Finnish Trust Network

Danske Bank's Broker
Business Documentation

Table of Content

Change log

Version	Date	Change Summary
1.0	20-05-2019	Initial version
2.0	20-06-2020	Misc. changes in all sections

1 Abbreviations

FTN = Finnish Trust Network.

OIDC = OpenID Connect.

SP = Service Provider, provides a service to the end-user.

IdP = Identity Provider within the FTN.

JWT = JSON Web Token (RFC 7519).

JWK = JSON Web Key.

JWKS = JSON Web Key Set.

LoA = Level of Assurance.

2 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.

3 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.

3.1 Chained authentication

Danske Bank Broker supports Chained Authentication. The Service Provider must register with request for chained authentication with a dedicated Client Id and the respective Client Id must be used when there is a need for Chained Authentication while invoking Danske Bank Broker.

3.2 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 Danske Bank Broker.

3.3 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.

3.4 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.

3.5 Level of Assurance

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

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

3.6 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.

4 Operating Time / Service Availability

Days	Operating hours	Maintenance / Service window (If and when required)
Monday	00.00 - 24.00 EEST	None
Tuesday	00.00 - 24.00 EEST	None
Wednesday	00.00 - 24.00 EEST	None
Thursday	00.00 - 24.00 EEST	None
Friday	00.00 - 24.00 EEST	None
Saturday	00.00 - 24.00 EEST	None
Sunday and holidays	00.00 - 24.00 EEST	00.00 – 06.00 CET
Critical times	24x7	

5 Security

As per TRAFICOM recommendations, all URLs requested by the end-user browser and all correspondence between Service Provider and Danske Bank's Broker and between Danske Bank's Broker and a FTN Identity Provider MUST begin with https://.

All participants in the FTN universe (SP, Broker and IDP) MUST support TLS version 1.2 (RFC 5246) or higher. However, downgrade to TLS version 1.1 is allowed for the customer facing endpoints in order to accommodate the end-user's browser capabilities.

All data exchanged between Service Provider and Danske Bank's Broker and between Danske Bank's Broker and FTN Identity provider MUST be signed and encrypted using RSA key pairs, to maintain the data integrity and to avoid any third parties from changing the data without the knowledge of the involved parties.

The private part of the key pair MUST be stored securely by the issuing party and the public part of the key pair is shared with the other parties. The keys used in the FTN identification process are as follows:-

Issuer	Key type	Usage
Service Provider	Private Key	This key will be used to sign the assertion JWT which is to be sent in token endpoint call.
Service Provider	Public Key	This key will be exposed to Danske Bank Broker via Service Provider's JWKS URI. This key will be used by Danske Bank Broker to encrypt the identity token before sharing it with Service Provider It will also be used to verify signature of assertion JWT sent by Service Provider/ Broker.
Danske Bank Broker	Private Key	This key will be used by Danske Bank Broker to sign the identity token before it is encrypted using SP's public key.
Danske Bank Broker	Public Key	This key will be exposed to Service Providers/ Identity Providers via Danske Bank Broker's JWKS URI.

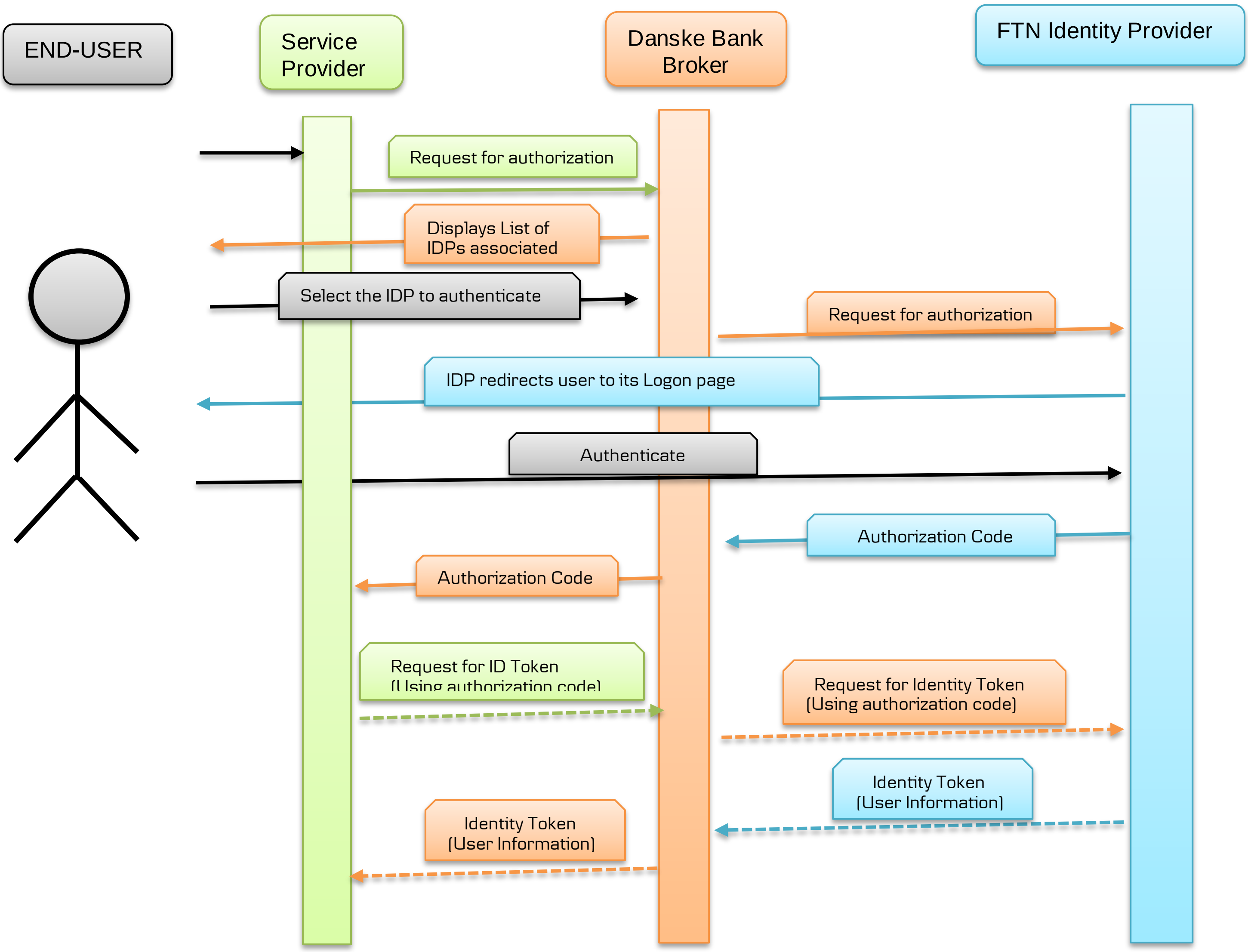
Service Provider and Danske Bank Broker are responsible for the security and correctness of the data and the RSA keys they use. The end-user is responsible for the protection of the credentials and other customer identification tools provided by Danske Bank. The end-user is also responsible for ensuring that they use their credentials ONLY on secured logon page of the FTN Identity Provider and not on any other third party sites.

6 Identification Flow

Danske Bank follows the FTN OIDC specifications as provided by TRAFICOM (**Finnish Trust Network OpenID Connect 1.0 Protocol Profile**) which is basically an adoption of the OIDC Authorization Code flow as per OIDC specifications defined in **OpenID Connect v1.0 protocol**.

The below diagram illustrates the flow for the process of an end-user performing authentication and authorization through a Service Provider registered with Danske Bank Broker and an FTN Identity Provider.

As per TRAFICOM, the whole process MUST be completed within 10 minutes from when the process first starts. All the FTN parties SHOULD monitor the time independently and any party may abort the entire identification process if the time limit is exceeded.


END-USER
Service Provider
Danske Bank Broker
FTN Identity Provider
Request for authorization
Displays List of IDPs associated
Select the IDP to authenticate
Request for authorization
IDP redirects user to its Logon page
Authenticate
Authorization Code
Authorization Code
Request for ID Token (Using authorization code)
Request for Identity Token (Using authorization code)
Identity Token (User Information)
Identity Token (User Information)

7 Registration

The Service Provider must first make an agreement with Danske Bank to use the Broker service.

When the agreement has been made, Service Providers must also provide onboarding data such as Redirect URIs, JWKS URI for sharing their public keys and identification methods. This information will be used by Danske Bank to provide a specific Client ID to be used to get access to Danske Bank's Broker services.

Any Service Provider already having an existing agreement will only be required to provide the configuration data as above and do not require to create a new agreement. However, they will still be getting a new Client ID required to consume Danske Bank's Broker services.

8 Information and Support

For any further information or onboarding onto Danske Bank's Broker Services, please contact the following:-

1. Danske Bank branch office in Finland during opening hours.
2. Call our Customer Support at +358 100 2580 on business days(Mon – Fri between 08:00-18:00)

In case of any technical issues while integrating with Danske Bank's Broker services, please send your technical queries to the following email address, providing the detailed issue/error description:-

r34bdftn@danksebank.dk