreibung

Bezeichnung	Beschreibung	Wertebereich	Beispiel
iss	issuer = _URL des Federation Master	URL	"https://app-ref.federationmaster0815.de"
sub	subject = URL der Entity, nach welcher gefragt wird	URL	"https://app-ref.federationmaster0815.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)
jwtks	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.		{ "keys": [{ "ktu": "EC", "crv": "P-256", "x": "cdlR8dLbqaGrzfgyu365KM5s00zjFq8DFaUFqBvrWLs", "y": "XVp1ySJ2kjElnpjTZy0wD59afEXELpck0fk7vrMWrbw", "kid": "puk_fedmaster_sig", "use": "sig", "alg": "ES256" }] }
authority_hin	Ausgehend von einer Entität		{

<code>tsmetadata {</code>	die Metadaten zu Entities werden in Metadattypen unterteilt. Dabei ist jeder ID-Metadattyp ein JSON-Objekt und hält eine Reihe von key/value-Paaren, die eigentlichen Metadaten in der Trust-Chain bis hin zum Tru. Wenn das ist eine Entity-Anweisung auf dieselbe Entität wie das sub verweist Anchor (z.B. beim Federation Master), muss die Liste darf nicht leer sein Entity-Anweisung einen Metadaten-claim enthalten.		<code>"http://idp4711.de", "http://master0815.de" }</code>
<code>federation_entity {</code>			
<code>federation_fetch_endpoint</code>	Am federation_fetch_endpoint können Teilnehmer der TI-Föderation Informationen zu anderen Teilnehmern der TI-Föderation abfragen.	URL	<code>"https://app-ref.federationmaster.de/federation/fetch"</code>
<code>federation_list_endpoint</code>	Am federation_list_endpoint kann die Liste aller in der TI-Föderation registrierten Teilnehmer abgefragt werden.	URL	<code>"federation_list_endpoint": "https://app-ref.federationmaster.de/federation/list"</code>
<code>idp_list_endpoint</code>	Am idp_list_endpoint können Informationen zu allen in der TI-Föderation registrierten sektoralen IDPs abgefragt werden.	URL	<code>"https://app-ref.federationmaster.de/federation/listidps"</code>
<code>metadata}}</code>	Metadaten zu Entities werden in Metadattypen unterteilt. Dabei ist jeder Metadattyp ein JSON-Objekt und hält eine Reihe von key/value-Paaren, die eigentlichen Metadaten. Wenn das ist		<code>metadata { federation_entity { <key>:<value>, <key>:<value> }}</code>

	einer Entity-Anweisung auf dieselbe Entität wie das sub- verweist (z.B. beim Federation Master), muss die Entity-Anweisung einen Metadaten-claim enthalten.		
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

Anforderungen an die konkrete Belegung der Attribute im Entity Statement des Federation Master sind in Kapitel 4.1 beschrieben .

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:

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 (scopes bzw. claims) 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 bspw. E-Rezept, ePA) oder DiGA)s sein. Die Anmeldung für alle Anwendungen erfolgt über genau den Identity Provider, bei dem die elektronische Identität des Nutzers hinterlegt ist. <u>Zur Ermittlung ist der richtige Identity Provider wird nicht bekannt, so kann die Liste aller in der Föderation registrierten Identity Provider zur Ermittlung des richtigen Identity Provider vom Federation Master abgefragt werden.</u> Die Auswahl <u>trifftkann</u> dann <u>der Nurch den Nutzer im Kontext der Anmeldung getroffen werden.</u>
IDP-Liste bereitstellen	Federation Master	Zu allen in der Föderation registrierten Identity Providern werden die Informationen 'Organisationsname', 'Logo' und 'Zieladresse (URL)' ermittelt und als Liste bereitgestellt.
Autorisierung	Fachanwendung	Der Anwendungsfall <i>Autorisierung prüfen</i> ist

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

		und Adressen der Teilnehmer und beglaubigt sie gegenüber anderen Diensten. Das Einbringen der Daten neuer Teilnehmer bzw. das Löschen der Daten auszuschließender Teilnehmer erfolgt über organisatorische Prozesse (Teilnehmer registrieren, Teilnehmer löschen).
--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

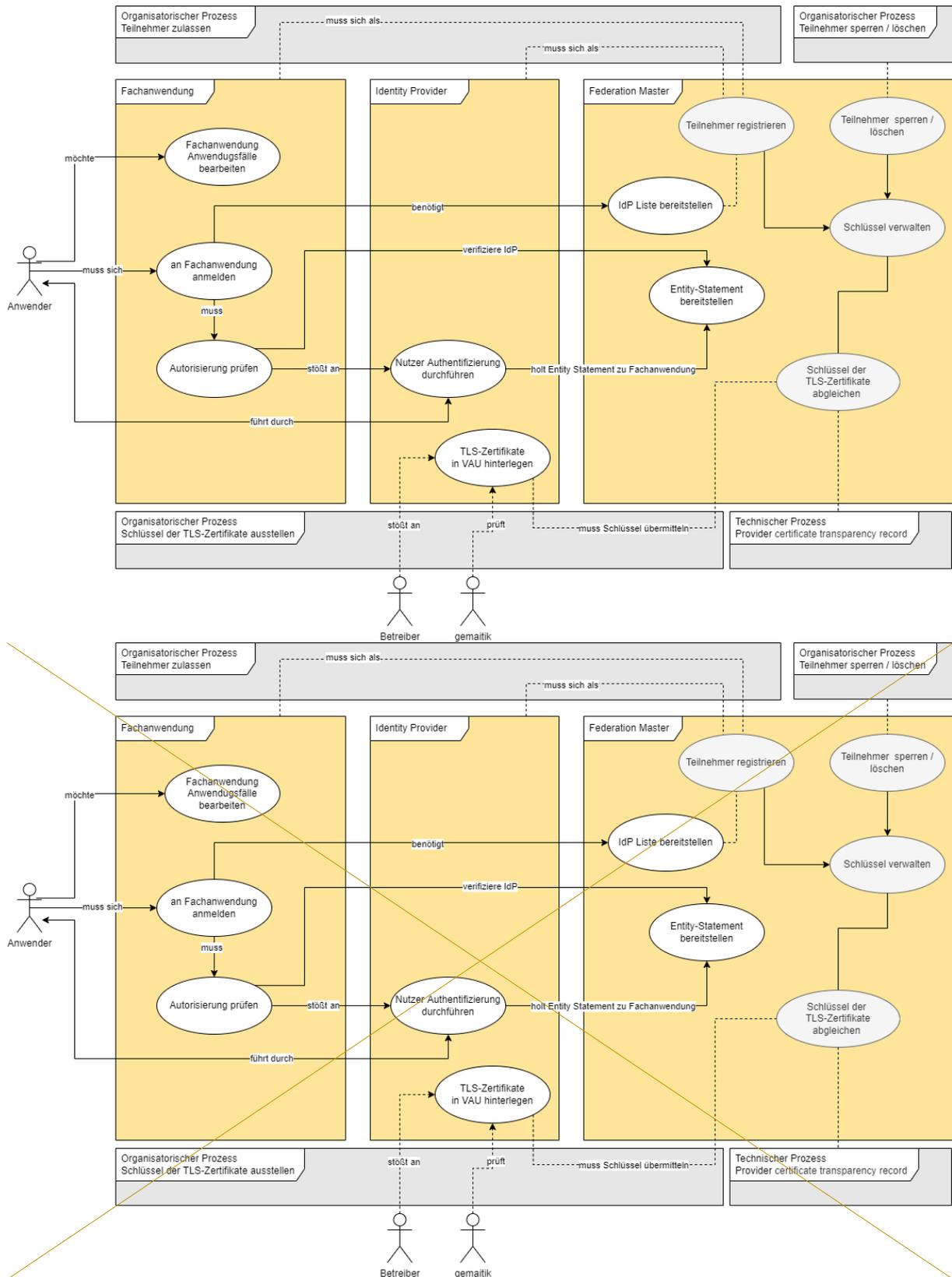


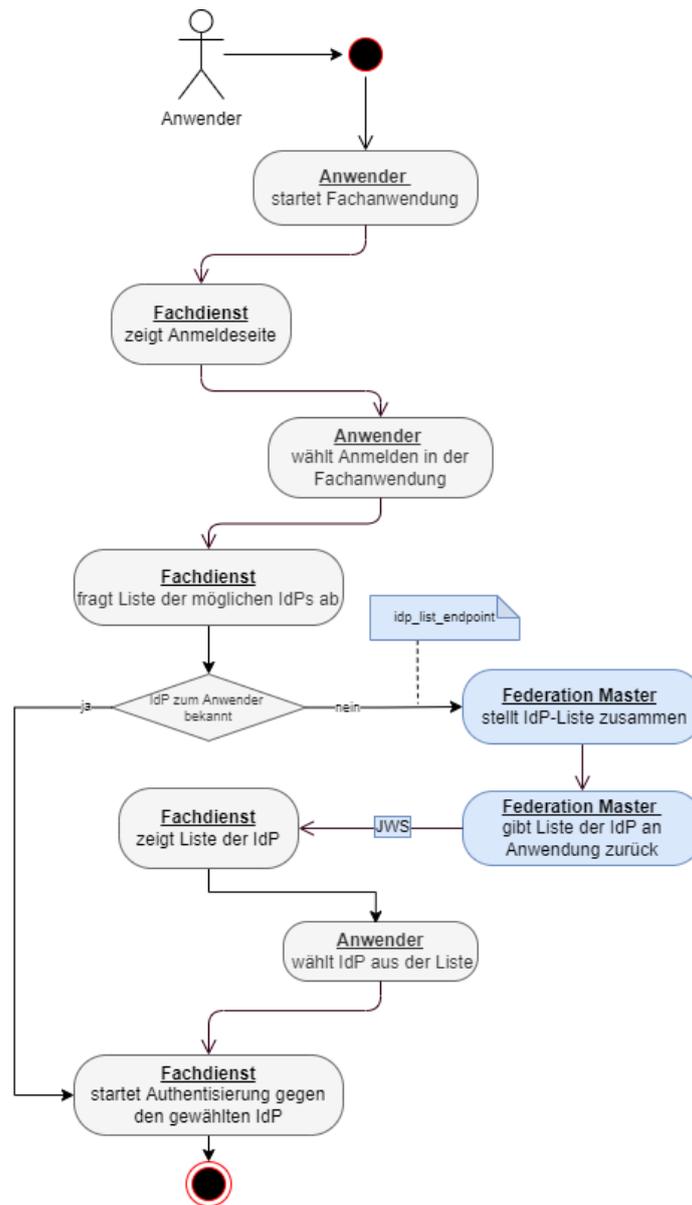
Abbildung 4: Anwendungsfälle Federation Master

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 löschen

Die technischen Anwendungsfälle des Federation Master werden hier im Detail beschrieben. Details zu den organisatorischen Anwendungsfällen des Federation Master finden sich in Kapitel [14.2 – Organisatorische Prozesse am Federation Master](#) [4.2-Organisatorische Prozesse am Federation Master](#). Die Ausprägung der Anwendungsfälle anderer Komponenten spielt im Rahmen dieser Spezifikation keine Rolle.

3.2 Anwendungsfall - IDP-Liste bereitstellen



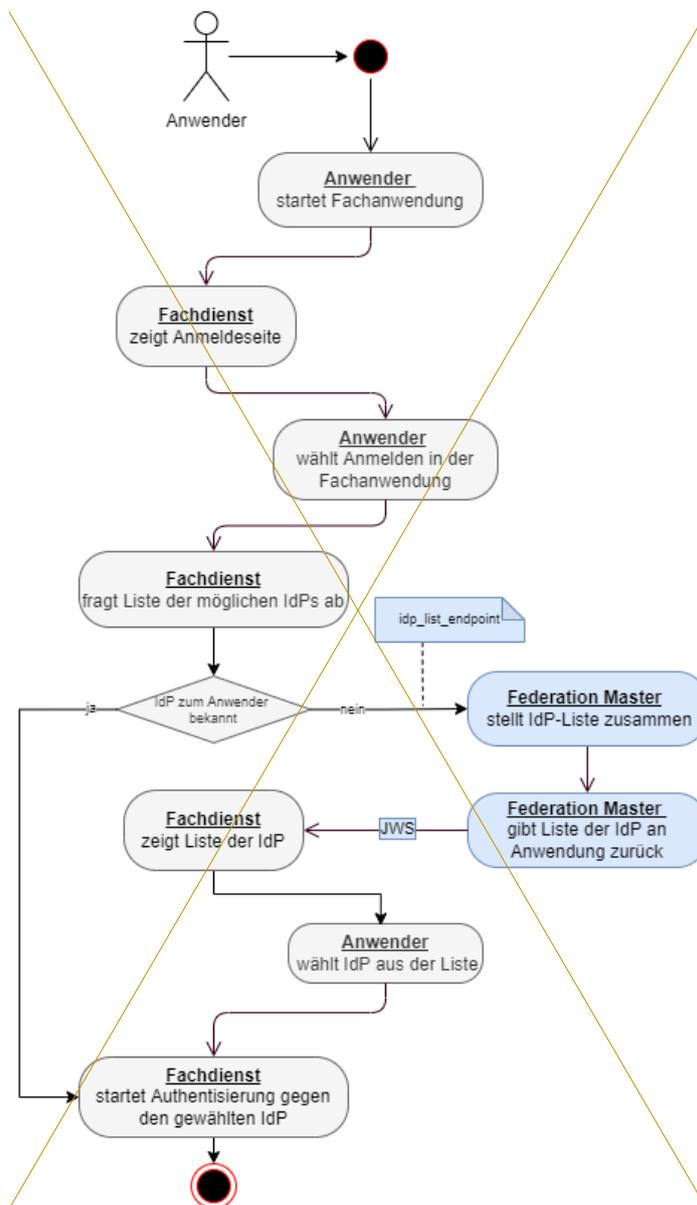


Abbildung 5: Aktivitätsdiagramm "Auswahl sektorale Identity Provider"

AF_10100-01 - Bereitstellung Liste registrierter Identity Provider

Tabelle 6: Anwendungsfall "Bereitstellung Liste registrierter Identity Provider"

Attribute	Bemerkung

<p>Beschreibung</p>	<p>Ein Anwender möchte einen in der TI registrierten 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 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. 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). • Information, ob es sich um einen sektoralen Identity Provider einer gesetzlichen oder privaten Krankenkasse handelt <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>
<p>Akteur</p>	<p>Anwender der Fachanwendung</p>
<p>Auslöser</p>	<p>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).</p>
<p>Komponenten</p>	<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

	<p>Verfügung und die unter dem Attribut <code>idp_list_endpoint</code> benannte URL MUSS aus dem Internet erreichbar sein.</p> <p>5. Der Federation Master hat die Entity Statements aller registrierten (sektoraler) Identity Provider innerhalb der letzten 24h aktualisiert</p>
<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 diese Attribute enthalten: <ol style="list-style-type: none"> a. Name der Organisation b. URI (iss) des sektoralen Identity Provider c. Logo der Organisation d. Unterstützte Anwendertypen e. Information, ob es sich um den sektoralen Identity Provider einer gesetzlichen oder privaten Krankenkasse handelt 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>2  ML-128409  ML-128409, 3  ML-143019  ML-143019</p>
<p>Alternativen</p>	<p>Die Fachanwendung kennt (z.B. aus früheren Sitzungen) den sektoralen Identity Provider des Anwenders. In diesem Fall KANN der Anwendungsfall ausgeführt werden.</p>

Tabelle 7: Liste sektorale Identity Provider - Payload-Attribute des signierten JSON-Web-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 der Liste (maximal iat + 24 Stunden)
idp_entity			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. <i>Hinweis: Ist ein sektoraler IDP ggf. temporär nicht erreichbar, so sollte das Herunterladen des Entity Statements über den sektoralen IDP weiter (z.B. stündlich) versucht werden.</i>
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.
pkv	Boolean (true/false)	true	Signalisiert, ob der Föderationsteilnehmer Teil der privaten Krankenversicherungen ist.

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

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

Name	Werte	Beispiel	Anmerkungen
alg	ES256	<-	
kid	wie aus jwks im Body des Entity		Identifiziert den verwendeten Schlüssel aus dem jwks im

	Statement		Body des Entity Statement des Federation Master
typ	idp-list+jwt	<-	

[<=]

3.2.1 Akzeptanzkriterien - IDP-Liste bereitstellen

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

Der Request vom Fachdienst an URL, welche im Entity Statement des Federation Master unter dem Attribut idp_list_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-143019 - AF_10100 - Payload des JWS-Token enthält Informationen zu jedem registrierten sektoralen Identity Provider der Föderation

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

- Organisationsname
- URL, unter welcher das Logo der Organisation abrufbar ist
- URI des sektoralen Identity Provider, welcher dem Identifier (iss) des sektoralen Identity Provider entspricht
- Liste der supporteten Usertype
- Information darüber ob der sektoralen Identity Provider für gesetzliche oder privatversicherte Patienten verwendet wird

[<=]

3.3 Anwendungsfall - Entity Statement bereitstellen

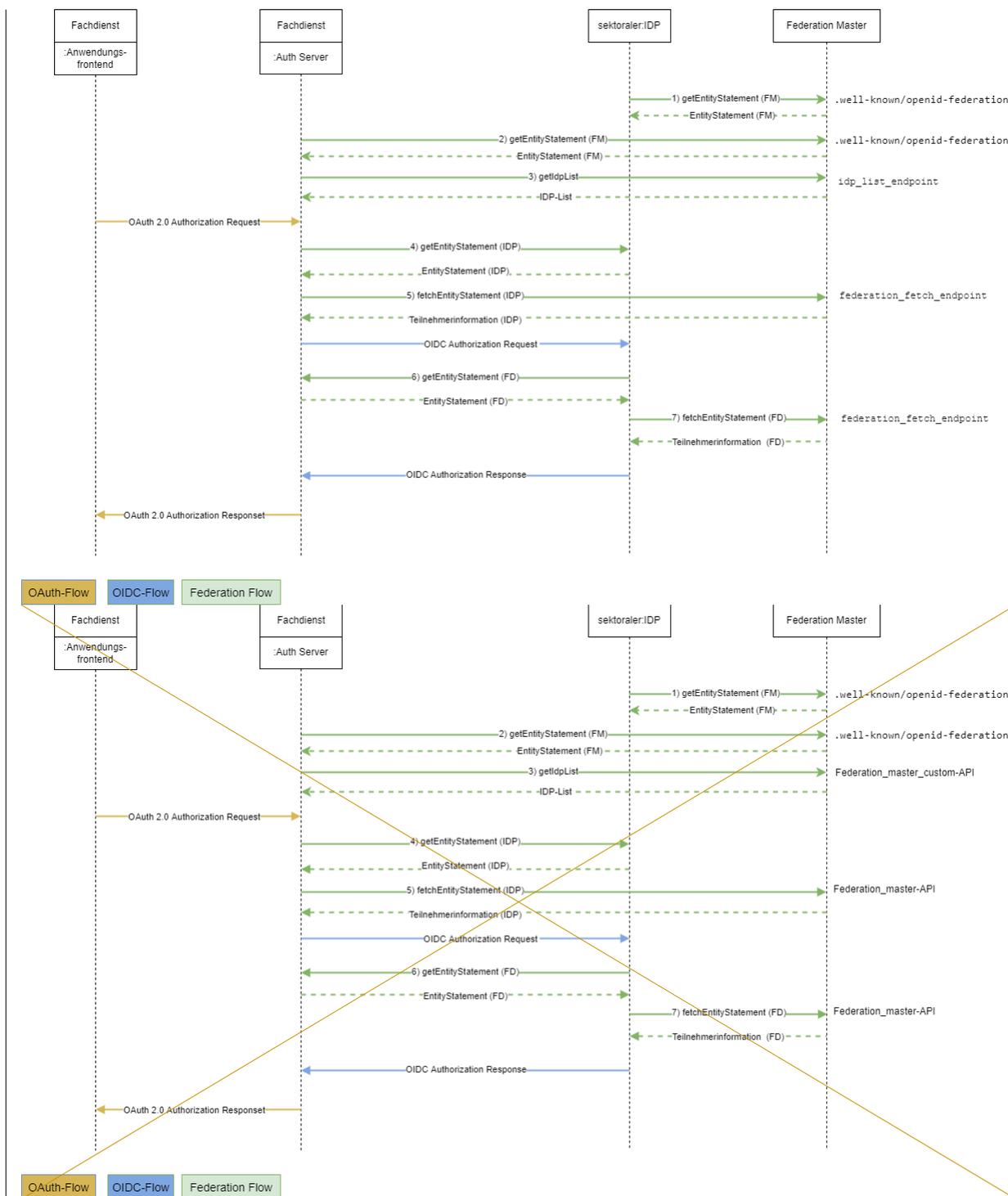


Abbildung 6: Federation Master im Authorization-Flow

Tabelle 9: Federation Master im Authorization-Flow

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

1 - getEntityStatement(FM)	sektoraler Identity Provider, Federation Master	Request zum Abholen des Entity Statement des Federation Master <u>am Endpunkt</u> .well-known/openid-federation/Federation Masters durch den sektoralen Identity Provider.
2 - getEntityStatement(FM)	Fachdienst, Federation Master	Request zum Abholen des Entity Statement des Federation Master- <u>am Endpunkt</u> .well-known/openid-federation/Federation Masters durch den Fachdienst.
3 - getIdpListe	Fachdienst, Federation Master	Request zum Abholen der Liste der in der Föderation registrierten sektoralen Identity Provider vom Federation Master durch den Fachdienst <u>am idp_list_endpoint Endpunkt des Federation Masters</u> .
4 - getEntityStatement(IDP)	Fachdienst, sektoraler Identity Provider	Request 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 <u>am Endpunkt federation_fetch_endpoint des Federation Masters</u> .
6 - getEntityStatement(FD)	sektoraler Identity Provider, Fachdienst	Request zum Abholen des Entity Statement des Fachdienstes vom Fachdienst durch den sektoralen Identity Provider.
7 - fetchEntityStatement(FD)	sektoraler Identity Provider, Federation Master	validieren des Fachdienstes als Teilnehmer der Föderation beim Federation Master durch den sektoralen Identity Provider <u>am Endpunkt federation_fetch_endpoint des Federation Masters</u> .

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.

28405AF_10101-01 - Bereitstellung von Informationen zu Teilnehmern der Föderation durch den Federation Master

Tabelle 10: 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"> • Federation Master • Fachdienst der TI • sektoraler Identity Provider
Vorbedingung	<ul style="list-style-type: none"> • Der Fachdienst ist in der TI-Föderation registriert und sein öffentlicher Schlüssel und sein Entity Statement sind beim Federation Master hinterlegt. • Der sektorale Identity Provider ist in der TI-Föderation registriert und 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_fetch_endpoint</code> benannte URL MUSS aus dem Internet erreichbar sein.
Ablauf	<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_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_fetch_endpoint</code> im Entity Statement des

	<p>Federation Master festgelegte URL. Der Request MUSS die in Tabelle "Teilnehmer Validierung Abfrage - Request Parameter" Parameter umfassen.</p> <ul style="list-style-type: none"> 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-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	<p>4  ML-128451  ML-128451 , 5  ML-128452  ML-136402 , 6  ML-136402  ML-152179</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 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)
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.

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

Attribut	Werte /	Beispiel	Anmerkungen
----------	---------	----------	-------------

	Typ		
iss	URL	"http://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, 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 Liste (maximal iat + 24 Stunden)
kwks	JWKS Objekt		öffentlicher Schlüssel des angefragten Teilnehmer (sektoraler Identity Provider bzw. Fachdienst)

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

Tabelle 13: Teilnehmer Validierung - Response-Header-Attribute des signierten JSON-Web-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 Statement
typ	entity-statement+jwt	<-	

[<=]

3.3.1 Akzeptanzkriterien - Entity Statement bereitstellen

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. [<=]

Hinweis: Für den Fetch Entity Request gelten die Festlegung im Standard [OpenID Connect Federation 1.0] Kapitel 7.1.1.

28452ML-12845252179 - 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~~ [gemSpec_IDP_Sek - Anhang B - Abläufe](#)):

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

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

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

| [\leq]

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

| 3.4 Anwendungsfall - Schlüssel verwalten

AF_10110 - Monitoring der TLS- Zertifikate der VAU

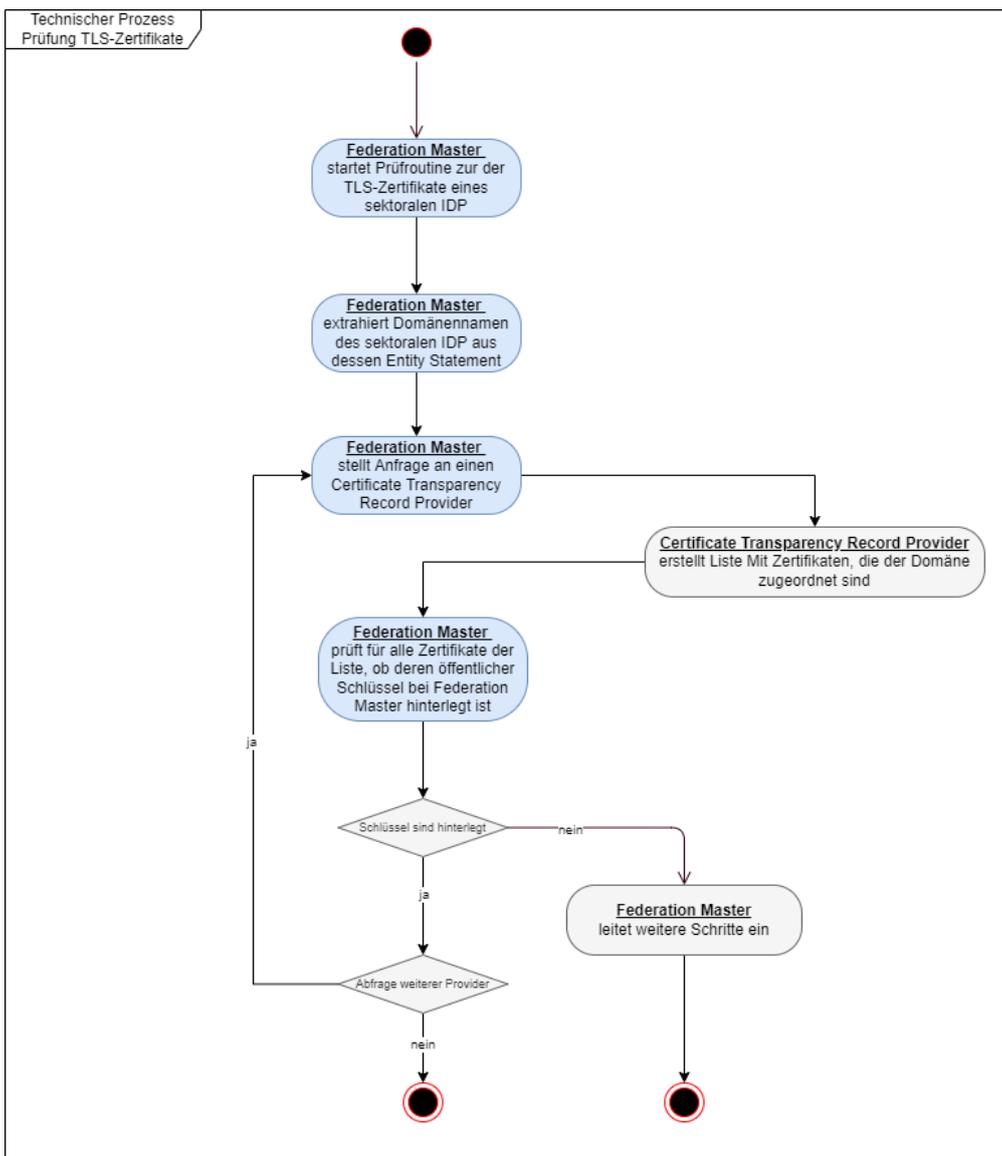


Abbildung 7: Prüfung der TLS-Zertifikate eines sektoralen Identity Provider am Federation Master

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-Dienstes mündet, wird erstellt. Regelmäßige Prüfung der veröffentlichten TLS-Zertifikate
Komponente	<ul style="list-style-type: none"> Federation Master sektoraler Identity Provider
Vorbedingung	<p>Der sektorale Identity Provider ist in der TI-Föderation registriert. Bei neu erstellten TLS-Zertifikaten wurde der Prozess <u>8Certificate Transparency TLS-Zertifikate der sektoralen Identity Provider prüfen</u> erfolgreich durchlaufen. Die öffentlichen Schlüssel des sektoralen Identity Provider und seine öffentliche TLS-Schlüssel 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-Dienstes 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 aus den im Entity Statement des sektoralen Identity Provider hinterlegten Adressen zum Token-, PAR- und Authorization-Endpunkt die Domännennamen.</p> <p>Der Federation Master fragt mit allen ermittelten Domännennamen die Schnittstelle mindestens zweier unterschiedlicher öffentlich zugänglicher Provider für Certificate Transparency Records ab (z.B. https://sslmate.com/ct_search_api/). Die Provider liefern alle registrierten Zertifikate zum Domännennamen.</p> <p>Der Federation Master MUSS jedes Zertifikat dahingehend 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 mindestens eine Prüfung negativ, MUSS der Federation Master weitere Schritte hinsichtlich des negativ geprüften sektoralen Identity Provider einleiten und einen "Security Incident" (gemäß 3.4 aus [gemRL_Betr_TI])</p>

	erstellen.
Akzeptanzkriterien	9  ML-132625  ML-132625 , 10  ML-132627  ML-132627
Alternativen	-

[<=]

3.4.1 Akzeptanzkriterien - Schlüssel verwalten

ML-132625 - AF_10110 - Ablage der TLS-Schlüssel im Federation Master

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

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

ML-132627 - AF_10110 - TLS-Schlüsselprüfung durch den Federation Master nicht erfolgreich

Gibt es mindestens ein TLS-Zertifikat zu einer second-level, third-level bzw. higher-level domain eines sektoralen Identity Provider, der in der VAU terminiert und dessen öffentlicher Schlüssel nicht oder falsch beim Federation Master registriert ist, so ist die Prüfung nicht erfolgreich. Der Betreiber des Federation Master hat Schritte zur Problemklärung (gemäß A_22968) eingeleitet. [<=]

4 Anforderungen an den Produkttyp

4.1 Aufbau und Inhalt des Federation Master Entity Statement

Der Federation Master bildet den Vertrauensanker der Föderation. Ebenso ist der Federation Master eine Entität innerhalb der Föderation. Gemäß dem verwendeten Standard OpenID Connect 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 nutzenden Anwendungen eine einheitliche Bezugsquelle für die Adressierung von Schnittstellen zu schaffen, werden die für alle Akteure grundlegenden Schnittstellen im sogenannten Entity Statement zusammengefasst und dort unter der ".well-known/openid-federation" gemäß [[OpenID Connect Federation 1.0#rfc.section.6](#)] veröffentlicht.

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

- Validierung der Vertrauenskette in der Kommunikation zwischen Fachdiensten und sektoralem Identity Provider
- Validierung anderer Kommunikationsteilnehmer in der Föderation
- Ermittlung des API-Endpunktes des Federation Master
- Ermittlung der Liste aller in der Föderation registrierten sektoralen Identity Provider.

A_22947 - Aktualisierungszyklen für die Liste der registrierten sektoralen Identity Provider

Der Federation Master MUSS die Liste der registrierten sektoralen Identity Provider täglich aktualisieren. Darüber hinaus MUSS der Federation Master die Liste bei Neuregistrierung oder Löschung von sektoralen Identity Providern aktualisieren. [**<=**]

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. [**<=**]

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. [**<=**]

Hinweis: Ist ein sektoraler IDP ggf. temporär nicht erreichbar, so sollte das Herunterladen des Entity Statements über den Federation Master weiter (z.B. stündlich) versucht werden.

A_25414 - Prüfung der Entity Statements von Fachdiensten

Der Anbieter des Federation Master MUSS einen Prozess etablieren, in dem der Anbieter des Federation Master mindestens täglich die Entity Statements der Fachdienste abfragt und die Werte der in Tabelle "Prüfung der Entity Statements von Fachdiensten"

aufgeführten Attribute hinsichtlich der bei der Registrierung hinterlegten Werte prüft. Stimmen die Werte nicht überein, so MUSS der Federation Master die in der Tabelle aufgeführten Maßnahmen treffen.

Tabelle 15 : Prüfung der Entity Statements von Fachdiensten

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

	<u>Fachdienst anfragbaren claims hat sich geändert.</u>	Umfang, der anfragbaren claims erweitert, so besteht die Gefahr des unberechtigten Zugriffs auf Identitätsdaten Eine Verringerung des Umfangs der anfragbaren claims hat keine negativen Auswirkungen.	en eines Incident und Sperren des Teilnehmers in der Föderation
<u>redirect_uris</u>	<u>Der Inhalt der Liste der URLs, an den die vom IDP ausgestellten Identitätsinformationen geschickt werden, hat sich geändert.</u>	Die vom IDP ausgestellten Identitätsinformationen können ggf. an unberechtigte Endpunkte verschickt werden, so besteht die Gefahr des unberechtigten Zugriffs auf Identitätsdaten	Einstellen eines Incident und Sperren des Teilnehmers in der Föderation
<u>metadata.openid_relying_party.organization_name</u>	<u>Der Name der Organisation hat sich geändert.</u>	Die Änderung kann zu Anzeigeproblemen bei den Nutzern führen.	Einstellen eines Incident
<u>metadata.openid_relying_party.client_name</u>	<u>Der Name des Fachdienstes (redundant zu metadata:federation_entity:name) hat sich geändert.</u>	Die Änderung kann zu Anzeigeproblemen bei den Nutzern führen.	Einstellen eines Incident
<u>metadata.federation_entity.name</u>	<u>Der Name des Fachdienstes (redundant zu metadata:openid_relying_party:client_name) hat sich geändert.</u>	Die Änderung kann zu Anzeigeproblemen bei den Nutzern	Einstellen eines Incident

		führen.
--	--	---------

[<=]

Hinweis 1: 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 https://openid.net/specs/openid-federation-1_0.html#error_response mit Error Code HTTP-401 invalid_client.

Hinweis 2: Zum Entsperren muss der Fachdienst die Abweichungen in seinem Entity Statement korrigieren oder im Fall gewollter Änderungen zur Aktualisierung den organisatorischen Registrierungsprozess erneut durchlaufen.

2A_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.[<=]

Hinweis: Die Anforderung ist als SOLL formuliert. Von dieser Anforderung kann abgewichen werden, wenn es begründete Bedenken (z.B. weitere Incidents) gegen die Zulassung des Fachdienstes gibt.

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 Connect Federation 1.0#rfc.section.3.1](#)] im Internet veröffentlichen.[<=]

A_22605 - Entity Statement Veröffentlichung

Der Federation Master MUSS sein Entity Statement im Internet gemäß [[OpenID Connect Federation 1.0#rfc.section.6](#)] unter ".well-known/openid-federation" veröffentlichen.[<=]

A_22606 - Entity Statement - Prüfung der angebotenen URL

Der Anbieter des Federation Master MUSS alle von ihm im Entity Statement angebotenen URL ständig auf bloße Erreichbarkeit prüfen.[<=]

A_22607 - Inhalte des Federation Master Entity Statement

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

Tabelle 16: 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
jwtks	JWKS	Schlüssel für die Signatur des Entity Statement	"master0815-1"

exp	long	Alle time-Werte in Sekunden seit 1970, RFC 7519 Sect.2	1645484400 = Gültigkeit von 24 Stunden in Bezug auf den Wert in iat
-----	------	------------------------------------------------------------------------	---------------------------------------------------------------------

[<=]

A_22608 - Inhalte des Metadata Federation API-Endpunkt im Federation Master Entity Statement

Der Federation Master MUSS im Entity Statement gemäß [[OpenID Connect Federation 1.0#rfc.section.4.6](#)] mindestens die folgenden Attribute als metadata/federation_entity angeben:

Tabelle 17: 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	"http://master0815.de/federation_fetch"
federation_list_endpoint	URL	Adresse des Endpunktes zum Abrufen der Liste aller bekannten Entity Identifier	"http://master0815.de/federation_list"

[<=]

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

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

Tabelle 18: 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, Identifier und Nutzergruppe	"http://master0815.de/idp_list.jws"

[<=]

A_23087 - Entity Statements gelöschter Teilnehmer

Der Federation Master MUSS sicherstellen, dass der Abruf des Entity Statement gelöschter Teilnehmer über das Federation Master API zu einer Fehlermeldung unter Berücksichtigung des Standards [[OpenID Connect Federation 1.0#rfc.section.7.5](#)] führt.

[<=]

4.2 Organisatorische Prozesse am Federation Master

A_22675-01 - Teilnehmerregistrierung am Federation Master

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

[<=]

Hinweis 1: Der Aufbau und die Verwendung der hierarchischen Vertrauensbeziehung (Trust Chain) ist im Standard [[OpenID Connect Federation 1.0](#)] festgelegt und wird darüber hinaus hier nicht weiter spezifiziert.

Hinweis 2: Die Registrierung MUSS für jede Betriebsumgebung separat erfolgen. Betriebsumgebungen sind Test-Umgebung (TU), Referenz-Umgebung (RU) und die Produktiv-Umgebung (PU). Die Registrierung für die Produktiv-Umgebung erfolgt erst nach Zulassung oder Bestätigung.

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

Mainline_OPB1/ML_145784A_22741-01 – Prüfung "scope" 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 dort aufgeführten scopes und claims hinsichtlich der bei der Registrierung hinterlegten scopes und claims prüft. Ist die Prüfung nicht erfolgreich, MUSS der Anbieter des Federation Master organisatorische und/oder technische Prozesse mit geeigneten Maßnahmen zur Problembeseitigung etablieren.~~

[<=]

~~*Hinweis 1: Geeignete Maßnahmen können je nach Analyseergebnis z.B. das Einstellen von Security-Bugs beim Betreiber des Fachdienstes, die Einstellung eines sicherheitsrelevanten Notfalls gegen den Anbieter des entsprechenden Fachdienstes*~~

durch den Federation Master im TI-ITSM (für TI-ITSM Teilnehmer), aber auch das Löschen des betroffenen Fachdienstes sein.

Hinweis 2: Ist ein sektoraler IDP ggf. temporär nicht erreichbar, so sollte das Herunterladen des Entity Statements über den sektoralen IDP weiter (z.B. stündlich) versucht werden.

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. [\leq]

Hinweise 1: Die Abwicklung kann über Service Request durch gematik. oder durch definierte Trigger im Rahmen eines Sicherheitsvorfalls erfolgen.

Hinweis 2: Beim Löschen eines sektoralen Identity Providers aus der Föderation wird zusätzlich die Sperrung der Signaturzertifikate in der Komponenten-PKI veranlasst, welche dieser zur Signatur seiner ID_TOKEN verwendet. Dies geschieht selbstständig durch den Anbieter des IDP oder bei "Wegfall der Voraussetzung für den Betrieb" durch die gematik.

A_22945 - Schlüssel für Certificate Transparency TLS-Zertifikate übergeben

Der Anbieter des Federation Master MUSS einen organisatorischen Prozess etablieren, über den die Übergabe der öffentlichen Schlüssel von TLS-Zertifikaten zu Domänen eines sektoralen Identity Provider, welche in der VAU terminieren, vom Anbieter des sektoralen IDP an den Federation Master erfolgt. [\leq]

Hinweis: Für den Ablauf der Schlüsselprüfungen siehe [113.4-1-Monitoring der TLS-Zertifikate der VAU](#) [3.4-1-Monitoring der TLS-Zertifikate der VAU](#)

A_22968 - Maßnahmen bei nicht erfolgreicher TLS-Zertifikatsprüfung durch den Federation Master

Gibt es mindestens ein TLS-Zertifikat der Domäne/Unterdomeäne eines sektoralen 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 geeigneten Maßnahmen zur Analyse und Problembeseitigung etablieren. [\leq]

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

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:

- Privater Schlüssel und öffentlicher Schlüssel des Federation Master
- 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.

[<=]

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. [<=]

4.4 Sicherheit der Netzübergänge

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). [<=]

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. [<=]

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. [<=]

A_22594 - Federation Master - Verhalten bei Vollausslastung

Der Anbieter des Federation Master MUSS den Paketfilter des Federation Master so konfigurieren, dass bei Vollausslastung der Systemressourcen im Federation Master keine weiteren Verbindungen angenommen werden. [<=]

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

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 unbekanntes 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. [<=]

4.5 Fehlermeldungen

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 Connect Federation 1.0#rfc.section.7.5](#)] MÜSSEN bei der Definition der Meldungsinhalte berücksichtigt werden. <=[<=]

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#rfc.section.7.5](#)] MÜSSEN bei der Definition der Fehlercodes berücksichtigt werden. [<=]

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. [<=]

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. [<=]

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. [<=]

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. [<=]

5 Anhang - Verzeichnisse

5.1 Abkürzungen

Tabelle 19: 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

5.2 Glossar

Tabelle 20: 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 claim 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 ACCESS_TOKEN. Das JWT ermöglicht den Austausch von verifizierbaren claims innerhalb seines Payloads.
Nutzergruppen	Nutzergruppen sind Personengruppen mit bestimmten Rollen im Kontext der TI-Anwendungslandschaft. Nutzergruppen sind beispielsweise Versicherte und Leistungserbringer (ggf. weiter differenziert - Ärzte, Zahnärzte, etc.)
Open Authorization 2.0	Ein Protokoll zur Autorisierung für Web-, Desktop und Mobile Anwendungen. Dabei wird es einem Endbenutzer (Resource Owner) ermöglicht, einer Anwendung (Client) den Zugriff auf Daten oder Dienste (Resources) zu ermöglichen, die von einem Dritten (Resource Server) bereitgestellt werden.
OpenID Connect	OpenID Connect (OIDC) ist eine Authentifizierungsschicht, die auf dem Autorisierungsframework OAuth 2.0 basiert. Es ermöglicht Clients, die Identität des Nutzers anhand der Authentifizierung durch einen Authorization-Server zu überprüfen (siehe [OpenID Connect Core 1.0]).
Pushed Authorization Request (PAR)	Der Pushed Authorization Request (PAR) ermöglicht es Clients, eine OAuth 2.0-Autorisierungsanforderung direkt an den Authorization-Server des sektoralen Identity Provider zu senden. Die übergeben redirect-URI ist Autorisierungsendpunkt und wird im weiteren Flow verwendet. https://datatracker.ietf.org/doc/html/rfc9126
Resource Owner	OAuth2-Rolle (siehe [RFC6749 # section-1.1]): Eine Entität (Nutzer), die einem Dritten den Zugriff auf ihre geschützten Ressourcen gewähren kann. Diese Ressourcen werden durch den Resource Server bereitgestellt. Ist der Resource Owner eine Person, wird dieser als Nutzer bezeichnet.
Resource Server	OAuth2 Rolle (siehe [RFC6749 # section-1.1]): Der Server (Dienst), auf dem die geschützten Ressourcen (Protected Resources) liegen. Er ist in der Lage, auf Basis von Access Tokens darauf Zugriff zu gewähren. Ein solcher Token repräsentiert die delegierte Autorisierung des Resource Owners.
Scope	scopes definieren ein festgelegtes Set an claims. Mit scopes lässt sich steuern, dass Anwendungen oder Anwendungsgruppen nur genau die Informationen einer Identität bekommen, die für die Anwendungsfälle der Anwendung(en) notwendig sind. Im Kontext OIDC gibt es vordefinierte scopes wie <i>openid</i> , <i>profile</i> und <i>email</i> , die verwendet werden können (siehe auch OpenID Connect Basic Client Implementer's Guide 1.0#Scopes). In der

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

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

5.3 Abbildungsverzeichnis

Abbildung 1: Überblick TI-Föderation.....	9
Abbildung 2: Systemkontext.....	10
Abbildung 3: Übersichtsschaubild OIDC Federation.....	11
Abbildung 4: Anwendungsfälle Federation Master.....	18
Abbildung 5: Aktivitätsdiagramm "Auswahl sektorale Identity Provider".....	20
Abbildung 6: Federation Master im Authorization-Flow.....	26
Abbildung 7: Prüfung der TLS-Zertifikate eines sektoralen Identity Provider am Federation Master.....	33
Abbildung 1: Überblick TI-Föderation.....	10
Abbildung 2: Systemkontext.....	12
Abbildung 3: Übersichtsschaubild OIDC Federation.....	14
Abbildung 4: Anwendungsfälle Federation Master.....	23
Abbildung 5: Aktivitätsdiagramm "Auswahl sektorale Identity Provider".....	26
Abbildung 6: Federation Master im Authorization-Flow.....	33
Abbildung 7: Prüfung der TLS-Zertifikate eines sektoralen Identity Provider am Federation Master.....	41

5.4 Tabellenverzeichnis

Tabelle 1: Request zur Teilnehmerabfrage an den Federation Master.....	12
Tabelle 2: Akteure und Rollen.....	12
Tabelle 3: Attributbeschreibung.....	14
Tabelle 4: Übersicht über die Anwendungsfälle im Gesamtkontext Federation Master.....	16
Tabelle 5: Anwendungsfälle Federation Master.....	18

	Tabelle 6: Anwendungsfall "Bereitstellung Liste registrierter Identity Provider".....	20
	Tabelle 7: Liste sektorale Identity Provider –Payload-Attribute des signierten JSON-Web-Token.....	23
	Tabelle 8: Liste sektorale Identity Provider –Headerattribute des signierten JSON-Web-Token.....	25
	Tabelle 9: Federation Master im Authorization-Flow.....	26
	Tabelle 10: Anwendungsfall "Bereitstellung von Informationen zu Teilnehmern der Föderation durch den Federation Master".....	28
	Tabelle 11: Teilnehmer Validierung Abfrage –Request-Parameter.....	29
	Tabelle 12: Teilnehmer Validierung Abfrage – Response-Payload-Attribute des signierten-JSON-Web-Token.....	30
	Tabelle 13: Teilnehmer Validierung – Response-Header-Attribute des signierten JSON-Web-Token.....	31
	Tabelle 14: Anwendungsfall "Monitoring der TLS-Zertifikate der VAU".....	33
	Tabelle 15: Attribute Entity Statement Federation Master.....	37
	Tabelle 16: Attribut "Federation API Endpoint".....	37
	Tabelle 17: Attribut "IDP List Endpoint".....	38
	Tabelle 18: Abkürzungen.....	43
	Tabelle 19: Glossar.....	43
	Tabelle 20: Quellen.....	47
	Tabelle 21: Weitere Dokumente.....	48
	Tabelle 1: Request zur Teilnehmerabfrage an den Federation Master.....	15
	Tabelle 2: Akteure und Rollen.....	16
	Tabelle 3: Attributbeschreibung.....	17
	Tabelle 4: Übersicht über die Anwendungsfälle im Gesamtkontext Federation Master.....	20
	Tabelle 5: Anwendungsfälle Federation Master.....	24
	Tabelle 6: Anwendungsfall "Bereitstellung Liste registrierter Identity Provider".....	26
	Tabelle 7: Liste sektorale Identity Provider - Payload-Attribute des signierten JSON-Web-Token.....	29
	Tabelle 8: Liste sektorale Identity Provider - Headerattribute des signierten JSON-Web-Token.....	31
	Tabelle 9: Federation Master im Authorization-Flow.....	33
	Tabelle 10: Anwendungsfall "Bereitstellung von Informationen zu Teilnehmern der Föderation durch den Federation Master".....	35
	Tabelle 11: Teilnehmer Validierung Abfrage - Request-Parameter.....	36
	Tabelle 12: Teilnehmer Validierung Abfrage - Response-Payload-Attribute des signierten JSON-Web-Token.....	37
	Tabelle 13: Teilnehmer Validierung - Response-Header-Attribute des signierten JSON-Web-Token.....	38
	Tabelle 14: Anwendungsfall "Monitoring der TLS-Zertifikate der VAU".....	41

Tabelle 15 : Prüfung der Entity Statements von Fachdiensten.....45
 Tabelle 16: Attribute Entity Statement Federation Master.....48
 Tabelle 17: Attribut "Federation API Endpoint".....48
 Tabelle 18: Attribut "IDP List Endpoint".....49
 Tabelle 19: Abkürzungen..... 54
 Tabelle 20: Glossar..... 54
 Tabelle 21: Quellen..... 59
 Tabelle 22: Weitere Dokumente.....60

5.5 Referenzierte Dokumente

5.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur.

Tabelle 21: 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

5.5.2 Weitere Dokumente

Tabelle 22: Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
JWT [RFC7519]	JSON Web Token (JWT) (Mai 2015) https://datatracker.ietf.org/doc/html/rfc7519
OAuth 2.0 Spezifikation	The OAuth 2.0 Authorization Framework (Oktober 2012) https://datatracker.ietf.org/doc/html/rfc6749

[[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 (Draft 21, 2022) https://openid.net/specs/openid-connect-federation-1_0-21.html
[Pushed Authorization Request]	OAuth 2.0 Pushed Authorization Requests (September 2021) https://datatracker.ietf.org/doc/html/rfc9126
PKCE ([RFC7636])	Proof Key for Code Exchange by OAuth Public Clients (September 2015) https://datatracker.ietf.org/doc/html/rfc7636
CAB-Forum	https://cabforum.org/
OWASP	Open Web Application Security Project https://owasp.org/
Certificate Transparency (CT)	Certificate Transparency Version 2.0 (Dezember 2021) https://datatracker.ietf.org/doc/html/rfc9162

