Finnish Trust Network

Danske Bank's Broker
OIDC key exchange

Table of Content

1 Introduction 3
1.1 Abbreviations 3
2 Key Exchange Process 4
2.1 Public key exchange from Danske Bank to SP 4
2.2 Public key exchange from SP to Danske Bank 4
2.3 Key Exchange 4
2.4 Algorithms and Key sizes 5
2.5 Key update and revocation 5
2.6 Key usage 6
3 References 7

Change log

Version	Date	Change Summary
1.0	08-05-2019	Initial version
2.0	03-11-2023	Updated as per M72B regulation

1 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.

Danske Bank Broker Services implements OpenID Connect Authorization Code flow authentication as per recommendations from FICORA in FTN OIDC profile. FICORA instructs the use of asymmetric public signing/encryption keys which needs to be exchanged beforehand between Service Provider or Broker and Danske Bank Broker Service. Protection of customer identities is based on public key cryptography using RSA key pairs. These keys are used for signing and encrypting Id Token and signing of JWT assertion. Secure key exchange by Danske Bank Broker Service is implemented based on FTN recommendations.

1.1 Abbreviations

FTN	Finnish Trust Network
OIDC	OpenID Connect
RSA	Public Key Cryptosystem (**Rivest–Shamir–Adleman**)
JWT	Json Web Token
SP	Service Provider
IdP	Identity Provider
JWKS	JSON Web Key Set

2 Key Exchange Process

Key exchange needs to be done between Service Provider (SP) and Danske Bank Broker Services.

2.1 Public key exchange from Danske Bank to SP

Danske Bank Broker Service has exposed Signed JWKS URI as below. This URI can be invoked to get Danske Bank Broker services public key. Danske Bank expects SP to fetch keys from this URI in regular interval to avoid issue in case of key renewed by Danske Bank.

https://userapi2.danskebank.com/prod/external/ftn/broker-oidc/signed-jwks

2.2 Public key exchange from SP to Danske Bank

Danske Bank expects to receive similar Signed JWKS URI or keys shared via secure email from SP. Usage of Signed JWKS will remove manual intervention in case of key renewal. SP would be able to renew their keys and publish in Signed JWKS URI. It will be Danske Bank's responsibility to fetch keys in regular interval from this Signed JWKS URI provided by SP.

2.3 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.

The private part of the key must be stored secretly by the issuing party. Only the public part of the key should be shared via Signed JWKS URI.

The public key should always be issued by globally recognized CA. Self-issued public key is not recommended by FICORA and will not be accepted.

Format	Data	Issuer
URI (must be HTTPS)	GET https://userapi2.danskebank.com/prod/external/ftn/broker-oidc/signed-jwks	Danske Bank
URI (must be HTTPS)	Address of Signed JWKS web page	Service Provider

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 Key update and revocation

It will be issuer's responsibility to renew the RSA key pair in case the key is expired or public key is compromised. Danske Bank recommends to have expiration date to keys for security reasons.

In case of expiration of keys, the key must be renewed in advance and new key should be published in the Signed JWKS URI along with existing key. Later after actual expiry of the keys the old key must be removed from Signed JWKS URI.

In case key is compromised, the issuer of the key should immediately remove the keys from Signed JWKS URI and replace it with new keys.

2.6 Key usage

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 Signed JWKS URI. This key will be used by Danske Bank Broker to encrypt the identity token before sharing it with SP. It will also be used to verify signature of assertion JWT sent by SP
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 SP via Signed JWKS URI

3 References

Name	Link
FTN OIDC Profile - Finnish Trust Network OpenID Connect 1.0 Protocol Profile	https://www.traficom.fi/sites/default/files/media/file/Traficom_S213_2023_OIDC_Profile_v2_2_for_the_Finnish_Trust_Network_EN.pdf
OpenId Connect specification	http://openid.net/specs/openid-connect-core-1_0.html
RFC 7517 - JSON Web Key specification	https://tools.ietf.org/html/rfc7517
RFC 7519 - JSON Web Token specification	https://tools.ietf.org/html/rfc7519
RFC 7515 - JSON Web Signature specification	https://tools.ietf.org/html/rfc7515
RFC 7516 - JSON Web Encryption specification	https://tools.ietf.org/html/rfc7516