Finnish Trust Network

Danske Bank's Identity Provider
Business Documentation

Table of Content

Change log

Version	Date	Change Summary
1.0	16-04-2019	Initial version

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).

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 services with trusted identity and service 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. **Finnish communications regulatory authority (FICORA)** is the public authority responsible of communication regulations in Finland and has recommendation for two interfaces for SAML 2 (Security Assertion Markup Language) and OIDC (OpenID Connect) to use in FTN. There are 3 Roles in FTN, FTN Identity Service Providers, FTN Broker service provider and Service Providers/Relying Parties.

Danske Bank having the Identity Information, is offering FTN Identity Provider Services following the above recommendations from FICORA. As per the terms of the service (as recommended by FICORA), Danske Bank will identify the end-user (customer) and provide relevant personal information about the end-user to the Service Provider, for which the end-user is authenticating.

Danske Bank along with other similar Identity Providers will form the trust network (a network of service providers rendering their services according to the Finnish law of electronic identification which is supervised by the Finnish Communications Regulatory Supervisory Authority, TRAFICOM, formerly FICORA) for all Finland concerned Service Providers to serve their regional customers/clients by providing a secure, faster and simpler log-on process.

3 Service Description

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

The Identify Broker Services and Service Providers MUST exchange metadata with Danske Bank's Identify Provider, agreed at the time of subscription, which will be used to form a technical trust between parties. Parties exchange metadata or address referring to it at the time of service subscription or the signing of the service agreement.

The parties MUST identify each other at subscription. Authentication of the end user is only possible by using endpoint addresses to communicate and the keys specified in the metadata to sign, encrypt, verify and decrypt messages.

If there are changes, the parties are REQUIRED to communicate with each other in advance about changes in the details of the metadata. If there are changes to the technical and/or business representatives of the service agreement, the contact details of the representatives, the new representatives MUST be identified as was done at the time of initial subscription.

A typical scenario when Danske Bank's Identity Provider can be used is as follows:-

1. A Finnish citizen wants to use the services of a typical FTN Service Provider.
2. The Service Provider needs to identify the person who wants to use its services.
3. In order to identify the person, the Service Provider sends an identification request to the person.
4. If the person has Danske Bank credentials, he/she can select Danske Bank's Identity Provider and enter his/her login credentials.
5. Danske Bank's Identity Provider identifies the person and sends back an authorization code to the Service Provider.
6. In order to complete the flow, the Service Provider needs to exchange this authorization code with Danske Bank's Identity Provider for an ID Token.
7. The ID Token contains personal details (attributes) of the authenticated person as an encrypted and signed JWT, which can be used by the Service Provider to identify the person and enable him/her to use its services.

3.1 Supported Attributes and shared personal data

Danske Bank Identity provider Service supports only the REQUIRED attributes profile of a Natural Person from the FTN OIDC Specification.

Danske Bank Identity provider can be used to identify only Natural Persons in domestic scheme.

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

Danske Bank Identity Provider cannot be used to identify legal entities as of this moment. Any changes in the availability of this feature can and will be circulated in future correspondences on Danske Bank Finland's homepage.

3.2 Chained authentication

If for some reason, an FTN Identity Provider cannot identify a user/customer, it can forward the task of identification to another FTN Identity Provider. This concept is known as chained authentication from an FTN perspective.

This document will not delve into the details of Chained Authentication.

For more details, please check the Finnish Transport and Communications Agency (Traficom) site.

Danske Bank Identity provider currently does not support Chained Authentication.

3.3 Metadata

Danske Bank publishes the metadata of Identity according to the OIDC Connect Discovery 1.0 specification. The endpoint URI will be released at the time of subscription.

The metadata endpoint address is in form of:
https://userapi2.danskebank.com/prod/external/ftn/idp-oidc/.well-known/openid-configuration

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

3.4 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.

3.5 Level of Assurance

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

- http://ftn.ficora.fi/2017/loa2
- http://ftn.ficora.fi/2017/loa3
- http://eidas.europa.eu/LoA/substantial
- http://eidas.europa.eu/LoA/high

3.6 Single Sign-On (SSO)

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

3.7 User Consent

User Consent information is not included in Danske Bank's Identity Provider as it is not included in the scope of FTN OIDC specifications (as per FICORA).

As per FTN, for a typical authentication use case, the consent is implicit and it is not necessary for the Service Provider/ Broker to individually ask for user consent for every transaction made by the end-user.

If any Service Provider/ Broker needs the consent from the end-user, they must do so of their own volition.

3.8 Usability Criteria

Danske Bank's Identity Provider can be used to identify all persons who are customers of the Bank holding an active private customer agreement and logon credentials.

Danske Bank's Identity Provider will not identify any persons who do not have a Finnish Identity Number (HETU).

3.9 Service Availability.

Days	Operating hours	Maintenance / Service window (If and when required)
Monday	00.00 – 24.00 EEST	
Tuesday	00.00 – 24.00 EEST	
Wednesday	00.00 – 24.00 EEST	
Thursday	00.00 – 24.00 EEST	
Friday	00.00 – 24.00 EEST	
Saturday	00.00 – 24.00 EEST	
Sunday and holidays	00.00 – 24.00 EEST	06.00 – 12.00 EEST
Critical times	24x7	

3.10 Security

As per FICORA recommendations, all URLs requested by the end-user browser and all correspondence between Service Provider/ Broker and Danske Bank's 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/ Broker and Danske Bank's 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 both Service Provider/ Broker and Danske Bank.

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

Both the Service Provider/ Broker and Danske Bank are responsible for the security and correctness of the data and the RSA keys they use.

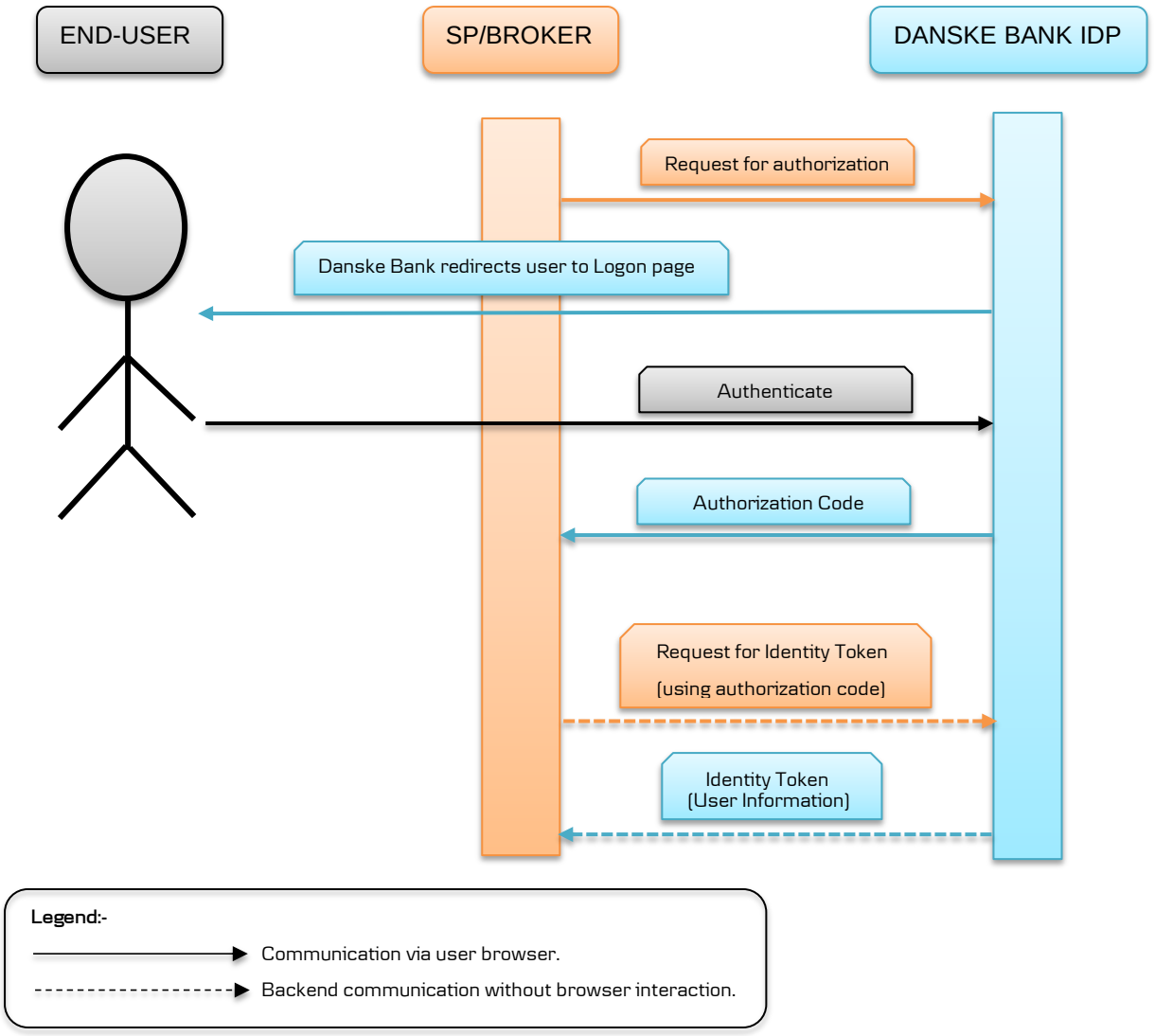
The end-user is responsible for the protection of the credentials and other customer identification tools provided by Danske Bank. The end-user is also responsible for ensuring that they use their Danske Bank's credentials ONLY on Danske Bank's secured logon page and not on any other third party sites.

4 Identification Flow

Danske Bank follows the FTN OIDC specifications as provided by FICORA (**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 Danske Bank's Identity Provider.

As per FICORA, 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.



5 Registration

The Service Provider/ Broker must first make an agreement with Danske Bank on the features and use of the Identity Provider service.

When the agreement has been made, Service Providers/ Brokers must also provide configuration 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 Identity Provider 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 call Danske Bank's Identity Provider services.

6 Information and Support

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

1. Your own Danske Bank branch office during opening hours.
2. Call our Customer Support at +358 100 2580 Mon – Fri 08-18.

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

r34bdftn@danksebank.dk