

## **Elektronische Gesundheitskarte und Telematikinfrastruktur**

# **Konzept TI-Föderation**

Version:	1.0.0_CC
Revision:	1613623
Stand:	28.05.2026
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemKPT_TI-Föderation

---

## Dokumentinformationen

---

### Gender-Hinweis

Aus Gründen der besseren Lesbarkeit wird in diesem Dokument überwiegend die männliche Form verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

### Änderungen zur Vorversion

Es handelt sich um eine Erstveröffentlichung.

### Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0_CC	28.05.2026		Initiale Struktur	gematik

---

## Inhaltsverzeichnis

---

<b>1 Einordnung des Dokuments.....</b>	<b>6</b>
<b>1.1 Zielsetzung.....</b>	<b>6</b>
<b>1.2 Zielgruppe.....</b>	<b>6</b>
<b>1.3 Geltungsbereich.....</b>	<b>6</b>
<b>1.4 Abgrenzung des Dokuments.....</b>	<b>7</b>
<b>1.5 Methodik.....</b>	<b>7</b>
1.5.1 Technische Beschreibung.....	7
1.5.2 Normative Festlegungen.....	7
1.5.3 Hinweis auf offene Punkte <<optional, nur bis einschl. Abstimmphase >>.....	7
<b>2 Fachliche &amp; technische Rahmenbedingungen.....</b>	<b>8</b>
<b>2.1 Fachliche Grundlagen.....</b>	<b>8</b>
2.1.1 Begriffsbestimmungen.....	8
2.1.2 Technische Grundlagen.....	9
2.1.3 Identifikationsmittel und -systeme.....	9
<b>2.2 Die Ausgangslage im deutschen Gesundheitswesen.....</b>	<b>10</b>
2.2.1 Identitätsherausgeber, Identitätsträger und Trust Service Provider.....	11
2.2.2 Der Weg zur TI 2.0.....	12
2.2.3 Gesetzliche Rahmenbedingungen.....	12
<b>2.3 Fachliche Einordnung der sektoralen Identity Provider.....</b>	<b>14</b>
<b>2.4 Rahmenbedingungen des Authentisierungs-Flows.....</b>	<b>14</b>
2.4.1 Relevante Anwendungen der IDP-Nutzung.....	14
2.4.2 Ablauf der Authentisierung.....	16
<b>3 Systemüberblick.....</b>	<b>18</b>
<b>3.1 Allgemeiner Überblick.....</b>	<b>18</b>
<b>3.2 Schnittstellen zu Umsystemen.....</b>	<b>21</b>
<b>4 Lösungsstrategie.....</b>	<b>23</b>
<b>4.1 Anwendungsfälle.....</b>	<b>23</b>
<b>4.2 Aufbau und Kommunikation.....</b>	<b>26</b>
<b>4.3 Akteure und Rollen.....</b>	<b>29</b>
<b>4.4 Schnittstellen.....</b>	<b>33</b>
<b>4.5 Schlüsselmanagement.....</b>	<b>37</b>
<b>5 Abläufe &amp; Interaktionen.....</b>	<b>41</b>
<b>5.1 Kurzbeschreibung.....</b>	<b>41</b>
<b>5.2 App2App-Flow.....</b>	<b>42</b>
5.2.1 Vorbedingungen.....	42
5.2.2 Flow - OIDC.....	43
5.2.2.1 Flow Diagramm.....	43

70	5.2.2.2 Ablaufbeschreibung App2App-Flow.....	43
71	5.2.2.3 Schnittstellenbeschreibung.....	46
72	<b>6 Metadata.....</b>	<b>50</b>
73	<b>6.1 OpenID Connect Relying Party.....</b>	<b>69</b>
74	<b>6.2 Web2App-Flow.....</b>	<b>83</b>
75	6.2.1 Vorbedingungen.....	83
76	6.2.2 Flow - OIDC.....	84
77	6.2.2.1 Flow Diagramm.....	84
78	6.2.2.2 Ablaufbeschreibung Web2App-Flow.....	84
79	<b>6.3 2-Geräte-Flow.....</b>	<b>86</b>
80	6.3.1 Vorbedingungen.....	86
81	6.3.2 Flow - OIDC.....	87
82	6.3.2.1 Flow Diagramm.....	87
83	6.3.2.2 Ablaufbeschreibung 2-Geräte-Flow.....	87
84	<b>6.4 Flow Desktop-Anwendung mit integriertem Authenticator-Modul.....</b>	<b>89</b>
85	6.4.1 Vorbedingungen.....	90
86	6.4.2 Flow - OIDC.....	90
87	6.4.2.1 Flow Diagramm.....	90
88	6.4.2.2 Ablaufbeschreibung Desktop-App-Flow.....	90
89	<b>6.5 Unterstützung Single-Sign-On auf Anwendungsebene.....</b>	<b>92</b>
90	6.5.1 Prinzipieller Ablauf mit SessionID und Schlüsselpaar.....	94
91	6.5.2 SSO-Unterstützung auf Anwendungsebene innerhalb einer APP.....	97
92	6.5.3 SSO-Unterstützung auf Anwendungsebene bei separater Authenticator-APP...97	
93	6.5.4 Ablaufbeschreibung SSO-Flow.....	98
94	<b>7 Betriebliche Aspekte.....</b>	<b>107</b>
95	<b>7.1 Verfügbarkeiten.....</b>	<b>107</b>
96	7.1.1 Sektorale IDPs.....	107
97	7.1.2 Federation Master.....	108
98	7.1.2.1 TI-Trust Anchor.....	108
99	7.1.2.2 Intermediate Entities.....	108
100	7.1.3 Fachdienst Authorization Server.....	108
101	<b>7.2 Bearbeitungszeiten.....</b>	<b>108</b>
102	7.2.1 Sektorale IDPs.....	108
103	7.2.2 Federation Master.....	110
104	7.2.2.1 TI-Trust Anchor.....	110
105	7.2.2.2 Intermediate Entities.....	110
106	7.2.3 Fachdienst Authorization Server.....	110
107	<b>8 Querschnittliche Konzepte.....</b>	<b>111</b>
108	<b>9 Qualitätsszenarien.....</b>	<b>112</b>
109	<b>10 Anhang - Verzeichnisse.....</b>	<b>114</b>
110	<b>10.1 Abkürzungen.....</b>	<b>114</b>
111	<b>10.2 Glossar.....</b>	<b>115</b>
112	<b>10.3 Abbildungsverzeichnis.....</b>	<b>123</b>
113	<b>10.4 Tabellenverzeichnis.....</b>	<b>124</b>
114	<b>10.5 Referenzierte Dokumente.....</b>	<b>125</b>

115

116

---

## 1 Einordnung des Dokuments

---

### 1.1 Zielsetzung

Das Dokument beschreibt den Aufbau der TI-Föderation gemäß des Standards [OpenID Federation 1.1]. Die TI-Föderation ist der Vertrauensraum für eine Anwendungslandschaft im Gesundheitswesen. Ziele dieses Vertrauensraum sind

- die Erhöhung der Sicherheit in der Kommunikation der Teilnehmer des Vertrauensraum untereinander durch Einsatz etablierter und standardisierter Identifikations- und Authentisierungsverfahren
- die Reduktion der Komplexität von notwendigen Vertrauensbeziehungen durch Bildung von Vertrauensketten
- die Nutzung standardisierter Features zur Umsetzung von Vertrauensregeln (Policies) und Nachweisen (TrustMarks)

Die TI-Föderation bildet die Möglichkeit Technologie unabhängig die Authentifizierung von Anwendungen und Nutzern in einem Vertrauensraum abzubilden.

### 1.2 Zielgruppe

Das Dokument richtet sich an

- Hersteller, die Komponenten der TI-Föderation herstellen
- Anbieter, die Komponenten der TI-Föderation betreiben
- Architekten der gematik für das Verständnis des Vertrauensraum und die potentielle Nutzung für die Produkte der TI 2.0
- Sicherheitsexperten der gematik zur Bewertung der IT-Sicherheit der Gesundheitsanwendungen in der TI-Föderation
- Betriebsexperten der gematik zur Bewertung und Erfassung betrieblicher Rahmenbedingungen und Anforderungen
- Aufsichtsbehörden und Gesellschafter zur fachlichen und technischen Bewertung

### 1.3 Geltungsbereich

#### Wichtiger 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 Abgrenzung des Dokuments

Diese Dokument enthält keine konkreten Anforderungen an ein Produkt der TI-Föderation. Diese Anforderungen sind in den Spezifikationsdokumenten der Produkttypen [gemSpec\_IDP\_FedMaster] und [gemSpec\_IDP\_Sek] sowie in [gemSpec\_IDP\_FD] zur Berücksichtigung in den Produkttypen der Fachdienste beschrieben.

Das Dokument beschreibt nicht allumfassend, wie Komponenten außerhalb der TI-Föderation mit den Komponenten der TI-Föderation interagieren bzw., wie Artefakte (z.B. ID-Token, Access-Token) außerhalb der TI-Föderation zu verwenden sind.

## 1.5 Methodik

### 1.5.1 Technische Beschreibung

Das Dokument beschreibt die technischen Konzepte der TI-Föderation auf verschiedenen Abstraktionsebenen:

- Beteiligte technische Systeme und deren Aufgaben
- Schnittstellen zwischen den Systemen
- Schnittstellen zu Systemen außerhalb der TI-Föderation
- Schnittstellen zu Nutzern

Die technische Beschreibung erfolgt auf verschiedenen Granularitätsebenen mit unterschiedlichen Sichten auf die Gesamtarchitektur.

### 1.5.2 Normative Festlegungen

Das Konzeptdokument enthält keine normativen Festlegungen. Die normativen Festlegungen der beteiligten Systeme sind in den betreffenden Spezifikationen beschrieben:

- gemSpec\_IDP\_FedMaster - Anforderungen an Trust Anchor und Intermediate (Superior Entity) und allgemeine Anforderungen an Teilnehmer der TI-Föderation
- gemSpec\_IDP\_Sek - Anforderungen an sektorale Identity Provider (OpenID Provider)
- gemSpec\_IDP\_FD - Anforderungen an Fachdienst Authorization Server (OpenID Relying Party) und Fachdienst Resources (OAuth Protected Resource)

### 1.5.3 Hinweis auf offene Punkte <<optional, nur bis einschl. Abstimmphase >>

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

---

## 2 Fachliche & technische Rahmenbedingungen

---

### 2.1 Fachliche Grundlagen

#### 2.1.1 Begriffsbestimmungen

Zum weiteren Verständnis ist es notwendig zunächst die wesentlichen Begrifflichkeiten zu klären.

**Identität:** Eine Identität ist eine Menge von Identitätsattributen, die einer [Person oder Organisation] zugeordnet sind. Eine eindeutige Identität ist eine Identität, die innerhalb eines bestimmten Anwendungskontextes die zugehörige Entität eindeutig repräsentiert, unterschiedliche Entitäten haben unterschiedliche eindeutige Identitäten. Eine Identität (das heißt eine Menge von Identitätsattributen), die innerhalb eines Anwendungskontextes eindeutig ist, ist dies nicht notwendigerweise auch in einem anderen Kontext. (BSI TR-03107)

**Attribut:** Ein Identitätsattribut oder ein Identitätsdatum ist eine Charakteristik oder eine Eigenschaft einer Entität. Beispiele für Identitätsattribute einer natürlichen Person sind Name, Geburtsdatum oder die Eigenschaft, ein bestimmtes Alter erreicht zu haben. Identitätsattribute von Behörden umfassen etwa Bezeichnung der Behörde oder deren Webadresse. (BSI TR-03107)

**Authentisierung/Authentifizierung:** „Authentifizierung“ ist ein elektronischer Prozess, der die Bestätigung der elektronischen Identifizierung einer natürlichen oder juristischen Person oder die Bestätigung des Ursprungs und der Unversehrtheit von Daten in elektronischer Form ermöglicht. (eIDAS)

Eine Authentisierung ist das Versehen einer Identität oder anderer übermittelter Daten mit Metadaten, die es einer vertrauenden Entität ermöglichen, die Herkunft, Echtheit und Gültigkeit der Identität oder der Daten zu überprüfen. Der Überprüfungsvorgang durch die vertrauende Entität ist die Authentifizierung der Identität/der Daten. (BSI TR-03107)

**Authentisierungsmittel:** Authentisierungsmittel sind technische Mittel, die es dem Inhaber erlauben, eine Identität (das heißt eine Menge von Identitätsattributen) oder andere Daten zu authentisieren. Beispiele für Authentisierungsmittel sind Passwörter, der Personalausweis oder kryptographische Token. Sind mehrere technische Mittel notwendig (etwa Chipkarte und PIN), so besteht das vollständige Authentisierungsmittel aus mehreren Authentisierungsfaktoren. (BSI TR-03107).

**Multifaktor-Authentisierung:** Multifaktor-Authentisierung ist eine Form der Authentisierung, bei welcher zur Identitätsbestätigung mehrere unabhängige Merkmale (Faktoren) überprüft werden. Üblicherweise werden für eine Zwei-Faktor-Authentisierung unterschiedliche Merkmale aus Wissen, Besitz, Biometrie, Standort miteinander kombiniert. Am häufigsten kommt im Bereich der mobilen Anwendungen die Kombination aus Faktor Besitz (repräsentiert durch das Smartphone) und Faktor Biometrie (z. B. durch FaceID oder TouchID) bzw. Faktor Wissen (z. B. eine PIN) zum Einsatz.

**Enrolment:** Das Enrolment ist die Registrierung einer Entität in einem Authentisierungssystem, meist verbunden mit einer Identitätsprüfung, die in der Ausgabe von Authentisierungsmitteln mündet. (BSI TR-03107)

**Identifizierung:** Eine Identifizierung ist die Übermittlung von anwendungsbezogen geeigneten Identitätsattributen (einer Identität), einschließlich authentisierender



Metadaten (Authentisierung), sowie die Überprüfung (Authentifizierung) dieser Identität durch die vertrauende Entität. (BSI TR-03107)

**Identifizierungsdiensteanbieter:** Diensteanbieter, deren Dienst darin besteht, für einen Dritten eine einzelfallbezogene Identifizierungsdienstleistung mittels des elektronischen Identitätsnachweises nach § 18 zu erbringen (§ 2 Abs. 3a PAuswG).

**Autorisierung:** Die Autorisierung einer Entität ist die Zuordnung und Überprüfung von Rechten zu einer Entität, zum Beispiel Zugriffsrechte oder das Recht, eine bestimmte Anwendung zu nutzen. Eine Autorisierung erfolgt immer anwendungsbezogen [...]. (BSI TR-03107)

## 2.1.2 Technische Grundlagen

Für ein grundlegendes Verständnis des Konzeptes des föderierten Identitätsmanagements werden in diesem Kapitel zunächst die Grundlagen des eingesetzten Authentifizierungsprotokolls und die relevanten technischen Parameter kurz erläutert. Unter einem Authentifizierungsprotokoll versteht man im Allgemeinen eine Reihe an Befehlen, die zur Verifizierung einer Nutzeridentität zwischen zwei Entitäten verwendet werden. Für unterschiedliche Einsatzszenarien haben sich verschiedene Authentifizierungsprotokolle und De-Facto-Standards etabliert. Im Rahmen der Mensch-zu-Gerät-Authentisierung in der Telematikinfrastruktur wird das sog. OpenID Connect Protokoll verwendet, welches auf dem sog. OAuth 2.0-Standard basiert und diesen um Informationen zur Identität über Attribute erweitert.

**OAuth 2.0:** Hinter dem Begriff verbirgt sich ein **Autorisierungsdienst**, welcher es einem registrierten Nutzer ermöglicht, die Kontrolle über die Art und den Umfang der von ihm erteilten Freigaben zu steuern. Der Benutzer kann mittels OAuth der anfragenden Drittanwendung (dem sog. „**Client**“) erlauben, auf Daten des Nutzers auf einem **Resource-Server** (z. B. Bilder, Dokumente, u.ä.) zuzugreifen. Dazu authentisiert ein **Authorization-Server** den Nutzer z. B. mit username + Passwort und fordert von ihm die Erlaubnis (**Consent**) für den Zugriff des Client auf die Resource ein. Für den Zugriff auf die Daten des Nutzers vom Resource-Server erhält der Client ein Access-Token, welches dieser bei jedem Aufruf des Resource-Server mit übertragen muss. Vor Herausgabe der Daten prüft der Resource-Server durch eine Abfrage beim Authorization-Server, ob die Datenherausgabe an den Client legitim ist. OAuth 2.0 unterstützt scopes (Gruppe von Informationen), allerdings ohne diese weiter zu benennen. OAuth 2.0 kümmert sich ausschließlich um die Autorisierung von Zugriffen durch einen Nutzer, nicht aber um dessen Authentifizierung.

**OpenID Connect (OIDC):** Der OIDC-Standard erweitert OAuth 2.0 um die Fähigkeit der Nutzer-**Authentisierung**. Neben dem Zugriffstoken (Access-Token) liefert die Erweiterung OIDC nach erfolgreicher Nutzer-Authentisierung einen **ID-Token**, welche Informationen (claims) zum Nutzer selbst enthält. Claims sind Eigenschaftsattribute (z. B. der Vorname oder die Mailadresse). Die Zusammenfassungen von claims zu logischen Gruppen werden als scopes bezeichnet. Diese Identitätsdaten des Nutzers werden von einem **Identity Provider** in dem ID-Token verpackt und als JSON Web Token (**JWT**) einem anfragenden Client zur Verfügung gestellt.

## 2.1.3 Identifikationsmittel und -systeme

Es gibt je nach Schutzbedarf und Regulierungsniveau der zu verwendenden Anwendung unterschiedliche Möglichkeiten, eine Identifizierung des Nutzers durchzuführen. Gesundheitsdaten weisen nach DSGVO einen besonders schützenswerten Charakter auf. Folglich muss bei deren Zugriff zweifelsfrei sichergestellt sein, dass dieser nur durch berechnete Personen möglich ist. Hierfür gibt es in Deutschland unterschiedliche hoheitliche Identifikationssysteme mit einer jeweiligen Zweckbindung. Sie dienen dazu, eine Person oder ein Objekt eindeutig innerhalb eines

Nutzungskontextes zu identifizieren. Im Kontext des Gesundheitswesens dient die Gesundheitskarte mit zugehöriger Krankenversicherungsnummer als Identifikationsmittel mit entsprechender Zweckbindung. Diese kann über einen Chip entweder kontaktbehaftet oder mit NFC Funktionalität und einem auf ihr enthaltenen Lichtbild für Vor-Ort-Identifizierung bzw. eine PIN für eine Identifizierung online und vor Ort eingesetzt werden. Des Weiteren stellt der neue Personalausweis bzw. der elektronische Aufenthaltstitel bzw. die ID-Karte für EU/EWR-Bürger/innen mit integrierter eID-Funktionalität ein universell einsetzbares Identifikationssystem dar. Zu dessen digitaler Verwendung muss die zugehörige PIN durch den Nutzer freigeschaltet werden. Auf Basis des Personalausweises existieren unterschiedliche Identifizierungsverfahren. Das sicherste Verfahren ist das Online-Ausweisident-Verfahren, bei welchem das Auslesen des Datensatzes mittels NFC-Schnittstelle über die Eingabe der PIN abgesichert wird.

## 2.2 Die Ausgangslage im deutschen Gesundheitswesen

Die Telematikinfrastruktur (TI) ist die Plattform für Gesundheitsanwendungen in Deutschland. Millionen Versicherte profitieren durch die digitalen Anwendungen der TI von einer verbesserten medizinischen Versorgung. Ziel und Aufgabe der gematik ist es, diese Infrastruktur auszubauen, zu modernisieren und so fit für das digitale Gesundheitswesen der Zukunft zu machen.

Im Jahr 2005 wurde mit dem Aufbau der Telematikinfrastruktur durch die gematik begonnen. Mit dem Whitepaper zur Telematikinfrastruktur 2.0 wurde 2020 von der gematik ein Impuls veröffentlicht, die TI als zukunftsfähige Arena für digitale Medizin voranzutreiben.

Die Architektur der TI 2.0 basiert demnach auf sechs fundamentalen Säulen:

1. Einem föderierten Identitätsmanagement, weil mit dieser "Brücke" mehr Flexibilität und Nutzerfreundlichkeit durch die einfache Nutzung von Identitätsbestätigungen der TI für eigene digitale Angebote der Nutzergruppen möglich ist.
2. Der universellen Erreichbarkeit der Dienste, weil der Wegfall proprietärer IT-Lösungen (z. B. Konnektor) Kosten senkt und den Betrieb stabilisiert.
3. Einer modernen Sicherheitsarchitektur, weil diese die eigenständige Bereitstellung von Diensten durch unterschiedliche Anbieter ermöglicht und sowohl sicherer als auch effizienter ist.
4. Verteilten Diensten, weil aus Sicht optimierter Versorgungsprozesse die Verknüpfung von Daten aus verschiedenen Quellen notwendig ist.
5. Interoperabilität und strukturierte Daten, weil die anwendungsfallbezogene Versorgung und Forschung eine Verbesserung der Datenqualität erfordert. Standardbasierte strukturierte Daten und Schnittstellen erhöhen die Verfügbarkeit bei Produkten und Services.
6. Einem automatisiert verarbeitbaren Regelwerk der TI, weil eine automatisierte Überprüfung der Sicherheit und des Datenschutzes sowie der Interoperabilität und Verfügbarkeit das Vertrauen in die TI stärken.

Das vorliegende Dokument stellt die spezifikatorische Grundlage für die erste Säule des föderierten Identitätsmanagements.

Zu deren Verständnis werden im weiteren Verlauf dieses Kapitels zunächst die elementaren Grundpfeiler des Identitätsmanagements im Gesundheitswesen vorgestellt und soweit notwendig erläutert.

## 2.2.1 Identitätsherausgeber, Identitätsträger und Trust Service Provider

Unter Identitätsherausgeber versteht man diejenigen Instanzen, welche die Datenhoheit über die (digitalen) Identitäten und deren zugehörige Attribute besitzen. Für unterschiedliche Sektoren gibt es unterschiedliche Identitätsherausgeber, welche im SGB V geregelt werden. Je Sektor existieren spezifische Identitätsträger, welche in der Telematikinfrastruktur 1.0 über Smartcards repräsentiert werden und in der TI 2.0 durch digitale Identitäten bereitgestellt werden sollen.

Im gesetzlichen Versichertensektor agieren die Krankenkassen als Identitätsherausgeber, welche für ihre Versicherten die elektronische Gesundheitskarte als Identitätsträger herausgeben. Die gesetzliche Grundlage hierfür bildet §291 SGB V. In Deutschland gibt es derzeit rund 95 gesetzliche Krankenkassen (Stand 01.01.2026). Jede Kasse ist selbst für die Ausgabe der Identitätsträger zuständig. Eine Ausgabe von elektronischen Gesundheitskarten als Identitätsträger durch private Krankenversicherer und sonstige Kostenträger gibt es derzeit nicht.

Im Leistungserbringerbereich wird die Identitätsherausgabe, im engeren Sinne die Ausgabe von elektronischen Heilberufs- und Berufsausweisen sowie von Komponenten zur Authentifizierung von Leistungserbringerinstitutionen, in § 340 SGB V geregelt. In der praktischen Umsetzung ergibt sich hieraus die Zuständigkeit für die Herausgabe der elektronischen Heilberufsausweise durch die Kammern auf Landesebene (z. B. Landesärztekammern, Landeszahnärztekammern, Psychotherapeutenkammern, Apothekerkammern, Handwerkskammern). Darüber hinaus übernehmen die gematik und das elektronische Gesundheitsberufsregister (eGBR) für ausgewählte Gruppen die Rolle des Identitätsherausgebers, sodass sich in Summe für den Identitätsträger eHBA rund 100 Identitätsherausgeber ergeben. Die Herausgabe der SMC-Karte als Identitätsträger für Leistungserbringerinstitutionen übernehmen je Sektor die Kassenärztlichen Vereinigungen, Kassenzahnärztliche Vereinigungen, Apothekerkammern, DKTIG, gematik, Gesundheitsberufsregister und Handwerkskammern. Hier agieren in Summe rund 70 Identitätsherausgeber für den Identitätsträger der SMC-B-Karte.

Mit der Bereitstellung der Identitätsträger werden bei Bedarf sog. Trust Service Provider beauftragt. Ein Trust Service Provider oder Vertrauensdiensteanbieter ist eine Organisation, welche digitale Zertifikate bereitstellt, um elektronische Signaturen zu erstellen und zu validieren und ihre Unterzeichner im Allgemeinen zu authentifizieren.

### Elektronische Gesundheitskarte (eGK)

Die elektronische Gesundheitskarte (eGK) ist eine personenbezogene Smartcard. Die eGK gilt seit Anfang 2015 als ausschließlicher Krankenversicherungsnachweis für gesetzlich Versicherte. Neben den kryptographischen Schlüsseln und dazugehörigen Zertifikaten zur Authentisierung gegenüber der TI dient sie abhängig des Ausgabezeitpunktes auch als dezentraler Speicher für die Datensätze Notfalldaten-Management, Datensatz Persönliche Erklärung, Organpendeerklärung, E-Medikationsplan und den Versichertenstammdaten (gemäß §291 Absatz 2 Nummer 3 SGB V ermöglicht die eGK - sofern sie nach dem 1. Januar 2023 ausgestellt wurde, nur noch die Speicherung von Daten nach § 291a Absatz 2 Nummer 1 bis 3 und 6).

### Elektronischer Heilberufsausweis (HBA)

Der elektronische Heilberufsausweis ist eine personenbezogene Smartcard, welche an Leistungserbringer wie Ärzte, Zahnärzte oder Apotheker ausgegeben wird. Er enthält das kryptographische Schlüsselmaterial und die zugehörigen Zertifikate zur Authentisierung gegenüber der TI, zum Ausstellen einer qualifizierten elektronischen Signatur für die E-Rezept-Ausstellung, die Signatur von KIM-Nachrichten, Notfalldaten und dem elektronischen Arztbrief sowie der Verschlüsselung, Entschlüsselung und Umschlüsselung von Nachrichten.

### Institutionsbezogene Identität SM(C)-B

Die Security Module (Card) Typ B ist eine institutionsbezogene Identität, welche an eine Smartcard oder als Zertifikatsbundle gekoppelt herausgegeben wird. Sie repräsentiert eine Institution innerhalb der TI und sie stellt Zertifikate für Authentisierung, Ver-, Ent- und Umschlüsselung sowie elektronische Signaturen zur Verfügung.

## 2.2.2 Der Weg zur TI 2.0

Die drei genannten Smartcard-Typen stellen in der Telematikinfrastruktur 1.0 die primären Identitätsträger dar. Jedoch bringt die Anwendung (ausschließlich) kartenbasierter Identitätsträger eine Reihe an Nachteilen und Einschränkungen mit sich. Als wesentliche Grenzen seien an dieser Stelle genannt:

- Smartcards schränken die Usability ein, insbesondere im Einsatz mit mobilen Endgeräten
- In mobilen Szenarien ist die Einsetzbarkeit von Smartcards abhängig von der Gerätehardware (Vorhandensein und Platzierung des NFC-Moduls)
- Änderungen an Rollen oder Attributen in Zertifikaten auf Smartcards können nur schwer nachgerüstet werden. Für neue Nutzergruppen müssen neue Smartcards durch Herausgeber und TSPs bereitgestellt werden. Insbes. unter den aktuellen Lieferengpässen von Hardware und Chipkarten stellt dies eine große Einschränkung der Nutzeranbindung dar.
- Lange (Wieder-)beschaffungszeiten, insbesondere bedingt durch den aktuellen Engpass von Chipkarten.

Auch auf Seite des Gesetzgebers wurden diese Einschränkungen erkannt und die Einführung digitaler Identitäten vorgesehen. Die Konzeption der digitalen Identitäten strebt an, die Gesamtheit der relevanten Use Cases in Bezug auf die Authentisierung zu betrachten, welche zuvor für den aktuellen Einsatz der Smartcards vorgestellt wurden. Diese sollen auch um die Einsatzszenarien der digitalen Identitäten erweitert werden.

Darüber hinaus kommen mit gSMC-K und gSMC-KT zwei gerätespezifische Sicherheitsmodulkarten in der TI zum Einsatz. Für das föderierte Identitätsmanagement finden diese jedoch keine Anwendung und werden deswegen nicht weiter betrachtet.

## 2.2.3 Gesetzliche Rahmenbedingungen

In diesem Kapitel folgt eine Übersicht über die relevantesten rechtlichen Grundlagen der vorliegenden Konzeption. Sie erhebt keinen Anspruch auf Vollständigkeit. Zum 01.01.2023 trat das Krankenhauspflegeentlastungsgesetz (KHPfLEG) in Kraft, welches zu einer Änderung der §§291 und 340 SGB V führte. Die Neuerungen finden bereits Berücksichtigung in diesem Kapitel.

Die Begründung der verpflichtenden Einführung der digitalen Identitäten im Gesundheitswesen findet sich im fünften Sozialgesetzbuch. Hier heißt es:

„Spätestens ab dem 1. Januar 2024 stellen die Krankenkassen den Versicherten ergänzend zur elektronischen Gesundheitskarte auf Verlangen eine sichere digitale Identität für das Gesundheitswesen barrierefrei zur Verfügung, die die Vorgaben nach Absatz 2 Nummer 1 und 2 erfüllt und die Bereitstellung von Daten nach § 291a Absatz 2 und 3 durch die Krankenkassen ermöglicht.“ **(§291 Absatz 8 Satz 1 SGB V).**

Eine analoge Vorgabe für Leistungserbringer und deren Institutionen findet sich in Paragraph 340:

„(6) Spätestens ab dem 1. Januar 2024 haben die Stellen nach Absatz 1 Satz 1 Nummer 1 sowie den Absätzen 2 und 4 ergänzend zu den Heilberufs- und Berufsausweisen auf Verlangen des Leistungserbringers eine digitale Identität für das Gesundheitswesen zur

Verfügung zu stellen, die nicht an eine Chipkarte gebunden ist“ (**§340 Absatz 6 Satz 1 SGB V**).

„(7) Spätestens ab dem 1. Januar 2025 haben die Stellen nach Absatz 1 Satz 1 Nummer 3 sowie den Absätzen 2 und 4 ergänzend zu den Komponenten zur Authentifizierung von Leistungserbringerinstitutionen auf Verlangen der Leistungserbringerinstitution eine digitale Identität für das Gesundheitswesen zur Verfügung zu stellen, die nicht an eine Chipkarte gebunden ist.“ (**§340 Absatz 7 Satz 1 SGB V**).

Des Weiteren definieren die jeweiligen Paragraphen die Rolle der Verantwortlichkeiten:

„Die Gesellschaft für Telematik legt die Anforderungen an die Sicherheit und Interoperabilität der digitalen Identitäten fest. Die Festlegung der Anforderungen an die Sicherheit und den Datenschutz erfolgt dabei im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit auf Basis der jeweils gültigen Technischen Richtlinien des Bundesamts für Sicherheit in der Informationstechnik und unter Berücksichtigung der notwendigen Vertrauensniveaus der unterstützten Anwendungen.“ (**§291 Absatz 8 Satz 3 und 4 SGB V** bzw. sinngemäß **§340 Absatz 8 Satz 1 und 2 SGB V**).

Sowohl für digitale Identitäten für Versicherte nach § 291 Abs. 8 SGB V als auch für Leistungserbringende und Leistungserbringerinstitutionen nach § 340 Abs. 8 SGB V muss das '[...] Sicherheits- und Vertrauensniveau der Ausprägung einer digitalen Identität [...] mindestens dem Schutzbedarf der Anwendung entsprechen, bei der diese eingesetzt wird (§ 291 Absatz 8 Satz 6 bzw. § 340 Absatz 8 Satz 4 SGB V, gleichlautend).

Mit den Änderungen des KHPfIEG wurde des Weiteren Satz 7 in §291 SGB V aufgenommen: "Abweichend von Satz 6 kann der Versicherte nach umfassender Information durch die Krankenkasse über die Besonderheiten des Verfahrens in die Nutzung einer digitalen Identität einwilligen, die einem anderen angemessenen Sicherheitsniveau entspricht." (**§291 Absatz 8 Satz 7 SGB V**)

Die entsprechenden Technischen Richtlinien des Bundesamts für Sicherheit in der Informationstechnik beziehen sich auf:

- **BSI TR-03107-1** Elektronische Identitäten und Vertrauensdienste im E-Government
- **BSI TR-03147** Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen.

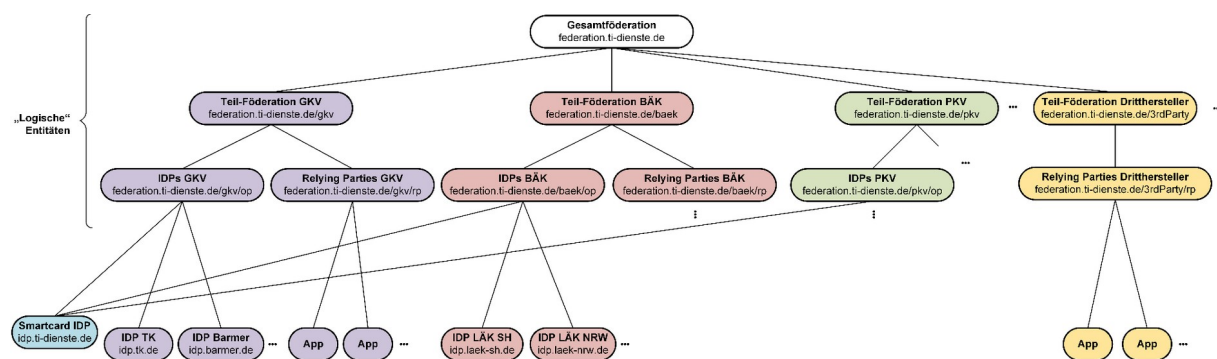
Allgemein gilt nach EU-DSGVO, dass Gesundheitsdaten von besonders schützenswertem Charakter sind. Entsprechend ist das Vertrauensniveau nach TR-03107-1 mit einem hohen Vertrauensniveau zu bewerten.

Ferner beeinflussen Inhalte der Verordnung „über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“ (kurz: **eIDAS-Verordnung**, [eIDAS]) die Anforderungen an die Bereitstellung der digitalen Identitäten.

## 2.3 Fachliche Einordnung der sektoralen Identity Provider

Aufbau, Funktionsumfang und Schnittstellen der Identity Provider, sollen im Rahmen einer Föderation den Zugang zur Telematikinfrastruktur alternativ der kartengebundenen Identitäten ermöglichen.





**Abbildung 1 : Idee des Aufbaus einer TI-Föderation auf Basis des OpenID Federation Standards**

Unter Föderation versteht sich, dass jeder Sektor, und innerhalb der Sektoren die jeweiligen Identitätsherausgeber einen eigenen Identity Provider für dessen Mitglieder bereitstellt. Bei den digitalen Identitäten für den Sektor „Versicherte“ stellen die Kostenträger, sprich die gesetzlichen Krankenversicherungen und die privaten Versicherungsunternehmen jeweils eigene Identity Provider zur Verfügung, über welchen sich deren Versicherte gegenüber den Diensten der TI und kasseneigenen sowie Drittdiensten authentisieren können. Dabei ist es auch möglich, dass mehrere Institutionen auf freiwilliger Basis einen gemeinsamen IDP bereitstellen. Die Anforderungen an die Identity Provider der unterschiedlichen Sektoren unterscheiden sich. Dies liegt vor allem darin begründet, dass die Anwendungsfälle und Anwendungen, welche eine Authentifizierung eines Nutzers über einen IDP erfordern für Versicherte andere sind als z.B. für Ärzte in Praxen und Krankenhäusern oder für andere medizinische Berufe wie Hebammen und Pflegedienste.

Die Orchestrierung der unterschiedlichen Identity Provider in der Föderation erfolgt über den sog. Federation Master. Ziel der Föderation aus Versichertensicht ist es, dass sich jeder Nutzer an jedem relevanten Dienst der TI, der Kassen und an digitalen Gesundheitsanwendungen (DiGAs) mit einem zentralen Zugang über den IDP seiner Krankenversicherung authentisieren kann. Hierbei soll der IDP einen relevanten Basisdatensatz an Attributen, welcher zur Anwendungsnutzung benötigt wird, bereitstellen und in Form eines Tokens an die jeweilige Anwendung übergeben. Auf diese Weise soll den Versicherten über den zentralen Zugang eine komfortable und niederschwellige Nutzung ermöglicht sowie auf Seiten der Anwendungen eine Konzentration auf deren Kernprozesse vereinfacht werden.

## 2.4 Rahmenbedingungen des Authentisierungs-Flows

### 2.4.1 Relevante Anwendungen der IDP-Nutzung

Die Einführung digitaler Identitäten in Föderation beschreibt keinen Selbstzweck. Es geht dabei vordergründig darum, über einen zentralen Zugang die Nutzung sämtlicher Anwendungen des Gesundheitswesens sicher und komfortabel nutzen zu können. Dabei kommen Anwendungen zum Einsatz, welche kassenspezifisch und kassenübergreifend bereitgestellt werden.

Kassenübergreifende Anwendungen werden dadurch charakterisiert, dass die gleiche Anwendung für jeden Versicherten unabhängig seiner Krankenversicherung angeboten wird. Dabei müssen sich Versicherte unterschiedlicher Kassen über deren jeweiligen Kassen-IDP authentisieren können. Als kassenübergreifende Anwendungen sind insbesondere relevant:

- **E-Rezept:** Hierbei handelt es sich um eine kassenübergreifende Anwendung, welche zentral durch die gematik für alle Kassen bereitgestellt wird. Die entsprechenden Regelungen finden sich in §360 SGB V. Das E-Rezept ist eine zentrale Anwendung der Telematikinfrastruktur und somit eine der Kernnutzungsanwendung der digitalen Identitäten.
  - **Digitale Gesundheitsanwendungen:** Der Leistungsanspruch auf digitale Gesundheitsanwendungen (kurz: DiGA) begründet sich auf das Digitale-Versorgung-Gesetz. In der zugehörigen DiGA-Verordnung ist u.a. festgeschrieben, dass DiGA-Hersteller eine Authentisierung über die Kassen-IDPs ermöglichen müssen.
  - **Drittanwendungen** mit Gesundheitsbezug: Des Weiteren soll es über die Kassen-IDPs auch ermöglicht werden, kassenübergreifende Dritt-Anwendungen, vordergründig mit einem Bezug zum Gesundheitswesen, nutzbar zu machen. Beispielsweise könnte dies eine kassenunabhängige App zur digitalen Terminbuchung von Arztterminen sein, an welcher sich ein Versicherter mit seinem Zugang des Kassen-IDPs authentisieren kann. Die Nutzung dieser Anwendungen ist nicht gesetzlich reguliert und obliegt der Hoheit der jeweiligen Kasse.
- Darüber hinaus sollen über die digitalen Identitäten kasseneigene Anwendungen für Versicherte nutzbar gemacht werden. Diese müssen jeweils nur eine Authentisierung über den eigenen IDP ermöglichen. Versicherte anderer Kostenträger müssen an dieser Stelle nicht berücksichtigt werden. Es handelt sich insbesondere um folgende Anwendungen:
- **Elektronische Patientenakte:** Die Bereitstellung der elektronischen Patientenakte (kurz: ePA) durch die Kassen wird in §341 SGB V geregelt. Folglich ist diese Anwendung kassenspezifisch und muss entsprechend nur mit dem eigenen IDP kommunizieren können.
  - **Kasseneigene Service-Anwendungen:** Dies können beispielsweise kasseneigene Service-Apps, Online-Geschäftsstellen oder Informations-Apps sein. Aus nutzerorientierten und wirtschaftlichen Gesichtspunkten heraus soll es den Kassen nach eigenem Ermessen möglich sein, auch für diese Anwendungen eine Nutzung mittels sektorialem Kassen-IDP zu implementieren.

Die im Februar 2023 veröffentlichte Spezifikation der gematik richtet sich aufgrund der gesetzlichen Anforderungen vordergründig an den Anwendungen E-Rezept, DiGAs und ePA aus. Die Erweiterung des Funktionsumfangs eines Kassen-IDPs zur Nutzung weiterer, insbes. kasseneigener Anwendungen obliegt dem Kostenträger und ist außerhalb des Anwendungsbereichs der Spezifikation der gematik zu sehen, sofern sicherheitskritische Aspekte nicht beeinträchtigt werden.

## Vertrauensniveaus

Das Vertrauensniveau einer Anwendung definiert sich aus dem Schutzbedarf der Daten, welche innerhalb der Anwendung verarbeitet werden. Die Zuordnung zu einem Vertrauensniveau berücksichtigt dabei u.a. die technische und organisatorische Sicherheit des Verfahrens sowie rechtliche Rahmenbedingungen. Die zugrundeliegende TR-03107 des BSI definiert hierbei 3 Vertrauensniveaus: normal, substantiell, hoch. Die zuvor beschriebenen Fokusanwendungen E-Rezept, DiGAs und ePA haben das Vertrauensniveau hoch inne. Folglich fokussiert sich die Spezifikation auf dieses Vertrauensniveau. Die Unterstützung von weiteren Vertrauensniveaus obliegt der Kasse und wird nicht durch die Spezifikation tangiert, sofern sicherheitskritische Aspekte nicht beeinträchtigt werden.

## Bereitstellung von claim

Anwendungen fragen im Rahmen der Authentisierung spezifische scopes beim IDP an, welche sich aus vordefinierten claims zusammensetzen. Damit sichergestellt ist, dass der IDP für die Fokusanwendungen E-Rezept, DiGAs und ePA die

erforderlichen scopes bereitstellen kann, wird ein sog. minimal claims Set definiert, welches ein IDP mindestens vorhalten muss, um an der Föderation teilzunehmen.

## Zugriffsmedien

Die zuvor beschriebenen Anwendungen sollen über unterschiedliche Medien und Anwendungstypen ermöglicht werden. Im Grunde unterscheiden sich die Zugriffsmedien zwischen Smartphone (und hier weiter zwischen mobiler App und Browseranwendung) und zwischen Desktop-PCs. Sämtliche betrachteten Anwendungen können sowohl über eine App als auch über eine Browseranwendung bereitgestellt werden.

Hieraus ergibt sich der Bedarf an unterschiedlichen Flows, welche durch die IDPs zu unterstützen sind.

- **App-App-Flow:** Der App-App-Flow beschreibt die Einzelschritte für die Authentifizierung eines Nutzers im Rahmen einer Fachanwendung, bei der die Fachanwendung eine App ist, welche auf demselben Gerät wie die Authenticator-App installiert ist. Beispielsweise kommt dieser Flow zum Tragen, wenn ein Nutzer die E-Rezept-App auf seinem Smartphone benutzen möchte und sich mit der Kassen-App auf dem gleichen Gerät authentisiert.
- **Web-App-Flow auf einem Gerät:** Der Web-App-Flow beschreibt die Einzelschritte für die Authentifizierung eines Nutzers im Rahmen einer Web-Anwendung, welche im Browser desselben Geräts ausgeführt wird, auf dem auch die Authenticator-App installiert ist. Ein Beispiel hierfür ist eine DiGA als Webanwendung, für welche die Authentisierung per Kassen-App auf demselben Smartphone erfolgt.
- **Zwei-Geräte-Flow:** Der Zwei-Geräte-Flow beschreibt die Einzelschritte für die Authentifizierung eines Nutzers im Rahmen einer Fachanwendung, wobei die Fachanwendung eine App oder Web-Anwendung sein kann, welche auf einem anderen Gerät als die Authenticator-App ausgeführt wird. Als Beispiel ist hier ein Zugriff auf die ePA über einen Desktop-Browser zu nennen, für welche die Authentisierung per Kassen-App auf dem Smartphone erfolgt.

## 2.4.2 Ablauf der Authentisierung

Der genaue Ablauf der Authentisierung hängt von den beschriebenen Rahmenbedingungen ab. Diese entscheiden maßgeblich darüber, für welche Anwendung, über welches Medium und mit welchen Authentisierungsmitteln zugegriffen werden kann. Unabhängig der Rahmenbedingungen kommt der zuvor beschriebene Standard des OpenID Connect Protokolls zum Einsatz. In dessen Kontext wird nach erfolgreicher Authentifizierung des Nutzers beim IDP ein ID-Token generiert und an die Fachanwendung übermittelt. Dieser Token enthält die durch den Client angefragten scopes einschließlich weiterer relevanter Daten. Nach Erhalt des ID-Token ist das eigentliche Zugriffsmanagement in der Verantwortung der Fachanwendung. Diese prüft, welche Berechtigungen und ggf. Bevollmächtigungen für die Entität des ID-Token vorliegen. Das Ergebnis dieser Prüfung äußert sich in der Ausstellung des Access-Token durch die Fachanwendung, über welchen der authentifizierte Nutzer die Zugriffsberechtigung auf die Daten der Fachanwendung erhält.



## 3 Systemüberblick

### 3.1 Allgemeiner Überblick

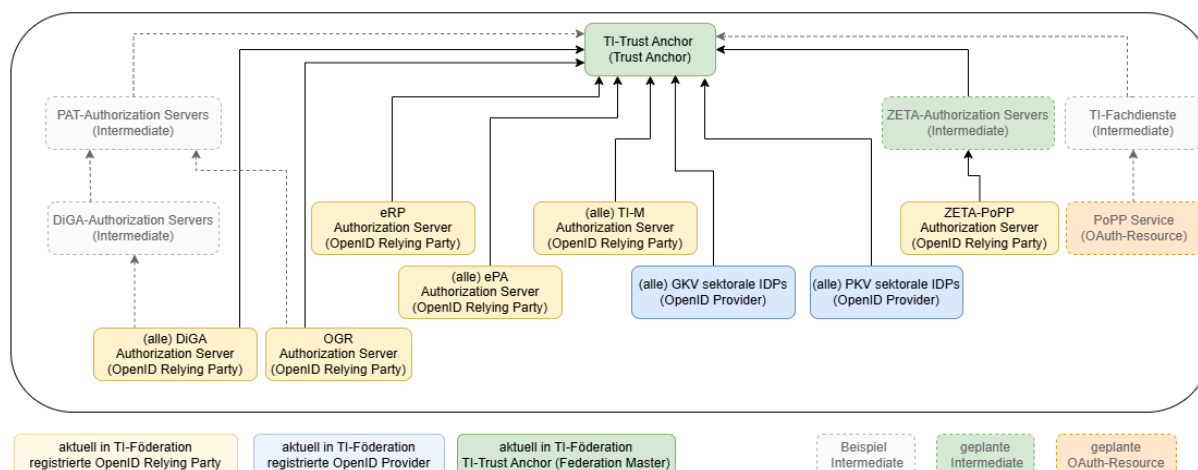
Zentrales Merkmal der zu entwickelnden Gesamtlösung der sektoralen IDP ist das Prinzip der Föderation. Die Funktionalität des IDP wird nicht von einem einzigen zentralen Dienst bereitgestellt, sondern kollektiv durch eine Menge von sektoralen IDP, für die jeweils die entsprechenden identitäts herausgebenden 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 IDP nutzen können, sind in bestimmten Bereichen einheitliche Vorgaben für die technische und organisatorische Umsetzung zu erstellen:

- Einheitliche Identitätsattribute für die Nutzergruppen (Scopes, Claims),
- Einheitliche Verfahren zum Auffinden von sektoralen IDP (IDP Discovery),
- Grundstruktur der Vertrauensbeziehungen der Föderierung (zwischen Fachdiensten und IDP),
- Einheitliche Vertrauensniveaus (Trust Framework).

Die Abbildung "Beispiel des Aufbau der TI-Föderation" zeigt, wie eine TI-Föderation strukturiert werden könnte. Alle sektoralen Identity Provider der Föderation sind beim Federation Master registriert. Wenn bei Erweiterung der TI-Föderation um andere Sektoren signifikant andere Anforderungen an sektoralen IDPs gestellt werden, kann es sinnvoll sein die sektoralen IDP der unterschiedlichen Sektoren unter Intermediates zusammenzufassen. Alle Authorization Server der Fachanwendungen, welche die bei den Identity Providern hinterlegten digitalen Identitäten nutzen möchten, sind ebenfalls beim Federation Master oder bei einem Intermediate registriert. Alle Intermediate sind bei einem anderen Intermediate oder beim Federation Master registriert.

*Hinweis: Abweichend zum dargestellten Beispiel sind aktuell alle sektoralen IDPs und auch alle DiGA-Authorization Server sowie der OGR Authorization Server direkt am Federation Master registriert. Die Spezifikation und Umsetzung von Intermediates erfolgt, wenn ein Bedarf, z.B. speziell für einen Teil der TI-Föderationsteilnehmer geltende Policies oder benötigte TrustMarks, besteht.*



**Abbildung 2 :Beispiel des Aufbau der TI-Födeartion**

Die TI-Föderation besteht aus unterschiedlichen Systemen, welche untereinander über standardisierte Schnittstellen kommunizieren. Zusammen bilden die beteiligten Systeme einen Vertrauensraum.

Nutzer verwenden verschiedene Fachdienste der Telematik Infrastruktur (TI). Die Fachdienste sind Apps oder Browseranwendungen. Hier werden Nutzern spezielle, in der Regel medizinische, digitale Services angeboten. Die Fachdienste nutzen sektorale IDP zur Überprüfung, ob ein Anwender zur Nutzung des Fachdienstes befugt (autorisiert) ist. Jeder Fachdienst verfügt dazu über einen eigenen Authorization Server, welcher basierend auf den Informationen der sektoralen Identity Provider über den jeweiligen Nutzer dessen Zugriffsrechte definiert. Diese Fachdienst Authorization Server sind OpenID Relying Parties gemäß [OpenID Federation 1.1] Komponenten der TI-Föderation.

Als sektoraler IDP wird ein Dienst zur Authentifizierung von Nutzern bezeichnet. Nach erfolgreichem Durchlaufen des Authentifizierungsprozesses stellt der sektorale IDP Identitätsinformationen für die Nutzer in Form eines ID-Token aus. Der Inhalt der Informationen ist spezifisch für eine bestimmte Gruppe von Nutzern, welche einem Sektor innerhalb der Telematikinfrastruktur des Gesundheitswesens zuzuordnen sind. Die Identitätsinformationen der Nutzer werden durch den anfordernden Fachdienst zur Prüfung verwendet, auf welche Fachdaten und -prozesse der Nutzer zuzugreifen darf. Insbesondere umfasst ein Sektor die Krankenkassen mit den Versicherten als Nutzer. Es ist nicht ausgeschlossen, dass ein sektoraler IDP Identitätsinformationen mehrerer Nutzergruppen bedienen kann (siehe auch Parameter "user\_type\_supported" als claim der Entity Configuration eines sektoralen IDP in [gemSpec\_IDP\_Sek]). Diese sektoralen IDP sind OpenID Provider gemäß [OpenID Federation 1.1] ebenfalls Komponenten der TI-Föderation.

Der TI-Vertrauensraum wird durch Superiors Entities gemäß [OpenID Federation 1.1] aufgespannt, die entweder als Trust Anchor oder Intermediates ausgeprägt sein können. Alle Teilnehmer der TI-Föderation sind bei einem Superior registriert, nur registrierte Teilnehmer sind berechtigt, die Dienste der TI-Föderation in Anspruch zu nehmen.

Der Trust Anchor der TI-Föderation ist der Federation Master (siehe [gemSpec\_IDP\_FedMaster]). Der Federation Master ist eine zentrale Komponente für alle Teilnehmer - Intermediates, Fachdienste Authorization Server und sektoralen IDPs - in der TI-Föderation. Intermediates sind Trust Anchor für einen Teil der TI-Föderation, der sich durch spezielle Regeln von andern Teilnehmern unterscheidet (z.B. ZETA-Intermediate für alle ZETA-Authorization Server, DiGA-Intermediate für alle DiGA Authorization Server).

Neben Fachdienst Authorization Servern (Relying Party) sektoralen IDP (OpenID Provider), Intermediates und Federation Master (Superior) können weitere Komponenten (Entity Types) Teil der TI-Föderation werden, z.B. TI-Fachdienste selbst als OAuth-Resource gemäß [OpenID Federation 1.1].

Die Kommunikation zwischen den Systemen in der TI-Föderation basiert auf den Standards für OpenID Federation, OpenID connect (OIDC), OAuth 2, JWT und weitere.

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 Bestandssysteme, in denen aktuell die Informationen zu Nutzern gepflegt werden.

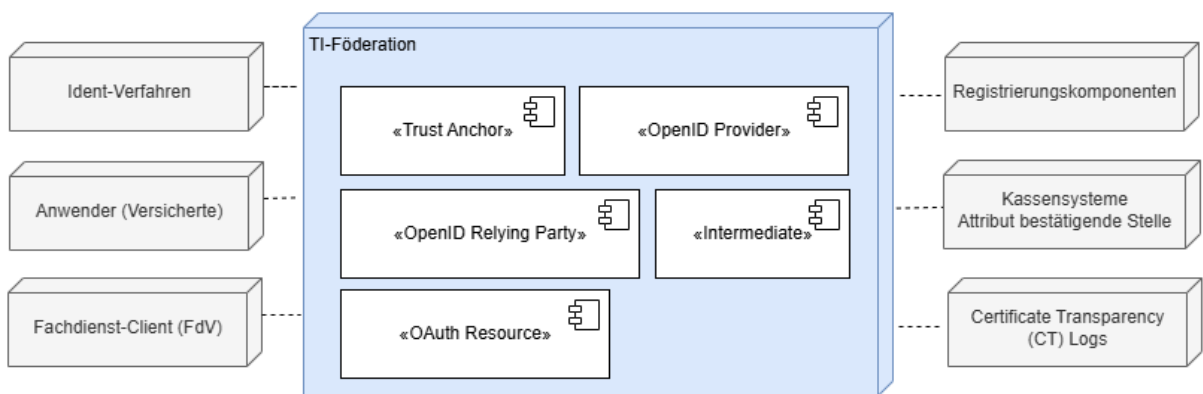


Abbildung 3 : TI-Föderation und Nachbarsysteme

**Anwender / Versicherte:**Anwender sind die Versicherten, die einen Fachdienst(über ein FdV) nutzen möchten. Um diesen Fachdienst nutzen zu können, müssen sich die Anwender authentifizieren. Die Authentifizierung mit GesundheitsID erfolgt dabei über die Komponenten der TI-Föderation. Zur Einwilligung in die Datenweitergabe an einen Fachdienst und bei der Nutzung eines Authentisierungsmittel sind die Anwender aktiv in den Authentifizierungsablauf eingebunden.

**Fachdienst-Client:**Fachdienst-Client ist in der derzeitigen TI-Föderation, die ausschließlich die Authentifizierung von Versicherten unterstützt, das Frontend des Versicherten (FdV). Anforderungen zur Nutzerauthentifizierung werden aus dem FdV an eine Relying Party der TI-Föderation geschickt. Je nach konkreter Umsetzung des Fachdienstes wird das Ergebnis der Authentifizierung dem Fachdienst-Client zurückgegeben. Ist die Kommunikation zwischen Fachdienst-Client und Relying Party z.B. nach OAuth-Standard umgesetzt erhält der Fachdienst-Client ein Access-Token. Zum anderen ist die Frontend-Komponente des OpenID-Provider, das Authenticator-Modul, für die Interaktion mit dem Nutzer im Authentifizierungsprozess in ein FdV integriert.

**Kassensysteme:** Die Kassensysteme sind die Datenquellen für die zu authentifizierenden Versicherten. Die für die Versicherten Authentifizierung notwendigen Daten werden von den sektoralen IDPs der Krankenkassen aus deren Kassensystemen bezogen.

**Registrierungskomponente:** Die Registrierung von Teilnehmern in der TI-Föderation wird über eine Registrierungskomponenten durchgeführt. Aktuell ist dies ein organisatorischer Prozess mit mehreren beteiligten Organisationen und Systemen. Zukünftig wird dieser organisatorische Prozess automatisiert.

**Certificate Transparency (CT) Logs:** Die TI-Föderation bezieht von Anbietern Certificate Transparency (CT) Logs für die Überprüfung der TLS-Schlüssel von sektoralen IDPs.

**Ident-Verfahren:** Zur sicheren Identifikation von Versicherten müssen diese sich mit einem sicheren Identifikationsverfahren (z.B. Online-Ausweisfunktion, Post-Ident, eGK mit PIN) gegenüber sektoraler IDPs identifizieren.

3.2 Schnittstellen zu Umsystemen

Tabelle 1 : Schnittstellen zu Umsystemen

Schnittstelle	Komponente/System in der TI-Föderation	fachliche Schnittstellenbeschreibung
---------------	--	--------------------------------------

Anwender / Versicherte	sektoraler IDP - Authenticator Modul	<ul style="list-style-type: none"> <li>Die Nutzerauthentifizierung durch den sektoralen IDP erfolgt über das Authenticator-Modul.</li> <li>Die Interaktion des Nutzers zur Nutzerauthentifizierung, Consent Freigabe und Einsichtnahme in die Datennutzung erfolgt über das Authenticator-Modul.</li> </ul>
Fachdienst-Client	Fachdienst-Authorization Server	<ul style="list-style-type: none"> <li>Sendet Anfragen zur Nutzerauthentifizierung an den Fachdienst-Authorization Server</li> <li>Wenn die Kommunikation zwischen Fachdienst-Client und Fachdienst-Authorization Server auf Basis OAuth2 durchgeführt wird (empfohlen), erhält der Fachdienst-Client ein Acces-Token für den Zugriff auf den Fachdienst (OAuth-Resource)</li> <li>Die Schnittstellen zwischen Fachdienst-Client und Fachdienst-Authorization Server ist Fachdienst spezifisch und nicht Teil der TI-Föderation</li> </ul>
Kassensysteme Attribut bestätigende Stelle	sektoraler IDP	<ul style="list-style-type: none"> <li>Die Kassensysteme sind die Quellsysteme der Versichertendaten.</li> <li>Die Schnittstellen zwischen dem Kassensystem und dem sektoralen IDP ist Kassen spezifisch und nicht Teil der TI-Föderation</li> </ul>
Registrierungskomponente	Federation Master	<ul style="list-style-type: none"> <li>Über Prozesse der Registrierungskomponente registrieren / deregistrieren sich Teilnehmer in der TI-Föderation bzw. ändern ihre Registrierungsdaten.</li> <li>Nach Prüfung der Teilnehmerdaten ruft die Registrierungskomponente Schnittstellen am Federation Master zur Aufnahme, Änderung oder Löschung von Teilnehmern im Vertrauensraum der TI-Föderation auf.</li> <li>Die Schnittstellen zwischen Registrierungskomponente und Federation Master sind Teil der TI-Föderation und der aktuell über einen organisatorischen Prozess abgebildet.</li> </ul>
Certificate Transparency (CT) Log	Federation Master	<ul style="list-style-type: none"> <li>Zur Prüfung der TLS-Schlüssel der sektoralen IDPs ruft der Federation Master Certificate Transparency (CT) Logs ab</li> </ul>

		<ul style="list-style-type: none"> <li>Die Schnittstelle zum Abruf des CT-Log ist abhängig von den eingesetzten Produkten und nicht Teil der TI-Föderation</li> </ul>
Ident-Verfahren	sektoraler IDP	<ul style="list-style-type: none"> <li>Zur Einrichtung der GesundheitsID ist die Identifikation der Versicherten über ein Ident-Verfahren notwendig</li> <li>Die Schnittstellen zwischen den sektoralen IDPs und den Ident-Verfahren sind Verfahren spezifisch und nicht Teil der TI-Föderation</li> </ul>

707

## 4 Lösungsstrategie

### 4.1 Anwendungsfälle

Superior Entities (federation\_entity) können gemäß [[OpenID Federation](#)] (Kapitel "Introduction") entweder Trust Anchor oder Intermediate sein. Jeder Teilnehmer der TI-Föderation, so auch die Superior Entities, müssen eine Selbstauskunft (Entity Configuration) in einem das Entity Statement veröffentlichen. Die Inhalte des Entity Statement sind im [[OpenID Federation](#)] Standard festgelegt (Kapitel "Claims that MUST or MAY Appear in both Entity Configurations and Subordinate Statements", "Federation Entity").

Superior Entities sind Komponenten, welche in den Kommunikationsfluss bei der Nutzung von Fachdiensten der TI eingebunden sind. Zudem sind Superior Entities an notwendigen organisatorischen Prozessen beteiligt. Folgende Anwendungsfälle dienen der Beschreibung der Anforderungen an Superior Entities:

**Tabelle 2 : Übersicht über die Anwendungsfälle im Gesamtkontext Federation Master**

Use Case	Komponente	Kurzbeschreibung
Teilnehmer registrieren	Federation Master / Intermediate	<p>Jeder Authorization Server einer Fachanwendung, jeder sektorale IDP und jede protected Resource muss sich als Teilnehmer bei einer Superior Entity (Federation Master oder Intermediate) registrieren. Im Zuge der Registrierung wird der öffentliche Teil des Schlüssels, mit dem der Teilnehmer sein Entity Statement signiert, bei einer Superior Entity hinterlegt.*</p> <ul style="list-style-type: none"> <li>Für jede Fachanwendung wird zusätzlich hinterlegt, welche Informationen zum Nutzer (Scope bzw. Claims) diese beim Identity Provider erfragen dürfen.</li> <li>Für jeden Identity Provider werden die Schlüssel für die TLS-Verbindungen in der VAU erzeugt.</li> </ul> <p>Die Deregistrierung erfolgt ebenfalls bei der Superior Entity, bei welcher der Teilnehmer registriert wurde. Nach der Deregistrierung stellt die Superior Entity kein Subordinate Statement zum Teilnehmer mehr aus.</p> <p>Die Registrierung erfolgt durch Übergabe der Teilnehmerdaten an einer Registrierungsschnittstelle durch die Registrierungskomponente**.</p>
an Fachanwendung anmelden	Authorization Server der Fachanwendung	<p>Der Nutzer meldet sich an einer Fachanwendung an. Fachanwendungen können z.B. Anwendungen von Krankenkassen, TI-Anwendungen (wie bspw. E-Rezept, ePA) oder DiGAs sein. Die Anmeldung für alle Anwendungen erfolgt über genau den Identity Provider, bei dem die elektronische Identität des Nutzers hinterlegt ist. Ist der richtige Identity Provider nicht bekannt, so kann die Liste aller in der</p>

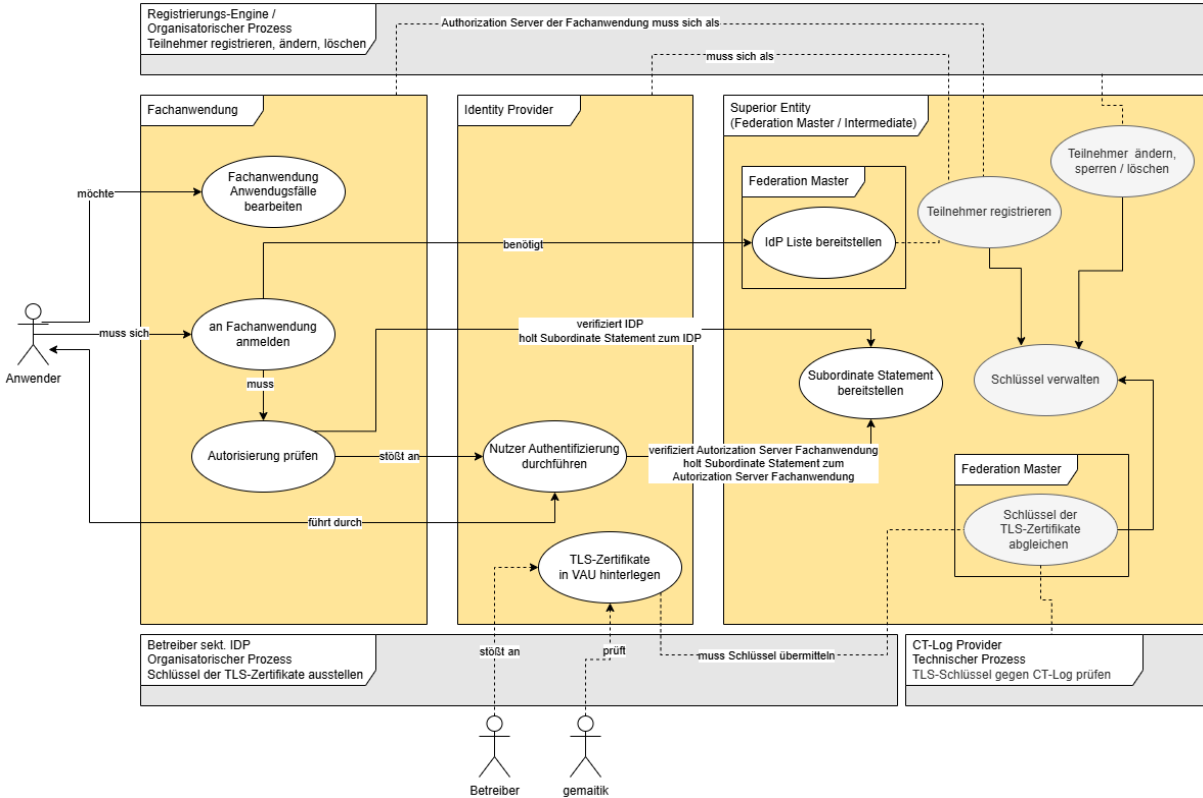
		TI-Föderation registrierten Identity Provider zur Ermittlung des richtigen Identity Provider von den Superior Entities der TI-Föderation abgefragt werden. Die Auswahl kann dann durch den Nutzer im Kontext der Anmeldung getroffen werden.
IDP-Liste bereitstellen	Federation Master	Zu allen in der TI-Föderation registrierten sektoralen Identity Providern von Krankenversicherungen werden die Informationen 'Organisationsname', 'Logo' und 'Zieladresse (URL)' ermittelt und als Liste bereitgestellt.
Autorisierung prüfen	Fachanwendung	Der Anwendungsfall <i>Autorisierung prüfen</i> 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.
Subordinate Statement bereitstellen	Federation Master / Intermediate	Superior Entities stellen zu jedem direkt registrierten Teilnehmer ein Subordinate Statement aus.
Nutzer authentifizieren	Identity Provider	Vor der eigentlichen Authentifizierung des Nutzers wird in diesem Anwendungsfall geprüft, ob der anfragende Fachanwendung Authorization Server Teil der TI-Föderation ist und dieser die Berechtigung hat, die geforderten Informationen zum Nutzer (Scope, Claims) einzuholen. Dazu wird das Subordinate Statement zum Fachdienst Authorization Server von dessen Superior Entity (Federation Master oder Intermediate) 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 und Metadaten verwalten	Federation Master / Intermediate	Superior Entities verwalten die Schlüssel und einige Metadaten der Teilnehmer. Superior Entities beglaubigten die bei ihnen direkt registrierten Teilnehmer sie gegenüber anderen Diensten und Form signierter Subordinate Statements. Das Einbringen der Daten neuer Teilnehmer bzw. das Löschen der Daten auszuschließender Teilnehmer erfolgt über organisatorische Prozesse (Teilnehmer registrieren, Teilnehmer löschen).

722 \* Die sektoralen IDPs der Krankenversicherungen sind bzw. werden direkt beim  
723 Federation Master (TI-Trust Anchor) registriert. Registrierungen von Fachdienst  
724 Authorization Server am Federation Master bleiben bestehen. Alle neu zu registrierenden  
725 ZETA-Authorization Server werden bei einem ZETA-AS Intermediate registriert. Dafür  
726 muss der ZETA-AS Intermediate beim Federation Master registriert sein. Weiter  
727 Intermediate z.B. zur Gruppierung aller DiGA-Authorization Server können je nach Bedarf  
728 implementiert werden.

729 \*\* Die Automatisierung der Registrierungskomponente erfolgt über ein eigens Produkt,  
730 die Registrierungs-Engine. Diese befindet sich aktuell in der Spezifikation. Bis zur  
731 Produktivsetzung der Registrierungs-Engine erfolgt die Registrierung von Teilnehmern  
732 durch einen manuellen Prozess, gesteuert über das ITSM.



733  
734

Abbildung 4 : Anwendungsfälle TI-Föderation



## 4.2 Aufbau und Kommunikation

Der Aufbau der und die Kommunikation in der TI-Föderation sind am Standard [OpenID Federation 1.1] und weiterer dort referenzierter Standards ausgerichtet. Die Ausrichtung an [OpenID Federation 1.1] liefert die Vorgaben und Rahmenbedingungen für den Aufbau des TI-Föderation Vertrauensraums. Die TI-Föderation weicht nur dort vom Standard ab, wo spezifische Anforderungen der gematik notwendig sind, entweder durch Verschärfung optionaler Anforderungen des Standards oder Erweiterungen bzw. Präzisierung von Anforderungen angepasst an die Rahmenbedingungen der gematik.

Jeder TI-Föderation Teilnehmer muss eine OpenID Federation Standard konforme Entity Configuration in Form eines Entity Statement öffentlich bereitstellen.

Federation Entities (Superior-Entity) sind Komponenten des Produkttyp "Federation Master". Dies ist einerseits der Federation Master selbst (Trust Anchor) und andererseits sind Intermediate (siehe Abbildung "Beispiel des Aufbau der TI-Föderation").

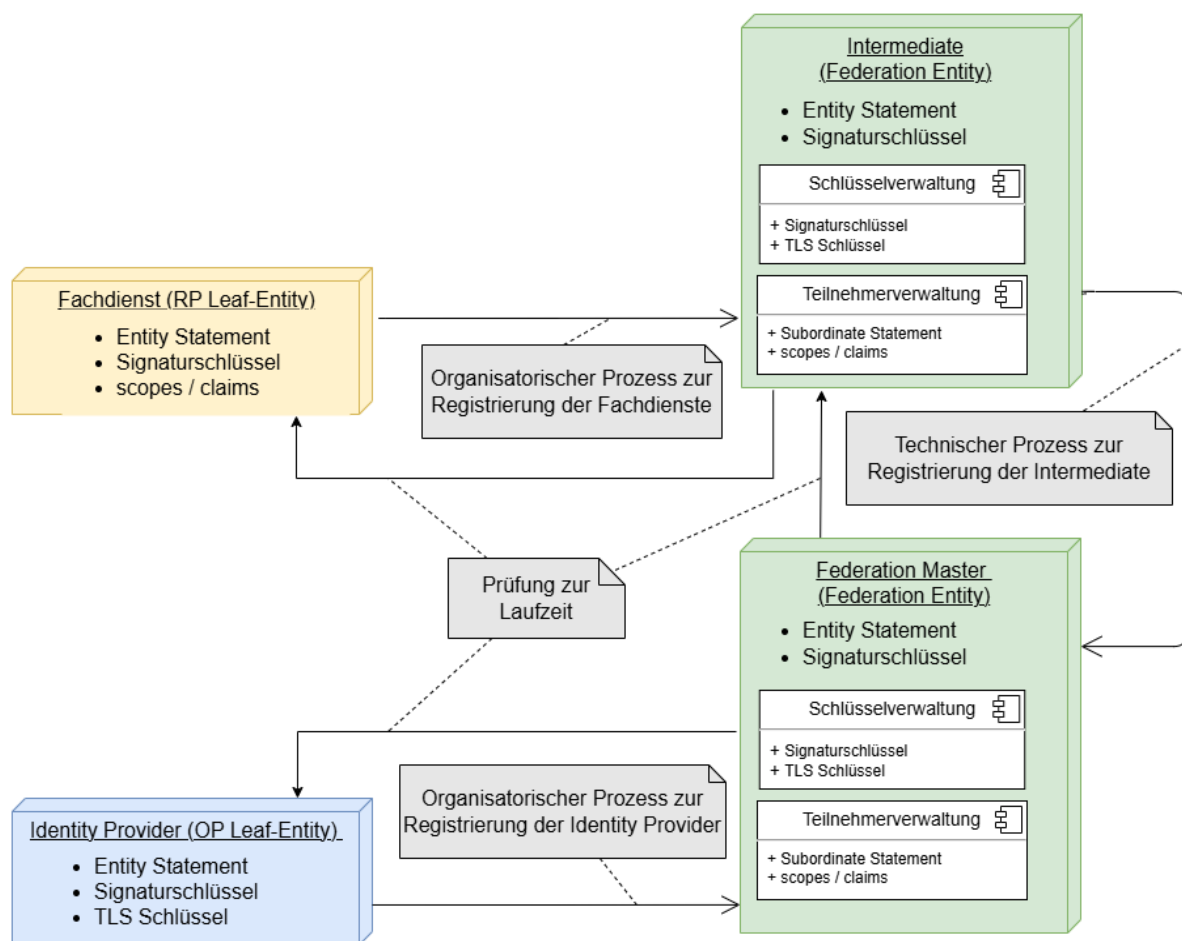
Die Identity Provider (Produkttyp "sektoraler IDP") der TI-Föderation stellen sicher, dass nur identifizierte Nutzer für anfragende Fachdienste authentifiziert werden. Ebenso wird sichergestellt, dass die Nutzer den Anwendungen Zugriff auf eine Teilmenge ihrer Daten gewähren (Consent).

Die in der TI-Föderation registrierten Fachdienste (Fachdienst Authorization Server) 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. Fachdienst Authorization Server sind Komponenten der jeweiligen Fachdienst-Produkttypen.

Der Vertrauensraum der TI-Föderation wird etabliert, indem sich jeder Teilnehmer (Leaf-Entity) über einen organisatorischen Prozess in der TI-Föderation registriert. Diese initiale Registrierung erfolgt unabhängig vom späteren Ablauf.

Intermediate als Komponenten des Produkttyp "Federation Master" müssen nicht über den organisatorischen Registrierungsprozess laufen. Die Registrierung im Vertrauensraum der TI-Föderation erfolgt technisch innerhalb des Produkttypes.

Zur Laufzeit kann jeder Teilnehmer prüfen, ob das System, mit dem er kommunizieren möchte ebenfalls registrierter TI-Föderationsteilnehmer ist und welche Eigenschaften das System innerhalb der TI-Föderation besitzt. Jeder Teilnehmer stellt die Vertraulichkeit einer Kommunikation sicher, indem die Vertrauensbeziehungen bis hoch zum Trust Anchor der TI-Föderation validiert werden (Trust Chain).



**Abbildung 5 : Komponenten der TI-Föderation im Überblick**

Im Prozess der Authentifizierung eines Nutzers für eine Anwendung ist der Federation Master als Vertrauensstelle eingebunden. Die Voraussetzung für die Kommunikation zwischen Fachdienst Authorization Server und sektoralen Identity Providern ist deren Registrierung im Vertrauensbereich der TI- Föderation.

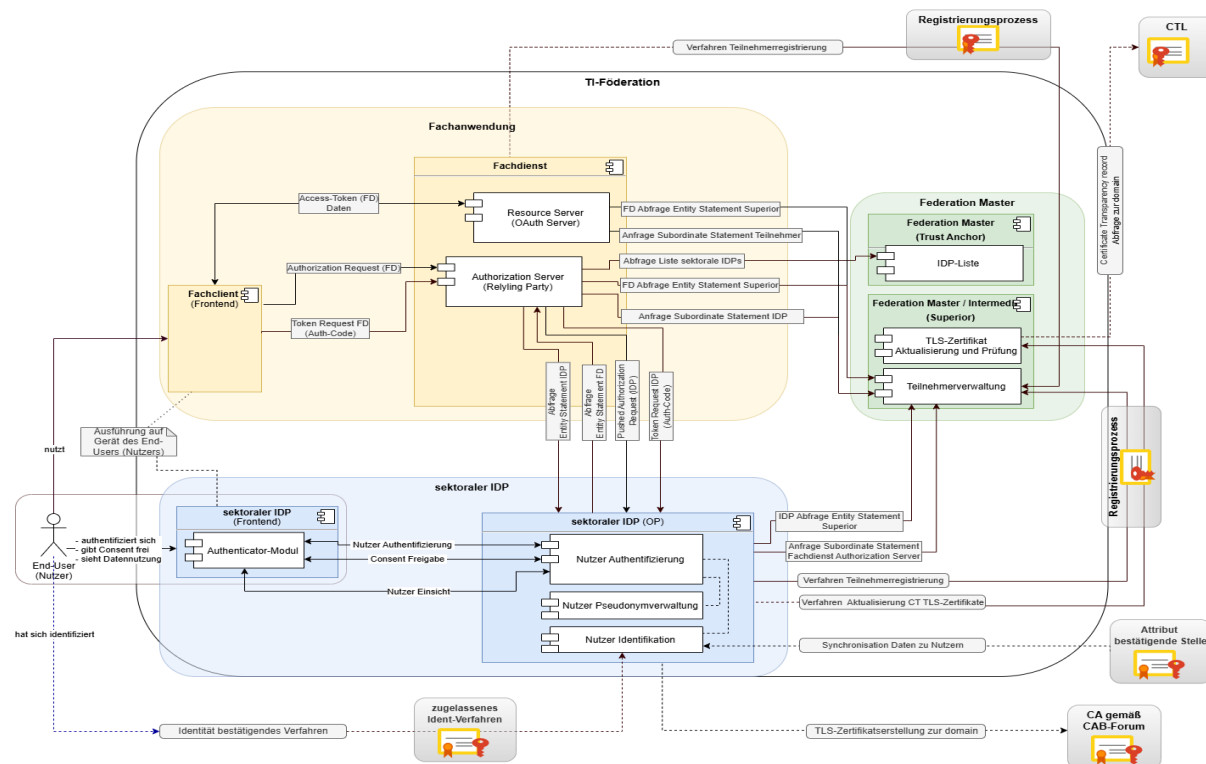
Voraussetzungen für die Prüfung der beteiligten Komponenten im Kontext eines Nutzungsflows:

- Die aktuellen Signaturschlüssel der beteiligten sektoralen Identity Provider und Fachdienste Authorization Server wurden über den Registrierungsprozess bei der Superior Entity hinterlegt (Federation Master oder Intermediate) bei welcher der Teilnehmer registriert ist.
- Jeder Teilnehmer (Leaf-Entity) hat als Ergebnis der Registrierung den öffentlichen Schlüssel, mit dem der Federation Master (Trust Anchor) sein Entity Statement signiert, zugestellt bekommen.
- Die Entity Statements der beteiligten sektoralen Identity Provider und Fachdienste Authorization Server entsprechen den Vorgaben [OpenID 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 TI-Föderation.

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

Die Kommunikation zwischen dem Fachdienst Authorization Server (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 6 : Komponenten der TI-Föderation mit Schnittstellen**

Erläuterungen zur obigen Abbildung:

Die jeweiligen Teilnehmer Typen (entity\_type) sind farblich unterscheidlich dargestellt.

Die Authorization Server der Fachdienste (gelb), welche eine Nutzerauthentifizierung benötigen sind in der TI-Föderation Relying Parties (entity\_type = openid\_relying\_party). Der Resource Server der Fachanwendung kann ebenfalls im Vertrauensraum der TI-Föderation (entity\_type = oauth\_resource) registriert werden.

Blau dargestellt sind die sektoralen IDP (entity\_type = openid\_provider). Diese halten die Identitätsinformationen der Nutzer und führen den Prozess der Nutzerauthentifizierung durch.

Der Federation Master (grün) enthält Komponenten (entity\_type = federation\_entity) mit Funktionen zur Prüfung der Vertrauenskette eines Teilnehmers bis hin zum Vertrauensanker, sowie Funktionen zur Beauskunftung zu Teilnehmern der TI-Föderation und Abbildung von Regeln (Policies) und Vertrauensnachweisen (Trust Marks).

Die Schnittstellen zwischen den Komponenten der TI-Föderation sind durchgezogene Linien während die gestrichelt dargestellten Schnittstellen organisatorische Prozesse und Verfahren mit Komponenten außerhalb der TI-Föderation visualisieren. Die Schnittstellen zwischen der Registrierungs-Engine und dem Federation Master sind jedoch Teil der Schnittstellenspezifikation.

Im Vertrauensraum der TI-Föderation müssen beteiligte Teilnehmer sicherstellen, dass der jeweilige Kommunikationspartner ebenfalls ein Mitglied der TI-Föderation ist. Jeder

Teilnehmer stellt dazu ein selbst signiertes Entity Statement bereit. Zur Herstellung der Vertrauensbeziehung laden die Teilnehmer jeweils das Entity Statement des Kommunikationspartners von dessen öffentlich erreichbaren /.well-known/openid-federation Schnittstelle. Von der Superior-Entity (Federation Master oder Intermediate), dem der Kommunikationspartner direkt untergeordnet ist, lädt der anfragende Teilnehmer ein Subordinate Statement mit Auskunft zu Eigenschaften des Kommunikationspartners in der TI-Föderation. Jeder Teilnehmer prüft die Vertrauensstellung vom Kommunikationsteilnehmern über die Validierung der Trust-Chain vom Entity Statement des Teilnehmers bis zum TI-Trust Anchor (Federation Master).

### 4.3 Akteure und Rollen

Im Systemkontext der TI-Föderation interagieren verschiedene Akteure (Nutzer und aktive Komponenten) in unterschiedlichen OAuth2-Rollen gemäß [RFC6749#section-1.1] und OpenID-Connect-Rollen gemäß [OpenID Connect Core 1.0] und [OpenID Federation 1.1].

Als sektoraler IDP wird ein Dienst bezeichnet, welcher die Nutzerauthentifizierung durchführt. Nach erfolgreicher Nutzerauthentisierung stellt der sektorale IDP Identitätsinformationen zum Nutzer bereit. Die Identitätsinformationen werden von den Fachdiensten zur Durchführung einer Nutzerautorisierung verwendet, also zur Feststellung, auf welche Fachdaten und -prozesse des Fachdienstes dem Nutzer Zugriff gewährt wird. Die bereitgestellten Identitätsinformationen sind spezifisch für die unterschiedlichen Gruppen von Nutzern bzw. Sektoren innerhalb der TI des Gesundheitswesens. Einen Sektor stellen insbesondere die Krankenkassen mit den Versicherten als Nutzer dar. Es können allerdings auch andere Personengruppen wie z. B. Ärzte oder Pflegeinstitutionen über sektorale IDP angebunden werden.

Die Abläufe zur Nutzerauthentifizierung für einen Fachdienst sowie der Herausgabe der Identitätsinformationen durch den sektoralen IDP sind als der innere und der äußere Flow im Kapitel "Interaktionen" erläutert.

**Tabelle 3 : Akteure und Rollen**

Akteur	Rolle "OAuth2"	Rolle "OIDC"	Rolle "OpenID Federation"
Nutzer (z. B. Versicherte)	Resource Owner	Resource Owner	
Fachdienst - Authorization Server	Authorization Server	OpenID Relying Party (RP)	Teilnehmer als OpenID Relying Party (openid_relying_party) der TI-Föderation
Fachdienst - Fachliche Services (Fachdaten und -Prozesse)	Protected Resource / OAuth-Resource (RS)	-	Kann auch als Teilnehmer (oauth_server) in der TI-Föderation registriert werden
Fachdienst - Anwendungs-Frontend (Web/App)	OAuth-Client, Nutzerschnittstelle als App	-	Kann auch als Teilnehmer (oauth_client) in der TI-Föderation registriert werden
sektoraler IDP	-	OpenID Provider (OP)	Teilnehmer als OpenID Provider (OP) der TI-Föderation

Authenticator-Modul des sektoralen IDP	-	Frontend des sektoralen IDP (OP)	-
Federation Master	-	-	Teilnehmer der TI-Föderation (Federation Entity) als Vertrauensanker (Trust Anchor) für alle Teilnehmer (RP, OP, RS, Intermediate) der TI-Föderation
Intermediate	-	-	Teilnehmer der TI-Föderation (Federation Entity), bei dem eine Gruppe anderer Teilnehmer mit gleichen Eigenschaften (technisch oder organisatorisch) registriert sind.
Attributbestätigende Stelle	-	-	kein Teilnehmer der Föderation
Registrierungs-Engine (Regine)	-	-	System, über welches sich Teilnehmer in der TI-Föderation registrieren, ihre Registrierungsdaten ändern oder ihre Registrierung löschen können.

#### Nutzer (Rolle: Resource Owner)

Der Resource Owner ist eine natürliche Person, welcher auf die beim Fachdienst (Resource Server) für ihn bereitgestellten Daten und Prozesse (Protected Resource) zugreift.

Der Resource Owner verfügt über die folgenden Komponenten:

- Endgerät des Nutzers,
- App mit Authenticator-Modul auf dem Endgerät,
- Anwendungsfrontend des Fachdienstes auf dem gleichen oder einem anderen Endgerät.

#### Fachdienst (Rolle: Authorization Server)

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 Anwendungsfrontends auf die Ressourcen des Fachdienstes. Der Authorization Server des Fachdienstes stellt eigene Access Token und Refresh Token für das Anwendungsfrontend aus.

#### Fachdienst (Rolle: Resource Server)

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 der Zugriffsberechtigung des Clients im Auftrag des Resource Owner.

**Anwendungsfrontend (Rolle: OAuth-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, auf einem Desktop-PC oder einem mobilen Gerät (z. B. Smartphone) oder als App auf einem mobilen Gerät ausgeführt werden. Finden für die Anwendung relevante Prozesse (Businesslogik) in einem Hintergrundsystem statt, so ist die Backend-Komponente, welche die UI für die Visualisierung 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 über den Nutzer (Scopes bzw. Claims), die für den Authorization Server der Fachanwendung zur Zugriffsentscheidung über den vom Resource Owner erlaubten Anwendungsbereich (Scope) benötigt werden.

Weitere Akteure im Kontext des sektoralen IDP sind:

**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 Kostenträger) werden innerhalb der TI über die Krankenversicherungsnummer des Versicherten und die Telematik-ID eines Leistungserbringers bzw. einer medizinischen Institution oder Organisation des Gesundheitswesens repräsentiert.

**Federation Master (Rolle: Trust Anchor, Superior)**

Der Federation Master ist eine zentrale Komponente und ein eigener Produkttyp [gemSpec\_IDP\_FedMaster] in der TI-Föderation. Der Federation Master bietet die Anwendungsfälle:

- Teilnehmer registrieren, deregistrieren und Teilnehmerdaten ändern
- Liste der direkt registrierten Teilnehmer bereitstellen,
- Liste der registrierten sektoralen IDPs IDP-Liste bereitstellen,
- Entity Statement bereitstellen,
- Subordinate Statements zu direkt registrierten Teilnehmern bereitstellen
- Trust-Marks zu direkt registrierten Teilnehmern bereitstellen
- Schlüssel der TLS-Zertifikate abgleichen,
- Schlüssel von direkt registrierten Teilnehmern verwalten.

Alle Teilnehmer der Föderation müssen bei einem Superior registriert sein. Teilnehmer der Föderation sind in diesem Kontext alle Fachdienste Authorization Server und sektoralen IDP (Leaf-Entities). Die Registrierung erfolgt durch Prozesse der Registrierungs-Engine und Schnittstellen am Federation Master\*. Der Federation Master verwaltet die öffentlichen Schlüssel aller direkt registrierten Teilnehmer und zusätzlich für direkt registrierte Fachdienste Authorization Server die jeweils zugelassenen



Scopes und Claims. Er stellt auf Anfrage Teilnehmerbestätigungen in Form von Subordinate Statements für direkt bei ihm registrierte Teilnehmer der TI-Föderation aus. Der Federation Master agiert als Trust Anchor im Sinne der [OpenID Federation 1.1] Spezifikation. Der Federation Master ist bei keiner weiteren Superoir Entity registriert und bildet somit das Ende einer Trust Chain gemäß [OpenID Federation 1.1] Die Vertrauenskette aller Teilnehmer der TI-Föderation muss sich auf den Federation Master zurückführen lassen [[OpenID Federation 1.1](#)] ("Trust Chain"). Der Federation Master stellt zusätzlich eine Schnittstelle bereit, über die eine Liste aller in der TI-Föderation registrierten sektoralen IDP abgerufen werden kann.

*\* Bis zur Produktivsetzung der Registrierungs-Engine erfolgt die Teilnehmerregistrierung über einen organisatorischen Prozess, der vom Anbieter des Produkttyp Federation Master bereitgestellt wird.*

### **Intermediate (Rolle: Superior)**

Die Eigenschaften eines Intermediate der TI-Föderation sind ebenfalls im Produkttyp [gemSpec\_IDP\_FedMaster] definiert. Ein Intermediate ist der Knotenpunkt für eine Teilstruktur der TI-Föderation und wie der Federation Master ebenfalls vom Typ Federation Entity. Alle Teilnehmer mit bestimmten Eigenschaften können bei einem entsprechenden Intermediate registriert sein. Ein Intermediate selbst ist ebenfalls ein Teilnehmer der TI-Föderation und muss demnach ebenfalls selbst bei einem anderen Intermediate oder beim Federation Master registriert sein. Die Registrierung erfolgt technisch innerhalb des Produkttyp "Federation Master". Wie der Federation Master, verwaltet ein Intermediate die öffentlichen Schlüssel aller direkt bei ihm registrierten Teilnehmer und zusätzlich für registrierte Fachdienst Authorization Server, die jeweils zugelassenen Scopes und Claims. Er stellt auf Anfrage Teilnehmerbestätigungen in Form von Subordinate Statements für direkt bei ihm registrierte Teilnehmer der TI-Föderation aus. Intermediates der TI-Föderation unterstützen die Anwendungsfälle:

- Teilnehmer registrieren, deregistrieren und Teilnehmerdaten ändern
- Liste der direkt registrierten Teilnehmer bereitstellen,
- Entity Statement bereitstellen,
- Subordinate Statements zu direkt registrierten Teilnehmern bereitstellen
- Trust-Marks zu direkt registrierten Teilnehmern bereitstellen
- Schlüssel von direkt registrierten Teilnehmern verwalten.

### **Registrierungskomponente:**

Die Registrierungskomponente übernimmt die Aufgabe, Registrierungsanträge der Teilnehmer der TI-Föderation entgegen zunehmen, zu validieren, mit anderen Systemen zu synchronisieren. Die Registrierungskomponente hat Schnittstellen zur TI-Föderation, zum Data Warehouse (DWH) der gematik, zum TI-ITSM der gematik und dem gematik myServices-Portal. Die TI-Föderation stellt Schnittstellen bereit, über die Registrierungskomponente Teilnehmer Konfigurationen (Entity Configuration) prüfen kann. Des weiteren stellt die TI-Föderation Schnittstellen für die Neuregistrierung, Registrierungsänderungen und Deregistrierung für Teilnehmer der TI-Föderation zur Verfügung. Die Registrierungskomponente bedient das Data Warehouse (DWH) der gematik mit den Teilnehmerdaten der TI-Föderation für Business Intelligence (BI), Berichterstellung und Analysen zur Unterstützung der Betriebsführung der gematik.

Nach erfolgreicher Prüfung von Teilnehmeranträgen erfolgt die Aktualisierungs des Vertrauensraum der TI-Föderation über Schnittstellen am Federation Master.

## **4.4 Schnittstellen**

968  
969**Tabelle 4 : Schnittstellen zwischen den Teilnehmern und Komponenten der TI-Föderation**

Schnittstelle	Komponente/System	fachliche Schnittstellenbeschreibung
Abfrage Liste Krankenkassen	<ul style="list-style-type: none"> <li>Fachdienst-Client</li> <li>Fachdienst Authorization Server (RP)</li> </ul>	Ist die Krankenkasse des Versicherten im Fachdienst-Client nicht bekannt, so stellt der Fachdienst-Client einen Request an den Fachdienst Authorization Server zum Laden der Liste aller Krankenkassen.
Abfrage Liste sektorale IDPs	<ul style="list-style-type: none"> <li>Fachdienst Authorization Server (RP)</li> <li>Federation Master</li> </ul>	Der Fachdienst Authorization Server stellt einen Request an den Federation Master zum Abruf der Liste aller in der TI-Föderation registrierten sektoralen IDP mit den Metainformationen zur jeweiligen Krankenkasse.
Authorization Request (FD)	<ul style="list-style-type: none"> <li>Fachdienst-Client</li> <li>Fachdienst Authorization Server (RP)</li> </ul>	Der Prozess der Nutzerauthentifizierung startet mit einem Authorization Request des Fachdienst-Client an den Fachdienst Authorization Server.
Anfrage Entity Statement IDP	<ul style="list-style-type: none"> <li>Fachdienst Authorization Server (RP)</li> <li>sektoraler IDP</li> </ul>	Zur Abfrage der Entity Configuration des sektoralen IDP stellt der Fachdienst Authorization Server einen Request an die ./well-known/openid-federation Schnittstelle des sektoralen IDP.
FD Abfrage Entity Statement Superior	<ul style="list-style-type: none"> <li>Fachdienst Authorization Server (RP)</li> <li>Superior-Entity(s)</li> </ul>	Im Rahmen der Validierung des Entity Statement des sektoralen IDP stellt der Fachdienst Authorization Server einen Request an die ./well-known/openid-federation Schnittstelle der Superior-Entity, bei welcher der sektorale IDP registriert ist und in Folge bei allen weiteren Superior-Entity bis zum Trust-Anchor (Federation Master). Die Information, welche URL aufzurufen ist bekommt der Fachdienst Authorization Server aus dem claim "authority_hints" der jeweiligen Entity Statements.
Anfrage Subordinate	<ul style="list-style-type: none"> <li>Fachdienst Authorization Server</li> </ul>	Zur Verifikation der



Statement IDP	(RP) <ul style="list-style-type: none"> <li>• Superior-Entity</li> </ul>	Vertrauensbeziehung zum angefragten sektorale IDP stellt der Fachdienst Authorization Server einen Request an die Superior-Entity, bei welcher der sektorale IDP als Teilnehmer der TI-Födeartion registriert ist (Federation Master oder Intermediate).
Pushed Authorization Request (IDP)	<ul style="list-style-type: none"> <li>• Fachdienst Authorization Server (RP)</li> <li>• sektoraler IDP</li> </ul>	Zur Ermittlung der Informationen zum Nutzer stellt der Fachdienst Authorization Server einen Pushed Authorization Request an den sektoralen IDP.
Abfrage Entity Statement FD	<ul style="list-style-type: none"> <li>• sektoraler IDP</li> <li>• Fachdienst Authorization Server (RP)</li> </ul>	Zur Ermittlung der Entity Configuration des Fachdienst Authorization Server stellt der sektorale IDP einen Request an an die ./well-known/openid-federation Schnittstelle des Fachdienst Authorization Server.
IDP Abfrage Entity Statement Superior	<ul style="list-style-type: none"> <li>• sektoraler IDP</li> <li>• Superior-Entity</li> </ul>	Im Rahmen der Validierung des Entity Statement des Fachdienst Authorization Server stellt der sektoralen IDP einen Request an die ./well-known/openid-federation Schnittstelle der Superior-Entity, bei welcher der Fachdienst Authorization Server registriert ist und in Folge bei allen weiteren Superior-Entity bis zum Trust-Anchor (Federation Master). Die Information, welche URL aufzurufen ist bekommt der sektoralen IDP aus dem claim "authority_hints" der jeweiligen Entity Statements.
Anfrage Subordinate Statement Fachdienst Authorization Server	<ul style="list-style-type: none"> <li>• sektoraler IDP</li> <li>• Superior-Entity</li> </ul>	Zur Verifikation der Vertrauensbeziehung zum anfragenden Fachdienst Authorization Server stellt der sektorale IDP einen Request an die Superior-Entity, bei welcher der Fachdienst Authorization Server als Teilnehmer der TI-Födeartion registriert ist (Federation Master oder Intermediate).
Token Request IDP (Auth-Code)	<ul style="list-style-type: none"> <li>• Fachdienst Authorization Server (RP)</li> </ul>	Der Fachdienst Authorization Server stellt einen Token

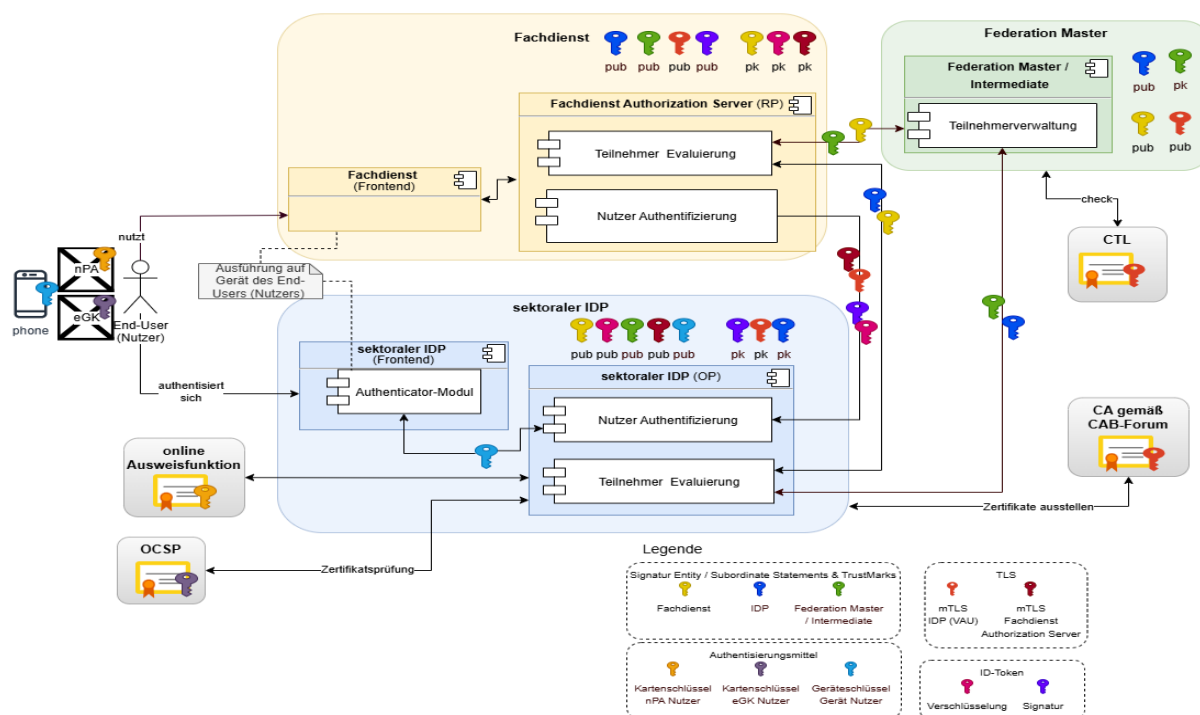
	<ul style="list-style-type: none"><li>• sektoraler IDP</li></ul>	Request an den sektoralen IDP und erhält im Austausch zu einem Authentication Code ein Access Token und ein ID Token.
--	--	---

Token Request FD (Auth-Code)	<ul style="list-style-type: none"> <li>Fachdienst-Client</li> <li>Fachdienst Authorization Server (RP)</li> </ul>	Wenn die für die Client-Authentifizierung OAuth mit Authorization-Code Flow eingesetzt wird, stellt der Fachdienst-Client einen Token Request an den Fachdienst Authorization Server und erhält im Austausch zu einem Authentication Code ein Access Token.
Interne Schnittstellen zwischen den Komponenten des sektoralen IDP		
Nutzer Authentifizierung	<ul style="list-style-type: none"> <li>sektoraler IDP</li> <li>Authenticator-Modul</li> </ul>	Der sektorale IDP und sein Authenticator-Modul führen die Abfragen zur Nutzerauthentifizierung durch. Die Schnittstelle ist Hersteller spezifisch.
Consent Freigabe	<ul style="list-style-type: none"> <li>sektoraler IDP</li> <li>Authenticator-Modul</li> </ul>	Der sektorale IDP und sein Authenticator-Modul führen die Abfragen zur Freigabe der Datennutzung durch den Versicherten durch. Die Schnittstelle ist Hersteller spezifisch.
Nutzer Einsicht	<ul style="list-style-type: none"> <li>sektoraler IDP</li> <li>Authenticator-Modul</li> </ul>	Der sektorale IDP und sein Authenticator-Modul führen die Abfragen zur Einsicht durchgeführter Authentifizierungsvorgänge durch den Versicherten durch. Die Schnittstelle ist Hersteller spezifisch.
Weitere Schnittstellen des sektoralen IDP sowie der Fachdienste		
Verfahren Teilnehmerregistrierung	<ul style="list-style-type: none"> <li>Registrierungskomponente</li> <li>Superior-Entity <ul style="list-style-type: none"> <li>Federation Master</li> <li>Intermediate</li> </ul> </li> </ul>	Schnittstellen zur Registrierung und Deregistrierung von Teilnehmern der TI-Föderation sowie zur Prüfung und Aktualisierung von Teilnehmerdaten über die Registrierungskomponente.
Certificate Transparency record Abfrage zur domain	<ul style="list-style-type: none"> <li>Federation Master</li> <li>Certificate Transparency Log</li> </ul>	Der Federation Master ruft über die Schnittstelle eines Anbieters das CT-Log zur Prüfung der TLS-Schlüssel der sektoralen IDPs ab. Die Schnittstelle ist abhängig vom eingesetzten Produkt (CT-Log Anbieter).

Verfahren Aktualisierung CT TLS-Zertifikate	<ul style="list-style-type: none"> <li>• Registrierungskomponente</li> <li>• Federation Master</li> </ul>	Organisatorische Schnittstelle zur Schlüsselregistrierung der im sektoralen IDP verwendeten TLS-Zertifikate beim Federation Master über die Registrierungskomponente
Synchronisation Daten zu Nutzern	<ul style="list-style-type: none"> <li>• Attribut bestätigende Stelle</li> <li>• sektoraler IDP</li> </ul>	Schnittstellen zur Registrierung und Deregistrierung von Teilnehmern der TI-Föderation sowie zur Prüfung und Aktualisierung von Teilnehmerdaten.
Access-Token (FD) - Daten	<ul style="list-style-type: none"> <li>• Fachdienst-Client</li> <li>• Fachdienst Resource Server</li> </ul>	Die Ausprägung der Schnittstelle zwischen Fachdienst-Client und Fachdienst Resource Server ist Fachdienst spezifisch. Wie in zur Authentifizierung OAuth eingesetzt, so muss bei der Kommunikation zwischen Fachdienst-Client und Fachdienst Resource Server i.d.R. ein vom Fachdienst Authorization Server ausgestelltes Access-Token mitgegeben werden.

## 4.5 Schlüsselmanagement

In der Kommunikation zwischen den Teilnehmern der TI-Föderation im Ablauf einer Nutzerauthentifizierung kommen unterschiedliche Verschlüsselungsmechanismen und Schlüssel zum Einsatz



**Abbildung 7 : Schlüsselmanagement für die Nutzerauthentifizierung in der TI-Föderation**

**Tabelle 5 : Schlüsselmanagement**

Zweck	Schlüssel	Bedeutung
Authentisierungsmittel	Kartenschlüssel nPA	Schlüssel auf dem Personalausweis des Nutzers für den Identifikationsprozess oder die Authentifizierung des Nutzers über die online Ausweisfunktion.
	Kartenschlüssel eGK	Schlüssel auf der eGK des Nutzers für den Identifikationsprozess oder die Authentifizierung des Nutzers über eGK mit PIN Eingabe
	Schlüssel auf dem Gerät des Nutzers	Gerätebindung des Gerät des Nutzers an den sekt. IDP zur Authentifizierung über das Gerät mit System-PIN, App-PIN oder Biometrie.
Signatur	Signaturschlüssel Fachdienst Authorization Server	Vom Fachdienst Authorization Server erstelltes asym. Schlüsselpaar. Der Fachdienst Authorization Server signiert mit diesem Schlüssel ausschließlich sein Entity Statement (Federation Entity signing key). Der öffentliche Teil des initialen Schlüssels wird im Registrierungsprozesse beim der federation_entity hinterlegt, unter welcher der Fachdienst Authorization Server registriert wird. Im Subordinate Statement der federation_entity zum Fachdienst Authorization Server wird der

		<p>Schlüssel an einen anfragenden Teilnehmer ausgeliefert.</p> <p>Das Entity Statement des Fachdienst Authorization Server übermittelt im claim "jwks" im Entity Statement ebenfalls den öffentlichen Teil des Schlüsselpaares.</p>
	Signaturschlüssel sekt. IDP	<p>Vom sekt. IDP erstelltes asym. Schlüsselpaar. Der sekt. IDP signiert mit diesem Schlüssel ausschließlich sein Entity Statement (Federation Entity signing key). Der öffentliche Teil des initialen Schlüssels wird im Registrierungsprozesse beim FederationMaster (der federation_entity) hinterlegt, wo der sekt. IDP registriert wird. Im Subordinate Statement des Federation Master zu m sekt. IDP wird der Schlüssel an einen anfragenden Teilnehmer ausgeliefert.</p> <p>Das Entity Statement des sekt. IDP übermittelt im claim "jwks" im Entity Statement ebenfalls den öffentlichen Teil des Schlüsselpaares.</p>
	Signaturschlüssel Federation Master / Intermediate	<p>Von der federation_entity (Federation Master oder Intermediate) erstelltes asym. Schlüsselpaar. Federation Master oder Intermediate signieren mit diesem Schlüssel (Federation Entity signing key) ihr Entity Statement, Subordinate Statements zu Teilnehmern und TrustMarks. Der öffentliche Teil des initialen Schlüssels wird im Falle eines Intermediate im Registrierungsprozess beim der federation_entity hinterlegt, unter welcher der Intermediate registriert wird. Im Subordinate Statement der federation_entity zu dem Teilnehmer wird der Schlüssel an einen anfragenden Teilnehmer ausgeliefert.</p> <p>Der Federation Master als TrustAnchor stellt den öffentlichen Teil seines Schlüssels über Wege außerhalb der TI-Föderationsprozesse zur Verfügung.</p> <p>Das Entity Statement von Federation Master oder Intermediate übermittelt im claim "jwks" im Entity Statement ebenfalls den öffentlichen Teil des Schlüsselpaares.</p>
ID-Token	Signaturschlüssel	<p>Vom sekt. IDP erstelltes asym. Schlüsselpaar. Der sekt. IDP signiert mit diesem Schlüssel das ausgestellte ID-Token. Der Schlüssel muss ungleich des Federation Entity signing key sein, mit dem der sekt. IDP sein Entity Statement signiert.</p> <p>Den öffentlichen Teil des Schlüssels veröffentlicht der sekt. IDP im Metadatenblock "openid_provider" in seinem Entity Statement entweder in</p>

		<p>einem claim "jwks" oder in einem Schlüsselset, welches unter der im claim "signed_jwks_uri" gesetzten URL abrufbar ist.</p>
	Verschlüsselungsschlüssel	<p>Vom Fachdienst Authorization Server erstelltes asym. Schlüsselpaar. Der sekt. IDP verschlüsselt mit dem öffentlichen Schlüssel das ausgestellte ID-Token, der Fachdienst Authorization Server als Empfänger des ID-Token kann diesen mit seinem privaten Schlüssel entschlüsseln. Den öffentlichen Teil des Schlüssels veröffentlicht der Fachdienst Authorization Server im Metadatenblock "openid_relying_party" in seinem Entity Statement entweder in einem claim "jwks" oder in einem Schlüsselset, welches unter der im claim "signed_jwks_uri" gesetzten URL abrufbar ist.</p>
TLS	TLS-Schlüssel sekt. IDP	<p>Der TLS-Schlüssel für den sekt. IDP wird vom sekt. IDP erzeugt und über einen organisatorischen Prozess dem Federation Master übermittelt. Der Federation Master führt regelmäßig eine Prüfung der ihm bekannten TLS-Schlüssel der sekt. IDP gegen ein Certificate Transparency (CT) Log durch. Den öffentlichen Teil des Schlüssels veröffentlicht der sekt. IDP im Metadatenblock "openid_provider" in seinem Entity Statement entweder in einem claim "jwks" oder in einem Schlüsselset, welches unter der im claim "signed_jwks_uri" gesetzten URL abrufbar ist.</p>
	TLS-Schlüssel des Fachdienst Authorization Server	<p>Der Fachdienst Authorization Server veröffentlicht seinen TLS-Schlüssel im Metadatenblock "openid_relying_party" in seinem Entity Statement entweder in einem claim "jwks" oder in einem Schlüsselset, welches unter der im claim "signed_jwks_uri" gesetzten URL abrufbar ist.</p> <p>Der Fachdienst Authorization Server kann self-signed certificate verwenden.</p>

Teilnehmer können im Metadatenblock weitere Schlüssel veröffentlichen. Für das Key-rollover werden ebenfalls die claims "jwks" im common-block des Entity Statement - für den Federation Entity signing key - und "jwks" oder "signed\_jwks\_uri" im jeweiligen Metadatenblock des Entity Statements für alle anderen Keys verwendet.

---

## 5 Abläufe & Interaktionen

---

### 5.1 Kurzbeschreibung

Der gesamte Authentifizierungsprozess basiert aus Gründen der Entkoppelung zwischen den Authentifizierungsmethoden und Token-Formaten der sektoralen IDP und des Fachdienstes aus zwei ineinander geschachtelten Abläufen. Zum einen den äußeren Flow zwischen Anwendungsfrontend und Authorization Server der Fachanwendung. Dieser Ablauf ist anwendungsspezifisch, sollte aber ein OAuth2-Flow mit Authorization Code-Flow sein. Der innere Flow ist ein OpenID-Connect (OIDC-Flow) zwischen registrierten Teilnehmern der TI-Föderation. Der inner Flow ist ein OAuth2 Authorization Code-Flow.

Im äußeren Flow wendet sich das Anwendungsfrontend als Client initial an den Authorization Server des Fachdienstes und signalisiert diesem über einen zusätzlichen Parameter, hier benannt mit `idp_iss`, den zur Authentifizierung zu verwendenden sektoralen IDP. Der innere Flow beginnt mit einem Pushed Authorization Request und endet mit der Herausgabe eines ID-Token vom sektoralen IDP an den Authorization Server des Fachdienstes.

Der Authorization Server des Fachdienstes tritt bzgl. des inneren Flow als Client auf. Die erste Anfrage an den sektoralen IDP geht am PAR-Endpunkt [[RFC9126#section-2](#)] ein. Der Authorization Server des Fachdienstes übermittelt am Endpunkt den Authorization Request zur Authentifizierung des Nutzers sowie zur Bestätigung von Scope und Claims der anfragenden Anwendung. Zusätzlich wird eine `code_challenge` eingereicht.

Der Scope und die Claims der angefragten Nutzdaten, die ein Fachdienst beim sektoralen IDP anfragen darf, sind im Entity Statement des Fachdienst Authorization Server hinterlegt. Dieses ist dem sektoralen IDP bekannt.

Im Ablauf des inneren (OIDC) Flow wird der Nutzer aufgefordert, sich unter Verwendung des Authenticator-Moduls des sektoralen IDP, zu authentisieren. Dies erfolgt über eine Schnittstelle zwischen dem Authenticator-Modul und Authorization-Endpunkt des sektoralen IDP.

Nach Consent-Freigabe durch den Nutzer und erfolgreicher Authentifizierung erstellt der sektorale IDP einen Authorization Code. Dieser wird an den Authorization Server des Fachdienstes übermittelt, welcher ihn am Token-Endpunkt [[RFC6749#section-3.2](#)] des sektoralen IDP einreicht. der sektorale IDP überprüft den Authorization Code und stellt bei positiver Validierung einen ID-Token aus.

Ist der äußere Flow ebenfalls ein OAuth2-Flows vom Typ `grant_type=authorization_code` erstellt der Authorization Server des Fachdienstes einen eigenen Authorization Code, der an das Anwendungsfrontend zurückgegeben wird. Der äußere Flow endet mit der Herausgabe eines Access-Token an das Anwendungsfrontend. Das Anwendungsfrontend verwendet das Access-Token für die anwendungsspezifischen Aufrufe bei eigentlichen Fachdienst.

In diesem Kapitel werden die Abläufe für App2App Kommunikation, Web-App Kommunikation und Kommunikation unter Beteiligung von zwei Geräten beschrieben.

Vorbereitende Maßnahmen:

- Die sektoralen IDPs haben bei der Registrierung am Federation Master in der TI-Föderation den öffentlichen Schlüssel ihres "federation entity signing key" hinterlegt und den öffentlichen Schlüssel des "federation entity signing key" des Trust Anchors der TI-Föderation (Federation Master) zur Validierung der Trust Chain bekommen.



- Der Fachdienst Authorization Server hat bei der Registrierung an einem Superior (Federation Master oder Intermediate) der TI-Föderation den öffentlichen Schlüssel seines "federation entity signing key" hinterlegt und den öffentlichen Schlüssel des "federation entity signing key" des Trust Anchors der TI-Föderation (Federation Master) zur Validierung der Trust Chain bekommen.
- Der Fachdienst Authorization Server hat bei der Registrierung an einer Superior-Entity (Federation Master oder Intermediate) die Scopes hinterlegt, welche er für die Autorisierung eines Nutzers zwingend benötigt.

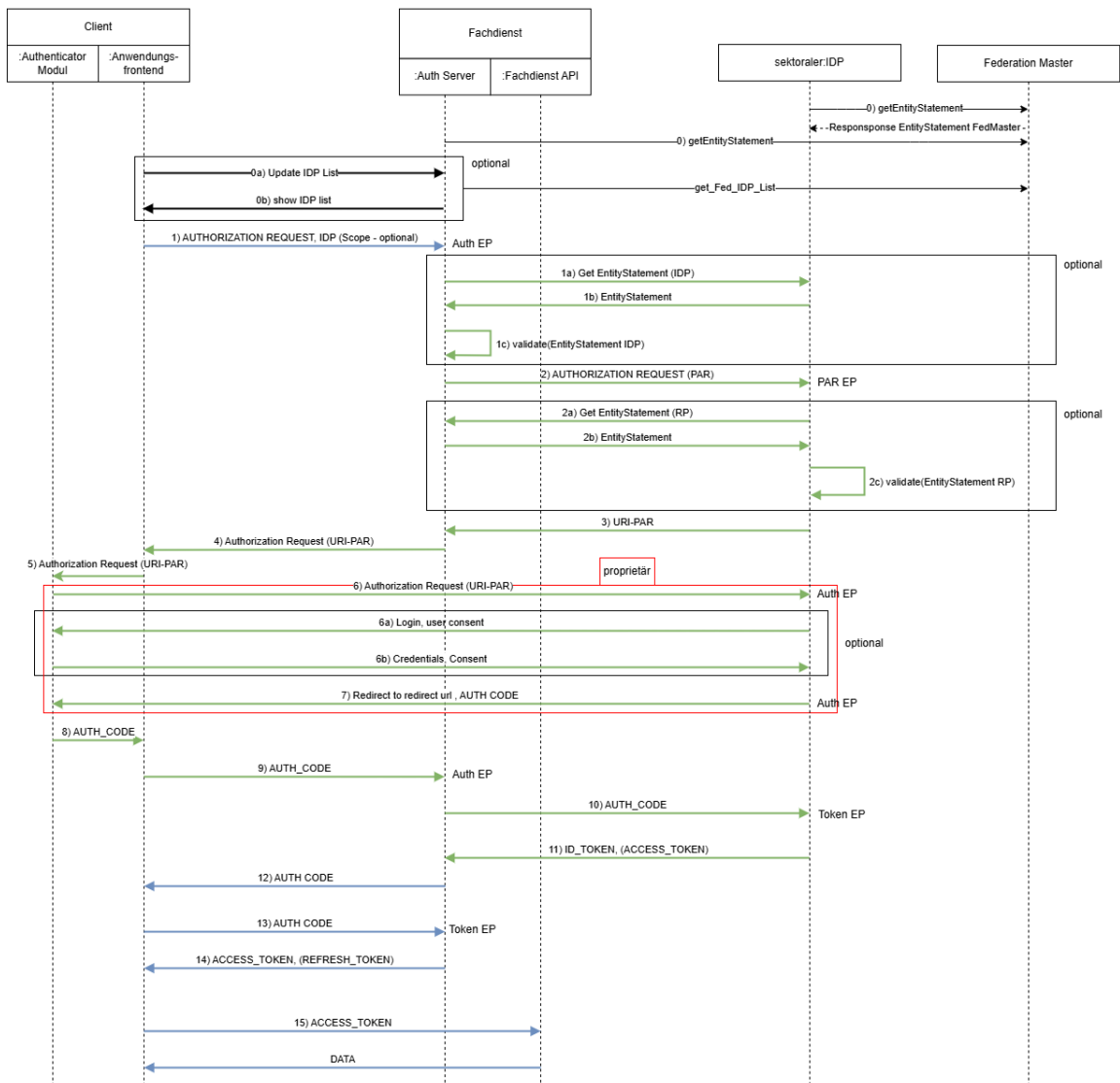
## 5.2 App2App-Flow

### 5.2.1 Vorbedingungen

- Registrierung des App-Link/Universal-Link für das Frontend auf dem Gerät des Nutzers (auf redirect Adresse des Fachdienst) - oder einreichen über Web.
- Registrierung des App-Link/Universal-Link für das Authenticator-Modul des IDP auf dem Gerät des Nutzers (auf Adresse des IDP) - oder Anfragen über Web.

5.2.2 Flow - OIDC

5.2.2.1 Flow Diagramm



Legende:

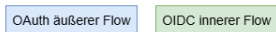


Abbildung 8 : Ablauf App2App-Flow

5.2.2.2 Ablaufbeschreibung App2App-Flow

Tabelle 6 : Ablaufbeschreibung App2App-Flow

Schritt	Beschreibung
0	Bezug des Entity Statement des Federation Master unter Nutzung des bekannten Signaturschlüssels "federation entity signing key".

		Fachdienst Authorization Server und sektorale IDPs laden in regelmäßigen Abständen die aktuellen Entity Statements der Superior-Entities, bei denen sie als Teilnehmer der TI-Föderation registriert sind und validieren die Vertrauenskette ausgehend vom geladenen Entity Statement bis zum Vertrauensanker (Trust Anchor) der TI-Föderation.
	0-a	<p>Bei Bedarf ruft das Anwendungsfrontend beim Fachdienst Authorization Server die Liste aller in der TI-Föderation registrierten sektoralen IDPs ab. Die Ermittlung der registrierten sektoralen IDPs erfolgt über einen Schnittstelle des Federation Master. Beim Federation Master sind zentrale Informationen aus den Entity Statements aller registrierten sektoralen IDPs hinterlegt. Die Bereitstellung der Liste kann über zwei Wege erfolgen:</p> <p>a) Der Fachdienst Authorization Server verwendet das Standard konforme OIDC Federation API (federation_list_endpoint). Der Fachdienst muss dann aus dem Response die sektoralen IDPs anhand des Entity Typs "openid_provider" herausfiltern, die für eine Auswahl notwendigen Informationen aus den Entity Statements der sektoralen IDPs extrahieren und seinen Anwendungsfrontends zur Verfügung stellen.</p> <p>b) Der Fachdienst Authorization Server verwendet das custom API am Federation Master (idp_list_endpoint). Hier liefert der FederationMaster eine Liste aller registrierten sektoralen IDPs mit für eine Auswahl notwendigen Informationen (Name der Organisation/Kasse, Icon, Client-ID in der TI-Föderation). Die Adresse des API kann als custom-metadata im Entity Statement des Federation Master hinterlegt werden.</p>
	0-b	<p>Der Fachdienst Authorization Server antwortet dem Anwendungsfrontend mit der Liste aller IDPs.</p> <p>Das Anwendungsfrontend zeigt dem Nutzer eine Suchfunktion an, in der er in der Liste seine Kasse per Name und mit Icon auswählen kann.</p>
1		<p>Das Anwendungsfrontend sendet dem Fachdienst Authorization Server des Fachdienstes einen Authorization-Request mit der Information, welcher sektorale IDP zur Authentifizierung des Versicherten zu verwenden ist (Client-ID in der TI-Föderation).</p> <p>Wenn die Wahl des sektoralen IDP nicht im Anwendungsfrontend getroffen wurde (0a) kann der Fachdienst Authorization Server in diesem Schritt einen AuswahlDialog anzeigen lassen.</p>
	1-a	Falls der Fachdienst Authorization Server das Entity Statement des sektoralen IDP noch nicht kennt, lädt er dies herunter. (<Client-ID in der TI-Föderation>/.well-known/openid-federation)
	1-b	Der sektorale IDP sendet sein Entity Statement an den Authorization Server des anfragenden Fachdienstes zurück.
	1-c	Der Fachdienst Authorization Server validiert das Entity Statement und die Trust Chain beginnend mit dem Entity Statement des sektoralen IDP bis zum Trust Anchor der TI-Föderation.
2		Der Fachdienst Authorization Server sendet einen Pushed Authorization Request (PAR) inkl. code-challenge und benötigter scopes an den sektorale IDP.

	2-a	Falls der sektorale IDP das Entity Statement des Fachdienst Authorization Server noch nicht kennt, lädt er dieses herunter. (<Client-ID in der TI-Föderation>/.well-known/openid-federation)
	2-b	Der Fachdienst Authorization Server sendet sein Entity Statement zurück. Der sektorale IDP validiert das Entity Statement und registriert den Fachdienst Authorization Server als Client.
	2-c	Der sektorale IDP validiert das Entity Statement und die Trust Chain beginnend mit dem Entity Statement des Fachdienst Authorization Server bis zum Trust Anchor der TI-Föderation.
3		Der sektorale IDP sendet erzeugt und eine Request-URI mit Bezug zum eingegangenen Authorization-Request an den Fachdienst Authorization Server.
4		Der Fachdienst Authorization Server sendet die Request-URI und Client ID an das Anwendungsfrontend des Fachdienstes zur Weiterleitung an den sektoralen IDP.
5		Der Aufruf aus dem Anwendungsfrontend des Fachdienstes öffnet das Authenticator-Modul (Deep-Link/Universal-Link).
6		Das Authenticator Modul führt nun den Aufruf der Request-URI am sektoralen IDP aus.
	6-a	<p>Der sektorale IDP ordnet anhand der Request-URI den Request einem vorherigen Authorization-Request zu.</p> <p>Der Authorization-Endpunkt des IDP stellt entsprechend den angefragten claims einen Consent (Zustimmung des Nutzers zur Verarbeitung der angezeigten Daten) zusammen, wenn diese Zustimmung noch nicht vorliegt.</p> <p>Der sektoralen IDP überträgt die Consent-Abfrage und für die Authentifizierung des Nutzers notwendige Daten zu dem Authenticator-Modul des sektoralen IDP.</p>
	6-b	<p>Das Authenticator-Modul des sektoralen IDP fordert den Nutzer zur Consent-Zustimmung auf, wenn diese noch nicht erfolgt ist. Und führt die Authentifizierung des Nutzers nach einem zulässigen Authentifizierungsverfahren durch. Die für den Nutzer zulässigen Authentifizierungsverfahren sind im sektoralen IDP hinterlegt. Das notwendige Vertrauensniveau, mit die Nutzerauthetifizierung durchgeführt werden soll, ist im acr-claim des Pushed Authorization Request angegeben.</p> <p>Das Authenticator-Modul des sektoralen IDP bestätigt diesem die erfolgreiche Durchführung der Authentifizierung.</p> <p>Der sektorale IDP erstellt einen Authorization Code.</p>
7		Der sektorale IDP antwortet dem Authenticator Modul mit dem Authorization Code und einem Redirect zum Fachdienst Authorization Server.

8		Das Authenticator Modul des sektoralen IDP ruft Redirect-URL mit dem Authorization Code als Parameter auf. Über einen App-Link bzw. Universal-Link wird das Anwendungsfrontend des Fachdienstes geöffnet.
9		Die Anwendungsfrontend des Fachdienstes sendet den Authorization Code an den Fachdienst Authorization Server.
10		Der Fachdienst Authorization Server reicht den Authorization Code beim Token-Endpunkt des sektoralen IDP ein.
11		Der Fachdienst Authorization Server erhält vom Token-Endpunkt des sektoralen IDP einen ID-Token mit den im Pushed Authorization Request angeforderten Informationen zum Versicherten. Der Fachdienst Authorization Server entschlüsselt das ID-Token und validiert die Signatur.
12		Fachdienst Authorization Server erstellt und sendet dem Anwendungsfrontend des Fachdienstes einen weiteren Authorization-Code, wenn zwischen Anwendungsf frontend und Authorization Server des Fachdienst ebenfalls OAuth Authorization Code-Flow zum Einsatz kommt.
13		Anwendungsfrontend des Fachdienstes übergibt dem Fachdienst Authorization Server diesen Authorization Code.
14		Anwendungsfrontend des Fachdienstes erhält vom Fachdienst Authorization Server ein Access-Token und Refresh-Token.
15		Das Anwendungsfrontend des Fachdienstes gibt bei jedem Aufruf des Fachdienstes das Access-Token mit. Nach erfolgreicher Validierung des Access-Token gibt die Fachdienst API den Zugriff auf die Fachdaten dieser Identität frei.

### 5.2.2.3 Schnittstellenbeschreibung

#### (0) Vorbedingung - Abruf der Schlüssel des Federation Master

Das selbst signierte Entity Statement des Federation Master wird von einem Teilnehmer der TI-Föderation abgerufen und gegen den bei der Registrierung bekanntgemachten Signaturschlüssel des Federation Master geprüft.

- Request zum Abruf des Entity Statements des Federation Masters

GET /.well-known/openid-federation

Host: app-ref.federationmaster.de

- Response mit beispielhaften Werten

- HTTP 200
- Content-Type: application/entity-statement+jwt
- Signatur Header des JWS

```
{
  "typ": "entity-statement+jwt",
  "kid": "puk_fedmaster_sig",
  "alg": "ES256"
}
```

- Payload

Die Tabelle zeigt und erläutert einige wichtige Attribute der Entity Configuration des Federation Masters

**Tabelle 7 : Entity Configuration des Federation Maste**

Name	Werte	Beispiel	Anmerkungen
iss	URL	"https://app-ref.federationmaster.de"	Eindeutiger Identifier (ID) des Federation Master in der TI-Föderation
sub	URL	"https://app-ref.federationmaster.de"	Identisch mit iss, dadurch ist festgelegt dass es sich bei dem Entity Statement um die Entity Configuration des Federation Master handelt
iat	Alle time Werte in Sekunden seit 1970, <a href="#">RFC 7519 Sect.2</a> ,	1773930901 = 19.03.2026 15:35:01	Zeitpunkt der Ausstellung des Entity Statements
exp	Alle time Werte in Sekunden seit 1970, <a href="#">RFC 7519 Sect.2</a> ,	1774017301 = 20.03.2026 15:35:01	Zeitpunkt des Ablaufs der Gültigkeit des Entity Statements
jwks	JWKS Objekt	{       "kty": "EC",       "crv": "P-256",       "x": "aaxglv7_eqkD...",       "y": "hg5uKlgltaM...",       "kid": "puk_fedmaster_sig",     }	Schlüssel, mit dem der Federation Master sein Entity Statement, ausgestellte Subordinate Statements und Trust Marks signiert (federation entity signig key). Das Format

		<pre>"use": "sig", "alg": "ES256" }</pre>	<p>ist ein Key-Set, da hier auch Schlüssel für einen Key-Rollover veröffentlicht werden <a href="#">[OpenID Federation 1.1]</a> ("Updating Metadata, Key Rollover, and Revocation")</p>
metadata {			<p>Der Block metadata enthält eine Reihe von <a href="#">[OpenID Federation 1.1]</a> ("Metadata"). Für jeden Entity Typ, die ein Teilnehmer unterstützt beinhaltet der Block metadata einen Bereich.</p>
federation_entity {			<p>Der Block federation_entity enthält die Metadaten für eine <a href="#">[OpenID Federation 1.1]</a><a href="https://openid.net/specs/openid-federation-1_0.html#name-federation-entity">https://openid.net/specs/openid-federation-1_0.html#name-federation-entity</a>("Federation Entity").</p>
federation_fetch_endpoint	URL	"https://app-ref.federationmaster.de/federation/fetch"	<p>Adresse des Endpunktes zum Abrufen von Subordinate Statements, welche der Federation zu einem bei ihm registrierten Teilnehmer ausstellt. Das Ergebnis der Anfrage ist ein vom Federation Master mit seinem federation entity signing key signiertes JWT mit den Metainformationen zum Teilnehmer.</p>
federation_list_endpoint	URL	"https://app-ref.federationmaster.de/federation/list"	<p>Adresse des Endpunktes zum Abrufen einer Liste aller TI-Föderationsteilnehmer, die beim Federation Master registriert sind. Das Ergebnis des Aufrufs ist eine Liste der Identifier (iss) eines jeden Teilnehmers.</p>
idp_list_endpoint	URL	"https://app-ref.federationmaster.de/federation/listidps"	<p>Adresse des Endpunktes zum Abrufen einer Liste aller beim Federation Master registrierten sektoralen IDPs. Das Ergebnis des Aufrufs ist ein JSON Array. Für jeden sektoralen IDP enthält das Array einen Eintrag mit Metainformationen zum sekt. IDP.</p>
}			<p>Ende des Blocks federation_entity</p>
}			<p>Ende des Blocks metadata</p>



--	--	--	--

## 6 Metadata

### Liste aller registrierten sektoralen IDPs

Jede Krankenversicherung unterhält einen eigenen sektoralen IDP. Die Liste aller in der TI-Föderation registrierten sektoralen IDPs kann am `idp_list_endpoint` des Federation Master abgefragt werden. Die Integrität der Liste wird mittels Signatur über einen Schlüssel aus dessen Keyset sichergestellt.

### (0 a/b) Abfrage der Liste aller in der TI-Föderation registrierten sektoralen IDPs

Die Liste aller in der TI-Föderation registrierten sektoralen IDPs wird von Anwendungen verwendet, um ihren Nutzern die Auswahl ihrer Krankenversicherung anzubieten. Die Auswahl der richtigen Krankenversicherung ist notwendig, da die Authentifizierung mit der GesundheitsID über den sektorale IDP der Krankenversicherung erfolgt.

- Request zum Abruf in der in der TI-Föderation registrierten sektoralen IDPs über den Federation Masters

```
GET /federation/listidps
```

```
Host: app-ref.federationmaster.de
```

- Response mit beispielhaften Werten

- HTTP 200
- Content-Type: `idp-list+jwt`
- 

- Signatur Header des JWS

```
{
  "typ": "idp-list+jwt",
  "kid": "puk_fedmaster_sig",
  "alg": "ES256"
}
```

- Payload

Die Tabelle zeigt und erläutert die Attribute in der Auskunft des Federation Master zur Liste registrierten sektoralen IDPs

**Tabelle 8 : Liste registrierten sektoralen IDPs**

Name	Werte	Beispiel	Anmerkungen
iss	URL	"https://app-ref.federationmaster.de"	Eindeutiger Identifier (ID) des Federation Master in der TI-Föderation
iat	Alle time Werte in	1773930901 = 19.03.2026 15:35:01	Zeitpunkt der Ausstellung der

	Sekunden seit 1970, <a href="#">RFC 7519 Sect.2</a> ,		Liste der registrierten sekt. IDPs
exp	Alle time Werte in Sekunden seit 1970, <a href="#">RFC 7519 Sect.2</a> ,	1774017301 = 20.03.2026 15:35:01	Zeitpunkt des Ablaufs der Gültigkeit der Liste der registrierten sekt. IDPs
idp_entity [{			Der Block idp_entity enthält zu jedem in der TI- Föderation registrierten sektoralen IDP einen Datensatz mit Informationen zum sektoralen IDP.
organization_name	String	"gematik"	Der Name des sektoralen IDP zur Anzeige für Benutzer ist die Definition von "organization_name" im Entity Statement des sektoralen IDP.
iss	URL	"https://gsi-ref.dev.gematik.solutions"	Das Attribut "iss" ist die eindeutige ID des sektoralen IDP in der TI- Föderation und entspricht dem claim "iss" in dessen Entity Statement.
logo_uri	URI	„https://raw.githubusercontent.com/gematik/zero-lab/main/static/images/GID_App_light_mode.png“	Das Attribut "logo_uri" entspricht dem claim "logo_uri" aus dem Entity Statement des sektoralen IDP.
user_type_supported	[ HCI = Health Care Institution, HP = Health	"IP"	Das Attribut "user_type_supported" entspricht dem claim "user_type_supported" aus dem Entity

	Professional, IP = Insured Person]		Statement des sektoralen IDP.
pkv	true/false	"true"	Ist die Krankenversicherung eine Private Krankenversicherung, so ist der Wert "true", ansonsten "false". Diese Informationen benötigen die Anwendungen um Anwendungsfälle für privat oder gesetzlich Versicherte steuern zu können. Die Information zur Befüllung des Attribut "pkv" stammt aus der Registrierung des sektoralen IDP in der TI-Föderation.
}]			Ende des Blocks idp_entity

### (1) Anfrage vom Anwendungsclient an den Fachdienst Authorization Server

Das Anwendungsfrontend sendet ein Request an Fachdienst Authorization Server. Da das Anwendungsfrontend selbst nicht Teil der TI-Föderation ist, liegt es bei der Anwendung selbst, wie das Vertrauensverhältnis zwischen Fachdienst-Client und Fachdienst Authorization Server sichergestellt wird.

Hier kann z.B. auf den Standard aufsetzend der OAuth-Authorization-Code-Flow zur Sicherstellung der Vertrauensbeziehung verwendet werden.

### (1 a/b) Laden der Entity Configuration des sektoralen IDP

Der Fachdienst Authorization Server benötigt die Entity Configuration des sektoralen IDP, um einen Authorization Request zu formulieren, den der sektorale IDP akzeptiert. Der Fachdienst Authorization Server erhält die Entity Configuration, indem er das Entity Statement des sektoralen IDP lädt

- Request zum Abruf des Entity Statements des Federation Masters

```
GET /.well-known/openid-federation
Host: gsi-ref.dev.gematik.solutions
```

- Response mit beispielhaften Werten

- HTTP 200
- Content-Type: application/entity-statement+jwt
- Signatur Header des JWS

```
1126     {
1127         "typ": "entity-statement+jwt",
1128         "kid": "puk_idp_sig",
1129         "alg": "ES256"
1130     }
```

1131 • Payload

1132 Die Tabelle zeigt und erläutert einige wichtige Attribute der Entity Configuration eines  
1133 sektoralen IDP

1134

**Tabelle 9 : Entity Configuration eines sektoralen IDP**

Name	Werte	Beispiel	Anmerkungen
iss	URL	"https://gsi-ref.dev.gematik.solutions"	Eindeutiger Identifier (ID) des sektoralen IDP in der TI-Föderation
sub	URL	"https://gsi-ref.dev.gematik.solutions"	Identisch mit "iss", dadurch ist festgelegt dass es sich bei dem Entity Statement um die Entity Configuration des sektoralen IDP handelt
iat	Alle time Werte in Sekunden seit 1970, <a href="#">RFC 7519 Sect.2</a> ,	1773930901 = 19.03.2026 15:35:01	Zeitpunkt der Ausstellung des Entity Statements
exp	Alle time Werte in Sekunden seit 1970, <a href="#">RFC 7519 Sect.2</a> ,	1774017301 = 20.03.2026 15:35:01	Zeitpunkt des Ablaufs der Gültigkeit des Entity Statements
jwks	JWKS Objekt	{ "kty": "EC", "crv": "P-256", "x": "Abt2Uyrk6...", "y": "YZKBJtOUY...", "kid": "puk_idp_sig", "use": "sig", "alg": "ES256" }	Schlüssel, mit dem der sektorale IDP sein Entity Statement signiert (federation entity signig key). Das Format ist ein Key-Set, da hier auch Schlüssel für einen Key-Rollover veröffentlicht werden [ <a href="#">OpenID</a> ]

			<a href="#">Federation 1.1</a> ("Updating Metadata, Key Rollover, and Revocation").
authority_hints	[ string ]	"https://app-ref.federationmaster.de"	Identifiziert (iss) der Subordinate Entity, bei welcher der sektorale IDP registriert ist. Diese Entity wird zur Validierung der Vertrauensketten (Trust Chain) herangezogen.
metadata {			Der Block metadata enthält eine Reihe von <a href="#">[OpenID Federation 1.1]</a> ("Metadata"). Für jeden Entity Typ, der ein Teilnehmer unterstützt, beinhaltet der Block metadata einen Bereich.
openid_provider {			Der Block openid_provider enthält die Metadaten für einen <a href="#">[OpenID Federation for OpenID Connect 1.1]</a> ("OpenID Connect OpenID Provider").
issuer	URL	"https://gsi-ref.dev.gematik.solutions"	Eindeutiger Identifier in der TI-Föderation, der Wert entspricht dem "iss" im allgemeinen Teil des Entity



			Statements.
signed_jwks_uri	URL	"https://gsi-ref.dev.gematik.solutions/jws.json"	Ablageort für weitere Schlüssel welche der sektorale IDP verwendet, etwa zur Signatur der ID-Token.
organization_name	String	"gematik sektoraler IDP"	Der Name des sektoralen IDP - wird z.B. in der Auswahlliste zur Auswahl seiner Krankenversicherung durch den Benutzer verwendet.
logo_uri	URL	„https://raw.githubusercontent.com/gematik/zero-lab/main/static/images/GID_App_light_mode.png “	Abloageort des Logos der Organisation (Krankenversicherung). Das Logo wird z.B. in der Auswahlliste zur Auswahl seiner Krankenversicherung durch den Benutzer verwendet.
authorization_endpoint	URL	„https://gsi-ref.dev.gematik.solutions/auth “	Endpunkt des sektoralen IDP, an den ein Teilnehmer Authorization Requests senden muss.
token_endpoint	URL	"https://gsi-ref-mtls.dev.gematik.solutions/token"	Endpunkt des sektoralen IDP, an den ein Teilnehmer Token Requests senden muss.

pushed_authorization_request_endpoint	URL	„https://gsi-ref-mtls.dev.gematik.solutions/ PAR_Auth “	Endpunkt des sektoralen IDP, an den ein Teilnehmer Pushed Authorization Requests senden muss.
scopes_supported	["urn:telematik:geburtsdatum", "urn:telematik:given_name", "urn:telematik:versicherter", "urn:telematik:display_name", "urn:telematik:geschlecht", "urn:telematik:alter", "urn:telematik:family_name", "urn:telematik:email", "openid"]	["urn:telematik:geburtsdatum", "urn:telematik:given_name", "urn:telematik:versicherter", "urn:telematik:display_name", "urn:telematik:geschlecht", "urn:telematik:alter", "urn:telematik:family_name", "urn:telematik:email", "openid"]	Scopes, die der sektorale IDP supported. D.h., der sektorale IDP kann maximal die Attribute (claims) zu einer Identität beauskunften, die in den unterstützten scopes enthalten sind.
require_pushed_authorization_requests	true/false	true	Ist der Wert für dieses Attribut "true", so akzeptiert der sektorale IDP nur Pushed Authorization Request
token_endpoint_auth_methods_supported	[self_signed_tls_client_auth]		Der sektorale IDP unterstützt ausschließlich die Kommunikation TI-Föderationsteilnehmer TLS-Zertifikat (mTLS)
user_type_supported	[ IP ]	"IP"	IP = Insured Person - der sektorale IDP unterstützt ausschließlich die Authentifizierung von versicherten Personen (Versicherte)

}			Ende des Blocks openid_provider
}			Ende des Blocks metadata

1135

### (1 c) Validieren des Entity Statment des sektoralen IDP und Prüfung der Trust Chain

Der Fachdienst Authorization Server validiert die gesamte Trust Chain ausgehend vom Entity Statement des sektoralen IDP bis zum Trust Anchor der TI-Föderation.

Unter anderem ruft der Fachdienst Authorization Server dazu das Subordinate Statement zum sektoralen IDP beim Federation Master ab. In dem vom Federation Master ausgestellten und signierten Subordinate Statement liefert der Federation Master dem Fachdienst Authorization Server Informationen zu sektoralen IDP als Teilnehmer der TI-Föderation. Für die Anfrage muss die ID (iss) des Federation Master und die ID (sub) des Teilnehmers, zu dem die Anfrage gestellt wird, angegeben werden.

- Request zum Abruf des Entity Statements des Federation Masters

```
GET /federation/fetch?iss=https://app-
ref.federationmaster.de&sub=https://gsi-ref.dev.gematik.solutions
Host: app-ref.federationmaster.de
```

- Response mit beispielhaften Werten

- HTTP 200
- Content-Type: application/entity-statement+jwt
- Signatur Header des JWS

```
{
  "typ": "entity-statement+jwt",
  "kid": "puk_fedmaster_sig",
  "alg": "ES256"
}
```

- Payload

Die Tabelle zeigt und erläutert einige wichtige Attribute der Teilnehmerauskunft (subordinate Statement) zum sektoralen IDP

**Tabelle 10 : Subordinate Statement zu einem sektoralen IDP**

Name	Werte	Beispiel	Anmerkungen
iss	URL	"https://app-ref.federationmaster.de"	Eindeutiger Identifier (ID) des Federation Master in der TI-Föderation
sub	URL	"https://gsi-ref.dev.gematik.solutions"	Eindeutiger Identifier (ID) des sektoralen IDP, zu dem die Teilnehmerauskunft (Subordinate Statement) erteilt werden soll.
iat	Alle time Werte in Sekunden seit 1970, <a href="#">RFC 7519 Sect.2</a> ,	1773930901 = 19.03.2026 15:35:01	Zeitpunkt der Ausstellung des Subordinate Statements
exp	Alle time Werte in Sekunden	1774017301 = 20.03.2026 15:35:01	Zeitpunkt des Ablaufs der Gültigkeit des

	seit 1970, <a href="#">RFC 7519 Sect.2</a> ,		Subordinate Statements
jwt	JWT Objekt	<pre> "jwt": {   "keys": [     {       "kty": "EC",       "kid": "puk_idp_sig",       "crv": "P-256",       "x": "Abt2Uyrk6...",       "y": "YZKBJtOUY...",       "use": "sig",       "alg": "ES256"     }   ] } </pre>	Schlüssel, mit dem der sektorale IDP sein Entity Statement signiert (federation entity signing key)
metadata	JSON-Array	<pre> "metadata": {   "openid_provider": {     "client_registration_types_supported": [       "automatic"     ]   } } </pre>	Metadatenblock mit den Metadaten zum angefragten Teilnehmer der TI-Föderation

## (2) Der Autorisierungsserver des Fachdienstes sendet ein Pushed Authorization Request

Der innere Flows startet mit dem Pushed Authorization-Request ([RFC9126](#)) des Fachdienst an den `pushed_authorization_request_endpoint` des sektoralen IDP. Als `client_assertion` wird `self_signed_tls_client_auth` verwendet (siehe OIDC Standard [OpenID Connect Core 1.0 \(section-9\)](#)).

- Pushed Authorization Request

```

POST /PAR_Auth
Host: gsi-ref.dev.gematik.solutions
Content-Type: application/x-www-form-urlencoded scope=urn%3Atelematik
%3Adisplay_name+urn%3Atelematik
%3Aversicherter+openid&acr_values=gematik-ehealth-loa-
high&response_type=code&state=yyystateyyy&redirect_uri=https%3A%2F
%2Fredirect.testsuite.gsi&code_challenge_method=S256&nonce=vy7rM801AQ
w1or22GhrZ&client_id=https%3A%2F
%2Fidpfadi.dev.gematik.solutions&code_challenge=Shfl63eRGqtkndBuvWSFW
qnue67tHYSEgQozlntaoJQ

```

Der Pushed Authorization Request des Fachdienst zum sektoralen IDP enthält die folgenden Parameter:

**Tabelle 11 : Inhalte eines Pushed Authorization Request**

Name	Werte	Beispiel	Anmerkungen

client_id	URL	"https://idpfadi.dev.gematik.solutions"	Die client_id ist die ID des Fachdienst Authorization Server, der den Pushed Authorization Request stellt, in der TI-Föderation und entspricht dem claim "iss" in dessen Entity Statement.
state	VSCHAR	yyystateyyy	Vom Fachdienst Authorization Server erstellter Zufallswert, der in der weiteren Kommunikation mit dem sektoralen IDP zur Prüfung der Integrität verwendet wird.
redirect_uri	URL	https://redirect.testsuite.gsi	Adresse, an welche der vom sektoralen IDP ausgestellte Authorization Code zugestellt werden soll. I.d.R. ist dies der Fachdienst Authorization Server.
code_challenge	Hash über code_verifier.	Shfl63eRGqtkndBuvWSFWqnue67tHYSEgQozIntaoJQ	Hash über einen vom Fachdienst Authorization Server erzeugten "code_verifier".
code_challenge_method	S256	-	Methode, mit welcher der Hashwert "code_challenge" aus dem "code_verifier" erzeugt wurde.
response_type	code	-	Für den Authorization Code Flow ist "response_type"="code".
nonce	string	vy7rM801AQw1or22GhrZ	Die nonce ist ein vom Fachdienst

			Authorization Server ausgestellter Zufallswert.
scope	string	urn:telematik:display_name urn:telematik:versicherter openid	Im claim "scope" sind die Informationen (scopes) aufgeführt, die der Fachdienst Authorization Server im vom sektoralen IDP ausgestellten ID-Token erwartet.
acr_values	"gematik-ehealth-loa-high" oder "gematik-ehealth-loa-substantial"	"gematik-ehealth-loa-high"	Der claim "acr_values" gibt an, welche Vertrauensniveaus bei der Nutzerauthentifizierung eingehalten werden müssen, damit der Fachdienst der Authentifizierung vertrauen kann. Dieser Wert hat Einfluss darauf, welche Authentisierungsmitel dem Nutzer angeboten werden.

## (2 a/b) Laden der Entity Configuration des Fachdienst Authorization Server

Der sektorale IDP benötigt die Entity Configuration des Fachdienst Authorization Server, um zu prüfen, ob der Sender vertrauenswürdiger Teilnehmer der TI-Föderation und der empfangene Authorization Request korrekt ist. Der sektorale IDP erhält die Entity Configuration, indem er das Entity Statement des Fachdienst Authorization Server lädt.

- Request zum Abruf des Entity Statements des Fachdienst Authorization Server

```
GET /.well-known/openid-federation
Host: idpfadi.dev.gematik.solutions
```

- Response mit beispielhaften Werten

- HTTP 200
- Content-Type: application/entity-statement+jwt
- Signatur Header des JWS

```
{
  "typ": "entity-statement+jwt",
  "kid": "puk_fd_sig",
  "alg": "ES256"
}
```

- Payload



1205 Die Tabelle zeigt und erläutert einige wichtige Attribute der Entity Configuration eines  
1206 Fachdienst Authorization Server

1207

1208

**Tabelle 12 : Entity Configuration eines Fachdienst Authorization Server**

Name	Werte	Beispiel	Anmerkungen
iss	URL	"https://idpfadi.dev.gematik.solutions"	Eindeutiger Identifier (ID) des Fachdienst Authorization Server in der TI-Föderation
sub	URL	"https://idpfadi.dev.gematik.solutions"	Identisch mit "iss", dadurch ist festgelegt dass es sich bei dem Entity Statement um die Entity Configuration des Fachdienst Authorization Server handelt
iat	Alle time Werte in Sekunden seit 1970, <a href="#">RFC 7519 Sect.2</a> ,	1773930901 = 19.03.2026 15:35:01	Zeitpunkt der Ausstellung des Entity Statements
exp	Alle time Werte in Sekunden seit 1970, <a href="#">RFC 7519 Sect.2</a> ,	1774017301 = 20.03.2026 15:35:01	Zeitpunkt des Ablaufs der Gültigkeit des Entity Statements
jwks	JWKS Objekt	{ "kty": "EC", "crv": "P-256", "x": "9bjs27YAflMU...", "y": "P8lzNVROgTu...", "kid": "puk_fd_sig", "use": "sig", "alg": "ES256" }	Schlüssel, mit dem der Fachdienst Authorization Server sein Entity Statement signiert (federation entity signig key). Das Format ist ein Key-Set, da hier auch Schlüssel für einen Key-Rollover veröffentlicht werden [ <a href="#">OpenID Federation 1.1</a> ] ("Updating Metadata, Key Rollover, and Revocation").

authority_hints	[ string ]	"https://app-test.federationmaster.de"	Identifiziert (iss) der Subordinate Entity, bei welcher der Fachdienst Authorization Server registriert ist. Diese Entity wird zur Validierung der Vertrauensketten (Trust Chain) herangezogen.
metadata {			Der Block metadata enthält eine Reihe von <a href="#">[OpenID Federation 1.1]</a> ("Metadata"). Für jeden Entity Typ, der ein Teilnehmer unterstützt, beinhaltet der Block metadata einen Bereich.
openid_relying_party {			Der Block openid_relying_party enthält die Metadaten für eine <a href="#">[OpenID Federation for OpenID Connect 1.1]</a> ("OpenID Connect Relying Party").
signed_jwks_uri	URL	"https://idpfadi.dev.gematik.solutions/jws.json"	Ablageort für weitere Schlüssel, welche der Fachdienst Authorization Server verwendet, etwa für die Verschlüsselung der ID-Token.
organization_name	String	"Fachdienst007 des FedIdP POCs"	Der Organisationsname des Fachdienst Authorization Server kann z.B. für die Anzeige des Consent-Dialogs für die Nutzerzustimmung verwendet werden.
client_name	String	"Fachdienst007"	Der Name des Fachdienst Authorization Server kann z.B. für die Anzeige des Consent-Dialogs für die Nutzerzustimmung verwendet werden.

			werden.
logo_uri	URL	„https://idpfadi.dev.gematik.solutions/noLogoYet “	Ablageort des Logos des Fachdienst. Das Logo kann für Anzeigen am Benutzerfrontend verwendet werden.
redirect_uris	[URL]	["https://idpfadi.dev.gematik.solutions/auth", "https://Fachdienst007.de/client", "https://redirect.testsuite.gsi", "https://gries.dev.gematik.solutions/callback"]	Der claim "redirect_uris" enthält eine Liste der URLs, an welches der vom sektoralen IDP ausgestellte Authorization Code zugestellt werden darf. Die "redirect_uri" im Push Authorization Request muss mit einer URL dieser Liste übereinstimmen.
default_acr_values	[String]	["gematik-ehealth-loa-high"]	Ist in einem Pushed Authorization Request, den der Fachdienst Authorization Server an den sektoralen IDP stellt, der claim "acr_values" nicht gesetzt, so muss der sektorale IDP die Nutzer Authentifizierung auf den im claim "default_acr_values" angegebenen Vertrauensniveaus durchführen.
scope	String	"urn:telematik:given_name urn:telematik:versicherter"	Der claim "scope" enthält eine Aufzählung der scopes, welche der Fachdienst Authorization Server in einem Pushed Authorization Request anfordern darf.
}			Ende des Blocks openid_relying_party
}			Ende des Blocks metadata

--	--	--	--

## 6.1 OpenID Connect Relying Party

### (2 c) Validieren des Entity Statment des Fachdienst Authorization Server und Prüfung der Trust Chain

Der sektoralen IDP validiert die gesamte Trust Chain ausgehend vom Entity Statement des Fachdienst Authorization Server bis zum Trust Anchor der TI-Föderation.

Unter anderem ruft der sektorale IDP dazu das Subordinate Statement zum Fachdienst Authorization Server bei der Superior-Entity ab, bei welcher der Fachdienst Authorization Server registriert ist. In dem vom der Superior-Entity ausgestellten und signierten Subordinate Statement liefert diese dem sektoralen IDP Informationen zum Fachdienst Authorization Server als Teilnehmer der TI-Föderation. Für die Anfrage muss die ID (iss) der Superior-Entity und die ID (sub) des Teilnehmers, zu dem die Anfrage gestellt wird, angegeben werden.

- Request zum Abruf des Entity Statements des Federation Masters

```
GET /federation/fetch?iss=https://app-  
test.federationmaster.de&sub=https://idpfadi.dev.gematik.solutions  
Host: app-test.federationmaster.de
```

- Response mit beispielhaften Werten

- HTTP 200
- Content-Type: application/entity-statement+jwt
- Signatur Header des JWS

```
{  
  "typ": "entity-statement+jwt",  
  "kid": "puk_fedmaster_sig",  
  "alg": "ES256"  
}
```

- Payload

Die Tabelle zeigt und erläutert einige wichtige Attribute der Teilnehmerauskunft (subordinate Statement) zum Fachdienst Authorization Server

**Tabelle 13 : Subordinate Statement zu einem Fachdienst Authorization Server**

Name	Werte	Beispiel	Anmerkungen
iss	URL	"https://app-test.federationmaster.de"	Eindeutiger Identifier (ID) des Federation Master in der TI-Föderation
sub	URL	"https://idpfadi.dev.gematik.solutions"	Eindeutiger Identifier (ID) des Fachdienst Authorization

			Server, zu dem die Teilnehmersankunft (Subordinate Statement) erteilt werden soll.
iat	Alle time Werte in Sekunden seit 1970, <a href="#">RFC 7519 Sect.2</a> ,	1773930901 = 19.03.2026 15:35:01	Zeitpunkt der Ausstellung des Subordinate Statements
exp	Alle time Werte in Sekunden seit 1970, <a href="#">RFC 7519 Sect.2</a> ,	1774017301 = 20.03.2026 15:35:01	Zeitpunkt des Ablaufs der Gültigkeit des Subordinate Statements
jwks	JWKS Objekt	<pre>"jwks": {   "keys": [     {       "kty": "EC",       "kid": "puk_fd_sig",       "crv": "P-256",       "x": "9bJs27YAfl...",       "y": "P8lzNVROgT...",       "use": "sig",       "alg": "ES256"     }   ] }</pre>	Schlüssel, mit dem der Fachdienst Authorization Server sein Entity Statement signiert (federation entity signing key)
metadata	JSON-Array	<pre>"metadata": {   "openid_relying_party": {     "client_registration_types": [       "automatic"     ]   },   "claims": [],   "redirect_uris": [     "https://gries.dev.gematik.solutions/callback",     "https://idpfadi.dev.gematik.solutions/auth",     "https://redirect.testsuite.gsi",     "https://Fachdienst007.de/client" ],   "scope": "urn:telematik:versicherter urn:telematik:display_name openid " }</pre>	<p>Metadatenblock mit den Metadaten zum angefragten Teilnehmer der TI-Föderation. Das Subordinate Statement zu einem registrierten Fachdienst Authorization Server enthält die Informationen</p> <ul style="list-style-type: none"> <li>• Welche redirect_uris bei der Registrierung als zulässig angegeben wurden,</li> <li>• Welche claims bei der Registrierung</li> </ul>

			als zulässig angegeben wurden, <ul style="list-style-type: none"> <li>Welche scope bei der Registrierung als zulässig angegeben wurden,</li> </ul>
--	--	--	---

### (3) Antwort des sektoralen IDP auf den Pushed Authorization Request

Des sektoralen IDP antwortet dem Fachdienst Authorization Server auf den Pushed Authorization Request mit einer Request URI. Die Request-URI ist ein für einen einmaligen Authentifizierungsvorgang generierter Wert, der keine weiteren Informationen aus dem ursprünglichen Pushed Authorization Request enthält.

Zuvor verifiziert der IDP das TLS Clientzertifikat gegen einen Schlüssel aus dem Entity Statement des Fachdienstes.

- Response mit beispielhaften Werten
  - HTTP 201
  - Content-Type: application/json
  - ```
{
  "request_uri":
    "urn:https://idpfadi.dev.gematik.solutions:2f4c9dc66dcf350e",
  "expires_in": 90
}
```

Die Tabelle zeigt und erläutert die Attribute in der Antwort des sektoralen IDP auf den Pushed Authorization Request

**Tabelle 14 : Request URI, ausgestellt vom sektoralen IDP**

| Name        | Werte                    | Beispiel                                      | Anmerkungen                                                                                                                                     |
|-------------|--------------------------|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| request_uri | URI                      | urn:Fachdienst007:bwc4JK-ESC0w8acc191e-Y1LTC2 | Der sektorale IDP erzeugt eine einmalig gültige URI. An diese URI sendet das Authenticator Modul später den eigentlichen Authorization Request. |
| expires_in  | Gültigkeitsdauer der URI | 90                                            | Der Wert bestimmt die maximale Gültigkeitsdauer der Request-URI in Sekunden.                                                                    |

Diese URI wird vom Fachdienst Authorization Server als redirect an das Anwendungsfrontend gesendet um über das Authenticator Modul den sektoralen IDP zu erreichen.

### (4) Redirect der Request URI

- HTTP-302



- Location:  
https://gsi-ref.dev.gematik.solutions?client\_id=https://idpfadi.dev.gematik.solutions &  
request\_uri=urn:https://idpfadi.dev.gematik.solutions:2f4c9dc66dcf350e

Die Tabelle zeigt und erläutert die Attribute im Redirect zum sektoralen IDP

**Tabelle 15 : Inhalte des Redirect zum sektoralen IDP**

| Name        | Wert e | Beispiel                                                   | Anmerkungen                                                                                                                                                                                                        |
|-------------|--------|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| client_id   | URL    | "https://idpfadi.dev.gematik.solutions"                    | Die "client_id" ist die URL des Fachdienst Authorization Server, mit der dieser in der TI-Föderation registriert ist. Diese entspricht dem Attribut "iss" im Entity Statement des Fachdienst Authorization Server. |
| request_uri | URI    | urn:https://idpfadi.dev.gematik.solutions:2f4c9dc66dcf350e | Die vom sektorale IDP erzeugte einmalig gültige URI, an welche das Authenticator Modul später den eigentlichen Authorization Request sendet.                                                                       |

## (5) Das Anwendungsfrontend sendet den Authentication Request

- Request zum Abruf des Authorization Request  
GET /urn:https://idpfadi.dev.gematik.solutions:2f4c9dc66dcf350e?  
client\_id=https://idpfadi.dev.gematik.solutions  
Host: gsi-ref.dev.gematik.solutions

Das Authenticator Modul des sektoralen IDP fängt diesen Request dadurch das er diese Adresse für App2App Kommunikation im Betriebssystem registriert hat.

## (6) Das Authenticator Modul leitet den Authentication Request an den IDP weiter. (proprietär)

Die Schritte zur Nutzer-Authentifizierung und zur Erstellung des Authorization Code durch den IDP sind Hersteller spezifisch.

#### **(7) Der Authorization-Endpunkt des sektoralen IDP antwortet dem Authenticator Modul mit einem Redirect zum Fachdienst. (proprietär)**

Der der sektoralen IDP antwortet dem Authenticator Modul mit einem Redirect zum Fachdienst Authorization Server und übergibt den generierten Authorization Code.

- Response
  - HTTP-302
  - Location: `https://redirect.testsuite.gsi?state=yyystateyyy & code=cyd6LM-GUE2y0ce313g-A3NVE4`

Die Tabelle zeigt und erläutert die Attribute im Redirect zum Fachdienst Authorization Server

**Tabelle 16 : Inhalte des Redirect zum Fachdienst Authorization Server**

| Name     | Werte  | Beispiel                                    | Anmerkungen                                                                                                                                                                                                                                       |
|----------|--------|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location | URI    | <code>https://redirect.testsuite.gsi</code> | Der Authorization Code soll an die im Pushed Authorization Request angegebene "redirect_uri" gesendet werden.                                                                                                                                     |
| code     | String | <code>cyd6LM-GUE2y0ce313g-A3NVE4</code>     | Der sektoralen IDP stellt einen Authorization Code aus, den der Empfänger dann beim sektoralen IDP in ein ID-Token tauschen kann.                                                                                                                 |
| state    | String | <code>yyystateyyy</code>                    | Über den im Pushed Authorization Request angegebene state-Parameter kann der Fachdienst Authorization Server verifizieren, dass die Antwort auf den Pushed Authorization Request von dem sektoralen IDP kommt, an den der Request gestellt wurde. |

#### **(8) Das Authenticator Modul sendet den Request**

- Request zum Aufruf des Fachdienst Authorization Server vom Authenticator Modul des sektoralen IDP

`GET ?state=yyystateyyy&code=cyd6LM-GUE2y0ce313g-A3NVE4`

`Host: redirect.testsuite.gsi`

Das Anwendungsfrontend fängt diesen Request dadurch das er diese Adresse für App2App Kommunikation im Betriebssystem registriert hat.

#### **(9) Aufruf des Fachdienst Authorization Server**

Das Anwendungsfrontend ruft den Fachdienst Authorization Server auf und sendet asl Parameter den vom sektoralen IDP ausgestellten Authorization Code sowie den state-Parameter.

- Request zum Aufruf des Fachdienst Authorization Server vom Anwendungsfrontend der Fachanwendung

POST state=yyystateyyy&code=cyd6LM-GUE2y0ce313g-A3NVE4

Host: redirect.testsuite.gsi

state=yyystateyyy&code=cyd6LM-GUE2y0ce313g-A3NVE4

### (10) Abruf des ID-Token

Der Fachdienst Authorization Server reicht den Authorization Code beim Token-Endpunkt des sektoralen IDP ein.

- Request zum Abruf des ID-Token beim sektoralen IDP durch den Fachdienst Authorization Server

POST /token

Host: gsi-ref-mtls.dev.gematik.solutions

grant\_type=authorization\_code&code=cyd6LM-GUE2y0ce313g-A3NVE4?

code\_verifier=e8ctQxmraK130Hv8dAlQyBKlrN2E6F-

Bx3h48RaRX3lJURyD6Be1ehfNpiiJwz9zGehVW0Djow87JZfwZooAyg-

jeA858qWr\_Fd7EnK-xxkVc8zdomFJJTcjt9xIQdC4&client\_id=https://

idpfadi.dev.gematik.solutions&redirect\_uri=https://

redirect.testsuite.gsi

Die Tabelle zeigt und erläutert die Attribute für den Abruf des ID-Token vom sektoralen IDPs durch den Fachdienst Authorization Server

**Tabelle 17 : Attribute für den Abruf des ID-Token vom sektoralen IDP**

| Name       | Werte                | Beispiel                   | Anmerkungen                                                                                                                |
|------------|----------------------|----------------------------|----------------------------------------------------------------------------------------------------------------------------|
| grant_type | "authorization_code" | -                          | Bei der Kommunikation zwischen Fachdienst Authorization Server und sektoralen IDP wird Authorization Code Flow eingesetzt. |
| code       | String               | cyd6LM-GUE2y0ce313g-A3NVE4 | Der vom sektoralen IDP erstellte Authorization Code, den der Fachdienst Authorization Server beim sektoralen IDP           |

|               |        |                                                                                                                                  |                                                                                                                                                                                                                                                                                         |
|---------------|--------|----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |        |                                                                                                                                  | gegen ein ID-Token tauschen möchte.                                                                                                                                                                                                                                                     |
| code_verifier | String | e8ctQxmraK13OHv8dAlQyBKlrN2E6F-Bx3h48RaRX3lJURyD6Be1ehfNpiijwz9zGehVW0DjoW87JZfwZooAkg-jeA858qWr_Fd7EnK-xxkVc8zdomFJJTcjt9xIQdC4 | Der sektorale IDP muss aus dem Parameter "code_verifier" mit der "code_challenge_method", die im Pushed Authorization Request übertragen wurde eine "code_challenge" berechnen. Diese muss mit der im Pushed Authorization Request übertragenen "code_challenge" übereinstimmen (PKCE). |
| client_id     | URL    | "https://idpfadi.dev.gematik.solutions"                                                                                          | Die "client_id" ist die URL des Fachdienst Authorization Server, mit der dieser in der TI-Föderation registriert ist. Diese entspricht dem Attribut "iss" im Entity Statement des Fachdienst Authorization Server.                                                                      |
| redirect_uri  | URL    | "https://redirect.testsuite.gsi"                                                                                                 | Das ID-Token soll an die im Request angegebene "redirect_uri" gesendet werden.                                                                                                                                                                                                          |

## (11) Ausstellung des ID\_TOKEN

Der Fachdienst Authorization Server erhält vom Token-Endpunkt des sektoralen IDP ein ID-Token mit den gewünschten Claims. Das ID-Token ist mit einem Verschlüsselungsschlüssel des Fachdienst Authorization Server verschlüsselt. Der sektorale IDP verwendet für die Verschlüsselung einen Encryption Key aus dem Metadaten

Block im Entity Statement des Fachdienst Authorization Server. Der sektorale IDP signiert das ID-Token mit einem Signaturschlüssel dessen öffentlicher Teil im Metadaten Block seines Entity Statements veröffentlicht ist.

- Response

- HTTP-200
- Content-Type=application/json
- Cache-Control=no-store
- Pragma=no-cache
- JSON

```
{  
  "id_token": "eyJhbGciOiJSUzI1NiIsIm.ewogImlzc  
yI6ICJodHRwOi8vc2VydmVyLmV4YW1wbGUuY29tIiwKICJzdWIiOiAiMj  
Q4Mjg5  
NzYxMDAxIiwKICJ...",  
  "token_type": "Bearer",  
  "expires_in": 300  
}
```

- Encryption Header des JWS

```
{  
  "use": "enc",  
  "kid": "puk_fd_enc",  
  "alg": "ES256"  
}
```

- Signatur Header des JWS

```
{  
  "use": "sig",  
  "kid": "puk_fed_idp_token",  
  "alg": "ES256"  
}
```

- Payload

Die Tabelle zeigt und erläutert die Attribute des ID-Token

**Tabelle 18 : Attribute des ID-Token**

| Name | Werte  | Beispiel                                   | Anmerkungen                                                                                            |
|------|--------|--------------------------------------------|--------------------------------------------------------------------------------------------------------|
| iss  | URL    | https://gsi-ref-mtls.dev.gematik.solutions | Eindeutiger Identifier (ID) des sektoralen IDP in der TI-Föderation, der das ID-Token ausgestellt hat. |
| sub  | String | "UserC3PO-666"                             | Je Nutzer und Fachdienst erstellt der sektorale IDP einen eindeutigen Identifier, der                  |

|       |                                                                          |                                         |                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------|--------------------------------------------------------------------------|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       |                                                                          |                                         | keine Nutzerdaten enthält (Pseudonym bzw. pseudonyme Identität). Fachdienste, die aus Datenschutz rechtlichen Gründen keine Informationen zu einem Nutzer erhalten dürfen, können das Pseudonym als Ergebnis einer erfolgreichen Nutzerauthentifizierung verwenden.                                                                                                                                  |
| iat   | Alle time Werte in Sekunden seit 1970, <a href="#">RFC 7519 Sect.2</a> , | 1773934200 = 19.03.2026 16:30:00        | Zeitpunkt, an dem das ID-Token vom sektoralen IDP ausgestellt wurde.                                                                                                                                                                                                                                                                                                                                 |
| exp   | Alle time Werte in Sekunden seit 1970, <a href="#">RFC 7519 Sect.2</a> , | 1773934500 = 19.03.2026 16:35:00        | Zeitpunkt, bis zu dem das vom sektoralen IDP ausgestellte ID-Token gültig ist.                                                                                                                                                                                                                                                                                                                       |
| aud   | URL                                                                      | "https://idpfadi.dev.gematik.solutions" | Die Audience ist die URL des Fachdienst Authorization Server, mit der dieser in der TI-Föderation registriert ist. Diese entspricht dem Attribut "iss" im Entity Statement des Fachdienst Authorization Server.                                                                                                                                                                                      |
| nonce | String                                                                   | vy7rM801AQw1or22GhrZ                    | Die "nonce" ist der vom Fachdienst Authorization Server ausgestellte Zufallswert, den dieser im Pushed Authorization Request als Parameter an den sektoralen IDP übergeben hat. Der Fachdienst Authorization Server vergleicht ausgegebene und empfangene "nonce" und stellt so sicher, dass der sektorale IDP das ID-Token ausgestellt hat, an den der Pushed Authorization Request gesendet wurde. |
| acr   | "gematik-                                                                | gematik-ehealth-loa-high                | Der claim "acr" gibt an, mit welcher Stärke                                                                                                                                                                                                                                                                                                                                                          |

|                                   |                                                          |                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------|----------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                   | ehealth-loa-high" oder "gematik-ehealth-loa-substantial" |                        | die Authentifizierung des Nutzers durchgeführt wurde. Der Wert des claims ist abhängig vom eingesetzten Authentisierungsmittel.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| amr                               | String                                                   | urn:telematik:auth:eID | <p>Der claim "amr" gibt an, mit welcher Authentisierungsmethode die Authentifizierung des Nutzers durchgeführt wurde. Authentisierungsmethoden sind beispielsweise</p> <ul style="list-style-type: none"> <li>• urn:telematik:auth:eID = online Ausweisfunktion</li> <li>• urn:telematik:auth:eGK = Authentifizierung mittels eGK und PIN</li> <li>• urn:telematik:auth:other = Authentifizierung mittels System-PIN oder Biometrie</li> </ul>                                                                                                                                                                                                                                            |
| urn:telematik:claims:profession   | String                                                   | 1.2.276.0.76.4.49      | <p>Das ID-Token enthält die claims mit Informationen zum Versicherten, welche vom Fachdienst Authorization Server im Puhed Authorization Request angefragt wurden. Wurde der claim "urn:telematik:versicherter" angefragt, so liefert das ID-Token die Versichertendaten</p> <ul style="list-style-type: none"> <li>• urn:telematik:claims:profession - Profession-ID (immer 1.2.276.0.76.4.49)</li> <li>• urn:telematik:claims:organization - Krankenversicherungsnummer des Versicherten (KVNR)</li> <li>• urn:telematik:claims:organization - IK-Nummer des Kostenträgers, bei dem der Versicherte versichert ist</li> </ul> <p>IK-Nummer der Kasse.<br/>Abhängig von Scope/Claims</p> |
| urn:telematik:claims:organization | String                                                   | X123456789             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| urn:telematik:claims:id           | String                                                   | 109500969              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

|                                   |        |                                       |                                                                                                                                                                                        |
|-----------------------------------|--------|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                   |        |                                       | Hier muss die KVNR rein<br>Abhängig von Scope/Claims                                                                                                                                   |
| urn:telematik:claims:display_name | String | Prof. Dr. Freiherr Max von Mustermann | Der claim "display_name" zeigt den vollständigen Namen des Versicherten an. Dieser besteht neben Vor- und Nachnamen auch aus akademischen Titeln sowie Vor- und Nachsatzbezeichnungen. |

## (12) Authorization Code für das Anwendungsfrontend

Erfolgt die Kommunikation zwischen dem Anwendungsfrontend, dem Authorization Server und der eigentlichen Anwendung eines Fachdienstes ebenfalls über OAuth, so erzeugt der Fachdienst Authorization Server nun einen eigenen Authorization Code (AUTHORIZATION\_CODE\_AS) und sendet diesen an das Anwendungsfrontend zum Einreichen beim Token Endpunkt des Fachdienst Authorization Server.

- Response

- HTTP-200

- Content-Type: application/json

```
{
  "code": "urn:https://idpfadi.dev.gematik.solutions:2f4c9dc66dcf350e",
  "state": "state_frontend"
}
```

Die Tabelle zeigt und erläutert die Attribute der Response vom Fachdienst Authorization Server mit dem Authorization Code

**Tabelle 19 : Response vom Fachdienst Authorization Server an den Fachdienst-Client (Authorization-Code-Flow)**

| Nam e | Werte  | Beispiel                 | Anmerkungen                                                                                                                                                                                                                                                                         |
|-------|--------|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| code  | String | xyz-authorizationcode-fd | Der Fachdienst Authorization Server erzeugt einen Authorization Code, den das Anwendungsfrontend des Fachdienstes beim Fachdienst Authorization Server gegen ein Access-Token eintauschen kann.                                                                                     |
| state | String | xyz-state_frontend       | Der state ist ein Zufallswert, den das Anwendungsfrontend des Fachdienstes bei initialen (OAuth) Request an den Fachdienst Authorization Server geschickt hat. Das Anwendungsfrontend prüft gesendeten und erhaltenen state-Parameter um sicherzustellen, dass die Response von der |



|  |  |  |                                                                          |
|--|--|--|--------------------------------------------------------------------------|
|  |  |  | Komponente kommt, an welche der initiale (oauth) Request gestellt wurde. |
|--|--|--|--------------------------------------------------------------------------|

### (13) Abruf des Access-Token

Das Anwendungsfrontend des Fachdienstes reicht den Authorization Code beim Token-Endpunkt des Fachdienst Authorization Server ein.

- Request zum Abruf des Access-Token beim Fachdienst Authorization Server durch das Anwendungsfrontend des Fachdienstes

POST /token

Host: redirect.testsuite.gsi

Content-Type: application/x-www-form-urlencoded

grant\_type=authorization\_code&code=eaf8NQ-IWG4a2eg535i-C5PXG6?

code\_verifier=cwYI3ZkRp0JXArqKPxKJGB7QK0uI-

EqFPqzjZhoZ441Q5yMFt8imhra8uS3Uwje67lVsBjStk1AYxL2AfysCdQZgTE\_2pXSwup

v84RCvXyHiMGshN0SAyLxc6k-LX2yX&client\_id=xyz\_fachdienstes\_frontend\_id

Die Tabelle zeigt und erläutert die Attribute zum Abruf des Access-Token am Fachdienst Authorization Server

**Tabelle 20 : Abruf des Access-Token am Fachdienst Authorization Server**

| Name       | Werte                | Beispiel                   | Anmerkungen                                                                                                                                                                         |
|------------|----------------------|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| grant_type | "authorization_code" | -                          | Bei der Kommunikation zwischen Fachdienst Authorization Server und Anwendungsfrontend wird Authorization Code Flow eingesetzt.                                                      |
| code       | String               | eaf8NQ-IWG4a2eg535i-C5PXG6 | Der vom Fachdienst Authorization Server erstellte Authorization Code, den das Anwendungsfrontend des Fachdienstes Authorization Server beim gegen ein Access-Token tauschen möchte. |

|               |        |                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                      |
|---------------|--------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| code_verifier | String | cwYI3ZkRp0JXArqKPxKJGB7QKoul-EqFPqzjZhoZ441Q5yMft8imhra8uS3UwjE67IVsBjStk1AYxL2AfysCdQZgTE_2pXSwupv84RCvXyHiMGshN0SAyLXc6k-LX2yX | Der Fachdienst Authorization Server muss aus dem Parameter code_verifier mit der code_challenge_method, die im initialen (oauth) Request übertragen wurde eine code_challenge berechnen. Diese muss mit der im initialen (oauth) Request übertragenen code_challenge übereinstimmen (PKCE).                                          |
| client_id     | String | "xyz_fachdients_frontend_id"                                                                                                     | Die client_id ein eindeutiger Identifier, mit dem das Anwendungsfrontend am Fachdienst Authorization Server registriert ist.                                                                                                                                                                                                         |
| redirect_uri  | URL    | "https://fadi.dev.gematik.solutions"                                                                                             | Optional kann der Token-Abruf eine redirect_uri ( <a href="https://www.rfc-editor.org/rfc/rfc6749.html#section-4.1.1">https://www.rfc-editor.org/rfc/rfc6749.html#section-4.1.1</a> / <a href="https://www.rfc-editor.org/rfc/rfc6749.html#section-4.1.3">https://www.rfc-editor.org/rfc/rfc6749.html#section-4.1.3</a> ) enthalten. |

#### (14) Ausgabe des Access-Tokens auf Fachdienst

Anwendungsfrontend erhält vom Fachdienst Authorization Server ein Access-Token. Das weitere kann der Fachdienst Authorization Server auch ein Refresh-Token ausstellen.

- Response
  - HTTP-200
  - Content-Type=application/json
  - Cache-Control=no-store

```
1418     • Pragma=no-cache
1419     • JSON
1420     {
1421         "access_token" :
1422         "f72f1if22ceh919ce621f7012hee98881d949g85",
1423         "token_type" : "Bearer",
1424         "expires_in" : 12000,
1425         "refresh_token" :
1426         "VXxl4axvYNPR8DxI8WE7WMJZA4Ga8gGq02HUAcz8Ax0"
1427     }
```

### (15) Verwendung des Access-Token

Greift das Anwendungsfrontend auf die Fachdienst API zu, so wird bei jedem Zugriff das Access-Token mitgegeben. Der Fachdienst validiert das Access Token und autorisiert den Zugriff.

- Request
    - POST /resource HTTP/1.1
- ```
1433     Authorization: Bearer f72f1if22ceh919ce621f7012hee98881d949g85
1434     Host: idpfadi.dev.gematik.solutions
```

## 6.2 Web2App-Flow

Der OAuth 2.0 Flow ist im Detail abhängig von der konkreten Anwendungsarchitektur. Die Spezifikation [OAuth 2.0 for Browser based APPs](#) unterscheidet hier drei mögliche Architekturansätze, mit unterschiedlichen Auswirkungen auf den OAuth 2.0 Flow und den damit verknüpften Bedingungen.

- Die Fälle [OAuth 2.0 for Browser based APPs - 6.1 \(BFF\)](#), [OAuth 2.0 for Browser based APPs - 6.2 \(Token mediating backend\)](#) müssen in unserer Betrachtung nicht unterschieden werden.
- Der Fall, dass eine Fachanwendung nur im Browser läuft ( [OAuth 2.0 for Browser based APPs - 6.3](#) ) - also eine reine Browseranwendung darstellt - wird nicht als relevanter UseCase für eine Anwendung des Gesundheitswesens mit Bedarf einer Nutzerauthentisierung betrachtet.

Bei Web-Anwendungen sollten auf Seiten des jeweiligen Fachdienstes die in [OAuth 2.0 Security Best Current Practice](#) beschriebenen Sicherheitsaspekte berücksichtigt werden.

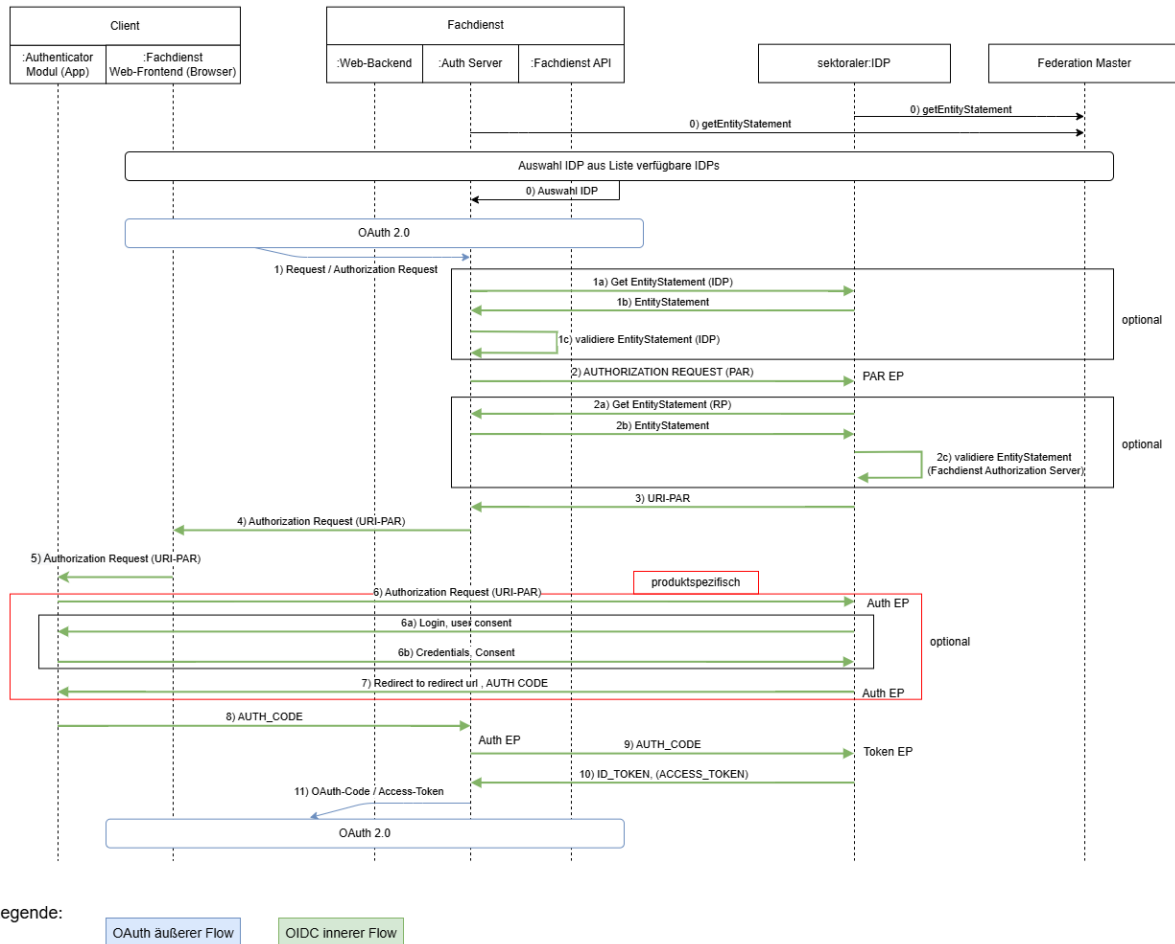
Der Ablauf des OIDC Flow ist prinzipiell identisch mit dem App-zu-App-Flow.

### 6.2.1 Vorbedingungen

- Registrierung des Fachdienst Authorization Server als RP in der TI-Föderation
- Registrierung des App-Link/Universal-Link für das Authenticator-Modul des sektoralen IDP auf dem Gerät des Nutzers (auf Adresse des sektoralen IDP) - oder Anfragen über Web.
- Der Fachdienst besitzt ein Web-Backend welches Anwendungslogik realisiert.

## 6.2.2 Flow - OIDC

### 6.2.2.1 Flow Diagramm



**Abbildung 9 : Ablauf Web2App-Flow**

### 6.2.2.2 Ablaufbeschreibung Web2App-Flow

**Tabelle 21 : Ablaufbeschreibung Web2App-Flow**

Schritt	Beschreibung
0	<ul style="list-style-type: none"> <li>Bezug des Entity Statement des Federation Master unter Nutzung des bekannten Signaturschlüssels "federation entity signing key". Fachdienst Authorization Server und sektoraler IDPs laden in regelmäßigen Abständen die aktuellen Entity Statements der Superior-Entities, bei denen sie als Teilnehmer der TI-Föderation registriert sind und validieren die Vertrauenskette ausgehend vom geladenen Entity Statement bis zum Vertrauensanker (Trust Anchor) der TI-Föderation.</li> <li>Auswahl des sektoralen IDP <ul style="list-style-type: none"> <li>Die Auswahl des richtigen sektoralen IDP ist optional. Ist der sektoraler IDP</li> </ul> </li> </ul>

		<p>bekannt (z.B. durch eine frühere Autorisierung) entfällt der Schritt</p> <ul style="list-style-type: none"> <li>Es gibt unterschiedliche Möglichkeiten den Ablauf der IDP-Ermittlung zu gestalten. Spätestens zum Schritt (1a) muss der Ziel-IDP bekannt sein</li> </ul>
1		Abweichend vom APP/APP-Flow kommt der Request vom Web-Backend der Anwendung und nicht von einem Anwendungsfrontend (App)
	1-a	Schnittstellendetails analog App-zu-App Flow (1a)
	1-b	Schnittstellendetails analog App-zu-App Flow (1b)
	1-c	Schnittstellendetails analog App-zu-App Flow (1c)
2		Schnittstellendetails analog App-zu-App Flow (2)
	2-a	Schnittstellendetails analog App-zu-App Flow (2a)
	2-b	Schnittstellendetails analog App-zu-App Flow (2b)
	2-c	Schnittstellendetails analog App-zu-App Flow (2c)
3		Schnittstellendetails analog App-zu-App Flow (3)
4		<p>Abweichend vom APP/APP-Flow läuft der Redirect über das Web-Backend zum Web-Frontend.</p> <p>Schnittstellendetails analog App-zu-App Flow (4)</p>
5		Schnittstellendetails analog App-zu-App Flow (5)
6		Schnittstellendetails analog App-zu-App Flow (6)
	6-a	Schnittstellendetails analog App-zu-App Flow (6a)
	6-b	Schnittstellendetails analog App-zu-App Flow (6b)
7		Schnittstellendetails analog App-zu-App Flow (7)

8		Abweichend vom APP/APP Flow führt das Authenticator Modul des sektoralen IDP den Redirect zum Fachdienst Authorization Server aus und übergibt den Authorization Code. Schnittstellendetails analog App-zu-App Flow (9)
9		Schnittstellendetails analog App-zu-App Flow (10)
10		Schnittstellendetails analog App-zu-App Flow (11)
11		Der Fachdienst Authorization Server reicht Access-Token und Refresh-Token an das Web-Backend der Anwendung weiter. Diese liegen zu keiner Zeit im Browser des Nutzers.
12		Der Access-Token (Refresh-Token) wird im Web-Backend der Anwendung persistiert. Die Kommunikation zwischen Web-Frontend und Web-Backend ist implementierungsspezifisch. Der Zugriff auf das Fachdienst-API erfolgt über das Web-Backend. Der Access-Token muss bei jedem Zugriff mitgegeben werden.

Schnittstellendetails analog App-zu-App Flow (10) Web-zu-App Flow

## 6.3 2-Geräte-Flow

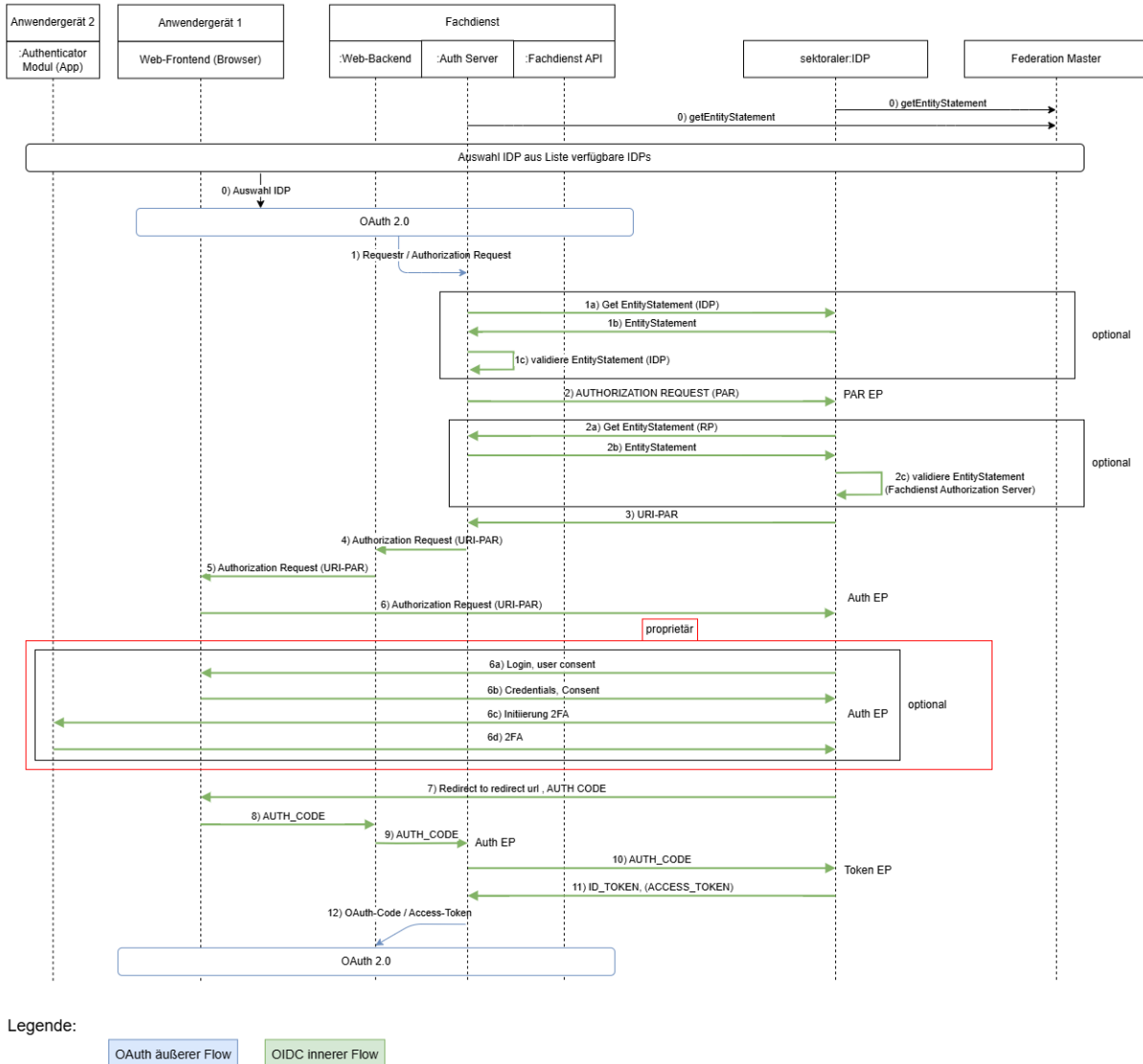
Der 2-Geräte-Flow bildet den Fall ab, wenn die Anwendungen, für die sich ein Nutzer authentifizieren muss, auf einem anderen Gerät läuft als die App mit dem Authenticator-Modul des sektoralen IDP.

### 6.3.1 Vorbedingungen

- Registrierung des Fachdienst Authorization Server als RP in der TI-Föderation
- Registrierung des App-Link/Universal-Link für das Authenticator-Modul des sektoralen IDP auf dem Gerät des Nutzers (auf Adresse des sektoralen IDP) - oder Anfragen über Web.
- Der Fachdienst besitzt ein Backend welches Anwendungslogik realisiert.
- Authenticator-Modul des sektoralen IDP (APP) läuft auf einem anderen Gerät als die Fachanwendung (z.B. App → Smartphone, Anwendung → PC-Browser)

## 6.3.2 Flow - OIDC

### 6.3.2.1 Flow Diagramm



**Abbildung 10 : Ablauf 2-Geräte-Flow**

### 6.3.2.2 Ablaufbeschreibung 2-Geräte-Flow

**Tabelle 22 : Ablaufbeschreibung 2-Geräte-Flow**

Schritt	Gerät	Beschreibung
0	1	<ul style="list-style-type: none"> <li>Bezug des Entity Statement des Federation Master unter Nutzung des bekannten Signaturschlüssels "federation entity signing key". Fachdienst Authorization Server und sektorale IDPs laden in regelmäßigen Abständen die aktuellen Entity Statements der Superior-</li> </ul>

			<p>Entities, bei denen sie als Teilnehmer der TI-Föderation registriert sind und validieren die Vertrauenskette ausgehend vom geladenen Entity Statement bis zum Vertrauensanker (Trust Anchor) der TI-Föderation.</p> <ul style="list-style-type: none"> <li>• Auswahl des sektoralen IDP <ul style="list-style-type: none"> <li>• Die Auswahl des richtigen sektoralen IDP ist optional. Ist der sektorale IDP bekannt (z.B. durch eine frühere Autorisierung) entfällt der Schritt</li> <li>• Es gibt unterschiedliche Möglichkeiten den Ablauf der IDP-Ermittlung zu gestalten. Spätestens zum Schritt (1a) muss der Ziel-IDP bekannt sein</li> </ul> </li> </ul>
1		1	Schnittstellendetails analog App-zu-App Flow (1)
	1-a		Schnittstellendetails analog App-zu-App Flow (1a)
	1-b		Schnittstellendetails analog App-zu-App Flow (1b)
	1-c		Schnittstellendetails analog App-zu-App Flow (1c)
2			Schnittstellendetails analog App-zu-App Flow (2)
	2-a		Schnittstellendetails analog App-zu-App Flow (2a)
	2-b		Schnittstellendetails analog App-zu-App Flow (2b)
	2-c		Schnittstellendetails analog App-zu-App Flow (2c)
3			Schnittstellendetails analog App-zu-App Flow (3)
4			Der Autorisierungsserver antwortet dem Web-Backend mit Request-URI und Client ID zur Weiterleitung über das Anwendungsfrontend an die Adresse des Authenticator des sektoralen IDP.
5		1	Das Web-Backend leitet den Redirect an das Anwendungsfrontend weiter.
6		1	Das Anwendungsfrontend öffnet die Web-Anwendung des sektoralen IDP für den Authentifikationsprozess.
	6a	1	Das Web-Frontend des IDP erfragt die Zugangsinformationen und ggf. Consent-Freigabe für die anfragende Anwendung beim Nutzer (1. Faktor, z.B. user/password)



	6b		Der Nutzer übermittelt seine Credentials an den sektoralen IDP.
	6c	2	Der sektorale IDP kann das Authenticator-Modul des IDP (z.B. 2FA) mit in den Prozess einbinden. Dazu sendet der sektorale IDP entweder eine push-Nachricht an die Authenticator-App oder fordert den Nutzer zum Start der Authenticator-App auf.
	6d		Der Nutzer tätigt die notwendigen Aktivitäten zur Authentifizierung über das Authenticator-Modul des sektoralen IDP.
7		1	Der Authorization-Endpunkt des IDP antwortet dem Aufruf des Anwendungsfrontend (Schritt 6) mit dem Authorization Code und einem Redirect zum Fachdienst.
8		1	Die Anwendungsfrontend leitet den Authorization Code an sein Web-Backend weiter.
9			Das Web-Backend leitet den Authorization Code an den Autorisierungsserver (redirected uri)
10			Schnittstellendetails analog App-zu-App Flow (10)
11			Schnittstellendetails analog App-zu-App Flow (11)
12		1	Schnittstellendetails analog Web-zu-App Flow (11)

## 6.4 Flow Desktop-Anwendung mit integriertem Authenticator-Modul

Für Anwendungen, die auf einem Desktop-PC laufen ist neben der Authentifizierung des Nutzers über den 2-Geräte-Flow auch eine Authentifizierung in der Desktop-Anwendung selbst möglich, wenn diese ein entsprechendes Authenticator-Modul implementiert. Diese Implementierung ist derzeit nur für ePA-Desktop-FdV umgesetzt. Die Authenticator-Module für die ePA-Desktop-FdV Anwendungen sind für alle gängigen Betriebssysteme verfügbar. Nutzer authentifizieren sich in diesen Fällen über angeschlossene Kartenleser mit ihrer eGK.

### 6.4.1 Vorbedingungen

- Registrierung des Fachdienst Authorization Server als RP in der TI-Föderation
- Authenticator Modul ist als Teil der Desktop Anwendung implementiert

## 6.4.2 Flow - OIDC

### 6.4.2.1 Flow Diagramm

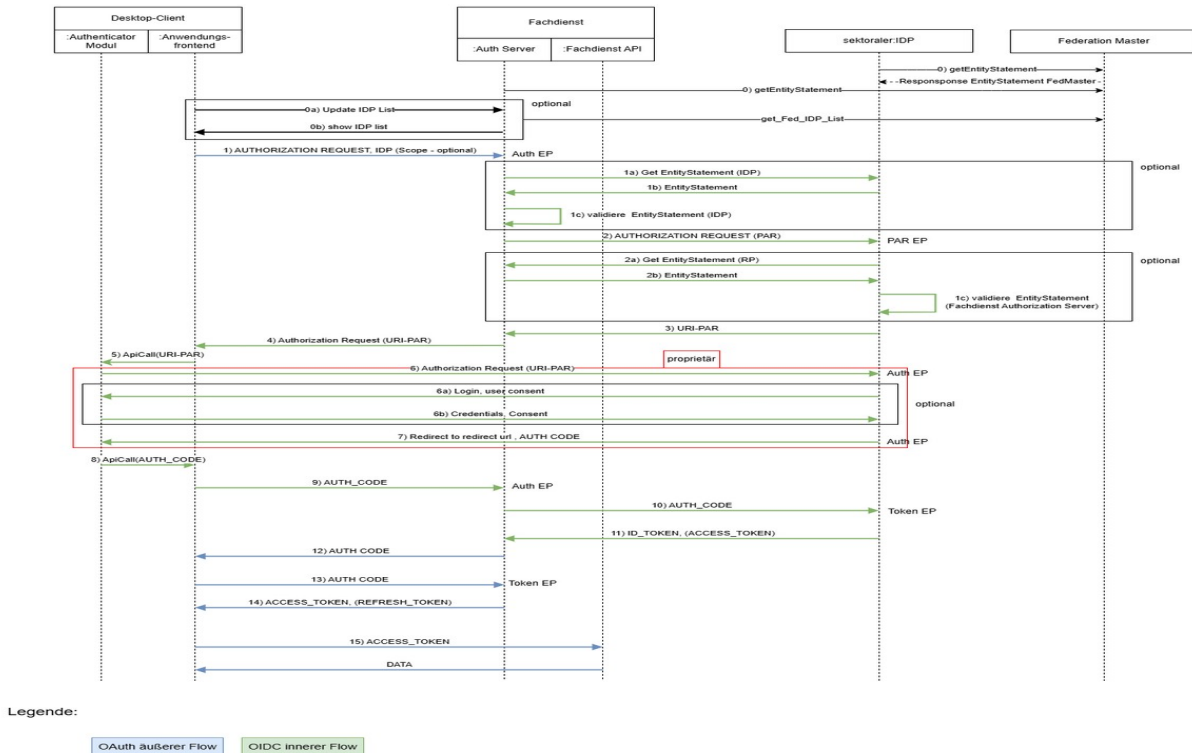


Abbildung 11 : Ablauf Desktop-App-Flow

### 6.4.2.2 Ablaufbeschreibung Desktop-App-Flow

Tabelle 23 : Ablaufbeschreibung Desktop-App-Flow

Schritt	Beschreibung
0	<ul style="list-style-type: none"> <li>Bezug des Entity Statement des Federation Master unter Nutzung des bekannten Signaturschlüssels "federation entity signing key". Fachdienst Authorization Server und sektorale IDPs laden in regelmäßigen Abständen die aktuellen Entity Statements der Superior-Entities, bei denen sie als Teilnehmer der TI-Föderation registriert sind und validieren die Vertrauenskette ausgehend vom geladenen Entity Statement bis zum Vertrauensanker (Trust Anchor) der TI-Föderation.</li> <li>Auswahl des sektoralen IDP <ul style="list-style-type: none"> <li>Die Auswahl des richtigen sektoralen IDP ist optional. Ist der sektorale IDP bekannt (z.B. durch eine frühere Autorisierung) entfällt der Schritt</li> <li>Es gibt unterschiedliche Möglichkeiten den Ablauf der IDP-Ermittlung zu gestalten. Spätestens zum Schritt (1a) muss der Ziel-IDP bekannt sein</li> </ul> </li> </ul>
1	Abweichend vom APP/APP-Flow kommt der Request vom Web-Backend der

		Anwendung und nicht von einem Anwendungsfrontend (App)
	1-a	Schnittstellendetails analog App-zu-App Flow (1a)
	1-b	Schnittstellendetails analog App-zu-App Flow (1b)
	1-c	Schnittstellendetails analog App-zu-App Flow (1c)
2		Schnittstellendetails analog App-zu-App Flow (2)
	2-a	Schnittstellendetails analog App-zu-App Flow (2a)
	2-b	Schnittstellendetails analog App-zu-App Flow (2b)
	2-c	Schnittstellendetails analog App-zu-App Flow (2c)
3		Schnittstellendetails analog App-zu-App Flow (3)
4		Schnittstellendetails analog App-zu-App Flow (4)
5		Anwendungsfrontend des Fachdienstes öffnet das Authenticator-Modul für die eigentliche Authentifizierung des Anwenders über einen API-Call mit der URI-PAR als Parameter in der Anwendung.
6		Schnittstellendetails analog App-zu-App Flow (6)
	6-a	Schnittstellendetails analog App-zu-App Flow (6a)
	6-b	Schnittstellendetails analog App-zu-App Flow (6b)
7		Schnittstellendetails analog App-zu-App Flow (7)
8		Das Authenticator Modul des sektoralen IDP ruft über einen API Call das Anwendungsfrontend des Fachdienstes auf und übergibt den authorization-code (IDP) und die Redirect-URL als Parameter.

9		Die Anwendungsfrontend des Fachdienstes sendet den Authorization Code an den Fachdienst Authorization Server.
9		Schnittstellendetails analog App-zu-App Flow (9)
10		Schnittstellendetails analog App-zu-App Flow (10)
11		Schnittstellendetails analog App-zu-App Flow (11)
12		Schnittstellendetails analog App-zu-App Flow (12)
13		Schnittstellendetails analog App-zu-App Flow (13)
14		Schnittstellendetails analog App-zu-App Flow (14)
15		Schnittstellendetails analog App-zu-App Flow (15)

1504

## 1505 6.5 Unterstützung Single-Sign-On auf Anwendungsebene

1506 Ein Single-Sign-On (SSO) auf Anwendungsebene bedeutet, dass sich der Nutzer innerhalb  
 1507 der Anwendung nur einmalig aktiv authentifizieren muss und dann auf jeden TI-  
 1508 Fachdienst zugreifen kann.

1509 Der Zugriff auf einem TI-Fachdienst aus einer Anwendung erfordert eigentlich jeweils eine  
 1510 aktive Authentifizierung des Nutzers. Allerdings ist unter bestimmten Voraussetzungen  
 1511 ein Single-Sign-On auf Anwendungsebene möglich:

- 1512 • Die Anwendung ist ein von der gematik zugelassenes FdV (z.B. ePA-FdV)
- 1513 • Der Nutzer hat eingewilligt, SSO für einen TI-Fachdienst zu nutzen

1514 Die Matrix zeigt ein Beispiel für eine Nutzerauthentifizierung mit SSO im ePA-FdV. In  
 1515 diesem Beispiel kann der Nutzer drei TI-Funktionen - E-Rezept, TI-Messenger und  
 1516 Patienten-Akte - und eine Kassen eigene Funktion aus dem ePA-FdV aufrufen. Allerdings  
 1517 hat in diesem Beispiel der Nutzer die Authentifizierung über SSO für das Öffnen seiner  
 1518 Patientenakte verweigert (will also beim Öffnen der Patientenakte eine aktive  
 1519 Authentifizierung durchführen).

1520 Das Single-Sign-On (SSO) ist spezifisch für eine Anwendung (ePA-FdV) und nicht  
 1521 übergreifend über weitere Anwendungen z.B. der E-Rezept App oder einer DiGA-App  
 1522 wirksam.

	Client-Modul im ePA FdV	Nutzerzustimmung liegt vor	Authorization Server im TI-Föderation Vertrauensraum	Authentifizierung über SSO
eRp Client-Modul (Funktion TI-Fachdienst)	erfüllt	erfüllt	erfüllt	möglich
TIM Client-Modul (Funktion TI-Fachdienst)	erfüllt	erfüllt	erfüllt	möglich
ePA Client-Modul (Funktion TI-Fachdienst)	erfüllt	nicht erfüllt	erfüllt	nicht möglich
spezifisches Client-Modul (Funktion Kassenanwendung)	erfüllt	erfüllt	nicht erfüllt	möglich
eRP-APP (Anwendung)	nicht erfüllt	nicht erfüllt	erfüllt	nicht möglich
DiGA (Anwendung)	nicht erfüllt	nicht erfüllt	erfüllt	nicht möglich

**Abbildung 12 : Beispiel Entscheidungsmatrix für SSO im ePA-FdV**

Beim Single-Sign-On (SSO) authentisiert sich der Nutzer spätestens beim Start des ersten TI-Fachdienstes der Anwendung einmalig gegenüber dem sektoralen IDP. Anschließend kann der Nutzer TI-Fachdienste (und Kassen spezifische Funktionen) innerhalb der Anwendung ohne weitere Interaktion zur Authentisierung für einen festgelegten Zeitraum nutzen. Der sektorale IDP stellt dabei sicher, dass jeder TI-Fachdienst seineigenes ID Token erhält.

Die fehlende Interaktion des Nutzers bei der Authentifizierung je TI-Fachdienst erfordert für ein SSO-Verfahren zusätzliche Sicherungsmaßnahmen zur Gewährleistung der Widerstandsfähigkeit gegen das vom Fachdienst geforderten Angriffspotentials.

Eine Möglichkeit der spezifikationskonformen Umsetzung ist die Verwendung einer vom sektoralen IDP generierten SessionID und eines an die Instanz des Anwendungskontext und die SessionID gebundenen Schlüsselpaares.

Informationen zu den SSO-Nutzerpräferenzen sowie zur Identifizierung der anfordernden Anwendung werden standardkonform als Request Parameter "authorization\_details[1]" (siehe [[RFC9396#name-request-parameter-authorization-details](#)], [[draft-ietf-oauth-rar-03.html#name-authorization-data-types](#)]) in den Authorization Requests mitgeteilt.

Ein Single-Sign-On ist aktuell nur für im ePA-FdV gebundene Fachdienste zulässig. Deshalb wird die Umsetzung anhand eines möglichen ePA-FdV mit integrierten TI-Anwendungen vorgestellt.

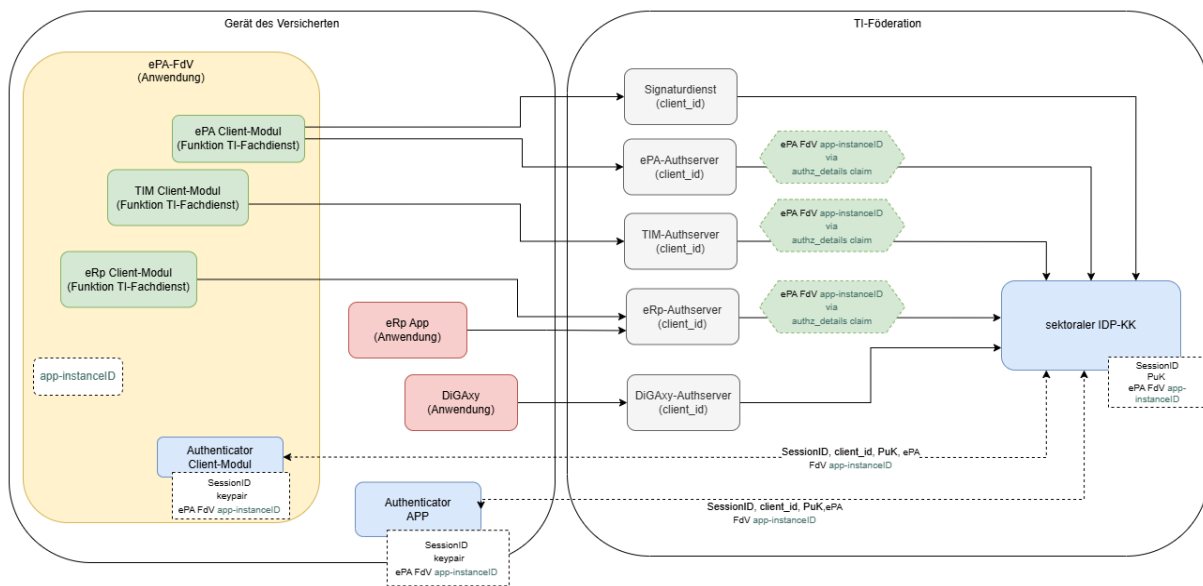


Abbildung 13 : ePA-FdV mit mehreren integrierten TI-Anwendungen

### 6.5.1 Prinzipieller Ablauf mit SessionID und Schlüsselpaar

**Beim ersten Funktionsaufruf auf einen TI-Fachdienst aus dem ePA-FdV durch den Nutzer**

- werden die im ePA-FdV erstellten SSO-Nutzerpräferenz für alle an das ePA-FdV gebundenen Fachdienste und eine eindeutig Instance-ID zur aufrufenden Instanz des ePA-FdV im Request Parameter "authorization\_details<sup>[1]</sup>" im Authorization Request an den Authorization Server übermittelt.
- werden die SSO-Nutzerpräferenz für alle an das ePA-FdV gebundenen Fachdienste und die eindeutig Instance-ID im Request Parameter "authorization\_details<sup>[1]</sup>" im Pushed Authorization Request an den sektoralen IDP übermittelt.
- muss sich der Nutzer über das Authenticator-Modul aktiv authentifizieren. Wenn in einer früheren Sitzung die Einwilligung noch nicht erklärt wurde, wird der Einwilligungsdialog für den TI-Fachdienst, zum Einholen der Einwilligung durch den Nutzer, geöffnet.
- wird die vom sektoralen IDP erstellte und übertragene SessionID vom Authenticator-Modul gespeichert.
- wird über Plattformmechanismen ein Schlüsselpaar im System eigenen Schlüsselspeicher erzeugt und an die laufende Instanz des ePA-FdV gebunden.
- wird die SessionID zum Authenticator-Modul mit dem PK des zugehörigen Schlüsselpaares signiert.
- wird der öffentliche Schlüssel des Schlüsselpaares und die signierte SessionID beim Authentifizierungsprozess dem sektoralen IDP übermittelt und dort an die ausgestellte Identität gebunden.
- erhält der TI-Fachdienst einen spezifischen einmaligen Authorization-Code.
- erhält der TI-Fachdienst ein fachdienst- und nutzerspezifisches ID Token und Access Token.

- bei APP-APP Konstellation wird die im Authorization Request (URI-PAR) in "authorization\_details<sup>[1]</sup>" übergebene eindeutige Instance-ID des ePA-FdV an SessionID gebunden, um sicherzustellen, dass die Authorization Requests immer vom diesem ePA-FdV kommen.

### Jeder weitere Funktionsaufruf auf einen Fachdienst aus der Anwendung

- wird die eindeutige Instance-ID zur aufrufenden Instanz des ePA-FdV im Request Parameter "authorization\_details<sup>[1]</sup>" im Authorization Request an den Authorization Server übermittelt.
- wird die eindeutige Instance-ID zur aufrufenden Instanz des ePA-FdV im Request Parameter "authorization\_details<sup>[1]</sup>" im Pushed Authorization Request an den sektoralen IDP übermittelt.
- wird vom Authenticator-Modul, über den im Authorization Request (URI-PAR) übergebene SSO-Parameter, geprüft, ob der Nutzer einem SSO für den relevanten Fachdienst zugestimmt hat.
- wird die SessionID zum Authenticator-Modul aus dem Speicher geladen.
- wird die SessionID zum Authenticator-Modul mit dem PK des zugehörigen Schlüsselpaars signiert.
- wird die signierte SessionID im Authorization Request an den IDP übertragen.
- erhält der TI-Fachdienst einen spezifischen einmaligen Authorization-Code.
- erhält der TI-Fachdienst eine fachdienst- und nutzerspezifisches ID Token (und Access Token).
- bei APP-APP Konstellation wird vom sektoralen IDP die im Authorization Request (URI-PAR) übergebene ePA-FdV Instance-ID gegen die der SessionID zugeordneten ePA-FdV Instance-ID geprüft.

### IN-APP-Konstellation vs. APP-APP-Konstellation

Die Varianten IN-APP (Authenticator-Modul ist in ePA-FdV integriert) und APP-APP (Authenticator-Modul als eigene APP neben dem ePA-FdV) unterscheiden sich ausschließlich durch den Aufruf und durch die eindeutige Zuordnung zu einem ePA-FdV.

In der APP-APP-Konstellation muss sichergestellt werden, dass die Authorization Request, die ein SSO erlauben, immer vom ePA-FdV kommen. Dazu wird die eindeutige ID der APP (ePA-FdV Instance-ID) im Authorization Request (URI-PAR) als Parameter an das Authenticator-Modul übergeben. Die Instance-ID muss dabei ein UUID V4 [<https://www.rfc-editor.org/rfc/rfc9562.html#name-uuid-version-4>] generierter Wert und unique für den Anwendungskontext sein. Die Instance-ID muss nach Beendigung der App (Beenden des Anwendungskontextes durch Nutzer oder Betriebssystem) ungültig sein. Der Anwendungskontext ist die Laufzeit des ePA-FdV vom Start bis zum Beenden auf dem Gerät des Nutzers.

**Tabelle 24: Unterschiede im Ablauf IN-APP-Konstellation vs. APP-APP-Konstellation**

Schritt im Ablauf	IN-APP	APP-APP

(5) Authorization Request (URI-PAR)	<ul style="list-style-type: none"> <li>• Aufruf erfolgt durch in-App-call</li> <li>• Zusätzlicher Parameter SSO=true/false</li> <li>• Zusätzlicher Parameter authorization_details[1] mit UserPreferenceSSO als authorization data type (siehe [<a href="#">RFC9396#name-request-parameter-authorization_details</a>], [<a href="#">draft-ietf-oauth-rar-03.html#name-authorization-data-types</a>])</li> </ul>	<ul style="list-style-type: none"> <li>• Aufruf erfolgt durch Plattform (deeplink/universal link)</li> <li>• Zusätzlicher Parameter <ul style="list-style-type: none"> <li>• SSO=true/false</li> <li>• ePA-FdV Instance-ID</li> </ul> </li> <li>• Zusätzlicher Parameter authorization_details[1] mit UserPreference SSO als authorization data type (siehe [<a href="#">RFC9396#name-request-parameter-authorization_details</a>], [<a href="#">draft-ietf-oauth-rar-03.html#name-authorization-data-types</a> ])</li> </ul>
(6b) Authentifizierung		Speicherung bzw. Überprüfung der ePA-FdV Instance-ID zur SessionID
(8) Rückgabe authcode	Die Rückgabe des vom IDP ausgestellten authcode erfolgt als Response auf den in-App-call (5)	Die Rückgabe des vom IDP ausgestellten authcode erfolgt durch Plattform (deeplink/universal link)

1612



## 6.5.2 SSO-Unterstützung auf Anwendungsebene innerhalb einer APP

Das Authenticator-Modul ist in das ePA-FdV integriert.

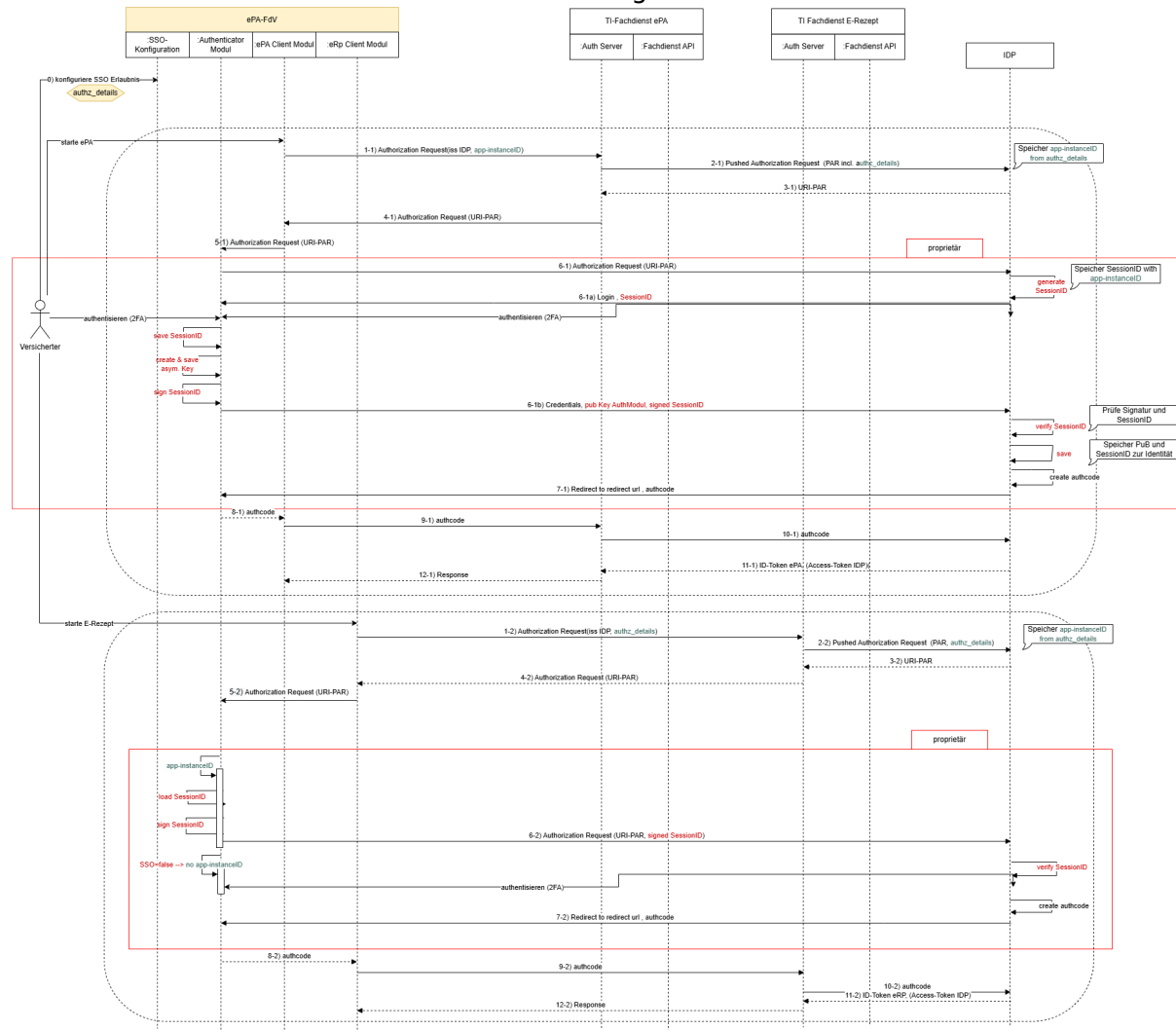
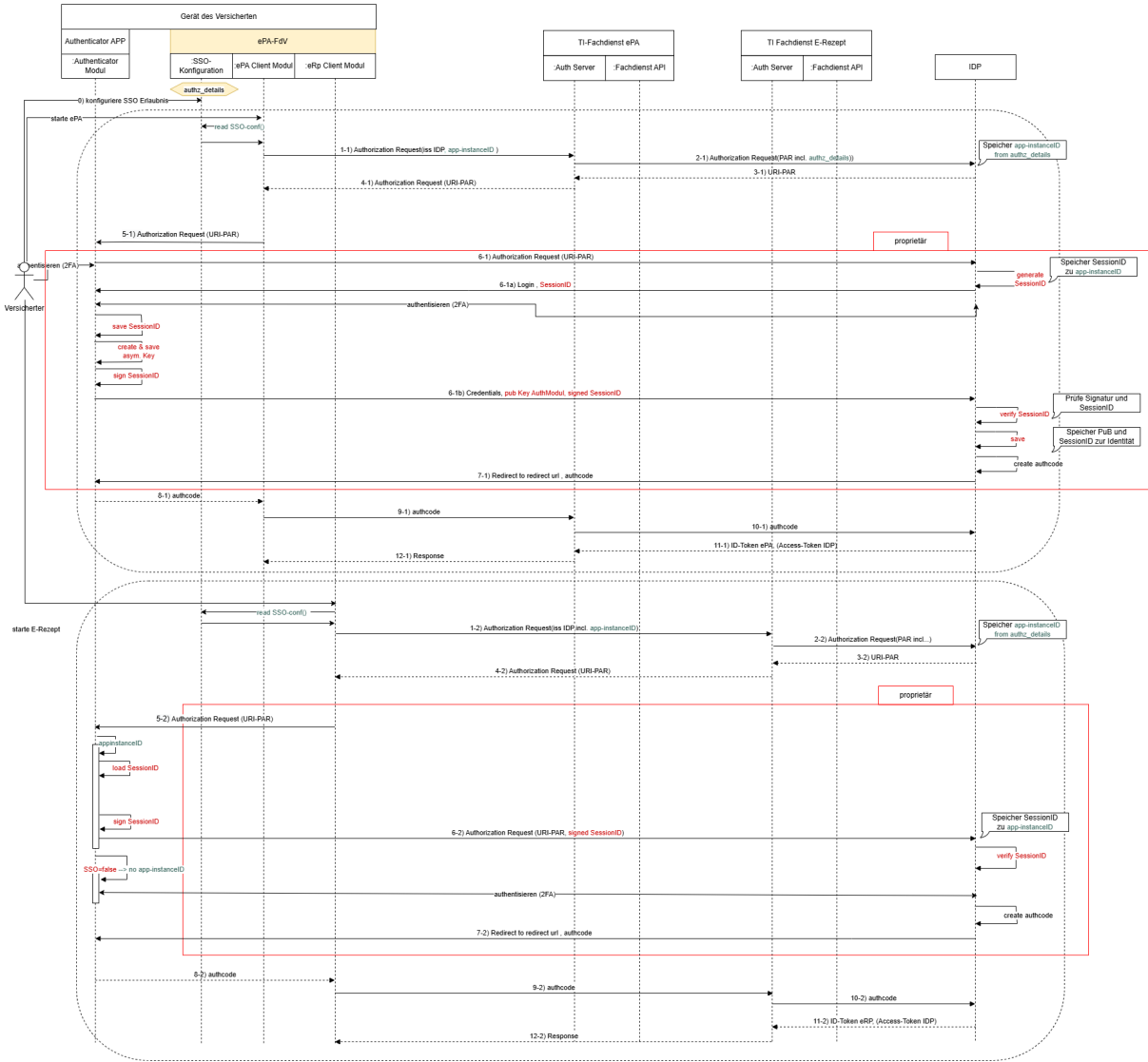


Abbildung 14: Beispiel für SSO bei Ausführung ePA Client Modul mit aktiver und E-Rezept Client Modul ohne aktive Nutzerauthentisierung aus dem ePA-FdV mit integriertem Authenticator-Modul

## 6.5.3 SSO-Unterstützung auf Anwendungsebene bei separater Authenticator-APP

Das Authenticator-Modul ist als eigene App implementiert.



**Abbildung 15: Beispiel für SSO bei Ausführung ePA Client Modul mit aktiver und E-Rezept Client Modul ohne aktive Nutzerauthentisierung aus dem ePA-FdV mit Authenticator-Modul in separater APP**

### 6.5.4 Ablaufbeschreibung SSO-Flow

**Tabelle 25: Ablauf der Aufrufe der TI-Client Module aus dem ePA-FdV**

Schritt	Teilschritt	"In-App-Authenticator-Modul"	"externe-Authenticator-Modul APP"
---------	-------------	------------------------------	-----------------------------------

0		Der Versicherte kann sich über eine Funktion die im ePA-FdV integrierten TI-Funktionen anzeigen lassen. Bei jeder dieser Funktionen kann der Versicherte entscheiden, ob eine Nutzerauthentisierung über SSO erlaubt ist. Die Einstellung sind durch den Nutzer jederzeit änderbar.	wie "In-App-Authenticator-Modul"
1	1-1 erstmaliger Aufruf eines TI-Fachdienstes aus dem ePA-FdV	<p>Der Versicherte möchte den TI-Fachdienst (TI-Fachdienst Client Modul) über die Oberfläche des ePA-FdV starten. Das ePA-FdV muss den Versicherten für die Nutzung des TI-Fachdienstes autorisieren. Dazu sendet das FdV des Fachdienstes einen Authorization Request an den Authorization Server des TI-Fachdienstes.</p> <p>Der Authorization Request wird um Request Parameter <code>authorization_details<sup>[1]</sup></code> erweitert und enthält:</p> <ul style="list-style-type: none"> <li>Die vom Nutzer im ePA-FdV hinterlegten SSO-Präferenzen hinsichtlich der TI-Anwendungen, die aus dem PA-FdV ausführbar sind mit: <ul style="list-style-type: none"> <li><code>client_id</code> (Claim iss aus dem Entity Statement des Fachdienstes)</li> <li>name des TI-Fachdienstes (Claim <code>client_name</code> aus dem Entity Statement des Fachdienstes)</li> </ul> </li> <li>Eine eindeutige Instance-ID des ePA-FdV</li> </ul>	wie "In-App-Authenticator-Modul"
	1-2 weiterer Aufruf eines TI-Fachdienstes aus dem ePA-FdV	analog (1-1)	wie "In-App-Authenticator-Modul"

2	2-1 erstmaliger Aufruf eines TI-Fachdienstes aus dem ePA-FdV	<p>Der Authorization Server des TI-Fachdienstes muss vor der Nutzerautorisierung diesen authentisieren und sendet dazu einen Pushed-Authorization-Request an den sektoralen IDP der Krankenkasse des Versicherten.</p> <p>Der Pushed Authorization Request wird um Request Parameter <code>authorization_details</code><sup>[1]</sup> erweitert und enthält:</p> <ul style="list-style-type: none"> <li>Die vom Nutzer im ePA-FdV hinterlegten SSO-Präferenzen hinsichtlich der TI-Anwendungen, die aus dem PA-FdV ausführbar sind mit: <ul style="list-style-type: none"> <li><code>client_id</code> (Claim <code>iss</code> aus dem Entity Statement des Fachdienstes)</li> <li>name des TI-Fachdienstes (Claim <code>client_name</code> aus dem Entity Statement des Fachdienstes)</li> </ul> </li> <li>Eine eindeutige Instance-ID des ePA-FdV</li> </ul>	wie "In-App-Authenticator-Modul"
	2-2 weiterer Aufruf eines TI-Fachdienstes aus dem ePA-FdV	analog (2-1)	wie "In-App-Authenticator-Modul"
3	3-1 erstmaliger Aufruf eines TI-Fachdienstes aus dem ePA-FdV	Der sektoralen IDP der Krankenkasse antwortet dem Authorization Server des TI-Fachdienstes mit HTTP-200 und einer URI, welche zur Durchführung der Nutzerauthentisierung aufgerufen werden muss (URI-PAR).	wie "In-App-Authenticator-Modul"
	3-2 weiterer Aufruf eines TI-Fachdienstes aus dem ePA-FdV	analog (3-1)	wie "In-App-Authenticator-Modul"
4	4-1 erstmaliger Aufruf eines TI-Fachdienstes aus dem ePA-FdV	Der Autorisierungsserver des Fachdienstes sendet die Request-URI und Client_ID zurück an das TI-Fachdienst FdV Modul im ePA-FdV zur Weiterleitung an das Authenticator-Modul des sektoralen IDP der Krankenkasse.	wie "In-App-Authenticator-Modul"

	4-2 weiterer Aufruf eines TI-Fachdienstes aus dem ePA-FdV	analog (4-1)	wie "In-App-Authenticator-Modul"
5	5-1 erstmaliger Aufruf eines TI-Fachdienstes aus dem ePA-FdV	<p>Das ePA-FdV öffnet das Authenticator-Modul für die eigentliche Authentifizierung des Anwenders über den Aufruf eine API-Schnittstelle das Authenticator-Modul für die Ein-App-SSO Integration.</p> <p>An der Schnittstelle werden diese Informationen übergeben:</p> <ul style="list-style-type: none"> <li>SSO soll ausgeführt werden, wenn möglich</li> <li>Instance-ID des laufenden ePA-FdV</li> </ul>	<p>Das ePA-FdV sendet den URI-PAR Authorization Request und ergänzt folgende Request Parameter (z.B. "authorization_details" oder als Parameter):</p> <ul style="list-style-type: none"> <li>SSO soll ausgeführt werden, wenn möglich</li> <li>Instance-ID des laufenden ePA-FdV</li> </ul>
	5-2 weiterer Aufruf eines TI-Fachdienstes aus dem ePA-FdV	analog (5-1)	analog (5-1)
6a	6-1a erstmaliger Aufruf eines TI-Fachdienstes aus dem ePA-FdV	<p>Das Authenticator-Modul prüft, ob eine SessionID zum laufenden Authenticator-Dienst im Gerät gespeichert ist. Da dies beim ersten Aufruf nicht der Fall ist, sendet das Authenticator-Modul den Authentication Request an seinen sektoralen IDP der Krankenkasse und übergibt als zusätzliche Request Parameter (z.B. als "authorization_details" oder als Parameter):</p> <ul style="list-style-type: none"> <li>SSO soll ausgeführt werden, wenn möglich</li> <li>Instance-ID des laufenden ePA-FdV</li> </ul>	wie "In-App-Authenticator-Modul"
	6-2a weiterer Aufruf eines TI-Fachdienstes aus dem ePA-FdV	<p>Das Authenticator-Modul:</p> <ul style="list-style-type: none"> <li>prüft, ob eine SessionID zum laufenden Authenticator-Dienst im Gerät gespeichert ist</li> <li>lädt die SessionID</li> <li>signiert die SessionID mit dem PK des Schlüsselpaares, welches zum Authenticator-Dienst angelegt wurde (siehe 6-1b)</li> <li>sendet den Authentication Request an seinen sektoralen IDP der Krankenkasse und übergibt als zusätzliche Request Parameter (z.B. als "authorization_details" oder als</li> </ul>	wie "In-App-Authenticator-Modul"

		<p>Parameter):</p> <ul style="list-style-type: none"> <li>• SSO soll ausgeführt werden, wenn möglich</li> <li>• Instance-ID des laufenden ePA-FdV</li> <li>• signierter SessionID</li> </ul>	
6b	6-1b erstmaliger Aufruf eines TI-Fachdienstes aus dem ePA-FdV	<p>Im Rahmen der Nutzerauthentisierung:</p> <ul style="list-style-type: none"> <li>• erzeugt der sektorale IDP der Krankenkasse eine eindeutig SessionID</li> <li>• bindet die Instance-ID an die SessionID</li> <li>• übergibt dieser die SessionID dem aufrufenden Authenticator-Modul</li> <li>• wird durch Plattformmechanismen auf dem Gerät des Versicherten ein Schlüsselpaar im System eigenen Schlüsselspeicher erzeugt und an die SessionID gebunden</li> <li>• sendet das Authenticator-Modul den öffentlichen Schlüssel des Schlüsselpaares (PuB) und die signierte SessionID an sektorale IDP der Krankenkasse.</li> </ul> <p>Nach erfolgreicher Nutzerauthentisierung bzw. Prüfung der Credentials durch den sektorale IDP der Krankenkasse:</p> <ul style="list-style-type: none"> <li>• validiert der sektorale IDP der Krankenkasse die Signatur der übergebenen SessionID mit dem übergebenen öffentlichen Schlüssel</li> <li>• prüft der sektorale IDP die vom Authenticator-Modul übergebene gegen die vom sektorale IDP erzeugte SessionID</li> <li>• speichert der sektorale IDP den öffentlichen Schlüssel und SessionID zur Nutzeridentität</li> <li>• erzeugt der sektorale IDP einen Authorization Code</li> </ul>	wie "In-App-Authenticator-Modul"

	6-2b weiterer Aufruf eines TI-Fachdienstes aus dem ePA-FdV	<p>Prüfung der Credentials durch den sektoralen IDP der Krankenkasse:</p> <ul style="list-style-type: none"> <li>validiert der sektoralen IDP der Krankenkasse die Signatur der übergebenen SessionID mit dem öffentlichen Schlüssel, den er zur SessionID gespeichert hat</li> <li>prüft der sektorale IDP die vom Authenticator-Modul übergebene gegen die vom sektoralen IDP erzeugte SessionID</li> <li>prüft der sektorale IDP, ob die übergebene Instance-ID mit der zur SessionID gespeicherten Instance-ID passt</li> <li>prüft der sektorale IDP, ob der Nutzer einem SSO für den anfragenden Fachdienst zugestimmt hat.</li> </ul> <p>Schlägt einer der Prüfungen fehl. so wird eine Nutzerauthentifizierung mit aktiver Beteiligung des Nutzers erzwungen.</p> <p>Nach erfolgreicher Authentifizierung (SSO oder aktiv)</p> <ul style="list-style-type: none"> <li>erzeugt der sektorale IDP einen Authorization Code</li> </ul>	wie "In-App-Authenticator-Modul"
7	7-1 erstmaliger Aufruf eines TI-Fachdienstes aus dem ePA-FdV	der sektorale IDP der Krankenkasse antwortet dem Authenticator-Modul auf dessen Authentication Request (6-1a, 6-2a) mit dem mit dem Authorization Code und einem Redirect zum Autorisierungsserver des TI-Fachdienstes.	wie "In-App-Authenticator-Modul"
	7-2 weiterer Aufruf eines TI-Fachdienstes aus dem ePA-FdV	analog (7-1)	wie "In-App-Authenticator-Modul"
8	8-1 erstmaliger Aufruf eines TI-Fachdienstes aus dem ePA-FdV	Das Authenticator-Modul des IDP antwortet auf den API-Aufruf (Schritt 5) und übergibt in der Antwort dem TI-Fachdienst FdV Modul im ePA-FdV die Redirect-URL und den Authorization Code.	Das Authenticator-Modul antwortet auf den Authorization Request (Schritt 5) mit einem Redirect an die Redirect-URL mit dem Authorization Code als Parameter

	8-2 weiterer Aufruf eines TI-Fachdienstes aus dem ePA-FdV	analog (8-1)	analog (8-1)
9	9-1 erstmaliger Aufruf eines TI-Fachdienstes aus dem ePA-FdV	Das TI-Fachdienst FdV Modul im ePA-FdV ruft die Redirect-URL mit dem Authorization Code als Parameter beim Autorisierungsserver des TI-Fachdienstes auf.	wie "In-App-Authenticator-Modul"
	9-2 weiterer Aufruf eines TI-Fachdienstes aus dem ePA-FdV	analog (9-1)	wie "In-App-Authenticator-Modul"
10	10-1 erstmaliger Aufruf eines TI-Fachdienstes aus dem ePA-FdV	Der Autorisierungsserver des TI-Fachdienstes reicht den Authorization Code beim Token-Endpunkt des IDP ein.	wie "In-App-Authenticator-Modul"
	10-2 weiterer Aufruf eines TI-Fachdienstes aus dem ePA-FdV	analog (10-1)	wie "In-App-Authenticator-Modul"
11	11-1 erstmaliger Aufruf eines TI-Fachdienstes aus dem ePA-FdV	Der Autorisierungsserver des TI-Fachdienstes erhält vom Token-Endpunkt des IDP einen ID Token mit den gewünschten Claims welches mit dem öffentlichen Schlüssel aus der Registrierung verschlüsselt ist. Der Autorisierungsserver des TI-Fachdienstes entschlüsselt das ID Token, prüft den Herausgeber, validiert die Signatur des ID Token gegen den zurkid passenden Schlüssel aus den JWKS des sektoralen IDP und zieht die Claims (d. h. die Key/Value-Paare im Payload eines Tokens) der authentisierten Identität aus dem ID Token.	wie "In-App-Authenticator-Modul"
	11-2 weiterer Aufruf eines TI-Fachdienstes aus dem ePA-FdV	analog (11-1)	wie "In-App-Authenticator-Modul"



12	12-1 erstmaliger Aufruf eines TI-Fachdienstes aus dem ePA-FdV	Der Autorisierungsserver des TI-Fachdienstes sendet die Autorisierung für den Versicherten an das TI-Fachdienst FdV Modul im ePA-FdV (z.B. als wiederum beim Autorisierungsserver einzulösenden Authorization Code oder als Access Token).	wie "In-App-Authenticator-Modul"
	12-2 weiterer Aufruf eines TI-Fachdienstes aus dem ePA-FdV	analog (12-1)	wie "In-App-Authenticator-Modul"

<sup>[1]</sup> [A\_23208\*] aus [gemSpec\_IDP\_Sek] und [A\_23209\*], [A\_25047\*] aus [gemSpec\_ePA\_FdV] fordern jeweils das Einholen der Nutzerzustimmung für ein SSO. In Abstimmung mit dem BSI muss der Nutzerkonsent nicht über das ePA-FdV und das Authenticator-Modul eingeholt werden (siehe auch [[FAQ Eintrag zu "doppeltes Einholen des SSO-Konsent" in der IDP Wissensdatenbank](#)]). In der aktuellen Umsetzung wird die Nutzerzustimmung über das ePA-FdV eingeholt. Perspektivisch sollen jedoch die Nutzerpräferenzen im Authenticator-Modul gepflegt werden. Für einen Übergangszeit wird deshalb der Parameter `authorization_details` nicht benötigt.

## 7 Betriebliche Aspekte

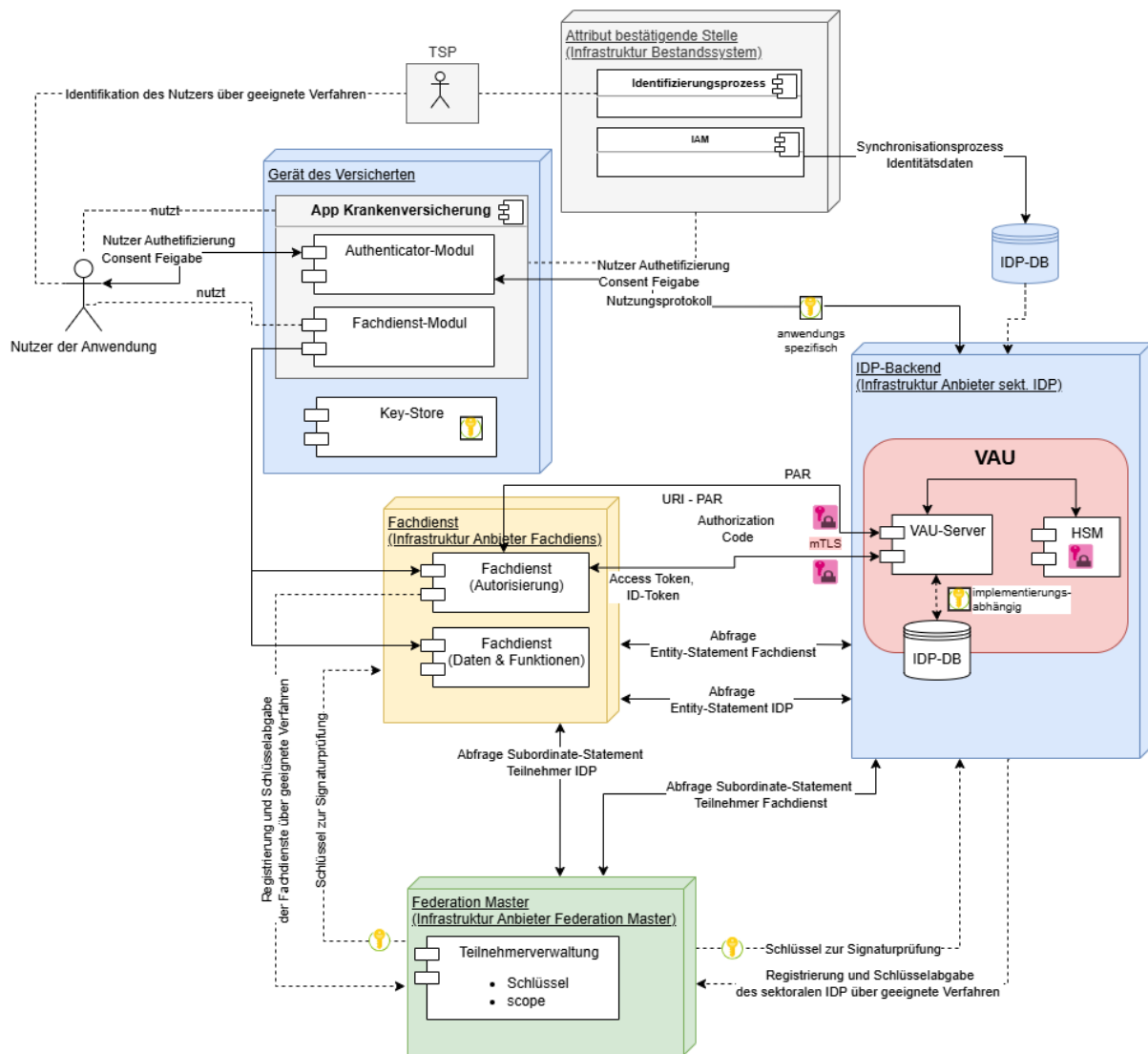


Abbildung 16 : Deploymentview TI-Föderation

### 7.1 Verfügbarkeiten

#### 7.1.1 Sektorale IDPs

Unabhängig vom Fachdienst ist bei jeder Nutzerauthentifizierung mit GesundheitsID der sektorale IDP involviert. Die Nutzung von TI-Fachdiensten über mobile Endgeräte soll für Versicherte 24x7 möglich sein. Eine Nutzerauthentifizierung mit GesundheitsID muss eine demensprechend hohe Ausfallsicherheit gewährleisten. Daraus ergeben sich folgerichtig

1651 Anforderungen an Georedundanz und Wiederherstellungszeiten (siehe auch Kapitel "9  
1652 Qualitätsszenarien").

### 1653 **7.1.2 Federation Master**

#### 1654 **7.1.2.1 TI-Trust Anchor**

1655 Der TI-Trust Anchor stellt Schnittstellen zur Abfrage von Subordinate-Statements,  
1656 historical Keys und der Liste der registrierten sektoralen IDP bereit. Diese Abfragen  
1657 erfolgen bei den Teilnehmern nicht bei jedem Authentifizierungsprozess sondern einmal  
1658 täglich. Die abgefragten Informationen können 24h durch die Teilnehmer gecached. Die  
1659 Anforderungen an die Verfügbarkeit des TI-Trust Anchor können entsprechend dieser  
1660 Rahmenbedingungen gestaltet werden.

#### 1661 **7.1.2.2 Intermediate Entities**

1662 Intermediate Entities stellen Schnittstellen zur Abfrage von Subordinate-Statements und  
1663 Trust Marks bereit. Die Anforderung an Verfügbarkeit richtet sich nach den fachlichen  
1664 Anwendungsfällen und müssen entsprechend bei Design der Intermediate Entities  
1665 berücksichtigt werden.

### 1666 **7.1.3 Fachdienst Authorization Server**

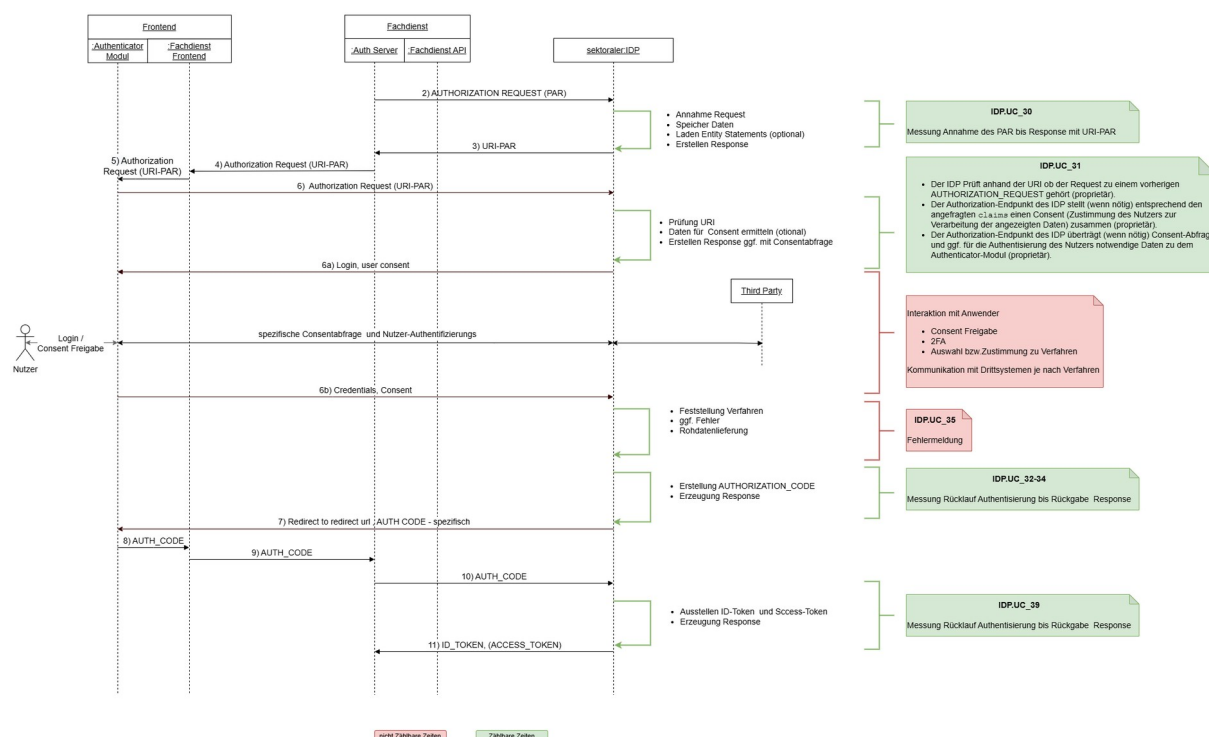
1667 Anforderungen an Verfügbarkeit von Fachdienst Authorization Server richtet sich nach  
1668 den fachlichen Anwendungsfällen und müssen entsprechend bei Design der Fachdienst  
1669 Authorization Server berücksichtigt werden.

## 1670 **7.2 Bearbeitungszeiten**

### 1671 **7.2.1 Sektorale IDPs**

1672 Das Monitoring der sekt. IDPs umfasst die Verarbeitungszeit innerhalb der sektoralen IDPs  
1673 aufgrund eingehender Requests. An die unterschiedlichen Requests (Use-Cases) werden  
1674 betrieblich Anforderungen zur Performance gestellt.

## Konzept TI-Föderation



**Abbildung 17 : Messpunkte der Bearbeitungszeiten sekt. IDPs**

**Tabelle 26: Use-Cases für Bearbeitungszeitvorgaben sektorale IDPs**

ID	Anwendungsfälle	Anwendungsfälle	
		IDP.UC_30	Processing of Pushed Authorization Requests
IDP.UC_31	Processing of Authorization Requests (alle Authentisierungsverfahren)		
IDP.UC_32, IDP.UC_33 IDP.UC_34	Response of Authorization Requests (mit online Ausweisfunktion) Response of Authorization Requests (mit eGK und PIN) Response of Authorization Requests (alternatives Authentisierungsverfahren)		
IDP.UC_35	Response of Authorization Requests (Gast-Login mit eGK und PIN)		
IDP.UC_39	Token Requests		

## 7.2.2 Federation Master

### 7.2.2.1 TI-Trust Anchor

Das Monitoring des TI-Trust Anchor umfasst die Verarbeitungszeit innerhalb des TI-Trust Anchor aufgrund eingehender Requests. An die unterschiedlichen Requests (Use-Cases) werden betrieblich Anforderungen zur Performance gestellt.

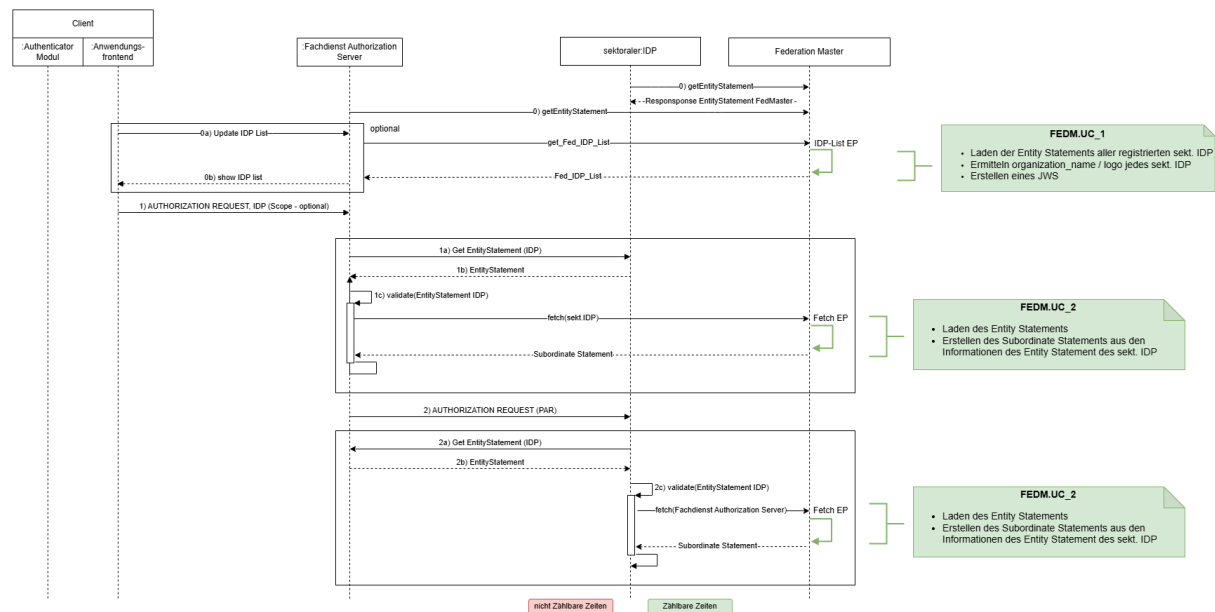


Abbildung 18 : Messpunkte der Bearbeitungszeiten Trust Anchor

Tabelle 27: Use-Cases für Bearbeitungszeitvorgaben Federation Master

ID	Anwendungsfälle		
		FEDM.UC_1	IDP-Liste bereitstellen
FEDM.UC_2	Subordinate Statement bereitstellen		

### 7.2.2.2 Intermediate Entities

Anforderungen an Performance der Intermediate Entities richtet sich nach den fachlichen Anwendungsfällen und müssen entsprechend bei Design der Intermediate Entities berücksichtigt werden.

## 7.2.3 Fachdienst Authorization Server

Anforderungen an Performance der Fachdienst Authorization Server richtet sich nach den fachlichen Anwendungsfällen und müssen entsprechend bei Design der Intermediate Entities berücksichtigt werden.

---

## 8 Querschnittsliche Konzepte

---

Die TI-Föderation setzt auf folgende Konzepte der Telematik-Infrastruktur auf:

- gemSpec\_Perf
- gemKPT\_Betr
- gemKPT\_Test
- gemSpec\_DS\_Hersteller
- gemSpec\_Krypt
- gemSpec\_OM
- gemSpec\_PKI
- gemSpec\_Systemprozesse\_dezTI

## 9 Qualitätsszenarien

**Tabelle 28 : Qualitätskriterien**

#	Qualitätsszenario
<b>Funktional</b>	
F.1	Die gesetzlichen Anforderungen nach §291 Absatz 8 Satz 1 SGB V sind umgesetzt
F.2	Die gesetzlichen Anforderungen nach §340 Absatz 6 Satz 1 SGB V sind umgesetzt
F.3	Die gesetzlichen Anforderungen nach §340 Absatz 7 Satz 1 SGB V sind umgesetzt
<b>Sicherheit</b>	
S.1	Kommunikation nur mit bekannten Kommunikationspartner: Die Kommunikation zwischen Teilnehmern der TI-Föderation muss kryptografisch abgesichert sein. Sektorale IDPs müssen prüfen, ob Anfragen von vertrauenswürdigen Clients kommen. Fachdienst Authorization Server müssen prüfen, ob Informationen zu Identitäten von vertrauenswürdigen Identity Providern ausgestellt werden.
S.2	Schutz vor Registrierung von malicious Anwendungen in der TI-Föderation: Es muss sichergestellt werden, dass Anwendungen von vertrauenswürdigen Herstellern über den Registrierungsprozess in der TI-Föderation registriert werden.
S.IDP.1	Sichere Schlüsselerzeugung und Ablage: Es muss sichergestellt werden, dass Schlüssel zur Signatur der Entity Statement und zur Verschlüsselung und Signatur von ID-Token sicher erzeugt und abgelegt werden.
S.IDP.2	Die ausgestellten ID-Token müssen manipulationssicher an die anfragende Relying Party übertragen.
S.IDP.3	Die ausgestellten ID-Token dürfen nur die Identitätsinformationen enthalten, für die eine anfragenden Relying Party erhalten darf
S.IDP.4	Die bei der Installation der Authenticator-App eingerichtete Gerätebindung muss, je nach Ausstattung der mobilen Endgeräte der Versicherten, regelmäßig durch ein Re-Ident erneuert werden.
<b>Performance</b>	
P.FM.1	Der TI Trust Anchor muss für ihre Anwendungsfälle FEDM.UC_1 und FEDM.UC_2 die Lastvorgaben nach [gemSpec_Perf] einhalten.
P.FM.2	Der TI Trust Anchor muss für ihre Anwendungsfälle FEDM.UC_1 und FEDM.UC_2 die Performancevorgaben nach [gemSpec_Perf] einhalten.
P.IDP.1	Sektorale IDPs müssen für ihre Anwendungsfälle IDP.UC_30 - IDP.UC_35, IDP.UC_39 die Lastvorgaben nach [gemSpec_Perf] einhalten.

P.IDP.2	Sektorale IDPs müssen für ihre Anwendungsfälle IDP.UC_30 - IDP.UC_35, IDP.UC_39 die Performancevorgaben nach [gemSpec_Perf] einhalten.
<b>Kompatibilität</b>	
K.1	Kompatibilität durch standard konforme Implementierung - Teilnehmer der TI-Föderation müssen sicherstellen, dass ihre Implementierungen konform zu den zugrunde liegenden Standards ist. der
K.FM.1	In Umgebungen zum Testen der Kompatibilität aller Komponenten der TI-Föderation muss für die jeweilige Umgebung ein eigener TI Trust Anchor zur Verfügung stehen.
K.FM.2	In Umgebungen zum Testen der Kompatibilität aller Komponenten der TI-Föderation muss für die jeweilige Umgebung ein eigener TI Trust Chain Resolver zur Verfügung stehen.
K.IDP.1	In Umgebungen zum Testen der Kompatibilität aller Komponenten der TI-Föderation muss jeder sektorale IDP eine Testinstanz für die jeweilige Umgebung zur Verfügung stellen.
<b>Verlässlichkeit</b>	
V.FM.1	Der TI Trust Anchor muss die in [gemSpec_Perf] festgelegten Vorgaben für den Federation Master zur Verfügbarkeit einhalten.
V.IDP.1	Sektorale IDPs müssen die in [gemSpec_Perf] festgelegten Vorgaben zur Verfügbarkeit einhalten.
V.IDP.2	Sektorale IDPs müssen die in [gemSpec_IDP_Sek] festgelegten Vorgaben zur Georedundanz einhalten.
<b>Usability</b>	
U.FM.1	Verständlicher Registrierungsprozess
U.IDP.1	Authenticator-Modul: Willenserklärungen und Freigabeninformation in verständlicher Sprache
U.IDP.2	Authenticator-Modul: Willenserklärungen und Freigabeninformation nicht gemischt mit weiteren andersgearteten Informationen zusammen
U.IDP.3	Authenticator-Modul: einfache Benutzerführung zur Information und Bearbeitung von Willens- und Freigabe erklärungen
U.IDP.4	Authenticator-Modul: Unterstützung des Ident- und Authent-Prozess durch klare gradlinige und verständliche Benutzerführung
U.IDP.5	Landing-Page: Bereitstellung einer Landing-Page
U.IDP.6	Landing-Page: Unterstützung zur Einrichtung der App mit Authenticator-Modul



1712

---

## 10 Anhang - Verzeichnisse

---

1713

### 10.1 Abkürzungen

Kürzel	Erläuterung
BI	Business Intelligence
CT-Log	Certificate Transparency Log
DiGA	Digitale Gesundheitsanwendung
DSGVO	Datenschutz-Grundverordnung
DWH	Data Warehouse
eGBR	Gesundheitsberufsregister
eGK	Elektronische Gesundheitskarte
ePA	elektronischen Patientenakte
FdV	Frontend des Versicherten
HBA	Elektronischer Heilberufsausweis
IDP	Identity Provider
ITSM	IT Service Management
JWT	JSON Web Token
KHPfLEG	Krankenhauspflegeentlastungsgesetz
NFC	Near Field Communication
nPA	neuen Personalausweis
OGR	Organspenderegister
OIDC	OpenID Connect
OP	OpenID Provider
PKCE	

RP	Relying Party
SM(C)-B	Security Module (Card) Typ B
SSO	Single Sign On
TLS	Transport Layer Security
TI	Telematik Infrastruktur
TSP	Trust Service Provider
UC	Use Case
ZETA	Zero Trust Architecture

1714

## 10.2 Glossar

Begriff	Erläuterung	Referenz / Standard
Access Token	Access Token werden für den Zugriff auf geschützte Ressourcen verwendet. Ein Access Token ist eine Zeichenfolge, die einem Client für den autorisierten Zugriff auf geschützte Ressourcen ausgestellt wird. Access Token werden vom Authorization Server eines Fachdienstes ausgestellt.	<a href="#">The OAuth 2.0 Authorization Framework</a>
Auth EP / Token EP	Authentication Endpunkt (Auth EP) , Token-Endpunkt (Token EP)	<a href="#">OpenID Connect Core 1.0 incorporating errata set 1</a>
Authentication	Prozess zur Verifikation einer bekannten Entität und Identität.	<a href="#">OpenID Connect Core 1.0 incorporating errata set 1</a>
Authorization Code Flow	OAuth 2.0-Flow, bei dem ein Autorisierungscode vom Autorisierungsendpunkt und alle Token vom Tokenendpunkt zurückgegeben werden.	<a href="#">OpenID Connect Core 1.0 incorporating errata set 1</a>
Authentication Request	Der OAuth 2.0-Authentication Request ist die Anforderung einer OpenID Connect-Relying-Party (Client) zur Authentifizierung eines	<a href="#">OpenID Connect Core 1.0 incorporating errata set 1</a>

	Endbenutzers durch einen OpenID Connect-Provider.	
Authorization Code (AuthCode)	Der Autorisierungscode ist ein temporärer Code, den der Client gegen ein Zugriffstoken austauscht. Der Autorisierungscode wird vom nach Authentisierung vom Autorisierungsendpunkt ausgestellt und an den Client übermittelt. Der Client kann mit dem Autorisierungscode ein Access-Token beim Tokenendpunkt des Autorisierungsserver anfordern.	<a href="#">The OAuth 2.0 Authorization Framework</a>
Authorization Grant	Authorization Grant definierte die Festlegung, wie ein resource owner autorisiert wird, um ein Access-Token für einen Zugang zu den geschützten Ressourcen zu erhalten. Die Spezifikation unterscheidet vier grant types -- authorization code, implicit, resource owner password credentials sowie client credentials.	<a href="#">The OAuth 2.0 Authorization Framework</a>
Authorization Request	Der Client fordert die Autorisierung vom Ressourceneigentümer durch einen Authorization Request an. Der Authorization Request kann direkt an den Ressourcenbesitzer oder indirekt über den Authorization-Server als Vermittler gestellt werden.	<a href="#">OpenID Connect Core 1.0 incorporating errata set 1</a>
Authorization Server	Der Server, der Zugriffstoken an den Client ausgibt, nachdem er den Nutzer erfolgreich authentifiziert und die nach den Zugriffsregeln zulässigen Ressourcen bestimmt hat.	<a href="#">The OAuth 2.0 Authorization Framework</a>
Claim	Einzelne Information über eine Entität	<a href="#">OpenID Connect Core 1.0 incorporating errata set 1</a>
Client	Eine Anwendung, die geschützte Ressourcenanforderungen im Namen des Ressourceneigentümers und	<a href="#">The OAuth 2.0 Authorization Framework</a>

	<p>mit seiner Autorisierung durchführt. Der Begriff „Client“ impliziert keine besonderen Implementierungsmerkmale (z. B. ob die Anwendung auf einem Server, einem Desktop oder anderen Geräten ausgeführt wird).</p> <p>Im Kontext der TI-Föderation ist das Anwendungsfrontend einer Fachanwendung der (OAuth)-Client bezüglich des Authorization-Servers bzw. des Resourceserver der Fachanwendung.</p> <p>Der Authorization-Server der Fachanwendung ist gleichzeitig auch der (OIDC)-Client bezüglich des sektoralen IDP.</p>	
Code Challenge	<p>Die code challenge wird vom Code Verifier abgeleitet und bei einer Autorisierungsanfrage an den Autorisierungsserver gesendet. Der Autorisierungsserver merkt sich die code challenge zu dem von ihm ausgegebenen Authorization Code. Beim Eintausch des Authorization Code gegen ein Access Token wird durch den Code Verifier die Legitimität der Anfrage verifiziert.</p>	<a href="#">Proof Key for Code Exchange by OAuth Public Clients</a>
Code Challenge Method	<p>Die code challenge method ist die Methode, mit der die code challenge aus dem code verifier erstellt wurde.</p>	<a href="#">Proof Key for Code Exchange by OAuth Public Clients</a>
Code Verifier	<p>Code Verifier ist eine kryptografisch zufällige Zeichenfolge. Bei einer Autorisierungsanforderung wird letztlich gegen diese Zeichenfolge validiert.</p>	<a href="#">Proof Key for Code Exchange by OAuth Public Clients</a>
Credential	<p>Daten, die als Beweis für das Recht zur Nutzung einer Identität oder anderer Ressourcen präsentiert werden.</p>	<a href="#">OpenID Connect Core 1.0 incorporating errata set 1</a>
End-User	<p>Nutzende natürliche Person</p>	<a href="#">OpenID Connect Core 1.0 incorporating</a>

(Nutzer/Anwender)	(Mensch)	<a href="#">errata set 1</a>
Entität	Etwas, das eine separate und eindeutige Existenz hat und das in einem Kontext identifiziert werden kann. Alle Entitäten in einem OpenID Federation-Verbund haben einen global eindeutigen Bezeichner → Entitätsbezeichner	<a href="#">OpenID Federation 1.1</a>
Entity Identifier / URI	Ein URI, der global eindeutig ist und an eine Entität gebunden ist.	<a href="#">OpenID Federation 1.1</a>
Entity Statement	Ein 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.	<a href="#">OpenID Federation 1.1</a>
Fachdienst / Fachanwendung	Fachdienste bzw. Fachanwendungen sind die Anwendungen, mit denen ein Nutzer arbeiten möchte. So sind z. B. E-Rezept und die elektronische Patientenakte TI-Fachanwendungen. Ebenso sind die digitalen Gesundheitsanwendungen (DiGA) Fachdienste. Die Fachdienste/Fachanwendungen benötigen eine Nutzerauthentifizierung um sicherzustellen, dass ein Nutzer die Anwendung überhaupt nutzen darf. Im OAuth/OIDC-Kontext besteht der Fachdienst aus einem Authorizationserver (zur Abwicklung der Authentifizierung über einen IDP) und der eigentlichen Fachanwendung (mit Daten und Prozessen). Aus OAuth/OIDC Sicht agiert der Authorizationserver als Relying Party, die eigentliche Fachanwendung als Resource Server. Für die Nutzerinteraktion verfügen Fachdienste bzw. Fachanwendungen über User	<a href="#">OpenID Federation 1.1</a>

	Interfaces (UI) in Form von nativen Apps, Web-Frontends oder Desktopanwendungen.	
Föderaler IDP	Allgemeiner Begriff für die IDP der Föderation. Konkret ist jeder IDP der Föderation für die Verwaltung von Identitäten bestimmter Sektoren (also = sektoraler IDP) zuständig.	
GesundheitsID	Die GesundheitsID ist die digitale Identität im Gesundheitswesen für Versicherte, welche durch die eigene Krankenversicherung bereitgestellt wird. Sie dient zur Anmeldung an TI-Anwendungen und weiteren versorgungsrelevanten Fachanwendungen und kann perspektivisch auch als Versicherungsnachweis - analog zur elektronischen Gesundheitskarte - verwendet werden.	
HSM	Hardware Security Module, Hardware-Sicherheitsmodul	
ID Token	<a href="#">JSON Web Token (JWT)</a> , welches Eigenschaften zur angefragten Identität und ggf. weitere Informationen enthält.	<a href="#">OpenID Connect Core 1.0 incorporating errata set 1</a>
Intermediate Entity	Intermediäre Entität: Eine Entität, die eine Entitätserklärung ausstellt, die zwischen den vom Vertrauensanker und der Blattentität in einer Vertrauensketten ausgestellten Erklärungen liegt. (Wird in der aktuellen Architektur nicht verwendet)	<a href="#">OpenID Federation 1.1</a>
Issuer	Ausstellende Entität für ein Token oder Entity Statement (über sich selbst oder eine andere Entität - dann als Subject bezeichnet)	<ul style="list-style-type: none"> <li><a href="#">OpenID Connect Core 1.0 incorporating errata set 1</a></li> <li><a href="#">OpenID Federation 1.1</a></li> </ul>

Leaf Entity	Blatt-Entität: Eine Entität, die durch ein bestimmtes Protokoll definiert ist, z. B. OpenID Connect Relying Party oder Provider.	<a href="#">OpenID Federation 1.1</a>
OpenID Provider (OP)	OAuth 2.0-Autorisierungsserver, der in der Lage ist, den Endbenutzer zu authentifizieren und einer vertrauenden Seite Informationen zur Authentifizierung und zum Endbenutzer bereitzustellen.	<ul style="list-style-type: none"> <li>• <a href="#">OpenID Connect Core 1.0 incorporating errata set 1</a></li> <li>• <a href="#">OpenID Federation for OpenID Connect 1.1</a></li> </ul>
PAR	Beim Pushed Authorization Request werden im Vorfeld des eigentlichen OpenID Authorization Code Flow die Parameter direkt zwischen RP und OP ausgetauscht und diese gegenseitig Authentifiziert.	<a href="#">OAuth 2.0 Pushed Authorization Requests</a>
PKCE	Proof Key for Code Exchange ist eine Erweiterung des Autorisierungscodeflusses, um CSRF- und Authorization- Code-Injection-Angriffe zu verhindern. Bei dieser Technik erstellt der Client zunächst bei jeder Autorisierungsanforderung ein Geheimnis und verwendet dieses Geheimnis dann erneut, wenn er den Autorisierungscode gegen ein Access Token austauscht.	<a href="#">Proof Key for Code Exchange by OAuth Public Clients</a>
Refresh Token	Refresh Token sind credentials, welche zum Abrufen von Access Token verwendet werden. Refresh Token werden vom Autorisierungsserver an den Client ausgegeben und verwendet, um ein neues Access Token zu erhalten, wenn das aktuelle Access Token ungültig wird oder abläuft, oder um zusätzliche Access Token mit identischem oder engerem Umfang zu erhalten. Access Token können	<a href="#">The OAuth 2.0 Authorization Framework</a>

	eine kürzere Lebensdauer haben und weniger Berechtigungen als vom Ressourceneigentümer autorisiert. Das Ausstellen eines Refresh Token ist optional.	
Relying Party (RP)	OAuth 2.0-Clientanwendung, die eine Endbenutzerauthentifizierung und Informationen von einem OpenID-Anbieter erfordert.	<ul style="list-style-type: none"> <li>• <a href="#">OpenID Connect Core 1.0 incorporating errata set 1</a></li> <li>• <a href="#">OpenID Federation for OpenID Connect 1.1https://openid.net/specs/openid-connect-core-1_0.html</a></li> </ul>
Request URI	URL, die auf eine Ressource verweist, welche vom Autorisierungsserver abrufbar sein muss.	<a href="#">OpenID Connect Core 1.0 incorporating errata set 1</a>
Resource Owner	Entität, die Zugriff auf eine geschützte Ressource gewähren kann. Wenn der Ressourceneigentümer eine Person ist, wird er als Endbenutzer bezeichnet.	<a href="#">The OAuth 2.0 Authorization Framework</a>
Resource Server	Der Server, der die geschützten Ressourcen hostet und in der Lage ist, Anforderungen für geschützte Ressourcen mithilfe von Zugriffstoken zu akzeptieren und darauf zu antworten.	<a href="#">The OAuth 2.0 Authorization Framework</a>
sektoraler IDP	Jeder IDP verwaltet die Identitäten zu einem bestimmten Sektor. So verwalten die IDPs der Krankenkassen beispielsweise den Sektor der Versicherten, während andere IDPs die verschiedenen Sektoren der Leistungserbringer abdecken können.	
Subject	Entität über welche ein Token oder Entity Statement ausgestellt wurde und für welche die darin genannten Informationen gelten.	<ul style="list-style-type: none"> <li>• <a href="#">OpenID Connect Core 1.0 incorporating errata set 1</a></li> <li>• <a href="#">OpenID Federation 1.1https://openid.net/specs/openid-federation-1_0.html</a></li> </ul>



Scope	Bezeichnung für eine bestimmte Berechtigung (OAuth2) oder einen Satz von Informationen (OpenID) welche angefragt werden.	<a href="#">OpenID Connect Core 1.0 incorporating errata set 1</a> <a href="#">The OAuth 2.0 Authorization Framework</a>
Trust Anchor	Vertrauensanker: Eine Entität, die eine vertrauenswürdige dritte Partei darstellt. (Der Federation Master)	<a href="#">OpenID Federation 1.1</a> <a href="https://openid.net/specs/openid-federation-1_0.html">https://openid.net/specs/openid-federation-1_0.html</a>
Trust Chain	Vertrauenskette: Eine Folge von Entitätsaussagen, die eine Kette darstellt, die bei einer Blatt-Entität beginnt und bei einem Vertrauensanker endet.	<a href="#">OpenID Federation 1.1</a> <a href="https://openid.net/specs/openid-federation-1_0.html">https://openid.net/specs/openid-federation-1_0.html</a>

## 10.3 Abbildungsverzeichnis

Abbildung 1 : Idee des Aufbaus einer TI-Föderation auf Basis des OpenID Federation Standards.....	14
Abbildung 2 :Beispiel des Aufbau der TI-Födeartion.....	19
Abbildung 3 : TI-Föderation und Nachbarsysteme.....	20
Abbildung 4 : Anwendungsfälle TI-Föderation.....	25
Abbildung 5 : Komponenten der TI-Föderation im Überblick.....	27
Abbildung 6 : Komponenten der TI-Föderation mit Schnittstellen.....	28
Abbildung 7 : Schlüsselmanagement für die Nutzerauthentifizierung in der TI-Föderation .....	38
Abbildung 8 : Ablauf App2App-Flow.....	43
Abbildung 9 : Ablauf Web2App-Flow.....	84
Abbildung 10 : Ablauf 2-Geräte-Flow.....	87
Abbildung 11 : Ablauf Desktop-App-Flow.....	90
Abbildung 12 : Beispiel Entscheidungsmatrix für SSO im ePA-FdV.....	93
Abbildung 13 : ePA-FdV mit mehreren integrierten TI-Anwendungen.....	94
Abbildung 14: Beispiel für SSO bei Ausführung ePA Client Modul mit aktiver und E-Rezept Client Modul ohne aktive Nutzerauthentisierung aus dem ePA-FdV mit integriertem Authenticator-Modul.....	97
Abbildung 15: Beispiel für SSO bei Ausführung ePA Client Modul mit aktiver und E-Rezept Client Modul ohne aktive Nutzerauthentisierung aus dem ePA-FdV mit Authenticator-Modul in separater APP.....	98
Abbildung 16 : Deploymentview TI-Föderation.....	107
Abbildung 17 : Messpunkte der Bearbeitungszeiten sekt. IDPs.....	109

Abbildung 18 : Messpunkte der Bearbeitungszeiten Trust Anchor.....	110
--	-----

## 10.4 Tabellenverzeichnis

Tabelle 1 : Schnittstellen zu Umsystemen.....	21
Tabelle 2 : Übersicht über die Anwendungsfälle im Gesamtkontext Federation Master....	23
Tabelle 3 : Akteure und Rollen.....	29
Tabelle 4 : Schnittstellen zwischen den Teilnehmern und Komponenten der TI-Föderation .....	34
Tabelle 5 : Schlüsselmanagement.....	38
Tabelle 6 : Ablaufbeschreibung App2App-Flow.....	43
Tabelle 7 : Entity Configuration des Federation Maste.....	47
Tabelle 8 : Liste registrierten sektoralen IDPs.....	50
Tabelle 9 : Entity Configuration eines sektoralen IDP.....	54
Tabelle 10 : Subordinate Statement zu einem sektoralen IDP.....	60
Tabelle 11 : Inhalte eines Pushed Authorization Request.....	62
Tabelle 12 : Entity Configuration eines Fachdienst Authorization Server.....	65
Tabelle 13 : Subordinate Statement zu einem Fachdienst Authorization Server.....	69
Tabelle 14 : Request URI, ausgestellt vom sektoralen IDP.....	71
Tabelle 15 : Inhalte des Redirect zum sektoralen IDP.....	72
Tabelle 16 : Inhalte des Redirect zum Fachdienst Authorization Server.....	73
Tabelle 17 : Attribute für den Abruf des ID-Token vom sektoralen IDP.....	74
Tabelle 18 : Attribute des ID-Token.....	77
Tabelle 19 : Response vom Fachdienst Authorization Server an den Fachdienst-Client (Authorization-Code-Flow).....	80
Tabelle 20 : Abruf des Access-Token am Fachdienst Authorization Server.....	80
Tabelle 21 : Ablaufbeschreibung Web2App-Flow.....	84
Tabelle 22 : Ablaufbeschreibung 2-Geräte-Flow.....	87
Tabelle 23 : Ablaufbeschreibung Desktop-App-Flow.....	90
Tabelle 24: Unterschiede im Ablauf IN-APP-Konstellation vs. APP-APP-Konstellation.....	95
Tabelle 25: Ablauf der Aufrufe der TI-Client Module aus dem ePA-FdV.....	98
Tabelle 26: Use-Cases für Bearbeitungszeitvorgaben sektorale IDPs.....	109
Tabelle 27: Use-Cases für Bearbeitungszeitvorgaben Federation Master.....	110
Tabelle 28 : Qualitätskriterien.....	112

## 10.5 Referenzierte Dokumente

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

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemSpec_IDP_FedMaster]	<a href="https://gemspec.gematik.de/docs/gemSpec/gemSpec_IDP_FedMaster/latest/">https://gemspec.gematik.de/docs/gemSpec/gemSpec_IDP_FedMaster/latest/</a>
[gemSpec_IDP_Sek]	<a href="https://gemspec.gematik.de/docs/gemSpec/gemSpec_IDP_Sek/latest/">https://gemspec.gematik.de/docs/gemSpec/gemSpec_IDP_Sek/latest/</a>
[gemSpec_IDP_FD]	<a href="https://gemspec.gematik.de/docs/gemSpec/gemSpec_IDP_FD/latest/">https://gemspec.gematik.de/docs/gemSpec/gemSpec_IDP_FD/latest/</a>
[gemSpec_Perf]	<a href="https://gemspec.gematik.de/docs/gemSpec/gemSpec_Perf/latest/">https://gemspec.gematik.de/docs/gemSpec/gemSpec_Perf/latest/</a>
[gemKPT_Betr]	<a href="https://gemspec.gematik.de/docs/gemKPT/gemKPT_Betr/latest/">https://gemspec.gematik.de/docs/gemKPT/gemKPT_Betr/latest/</a>
[gemKPT_Test]	<a href="https://gemspec.gematik.de/docs/gemKPT/gemKPT_Test/latest/">https://gemspec.gematik.de/docs/gemKPT/gemKPT_Test/latest/</a>
[gemSpec_DS_Hersteller]	<a href="https://gemspec.gematik.de/docs/gemSpec/gemSpec_DS_Hersteller/latest/">https://gemspec.gematik.de/docs/gemSpec/gemSpec_DS_Hersteller/latest/</a>
[gemSpec_Krypt]	<a href="https://gemspec.gematik.de/docs/gemSpec/gemSpec_Krypt/latest/">https://gemspec.gematik.de/docs/gemSpec/gemSpec_Krypt/latest/</a>
[gemSpec_OM]	<a href="https://gemspec.gematik.de/docs/gemSpec/gemSpec_OM/latest/">https://gemspec.gematik.de/docs/gemSpec/gemSpec_OM/latest/</a>
[gemSpec_PKI]	<a href="https://gemspec.gematik.de/docs/gemSpec/gemSpec_PKI/latest/">https://gemspec.gematik.de/docs/gemSpec/gemSpec_PKI/latest/</a>
[gemSpec_Systemprozesse_dezTI]	<a href="https://gemspec.gematik.de/docs/gemSpec/gemSpec_Systemprozesse_dezTI/latest/">https://gemspec.gematik.de/docs/gemSpec/gemSpec_Systemprozesse_dezTI/latest/</a>

### Weitere Referenzierungen:

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI TR-03107]	<a href="https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03107/TR-03107_node.html">https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03107/TR-03107_node.html</a>
[eIDAS]	<a href="https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/eIDAS-">https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/eIDAS-</a>

	<a href="#">Verordnung/eidas-verordnung_node.html</a>
[IDP Wissensdatenbank]	<a href="https://wiki.gematik.de/x/wxEEHg">https://wiki.gematik.de/x/wxEEHg</a>
[OAuth 2.0 Rich Authorization Requests]	<a href="https://www.ietf.org/archive/id/draft-ietf-oauth-rar-03.html">https://www.ietf.org/archive/id/draft-ietf-oauth-rar-03.html</a>
[OpenID Connect Core 1.0]	<a href="https://openid.net/specs/openid-connect-core-1_0.html">https://openid.net/specs/openid-connect-core-1_0.html</a>
[OpenID Federation 1.1]	<a href="https://openid.net/specs/openid-federation-1_1.html">https://openid.net/specs/openid-federation-1_1.html</a>
[OpenID Federation for OpenID Connect 1.1]	<a href="https://openid.net/specs/openid-federation-connect-1_1.html">https://openid.net/specs/openid-federation-connect-1_1.html</a>
[RFC6749]	<a href="https://datatracker.ietf.org/doc/html/rfc6749">https://datatracker.ietf.org/doc/html/rfc6749</a>
[RFC7636]	<a href="https://datatracker.ietf.org/doc/html/rfc7636">https://datatracker.ietf.org/doc/html/rfc7636</a>
[RFC9126]	<a href="https://datatracker.ietf.org/doc/html/rfc9126">https://datatracker.ietf.org/doc/html/rfc9126</a>
[RFC9396]	<a href="https://datatracker.ietf.org/doc/html/rfc9396">https://datatracker.ietf.org/doc/html/rfc9396</a>
[RFC9562]	<a href="https://www.rfc-editor.org/rfc/rfc9562.html">https://www.rfc-editor.org/rfc/rfc9562.html</a>

1780

1781