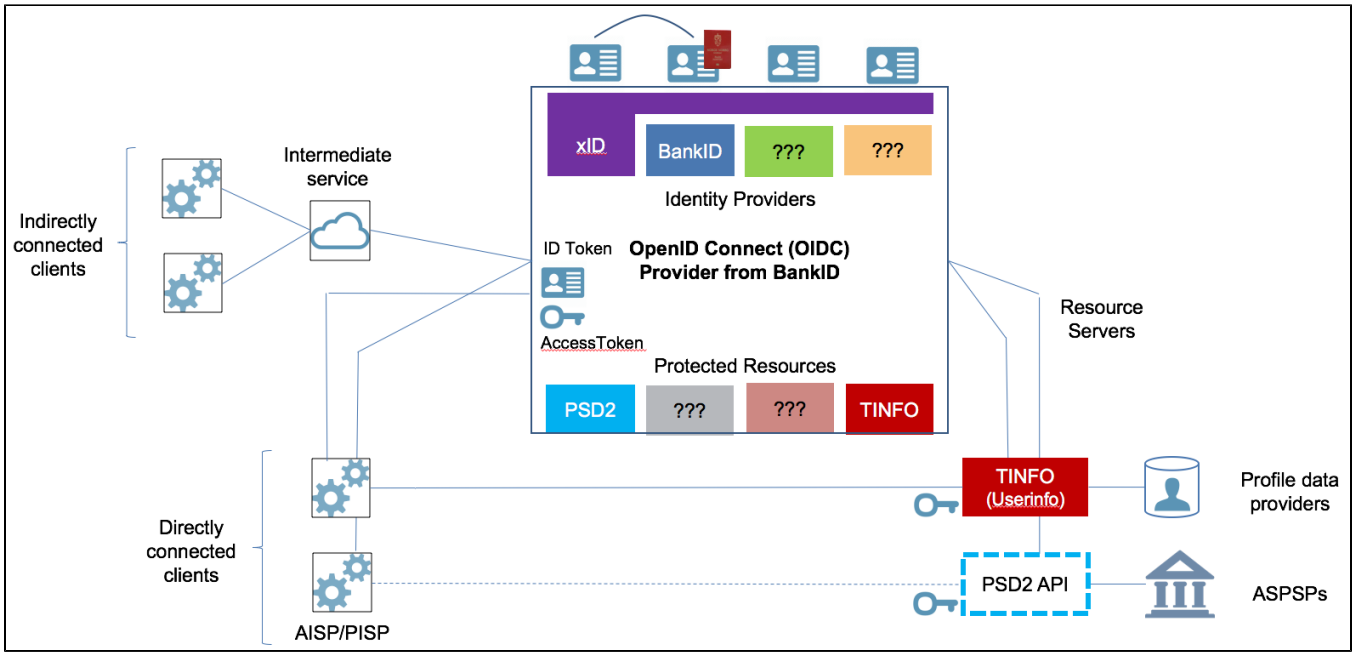
Overview

The OpenID Connect Provider from BankID (hereafter referred to as the OIDC Provider) is illustrated below. It consists of a industry-standard REST API (le ft side) in front of various Identity Providers (IDP) and Value Added Services (VAS). The REST API implements a set of Endpoints defined by the OpenID Connect 1.0 authentication standard and the OAuth 2.0 authorization framework. The OIDC Provider supports several message flows (grant types). Secur e consent handling is a key feature for any flow that involves access to resources owned by the end-user.

The preferred way to integrate with the OIDC Provider is to use a set of JavaScript connectors being front-end wrappers of the API.

A major benefit of the OIDC Provider is to allow merchants start using the BankID Services with minimum integration effort compared to the legacy integration option (ie. install BankID Server, add a BankID merchant certificate and integrate towards the proprietary API of BankID server). For the xID Service the OIDC Provider is the only integration option available to merchants.

As suggested by the figure, note that xID plays an important role among all IDP-options since it can be used to derive the user ID that other IDP-options may depend on. When xID is used with BankID in this way, the end-user is reliefed from entering his national identity number (or phone number) in the first BankID dialgoue.



The term OIDC Client is used for any application that integrates with the OIDC Provider, corresponding to the following terms in related vocabularies:

- OAUth2 clients in OAuth vocabulary
- Relying Party in OIDC vocabulary
- Merchant in BankID vocabulary
- Third Party Provider in PSD2 vocabulary.

OIDC Clients may integrate directly with the OIDC Provider or indirectly via an intermediate party as described in a separate section. OIDC Clients (directly connected or intermediate parties) must authenticate with the OIDC Provider. OIDC Clients use Scopes and Claims to specify content in ID Tokens and request privileges for Access Tokens. Access Tokens regulate access to Value Added Services (VAS). Such resources are available at corresponding Resources Servers (right side) behind protected endpoints.

The TINFO service implements a Resource Server providing end-user profile data over the standard Userinfo endpoint. Access to resources behind this protected endpoint is governed by a standard Access Token and a set of standard Scopes and Claims. Some non-standard Scopes and Claims are also supported for profile data specific for the OIDC Provider from BankID.

The PSD2 service consist of a range of (currently) non-standard Scopes, Claims and Access Tokens tailored for various use-cases under PSD2. In contrast to the TINFO service, note that the PSD2 service does not implement any corresponding Resource Server. PSD2 resources are made availble to AISP/PISPs over an APIs decided by each ASPSP.

The OIDC Provider comes with a default component responsible for all GUI handling. An OIDC Client may override the default GUI and provide its own customized GUI handling hosted at any URL.

Note

A good way to start exploring the OIDC Provider from BankID and its capabilities is to try out live test clients and also consult GitHub for various source code examples.

Some background reading is recommended for readers that are unfamiliar with OpenID Connect and OAuth2