Consent handling

A key feature of the OIDC Provider from BankID is to handle consent from the end-user to authorize OIDC Clients to access Value-Added Service (VAS) on behalf of the end-user. Consent handling takes place on a per scope basis and the end-user normally gives his consent in a dialogue tailored to the scope (s) and Value-added Service (VAS) in question. Since consent handling happens after the authentication phase of the message flow, any consent dialogue for a particular VAS is the same across all supported IDPs. This results in uniform consent handling and is a key characteristic of the OIDC Provider from BankID.

The ability to handle partial consents is another key characteristic of the OIDC Provider from BankID. The request from an OIDC Client for a given scope will most oftenly concern several claims. Partial consent referes to situation when the end-user gives his consent for some of the affected claims, but not all of them. The OIDC Provider will in such a case return a successful authentication, at the same time making note of the sub-set of claims that was actually consented. Consented claims are made available to the OIDC Client subsequently, either as part of the ID Token or as part of the response from an endpoint of a VAS-service supported by the OIDC Provider. Un-consented claims are not made available to the requesting OIDC Client.

Generic logic for consent handling is contained in the OIDC Provider together customization options. Consent handling is otherwise governed by external components as illustrated for the TINFO service in the example message flow. Each VAS-module supported by the OIDC Provider has its own component with GUI and logic for consent handling for that particular VAS. The OpenID Connect Provider from BankID uses web-client technology from BankID to reduce the surface of attack on such GUIs. Ensuring that the consent shown to the user is not spoofed and corresponds to the authorization actually granted is key to maintain trust in the OIDC Provider. This corresponds to the classical WYSIWYS-challenge associated with digital signing. Know-how from the BankID signing service is used to build a high-trust solution for consent handling in the OIDC Provider.

See further details on consent handling for each of the supported Value-Added Service.