OpenID Connect federation in Digital Access component

This article describes OpenID Connect in Smart ID Digital Access component (Hybrid Access Gateway).

- If you want to set up the Digital Access component as an OpenID provider, refer to Set up Digital Access component as OpenID provider.
- If you want to set up the Digital Access component as an OpenID Connect relying party, refer to Set up Digital Access component as OpenID Connect relying party.

What is OpenID Connect?

OpenID Connect is a federation technology, comparable with SAML 2.0, that is implemented as an identity layer on top of the OAuth 2.0 protocol.

With OpenID Connect, a range of clients, including Web-based, mobile, and JavaScript clients, can verify the identity of an end-user, based on authentication performed by an authorization server or identity provider (IdP). Clients can also obtain basic profile information about the end-user.

Several digital identities, such as Norwegian BankID and Verimi, are based on OpenID Connect.

OpenID Connect concepts

- **Relying party (RP)**
  An OAuth 2.0 client application requiring end-user authentication and claims from an OpenID provider.

- **OpenID provider (OP)**
  An OAuth 2.0 authorization server that authenticates the end-user and provides claims to a relying party about the authentication event and the end-user.

- **Claim**
  Piece of information asserted about an entity.

- **Scopes**
  The permissions a client is allowed to ask for.

- **Authentication request**
  An OAuth 2.0 authorization request using extension parameters and scopes defined by OpenID Connect. The request is that the end-user shall be authenticated by the authorization server, which is an OpenID provider, to the client, which is a relying party.

Related information

- Authentication methods
- Set up Digital Access component as OpenID Connect relying party
- Configure OAuth 2.0 in Digital Access