Authentication flows

Federated authentication means that a user logs in on another location (an Identity Provider) than that of the accessed service (a Service Provider). SURFconext is located between those locations. Each of the providers has only one trusted connection with SURFconext: this is why this is called a **hub-and-spoke federation**. The connections are 'trusted', because both the Service Provider and the Identity Provider have identified themselves to SURFconext.

Read on to find out more about the ***authentication flow*** when using SURFconext. Your service must use SAML or OpenID Connect when you connect with SURFconext. These are both standards for exchanging authentication and authorization data between parties, identity providers and service providers.

- SAML Authentication flow
  - SAML is an XML-based markup language for security assertions, statements that service providers use to make access-control decisions. Read this page to find out more about the authentication flow when your application supports SAML.
- OpenID Connect Authentication flow
  - OpenID Connect or OIDC is an identity layer on top of the OAuth 2.0 protocol, which allows computing clients to verify the identity of an end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end-user in an interoperable and REST-like manner. As an example, if you build a mobile app you will most likely use OIDC.

Navigate