Authentication and Authorisation

This section contains a description of the authentication and authorisation process when integrating with VMS.

1.

Authorization Code Flow With PKCE

An **Identity Provider (IdP)** has been established specifically for authentication and authorization purposes on our APIs. To interact with the APIs, it is essential to authenticate through the Identity Provider. This involves utilizing specific endpoints to obtain an Authorization Code and various tokens (Access token, ID token, and Refresh token).

2.

Client Credential Flow

An Identity Provider (IdP) was created for authentication and authorization purposes on the TaxCore API.

Authorization Code Flow With PKCE

An **Identity Provider (IdP)** has been established specifically for authentication and authorization purposes on our APIs. To interact with the APIs, it is essential to authenticate through the Identity Provider. This involves utilizing specific endpoints to obtain an Authorization Code and various tokens (Access token, ID token, and Refresh token).

Obtaining an Authorization Code

To issue an Authorization Code, initiate a GET request to endpoint

GET https://{{hostname}}/connect/authorize

Query parameters:

- response_type must be 'code', indicating that an authorization code is expected
- client_id assigned to each application by the administrator
- client_secret also assigned by the administrator
- redirect_uri specifies the URI to redirect the user to after authorization is completed
- **scope** a string provided by the administrator that denotes the set of endpoints the application can
- state a randomly generated string by your application, which will be verified for authenticity
- **code_challenge** a string created by hashing the code_verifier with SHA256 and encoding the result in base64 URL encoding
- code_challenge_method must be 'S256'

Issuing a Token

For token issuance, send a POST request to endpoint

POST https://{{hostname}}/connect/token

Request body parameters:

- grant_type should be 'authorization_code'
- code the code received from the previous request
- redirect_uri must match the redirect URI provided in the authorization request
- code_verifier a random string between 43 and 128 characters
- client_id assigned per application by the administrator
- client_secret assigned per application by the administrator

sequenceDiagram participant A as User participant B as Application participant C as Identity Provider (IdP) participant D as TaxCore API A->>B: Click login link B->>B: Generate code verifier

Request Authorization Code

+ challenge C->>A: Redirect to login/authorization prompt A->>C:
Authenticate and consent C->>B: Issue Authorization Code B->>C: Authorization Code

+ verifier C->>C:
Validate code verifier

+ Code challenge C->>B: Issue Access, ID and Refresh token B->>D: Request resource

+ access token D->>B: Return response

Using the Access Token

Utilize the obtained access token as a Bearer token for each API request by adding it to the request header:

Authorization: Bearer {access_token}

The access token is valid for a set period (currently 30 minutes), allowing multiple API requests with the same token. Any changes to the validity period will be communicated timely by the administrator.

Refreshing Tokens

You can exchange your refresh token for a new set of tokens (access, ID, and refresh tokens). The old set will be deactivated following this exchange, which helps ensure that users do not need to repeatedly enter their credentials while remaining active.

sequenceDiagram participant A as Application participant B as Identity Provider (IdP) A->>B: Client application id + secret + refresh token B->>A: Issue Access, ID and Refresh token

Client Credential Flow

An Identity Provider (IdP) was created for authentication and authorization purposes on the TaxCore API.

Before calling the TaxCore API, it is necessary to call the Identity Provider, by calling the endpoint **POST** https://{hostname}}/connect/token with a body containing 4 parameters:

- 1. **grant_type** always has the value *client_credentials*
- 2. client_id assigned per application by VMS
- 3. **client_secret** assigned per application by VMS
- 4. **scope** a string obtained from VMS and representing a set of endpoints to which the application is entitled

When the application makes a request, it receives an access token from the IDP as a response.

Use the obtained access token as a *Bearer* token for each request to TaxCore API. To do this, add the key *Authorization* with the value *Bearer access_token* to the header of each request.

The access token has a determined validity period, enabling multiple requests to the TaxCore API with the same token. The validity period of the token is configured by VMS and it is currently 30 minutes. Any change is timely communicated.

sequenceDiagram participant A as Application participant B as Identity Provider (IdP) participant C as TaxCore API A->>B: Authentication ClientID + Secret B-->>A: Issue Access Token A->>C: Request resource + Access token C-->>A: Return resource