Gematik IDP Identity Provider

Version 0.1-SNAPSHOT, 2020-10-31T23:18:46Z

Inhaltsverzeichnis

Kapitel 1. Übersicht

Der Gematik IDP Server dient zur Identifizierung von Versicherten und Leistungserbringenden Organisationen.

1.1. Aktuelle Version

Version : 0.1.0

1.2. Lizenzinformationen

Lizenz : Apache 2.0
Lizenz-URL : http://www.apache.org/licenses/LICENSE-2.0
Nutzungsbedingungen : null

1.3. URI Schema

Host : 172.17.0.2:8080
Basis-Pfad : /v2/api-docs

1.4. Tags

- Idp-Dienst : Idp Controller
- discovery-document-controller : REST Endpunkt für das Abfragen der öffentlichen Informationen des IDP Rest Services
- key-information-controller : Key Information Controller

Kapitel 2. Einführung

Der manual_content.adoc Gematik IDP Server dient zur Identifizierung von Versicherten und Leistungserbringenden Organisationen.

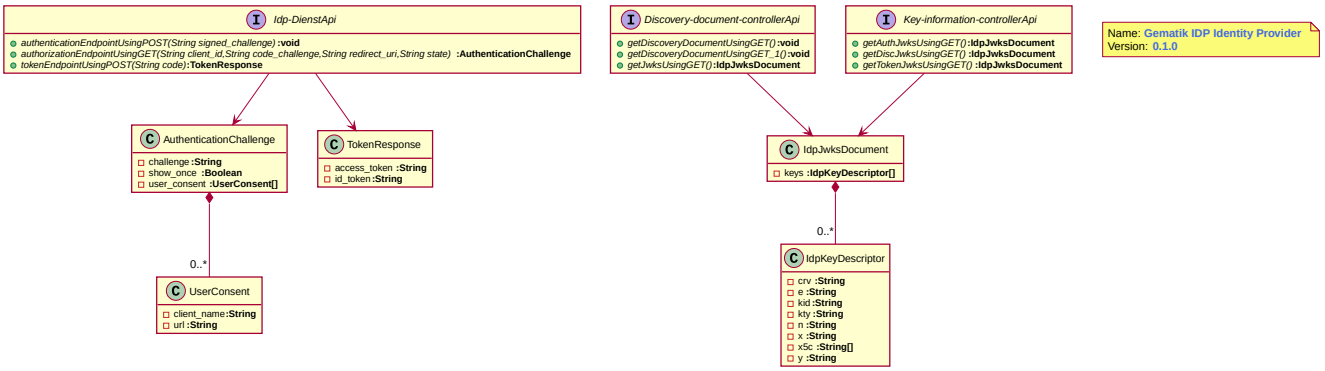

Abbildung 1. Klassenübersicht

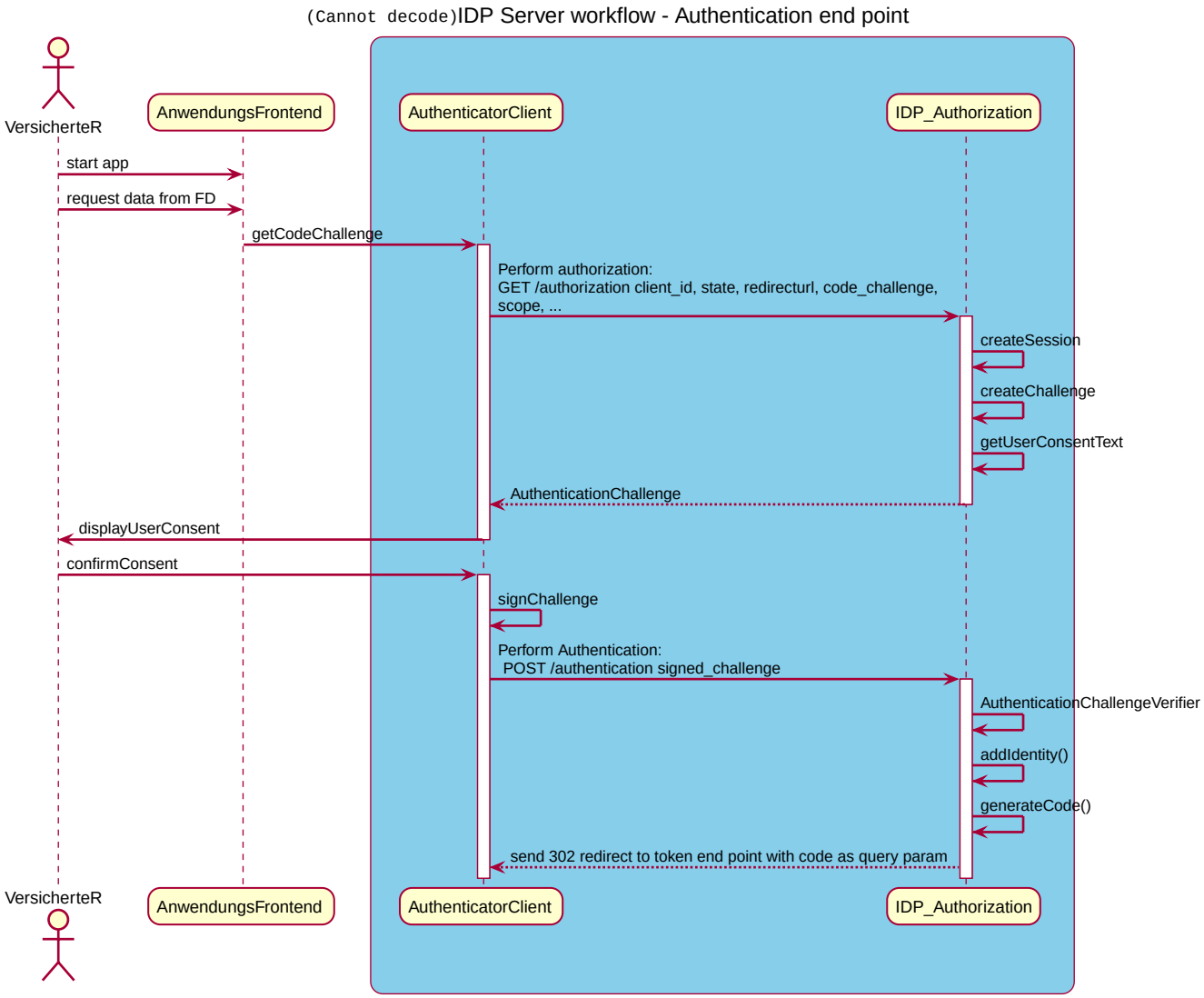

Abbildung 2. Ablauf Authentifizierung

Kapitel 3. Ressourcen

3.1. Idp-Dienst

Idp Controller

3.1.1. authenticationEndpoint

```
POST /authentication
```

Parameter

Typ	Name	Beschreibung	Typ
Query	**signed_challenge** *verpflichtend*	signed_challenge	string

Antworten

HTTP Code	Beschreibung	Typ
200	OK	Kein Inhalt
201	Created	Kein Inhalt
401	Unauthorized	Kein Inhalt
403	Forbidden	Kein Inhalt
404	Not Found	Kein Inhalt

Verarbeitet

- `application/json`

Erzeugt

- `*/*`

3.1.2. authorizationEndpoint

```
GET /authorization
```

Parameter

Typ	Name	Beschreibung	Typ
Query	**client_id** *verpflichtend*	client_id	string
Query	**code_challenge** *verpflichtend*	code_challenge	string
Query	**redirect_uri** *verpflichtend*	redirect_uri	string
Query	**state** *verpflichtend*	state	string

Antworten

HTTP Code	Beschreibung	Typ
200	OK	AuthenticationChallenge
401	Unauthorized	Kein Inhalt
403	Forbidden	Kein Inhalt
404	Not Found	Kein Inhalt

Erzeugt

- */*

3.1.3. Frage nach einem Token

```
POST /token
```

Beschreibung

Tokenanfrage mittels AUTHORIZATION_CODE

Parameter

Typ	Name	Beschreibung	Typ
Query	**code** *verpflichtend*	Toke response code	string

Antworten

HTTP Code	Beschreibung	Typ
200	Successfully retrieved list	TokenResponse
201	Created	Kein Inhalt
401	You are not authorized to view the resource	Kein Inhalt
403	Accessing the resource you were trying to reach is forbidden	Kein Inhalt
404	The resource you were trying to reach is not found	Kein Inhalt

Verarbeitet

- `application/json`

Erzeugt

- `*/*`

3.2. Discovery-document-controller

REST Endpunkt für das Abfragen der öffentlichen Informationen des IDP Rest Services

3.2.1. Liefere alle öffentlich verfügbaren Informationen zum IDP Server

```
GET /auth/realms/idp/.well-known/openid-configuration
```

Beschreibung

Diese Daten sind mit dem privaten Schlüssel des IDP Servers verschlüsselt(?)

Antworten

HTTP Code	Beschreibung	Typ
200	OK	string

HTTP Code	Beschreibung	Typ
401	Unauthorized	Kein Inhalt
403	Forbidden	Kein Inhalt
404	Not Found	Kein Inhalt

Erzeugt

- `application/json`

3.2.2. Liefere alle öffentlich verfügbaren Informationen zum IDP Server

```
GET /discoveryDocument
```

Beschreibung

Diese Daten sind mit dem privaten Schlüssel des IDP Servers verschlüsselt(?)

Antworten

HTTP Code	Beschreibung	Typ
200	OK	string
401	Unauthorized	Kein Inhalt
403	Forbidden	Kein Inhalt
404	Not Found	Kein Inhalt

Erzeugt

- `application/json`

3.2.3. Liefere das Jwks Dokument(?)

```
GET /jwks
```

Beschreibung

(?)

Antworten

HTTP Code	Beschreibung	Typ
200	OK	IdpJwksDocument
401	Unauthorized	Kein Inhalt
403	Forbidden	Kein Inhalt
404	Not Found	Kein Inhalt

Erzeugt

- */*

3.3. Key-information-controller

Key Information Controller

3.3.1. getAuthJwks

```
GET /authKey/jwks.json
```

Antworten

HTTP Code	Beschreibung	Typ
200	OK	IdpJwksDocument
401	Unauthorized	Kein Inhalt
403	Forbidden	Kein Inhalt
404	Not Found	Kein Inhalt

Erzeugt

- */*

3.3.2. getDiscJwks

```
GET /discKey/jwks.json
```

Antworten

HTTP Code	Beschreibung	Typ
200	OK	IdpJwksDocument
401	Unauthorized	Kein Inhalt
403	Forbidden	Kein Inhalt
404	Not Found	Kein Inhalt

Erzeugt

- */*

3.3.3. getTokenJwks

```
GET /tokenKey/jwks.json
```

Antworten

HTTP Code	Beschreibung	Typ
200	OK	IdpJwksDocument
401	Unauthorized	Kein Inhalt
403	Forbidden	Kein Inhalt
404	Not Found	Kein Inhalt

Erzeugt

- */*

Kapitel 4. Definitionen

4.1. AuthenticationChallenge

Name	Typ
challenge *optional*	string
show_once *optional*	boolean
user_consent *optional*	UserConsent

4.2. IdpJwksDocument

Name	Typ
keys *optional*	< IdpKeyDescriptor > array

4.3. IdpKeyDescriptor

Name	Typ
crv *optional*	string
e *optional*	string
kid *optional*	string
kty *optional*	string
n *optional*	string
x *optional*	string

Name	Typ
x5c *optional*	< string > array
y *optional*	string

4.4. TokenResponse

Antwort des Gematik IDP Servers auf Tokenanfragen

Name	Beschreibung	Typ
access_token *optional*		string
id_token *optional*	ID Token	string

4.5. UserConsent

Name	Typ
client_name *optional*	string
url *optional*	string