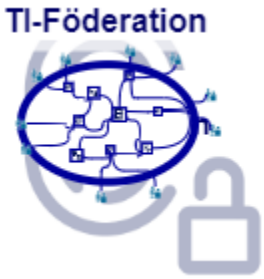
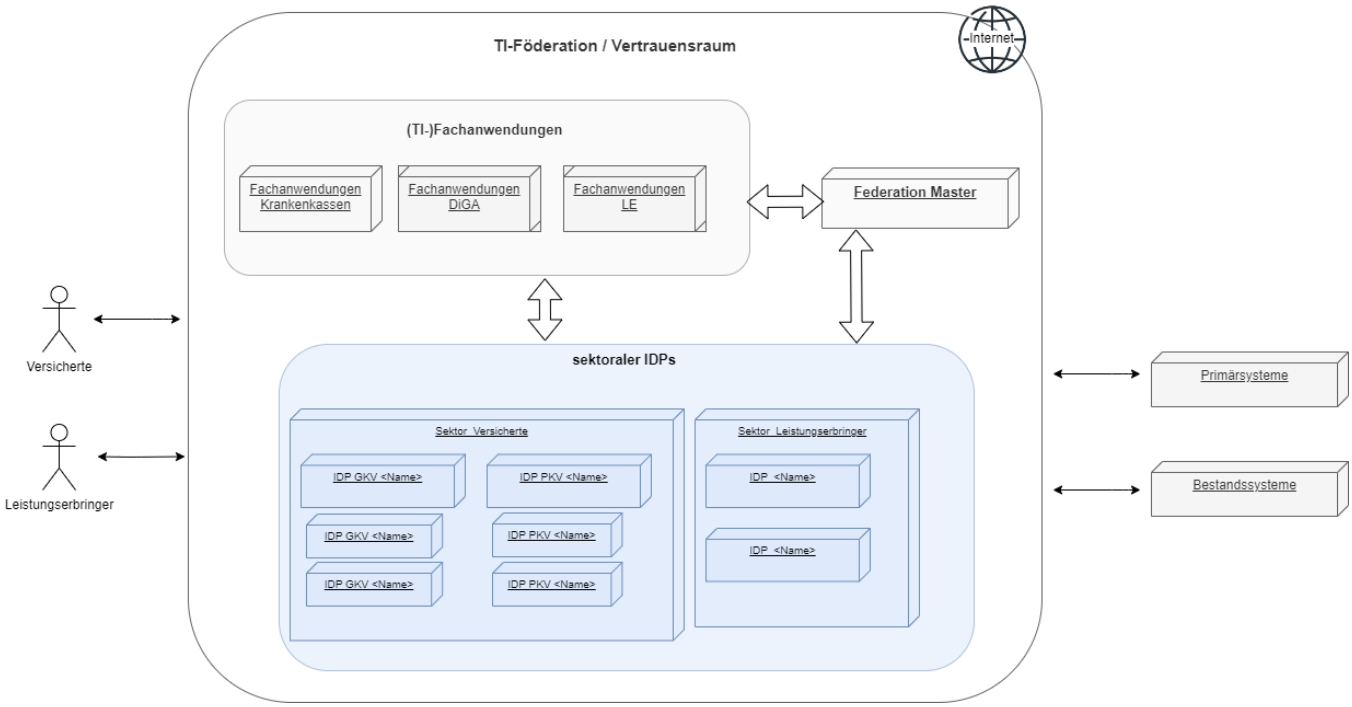
Sektoraler IDP



Überblick



Als sektoraler IDP wird ein Dienst zur Authentifizierung von Nutzern bezeichnet. Nach erfolgreichen Durchlaufen des Authentifizierungsprozesses stellt der sektorale IDP Identitätsinformationen für eine bestimmte Gruppe von Nutzern, welche einem Sektor zuzuordnen sind, innerhalb der Telematikinfrastruktur des Gesundheitswesens bereitstellt. Die Identitätsinformationen der Nutzer werden durch den anfordernden Fachdienst zur Prüfung verwendet, auf welche Fachdaten und -prozesse der Nutzer zuzugreifen darf.

Das Konzept der sektoralen IDP sieht vor, dass diese nicht ausschließlich von Fachdiensten der TI zur Authentifizierung von Anwendern zu verwenden sind. Vielmehr können (und sollen) auch Anwendungen außerhalb der TI (z. B. Anwendungen der Krankenkassen für ihr Versicherten) den sektoralen IDP zur Nutzerauthentifizierung und Attributübertragung verwenden.

Für Anwendungen, die nicht übergreifend durch mehrere IDPs unterstützt werden sollen, ist es ausreichend diese direkt bei den jeweiligen IDPs zu registrieren. Die Föderation bietet hier keinen Mehrwert da beide Kommunikationspartner sich ohnehin kennen und vertrauen. Die in den Spezifikationen der gematik festgelegten Anforderungen sind für diese Anwendungen und den Anmeldungsflow am sektoralen IDP nicht bindend. Die (z. B. kasseneigenen) Anwendungen können mit ihren Kassen-IDP weitere *scopes* und *claims* vereinbaren. Eine Registrierung am Federation Master f ür diese Anwendungen nicht notwendig, da sie nicht Teil der Föderation sind. Die Fachdienste müssen sich lediglich OIDC konform am sektoralen IDP (also dem OpenID Provider) registrieren. Der sektorale Identity Provider kann für diese Anwendungen auch zugleich als Authorization-Server agier en und *Access-Token* ausstellen.

Die untere Abbildung beschreibt den Systemkontext aus Sicht des sektoralen IDP. Das Anwendungsfrontend des Fachdienstes stellt die Anfrage zur Authentifizierung des Nutzers an den Authorization-Server des Fachdienstes. Dieser generiert eine *Code-Challenge* und stellt einen *Pushed Authorization Request* (PAR) an den entsprechenden sektoralen IDP. Der Fachdienst agiert diesem gegenüber als Client. Über das Authenticator-Modul des sektoralen IDP findet dann die Authentifizierung des Nutzers statt. Anschließend erhält der Authorization-Server des Fachdienstes einen *A uthorization-Code*, welchen er bei Token-Endpunkt des sektoralen IDP gegen einen *ID-Token* eintauscht. Der Authorization-Server des Fachdienstes erstellt nun ein *Access-Token* für das Anwendungsfrontend, mit welchem dieses auf die, für den Nutzer freigegebenen, Ressourcen des Fachdienstes zugreifen kann. Die Kommunikation zwischen Anwendungsfrontend und Authorization-Server des Fachdienstes kann ebenfalls über einen eigenen *Aut horization-Code* abgesichert werden.

Der Fachdienst und der sektoralen IDP müssen sich zuvor beim Federation Master in Form eines organisatorischen Prozesses registriert haben.

Der Produkttyp des sektoralen IDP besteht aus zwei Komponenten - der zentralen Komponente IDP (OP), dem eigentlichen OpenID-Provider und einer Frontend-Komponente u. a. für die Interaktion mit dem Nutzer, dem Authenticator-Modul. Das Authenticator-Modul unterstützt die Durchführung des Authentifizierungsprozesses und übernimmt die Ausführung der Nutzerauthentisierung.

Der sektorale IDP stellt über standardkonforme Schnittstellen die zentralisierte Identitätsprüfung der auf die Fachdienste zugreifenden Nutzer bereit. Als weitere Teile der Gesamtlösung sind neben dem sektoraler IDP die Clients (Anwendungsfrontend) und die Fachdienste zu nennen, auf denen Fachdaten für den Zugriff durch die Nutzer (z. B. Versicherte oder Bediener eines AVS, PVS oder KVS) bereitgestellt werden. Ein sektoraler IDP bietet seine Dienste Fachdiensten an, auf welche Millionen Nutzer zeitgleich zugreifen. Auch Anwendungen außerhalb der TI-Föderation, z. B. kassenspezifische Anwendungen, werden direkt den jeweiligen sektoralen IDP nutzen.

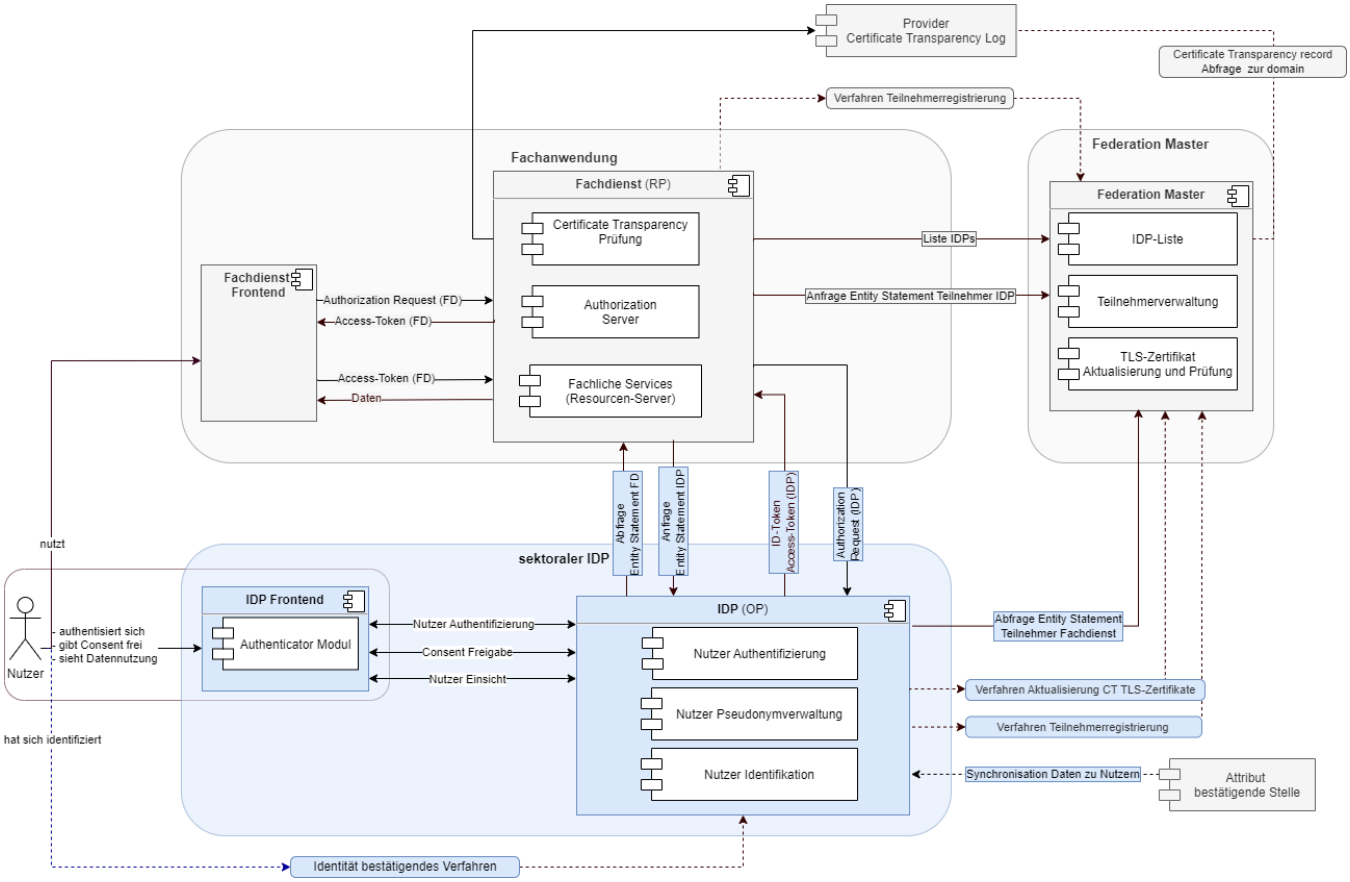
Schnittstellen und Interaktion

Ein sektoraler IDP bietet zahlreiche Schnittstellen gegenüber unterschiedlichen Akteuren an. Die Beschreibung der Interaktionen zwischen den beteiligten Systemen über die Schnittstellen soll die Funktionsweise anderen Akteure leichter verständlich machen.

Vorbereitende Maßnahmen:

- Der Fachdienst hat bei der Registrierung am Federation Master seine öffentlichen Schlüssel hinterlegt.
- Der Fachdienst hat bei der Registrierung am Federation Master die *scopes* hinterlegt, welche er für die Autorisierung eines Nutzers zwingend benötigt
- Der Fachdienst kennt das Entity Statement der sektoralen IDP und hat bei der Registrierung dort seine öffentlichen Schlüssel hinterlegt.

Schnittstellen

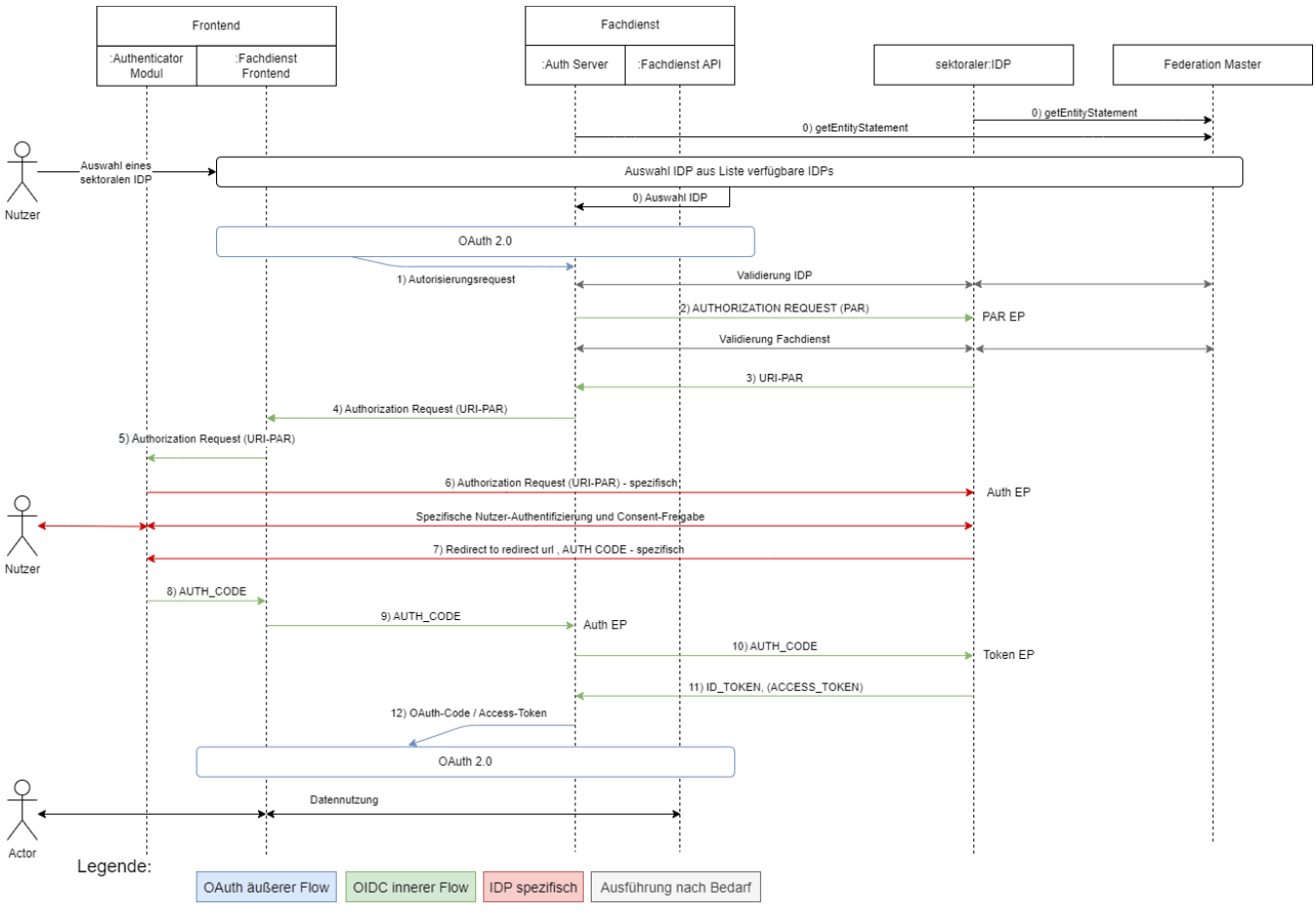


Aus der Abbildung des Systemkontextes ist ersichtlich, welche Schnittstellen der sektorale IDP zu welchen Systemen unterhält (externe Schnittstellen). Neben den notwendigen externen Schnittstellen sind relevante interne Schnittstellen zwischen dem eigentlichen IDP - dem OpenID-Provider - und dem Authenticator-Modul aufgeführt. Die Tabelle listet die für die Spezifikation des sektoralen IDP relevanten und in diesem Dokument näher beschriebenen Schnittstellen auf.

Schnittstelle	sektoraler IDP	Komponente /System	Typ	fachliche Schnittstellenbeschreibung
Authorization Request (IDP)	IDP (OP)	Fachdienst (RP)	extern	Zur Ermittlung der Informationen zum Nutzer stellt der Fachdienst einen Request an den sektoralen IDP.

Abfrage Entity Statement FD	IDP (OP)	Fachdienst (RP)	extern	Zur Ermittlung des Entity Statement des Fachdienstes stellt der sektorale IDP einen Request an den Fachdienst.
Anfrage Entity Statement IDP	IDP (OP)	Fachdienst (RP)	extern	Zur Abfrage des Entity Statement des sektorale IDP stellt der Fachdienstes einen Request an den sektorale IDP.
ID-Token, Access-Token (IDP)	IDP (OP)	Fachdienst (RP)	extern	Im Austausch zu einem Authentication Code liefert der sektorale IDP ein *Access-Token* und ein *ID-Token*
Abfrage Entity Statement Teilnehmer Fachdienst	IDP (OP)	Federation Master	extern	Zur Verifikation einen anfragenden Fachdienst stellt der sektorale IDP einen Request an den Federation Master.
Verfahren Aktualisierung CT TLS-Zertifikate	IDP (OP)	Federation Master	extern	Organisatorische Schnittstelle zur Schlüsselregistrierung der im sektoralen IDP verwendeten TLS-Zertifikate beim Federation Master
Verfahren Teilnehmerregistrierung	IDP (OP)	Federation Master	extern	Organisatorische Schnittstelle zur Registrierung des sektoralen IDP als Teilnehmer der TI-Föderation beim Federation Master
Synchronisation Daten zu Nutzern	IDP (OP)	Attribut bestätigende Stelle	extern	Die Daten über identifizierte Nutzer, welche über den sektoralen IDP authentifiziert werden können werden von der Attribut bestätigenden Stelle bereitgestellt.
Nutzer Authentifizierung	IDP (OP)	IDP Frontend	intern	Die Nutzerauthentifizierung durch den sektoralen IDP erfolgt über das Authenticator-Modul.
Consent Freigabe	IDP (OP)	IDP Frontend	intern	Die Consent Freigabe durch den Nutzer erfolgt über das Authenticator-Modul.
Nutzer Einsicht	IDP (OP)	IDP Frontend	intern	Die Einsichtnahme des Nutzers in Nutzung seiner Daten durch den sektoralen IDP erfolgt über das Authenticator-Modul.
Benutzer Aktion	IDP Frontend	Nutzer	extern	Die Interaktion des Nutzers zur Nutzerauthentifizierung, Consentfreigabe und Einsichtnahme in die Datennutzung erfolgt über das Authenticator-Modul.

Interaktionen



Der gesamte Authentifizierungsprozess (Abbildung: *"OAuth- und OIDC-Flow"*) basiert aus Gründen der Entkoppelung zwischen den Authentifizierungsmethoden und Token-Formaten der sektoralen IDP und des Fachdienstes aus zwei ineinander geschachtelten OAuth2-Flows vom Typ grant_type=*authorization_code*.

Im äußeren Flow (Schritt 1) wendet sich das Anwendungsfrontend als Client initial an den Authorization-Server des Fachdienstes und signalisiert diesem über einen zusätzlichen nicht im OIDC-Standard spezifizierten Parameter *idp_iss* den zur Authentifizierung zu verwendenden sektoralen IDP. Der innere Flow beginnt mit einem Authorization Request in Schritt 2 und endet mit Schritt 11, der Herausgabe eines *ID-Token* und *Access-Token* vom sektoralen IDP an den Authorization-Server des Fachdienstes.

Die erste Anfrage an den sektoralen IDP geht am PAR-Endpunkt [OAuth 2.0 Pushed Authorization Requests (section-2)] ein. Der Authorization-Server des Fachdienstes reicht dort am Endpunkt den Authorization Request zur Authentifizierung des Nutzers und zur Bestätigung des *scope* der anfragenden Anwendung sowie eine ein. Der *scope* der angefragten Nutzdaten ist im Entity Statement des Fachdienstes hinterlegt. Dieses ist dem sektoralen IDP bekannt. Ist das nicht der Fall, so wird das Entity Statement des Fachdienstes durch den sektoralen IDP abgefragt und durch den Federation Master bestätigt. Der Authorization-Server des Fachdienstes tritt bzgl. des inneren Flow als Client auf.

Im Weiteren Ablauf wird der Nutzer dann aufgefordert sich, unter Nutzung des Authenticator-Moduls des sektoralen IDP, zu authentisieren. Dies erfolgt über eine Schnittstelle zwischen dem Authenticator-Modul und Authorization-Endpunkt des sektoralen IDP.

Nach erfolgreicher Authentisierung und der Consent-Freigabe durch den Nutzer erstellt der sektorale IDP den *Authorization-Code*. Dieser wird an den Authorization-Server des Fachdienstes übermittelt, welcher ihn am Token-Endpunkt [The OAuth 2.0 Authorization Framework (section-3.2)] des sektoralen IDP einreicht. Der sektorale IDP überprüft den *Authorization-Code* und stellt bei positiver Validierung einen *ID-Token* und ein *Access-Token* aus.

Anschließend erstellt der Authorization-Server des Fachdienstes einen *Authorization-Code*, der an das Anwendungsfrontend zurückgegeben wird. Der äußere Flow endet mit der Herausgabe eines *Access-Token* an das Anwendungsfrontend bzw. im Fall von Web-Anwendungen an das Web-Backend des Anwendungsfrontends. Der weitere fachliche Ablauf zum Einreichen der Token und zur Nutzung der Fachdaten und Prozesse ist anwendungsspezifisch.

Schritt	Beschreibung
optional	Die Auswahl eines sektoralen IDP durch den Anwender am Anwendungsfrontend ist erforderlich, wenn der dem Fachdienst (z. B. aus früheren Sitzungen) nicht bekannt ist.
1	Das Anwendungsfrontend sendet einen Authorization Request mit dem zur Anmeldung gewünschten sektoralen IDP an den Authorization-Server des Fachdienstes.
optional	Falls der Authorization-Server das Entity Statement des sektoralen IDP noch nicht kennt, lädt er dies herunter. (*/.well-known/openid-federation*). Der sektorale IDP sendet sein Entity Statement zurück. Der sektorale IDP wird gegen den Federation Master validiert indem der Fachdienst das Entity Statement zum sektoralen IDP beim Federation Master abruft.
2	Der Authorization-Server sendet einen Pushed Authorization Request (PAR) inkl. und benötigter *scopes* an den sektoralen IDP und authentisiert sich als Client innerhalb der mTLS Verbindung. Die Erzeugung der erfolgt durch den Authorization-Server entsprechende der Spezifikation [RFC7636 - Proof Key for Code Exchange by OAuth Public Clients] (PKCE) über die Generierung eines Zufallswertes (*Codeverifier*) und die Erzeugung eines Hashwert für den *Codeverifier*. Die ist dann der base64-codierte Hashwert des *Codeverifier*.
optional	Falls der sektorale IDP das Entity Statement des Authorization-Servers noch nicht kennt, lädt er dies herunter. (/.well-known/openid-federation). Der Authorization-Server sendet sein Entity Statement zurück und der sektorale IDP registriert ihn als Client. Der Fachdienst wird gegen den Federation Master validiert indem der sektorale IDP das Entity Statement zum Fachdienst/Authorization-Server beim Federation Master abruft.
3	Der sektorale IDP sendet eine Request-URI (mit Bezug zum vorherigen *Authorization-Request*) an den Authorization-Server.
4	Der Authorization-Server sendet die Request-URI und Client ID an das Anwendungsfrontend zur Weiterleitung an die Adresse des Authenticator des sektoralen IDP.
5	Anwendungsfrontend öffnet den Authenticator für die eigentliche Authentifizierung des Anwenders (Deep-Link/Universal-Link).
6	Das Authenticator-Modul leitet den Authentication Request an den sektoralen IDP weiter.
spezifisch	Der Ablauf der Authentifizierung des Nutzers ist IDP spezifisch.
7	Der Authorization-Endpunkt des sektoralen IDP antwortet dem Authenticator-Modul mit dem *Authorization-Code* und einem Redirect zum Fachdienst.
8	Das Authenticator-Modul des sektoralen IDP ruft über einen App-Link bzw. Universal-Link entsprechend der Redirect-URL das Anwendungsfrontend auf (eigentlich ein Redirect zum Fachdienst aber das Frontend ist auf die Adresse registriert) und übergibt den *Authorization-Code*
9	Die Anwendungsfrontend leitet den *Authorization-Code (IDP)* an den Authorization-Server.
10	Der Authorization-Server reicht den *Authorization-Code (IDP)* und den *Code-Verifier* beim Token-Endpunkt des sektoralen IDP ein und authentisiert sich als Client innerhalb der mTLS Verbindung.
11	Der Authorization-Server erhält vom Token-Endpunkt des sektoralen IDP einen *ID-Token* und *Access-Token* mit den gewünschten *claims* , der mit dem öffentlichen Schlüssel aus der Registrierung verschlüsselt ist.
	Der weitere Ablauf entspricht dem OAuth-Flow und unterscheidet sich in Details je nach Ausprägung des Anwendungsfrontend als App oder Web-Anwendung.

Es gibt einige Unterschiede in den Abläufen für App-App Kommunikation, Web-App Kommunikation und Kommunikation unter Beteiligung von zwei Geräten.