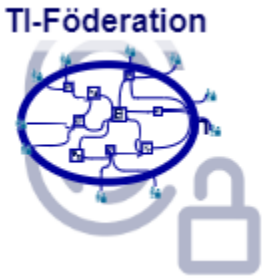
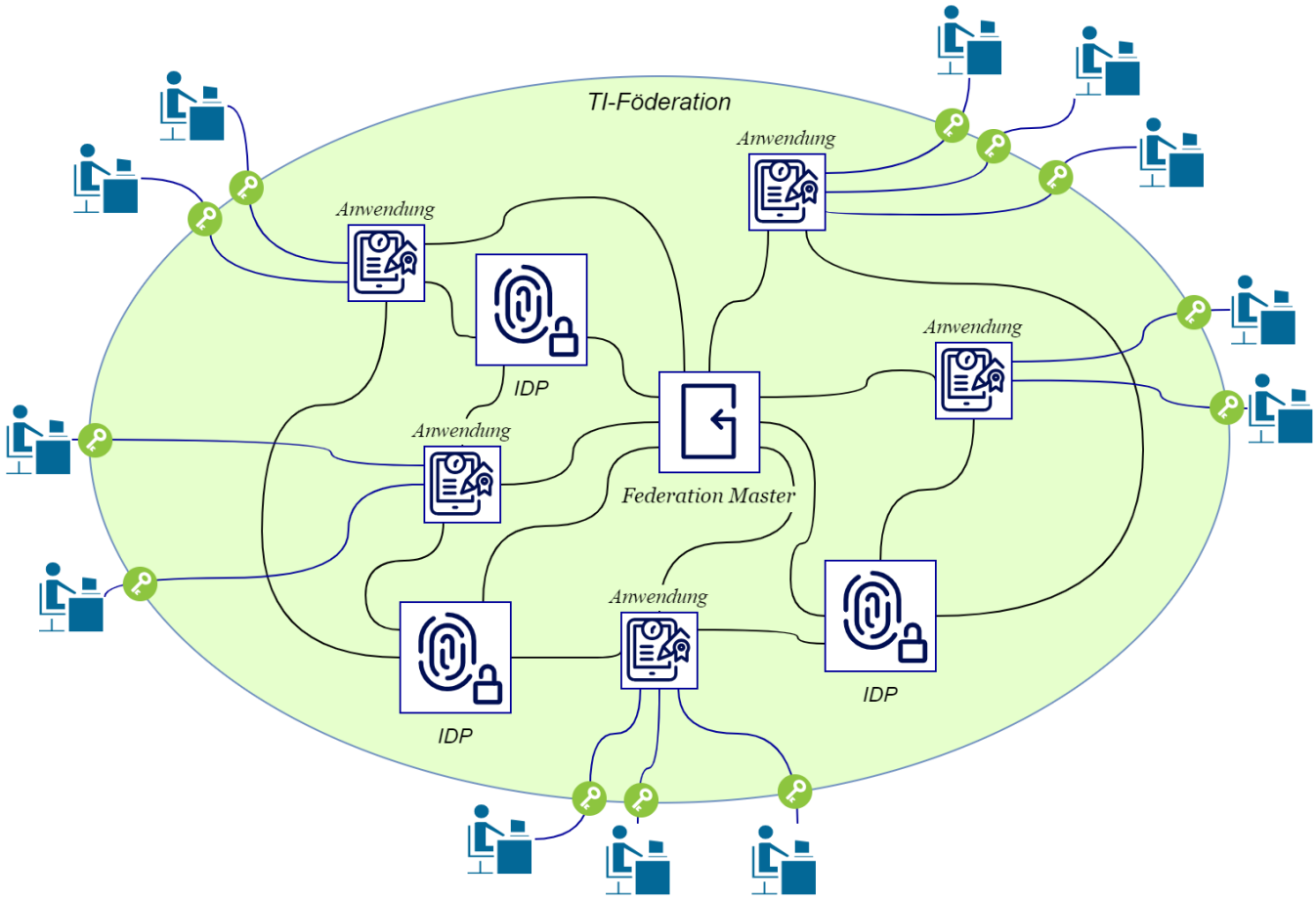
Systemüberblick



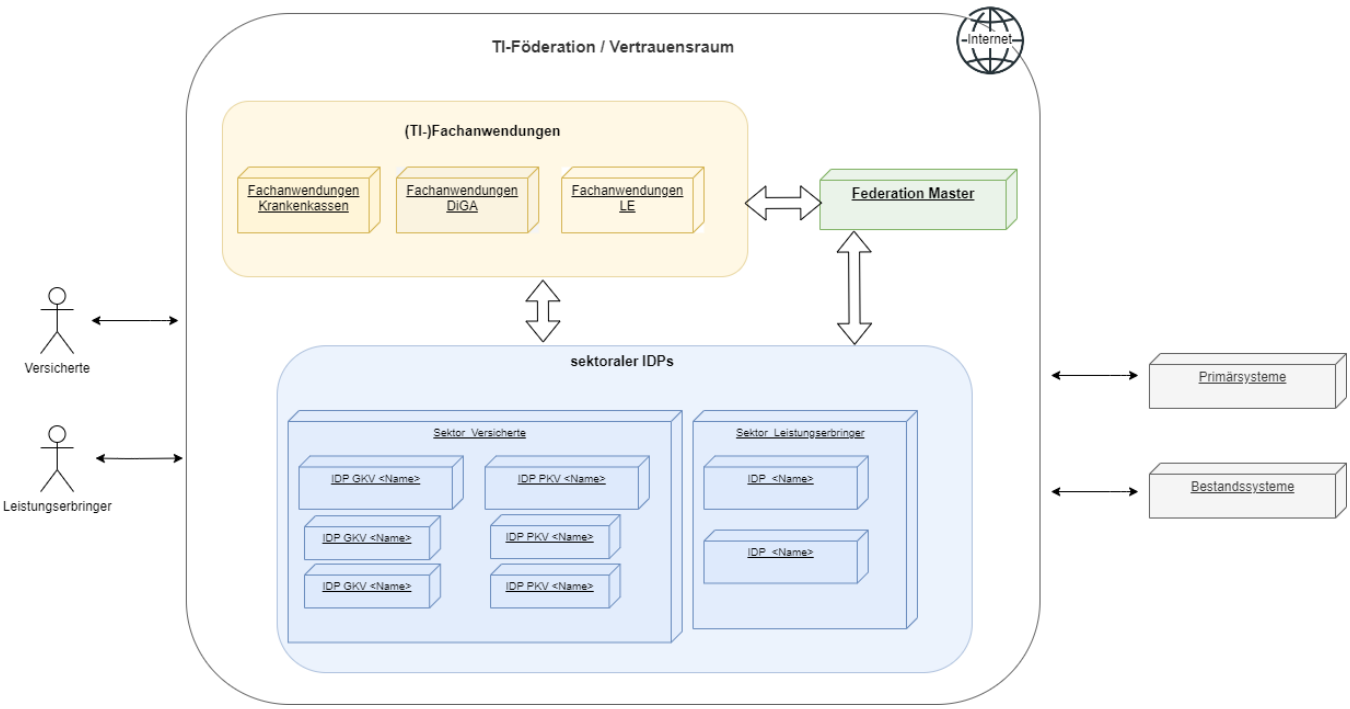
Beteiligte Systeme

Die TI-Föderation besteht aus drei Systemen, welche untereinander über standardisierte Schnittstellen kommunizieren. Zusammen bilden die beteiligten Systeme einen Vertrauensraum. Die TI-Föderation besteht aus mehreren Fachanwendungen. Die Fachanwendungen sind Apps, Browser- oder Desktopanwendungen. Hier werden Nutzern spezielle i. d. R. medizinische digitale Services angeboten. Die Fachanwendungen müssen prüfen, ob ein Nutzer überhaupt für die Verwendung befugt (autorisiert) ist. Dazu muss die Fachanwendung feststellen, um welchen Benutzer es sich handelt. Der Benutzer muss sich authentisieren. Damit nicht jede Fachanwendung eine eigene Benutzerverwaltung mit hohen Sicherheitsansprüchen implementieren muss und Anwender nicht eine Vielzahl von Zugangsinformationen (Login) verwalten müssen, wird die Nutzerauthentifizierung durch sektorale Identity Provider (IDPs) durchgeführt. Zum Schutz der Anwender vor Datenmissbrauch müssen alle an der TI-Föderation beteiligten Fachanwendungen und sektoralen IDPs hohen Sicherheitsanforderungen standhalten. Alle Teilnehmer der TI-Föderation müssen sich über einen organisatorischen Prozess beim Federation Master registrieren.



Jede Fachanwendung verfügt über einen eigenen Authorization-Server, welcher basierend auf den Informationen der sektoralen Identity Provider über den jeweiligen Nutzer dessen Zugriffsrechte definiert. Als sektoraler IDP wird ein Dienst zur Authentifizierung von Nutzern bezeichnet. Nach erfolgreichem Durchlaufen des Authentifizierungsprozesses stellt der sektorale IDP Identitätsinformationen für eine bestimmte Gruppe von Nutzern (Sektoren) innerhalb der Telematikinfrastruktur des Gesundheitswesens bereit. Die Identitätsinformationen der Nutzer werden durch den anfordernden Fachdienst zur Prüfung verwendet, auf welche Fachdaten und -prozesse der Nutzer zugreifen darf. Insbesondere umfasst ein Sektor die Krankenkassen mit den Versicherten als Nutzer. Zukünftig werden allerdings auch andere Personengruppen, wie z. B. Ärzte oder Pflegeinstitutionen, über Identity Provider für Leistungserbringer (LE) und Leistungserbringer-Institutionen (LEI) angebunden. Dabei ist nicht ausgeschlossen, dass ein sektoraler IDP Identitätsinformationen für mehrere Nutzergruppen bedienen kann. Der TI-Vertrauensraum wird durch den sogenannten Federation Master verwaltet. Der Federation Master ist eine zentrale Komponente für alle Fachdienste und sektoralen IDPs in der Föderation. Beim Federation Master sind alle Teilnehmer der Föderation registriert, nur dort registrierte Teilnehmer sind berechtigt, die Dienste der Föderation in Anspruch zu nehmen. Die Kommunikation zwischen den Systemen in der TI-Föderation basiert auf den Standards OpenID Connect (OIDC), Open Authorization 2.0 (OAuth 2) und JSON Web Token (JWT).

Neben den Systemen der TI-Föderation sind im Gesamtkontext weitere Systeme über Schnittstellen an die TI-Föderation angeschlossen (ohne selbst Bestandteil der Föderation zu sein). Das sind u. a. die Bestandsysteme, in denen aktuell die Informationen zu Nutzern gepflegt werden.

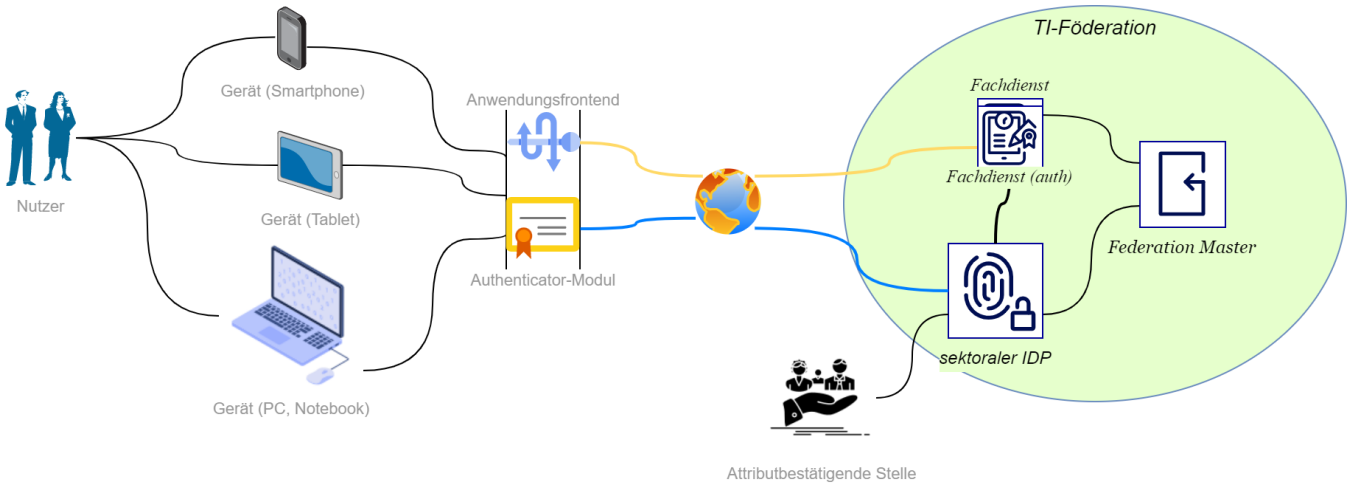


Akteure und Rollen

Im Systemkontext eines sektoralen IDP interagieren verschiedene Akteure (Nutzer und aktive Komponenten) in unterschiedlichen OAuth2-Rollen gemäß [The OAuth 2.0 Authorization Framework (section-1.1)] und OpenID-Connect-Rollen gemäß [OpenID Connect Core 1.0] und [OpenID Connect Federation 1.0]. Einige Akteure müssen registrierte Teilnehmer der Föderation sein. Andere Akteure agieren über Schnittstellen mit den Teilnehmern der Föderation.

Akteur	Rolle "OAuth2"	Rolle "OIDC"	Teilnehmer der Föderation
Nutzer (z. B. Versicherte)	Resource Owner	Resource Owner	Der Nutzer ist kein Teilnehmer der TI-Föderation. Er ist im Kontext von "OAuth2" und "OIDC" der Resource Owner. Der Nutzer ist im Kontext einer Anwendung i.d.R. genau einem Sektor zugeordnet (agiert als Versicherter, agiert als Arzt, …). Ein und derselbe Nutzer kann aber mehreren Nutzergruppen angehören. Der Nutzer interagiert über die Frontend-Komponenten der Fachanwendungen und dem -Modul mit den TI-Teilnehmen.
Fachdienst - Authorization-Server	Authorization-Server	Relying Party (RP)	Der Fachdienst - Authorization-Server ist als Relying Party (RP) Teilnehmer der Föderation und muss als solcher in der TI-Föderation registriert sein.
Fachdienst - Fachliche Services (Fachdaten und -Prozesse)	Protected Resource	-	Die eigentlichen Fachdienste und fachlichen Services sind nicht Teilnehmer der TI-Föderation. Nach erfolgreicher Nutzerauthentifizierung kann eine Interaktion zwischen Nutzer und den fachlichen Services eines Fachdienstes erfolgen.

Fachdienst - Frontend	Unterschiedliche Ausprägung • Client, Nutzerschnittstelle als native App • Client, Nutzerschnittstelle als Web-Anwendung • Client, Services der UI-Bereitstellung für Web-Anwendung	-	Die unterschiedlichen Frontend-Komponenten der Fachdienste sind keine Teilnehmer der TI-Föderation. Sie müssen nicht über organisatorische Prozesse in der TI-Föderation registriert werden. Allerdings müssen sie Informationen über sich für Monitoring- und Loggingprozesse bereitstellen.
sektoraler IDP	-	OpenID Provider (OP)	Sektorale IDP sind als OpenID Provider (OP) Teilnehmer der Föderation und müssen als solche in der TI-Föderation registriert sein.
Authenticator-Modul des sektoralen IDP	-	Frontend des sektoralen IDP - OpenID Provider (OP)	Authenticator-Module sind als Frontend-Komponenten Teil des sektoralen IDP und damit auch Teil der TI-Föderation. Authenticator-Module müssen nicht separat in der TI-Föderation registriert sein.
Federation Master	-	Vertrauensanker (Trust Anchor) für alle Teilnehmer (RP + OP) der TI-Föderation	Der Federation Master ist als Vertrauensanker (Trust Anchor) für alle Teilnehmer (RP + OP) der Föderation selbst ebenfalls Teilnehmer der TI-Föderation. Er wird als eigener Produkttyp für die TI zugelassen.
Attributbestätigende Stelle	-	-	Die Attributbestätigenden Stelle ist das System, in dem die Daten zu Nutzern erfasst und gepflegt werden. I.d.R. muss ich der Nutzer hier (einmalig) identifizieren. Neben den Daten zur Person werden hier auch weitere Daten (z.B. KVNR) gepflegt. Die Attributbestätigenden Stellen liefern den sektoralen IDPs die Daten zu den zu verifizierenden Nutzern. Die Attributbestätigenden Stellen selbst sind keine Teilnehmer der TI-Föderation.
externe Anwendung	-	Relying Party (RP)	Unter bestimmten Voraussetzungen kann eine externe Anwendung Relying Party (RP) gegenüber eines sektoralen IDP der Föderation sein, ohne selbst in der Föderation registriert sein zu müssen. Das betrifft z.B. Krankenkassen eigene Anwendungen , welche zur Nutzerauthentifizierung den sektoralen IDP der Kasse verwenden.



Nutzer (Rolle: Resource Owner)

Der Resource Owner ist eine natürliche Person, welche auf die beim Fachdienst (Resource Server) für ihn bereitgestellten Daten und Prozesse (Protected Resource) über eine UI zugreifen kann. Der Resource Owner bedient die UI über ein Endgerät (Smartphone, Tablet, Desktop). Mit diesem Geräte interagiert der Resource Owner mit den Anwendungsfrontends von Fachanwendungen. Die Nutzereingaben zur Authentifizierung erfolgen über ein Authenticator-Modul, das auf dem gleichen oder auf einem anderen Gerät des Anwenders installiert ist.

Fachdienst-Authorization-Server (Rolle: Relying Party)

Der Authorization-Server des Fachdienstes (OIDC Relying Party) stößt die Authentifizierung des Nutzers beim sektoralen IDP an und erhält als Ergebnis einen Authorization Code, den er gegen ein *ID-Token* und *Access-Token* beim sektoralen IDP eintauschen kann. Der Authorization-Server des Fachdienstes verwendet die Informationen aus dem *ID-Token* für die Feststellung der Zugriffsrechte des Anwendungsfrontend auf die Ressourcen des Fachdienstes. Der Authorization-Server des Fachdienstes stellt eigene *Access-Token* und *Refresh-Token* für das Anwendungsfrontend aus.

Fachdaten und Prozesse / Fachdienst-Resource Server (Rolle: Protected Resource)

Der Resource Server ist der Fachdienst, der dem Nutzer (Resource Owner) Zugriff auf seine Fachdaten und Prozesse (Protected Resource) gewährt. Der Fachdienst, der die geschützten Fachdaten (Protected Resources) anbietet, ist in der Lage, auf Basis von *Access-Token* Zugriff für Clients zu gewähren. Ein solches Token repräsentiert die delegierte Identifikation des Resource Owner.

Anwendungsfrontend (Rolle: Client)

Das Anwendungsfrontend (OAuth2 Client) greift auf Fachdienste (Resource Server) und ihre geschützten Fachdaten (Protected Resource) zu. Das Anwendungsfrontend kann auf einem Server als Webanwendung (Primärsystem als Terminalserver), auf einem Desktop-PC oder einem mobilen Gerät (z. B. Smartphone) oder als App auf einem mobilen Gerät ausgeführt werden. Ist das Anwendungsfrontend eine Webanwendung, so ist die Backend-Komponente, welche die UI für die Visualisierung im Browser auf dem Gerät des Nutzers realisiert, ebenfalls Teil des Clients.

Sektoraler IDP mit dem Authenticator-Modul als Frontend (Rolle: OpenID Provider)

Der Authorization-Server des sektoralen IDP authentifiziert den Resource Owner (Nutzer) und stellt einen *Authorization Code* aus. Dieser *Authorization Code* kann später gegen ein *ID-Token* beim sektoralen IDP eingetauscht werden. Das *ID-Token* enthält die Informationen für den vom Resource Owner erlaubten Anwendungsbereich (*scope*).

Attributbestätigende Stelle

Attributbestätigende Stellen sind legitimierte Organisationen, welche die Korrektheit der Attribute verantworten, die durch sie für einen Nutzer beim sektoralen IDP bestätigt werden. Als Teilprozess der Registrierung ist die zuverlässige und eindeutige Identifikation der Nutzer zwingend notwendig. Hierbei werden eindeutige Identifikationsmerkmale der realen Identitäten benötigt und letztlich als Identitätsinformationen dem sektoralen IDP zur Verfügung gestellt. Die eindeutigen Identitäten von natürlichen Personen (Versicherte, Leistungserbringer) bzw. juristischen Personen (medizinische Institutionen, Gesellschafterorganisations- und Kostenträgergeschäftsstellen) werden innerhalb der TI über die Krankenversichertennummer des Versicherten und die Telematik-ID eines Leistungserbringers bzw. einer medizinischen Institution oder Organisation des Gesundheitswesens repräsentiert.

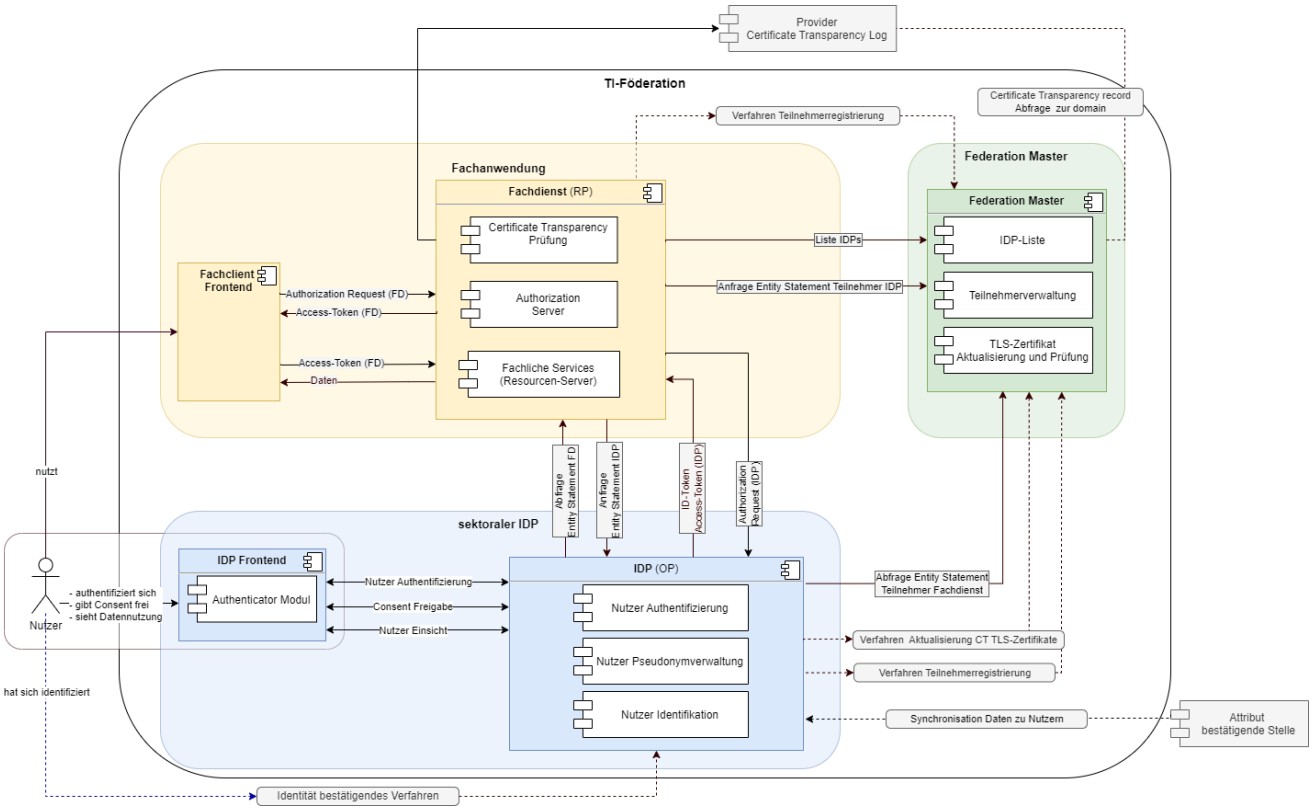
Federation Master

Der Federation Master ist eine zentrale Komponente und ein eigener Produkttyp in der TI. Der Federation Master bietet die Anwendungsfälle:

- Teilnehmer registrieren
- IDP-Liste bereitstellen
- Entity Statement bereitstellen
- Schlüssel der TLS-Zertifikate abgleichen
- Schlüssel verwalten

Alle Teilnehmer der Föderation müssen beim Federation Master registriert sein. Teilnehmer der Föderation sind in diesem Kontext alle Fachdienste und sektoralen IDP. Die Registrierung erfolgt durch einen organisatorischen Prozess, der vom Anbieter des Produkttyp Federation Master bereitgestellt wird. Der Federation Master verwaltet die öffentlichen Schlüssel aller Teilnehmer und zusätzlich für registrierte Fachdienste die jeweils zugelassenen *scopes*. Er stellt auf Anfrage Teilnehmerbestätigungen in Form von Entity Statements aus. Der Federation Master agiert als Trust Anchor im Sinne der OpenID-Connect-Federation Spezifikation. Für Fachdienst stellt der Federation Master eine Schnittstelle bereit, über die eine Liste aller in der Föderation registrierten sektoralen IDP abgerufen werden kann.

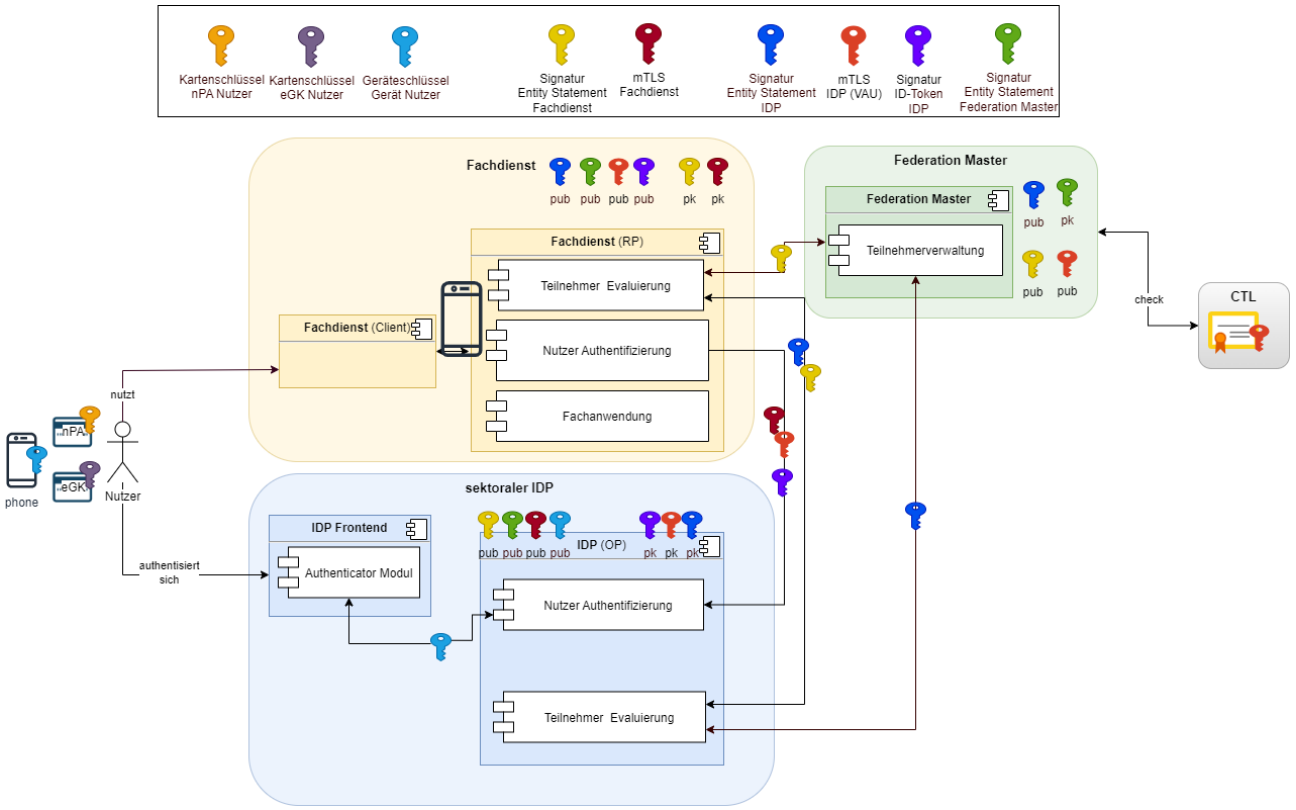
Übersicht über die Akteure und ihre Schnittstellen



Wie die Komponenten miteinander kommunizieren wird im Kapitel Sektoraler IDP dargestellt.

Sicherheit

Die Kommunikation innerhalb der TI-Föderation ist über Verschlüsselung und Signatur abgesichert. Die Anforderungen an die Schlüssel für die Signatur und Verschlüsselung von Entity Statements und Token finden sich im OIDC-Standard [OpenID Connect Federation 1.0] und darauf aufbauend den Beschreibungen zu den Abläufen.



Schlüssel	Beschreibung
Geräteschlüssel Gerät des Nutzers	Der Geräteschlüssel wird bei der Bindung des Gerätes des Nutzers an dessen Identität lokal erstellt und im Schlüsselspeicher des Gerätes abgelegt. Je nach Art des Schlüsselspeichers ist der Schlüssel über einen bestimmten Zeitraum gültig. In diesem Zeitraum kann das Geräte zur kartenlosen sicheren Nutzerauthentifizierung als Besitzfaktor verwendet werden.
Kartenschlüssel nPA des Nutzers	Der Kartenschlüssel ist nicht auslesbar im Kartenherausgabeprozess auf der Karte hinterlegt.
Kartenschlüssel eGK des Nutzers	Der Kartenschlüssel ist nicht auslesbar im Kartenherausgabeprozess auf der Karte hinterlegt.
mTLS Schlüssel des Fachdienstes	Der Fachdienst transportiert das mTLS-Zertifikat über sein Entity Statement signiert zum sektoralen IDP
Signaturschlüssel Entity Statement des Fachdienstes	Das Entity Statement wird vom Fachdienst selbst signiert. Der Signaturschlüssel ist beim Federation Master im Prozess der Teilnehmerregistrierung hinterlegt. Über die Schnittstelle zur Teilnehmerauskunft wird einem anfragenden IDP unter anderem der Schlüssel zur Validierung des Entity Statements des Fachdienstes mitgeliefert.
mTLS Schlüssel des IDP	Der mTLS-Schlüssel des IDP wird in einer vertrauenswürdigen Ausführungsumgebung im 4-Augen-Prinzip innerhalb der VAU in einem HSM generiert und über einen organisatorischen Prozess dem Federation Master bekanntgegeben. Der Federation Master prüft regelmäßig Certificate Transparency Logs auf ihm unbekannte (und damit nicht in der VAU erstellte) Schlüssel zu Zertifikaten der Domänen des IDP.

 Signaturschlüssel Entity Statement des IDP	Das Entity Statement wird vom IDP selbst signiert. Der Signaturschlüssel wird über einen organisatorischen Prozess dem Federation Master bekanntgegeben. Über die Schnittstelle zur Teilnehmerauskunft wird einem anfragenden Teilnehmer unter anderem der Schlüssel zur Validierung des Entity Statements des IDP mitgeliefert.
 Signaturschlüssel für Token des IDP	Token werden vom IDP selbst signiert. Die öffentlichen Signaturschlüssel werden den Fachdiensten über das signierte Entity Statement des IDP bekanntgegeben.
 Signaturschlüssel Entity Statement des Federation Master	Sein Entity Statement wird vom Federation Master signiert. Der Signaturschlüssel ist im Entity Statement des Federation Master unter dem claim jwks hinterlegt und wird den Teilnehmenden Diensten innerhalb der Föderation im Rahmen der Registrierung bekanntgegeben. Dieser wird als Vertrauensanker einmalig organisatorische in die Systeme (IDP und Fachdienst) eingebracht.