Preparation with OpenID Connect

If you want to use OpenID Connect you will have to make sure your software supports this protocol. Several software products already support OpenID Connect out of the box. If your software is amongst these, you can continue to to the paragraph about Claims and attributes below.

We strongly advise you **not** to build your own OpenID Connect implementation, but use one of the products already available. The official OpenID website provides a nice overview of certified and uncertified implementations.

Claims and attributes

Most services require extra information about the authenticated user, such as a name, email address or affiliation. In OpenID Connect (OIDC), this extra information comes in the form of **claims**, whereas in SAML, claims are called **attributes**. In SURFconext, the user authenticates at his Identity Provider (called *OpenID Provider* in OIDC) - this all happens using SAML. SURFconext translates the incoming SAML attributes to OIDC Claims and provides them at the userinfo endpoint for your Service Provider (called *Relying Party* in OIDC) to consume. Read this page to see which claims are available for use within your service.

SURFconext has a **data minimisation** policy, which means you only receive those claims that are **strictly needed** to make your service work.

Mobile Apps

If you are building a mobile app you will most likely use OIDC. Please follow the guidelines as depicted here.

Next step

Once you have implemented OpenID Connect in your application and you want to start testing, you can connect to the SURFconext Test environment.

Navigate