Finnish Trust Network

Danske Bank's Identity Provider
API Document

Table of Content

Change log

Version	Date	Change Summary
1.0	07-02-2019	Initial version
1.1	19-03-2019	Changes made in sections 6, 7, 8 and 9
1.2	01-04-2019	Changes made in section 6.1.5
1.3	04-04-2019	Changes made in sections 8.1.2 and 8.1.3
1.4	11-04-2019	Changes made in sections 8.1.4 and 8.1.5
1.5	04-07-2019	Changes made in section 8.1.6 and 8.2.5 (sub)
1.6	05-08-2019	Changes made in section 7.2.2 (error code) Changes in section 2.1(split to sub sections)
1.7	19-09-2019	New section 8.2.4
1.8	14-05-2020	Changes in section 2.6, 7.1.4 accepted values for acr_values updated to loa2 only. Changes in section 2.2 for support of Chained authentication.
1.9	21-01-2021	- Removed /register endpoint - Change in section 2.2 for chained authentication -Changed in section 4.2.4(request_parameter_supported=true) - New section 6.1.6, 6.1.7, 6.1.8 - Updated section 6.1.4(ftn_chain_level and request) -Updated section 6.2.2(added invalid request object) and 6.2.3(added invalid_request_object)

1.10	03-03-2023	- Signed request object made mandatory. - Parameter updates for authorization endpoint. - Test production and Production document is combined. - Added new section for entity statement. - Added new section for signed jwks. - Removed section for jwks and well known configuration.
1.11	08-05-2023	expires_in in token response is changed from string to numeric as per OIDC standard

1 Introduction

The Finnish Trust Network (FTN) is a mechanism for connecting large scale, consumer-facing service providers with trusted identity providers in Finland. The FTN is a legal framework under which different notified IDP's are mandated to provide strong authentication services for citizens to access public and private services in Finland.

TRAFICOM (Finnish Transport and Communications Agency, formerly FICORA) is the public authority responsible of communication regulations in Finland and has recommendation for two authentication protocols, i.e., **SAML 2** (Security Assertion Mark-up Language) and **OIDC** (OpenID Connect) to be used in FTN.

There are 3 Roles in FTN, namely –

- Identity service providers
- Broker service provider
- Consumer Service Providers / Relying Parties.

This document deep dives in the FTN Identity Provider Services that Danske Bank is offering following the above recommendations by TRAFICOM.

2 Service Description

The Danske Bank Identity Provider implements OpenID Connect Authorization Code flow authentication as defined in FTN OIDC Protocol

The Danske Bank's Identity Provider Service can be integrated with the **Service Providers**. Information exchange MUST take place with both the roles in order to complete the technical integration handshake. Parties exchange the necessary information at the time of service subscription or at the time of signing of the service agreement.

Service Providers can get their end users authenticated using the Danske Bank's Identity Provider service. Service providers can communicate with Danske Bank's identity provider service via specified API endpoints and the keys (SIGNED JWKS) to encrypt and verify messages during the transaction.

If there are changes in the service agreement, the technical and/or business representatives of the parties are REQUIRED to communicate with each other in advance about changes in detail.

2.1 Attributes

2.1.1 Natural person attributes

Danske Bank Identity Provider Service supports only the REQUIRED attributes profile of a Natural Person as per the FTN OIDC Specification. Danske Bank Identity provider can be used to identify only Natural Persons of its Finnish customers.

The Danske Bank Identity Provider service relays/shares the Finnish personal identity code (HETU), family name (FamilyName), first name (FirstNames) and date of birth (DateOfBirth) to the Service Provider / Broker.

2.1.2 Legal attributes

Danske Bank Identity Provider Service supports only the REQUIRED attributes profile of a Legal Person as per the FTN OIDC Specification. Danske Bank Identity provider can be used to identify the legal entity.

The Danske Bank Identity Provider service relays/shares the name of legal person (LegalName) and the VAT registration number (VATRegistration) to the Service Provider / Broker.

2.2 Chained authentication

Danske Bank Identity provider supports Chained Authentication by registering with Danske Bank Identity provider using new Client-Id. If Service Provider or Broker needs to invoke Danske Bank using Chained authentication or normal authentication, then respective Client-Id should be used. Signed JWT request is mandatory for chained authentication during the Authorize request along with the use of the Client ID registered for chained authentication.

2.3 Domain Name

Danske Bank Identity Provider service is implemented in both Test Production and Production environment. Correct domain should be used while invoking the service in required environment.

Production –

https://userapi2.danskebank.com/prod/external/ftn/idp-oidc

Test Production -

https://sandbox-userapi2.danskebank.com/sandbox/external/ftn/idp-oidc

Note: Remember to replace <domain> in all Urls mentions in this document with any of above 2 values as per integration environment.

2.4 Metadata

Danske Bank publishes the metadata of Identity according to the OIDC Connect Discovery 1.0 specification.

The metadata endpoint address is in form of: <domain>/entity-statement

The metadata also includes the SIGNED JWKS URI for the Service Provider/ Broker to fetch the keyset of the identity provider.

2.5 Key Exchange

The public keys used in signing and encryption are exchanged by reference (SIGNED JWKS URI).

The change of signing and encryption keys is done by adding the new key to published keyset in advance of its usage. Both the new and the old keys are concurrently present in the keyset at the time of key change. The new key MUST be published at least 10 (cache) minutes before starting the use of the key. The old key SHOULD be removed from the keyset when the new key has been taken in to use.

2.6 Algorithms and Key sizes

FTN OIDC profile specifies the Cryptographic algorithms for JWT protection in the FTN in signing and encryption of messages.

Danske Bank Identity Provider implements RSASSA-PKCS1-v1_5 using SHA-256 algorithm for signing of messages.

Danske Bank Identity Provider implements RSA-OAEP algorithm using default parameters for key exchange.

Danske Bank Identity Provider implements A128GCM, AES GCM using 128-bit key algorithm for encryption of messages.

Other optional algorithms from FTN OIDC profile are not implemented if not separately and specifically agreed.

2.7 Level of Assurance

Danske Bank Identity Provider implements following Level of Assurance specified in FTN OIDC Profile:

Production - http://ftn.ficora.fi/2017/loa2
Test Production - http://ftn.ficora.fi/2017/loatest2

2.8 Single Sign-On (SSO)

Danske Bank's Identity Provider currently doesn't support Single Sign-On (SSO). An authentication IS REQUIRED from the end user on each Authentication Request.

3 List of endpoints

The list of endpoints of FTN Identity Provider service are listed below –

Sl. No.	Endpoints / API Gateway URI	Name
1	GET <domain>/entity-statement	Entity statement
2	GET <domain>/signed-jwks	Signed JWKs
3	GET <domain>/connect/authorize	Authorize endpoint
4	POST <domain>/connect/token	Token endpoint

4 GET /entity-statement

4.1 Request details

4.1.1 Request endpoint URI

GET	<domain>/entity-statement

4.1.2 Request header

JSON	accept: application/json

4.1.3 Request body

N/A	Not Applicable

4.2 Response details

4.2.1 Response details

The response of this uri is setup according to specification present in OpenID federation. URL for the specification is present below.

https://openid.net/specs/openid-connect-federation-1_0.html#section-4.1

4.2.2 Response type

text/plain	A JWT (Json web token) that contains the information to participate in federation(s).

4.2.3 Response codes

https://userapi2.danskebank.com/prod/external/ftn/idp-oidc/errorcodes

4.2.4 Response example (success)

Ex.	eyJhbGciOiJSUzI1NiIsImtpZCI6InNpZy1kYi1mdG4tMzE4MDY3NzYx IiwidHlwIjoiZW50aXR5LXN0YXRlbWVudCtqd3QifQ.eyJpc3MiOiJod HRwczovL3N5c3QtdXNlcmFwaTIuZGFuc2tlYmFuay5jb20vZnRuLWlkc CIsInN1YiI6Imh0dHBzOi8vc3lzdC11c2VyYXBpMi5kYW5za2ViYW5rL mNvbS9mdG4taWRwIiwiaWF0IjoxNjc5MDM0NDM4LCJleHAiOjE2NzkwN DE2MzgsImp3a3MiOnsia2V5cyI6W3sia3R5IjoiUlNBIiwidXNlIjoic 2lnIiwia2lkIjoic2lnLWRiLWZ0bi0zMTgwNjc3NjEiLCJhbGciOiJSU zI1NiIsImUiOiJBUUFCIiwibiI6IjRRY0c1TkVHWUgwS3R4Tnd0UUQ5V npMSU9oanJxekg0WTlrMjVoVkJjNnBBQVRMTE1oU2VJcnlKQmxteTdQT DZLNmZKOWFtUUVfR2pjelhVX1BFVXRxTlFzaWt2MUo5WGsyOG9yZnNpY XJPY2tQeGN3emVMekxGcHpxcTh0ZFI0OVFiajZ3XzEzSTlyVU5saTlIe E9HZ1NqRHl2MEhFeDRpemZmWTN6Q2dSMXhzUkNyWEMyMTl6VHhrc2dBb HZPMHVQcUVjOVhnNm5qRzhoa215RlhmZE1YOVBrOVYyRTNOSUtlWndZa 0U4ejQxQzJyUTJLdUlqdzFVM1ljV0JCTnZTN2lHT3hsM2E2b1h3dm5Ia zhEUGpaV1pteURZaVNkcUZQVVhZSUxadWJqVDh1bnlBSGlNQTcxT1NSb 2QtenV5X3BsbzBVOFc2eWE3T3pfSE80T29idyJ9LHsia3R5IjoiUlNBI iwidXNlIjoiZW5jIiwia2lkIjoiZW5jLWRiLWZ0bi0zMTgwNjc3NjEiL CJhbGciOiJSU0EtT0FFUCIsImUiOiJBUUFCIiwibiI6IjRRY0c1TkVHW UgwS3R4Tnd0UUQ5VnpMSU9oanJxekg0WTlrMjVoVkJjNnBBQVRMTE1oU 2VJcnlKQmxteTdQTDZLNmZKOWFtUUVfR2pjelhVX1BFVXRxTlFzaWt2M Uo5WGsyOG9yZnNpYXJPY2tQeGN3emVMekxGcHpxcTh0ZFI0OVFiajZ3X zEzSTlyVU5saTlIeE9HZ1NqRHl2MEhFeDRpemZmWTN6Q2dSMXhzUkNyW EMyMTl6VHhrc2dBbHZPMHVQcUVjOVhnNm5qRzhoa215RlhmZE1YOVBrO VYyRTNOSUtlWndZa0U4ejQxQzJyUTJLdUlqdzFVM1ljV0JCTnZTN2lHT 3hsM2E2b1h3dm5IazhEUGpaV1pteURZaVNkcUZQVVhZSUxadWJqVDh1b

nlBSGlNQTcxT1NSb2QtenV5X3BsbzBVOFc2eWE3T3pfSE80T29idyJ9X
X0sIm1ldGFkYXRhIjp7Im9wZW5pZF9wcm92aWRlciI6eyJpc3N1ZXIiO
iJodHRwczovL3N5c3QtdXNlcmFwaTIuZGFuc2tlYmFuay5jb20vZnRuL
WlkcCIsImF1dGhvcml6YXRpb25fZW5kcG9pbnQiOiJodHRwczovL3N5c
3QtdXNlcmFwaTIuZGFuc2tlYmFuay5jb20vc3lzdC9leHRlcm5hbC9md
G4vaWRwLW9pZGMvY29ubmVjdC9hdXRob3JpemUiLCJ0b2tlbl9lbmRwb
2ludCI6Imh0dHBzOi8vc3lzdC11c2VyYXBpMi5kYW5za2ViYW5rLmNvb
S9zeXN0L2V4dGVybmFsL2Z0bi9pZHAtb2lkYy9jb25uZWN0L3Rva2VuI
iwic2Vydmljz9kb2N1bWVudGF0aW9uIjoiaHR0cHM6Ly9kYW5za2ViY
W5rLmZpL3lyaXR5a3NpbGxlL2RpZ2l0YWFsaXNldC1wYWx2ZWx1dC9hc
2lvaW50aXBhbHZlbHV0L3R1bm5pc3R1c3BhbHZlbHUiLCJvcmdhbml6Y
XRpb25fbmFtZSI6IkRhbnNrZSBCYW5rIiwic2lnbmVkX2p3a3NfdXJpI
joiaHR0cHM6Ly9zeXN0LXVzZXJhcGkyLmRhbnNrZWJhbmsuY29tL3N5c
3QvZXh0ZXJuYWwvZnRuL2lkcC1vaWRjL3NpZ25lZC1qd2tzIiwic2Nvc
GVzX3N1cHBvcnRlZCI6WyJvcGVuaWQiLCJmdG5faGV0dSJdLCJyZXNwb
25zZV90eXBlc19zdXBwb3J0ZWQiOlsiY29kZSJdLCJncmFudF90eXBlc
19zdXBwb3J0ZWQiOlsiYXV0aG9yaXphdGlvbl9jb2RlIl0sImlkX3Rva
2VuX3NpZ25pbmdfYWxnX3ZhbHVlc19zdXBwb3J0ZWQiOlsiUlMyNTYiX
SwiaWRfdG9rZW5fZW5jcnlwdGlvbl9hbGdfdmFsdWVzX3N1cHBvcnRlZ
CI6WyJSU0EtT0FFUCJdLCJpZF90b2tlbl9lbmNyeXB0aW9uX2VuY192Y
Wx1ZXNfc3VwcG9ydGVkIjpbIkExMjhHQ00iXSwidG9rZW5fZW5kcG9pb
nRfYXV0aF9tZXRob2RzX3N1cHBvcnRlZCI6WyJwcml2YXRlX2tleV9qd
3QiXSwicmVxdWVzdF9hdXRoZW50aWNhdGlvbl9tZXRob2RzX3N1cHBvc
nRlZCI6WyJwcml2YXRlX2tleV9qd3QiXSwicmVxdWVzdF9hdXRoZW50a
WNhdGlvbl9zaWduaW5nX2FsZ192YWx1ZXNfc3VwcG9ydGVkIjpbIlJTM
jU2Il19fX0.xOvPaQpJJsDDYNNgqEr3pfR4hS5wAY_KKVtIwZFHElvsP
x43vD1dwlzTAl-A5Gln5VhDpDKWu3x3D2GtF-R__0HXJYch6Wn-
J1797dxbGD53XT1QKmxcLTSYz7HOk4rO54visi8-
GaxL2AThjM2Uv4hOg4mv4wayJ9CbeoK9ed5lxpKEJbu66A54eG5bj1zT
LlZHEfLh75gYOOIW_ynJvq6l1E3M6KHLzng71v6lntD8e7NBiXAtCIuT
0Avbj_lejwp-wPZh_7073j6TLwyNYtn4rhxywH-HjGleXfSNXuNu-P4-
6ydVNpNRmOKycIAePgsPIHtAnlkwW9Igt8oQCg

4.2.5 Response example (error)

Ex.

```
{
    "error": "server_error",
    "error_description": "Server Error. A technical problem has occurred. Please try again later. If the problem reoccurs, kindly contact the Service Provider with Trace ID information. TraceId: 815f739ad044ca9a477bffc1a63cbec3 ",
    "error_uri": "https://userapi2.danskebank.com/prod/external/ftn/idp-oidc/errorcodes"
}
```

5 GET /signed-jwks

5.1 Request details

5.1.1 Request endpoint URI

GET	<domain>/ signed-jwks

5.1.2 Request header

JSON	accept: application/json

5.1.3 Request body

N/A	Not Applicable

5.2 Response details

5.2.1 Response details

The response of this uri is signed JWKS which is a signed JWT having the entity's JWK Set as payload. The JWT is signed with a key that was included in the JWK set that the entity published in its (self-signed) Entity Statement.

https://openid.net/specs/openid-connect-federation-1_0.html#section-3.1

5.2.2 Response type

text/plain	Signed JWKS which is a signed JWT having the entity's JWK Set as payload.

5.2.3 Response codes

https://userapi2.danskebank.com/prod/external/ftn/idp-oidc/errorcodes

5.2.4 Response example (success)

Ex.	eyJhbGciOiJSUzI1NiIsImtpZCI6InNpZy1kYi1mdG4tMzE4MDY3NzYx IiwidHlwIjoiSldTIn0.eyJrZXlzIjpbeyJrdHkiOiJSU0EiLCJ1c2Ui OiJzaWciLCJraWQiOiJzaWctZGItZnRuLTMxODA2Nzc2MSIsImFsZyI6 IlJTMjU2IiwiZSI6IkFRQUIiLCJuIjoiNFFjRzVORUdZSDBLdHhOd3RR RDlWekxJT2hqcnF6SDRZOWsyNWhWQmM2cEFBVExMTWhTZUlyeUpCbG15 N1BMNks2Zko5YW1RRV9HamN6WFVfUEVVdHFOUXNpa3YxSjlYazI4b3Jm c2lhck9ja1B4Y3d6ZUx6TEZwenFxOHRkUjQ5UWJqNndfMTNJOXJVTmxp OUh4T0dnU2pEeXYwSEV4NGl6ZmZZM3pDZ1IxeHNSQ3JYQzIxOXpUeGtz Z0Fsdk8wdVBxRWM5WGc2bmpHOGhrbXlGWGZkTVg5UGs5VjJFM05JS2Va d1lrRTh6NDFDMnJRMkt1SWp3MVUzWWNXQkJOdlM3aUdPeGwzYTZvWHd2 bkhrOERQalpXWm15RFlpU2RxRlBVWFlJTFp1YmpUOHVueUFIaU1BNzFP U1JvZC16dXlfcGxvMFU4VzZ5YTdPel9ITzRPb2J3In0seyJrdHkiOiJS U0EiLCJ1c2UiOiJlbmMiLCJraWQiOiJlbmMtZGItZnRuLTMxODA2Nzc2 MSIsImFsZyI6IlJTQS1PQUVQIiwiZSI6IkFRQUIiLCJuIjoiNFFjRzVO RUdZSDBLdHhOd3RRRDlWekxJT2hqcnF6SDRZOWsyNWhWQmM2cEFBVExM TWhTZUlyeUpCbG15N1BMNks2Zko5YW1RRV9HamN6WFVfUEVVdHFOUXNp a3YxSjlYazI4b3Jmc2lhck9ja1B4Y3d6ZUx6TEZwenFxOHRkUjQ5UWJq NndfMTNJOXJVTmxpOUh4T0dnU2pEeXYwSEV4NGl6ZmZZM3pDZ1IxeHNS Q3JYQzIxOXpUeGtzZ0Fsdk8wdVBxRWM5WGc2bmpHOGhrbXlGWGZkTVg5 UGs5VjJFM05JS2Vad1lrRTh6NDFDMnJRMkt1SWp3MVUzWWNXQkJOdlM3 aUdPeGwzYTZvWHd2bkhrOERQalpXWm15RFlpU2RxRlBVWFlJTFp1YmpU OHVueUFIaU1BNzFPU1JvZC16dXlfcGxvMFU4VzZ5YTdPel9ITzRPb2J3 In1dLCJpc3MiOiJodHRwczovL3N5c3QtdXNlcmFwaTIuZGFuc2tlYmFu

ay5jb20vZnRuLWlkcCIsInN1YiI6Imh0dHBzOi8vc3lzdC11c2VyYXBp
Mi5kYW5za2ViYW5rLmNvbS9mdG4taWRwIiwiaWF0IjoxNjc5MDM0NDg5
LCJleHAiOjE2NzkwNDE2ODl9.kxC7AvfTBqIwWrTMqtXrDIh7B5ugMkY
upaezUSc7UGLKQv6mCrvuDWNn3Osnx4Nynj846171-
FG6xFCnKGaaLXpYI0ulG8wg4yEeWgmB2TZDdwtprrQpMFjnoibToa6Yz
90Sk611znbV3loBAlo9PJJW4_35wxFMRJ83zFI-M_o6-
41YaMgqGNyI20lsdax7eA9T4n1Oxikpqzhu2wBxcg4j2rlCwo85ZMmce
XFmS6qANE9lCsz5DZk2IIjezr4LLyBdYArdC3hKDjoRL-zn-
nyldXDJ2OS855S-
vilGvg1THLizpGX3Hi4qqlXjJPXPwqcHabnjiZtgp_1AhSzViQ

5.2.5 Response example (error)

Ex.

{
"error": "server_error",
"error_description": "Server Error. A technical problem has occurred. Please try again later. If the problem reoccurs, kindly contact the Service Provider with Trace ID information. TraceId: 815f739ad044ca9a477bffc1a63cbec3 ",
"error_uri": "https://userapi2.danskebank.com/prod/external/ftn/idp-oidc/errorcodes"
}

6 GET /connect/authorize

6.1 Request details

6.1.1 Request endpoint URI

GET	<domain>/connect/authorize

6.1.2 Request header

JSON	accept: application/json

6.1.3 Request body

N/A	Not Applicable

6.1.4 Request URI query parameters

Parameter name	Required / Optional, Description and Accepted / Default values	Examples
client_id	**REQUIRED.** MUST be a **string**.	**Example –**

	Identifier of the party initiating the authentication (Service Provider / Broker), assigned to the Service Provider / Broker by the Identity Provider. **Accepted values –** MUST be the same as the Client ID received during client registration.	client_id=0234a472-b4ea-4e62-9ec0-ea1ac96789ab
response_type	**REQUIRED.** MUST be a **string**. **Accepted values –** MUST always be "**code**".	**Example –** response_type=code
scope	**REQUIRED.** MUST be a **string**. MUST be a space-separated list of scopes. Refers to the scopes to be returned. **Accepted value –** MUST have **openid** as a scope. MAY have **ftn_hetu** as scope if the client needs to get user data like first names, last name, date of birth, and person identifier. This is the only scope supported by	**Example –** scope=openid ftn_hetu

	Danske Bank which provides the mandatory natural person attributes. Danske Bank does not support any Legal Person attributes as of now.	
request	**REQUIRED** **MUST** be signed JWT. The request Authorization Request parameter enables OpenID Connect requests to be passed in a single, self-contained parameter and it must be signed.	**Example** – request=eyJhbGciOiJQ.eyJhdWQiOiJodHRwczovL3NlifQ.

6.1.5 Request example

Ex.	<domain>/connect/authorize? client_id=<insert_value_here>& response_type=<insert_value_here>& scope=<insert_value_here>& request=<insert_value_here>

6.1.6 Request object JWT header parameters

Parameter name	Required / Optional and Description	Examples
alg	**REQUIRED.** MUST be a **string**. The value MUST be "**RS256**".	**Example –** "alg": "RS256"
	REQUIRED. MUST be a **string**.	**Example –**

	The value MUST be the same key ID value that is used to sign the JWT. This MUST be same as the one shared at the time of registration.	"kid": "DSF557GHJ8HUK"
typ	**OPTIONAL.** MUST be a **string** if passed. The value MUST be "JWT" if passed.	**Example –** "typ": "JWT"

6.1.7 Request object JWT payload parameters

When the request parameter is used, the OpenID Connect request parameter values contained in the JWT supersede those passed using the OAuth 2.0 request syntax as per section 6.1 of OIDC Core 1.0 section 6.1.

iss	**REQUIRED.** **MUST be a** string. **Represents** issuer. Accepted values – **MUST be the client ID provided at the time of registration.**	**Example** – **"iss": "**0234a472-b4ea-4e62-9ec0-ea1ac96789ab**"**
aud	**REQUIRED.** MUST be a **string**. Represents **audience**. **Accepted values –** MUST be the URL of OP's (OpenID provider) Issuer Identifier URL. **Production** "aud": "https://userapi2.danskebank.com/ftn-idp" **Test Production**	**Example –** "aud": "https://userapi2.danskebank.com/ftn-idp"

	"aud": "https://sandbox-userapi2.danskebank.com/ftn-idp"	
exp	**REQUIRED.** MUST be a **number**. Represents **expiry time**. The time on or after which the JWT token will not be accepted for processing. The processing of this parameter requires that the current date/time MUST be before the expiration date/time listed in the value. Its value is a JSON number representing the number of seconds from 1970-01-01T00:00:00Z as measured in UTC until the date/time. **Accepted values –** MUST be 10 minutes or less into the future from the token issued timestamp.	**Example –** "exp": "1550032168"
prompt	**REQUIRED.** MUST be a **string**. **Accepted values –** the prompt authentication request parameter MUST be set to value "login"	**Example –** "prompt": "login"
scope	**REQUIRED.** MUST be a **string**. MUST be a space-separated list of scopes.	**Example –** "scope": "openid ftn_hetu"

	Refers to the scopes to be returned. **Accepted value –** MUST have **openid** as a scope. MAY have **ftn_hetu** as scope if the client needs to get user data like first names, last name, date of birth, and person identifier. This is the only scope supported by Danske Bank which provides the mandatory natural person attributes. Danske Bank does not support any Legal Person attributes as of now.	
nonce	**REQUIRED.** MUST be a **string**. **Accepted values –** MUST contain at least 128 bits of entropy (for example at least 22 random characters A-Z, a-z, 0-9).	**Example –** "nonce": "d71a4edca5504b93a585f03dfb14267a"
state	**REQUIRED.** MUST be a **string**. **Accepted values –** MUST contain at least 128 bits of entropy (for example at least 22 random characters A-Z, a-z, 0-9).	**Example –** "state": "9034a5d8-12b9-58a8-b123-98b76f54a220"
acr_values	**REQUIRED.** MUST be a **string**.	**Example –** "acr_values": "http://ftn.ficora.fi/2017/loa2"

	MUST be a space-separated list of requested FTN authentication context class reference values. **Accepted values –** **Production** http://ftn.ficora.fi/2017/loa2 **Test Production** http://ftn.ficora.fi/2017/loatest2	
response_type	**REQUIRED.** MUST be a **string**. **Accepted values –** MUST always be "**code**" if this parameter is passed.	**Example –** "response_type": "code"
redirect_uri	**REQUIRED.** MUST be a **string**. URI for returning the authentication response to. **Accepted values –** MUST be the same as what is configured at the Identity Provider for the corresponding Client ID.	**Example –** "redirect_uri": "https://dummy-client-redirect-uri.com"
ui_locales	**OPTIONAL.** MUST be a **string**. End user language preference tags (BCP 47). **Accepted values –** ▪ en	**Example –** "ui_locales": "en"

	▪ fi ▪ sv **Default value –** fi	
prompt	**REQUIRED for Chained** **OPTIONAL for Normal** MUST be a **string**. **Accepted value –** MUST always be "**login**" if this parameter is passed.	**Example –** "prompt": "login"
response_mode	**OPTIONAL.** MUST be a **string**. **Accepted values –** MUST always be "**form_post**" if this parameter is passed.	**Example –** "response_mode": "form_post"
ftn_spname	**REQUIRED** MUST be a **string**. **Accepted values –** Name to be displayed in authentication flow	**Example –** "ftn_spname":"Danske Bank Test Client"

Important Note: request and request_uri parameters MUST NOT be included in Request Objects.

6.2 Response details

6.2.1 Response type

URI	Redirect

6.2.2 Response codes

https://userapi2.danskebank.com/prod/external/ftn/idp-oidc/errorcodes

6.2.3 Response parameters

Parameter name	Description	Examples
code	The authorization code of OIDC protocol. This code is valid for **60** seconds from the time it is received by the client.	**Example –** code=SAD35F67HD8H
state	The same value that is provided by the Service Provider / Broker in the authorization request.	**Example –** state=9034a5d8-12b9-58a8-b123-98b76f54a220
error	Returns this parameter only in case of an error. Error messages provided – ▪ invalid_request ▪ invalid_request_object ▪ unauthorized_client ▪ invalid_client ▪ invalid_scope ▪ unsupported_response_type	**Example –** error=invalid_scope

	▪ server_error	
error_description	Returns this parameter only in case of an error. This contains an error id (Trace ID) which can be forwarded to Danske Bank to analyze errors, if required.	**Example –** error_description= Invalid_scope. {Trace ID:- b5361c4b-e84d-4382-a0ab-d776165a1998}.
error_uri	Returns this parameter only in case of an error. Gives the link to the error codes page which will give more information on the error. Value is always, '<domain>/errorcodes '.	**Example –** error_uri= <domain>/errorcodes

6.2.4 Response example (success)

Ex.	https://dummy-client-redirect-uri.com? code=SAD35F67HD8H& state=9034a5d8-12b9-58a8-b123-98b76f54a220

6.2.5 Response example (error)

Ex.	https://dummy-client-redirect-uri.com? error=invalid_scope& state=9034a5d8-12b9-58a8-b123-98b76f54a220& error_description=invalid_scope. {Trace ID:-b5361c4b-e848-4382-a0ab-d776165a1998}.& error_uri=https://userapi2.danskebank.com/prod/external/ftn/idp-oidc/errorcodes

7 POST /connect/token

7.1 Request details

7.1.1 Request endpoint URI

POST	<domain>/connect/token

7.1.2 Request header

URL ENCODED	accept: application/x-www-form-urlencoded

7.1.3 Request body

Ex.	{
	
	"client_assertion":"jwt_value_here"
	"client_assertion_type":"urn:ietf:params:oauth:client-assertion-type:jwt_bearer"
	"client_id":"my_service_client_id"
	"code":"code_value_here"
	"grant_type":"authorization_code"
	"redirect_uri"https://myclient_redirect_url.com
	}

7.1.4 Request body parameters

Parameter name	Required / Optional and Description	Examples
client_id	**REQUIRED.** MUST be a **string**. Identifier of the party initiating the authentication (Service Provider / Broker), assigned to the Service Provider / Broker by the Identity Provider. **Accepted values –** MUST be the same as the Client ID received during client registration.	**Example –** "client_id": "0234a472-b4ea-4e62-9ec0-ea1ac96789ab"
code	**REQUIRED.** MUST be a **string**. **Accepted values –** MUST be as received after completion of the authorize endpoint from Identity Provider.	**Example –** "code": "JH2GF3RXH5CT6VKIB"
grant_type	**REQUIRED.** MUST be a **string**. **Accepted values –** MUST always be "**authorization_code**".	**Example –** "grant_type": "authorization_code"
redirect_uri	**REQUIRED.**	**Example –**

	MUST be a **string**. **Accepted values –** MUST be the same as the one used in authorization end-point.	"redirect_uri": "https://myclient_redirect_url.com"
client_assertion_type	**REQUIRED.** MUST be a **string**. **Accepted values –** MUST always be "**urn:ietf:params:oauth:client-assertion-type:jwt-bearer**".	**Example –** "client_assertion_type": "urn:ietf:params:oauth:client-assertion-type:jwt-bearer"
client_assertion	**REQUIRED.** MUST be a signed **JWT**. The required values in the JWT payload are listed in section **7.1.5**. **Accepted values –** MUST include the claims iss, sub, aud, jti, and exp.	**Example –** "client_assertion": "eyJhbGci0.V7g8UwCv3svCENau_N4.w9CA4gN152dTdQnp"

7.1.5 Request client assertion JWT header parameters

Parameter name	Required / Optional and Description	Examples
alg	**REQUIRED.** MUST be a **string**. The value MUST be "**RS256**".	**Example –** "alg": "RS256"
kid	**REQUIRED.** MUST be a **string**.	**Example –**

	The value MUST be the same key ID value that is used to sign the JWT. This MUST be same as the one shared at the time of registration.	"kid": "DSF557GHJ8HUK"
typ	**OPTIONAL.** MUST be a **string** if passed. The value MUST be "JWT" if passed.	**Example –** "typ": "JWT"

7.1.6 Request client assertion JWT payload parameters

Parameter name	Required / Optional and Description	Examples
iss	**REQUIRED.** MUST be a **string**. Represents **issuer**. **Accepted values –** MUST be the client ID provided at the time of registration.	**Example –** "iss": " 0234a472-b4ea-4e62-9ec0-ea1ac96789ab"
sub	**REQUIRED.** Represents **Subject Identifier** MUST be locally unique. **Accepted Values -** Value is Unique ID for each Identification request.	**Example –** "sub": "f9aeb649517b9d4fe46c4ea55d751359033512bbfa8c516c681aa0434fb8ffbe"
aud	**REQUIRED.** MUST be a **string**.	**Example –**

	Represents **audience**. **Accepted values –** MUST be the URL of Danske Bank Identity Provider's Token Endpoint (as obtained from "token_endpoint" parameter in Section 4.2.3).	"aud":"<domain>/connect/token"
exp	**REQUIRED.** MUST be a **number**. Represents **expiry time**. The time on or after which the JWT token will not be accepted for processing. The processing of this parameter requires that the current date/time MUST be before the expiration date/time listed in the value. Its value is a JSON number representing the number of seconds from 1970-01-01T00:00:00Z as measured in UTC until the date/time. **Accepted values –** MUST be 10 minutes or less into the future from the token issued timestamp.	**Example –** "exp": "1550032168"
jti	**REQUIRED.** MUST be a **string**. Any random value to be used uniquely. **Accepted values –**	**Example –** "jti": "abcdefghijlkmno"

	MUST NOT be repeated by a specific Service Provider/ Broker (with a unique Client ID) in the last 10 minutes.	

7.1.7 Request example

Ex.	**POST** <domain>/connect/token

7.2 Response details

7.2.1 Response type

JSON	JavaScript Object Notation (**JSON**) type

7.2.2 Response codes

https://userapi2.danskebank.com/prod/external/ftn/idp-oidc/errorcodes

7.2.3 Response parameters

Parameter name	Description	Examples
access_token	This is an encrypted string. 'access_token' is not necessarily used in the typical FTN use case, but it is required by OAuth 2.0.	**Example –** "access_token": "ASDJAKSDHJADHAHSDKJAJHKSAJHDKADS"

token_type	Value is always '**Bearer**'.	**Example –** "token_type": "Bearer"
expires_in	The number of seconds the access token (access_token) is valid for.	**Example –** "expires_in": 600
id_token	This is a JWT signed using Danske Bank Identity Provider's private key and then encrypted using Service Provider's / Broker's public key. This contains information about the end user that authenticated. The required values in the JWT header and payload are listed in sections. **7.2.4 Response ID Token header parameters** and **7.2.5 Response ID Token payload parameters** respectively.	**Example –** "id_token": " eyJhbGci0.V7g8UwCv 3svCENau_N4.w9CA 4gN152dTdQnp.fdsf78 786fdf"
error	Returns this parameter only in case of an error. Error messages provided – ▪ invalid_request ▪ unauthorized_client ▪ invalid_client ▪ invalid_scope ▪ invalid_grant ▪ unsupported_grant_type ▪ server_error	**Example –** "error": "invalid_grant"

error_description	Returns this parameter only in case of an error. This contains an error id (Trace ID) which can be forwarded to Danske Bank to analyze errors, if required.	"error_description": "invalid_grant. {Trace ID:- b5361c4b-e84d-4382-a0ab-d776165a1998}."
error_uri	Returns this parameter only in case of an error. Gives the link to the error codes page which will give more information on the error. Value is always 'https://userapi2.danskebank.com/prod/external/ftn/idp-oidc/errorcodes '.	"error_uri": "https://userapi2.danskebank.com/prod/external/ftn/idp-oidc/errorcodes"

7.2.4 Encrypted id_token response header parameters

Parameter name	Description	Examples
alg	Value is always "**RSA-OAEP**".	**Example –** "alg": "RSA-OAEP"
enc	Value is always "**A128GCM**".	**Example –** "alg": "A128GCM"
kid	This will be the Service Provider's kid of type 'enc' The kid will be of type 'sig' if 'enc' is not present in the	**Example –** "kid": "DSF557GHJ8HUK"

	JWKS URL of the Service Provider.	
typ	Value is always "**JWT**".	**Example –** "typ": "JWT"

The payload of the id_token MUST be decrypted to get the decrypted/signed id_token for the required claims as mentioned below.

7.2.5 Decrypted id_token response header parameters

Parameter name	Description	Examples
alg	Value is always "**RS256**".	**Example –** "alg": "RS256"
kid	Will be the key ID value present in the Danske Bank's JWKs URL with typ as 'sig'.	**Example –** "kid": "DSF557GHJ8HUK"
typ	Value is always "**JWT**".	**Example –** "typ": "JWT"

7.2.6 Decrypted id_token response payload parameters

Parameter name	Description	Examples
iss	Represents **issuer**. **Production** https://userapi2.danskebank.com/ftn-idp	**Example –** "iss": "https://userapi2.danskebank.com/ftn-idp"

	Test Production "https://sandbox-userapi2.danskebank.com/ftn-idp"	
sub	Represents **Subject Identifier** MUST be locally unique. **Accepted Values -** Value is Unique ID for each Identification request.	**Example –** "sub": "f9aeb649517b9d4fe46c4ea55d751359033512bbfa8c516c681aa0434fb8ffbe"
aud	Represents **audience**. Value is client ID provided at the time of registration.	**Example –** "aud": "0234a472-b4ea-4e62-9ec0-ea1ac96789ab"
exp	Represents **expiry time**. The time on or after which the JWT token MUST NOT be accepted for processing. The processing of this parameter requires that the current date/time MUST be before the expiration date/time listed in the value. All FTN participants SHOULD be configured with a reliable UTC time source. Its value is a JSON number representing the number of seconds from 1970-01-01T00:00:00Z as measured in UTC until the date/time.	**Example –** "exp": "1550032168"

iat	Time at which the JWT was issued, number of seconds since the beginning of 1970 UTC.	**Example –** "iat": "1550032162"
auth_time	Time when the end-user authentication occurred, number of seconds since the beginning of 1970 UTC.	**Example –** "auth_time": "1550032155"
nonce	Case sensitive string from the authentication request to associate an end-user with an ID token and to mitigate replay attacks. The FTN Service Provider / Broker MUST verify that the nonce claim value is equal to the value of the nonce parameter sent in the authentication request.	**Example –** "nonce": "d71a4edca5504b93a585f03dfb14267a"
acr	The Authentication Context Class Reference string for this authentication transaction. This will be the same value as received during authorization endpoint request.	**Example –** "acr": "http://ftn.ficora.fi/2017/loa2"

Apart from these, the ID token payload will also contain the user claims as per the scopes requested during the authorization endpoint call.

7.2.7 Response example (success)

Ex.

{

"id_token":"eyJhbGci0.V7g8UwCv3svCENau_N4.w9CA4gN152dTdQnp.fdsf78786fdf",
"access_token":"ASDJAKSDHJADHJHSDKJAJHKSAJHDKADS",
"token_type":"Bearer",
"expires_in":600,
}

7.2.8 Response example (error)

Ex.

{

"error"="invalid_grant",
"error_description"="invalid_grant. {Trace ID:-b5361c4b-e848-4382-a0ab-d776165a1998}",
"error_uri"="https://userapi2.danskebank.com/prod/external/ftn/idp-oidc/errorcodes"
}

.