Nordea

Nordea e-identification

Service description

Nordea

Change log

Version	Description/ Changes
1.0	Initial version
1.1	Minor updates to examples & service hours
1.2	Updated footer
1.3	“lang” parameter replaced with “ui_locales”
1.4	client_assertion_type value fixed to follow OIDC specification
1.5	Other scopes than ftn_hetu deprecated Encryption algorithm must be RSA-OAEP

Nordea

Contents

1 Abbreviations

FTN	Finnish Trust Network
JWK	JSON Web Key
JWKs	JSON Web Key Set
JWT	JSON Web Token
LoA	Level of Assurance
OIDC	OpenId Connect
RP	Relying Party (Broker or Service Provider)
SP	Service Provider
IDP	Identity Provider

Nordea

2 Introduction

Nordea's e-identification enables the service providers in Finnish Trust Network (FTN) a mechanism for connecting large scale, consumer facing services with trusted identity using Nordea's electronic identification solutions to reliably identify its customers on the Internet. (*FTN OIDC Profile, page 1*.)

In the service Nordea identifies the customer on behalf of the service provider. The Trust Network follows the requirements and objectives of the European eIDAS regulation for a network of trust service providers enabling Citizen-to-Business-to-Government secure and trusted electronic service provisioning. The Network is built upon strong privacy and security principles and enables a user-centric attribute consent model. If specifically agreed between a customer and the service provider, the identification data transferred in the service can also be used to form a digital signature. Nordea issues the identification tools needed in the e-identification service. Nordea delivers the RSA keys to the service provider and the digital identification tools (e.g. Nordea Codes) supported by Nordea to the identifying customer. Nordea e-identification is following the Regulation 72 on Electronic Identification and Trust Services (pdf) and the recommendations defined by Finnish Communications Regulatory Authority (FICORA) in Finnish Trust Network - OpenID Connect 1.0 Protocol Profile

FTN OpenId Connect protocol interface is based on a standard OpenId Connect (OIDC) API (*OpenId Connect (OIDC) specification*)

Nordea's e-identification is part of FTN and together with similar services of other Finnish banks in the trust network the service provider can reach several million Finnish private persons on the Internet and increase its customer base. Nordea is listed in the register of suppliers of strong electronic identification service maintained by FICORA. The e-identification service offered by Nordea is a service of strong electronic identification as referred to in the identification act when the identification is made to a natural person who has a Finnish personal identity number. Nordea offers two kinds of e-identification services.

Traditional e-identification

- One method of identification per login.
- The bank is responsible for the correctness of the identification transaction.

E-identification for customers creating their own weak identification credentials (e.g. username & password):

- The customer identifies himself/herself/itself with the e-identification once.
- The service provider may issue its own identification credentials to the customer and those can be used to access the service in the future.
- The bank is responsible for the correctness of the identification transaction when e-identification is used.
- The service provider is responsible for identification transactions made with the customer's own codes.

E-identification for customers issuing a new substantial level strong identification service (e.g. new bank credentials):

- The customer identifies himself/herself/itself with the e-identification once.
- The service provider may issue its own strong identification service to the customer
- The bank is responsible for the correctness of the identification transaction when e-identification is used.
- The service provider is responsible for all authentication made with the new strong authentication service.

User consent information transfer is not included in the scope of FTN OIDC profile. Asking for user consent when needed is the responsibility of the party needing the consent. For the typical use case of authenticating a user to a Service Provider (without enrichment) the consent is implicit, and it is not necessary for the FTN Broker or IdP to separately ask for user consent for each authentication transaction. (*FTN OIDC Profile, page 2.)*

2.1 Advantages of e-identification

Nordea's e-identification, a service provider can make use of the same identification solutions that are used in Nordea's Netbank services. Possibility to use familiar identification methods increases the user-friendliness. With E- identification makes all Nordea's Netbank customers potential customers to the service provider. With e-identification the service provider can reliably identify its customers without separate access codes and passwords. This brings considerable savings to development and maintenance costs. A service provider and its customer can agree that e-identification is used in the creation of the customer's digital signature to conclude a legal transaction between them. This allows the customer to send applications to and make agreements with the service provider on the Internet. In a legal transaction, the bank's responsibility in the e-identification is the identification of the customer. The service provider must take care of other issues required in a digital signature, such as the supervision of transmitted information, recording of a return message and immutability of its service.

E-identification also increases the safety of making payments in online shops. For example, with e-identification the service provider and the customer can agree on a method for making orders and for invoicing. In addition, e-identification increases the safety of e-payment, because the use of due dated payments is more risk- free if the client identity is confirmed and the order is dated.

2.2 General description of e-identification

The starting point of the service is a customer who wants to identify him- or herself on the Internet. It is the customer who directs the transfer of his or her information between Nordea and the service provider. The identification given by Nordea is unique. The service transaction is traceable to the service provider and to the customer. When a service provider needs to identify a customer, it sends him or her an identification request. To perform the identification, the customer can select to use Nordea's e-identification service in the application, typically running in a web browser, provided by the service provider. Selecting Nordea's e-identification service transfers the service provider's identification request from the customer to Nordea, who identifies the customer and sends back a customer authentication response to the service provider via browser redirect. The customer can cancel the identification in Nordea e-identification service before the authentication. If the identification is cancelled, the customer's information is not transmitted to the service provider. To complete the authorization code flow, relying party needs

to exchange the authorization code received in the authentication response for an Id Token. Id Token contains the details of the authenticated customers in encrypted and signed JSON Web Token (*RFC 7519*)

The option to use the identification data in creation of digital signatures is based on a mutual agreement between the customer and the service provider allowing the identification data to be used as part of the digital signature in a legal transaction between them. The use of e-identification in a digital signature is also supported by the terms and conditions of Nordea's Netbank agreement and recorded with the time stamps of the return message and Nordea's log file. If the parties wish to use the service to make agreements or applications, the service provider must take care of other issues required in a digital signature, such as the supervision of transmitted information, recording of a return message and immutability of its service. Nordea is not responsible for the content or the validity of an agreement or other legal transaction between the service provider and the identifying customer nor for the eligibility or powers of a person using a company's identification data to represent the company or corporation.

2.3 Usability and availability

The e-identification service is intended for electronic services inside Finnish Trust Network which are directed at Finnish private persons and require strong identification. Strong electronic identification is based on personal identification tools provided by Nordea. Consequently, in the e-identification service it is not possible to identify persons who do not have a Finnish personal identity number, persons who have a substitute ID or estates.

The e-identification service is available 24 hours a day, seven days a week, excluding cut-off times caused by maintenance, updating, etc.

2.4 Security

The service uses SSL/TLS encryption protocol in the HTTP communication between the parties. A third party cannot see or change the data. The service provider's server software must support TLS version 1.2 (*RFC 5246*) or higher. However, the TLS version used in the customer serving endpoints is determined by the properties of the browser used by the customer and downgrade to TLS version 1.1 is allowed in that case. The integrity of the data in the identification request and the identity returned is signed and encrypted with RSA Keys, so the customer who directs the transfer of the identification data cannot change the data without the service provider and Nordea noticing it.

Each party is responsible for the protection, security and correctness of the data and the RSA keys they store. The identifying customer is responsible for safeguarding codes or other identification tools given by Nordea from a third party. The customer is also responsible for keeping his or her identification tools out of reach of outsiders and must ensure that the identification tools are only used when authenticating using identification services provided by Nordea. The customer also recognises the service provider from the identification in the Nordea e-identification service and accepts the transfer of the e-identification.

Nordea

3 Integrity and non-repudiation

Integrity and non-repudiation of the customer identities is based on public key cryptography using RSA key pairs. 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. E-identification service includes following RSA keys.

Key purpose	Description	Issuer
Id Token signing	Id Token is signed with a private key issued by Nordea	Nordea
Id Token encryption	Id Token is encrypted using a public key provided by Service Provider	Service Provider
JWT assertion signing	JWT (*RFC 7519*) Assertion is signed with a private key issued by Service provider	Service Provider

The service provider must provide Nordea a JWKS endpoint for fetching the public key for Id Token encryption and for the JWT Assertion signature validation. All communication regarding key exchange between SP and Nordea must be done using a standard secure communication channel provided by Nordea customer service.

Nordea provides a JWKS endpoint for fetching the public key for Id Token validation. Id Token contains the id of the key, available in the JWKS endpoint, that MUST be used to validate the token signature.

3.1 Key request

GET	{keys-api-path}/keys

Key	Description
kty	Key type.
e	Key value exponent (base64 encoded)
n	Key value modulus (base64 encoded)

kid	Key id.
use	Intended use of the public key Optional Possible values: - sig for signing - enc for encryption

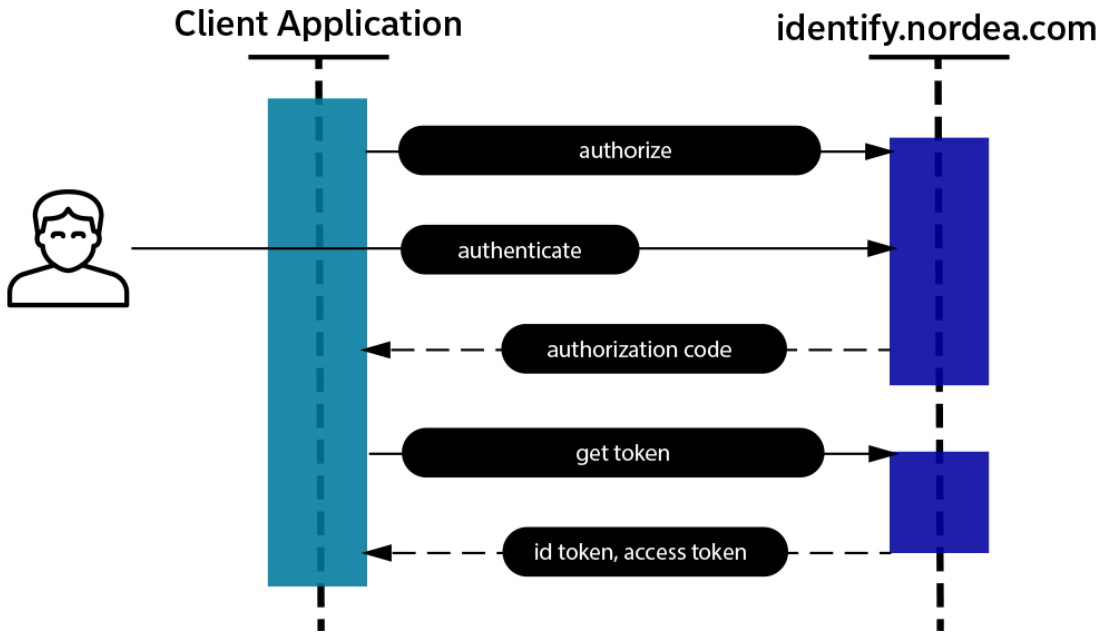
Example

```
{
    "keys": [
        {
            "kty": "RSA",
            "e": "ABCD",
            "n": "…bW/RpKE6s/FB4VnLjMXRgvYUx5ko/ +2gF5ucjnI/S…",
            "kid": "test-key-id"
            "use": "enc"

        }
    ]
}
```

4 E-identification flow

Nordea e-identification API follows Traficom recommendation for Finnish Trust Network - OpenID Connect 1.0 Protocol Profile. It is based on the common OIDC Authorization Code flow defined in OpenID Connect v1.0 protocol (*OpenId Connect (OIDC) specification)* and supports the parameter values defined below. Clients should follow the security recommendations defined in OAuth2 Security Topics.



Basic steps of the E-identification flow are described in the picture below.

Authentication code flow steps:

1. Client prepares and sends an Authentication Request containing the desired request parameters to Authorization Server (identify.nordea.com).
2. Authorization Server Authenticates the End-User.
3. Authorization Server obtains End-User Consent/Authorization.
4. Authorization Server sends the End-User back to the Client with an Authorization Code.
5. Client sends request with Authorization code to Token Endpoint.
6. Client receives a response that contains an Id Token and Access Token in the response body.
7. Client validates the Id Token and retrieves the End-User's identity.

4.1 Authorization request

GET	https://identify.nordea.com

Parameters	
client_id	**REQUIRED**. Identifier of the client initiating the authentication. Obtained during registration process.
redirect_uri	**REQUIRED**. Redirection URI to which the response will be sent. This URI must exactly match one of the redirection URI values for the client pre-registered at Nordea. URI must not contain hashes but can include query parameter.
response_type	**REQUIRED**. OAuth 2.0 Response Type value that determines the authorization processing flow to be used, including what parameters are returned from the endpoints used. Nordea e-identification supports only the Authorization Code Flow and thus this is required to be *code*
state	**REQUIRED**. An opaque value used by the client to maintain state between the request and call-back. The authorization server includes this value when redirecting the user-agent back to the client. The parameter should be used for preventing cross-site request forgery as described in [RFC 6749 Section 10.12] (https://tools.ietf.org/html/rfc6749#section-10.12)
nonce	**REQUIRED**. String value used to associate a client session with an Id Token, and to mitigate replay attacks. The value is passed through unmodified from the Authentication Request to the Id Token. Sufficient entropy must be present in the nonce values used to prevent attackers from guessing values. For implementation notes, see [OIDC specification Section 15.5.2] http://openid.net/specs/openid-connect-core-1_0.html#NonceNotes.
scope	**REQUIRED**. Space separated list of strings to define requested information. Must contain value `openid`. Also `ftn_hetu` scope can be used for retrieving Finnish personal identifier.
acr_values	**REQUIRED**. Requested Level of Assurance (LoA) for end-user. Supported authentication assurance levels: http://ftn.ficora.fi/2017/loa2, http://eidas.europa.eu/LoA/substantial.
login_hint	**OPTIONAL**. Prefills authentication method and user inputs such as user id. Starts authentication flow automatically if all parameters are valid. Format is amr:input_value. At minimum amr is required if this parameter is used. More information about the amr in the Id Token chapter.
ui_locales	**OPTIONAL**. Preferred locale used in authentication flow. Supported languages: Finnish fi, Finnish Swedish sv-FI, English en

Example authorization request with mandatory parameters:

```
https://[auth-server-url]/?client_id=[consumer-
clientid]&response_type=code&scope=openid+ftn_hetu&redirect_uri=[consumer-
redirect-uri]%2Fcode&state=91392088-79c2-4c66-b22f-
47c5cafb1a60&ui_locales=en&nonce=5f060035ad32fe5d770c916a122f86068dc4986d14
c8373724e35b61ed728b5d&acr_values=http%3A%2F%2Fftn.ficora.fi%2F2017%2Floa2
```

4.2 Authorization request responses

4.2.1 User successfully authenticated

Field	Description
code	**REQUIRED**. Authorization code, which can be later exchanged to Id Token.
state	**REQUIRED**. Parameter provided by the service provider in the authentication request.

Example

```
https://[consumer-redirect-uri]?code=[code]&state=91392088-79c2-4c66-b22f-
47c5cafb1a60
```

4.2.2 User authentication failed

Field	Description
error	**REQUIRED**. Error code. `invalid_request`: Invalid or missing request parameters in authorize request. `invalid_scope`: Missing or invalid scope parameter in authorization request. Authorize request must always contain openid scope. `unsupported_response_type`: Response type should always be code. `unauthorized_client`: The client is not authorized to request an authorization code.

state	**REQUIRED**. Parameter from Authentication request.

Example

```
https://[consumer-redirect-uri]?error=invalid_scope&state=2af87311-e5d3-4740-b2e2-bcdd825460a2
```

4.3 Token request

POST	/api/dbf/ca/token-service-v3/oauth/token

Parameters (Content-Type x-www-forl-urlencoded)	
client_id	**REQUIRED**. Identifier of the client initiating the authentication. Obtained during registration process.
redirect_uri	**REQUIRED**. Redirection URI to which the Authorization endpoint response was sent to. Must match with the redirect_uri registered in Nordea for the client.
grant_type	**REQUIRED**. OAuth 2.0 Grant Type value that determines the type of the grant used to exchange the token. Must be set to `authorization_code`.
code	**REQUIRED**. Authorization code to be exchanged for the token. The code is received from a successful user authorization response.
client_assertion	**REQUIRED**. Client assertion to authenticate client. Signed JWT (*RFC 7519*) which must include claims iss, sub, aud, jti, and exp.
client_assertion_type	**REQUIRED**. Only signed JWT (urn:ietf:params:oauth:client-assertion-type:jwt-bearer) is supported.

Example request with mandatory parameters

```
POST /oauth/token HTTP/1.1

Host: [token-service-url]

Content-Type: application/x-www-form-urlencoded

client_id=[consumer-clientid]&code=[code_from_authorization_response]
&redirect_uri=[consumer-redirect-uri]
&grant_type=authorization_code&client_assertion=[client_assertion]
&client_assertion_type=urn:ietf:params:oauth:client-assertion-
type:jwt-bearer
```

4.4 Token request responses

4.4.1 200 Success – Token successfully issued

Name	Description
access_token	An access token to access additional APIs like user-info endpoint of Nordea e-identification. Currently such APIs do not exist.
expires_in	Expiration time of the Access Token in seconds since the response was generated.
token_type	Always set to `Bearer`.
id_token	Id Token. JWT (*RFC 7519*) token containing requested user information.
scope	Scope of the access request.

Example


```
{
  "access_token": "eyJ0dHlwIjoiYWNjZXNzX3Rva2VuIiwidmV…",
  "expires_in": 180,
  "token_type": "Bearer",
  "id_token":"eyJjdHkiOiJKV1QiLCJlbmMiOiJBMTI4R0NNYWxnI…",
  "scope": "openid ftn_hetu"
}
```


4.4.2 400 – Error

Name	Description
error	Error code. Possible values: `invalid_request`, `invalid_client`, `invalid_grant`, `unauthorized_client`, `unsupported_grant_type`, `invalid_scope`
error_description	Human readable description of the error.

Example


```
{
  "error": " unsupported_grant_type",
  "error_description": " The authorization grant type is not
supported by the authorization server."
}
```


4.4.3 Id Token

The Id Token is a security token that contains claims about the authentication of an End-User by an Authorization Server and potentially other requested Claims. The Id Token is represented as a JSON Web Token (RFC 7519). In FTN Id Token is signed (*JSON Web Signature specification*) and encrypted (*JSON Web Encryption specification*).

Id Token provides the means for the service providers to verify the identity of the authenticated user and to share the identity information with the counter parties. Consumers must validate Id Token response as described in OIDC Core 1.0 section 3.1.3.5.

Nordea

Claims included to Id Token depends on the scope value in the authorization request. The openid value must be always present. Optional scope ftn_hetu can be utilized also.

Id token is encrypted using the public RSA key provided by service provider and should be decrypted using the private part of the same key pair. The used key can be identified from the key id (kid) parameter in the JWE header. Id Token is also signed with Nordea's private key and the client application should verify the signature of the issued Id Token with the public key provided by Nordea. Public key can be identified using key id (kid) parameter in the JWS header. Public keys can be retrieved programmatically from the Nordea JWK endpoint. The keys MUST be cached in the service provider side and JWKS endpoint should only be called to refresh the cache.

Supported cryptographic algorithms for JWT protection are following.

Header	Usage	Value	Algorithm
alg	JWS	RS256	RSASSA-PKCS1-v1_5 using SHA-256
alg	JWE	RSA-OAEP	RSAES OAEP using default parameters
enc	JWE	A128GCM	AES GCM using 128-bit key

The Id Token is encrypted JWE with the following header components.

Key	Data type	Allowed values	Description
cty	string	JWT	Content type. Always JWT.
enc	string	A128GCM	The encryption key used to encrypt the JWS. Always A128GCM.
alg	string	RS256	Identifies the cryptographic algorithm used to encrypt the encryption key. Always RSA using SHA-256 hash algorithm.

Key	Data type	Allowed values	Description
kid	string		A hint indicating which RSA key was used to encrypt the encryption key. The value is used to find a suitable private key to decrypt the Id Token.
ver	string		A three-digit (major.minor.patch) version of the Id Token. Follows the semantic versioning principles.

The decrypted Id Token is a JWS with the following header components.

Key	Data type	Allowed values	Description
typ	string	JWT	The type of the token. Always JWT.
alg	string	RS256	Identifies the cryptographic algorithm used to secure the JWS. Always RSA using SHA-256 hash algorithm.
kid	string		A hint indicating which key was used to secure the JWS. The value is used to find a suitable public key to validate the Id Token signature.
ver	string		A three-digit (major.minor.patch) version of the Id Token. Follows the semantic versioning principles.

Nordea

Id Token has following set of claims.

Claim	Data type	Required	Description
jti	string	true	Provides a unique identifier for the JWT.
iss	string	true	Issuer Identifier for the Issuer of the response. The iss value is a case sensitive URL using the https scheme that contains scheme, host, and optionally, port number and path components and no query or fragment components.
sub	string	true	Subject identifier.
aud	array	true	Audience(s) that this Id Token is intended for. It must contain the OAuth 2.0 client_id of the Relying Party (RP) as an audience value.
exp	number	true	Expiration time on or after which the Id Token must 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 1970-01-01T0:0:0Z as measured in UTC until the date/time. See RFC 3339 (*RFC 3339*) for details regarding date/times in general and UTC in particular.
iat	number	true	Time at which the JWT was issued. Its value is a JSON number representing the number of seconds from 1970-01-01T0:0:0Z as measured in UTC until the date/time.
auth_time	number	true	Time when the end-user authentication occurred, number of seconds since the beginning of 1970 UTC.
nonce	string	true	String value used to associate a Client session with an Id Token, and to mitigate replay attacks. The value is passed through unmodified from the Authentication Request to the Id Token. If present in the Id Token, **Clients must verify that the nonce Claim Value is equal to the value of the nonce parameter sent in the Authentication Request.** If present in the

			Authentication Request, Authorization Servers must include a nonce Claim in the Id Token with the Claim Value being the nonce value sent in the Authentication Request. Authorization Servers should perform no other processing on nonce values used. The nonce value is a case sensitive string.
acr	string	true	Authentication Context Class Reference. String specifying an Authentication Context Class Reference value that identifies the Authentication Context Class that the authentication performed satisfied.
nbf	number	false	The nbf (not before) claim identifies the time before which the JWT must not be accepted for processing.
amr	array	false	Authentication Methods References. JSON array of strings that are identifiers for authentication methods used in the authentication. For instance, values might indicate that both password and OTP authentication methods were used. The amr value is an array of case sensitive strings.

Following natural person claims are included to Id Token depending on scope value in authorization request.

Claim	Data type	Required	Description
urn:oid: 1.2.246.21	string	true	HETU, Finnish personal identity code, henkilötunnus `291292-918R`
urn:oid: 2.5.4.4	string	true	FamilyName `Virtanen`
urn:oid: 1.2.246.575.1.14	string	true	FirstNames `Aino Olivia`
urn:oid: 1.3.6.1.5.5.7.9.1	string	true	DateOfBirth (YYYY-MM-DD) `1992-12-29`

5 Example flows

Authorize

Request

```
GET https://[auth-server-url]/?client_id=[consumer-
clientid]&response_type=code&scope=openid+ftn_hetu&redirect_uri=[consumer-
redirect-uri]%2Fcode&state=91392088-79c2-4c66-b22f-
47c5cafb1a60&ui_locales=en&nonce=d6ee88d65252ca77088f538c7eb2f9e0d0d8ec2f19f77
352b1af712104661d18&acr_values=http%3A%2F%2Fftn.ficora.fi%2F2017%2Floa2%2Fcode
&state=91392088-79c2-4c66-b22f-
47c5cafb1a60&ui_locales=en&nonce=d6ee88d65252ca77088f538c7eb2f9e0d0d8ec2f19f77
352b1af712104661d18&acr_values=http%3A%2F%2Fftn.ficora.fi%2F2017%2Floa2
```

Response

```
https://[consumer-redirect-uri]?code=[code]&state=91392088-79c2-4c66-b22f-
47c5cafb1a60
```

Exchange Token

Request

```
POST [token-end-point] HTTP/1.1

Host: [token-service-host]

Content-Type: application/x-www-form-urlencoded

grant_type=authorization_code&code=[code]&client_id=[consumer-
clientid]&redirect_uri=[consumer-redirect-
uri]&client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-assertion-
type%3Ajwt-bearer&client_assertion=[client-assertion]
```

Response

```
{"access_token":[access-token],
"expires_in":180,"token_type":"Bearer","id_token":[id-token],"scope":"openid
ftn_hetu"}
```

6 Registration process

Agreement

To be able to use the service, the service provider must first sign an e-identification agreement with Nordea. The existing e-identification agreements will be updated to new ones. Your Nordea contact person will be contacting you about the matter. Integration towards the service can be started even without the agreement. For more information about the process, please contact your Nordea contact person or Nordea Business Centre.

Configuration

Service provider must also provide technical configuration data such as preferred identification methods, redirect addresses and RSA public keys. These will be used for creating a client specific configuration. When client configuration is completed, Nordea will provide a dedicated client id for the Service Provider. In addition, Nordea will provide a JSON Web Key Set (*RFC 7517*) URL defining the RSA public keys supported by Nordea to validate the Id Token.

Nordea

7 References

FTN OIDC Profile - Finnish Trust Network OpenID Connect 1.0 Protocol Profile version 1.0 213/2018 S 2018-01-26 (https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ftn_oidc_profile_v1.0_ficora_rec_213_2018_s.pdf)

FICORA Regulation 72 Notes – Explanatory notes to Regulation 72 2016-12-7 (Regulation 72 on Electronic Identification and Trust Services (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

RFC 3339 - Date and Time on the Internet: Timestamps, https://www.ietf.org/rfc/rfc3339.txt

RFC 5246 - The Transport Layer Security (TLS) Protocol, https://tools.ietf.org/html/rfc5246

8 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.