Nordea

Nordea e-identification

OIDC key exchange

Nordea

Change log

Version	Description/ Changes
1.0	Initial version

Nordea

Contents

Nordea

1 Context

Nordea e-identification service implements OpenID Connect Authorization Code flow authentication as defined in Finnish Trust Network (FTN) OIDC Profile. Integrity and non-repudiation of the customer identities in FTN is based on public key cryptography using RSA key pairs. Keys are needed for Id Token signing and encryption, and JWT assertion signing. Key Exchange in the context of Nordea E-identification service is implemented based on the Finnish Trust Network's recommendation for secure key exchange.

1.1 Abbreviations

FTN	Finnish Trust Network
JWK	JSON Web Key
JWKS	JSON Web Key Set
JWT	JSON Web Token
OIDC	OpenId Connect
RP	Relying Party (Broker or Service Provider)
SP	Service Provider (The company, organization or other party providing a service to end users and consuming Nordea’s e-identification service)
IdP	Identity Provider (Nordea in the context of this document)
RSA	Widely used public key cryptosystem

Nordea

2 Configuration for key exchange

Prior to key exchange, the Service Provider (SP) and the Identity Provider (IdP) both must integrate to the counter party's key exchange system. Nordea is the Identity Provider in the context of this document.

2.1 Establishment of secured channel

All communication regarding key exchange between SP and Nordea must be done using a standard secure communication channel. Note that also all the configuration data must be exchanged using the secure email channel.

Nordea uses secure email as the secure communication channel. The secure email service sends notification of the message to email address and message pin code to mobile phone number as a SMS message. The encrypted email can be read from a web service by entering the given pin code as an authentication input. Prerequisite for usage of the secure email system is that SP provides Nordea the email address and the mobile phone number of the SP's contact person when signing the agreement for e-identification service. If the contact person or his/her contact information changes, SP MUST inform Nordea well advanced.

2.2 Exchange of configuration data

Parties provide each other following key exchange configuration data through the secured channel:

Data	Format	Issuer
Address of the JWKS web page	URL (must be HTTPS)	Both Service Provider and Nordea
Client id	string	Nordea

The JWKS web page returns the public key set in the JWKS format. Usage of JWKS web page reduces amount of manual labor in case of key update. Client id is the public identifier for the SP's application.

The SP must provide Nordea a JWKS web page for fetching the public key for Id Token encryption and for the JWT Assertion signature validation. SP MUST inform Nordea minimum one month before changing the JWKS web page address. Nordea provides the JWKS web page address to the SP for fetching the public key for Id Token validation. Nordea also creates a unique client id and delivers it to the SP via secure channel.

Nordea

3 Key exchange

The private part of the key pair MUST be stored and kept secret by the issuing party. The public part of the key is shared with the counter party. Nordea E-identification service includes following RSA keys:

Key Type	Description	Issuer
Id Token signing key	Id Token is signed with a private key. The encryption key id (kid) is included in the header of issued JWS (https://tools.ietf.org/html/rfc7515#section-4.1.4).	Nordea
JWT assertion validation and Id Token encryption key	JWT (RFC 7519) Assertion is validated using a public key provided by the SP. The id of the key to be used MUST be included as a header in the JWT assertion JWS (https://tools.ietf.org/html/rfc7515#section-4.1.4). Id Token is encrypted using the same public key that the SP asked to use for validation of the JWT assertion. The encryption key id (kid) is included in the header of the issued JWE (https://tools.ietf.org/html/rfc7516#section-4.1.6).	Service Provider

Nordea publishes the public keys on Nordea's JWKS web page. Header of the public key response contains id of the Nordea's key pair. That key id MUST be used to validate the token signature. The SP publishes the public keys on SP's JWKS web page. The SP MUST provide the key pair's key id in the header. The SP MUST use unique key id for each IdP's key pair.

3.1 Key update and revocation

The key pairs must be updated if there is a reason to believe that the keys have been compromised, and in case of expiration.

In the case of expiration, the new keys must be created minimum one month before the expiration and new public keys should be published together with the existing keys in the JWKS web page. After that, key ids in identity authentication messages are changed and based on them, receiving party can download new keys from updated JWKS URI –pages when previously unknown key id has been detected.

If the private key has been compromised, then it needs to be removed from use immediately, a new key-pair needs to be created and the counter party needs to be informed about the key-change.

4 Sequence diagram

The main steps of the key exchange process are illustrated in the figure 1.

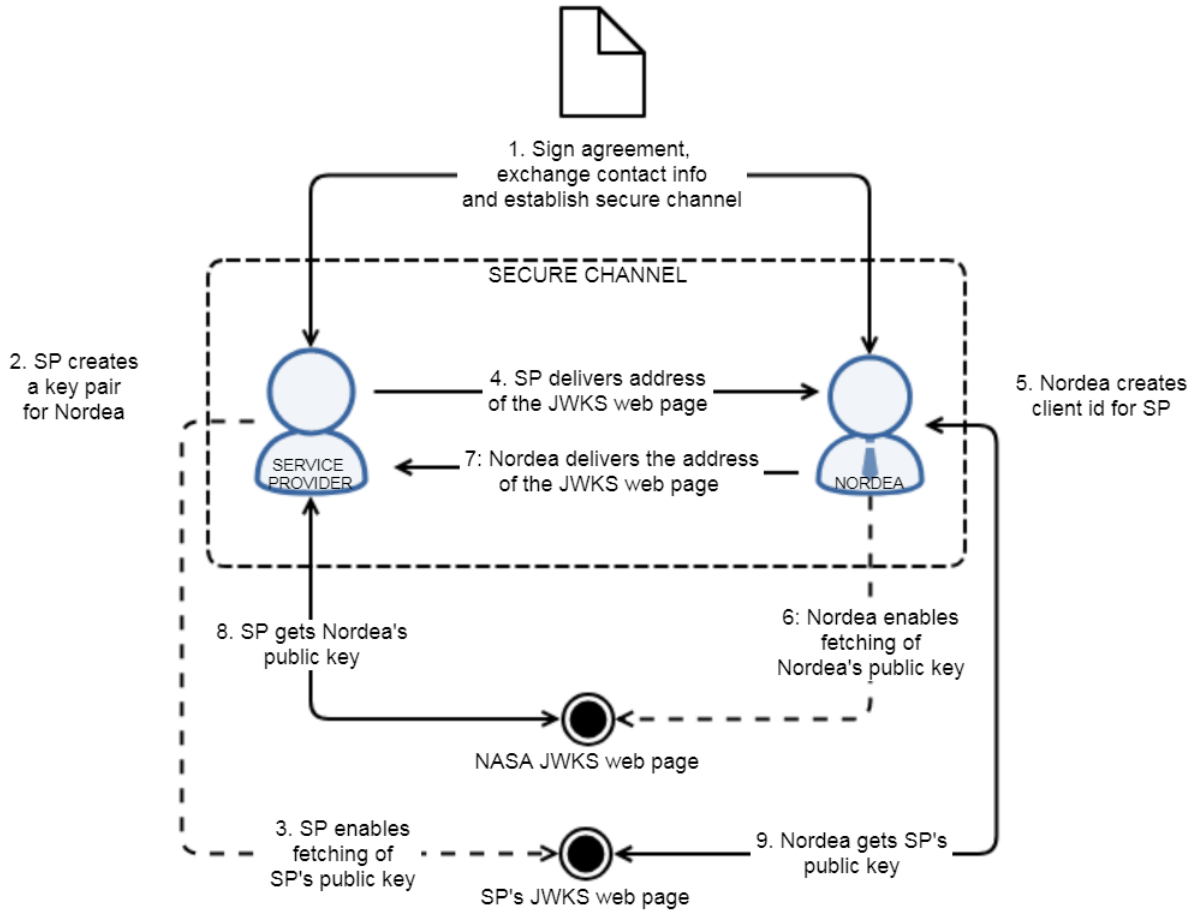

Figure 1 The key exchange process

Nordea

5 References

FTN OIDC Profile - Finnish Trust Network OpenID Connect 1.0 Protocol Profile version 1.0 213/2018 S 2018-01-26 (https://www.viestintavirasto.fi/attachments/suositukset/ftn_oidc_profile_v1.0_ficora_rec_213_2018_s.pdf)

FICORA Regulation 72 Notes – Explanatory notes to Regulation 72 2016-12-7 (https://www.viestintavirasto.fi/attachments/maaraykset/M72_2016_MPS_EN.pdf)

OpenId Connect (OIDC) 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

6 Information and support

In problem situations call the E-support for corporate customers on banking days:

In Finnish: 0200 67210 (8-17), local network charge/mobile call charge or international call charge

In Swedish: 0200 67220 (9-16.30), local network charge/mobile call charge or international call charge

In English: (+358) 200 67230 (9-17), local network charge/ mobile call charge or international call charge

Giving your customer ID speeds up service.