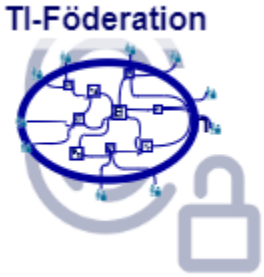
Federation Master

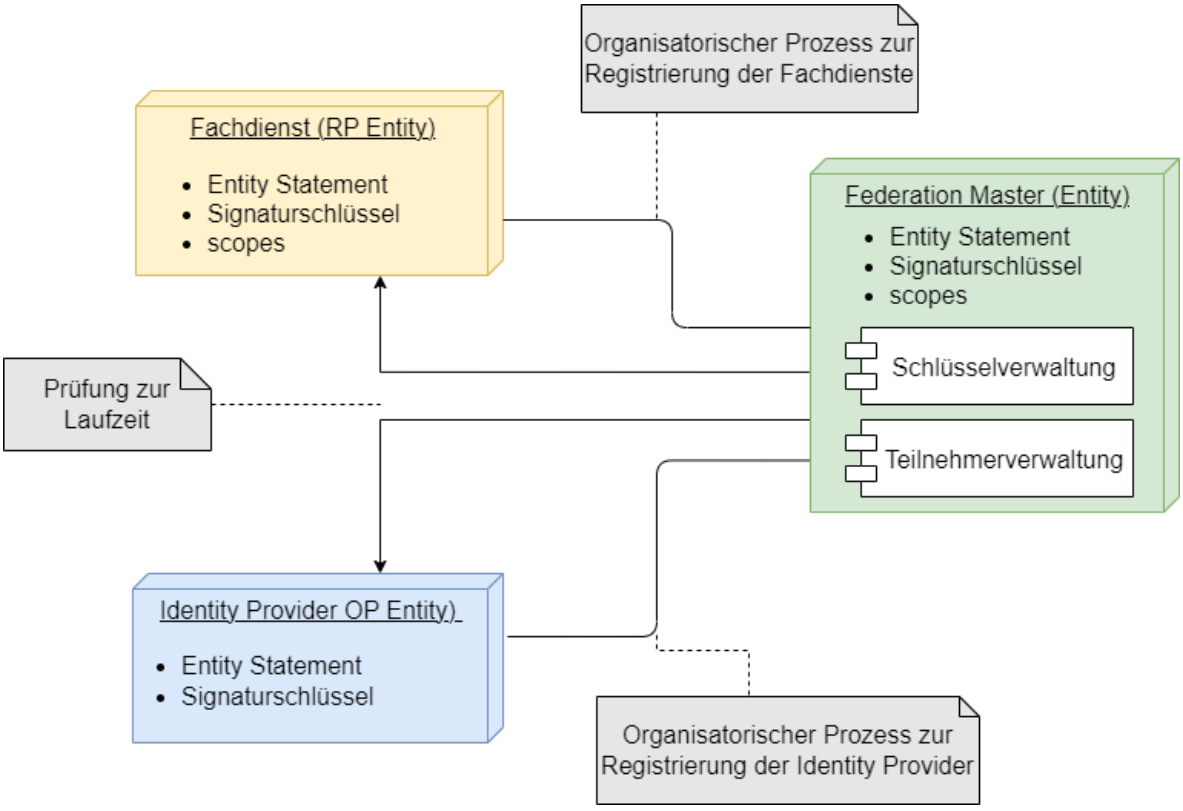


Überblick

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 notwendig:

- 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).

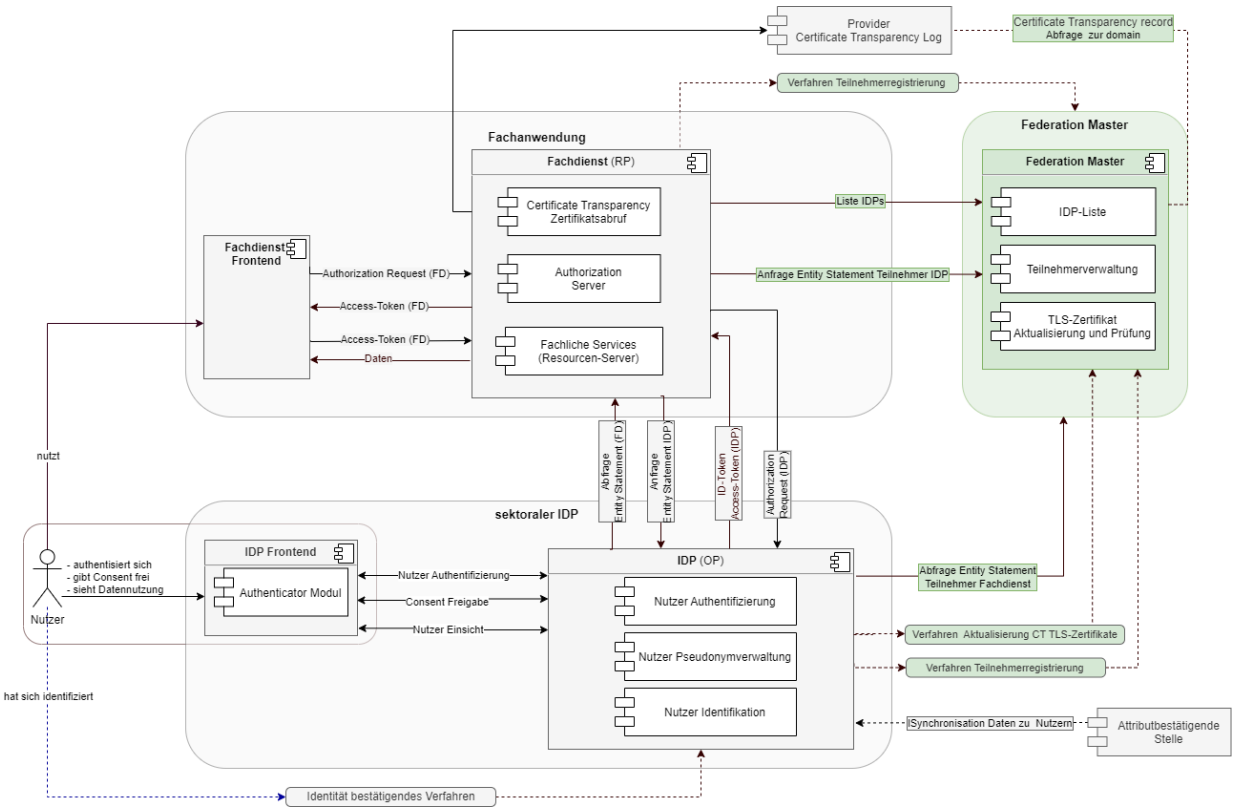
Die Grundidee der Föderation ist die Erstellung eines Vertrauensraums, in dem verschiedene Anwendungen und Identity Provider abgesichert über Vertrauensketten (Trust chain) miteinander kommunizieren, ohne zuvor über organisatorische Prozesse miteinander verknüpft zu werden. Diese Anwendungen und Identity 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 [Auth 2.0] und [OpenID Connect].



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 sowie des Federation Master entsprechen den Vorgaben [OpenID Connect Federation 1.0]

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 Anwendungsfrontend 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 (OpenID Connect Core 1.0) und Pushed Authorization Request (RFC9126) und wird hier ebenfalls nicht detailliert beschrieben.



Grün dargestellt sind die Komponenten und Schnittstellen des Federation Master. Grau dargestellt sind die weiteren beteiligten Komponenten und Schnittstellen der Föderation. 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.

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. 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. 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. Nur bei erfolgreicher Rückmeldung des Federation Master zum angefragten Teilnehmer wird der Ablauf zur Nutzerauthentifizierung durchgeführt.

Tabelle : 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

Akteure & Rollen

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 registrieren sektoralen Identity Provider.

Tabelle : Akteure und Rollen

Komponente	Beschreibung
Federation Master	• Der Federation Master bildet den Vertrauensanker der Föderation gemäß [OpenID Connect Federation 1.0] • Der Federation Master ist eine Entität im Sinne von OIDC und muss ein Entity Statement (Entitätsaussage) mit den Eigenschaften der Entität veröffentlichen. • 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.
sektoraler Identity Provider	• 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 veröffentlichen. • 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.
Fachdienst	• 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 veröffentlichen. • 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.

Attributbeschreibung

Entity Statement

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 : Attributbeschreibung des Entity Statements

Bezeichnung	Beschreibung	Wertebereich	Beispiel
iss	issuer = URL des Federation Master	URL	"http://master0815.de"
sub	subject = URL 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	1646002800 (2022-

		seit 1970, RFC 7519 Sect.2	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"]

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

Metadaten im Entity Statement

Die Metadaten im Entity Statement des Federation Master enthalten nach [OpenID Connect Federation 1.0#rfc.section.4.6] die Attribute :

T*abelle : 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"

In der TI-Föderation werden die Metadaten im Entity Statement des Federation Master zusätzlich zu den im Standard geforderten Attributen noch um das Attribut "idp_list_endpoint" erweitert.

Tabelle : 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"

Diese zusätzliche Schnittstelle wird von den Fachanwendungen der TI-Föderation verwendet, um alle in der TI-Föderation verfügbaren Identity Provider zu ermitteln. Der Standard sieht für die Teilnehmerermittlung zwar die Schnittstelle "federation_list_endpoint" vor, die zusätzliche Schnittstelle erspart den Fachanwendungen jedoch Logik zum Ausfiltern der sektoralen IDP aus der gesamten Teilnehmerliste. Außerdem werden über diese Schnittstelle hilfreiche zusätzliche Informationen zu den sektoralen IDPs an die anfragende Fachanwendung übermittelt.

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:

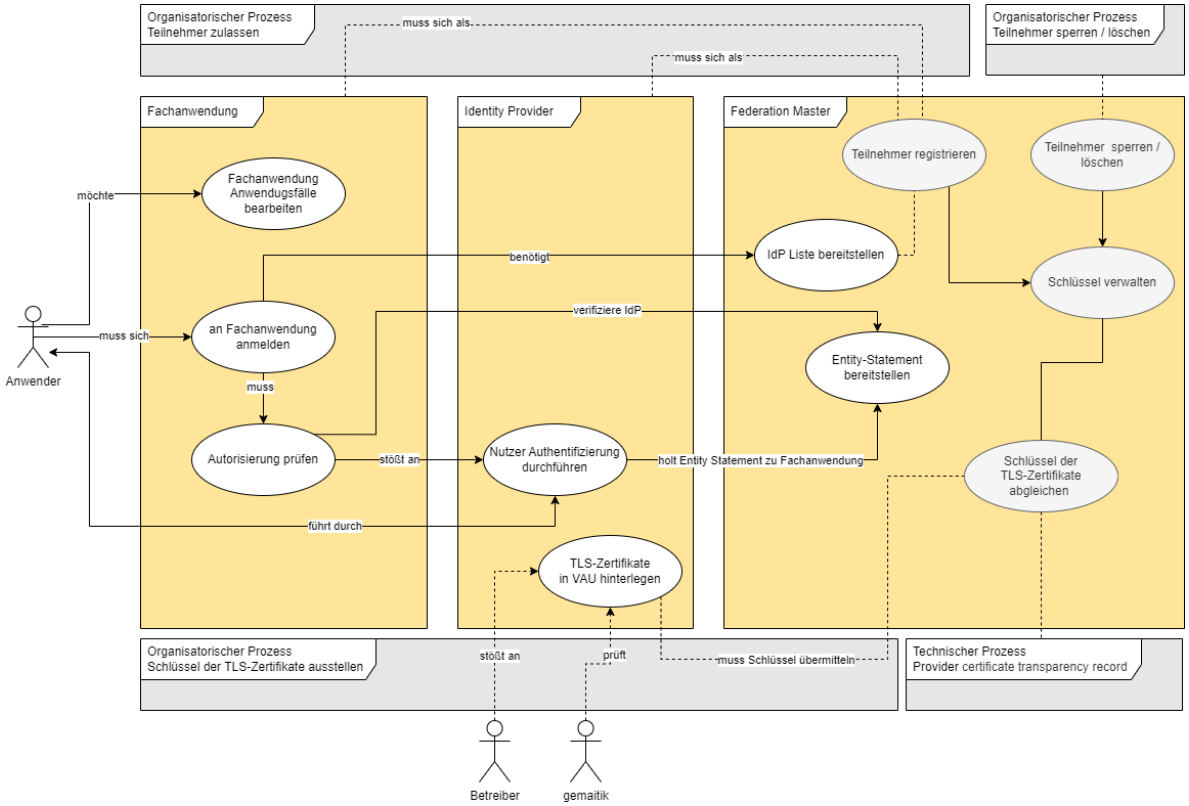


Tabelle : Übersicht über die Anwendungsfälle im Gesamtkontext Federation Master

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*) 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 eine DiGA) sein. Die Anmeldung für alle Anwendungen erfolgt genau den Identity Provider, bei dem die elektronische Identität des Nutzers hinterlegt ist. Zur Ermittlung des richtigen Identity Provider 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 'Organisationsname', 'Logo' und 'Zieladresse (URL)' ermittelt und als Liste bereitgestellt.
Autorisierung prüfen	Fachanwendung	Der Anwendungsfall Autorisierung prüfen ist 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-Anwendu	Fachanwendung	Nach erfolgreicher Nutzerauthentifizierung kann der Nutzer die Anwendungsfälle der Fachanwendung bearbeiten, für die er autorisiert ist.

ngsfälle bearbeiten		
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).

Tabelle : 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

Anwendungsfall - IDP-Liste bereitstellen

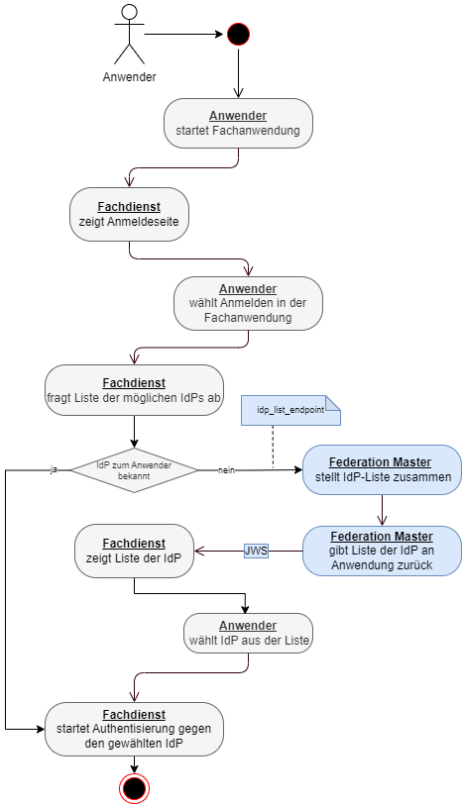


Tabelle : Anwendungsfall "Bereitstellung Liste registrierter Identity Provider"

Attribute	Bemerkung
Beschreibung	Ein Anwender möchte einen in der TI registrierten Fachdienst nutzen. Der Fachdienst muss sicherstellen, dass der Anwender zur Nutzung des Dienstes berechtigt ist. 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. 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. 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: • 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). 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.
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	• Fachdienst der TI • Federation Master
Vorbedingung	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 idp_list_endpoint benannte URL muss aus dem Internet erreichbar sein.
Ablauf	

	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 idp_list_endpoint 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: a. Name der Organisation b. URI (iss) des sektoralen Identity Provider c. Logo der Organisation d. 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 "Liste sektorale Identity Provider - Payload-Attribute des signierten JSON-Web-Token" und "Liste sektorale Identity Provider - Headerattribute des signierten JSON-Web-Token" aufgeführten Attribute enthalten.
Ergebnis	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.

Die Attribute des signierten JSON-Web-Token in der Response des Federation Master zum Request sind:

Tabelle : 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 des Liste (maximal *iat* + 24 Stunden)
idp_entity {			Der Block *idp_entity* 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.
}			Ende des Blocks *idp_entity*

Der Header der Response des Federation Master zum Request umfasst die Parameter:

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

Name	Werte	Anmerkungen
alg	ES256	
kid	wie aus jwks im Body des Entity Statement	Identifier des verwendeten Schlüssels aus dem jwks im Body des Entity Statement des Federation Master
typ	idp-list+jwt	

Anwendungsfall - Entity Statement bereitstellen

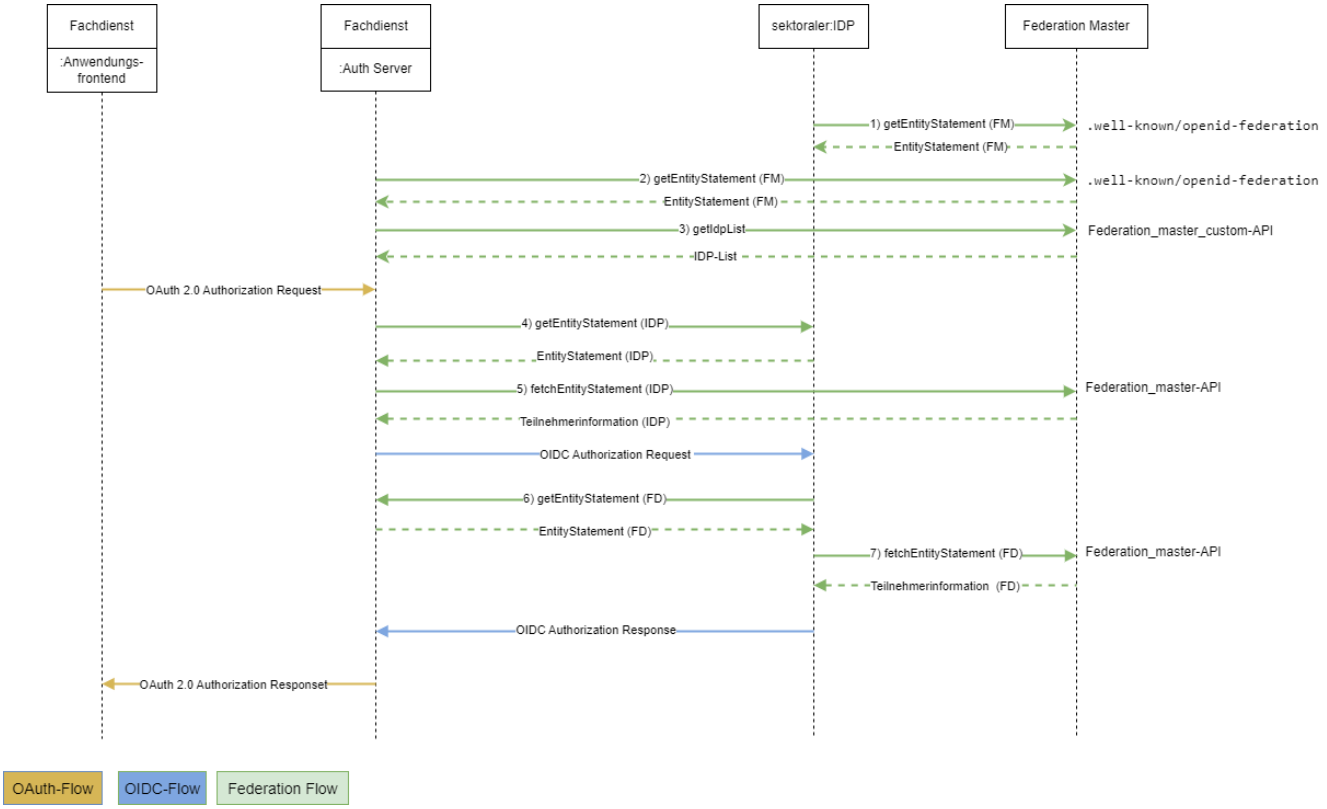


Tabelle : Federation Master im Authorization-Flow

Schritt	Beteiligte Parteien	Beschreibung
1 - getEntityStatement(FM)	sektoraler Identity Provider, Federation Master	Request zum Abholen des Entity Statement des Federation Master durch den sektoralen Identity Provider
2 - getEntityStatement(FM)	Fachdienst, Federation Master	Request zum Abholen des Entity Statement des Federation Master 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
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
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

Tabelle : 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	• Federation Master • Fachdienst der TI • sektoraler Identity Provider
Vorbedingung	• 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 federation_fetch_endpoint benannte URL muss aus dem Internet erreichbar sein.
Ablauf	• 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 federation_fetch_endpoint 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 federation_fetch_endpoint 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-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.

T*abelle : 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"	Identifier des anfragenden Teilnehmers. Wird dieser *claim* nicht gesetzt, so kann alternativ die bei der Registrierung des Fachdienstes/IDP vergebene Member-ID im UserAgent gesetzt werden.

Tabelle : 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 Liste (maximal *iat* + 24 Stunden)
jwks	JWKS Objekt		öffentlicher Schlüssel des angefragten Teilnehmer (sektoraler Identity Provider bzw. Fachdienst

Der Header der Response des Federation Master zum Request umfasst die Parameter:
Tabelle : Teilnehmer Validierung - Response-Header-Attribute des signierten JSON-Web-Token

Name	Werte	Anmerkungen

alg	ES256	
kid	wie aus jwks im Body des Entity Statement	Identifier des verwendeten Schlüssels aus dem jwks im Body des Statement
typ	entity-statement+jwt	

Anwendungsfall - TLS/VAU Schlüssel verwalten

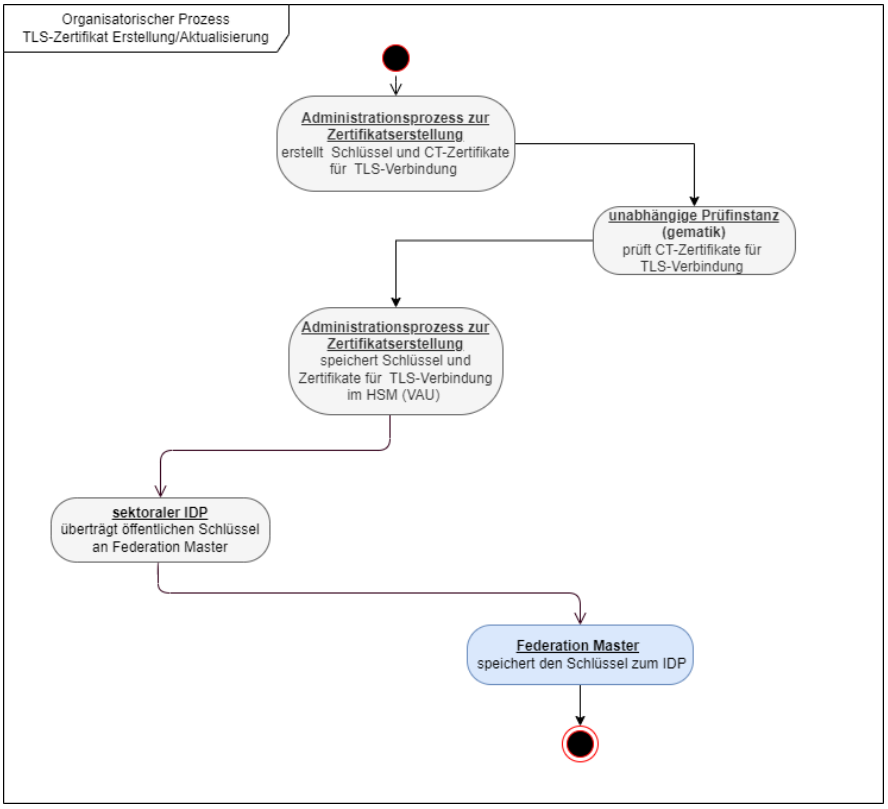


Tabelle : Anwendungsfall "Monitoring der TLS-Zertifikate der VAU"

Attribute	Bemerkung
Beschreibung	Certificate Transparency Monitor für die TLS-Zertifikate
Akteur	Federation Master
Auslöser	• 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	• Federation Master • sektoraler Identity Provider
Vorbedingung	Der sektorale Identity Provider ist in der TI-Föderation registriert. Bei neu erstellten TLS-Zertifikaten wurde der Prozess "Certificate Transparency TLS-Zertifikate" der sektoralen Identity Provider prüfen erfolgreich durchlaufen. Die öffentlichen Schlüssel des sektoralen Identity Provider und seine öffentliche TLS-Schlüssel sind beim Federation Master hinterlegt.
Ablauf	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 aus den im Entity Statement des sektoralen Identity Provider hinterlegten Adressen zum Token- , PAR- und Authorization-Endpunkt die Domänennamen. Der Federation Master fragt mit allen ermittelten Domänennamen 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 Domänennamen. 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.

Ergebnis	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.

Anwendungsfall - Teilnehmerregistrierung am Federation Master

Die Registrierung von Teilnehmern der Föderation beim Federation Master erfolgt über einen organisatorischen Prozess. Alle Teilnehmer der Föderation müssen über diesen Prozess ihre öffentlichen Schlüssel, für die Signatur des Entity Statement, beim Federation Master hinterlegen. Fachdienste müssen zusätzlich die für ihre Anwendungsfälle notwendigen *scopes* beim Federation Master hinterlegen. Ein Fachdienst darf nur die *scopes* von einem sektoralen IDP erfragen, die er zwingend für die Ausführung der fachlichen Anwendungsfälle benötigt. Deshalb wird zur Prüfung der Rechtmäßigkeit gewünschter *scopes* die gematik im Prozess der Registrierung eines Fachdienst beim Federation Master mit eingebunden. Im laufenden Betrieb lädt dann der Federation Master regelmäßig die aktuellen Entity Statements aller registrierten Fachanwendungen und prüft, ob die darin enthaltenen Werte für den Parameter *scope*, mit den beim Federation Master bei der Registrierung hinterlegten Werten übereinstimmt.

Anwendungsfall - Teilnehmer am Federation Master löschen

Das Löschen oder Sperren von Teilnehmern in der Föderation erfolgt ebenfalls über einen organisatorischen Prozess. Das Erteilung von Lösch- oder Sperraufträgen sowie das physische Löschen erfolgt im 4-Augen-Prinzip. Damit soll verhindert werden, dass Fachanwendungen oder IDPs ungewollt oder unautorisiert gelöscht oder gesperrt werden. Das Löschen oder Sperren kann zur Folge haben, dass Anwendungen für eine Vielzahl von Nutzern nicht mehr erreichbar ist.

Anwendungsfall - Schlüssel für Certificate Transparency TLS-Zertifikate übergeben

Bei der Registrierung sektoraler IDP am Federation Master werden die öffentlichen Schlüssel, welche für die TLS-Verbindungen mit Fachdiensten verwendet werden, beim Federation Master hinterlegt. Diese Schlüssel werden regelmäßig aktualisiert. Das hintelegen der jeweils aktuellen Schlüssel beim Federation Master wird ebenfalls über einen organisatorischen Prozess durchgeführt. Im Ablauf dieses Prozesses ist es möglich im Rahmen einer Schlüsselzeremonie zu überprüfen (z.B. durch die gematik), ob diese Schlüssel aus der Vertrauenswürdigen Ausführungsumgebung (VAU) des sektoralen IDP stammen.