

Finnish Trust Network

Danske Bank's Broker
API Document

Table of Content

1	Introduction	5
2	Service Description	6
2.1	Chained authentication	6
2.2	Domain Name	6
2.3	Metadata	7
2.4	Key Exchange	7
2.5	Algorithms and Key sizes	7
2.6	Level of Assurance	8
2.7	Single Sign-On (SSO)	8
3	List of endpoints	9
4	GET /entity-statement	10
4.1	Request details	10
4.1.1	Request endpoint URI	10
4.1.2	Request header	10
4.1.3	Request body	10
4.2	Response details	11
4.2.1	Response details	11
4.2.2	Response type	11
4.2.3	Response codes	11
4.2.4	Response example (success)	11
4.2.5	Response example (error)	13
5	GET /signed-jwks	14
5.1	Request details	14
5.1.1	Request endpoint URI	14
5.1.2	Request header	14
5.1.3	Request body	14
5.2	Response details	15
5.2.1	Response details	15
5.2.2	Response type	15
5.2.3	Response codes	15
5.2.4	Response example (success)	15
5.2.5	Response example (error)	16
6	GET /connect/authorize	17
6.1	Request details	17
6.1.1	Request endpoint URI	17
6.1.2	Request header	17
6.1.3	Request body	17
6.1.4	Request URI query parameters	17
6.1.5	Request example	19
6.1.6	Request object JWT header parameters	19
6.1.7	Request object JWT payload parameters	20
6.2	Response details	26
6.2.1	Response type	26
6.2.2	Response codes	26
6.2.3	Response parameters	26
6.2.4	Response example (success)	27
6.2.5	Response example (error)	27
7	POST /connect/token	29
7.1	Request details	29
7.1.1	Request endpoint URI	29
7.1.2	Request header	29
7.1.3	Request body	29
7.1.4	Request body parameters	30
7.1.5	Request client assertion JWT header parameters	31
7.1.6	Request client assertion JWT payload parameters	32
7.1.7	Request example	34
7.2	Response details	34

7.2.1	Response type	34
7.2.2	Response codes	34
7.2.3	Response parameters	34
7.2.4	Encrypted id_token response header parameters	36
7.2.5	Decrypted id_token response header parameters	37
7.2.6	Decrypted id_token response payload parameters	37
7.2.7	Response example (success)	40
7.2.8	Response example (error)	40

Change log

Version	Date	Change Summary
1.0	29-03-2019	Initial version
1.1	05-07-2019	Changes made in section 8.1.6 and 8.2.5 (sub)
1.2	08-08-2019	Changes made in section 2.1. and 8.1.4 (client_id) and 8.1.6 (sub)
1.3	20-09-2019	New section 8.2.4
1.4	18-05-2020	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.
1.5	10-06-2020	Improved document introduction in section 1 and 2
1.6	15-01-2021	<ul style="list-style-type: none"> - Removed /register endpoint - Change in section 2.1 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) and 6.1.5 (request) - Updated section 6.2.2(added invalid request object) and 6.2.3(added invalid_request_object)

1.7	03-03-2023	<ul style="list-style-type: none">- 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.
1.8	08-05-2023	<ul style="list-style-type: none">- 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 Broker Services that Danske Bank is offering following the above recommendations by TRAFICOM.

2 Service Description

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

The Danske Bank's Broker Service can be integrated with two roles namely the **Identity Providers** and **Service Providers**. Information exchange **MUST** take place with both the roles 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 Identity Providers integrated with Danske Bank's Broker service. Service providers can communicate with Danske Bank's broker 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 Chained authentication

Danske Bank Broker supports Chained Authentication. The Service Provider must register with request for chained authentication with a new Client Id and the respective Client Id must be sent for Danske Bank Broker to invoke chained authentication. Signed JWT request is mandatory for chained authentication during the Authorize request along with the use of the Client ID registered for chained authentication.

2.2 Domain Name

Danske Bank Broker 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/broker-oidc>

Test Production -

<https://sandbox-userapi2.danskebank.com/sandbox/external/ftn/broker-oidc>

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

2.3 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 to fetch the keyset of the Broker.

2.4 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.

2.5 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 Broker implements RSASSA-PKCS1-v1_5 using SHA-256 algorithm for signing of messages.

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

Danske Bank Broker 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.

2.6 Level of Assurance

Danske Bank Broker 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>

2.7 Single Sign-On (SSO)

Danske Bank's Broker currently doesn't support implement 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 Broker service are listed below -

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

1VuUSJ9XX0sIm1ldGFkYXRhIjpb7Im9wZW5pZF9wcm92aWRlciI6eyJpc
3N1ZXIiOiJodHRwczovL3N5c3QtdXNlcmFwaTIuZGFuc2t1YmFuay5jb
20vZnRuLWJyb2t1ciIsImFlldGhvcml6YXRpb25fZW5kcG9pbnQiOiJod
HRwczovL3N5c3QtdXNlcmFwaTIuZGFuc2t1YmFuay5jb20vc3lzdC9le
HRlcm5hbC9mdG4vYnJva2VyLW9pZGMvY29ubmVjdC9hdXRob3JpemUiL
CJ0b2t1bl9lbnRwb2ludCI6Imh0dHBzOi8vc3lzdC11c2VyYXBmMi5kY
W5za2ViYW5rLmNvbS9zeXN0L2V4dGVybmFsL2Z0bi9icm9rZXItb2lkY
y9jb25uZWN0L3Rva2VuIiwic2Vydm1jZV9kb2N1bWVudGF0aW9uIjoia
HR0cHM6Ly9kYW5za2ViYW5rLmZpL3l1yaXR5a3NpbGx1L2Rpb210YWFsa
XNldC1wYXZlZW5ldC9hc2lvaW50aXBhbHZlbHV0L3R1bm5pc3Rlc3Bhb
HZlbHUIlCJvcmdhbml6YXRpb25fYmFtZSI6IkhbnNrZSBCYW5rIiwic2
l1bnmVkX2p3a3NfdXJpIjoiaHR0cHM6Ly9zeXN0LXVzZXJhcGkyLmRhb
nNrZWJhbmsuY29tL3N5c3QvZXh0ZXJ1YVwvZnRuL2Jyb2t1ci1vaWRjL
3NpZ25lZC1qd2t2Iiwic2NvcGVzX3N1cHBvcnRlZCI6WyJvcGVuaWQiL
CJmdG5faGV0dSjdLCJyZXNwb25zZV90eXB1c19zdXBwb3J0ZWQiOlsiY
29kZSjdLCJncmFudF90eXB1c19zdXBwb3J0ZWQiOlsiYXV0aG9yaXphd
Glvlbl9jb2RlIi10sIm1kX3Rva2VuX3NpZ25pbmdfYWxnX3ZhbHVlc19zd
XBwb3J0ZWQiOlsiU1MyNTYiXSwiaWRfdG9rZW5fZW5jcmlwdGlvlbl9hb
GdfdmFsdWVzX3N1cHBvcnRlZCI6WyJSU0EtT0FFUCJdLCJpZF90b2t1b
l9lbnNyeXB0aW9uX2VuY192YWx1ZXNfc3VwcG9ydGVkIjpbIkeXmJhHQ
00iXSwidG9rZW5fZW5kcG9pbnRfYXV0aF9tZXRob2RzX3N1cHBvcnRlZ
CI6WyJwcm12YXRlX2tleV9qd3QiXSwicmVxdWVzdF9hdXR0ZW50aWNhd
Glvlbl9tZXRob2RzX3N1cHBvcnRlZCI6WyJwcm12YXRlX2tleV9qd3QiX
SwicmVxdWVzdF9hdXR0ZW50aWNhdGlvlbl9zaWduaW5nX2FsZl92YWx1Z
XNfc3VwcG9ydGVkIjpbI1JTMjU2I1l19LCJvcGVuaWRfcmVseWluZl9wY
XJ0eSI6eyJyZWVudF90eXB1c19zdXBwb3J0ZWQiOlsiYXV0aG9yaXphd
XBmMi5kYW5za2ViYW5rLmNvbS9zeXN0L2V4dGVybmFsL2Z0bi9icm9rZ
XIitb2lkYy9jb25uZWN0L3NpZ24taW4iLCJodHRwczovL3N5c3QtdXNlcm
FwaTIuZGFuc2t1YmFuay5jb20vc3lzdC9leHRlcm5hbC9mdG4vYnJva
2VyLW9pZGMvY29ubmVjdC9zaWduaW4tb2lkYyJdLCJhcHBsaWNhdGlvb
l90eXB1IjoiaHR0cHM6Ly9kYW5za2ViYW5rLmZpL3l1yaXR5a3NpbGx1L2
Rpb210YWFsaXNldC1wYXZlZW5ldC9hc2lvaW50aXBhbHZlbHV0L3R1bm5pc
3Rlc3BhbHZlbHUIlCJvcmdhbml6YXRpb25fYmFtZSI6IkhbnNrZSBCYW5rI
iwic2l1bnmVkX2p3a3NfdXJpIjoiaHR0cHM6Ly9zeXN0LXVzZXJhcGkyLmR
hbNnrZWJhbmsuY29tL3N5c3QvZXh0ZXJ1YVwvZnRuL2Jyb2t1ci1vaWRjL3
NpZ25lZC1qd2t2In19fQ.BpStrEdQcmBfmB
DTDXnckPLDt6ofQU2XF71a9JDAAtL56aEs3_8paG8aYn1b8CRmJLi-
TWbSOF5VUV_1089LLxBvnpDt2xQzDSgj_N5L5Kj04yih9BxbPmwEkQf
JnovA_h1wlY77AlhRt2lJ26oOvKa8T-
5pqimi1Klqy_RiMDWJ6uZWLK1jQcHq5CBkwcWrusAe_114n6Pybz5LCM
IARimyT4qef_zVWP4nA0b05rAB0kjQd3Kn1W-
tkXZNYi7QWqb5ZBB6WbHXTIhPd7vKlHJweGqTg7T-
FQjziuHv38j2KFaMMV06P3J_AU3u-cAhQl7ZQTsET02k-CV1Yr9aYw

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/broker-
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/broker-oidc/errorcodes>

5.2.4 Response example (success)

Ex.

```
eyJhbGciOiJSUzI1NiIsImtpZCI6InNpZy1kYi1mdG4tNEQyODVGMzVC
IiwidHlwIjoiSldlIn0.eyJrZXlziIjpbeyJrdHkiOiJSU0EiLCJlc2Ui
OiJzaWciLCJraWQiOiJzaWctZGItZnRuLTREMjg1RjM1QiIsImFsZyI6
IlJTMjU2IiwiaXNjaWkiOiJFRQUIiLCJuaWoiOiJFRQUIiLCJuaWoi
dmFWUURING52bHpiaU5PSEXjTWExTC1zWkE2a1RoQTZ1YTZlRENMNk
JUcVNNSTdNTURiel9lZnprYmNOVkVqSFg3czFnRnhQTFB6WHJuUU91
UWx5TWVhcW1hU21DZl82Y2RobWh5cmp2ejJkOF9JTDNBUm1US3Jvc0
Y5b1VlM0JmMklicW5iR0xZQm1STTRrQkxucGNfRndEWURkNUswdENub
E1PTFV2QTFaeG9Wb2VxTmptIVXUxb1RxxQ0IybW5LdVVoRFdOc0F0UDU
5WmttVEdaS3NRUnU3NE5CVUE1NjZ1SUFWYmhlVWhCYltpqaHNGVWV
TVGZMV21uZVRQmJLWXFwYThTekJRLWlEeXJZNndSbk9FNGNBV29FN
FhHNlN0YU5JSHVEYzlpMVRtZFFweUpSbGc4NERNeFdrY1FYZlFXWUd
OLUlvSUE1YUxNN3R0VG1SVW5RIn0seyJrdHkiOiJSU0EiLCJlc2UiOi
JlbnMiLCJraWQiOiJlbnMtZGItZnRuLTREMjg1RjM1QiIsImFsZyI6
IlJTMjU2IiwiaXNjaWkiOiJFRQUIiLCJuaWoiOiJFRQUIiLCJuaWoi
dmFWUURING52bHpiaU5PSEXjTWExTC1zWkE2a1RoQTZ1YTZlRENMNk
JUcVNNSTdNTURiel9lZnprYmNOVkVqSFg3czFnRnhQTFB6WHJuUU91
UWx5TWVhcW1hU21DZl82Y2RobWh5cmp2ejJkOF9JTDNBUm1US3Jvc0
Y5b1VlM0JmMklicW5iR0xZQm1STTRrQkxucGNfRndEWURkNUswdENub
E1PTFV2QTFaeG9Wb2VxTmptIVXUxb1RxxQ0IybW5LdVVoRFdOc0F0UDU
5WmttVEdaS3NRUnU3NE5CVUE1NjZ1SUFWYmhlVWhCYltpqaHNGVWV
TVGZMV21uZVRQmJLWXFwYThTekJRLWlEeXJZNndSbk9FNGNBV29FN
FhHNlN0YU5JSHVEYzlpMVRtZFFweUpSbGc4NERNeFdrY1FYZlFXWUd
OLUlvSUE1YUxNN3R0VG1SVW5RInldLCJpc3MiOiJodHRwczovL3N5c3
QtXN1cmFwaTIuZGFuc2t1YmFu
```

```
ay5jb20vZnRuLWJyb2t1ciIsInN1YiI6Imh0dHBzOi8vc3lzdC1lc2Vy
YXBpMi5kYW5za2ViYW5rLmNvbS9mdG4tYnJva2VyIiwiaWF0IjoxNjc5
MDMzOTY1LCJleHAiOjE2NzkwNDExNjV9.01N58xMvDXYkg6RLOCAKo_N
BsUA76rA4Aj2Hz5j42OFwa5yZyw0TAtBgmLFSDwTRhM8IaBq_quf-
kEMALUfd71k7zkDw1oRACwvvJ8yveXnoG2bmPxPsOUtGvFF8Jzhjirs
Pyz8-
W0mqPeZhCEzcIn4qz16Nccm2X9g8EFzPQcNbxWzBxEEkxRJ5Q_BJcFi
c7VR4GtHNGbMaY75oKDTD5kjLSq-
9sqI9s8vTb332kb5tWukxPfU6zaBsQRZvezkV-
D8dGkCmlUJi1puPl_4ICN62huV1lGg4tHPX7whovV8N8oZLEVNszjIbN
9Q5TsNWhmM48NjopXbOm54UsiJw
```

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/broker-
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 -

	<p>Identifier of the party initiating the authentication (Service Provider / Broker), assigned to the Service Provider / Broker by the Broker.</p> <p>Accepted values - MUST be the same as the Client ID received during client registration.</p>	<p>client_id=0234a472-b4ea-4e62-9ec0- ea1ac96789ab</p>
response_type	<p>REQUIRED. MUST be a string.</p> <p>Accepted values - MUST always be "code".</p>	<p>Example - response_type=code</p>
scope	<p>REQUIRED. MUST be a string. MUST be a space-separated list of scopes. Refers to the scopes to be returned.</p> <p>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</p>	<p>Example - scope=openid ftn_hetu</p>

	<p>the mandatory natural person attributes.</p> <p>Danske Bank does not support any Legal Person attributes as of now.</p>	
request	<p>REQUIRED</p> <p>MUST be signed JWT.</p> <p>The request Authorization Request parameter enables OpenID Connect requests to be passed in a single, self-contained parameter and it must be signed.</p>	<p>Example -</p> <pre>request=eyJhbGciOiJSUzI1NiIsImtpZCI6ImZFMEU5NzRBNTciLCJ0eXAiOiJqd3QifQ.eyJhdWQiOiJodHRwczovL3N5c3QtdXNlcmFwaTluZGFuc2se6a03xnLZik4JNCVfyc75zmf7YAw</pre>

6.1.5 Request example

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

6.1.6 Request object JWT header parameters

Parameter name	Required / Optional and Description	Examples
alg	<p>REQUIRED.</p> <p>MUST be a string.</p> <p>The value MUST be "RS256".</p>	<p>Example -</p> <p>"alg": "RS256"</p>
kid	<p>REQUIRED.</p> <p>MUST be a string.</p>	<p>Example -</p>

	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-broker"	Example - "aud": "https://userapi2.danskebank.com/ftn-broker"

	<p>Test Production</p> <p>"aud": "https://sandbox-userapi2.danskebank.com/ftn-broker"</p>	
exp	<p>REQUIRED.</p> <p>MUST be a number.</p> <p>Represents expiry time.</p> <p>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.</p> <p>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.</p> <p>Accepted values -</p> <p>MUST be 10 minutes or less into the future from the token issued timestamp.</p>	<p>Example -</p> <p>"exp": "1550032168"</p>
scope	<p>REQUIRED.</p> <p>MUST be a string.</p> <p>MUST be a space-separated list of scopes.</p> <p>Refers to the scopes to be returned.</p> <p>Accepted value -</p> <p>MUST have openid as a scope.</p>	<p>Example -</p> <p>"scope": "openid ftn_hetu"</p>

	<p>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.</p> <p>This is the only scope supported by Danske Bank which provides the mandatory natural person attributes.</p> <p>Danske Bank does not support any Legal Person attributes as of now.</p>	
nonce	<p>REQUIRED. MUST be a string.</p> <p>Accepted values - MUST contain at least 128 bits of entropy (for example at least 22 random characters A-Z, a-z, 0-9).</p>	<p>Example - "nonce": "d71a4edca5504b93a585f03dfb14267a"</p>
state	<p>REQUIRED. MUST be a string.</p> <p>Accepted values - MUST contain at least 128 bits of entropy (for example at least 22 random characters A-Z, a-z, 0-9).</p>	<p>Example - "state": "9034a5d8-12b9-58a8-b123-98b76f54a220"</p>
acr_values	<p>REQUIRED. MUST be a string.</p>	<p>Example - "acr_values": "http://ftn.ficora.fi/2017/1oa2"</p>

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

	<ul style="list-style-type: none"> ▪ en ▪ fi ▪ sv <p>Default value - fi</p>	
prompt	<p>REQUIRED for Chained OPTIONAL for Normal MUST be a string.</p> <p>Accepted value - MUST always be “login” if this parameter is passed.</p>	<p>Example - “prompt”: “login”</p>
response_mode	<p>OPTIONAL. MUST be a string.</p> <p>Accepted values - MUST always be “form_post” if this parameter is passed.</p>	<p>Example - “response_mode”: “form_post”</p>
ftn_idp_id	<p>OPTIONAL. MUST be a string. Accepted values -</p> <p>MUST only be the FTN id provided to the Identity Provider. (If this parameter is passed, Broker will not display the list of IDPs to authenticate from, instead will directly call this IDP for authentication).</p>	<p>Example - “ftn_idp_id”: “fi-danskebank”</p>

<p>ftn_spname</p>	<p>REQUIRED</p> <p>MUST be a string.</p> <p>Accepted values - Name to be displayed in authentication flow</p>	<p>Example -</p> <p>"ftn_spname": "Danske Bank Test Client"</p>
--------------------------	----------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------

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/broker-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=SAD35F67H D8H
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 - <ul style="list-style-type: none"> ▪ invalid_request ▪ invalid_request_object ▪ unauthorized_client 	Example - error=invalid_scope

	<ul style="list-style-type: none"> ▪ invalid_client ▪ invalid_scope ▪ unsupported_response_type ▪ server_error 	
error_description	<p>Returns this parameter only in case of an error.</p> <p>This contains an error id (Trace ID) which can be forwarded to Danske Bank to analyze errors, if required.</p>	<p>Example -</p> <p>error_description= Invalid_scope. {Trace ID:- b5361c4b-e84d-4382-a0ab-d776165a1998}.</p>
error_uri	<p>Returns this parameter only in case of an error.</p> <p>Gives the link to the error codes page which will give more information on the error.</p> <p>Value is always, 'https://userapi2.danskebank.com/prod/external/ftn/broker-oidc/errorcodes '.</p>	<p>Example -</p> <p>error_uri= https://userapi2.danskebank.com/prod/external/ftn/broker-oidc/errorcodes</p>

6.2.4 Response example (success)

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

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/broker-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	<p>REQUIRED. MUST be a string. Identifier of the party initiating the authentication (Service Provider / Broker), assigned to the Service Provider / Broker by the Broker.</p> <p>Accepted values - MUST be the same as the Client ID received during client registration.</p>	<p>Example - "client_id": "0234a472-b4ea-4e62-9ec0- ea1ac96789ab"</p>
code	<p>REQUIRED. MUST be a string.</p> <p>Accepted values - MUST be as received after completion of the authorize endpoint from Broker.</p>	<p>Example - "code": "JH2GF3RXH5CT6V KIB"</p>
grant_type	<p>REQUIRED. MUST be a string.</p> <p>Accepted values - MUST always be "authorization_code".</p>	<p>Example - "grant_type": "authorization_code"</p>
redirect_uri	<p>REQUIRED. MUST be a string.</p>	<p>Example -</p>

	<p>Accepted values - MUST be the same as the one used in authorization endpoint.</p>	<p>“redirect_uri”: “https://myclient_redirect_url.com”</p>
client_assertion_type	<p>REQUIRED. MUST be a string.</p> <p>Accepted values - MUST always be “urn:ietf:params:oauth:client-assertion-type:jwt-bearer”.</p>	<p>Example - “client_assertion_type”: “urn:ietf:params:oauth:client-assertion-type:jwt-bearer”</p>
client_assertion	<p>REQUIRED. MUST be a signed JWT. The required values in the JWT payload are listed in this document.</p> <p>Accepted values - MUST include the claims iss, sub, aud, jti, and exp.</p>	<p>Example - “client_assertion”: “eyJhbGciOi4V7g8UwCv3svCENau_N4.w9CA4gNI52dTdQnp”</p>

7.1.5 Request client assertion JWT header parameters

Parameter name	Required / Optional and Description	Examples
alg	<p>REQUIRED. MUST be a string. The value MUST be “RS256”.</p>	<p>Example - “alg”: “RS256”</p>
kid	<p>REQUIRED. MUST be a string.</p>	<p>Example -</p>

	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	<p>REQUIRED. MUST be a string. Represents audience.</p> <p>Accepted values - MUST be the URL of Danske Bank Broker's Token Endpoint (as obtained from "token_endpoint" parameter in Section 4.2.3).</p>	<p>Example - "aud": "<domain>/connect/token"</p>
exp	<p>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.</p> <p>Accepted values - MUST be 10 minutes or less into the future from the token issued timestamp.</p>	<p>Example - "exp": "1550032168"</p>
jti	<p>REQUIRED. MUST be a string. Any random value to be used uniquely.</p>	<p>Example - "jti": "abcdefghijklmno"</p>

	<p>Accepted values - MUST NOT be repeated by a specific Service Provider/ Broker (with a unique Client ID) in the last 10 minutes.</p>	
--	----------------------------------------------------------------------------------------------------------------------------------------------------	--

7.1.7 Request example

Ex.	<p>POST <domain>/connect/token</p>
------------	------------------------------------------------------

7.2 Response details

7.2.1 Response type

string	JavaScript Object Notation (JSON) type
---------------	----------------------------------------

7.2.2 Response codes

<https://userapi2.danskebank.com/prod/external/ftn/broker-oidc/errorcodes>

7.2.3 Response parameters

Parameter name	Description	Examples
access_token	This is an encrypted string.	Example -

	'access_token' is not necessarily used in the typical FTN use case, but it is required by OAuth 2.0.	"access_token": "ASDJAKSDHJADHA HSDKJAJHKSJHDK ADS"
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	<p>This is a JWT signed using Danske Bank Broker's private key and then encrypted using Service Provider's or Broker's public key. This contains information about the end user that authenticated.</p> <p>The required values in the JWT header and payload are listed in sections.</p> <p>Response ID Token header parameters and Response ID Token payload parameters respectively.</p>	Example - "id_token": " eyJhbGciOi4V7g8UwCv 3svCENau_N4.w9CA 4gNI52dTdQnp.fdsf78 786fdf"
error	<p>Returns this parameter only in case of an error.</p> <p>Error messages provided -</p> <ul style="list-style-type: none"> ▪ invalid_request ▪ unauthorized_client ▪ invalid_client ▪ invalid_scope 	Example - "error": "invalid_grant"

	<ul style="list-style-type: none"> ▪ invalid_grant ▪ unsupported_grant_type ▪ server_error 	
error_description	<p>Returns this parameter only in case of an error.</p> <p>This contains an error id (Trace ID) which can be forwarded to Danske Bank to analyze errors, if required.</p>	<p>"error_description": "invalid_grant. {Trace ID:- b5361c4b-e84d-4382-a0ab-d776165a1998}."</p>
error_uri	<p>Returns this parameter only in case of an error.</p> <p>Gives the link to the error codes page which will give more information on the error.</p> <p>Value is always 'https://userapi2.danskebank.com/prod/external/ftn/broker-oidc/errorcodes '.</p>	<p>"error_uri": "https://userapi2.danskebank.com/prod/external/ftn/broker-oidc/errorcodes"</p>

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		Example -

	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 JWKS URL of the Service Provider.	"kid": "DSF557GHJ8HUK"
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.

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 .	Example -

	<p>Value is always,</p> <p>Production https://userapi2.danskebank.com/ftn-broker</p> <p>Test Production "https://sandbox-userapi2.danskebank.com/ftn-broker"</p>	<p>"iss": "https://userapi2.danskebank.com/ftn-broker"</p>
sub	<p>Represents Subject Identifier MUST be locally unique.</p> <p>Accepted Values - Value is Unique ID for each Identification request.</p>	<p>Example - "sub": "f9aeb649517b9d4fe46c4ea55d751359033512bbfa8c516c681aa0434fb8ffbe"</p>
aud	<p>Represents audience.</p> <p>Value is client ID provided at the time of registration.</p>	<p>Example - "aud": "0234a472-b4ea-4e62-9ec0-ea1ac96789ab"</p>
exp	<p>Represents expiry time.</p> <p>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.</p> <p>All FTN participants SHOULD be configured with a reliable UTC time source.</p>	<p>Example - "exp": "1550032168"</p>

	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.	
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	<p>Case sensitive string from the authentication request to associate an end-user with an ID token and to mitigate replay attacks.</p> <p>The FTN Broker MUST verify that the nonce claim value is equal to the value of the nonce parameter sent in the authentication request.</p>	Example - "nonce": "d71a4edca5504b93 a585f03dfb14267a"
acr	<p>The Authentication Context Class Reference string for this authentication transaction.</p> <p>This will be the same value as received during authorization endpoint.</p>	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":"eyJhbGciOi4V7g8UwCv3svCENau_N4.w9CA4gN152dTdQ
np.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/broker-
oidc/errorcodes"
}
```