Finnish Trust Network

Danske Bank's Broker

SYST

API Document

Table of Content

Change log

Version	Date	Change Summary
1.0	29-03-2019	Initial version
1.1	04-07-2019	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	18-09-2019	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	- 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 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 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 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 (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, ftn_chain_level parameter both are mandatory for chained authentication during the Authorize request along with the use of the Client ID registered for chained authentication

2.2 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:

https://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/.well-known/openid-configuration

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

2.3 Key Exchange

The public keys used in signing and encryption are exchanged by reference (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.

2.4 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.

2.5 Level of Assurance

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

http://ftn.ficora.fi/2017/loa2

2.6 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 https://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/.well-known/openid-configuration	Well-known config URI
2	GET https://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/.well-known/openid-configuration/jwks	Well-known config jwks URI
3	GET https://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/connect/authorize	Authorize endpoint
4	POST https://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/connect/token	Token endpoint
5	GET https://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/errorcodes	Error codes information. Provides a list of errors thrown by Danske Bank API calls.

4 GET .well-known/openid-configuration

4.1 Request details

4.1.1 Request endpoint URI

GET	https://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/.well-known/openid-configuration

4.1.2 Request header

JSON	accept: application/json

4.1.3 Request body

N/A	Not Applicable

4.1.4 Request example

Ex.	**GET** https://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/.well-known/openid-configuration

4.2 Response details

4.2.1 Response type

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

4.2.2 Response codes

200	Success
404	Not found
500	Server error

4.2.3 Response parameters

Parameter name	Description
issuer	Identifies the issuer of the response
jwks_uri	Holds the JWKS URI path
authorization_endpoint	Points to the authorization endpoint
token_endpoint	Points to the token endpoint

scopes_supported	Lists the scopes supported
response_types_supported	Lists the response types supported
response_modes_supported	Lists the response modes supported
grant_types_supported	Lists the grant types supported
subject_types_supported	Lists the subject types supported
id_token_signing_alg_values_supported	Lists the ID token signing alg values supported
id_token_encryption_alg_values_supported	Lists the ID token encryption alg values supported
id_token_encryption_enc_values_supported	Lists the ID token encryption enc values supported
request_object_signing_alg_values_supported	Lists the request object signing alg values supported
token_endpoint_auth_methods_supported	

	Lists the token endpoint authorization methods supported
request_parameter_supported	Holds true or false if request parameter is supported
claims_supported	Lists the claims supported
code_challenge_methods_supported	Lists the code challenge methods supported

4.2.4 Response example

Ex.

```
{
    "issuer":"insert_value_here",
    "jwks_uri":" insert_value_here",
    "authorization_endpoint":" insert_value_here",
    "token_endpoint":" insert_value_here",
    "scopes_supported":[" insert_value_here"],
    "response_types_supported":[" insert_value_here"],
    "response_modes_supported":[" insert_value_here"],
    "grant_types_supported":[" insert_value_here"],
    "subject_types_supported":[" insert_value_here"],
    "id_token_signing_alg_values_supported":[" insert_value_here"],
    "id_token_encryption_alg_values_supported":["
insert_value_here"],
    "id_token_encryption_enc_values_supported":["
insert_value_here"],
    "token_endpoint_auth_methods_supported":[" insert_value_here"],
    "request_object_signing_alg_values_supported":["
insert_value_here"],
    "request_parameter_supported":true,
    "claims_supported":[" insert_value_here"],
    "code_challenge_methods_supported":[" insert_value_here"]
}
```

5 GET .well-known/openid-configuration/jwks

5.1 Request details

5.1.1 Request endpoint URI

GET	https://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/.well-known/openid-configuration/jwks

5.1.2 Request header

JSON	accept: application/json

5.1.3 Request body

N/A	Not Applicable

5.1.4 Request example

Ex.	**GET** https://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/.well-known/openid-configuration/jwks

5.2 Response details

5.2.1 Response type

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

5.2.2 Response codes

200	Success
404	Not found
500	Server error

5.2.3 Response parameters

Parameter name	Description
keys	Holds the JSON Web Key value. Consist of the parts – key, use, kid, x5t, e, n and x5c. The components are elaborated in section **5.2.4 Key Parameter Parts**.

5.2.4 Key parameter parts

Parameter name	Description
kty	Represents **key type**. Identifies the cryptographic algorithm family used such as RSA or EC.
use	Represents **public key type**. Identifies the intended use of public key such as **sig** (signature) or **enc** (encryption).
kid	Represents **key identity**. Parameter used to match to a specific key.
x5t	Represents **X.509 certificate SHA-1 thumbprint**. Parameter is Base64url encoded SHA-1 thumbprint of the DER encoding of an X.509 certificate.
e	Represents the **exponent**.
n	Represents the **modulus**.
x5c	Represents **X.509 certificate chain**. Contains a chain of one or more PKIX certificates.

5.2.5 Response example

Ex.


```
{
    "keys":
    [
        {
            "kty":"kty_value_here",
            "use":"use_value_here",
            "kid":"1234567890987654321",
            "x5t":"x5t_value_here",
            "e":"e_value_here",
            "n":"n_value_here",
            "x5c":["x5c_value_here"],
        }
    ]
}
```

6 GET /connect/authorize

6.1 Request details

6.1.1 Request endpoint URI

GET	https://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/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 Broker. **Accepted values –** MUST be the same as the Client ID received during client registration.	client_id=0234a472-b4ea-4e62-9ec0-ea1ac96789ab
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 Broker for the corresponding Client ID.	**Example –** redirect_uri=https://dummy-client-redirect-uri.com
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.	**Example –** scope=openid ftn_hetu

	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= d71a4edca5504b93 a585f03dfb14267a
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 –** ▪ http://ftn.ficora.fi/2017/loa2	
ui_locales	**OPTIONAL.** MUST be a **string**. End user language preference tags (BCP 47). **Accepted values –** ▪ en ▪ fi ▪ sv **Default value –** fi	**Example –** ui_locales=en
prompt	**OPTIONAL.** 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_idp_id	**OPTIONAL.** MUST be a **string**. Accepted values –	**Example –** ftn_idp_id=fi-danskebank

	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).	
ftn_chain_level	**OPTIONAL** **REQUIRED** in chained authentication flow. MUST be a **string** describing the Level of Assurance (LoA) of the authentication token/means being issued. It MUST be of the same LoA level that is used by the user to perform the authentication **Accepted values –** http://ftn.ficora.fi/2017/loa2	**Example –** ftn_chain_level =http://ftn.ficora.fi/2017/loa2
request	**OPTIONAL** **REQUIRED** in chained authentication flow. **MUST** be signed JWT. The request Authorization Request parameter enables	**Example** – request=eyJhbGciOiJSUzI1N.eyJhdWQiOiJodHRwczovL3N5c3Q.kqdX57bfih1xVLCICkcCOKRBhFz4

	OpenID Connect requests to be passed in a single, self-contained parameter and it's must be signed.	

6.1.5 Request example

Ex.

```
https://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/connect/authorize?
client_id=<insert_value_here>&
redirect_uri=<insert_value_here>&
response_type=<insert_value_here>&
scope=<insert_value_here>&
response_mode=<insert_value_here>&
nonce=<insert_value_here>&
state=<insert_value_here>&
acr_values=<insert_value_here>&
ui_locales=<insert_value_here>&
prompt=<insert_value_here>&
ftn_idp_id=<insert_value_here>&
request=<insert_value_here>
```

6.1.6 Request example - Chained

Ex.

```
https://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/connect/authorize?
client_id=<insert_value_here>&
redirect_uri=<insert_value_here>&
response_type=<insert_value_here>&
scope=<insert_value_here>&
response_mode=<insert_value_here>&
nonce=<insert_value_here>&
state=<insert_value_here>&
acr_values=<insert_value_here>&
ui_locales=<insert_value_here>&
prompt=<insert_value_here>&
ftn_idp_id=<insert_value_here>&
ftn_chain_level=<insert_value_here>&
request=<insert_value_here>
```

6.1.7 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"
kid	**REQUIRED.** MUST be a **string**. 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.	**Example –** "kid" : "DSF557GHJ8HUK"
typ	**OPTIONAL.** MUST be a **string** if passed. The value MUST be "JWT" if passed.	**Example –** "typ" : "JWT"

6.1.8 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**.	**Example –**

	Accepted values – MUST be the URL of OP's (OpenID provider) Issuer Identifier URL.	"aud": "https://syst-userapi2.danskebank.com/ftn-broker"
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	**OPTIONAL.** MUST be a **string**.	**Example –**

	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 Danske Bank which provides the mandatory natural person attributes. Danske Bank does not support any Legal Person attributes as of now.	"Scope"="openid ftn_hetu"
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	**OPTIONAL.** MUST be a **string**. MUST be a space-separated list of requested FTN authentication context class reference values. **Accepted values –** ▪ http://ftn.ficora.fi/2017/loa2	**Example –** "acr_values"="http://ftn.ficora.fi/2017/loa2"
response_type	**OPTIONAL.** MUST be a **string**. **Accepted values –** MUST always be "**form_post**", if this parameter is passed.	**Example –** "response_mode"="form_post"
ftn_chain_level	**OPTIONAL.** MUST be a **string**. **Accepted values –** MUST always be same as the acr_value mentioned above	**Example –** "ftn_chain_level"="http://ftn.ficora.fi/2017/loatest2"

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

302	Redirect
400	Invalid request Invalid client Invalid request object Invalid scope Unsupported response type
401	Unauthorized client
500	Server error

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 ▪ server_error	**Example –** error=invalid_scope
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 'https://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/errorcodes '.	**Example –** error_uri=https://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/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://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/errorcodes

7 POST /connect/token

7.1 Request details

7.1.1 Request endpoint URI

POST	https://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/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%3Aietf%3Aparams%3Aoauth%3Aclient-assertion-type:jwt_bearer&client_id=my_service_client_id&code=code_value_here&grant_type=authorization_code&redirect_uri=https%3A%2F%2Fmyclient_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 Broker. **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 Broker.	**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.** MUST be a **string**.	**Example –**

	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 **8.1.5**. **Accepted values –** MUST include the claims iss, sub, aud, jti, and exp.	**Example –** "client_assertion": "eyJhbGci0.V7g8UwCv3svCENau_N4.w9CA4gNl52dTdQnp"

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**. Represents **audience**.	**Example –**

	Accepted values – MUST be the URL of Danske Bank Broker's Token Endpoint (as obtained from "token_endpoint" parameter in Section 4.2.3).	"aud" : " https://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/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** https://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/connect/token

7.2 Response details

7.2.1 Response type

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

7.2.2 Response codes

200	Success
400	Invalid request Invalid client Invalid scope Invalid grant Invalid grant type

401	Unauthorized client
500	Server error

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" : "1550032168"
id_token	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. The required values in the JWT header and payload are listed in this document	**Example –** "id_token" : "eyJhbGci0.V7g8UwCv3svCENau_N4.w9CA4gN152dTdQnp.fdsf78786fdf"

	Response ID Token header parameters and **Response ID Token payload parameters** respectively.	
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://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/errorcodes '.	"error_uri": "https://syst-userapi2.danskebank.com/syst/external/ftn/broker-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 JWKS URL of the Service Provider.	**Example –** "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 as mentioned in Section 8.2.5.

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**. Value is always "https://syst-userapi2.danskebank.com/ftn-broker"	**Example –** "iss" : "https://syst-userapi2.danskebank.com/ftn-broker"
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	**Example –** "exp" : "1550032168"

	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.	
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 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 (parameter: acr_values).	**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":"150032168",
}

7.2.8 Response example (error)

Ex.

{

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

8 GET /errorcodes

8.1 Request details

8.1.1 Request endpoint URI

GET	https://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/errorcodes

8.1.2 Request header

N/A	Not Applicable

8.1.3 Request body

N/A	Not Applicable

8.1.4 Request example

Ex.	**GET** https://syst-userapi2.danskebank.com/syst/external/ftn/broker-oidc/errorcodes