

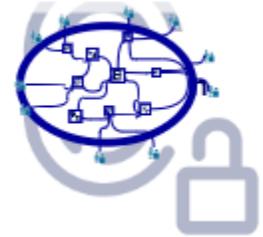
# Web-App Flow (2 Geräte)



Diese Seite beschreibt die Nutzung einer Web-Anwendung über einen Browser auf einem und dem Authenticator-Modul *auf einem zweiten mobilen Endgerät* im Kontext föderierter IDPs.

- [Terminologie](#)
- [Vorbedingungen](#)
- [Flow - OIDC](#)
  - [Flow Diagramm](#)
  - [Textuelle Beschreibung der Aktivitäten je Transaktion sowie in den Übergängen](#)
- [Schnittstellenbeschreibung](#)

## TI-Föderation



## Terminologie

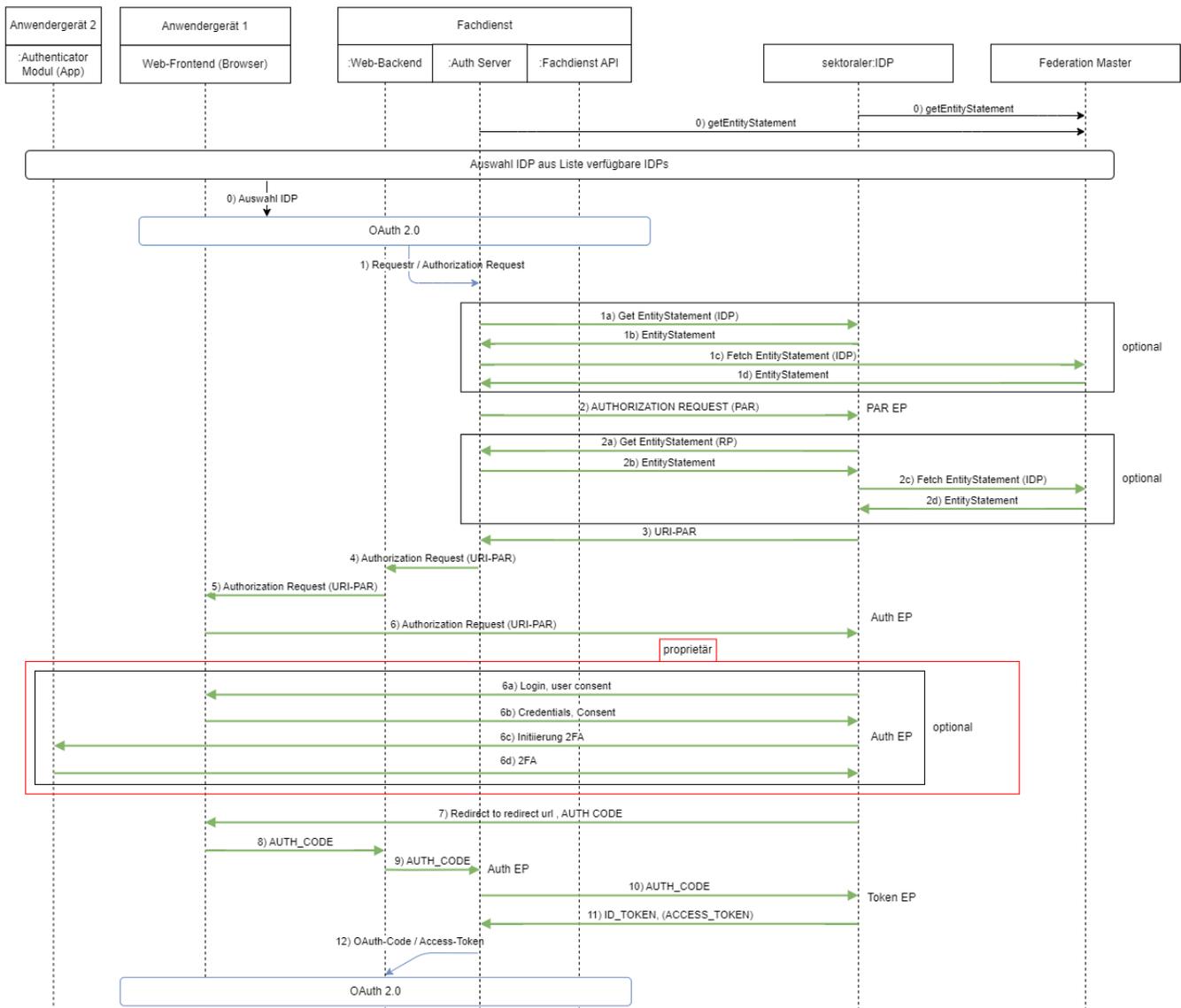
Erläuterungen zur verwendeten Terminologie analog sind zentral für alle Flows [hier](#) abgelegt.

## Vorbedingungen

- Registrierung der Fachanwendung als RP beim Federation Master
- 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.
- Aktueller Signaturschlüssel des Federation Master ist bekannt und vertrauenswürdig bei IDP und Fachdienst eingebracht worden.
- Sektorale IDP ist Teil des TI-Vertrauensraums und beim Federation Master registriert.
- Der Fachdienst besitzt ein Web-Backend welches Anwendungslogik realisiert.
- Authenticator-Modul des IDP (APP) läuft auf einem anderen Gerät als die Fachanwendung (z.B. App Smartphone, Anwendung PC-Browser)

## Flow - OIDC

## Flow Diagramm



Legende:



Exemplarische Beschreibung des Ablaufs einer Dienstnutzung sowie der Vor und Nachbedingungen

## Textuelle Beschreibung der Aktivitäten je Transaktion sowie in den Übergängen

Schritt	Gerät	Beschreibung
0	1	<ul style="list-style-type: none"> <li>• Abruf der Schlüssel des Federation Master</li> <li>• Flow zur Auswahl des IDP siehe "Flow - Ermittlung und Auswahl IDP" <ul style="list-style-type: none"> <li>◦ Die Auswahl des richtigen IDP ist optional. Ist der 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 <a href="#">Web-zu-App Flow (1)</a>
	1-a	Schnittstellendetails analog <a href="#">App-zu-App Flow (1a)</a>
	1-b	Schnittstellendetails analog <a href="#">App-zu-App Flow (1b)</a>
	1-c	Schnittstellendetails analog <a href="#">App-zu-App Flow (1c)</a>
	1-d	Schnittstellendetails analog <a href="#">App-zu-App Flow (1d)</a>

2			Schnittstellendetails analog <a href="#">App-zu-App Flow (2)</a>
	2-a		Schnittstellendetails analog <a href="#">App-zu-App Flow (2a)</a>
	2-b		Schnittstellendetails analog <a href="#">App-zu-App Flow (2b)</a>
	2-c		Schnittstellendetails analog <a href="#">App-zu-App Flow (2c)</a>
	2-d		Schnittstellendetails analog <a href="#">App-zu-App Flow (2d)</a>
3			Schnittstellendetails analog <a href="#">App-zu-App Flow (3)</a>
4			Der Autorisierungsserver antwortet dem Web-Backend mit Request-URI und Client ID zur Weiterleitung über das Anwendungsfrontend an die Adresse des Authenticator des IDP.
5		1	Das Web-Backend leitet den Redirect an das Anwendungsfrontend weiter.
6		1	Das Anwendungsfrontend öffnet die Web-Anwendung des 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 IDP.
	6c	2	Der IDP kann das Authenticator-Modul des IDP (z.B. 2FA) mit in den Prozess einbinden. Dazu sendet der 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 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(IDP)" an sein Web-Backend weiter.
9			Das Web-Backend leitet den "AUTHORIZATION_CODE(IDP)" an den Autorisierungsserver (redirected uri)
10			Schnittstellendetails analog <a href="#">App-zu-App Flow (10)</a>
11			Schnittstellendetails analog <a href="#">App-zu-App Flow (11)</a>
12		1	Schnittstellendetails analog <a href="#">Web-zu-App Flow (11)</a>

## Schnittstellenbeschreibung

Exemplarische Beschreibung des Ablaufs einer Dienstrutzung sowie der Vor und Nachbedingungen

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

Der Abruf der Schlüssel des Federation Master erfolgt analog dem [App-zu-App Flow \(Federation Master\)](#)

#### IDP Liste

Beschreibung zur IDP-Liste ist im [Web-zu-App Flow \(IDP-Liste\)](#) hinterlegt.

### (1) Authorization Request von Web-Backend zum Authentication Endpunkt (Auth ES) des Autorisierungsserver des Fachdienstes

- Web-Anwendung Request analog [Web-zu-App Flow \(1\)](#)

#### (1 a) Falls der Autorisierungsserver des Fachdienstes das EntityStatement des IDP noch nicht kennt, lädt er dies herunter

Request analog [App-zu-App Flow \(1a\)](#):

#### (1 b) Der IDP sendet sein EntityStatement zurück

Response analog [App-zu-App Flow \(1b\)](#)

#### signed\_jwks

Die Werte sind analog zu [App-zu-App Flow \(1b-signed\\_jwks\)](#)

#### (1 c) Der Autorisierungsserver des Fachdienstes ruft das Entity Statement zum IDP beim Federation Master ab

Request analog [App-zu-App Flow \(1c\)](#)

## **(1 d) Der Federation Master sendet sein EntityStatement über den angefragten sektoralen IDP zurück**

Response analog zu [App-zu-App Flow \(1d\)](#)

## **(2) Der Autorisierungsserver des Fachdienstes sendet ein (Pushed) Authorization Request an den Authentication Endpunkt (Auth ES) des sektoralen IDP**

HTTP-POST analog [App-zu-App Flow \(2\)](#) inclusive TLS Clientauthentisierung.

## **(2 a) Falls der IDP das EntityStatement des Autorisierungsserver des Fachdienst noch nicht kennt, lädt er dies herunter.**

Request analog [App-zu-App Flow \(2a\)](#)

## **(2 b) Der Autorisierungsserver des Fachdienst sendet sein EntityStatement zurück und der IDP registriert ihn als Client**

Response analog [App-zu-App Flow \(2b\)](#)

### **signed\_jwks**

Die Werte sind analog zu [App-zu-App Flow \(2b-signed\\_jwks\)](#)

## **(2 c) Abruf des Entity Statement zum Fachdienst beim Federation Master**

Request analog [App-zu-App Flow \(2c\)](#)

## **(2 d) Der Federation Master sendet sein Entity Statement über den Fachdienst zurück**

Response analog [App-zu-App Flow \(2d\)](#)

## **(3) Der Authentication-Endpunkt (Auth EP) des sektoralen IDP antwortet dem AS des Fachdienst mit einer Request URI**

Response analog [App-zu-App Flow \(3\)](#)

## **(4) Der Authorization Server des Fachdienst antwortet dem Web-Backend mit einem redirect und seiner Request URI**

Der Autorisierungsserver antwortet dem Web-Backend mit Request-URI und Client ID zur Weiterleitung über das Anwendungsfondend an die Adresse des Authenticator des IDP.

## **(5) Das Web-Backend antwortet dem Frontend mit einem redirect und seiner Request URI**

Das Web-Backend leitet den Redirect an das Anwendungsfondend weiter.

## **(6) Das Web-Frontend öffnet die URI und damit eine Authentifizierungsseite des IDP**

HTTP-GET analog [App-zu-App Flow \(5\)](#) - allerdings gibt es in diesem Fall eben kein Authenticator Modul des sektoralen IDP auf dem Gerät und daher wird unter der Adresse eine Authentifizierungsseite im Browser geöffnet.

## **(6a-d) Anwender authentifiziert sich nach dem Verfahren des IDP**

Der Anwender authentifiziert sich nach dem Verfahren des IDP. Dabei kann als 2. Faktor eine Authenticator-App auf einem 2. Gerät verwendet werden.

Beispielablauf:

6a) IDP Login-Seite im Browser Gerät 1 Identifikation des Nutzers (möglicherweise/ratsam über ersten Faktor z.B. Name/Passwort)

6b) IDP Prüfung der Credentials (Optional wenn 1 Faktor genutzt)

6c) Initiierung des 2. Faktor durch Aufforderung an den Anwender zum Öffnen des Authenticator-Modul auf einem 2. Gerät oder durch ein push des IDP auf das Gerät mit der Authenticator-Modul

6d) **Authenticator-Modul Gerät 2** IDP Abschluß der Authentisierung

Der Nutzer könnte auch im Schritt 6a einen Code vom IDP gezeigt bekommen und tippt/scant diesen im Authenticator-Modul ein. Auch dies kann eine Kopplung der App zum Prozess beim IDP herstellen.

Varianten gibt es verschiedene aber es muss klar sein zu welcher Session (Request URI) beim IDP diese Authentisierung gehört.

### **(7) Der Authorization-Endpunkt des sektoralen IDP antwortet dem Web-Frontend (Browser) mit einem Redirect zum Fachdienst**

Die Authentifizierungsseite des Authorization-Endpunkt des sektoralen IDP reagiert und sendet dem Web-Frontend einen Redirect zum Fachdienst und den "AUTHORIZATION\_CODE".

Redirect analog [App-zu-App Flow \(7\)](#)

### **(8) Das Web-Frontend (Browser) leitet den "AUTHORIZATION\_CODE" an das Web-Backend der Anwendung weiter**

Das Anwendungsfrentend gibt die Information mit dem "AUTHORIZATION\_CODE" an das Web-Backend der Anwendung weiter.

### **(9) Das Web-Backend der Anwendung leitet den "AUTHORIZATION\_CODE" an den Autorisierungsserver des Fachdienstes**

HTTP-POST analog [App-zu-App Flow \(9\)](#)

### **(10) Der Autorisierungsserver reicht den "AUTHORIZATION\_CODE" und den "Code\_Verifier" beim Token-Endpunkt des IDP ein.**

HTTP-POST analog [App-zu-App Flow \(10\)](#) inclusive TLS Clientauthentisierung.

### **(11) Der Autorisierungsserver erhält vom Token-Endpunkt des IDP einen ID\_TOKEN und ACCESS\_TOKEN mit den gewünschten Claims, der mit dem öffentlichen Schlüssel aus der Registrierung verschlüsselt ist.**

Response analog [App-zu-App Flow \(11\)](#)

### **(11) Einlösen des ACCESS\_TOKEN und Datenabruf**

- Web-Anwendung weiterer Ablauf analog ab [Web-zu-App Flow \(11\)](#)