REST API

The REST API comprises implementation of the following set of endpoints according to the OpenID Connect 1.0 and OAuth 2.0 standards. Since these standards are frameworks, any particular implementation of endpoints may make both restrictions and extensions. The OIDC Provider from BankID includes both restrictions by not supporting certain optional parts of the standards and also make extensions by adding non-standard capabilities. See Core Concepts for a closer description of topics like Scopes and claims, ID Tokens, Access Tokens, Consent Handling, etc. that are vital to understand before start using the REST API.

Note the following:

- The above endpoints are general and apply for any Identity Provider and Value Added Service (VAS). Endpoints that apply specifically for any particular VAS are described in the corresponding VAS-section.
- An OIDC Client may use a JS Connector as an alternative to direct integration with the REST API.
- An OIDC Client needs to authenticate with the OIDC Provider for many of the Endpoints.
- The OIDC Provider employs signing and encryption of certain data elements over the REST API. Important examples are signing of ID Tokens an d responses from Userinfo.

A separate section provides details on message flow both over the REST API as such and also the message flow with components behind the REST API.