Known issues

Known issues in this release of the OpenID Connect Provider from BankID are further described below in terms of:

- Restrictions
- Caveats
- Bugs

Restrictions

The following table summarizes restrictions in the latest release of OIDC Provider from BankID:

No	Restrictions
R1	The AML Service currently does not provide residential address from the National Registry. The service does until further return address information from available sources at Bisnode.
R2	Indirectly connected clients of the known-type via Intermediate Services are currently not supported. Such support is planned for a future release.
R3	Some authentication method for OIDC Clients are not supported
R4	Pure app-based applications using a completely embedded (API-based) user-experience is currently not supported. Such support is planned for a future release.
R6	POST method is not supported by Authorize endpoint
R7	Offline Refresh Tokens via the offline_access scope is currently not provided
R8	POST method is not supported by TINFO Userinfo endpoint
R9	The AML Service currently does not support search based on D-number.
R 10	Implicit flow (and hybrid flow) is not supported. Se Message flow details.

Caveats

The following table summarizes caveats in the latest release of the OIDC Provider from BankID:

No	Caveats
C1	The AML Service currently requires that the scope `profile` is provided along with the scope `aml_person/basic` in requests to the authorize endpoint.
C2	Merchants should not use hardcoded base URLs for supported endpoints that are included in the response from Openid-configuration. The recommended practise is to always use any endpoint URL that is contained in the output from Openid-configuration.
C3	The OIDC Provider currently support multi-audience access tokens but may change its support to single-audience token in the future. See the section on Access Tokens for further information on the recommended integration practise to be prepared for such a future possible change.
C4	The `nnin_altsub` claim is never part of an Access Token regardless of the presence of this claim in the corresponding ID Token. Resource Servers that are entitled to receive `nnin_altsub` must be configred to for such access and retrieve this claim via introspection
C5	The default userinfo endpoint in Keyacloak <oidc-baseurl>/protocol/openid-connect/userinfo is replaced by a corresponding userinfo endpoint for TINFO. The latter must be used and is reported in .well-knowi/openid-configuration. The default Keycloack userinfo still responds but does not contain any data that is not already part of the ID Token.
C6	Access to certain scopes may be granted even if such scopes are not explicitly included in the request to Authorize or Token endpoints. This will happen if the OIDC Client is configured with access to such scopes, and such scopes are defined as default in the OIDC Provider.
C7	Scopes requested via Authorize or Token endpoints may be silently ignored without any error to the OIDC Client if (i) the scope value is mis-spelled and (ii) the client in question is not configured for access to the scope(s) in question. To avoid mis-spelling, note that scopes values are case-sensitive.
C8	The scope parameter is disregarded for Refresh Token requests to the Token endpoint. Granted claims for a refreshed Access Token are always according to the scopes included in the original request to the Authorize or Token endpoints
C9	The `aud` claim in Access Tokens and Refresh Tokens has a singelton-format and not a list-format (with a single entry) if there is only one audience involved. Hence, implementors must deal with both singelton-values and list-values for this claim.

C10	JS Connector login window may not close on Internet Explorer / Edge browsers when Cross-domain messaging is used. If you follow the methods demonstrated in the example using cross-domain messaging from the redirect_uri to the JS Connector instance on the parent page, and you use window method, then you will most likely experience that Internet Explorer blocks the communication between the window and the parent. This can happen when the window being opened is on a different domain than the parent site. To work around this problem, you need to setup an endpoint on your domain as the `doInit` `oauth_url` parameter which then redirects to the proper Authorize endpoint. This way the window is opened on your own domain and cross domain messaging should work.
C11	Missing or empty query parameteres when calling JS Connector `doConnect` in certain cases. This is probably due to `doInit` not being called before `doConnect` is called for some reason. The `oidc-connector-loaded` event waits for the page to be loaded before firing. For example, if you call `doInit` when the OIDC loaded event fires, then if the page load slowly you may have a small window where `doConnect` is triggered before the `doInit` call was made. A workaround could be to always call `doInit` before doConnect or go for synchronous loading.

Bugs

The following table summarizes known bugs in the latest release of the OIDC Provider from BankID:

No	Bugs
B1	Language is sometimes not set according to the ui_locales parameter
B2	The error response from TINFO Userinfo is not according to standard
B5	There is a small anomaly with styling of OIDC-client in Microsoft Edge 41