VIDIS

(Pilot) Whitepaper zur Anbindung an VIDIS für Service Provider

Version: 13
Exportiert am 20-06-2022

Das Medieninstitut der Länder

Inhaltsverzeichnis

Informationen für Service Provider (SP)

Um die geordnete Anbindung eines "Service Providers" an das VIDIS-System zu ermöglichen, müssen entsprechende Metadaten gemäß https://openid.net/specs/openid-connect-discovery-1_0.html ausgetauscht werden.

In diesem Dokument wird ausschließlich auf den Fall einer Anbindung von Angeboten (Webseiten und Apps) als OpenID Connect Client eingegangen.

Es werden in späteren Projektphasen noch weitere SSO-Technologien für den Einsatz evaluiert. Es ist jedoch unwahrscheinlich, dass der produktive VIDIS-Dienst später viele weitere SSO-Technologien unterstützen wird.

Pilotsystem

Ein Demosystem / Proof of Concept (PoC) ist derzeit in Betrieb. Alle Tests, insbesondere die Test-Anbindungen, werden derzeit an diesem VIDIS-System durchgeführt. Dieses Demosystem wird in Zukunft dauerhaft als Integrations- und Testsystem für die VIDIS-Infrastruktur dienen und eine Anbindung wird Voraussetzung für die Anbindung an das Pilotsystem sein. Das Pilotsystem verhält sich analog und die Inbetriebnahme des Pilotsystems läuft aktuell.

Anbindung eines OpenID Connect Client

Für die Anbindung eines OpenID Connect Clients müssen folgende Parameter ausgetauscht und sowohl im VIDIS-System als auch beim anzubindenden OpenID Connect Client konfiguriert werden.

FWU/VIDIS an SP zusammengefasst

- **"ClientID":** der Identifikator des anzubindenden OpenID Connect Clients
- **"Client Secret"**: ein zwischen VIDIS und dem OpenID Connect Client geteiltes Geheimnis
- **"Authorize Endpoint":** https://aai.vidis.schule/auth/realms/vidis/protocol/openid-connect/auth
- **"Access Token Endpoint":** https://aai.vidis.schule/auth/realms/vidis/protocol/openid-connect/token

Die maschinenlesbare OpenID Connect Konfiguration befindet sich zusammengefasst unter: https://aai.vidis.schule/auth/realms/vidis/.well-known/openid-configuration

SP an FWU/VIDIS zusammengefasst

Notwendig:

- **"Valid Redirect URIs":** zulässige Redirect URIs

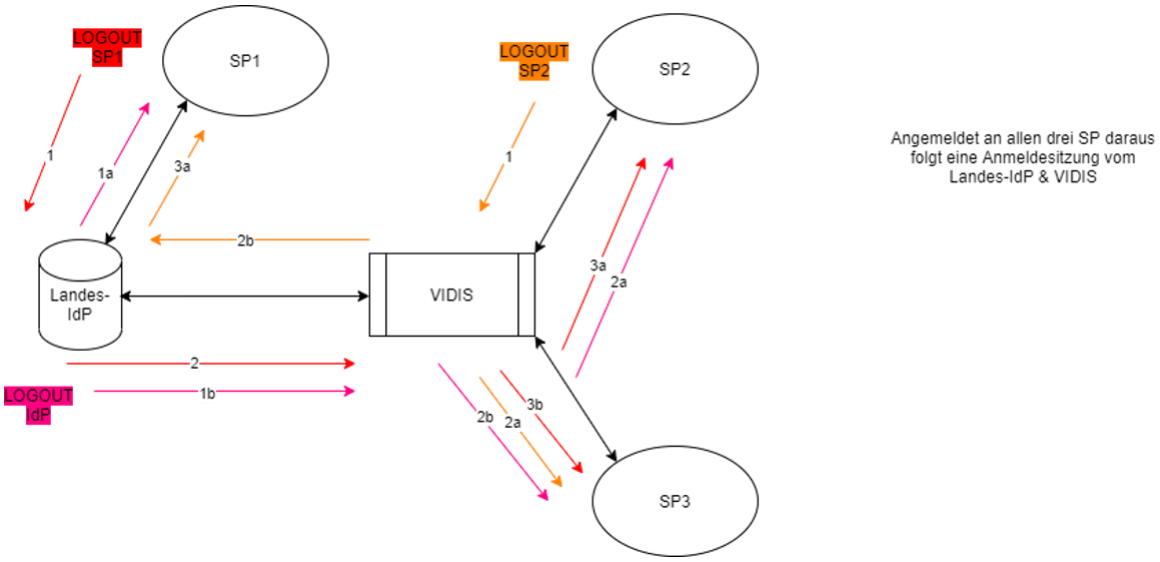
- **"BaseURL":** zum testen der Verbindung von FWU-Seite (Das ist der Einstiegspunkt bzw. das Login Formular)
- **"Deeplink" ins Angebot:** Wird benötigt um von Landesportalen mit Session direkt in Ihr Angebot zu springen ohne erneute Anmeldung. Dafür muss ein Parameter angehängt werden → "kc_idp_hint" (siehe unten: Weitere technische Voraussetzungen)

Optional:

- Social-Media-Vorschaubild für Deeplink: Hilfreich bei Verlinkung bzw. Anzeige in Lern-Management-Systemen, Mediatheken und Portalen

Single Log-out

Die Pilotländern haben die Anforderung nach einem „Logout from all Services and Devices" formuliert. Insbesondere aufgrund einer Vielzahl geteilter Endgeräte an Schulen. Dies entspricht dem höchstem Sicherheitsgrad. Folgendes Schaubild stellt die Prozesse des Logouts dar.

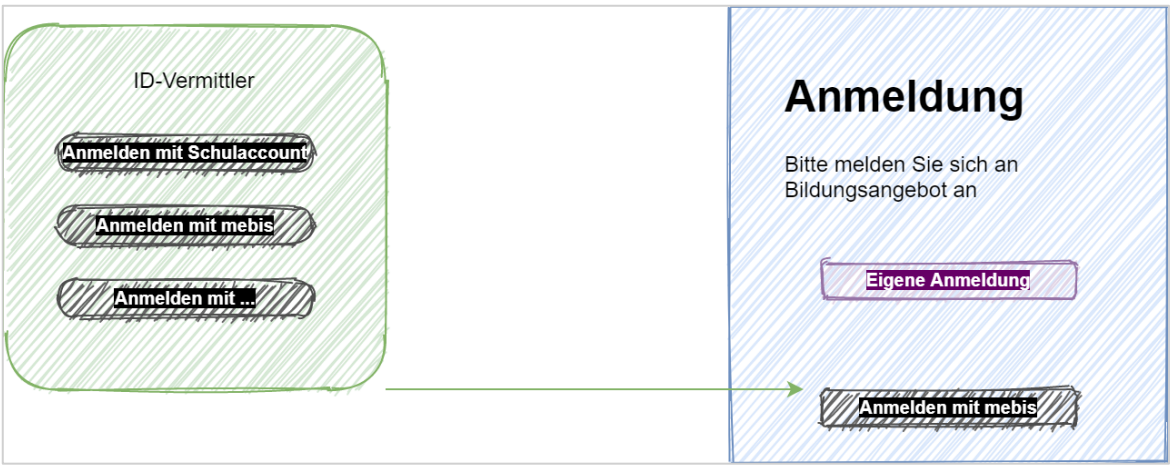


Konfiguration Single Log-out

Sie müssen als Serviceprovider sicherstellen dass beim Logout an Ihrem Dienst folgende URL aufgerufen wird: https://aai.vidis.schule/auth/realms/vidis/protocol/openid-connect/logout

Integration VIDIS Button

VIDIS bietet eine (JavaScript) Client-Bibliothek an, die von Bildungsangeboten eingebunden werden kann. Sie hat zum Ziel, die Usability deutlich zu verbessern, ohne zu stark in das User-Interface der Bildungsangebote einzugreifen. Eine Teilnahme an VIDIS ist auch ohne diese Client-Bibliothek möglich. Allerdings ist es wünschenswert den Button einzubinden.



Code zur Einbindung auf Anmeldeseite

Einbindung des Buttons in ihr Projekt.

Der VIDIS Button wird als Web Componente angeboten und ist über einen kleinen Codeschnipsel einzubinden. Die Scriptdatei liegt auf einem Server in einem unserer Rechenzentren. Sie können die js Datei entweder über CDN einbinden oder Runterladen und direkt in ihr Projekt integrieren. Dann haben Sie aber den Nachteil, ggf. nicht die neueste Version zur Verfügung zu haben.

Example - Einbindung des Buttons via Web Component

```
<!DOCTYPE html><meta charset="utf-8" /> <title>vidisLogin demo</title>
<script src="./vidisLogin.umd.js"></script>
<link rel="stylesheet" href="./vidisLogin.css" />
<vidis-login></vidis-login>
```

Weitere technische Voraussetzungen

Automatische Registrierung bei initialer Anmeldung

Voraussetzung für Service Provider ist, dass Nutzerinnen und Nutzer, die sich an dem digitalen Bildungsangebot erstmalig anmelden, bei der Anmeldung automatisch registriert werden.

Weitergabe des Parameter kc_idp_hint

Voraussetzung für Service Provider ist, die automatische Weitergabe des Parameter kc_idp_hint (z.B. "?kc_idp_hint=Landessystem") während der Anmeldung. Für einige Anwendungsfälle (z.B. Direktaufruf aus Landessystemen heraus) ist die Vorauswahl eines Landes-IdP wichtig. Der VIDIS-Dienst unterstützt diese Vorauswahl durch Übergabe des Parameter kc_idp_hint. Dieser Parameter muss also bei aufrufen (z.B. bei Authorization Requests) uneditiert weitergegeben werden und darf nicht herausgefiltert werden.

Userinfo überprüfen

Über den endpoint https://aai.vidis.schule/auth/realms/vidis/protocol/openid-connect/userinfo können Sie sich die Übermittelten Userdaten unsererseits ansehen.

Das funktioniert wie folgt.

Schritt 1: Zuerst muss ein Token generiert werden.

Dieser Token (access_token) fungiert als "Bearer Token" der zum Abruf der User Info genutzt werden kann und zu Debugging zwecken, der Redirect Flow wird bei der finalen Integration verwendet.

```
curl --location --request POST
'https://aai.vidis.schule/auth/realms/vidis/protocol/openid-connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'username=XXXXX' \
--data-urlencode 'password=XXXXX' \
--data-urlencode 'grant_type=password' \
--data-urlencode 'client_id=account'
```

Schritt 2: Jetzt lassen sich die Userdaten mit dem Token abrufen

```
curl --location --request GET
'https://aai.vidis.schule/auth/realms/vidis/protocol/openid-
connect/userinfo' \
--header 'Authorization: Bearer <TOKEN>
```

oder alternative zu Schritt 2 wäre es den JWT Token zu dekodieren, um die Nutzerdaten auslesen zu können. Hierzu kann beispielsweise auch ein entsprechendes Online Tool verwendet werden (z. B. über https://devtoolzone.com/decoder/jwt, https://jwt.io/ etc.), sofern es sich nicht um reale Nutzerdaten handelt.

Das Ergebnis ist ein JSON mit den Userdaten:


```
{
   "sub": "39e0063a-8377-4a1c-bd15-ea16f65a5a15",
}
```


Fragen & Anregungen

Für Fragen und Anregungen melden Sie sich gerne jederzeit unter vidis@fwu.de