ID Token

The OpenID Connect Provider from BankID provides ID Tokens with claims as shown in the below table. The origin column indicates non-standard claims. Such claims are either added by Keycloack or the result of customization made by the OIDC Provider from BankID.

The ID token structure builds on Keycloack. Three different token configurations are supported as suggested by the scope column, corresponding to three different combinations of the standard scopes `openid` and `profile` and the custom scope `nnin_altsub`.

- A **Minimum ID Token** (scope = openid) that contains a minimum set of claims, among which `sub` and `bankid_altsub` are the only claims that are linked to the actual user. A minimum ID Token can be used by OIDC Clients that need to authenticate end-users in an anonumous way. The `sub` and `bankid_altsub` values do not identify the user unless they are linked by the OIDC Client to other claims about the end user associated that identifies him more precisely.
- A **Regular ID Token** (scope = openid profile) that builds on a minimum ID Token by adding claims that identifies the end-user by his `name` and `birthdate`.
- A **Enchanced ID Token** (scope = ... nnin_altsub) that builds either on a minimum ID Token or a regular ID Token by adding a claim containing the Norwegian National Identity Number of the end-user

As suggested by the IDP column many claims are present for any IDP whereas other claims are dependent on the particular IDP being used. The Eligibility column indicates if a claim is available for any OIDC client or if specific conditions apply. In the latter case eligible OIDC clients must be configured for access in the provisioning process.

Note that the TINFO value-added service supports even more claims about the end-user beyond those contained in the ID Token. The major difference is that none of the claims contained in ID Tokens demand consent from the end user. This is in contrast to claims supported by TINFO that is subject to consent handling.

Note finally that the OIDC Provider form BankID supports signed ID Tokens in JWT format. The below table shows claims in the payload part of the JWT. Claims contained in the JWT header are not shown.

Claim	Origin	Scope	Example	IDP	Eligibility	Description	Comment
Minimum ID Token part							
`typ`	Keycloack	`openid`	`ID`	Any	Any	Token type	Always `ID` for ID Tokens
`acr`	Standard	`openid`	`4`	Any	Any	Authentication Context Class Reference	Level of Assurance (LoA) for IDP option being used
`amr`	Standard	`openid`	`BID`	Any	Any	Authentication Method Reference	Name of IDP option being used to authenticate the end-user. If the end-user is subject to authentication step-up, note that this value may differ from any `amr` value specified in the `login_hint` parameter of the Authorize end-point.
`aud`	Standard	`openid`	`oidc_testclient`	Any	Any	Audience	Always `client_id`
`auth_time`	Standard	`openid`	`1510497762`	Any	Any	Authentication time	Epoc time
`azp`	Standard	`openid`	`oidc_testclient`	Any	Any	Authorized party	Equals `client_id`
`bankid_altsub`	Custom	`openid`	`9578-5999-4-1765512`	BankID and xID	Any	Alternate BankID Subject Identifier	Personal Identifier (PID) / Serial Number) from associated BankID certificate.
`exp`	Standard	`openid`	`1510498063`	Any	Any	Expiration time	Epoc time. Corresponds to a forward session window after `iat`
`iat`	Standard	`openid`	`1510497763`	Any	Any	Issuing time	Epoc time Equal to `auth_time` for new sessions. Is otherwise set at each session refresh.
`iss`	Standard	`openid`	`<oidc-baseurl>`	Any	Any	Issuer Identifier for the Issuer	
`jti`	Standard	`openid`	`7f22fd6a-3d46-4d5a-ae56-6de3c53e1873`	Any	Any	Token identifier	
`nbf`	Standard	`openid`	`0`	Any	Any	Not before time	Epoc time
`nonce`	Standard	`openid`	<random value>	Any	Any	Nonce	
`session_state`	Keycloack	`openid`	`abf823c2-9810-4133-9369-7bff1223d6c1`	Any	Any	GUID related to session handling	
`sub`	Standard	`openid`	`e8c523ff-52a2-42e2-a7a5-f1d0fbb76204`	Any	Any	Subject Identifier	GUID that uniquely identifies the end user across the different IDPs
`updated_at`	Standard	`openid`	`1468582440`	Any	Any	Update time	Epoc time of issuing / create / enrollment of ID in question.
`at_hash`	Standard	`openid`	<hash value>	Any	Any	Access Token hash value	Included for hybrid- and implicit flows
`c_hash`	Standard	`openid`	<hash value>	Any	Any	Code hash value	Included for hybrid flow

`browserEnrolledAt`	Custom	`openid`	`1515437710549`	xID only	Any	Time at which the current browser was enrolled for the xID Service	Epoc time
`tid`	Custom	openid	`2e1eebb7-d5d7-4c55-9410-6ab178070a1c`	Currently only BankID	Any	Transaction ID (reference) for the completed authentication session	Currently used as an input parameter for the securityData endpoint of the Fraud Data service
Regular ID Token part							
`birthdate`	Standard	`profile`	`1966-12-18`	BankID and xID	Any	Birthdate	From associated BankID certificate
`family_name`	Standard	`profile`	`Nilsen`	BankID and xID	Any	Surname (last name)	From associated BankID certificate
`given_name`	Standard	`profile`	`Frode Beckmann`	BankID and xID	Any	Given name (first name)	From associated BankID certificate
`name`	Standard	`profile`	`Nilsen, Frode Beckmann`	BankID and xID	Any	Full name	From associated BankID certificate
Enhanced ID Token part							
`nnin_altsub`	Custom	`nnin_altsub`	`181266*****`	BankID and xID	Available for OIDC clients that uses NNIN as userID for its **already existing users**. For access to NNIN for **enrollment of new users**, see TINFO or AML.	Norwegian National Identity Number (NNIN) as alternate Subject Identifier	Only availble with authorization code flow.