Service description of Handelsbanken's identification service

Version 0.3

10 October 2023

Table of Contents

Versions

0.1	30 October 2018	First version
0.2	9 December 2018	- Section 6: Updated image 3 - Section 6: Changed production address (tunnistus.handelsbanken.fi) - Section 6: "The identification request is always signed by the identification brokering service or with the private keys of the transaction service ~~and it can also be encrypted with the public keys of the identification service~~." - Section 7: Added Samlink's technical support contact information
2.0	10 October 2023	Updated to reflect changes and reforms of Traficom Regulation M72B/2022 Paragraph 2: Added Entity Statement and Signed JWKS Paragraph 4: Added Entity Statement Processing Paragraph 5: Key exchange updated to match changes

1. GENERAL

When identification means issued by the bank are used for identification in services other than the bank's own electronic services, they are subject to the requirements of strong electronic identification.

These requirements are defined in the Act on Strong Electronic Identification and Electronic Trust Services and the regulation issued by the Finnish Transport and Communications Agency (Traficom) based on it. The Finnish Transport and Communications Agency Traficom monitors compliance with the requirements.

Using Handelsbanken's identification service, other identification service providers and transaction services can transmit and receive strong electronic identification events made through Handelsbanken's identification means.

2. KEY TERMS

Identification means holder

A natural person who possesses the identification means required for strong electronic identification.

Transaction service

A service in which the holder of the identification means is identified. The transaction service identifies the identification means holder either by means of an identification brokering service or through an identification event received directly from the identification means provider.

Identification brokering service

A service that transmits identification events based on strong electronic identification made through different identification means to transaction services. The identification brokering service provider must be part of the Strong Electronic Identification Trust Network.

Identification means provider

A party that offers a means for strong electronic identification to a natural person.

The identification means provider holds information about the identity of the identification means holder. In the service described in this service description, Handelsbanken is the identification means provider.

Finnish Transport and Communications Agency (Traficom)

Is the supervising authority, ensuring that identification service providers comply with the obligations set for them.

Finnish Trust Network (FTN)

A network of identification service providers (identification means providers and identification brokering service providers) registered with Traficom, the goal of which is to ensure the safety of electronic identification in cooperation between the parties involved.

Entity Statement
A signed JWT file containing, e.g., a SIGNED JWKS URI address, where the Signed JWKS file can be retrieved, as well as the public signature keys of the JWKS file in question.

https://openid.net/specs/openid-connect-federation-1_0.html#section-3.1

Signed JWKS
A signed JWT file containing the JWK Set of the identification means provider. The JWT in question has been signed with a key inside the entity statement.
https://openid.net/specs/openid-connect-federation-1_0.html#section-4.1

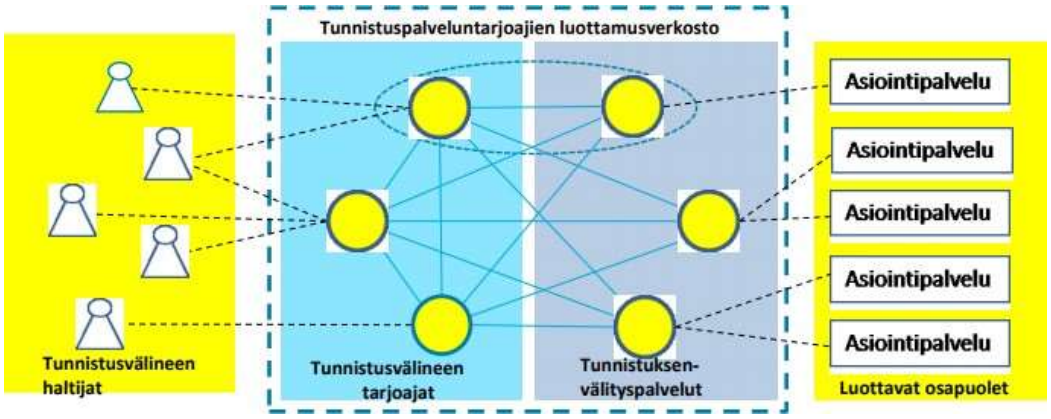

Figure 1. Trust network Source: Traficom

Tunnistuspalvelutarjoajien luottamusverkosto - Identification service providers' trust network
Asiointipalvelu - Transaction service
Tunnistusvälineen haltijat - Identification means holders
Tunnistusvälineen tarjoajat - Identification means providers
Tunnistuksenvälityspalvelut - Identification brokering services
Luottavat osapuolet - Trusting parties

3. HANDELSBANKEN'S IDENTIFICATION SERVICE

The identification service verifies the customer's identity for identification brokering services or transaction services. The use of the identification service requires an agreement with Handelsbanken.

Handelsbanken's identification service is produced by Samlink Ltd.

The identification service is based on Traficom's OpenID Connect -based Trust Network description. It is intended for electronic identification brokering service providers as well as transaction services providers.

4. FUNCTIONAL DESCRIPTION OF THE SERVICE

This section describes how to deploy the identification

service. Service deployment phases:

- entering into a service agreement with Handelsbanken
- exchanging entity statement files via e-mail
- configuring the service to the systems of the identification brokering service or

transaction service

The identification service is used in accordance with the OpenID Connect standard.

5. SERVICE DEPLOYMENT

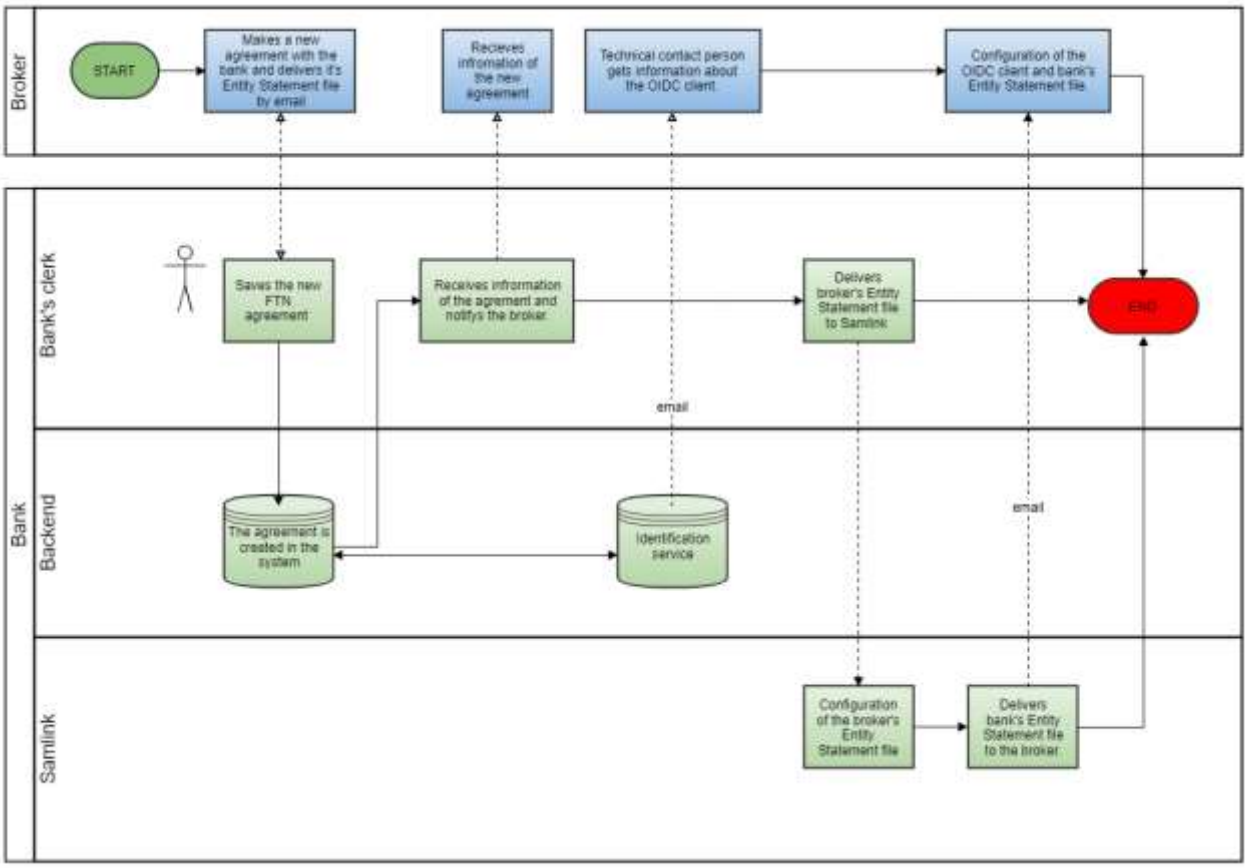

Figure 2. Service deployment

SERVICE AGREEMENT WITH HANDELSBANKEN

In the first stage, a Handelsbanken official enters into an agreement on an identification service with an identification brokering service or transaction service.

In connection with the agreement, the other contracting party is also provided with an authentication code related to the exchange of keys.

The agreement initiates a key exchange process, where the public keys required for OpenID Connect communication are exchanged.

EXCHANGE OF THE OPENID CONNECT ENCRYPTION AND SIGNATURE KEYS

The exchange of keys is based on public JWKS files that contain the public signature and encryption keys of both parties. The JWKS files are in JWT format and are signed with an identification brokering service's / bank's entity statement file.

The entity statement file of the identification brokering service or transaction service is handed over to Handelsbanken in connection with the conclusion of the agreement. Handelsbanken sends its own entity statement by e-mail to the identification brokering service. A Handelsbanken employee identifies a representative of an identification brokering service or transaction service.

CONFIGURING THE SERVICE IN IDENTIFICATION BROKERING SERVICE AND TRANSACTION SERVICE SYSTEMS

The identification brokering service or transaction service receives OpenID Connect configuration data related to the use of the identification service via secure email, similarly to the keys stated in the previous section.

This data includes an OpenID Connect Client ID, the URIs of invitation interfaces used in the authentication

process and the unsigned JWKS URI containing Handelsbanken's public keys. Broker should use the signed JWKS URI defined in the bank's entity statement.

The identification brokering service or transaction service configures the aforementioned information into the system of the identification brokering service or transaction service. The system must follow the OpenID Connection standard.

TESTING OF THE SERVICE

The identification brokering service or transaction service which deploys the service obtains instructions on how to test the identification service via secure email received when entering into an agreement.

6. USING THE SERVICE

The progress of the OpenID Connect authentication process is described below.

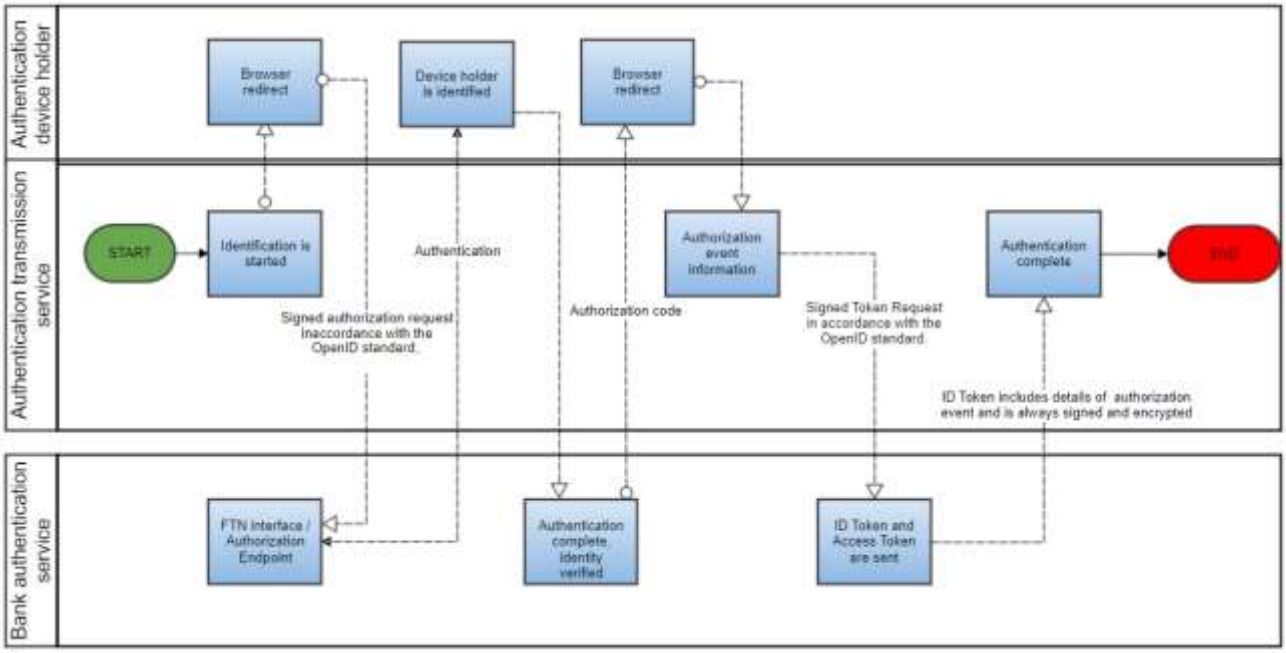

Figure 3. Authentication

SERVICE MESSAGES AND THE DATA THEY CONTAIN

The OpenID Connect standard adds an identity authentication layer on top of the OAuth 2.0 protocol. OAuth 2.0 offers services related to authorisations.

The OpenID Connect authentication process is carried out through a simple HTTPS REST interface. A full description of the OpenID Connect protocol is available on the following website:

https://openid.net/connect/

In its recommendation, Traficom defines how the OpenID Connect standard applies to trust networks. Traficom's document defines the trust network's OpenID Connect profile and the encryption algorithms and keys used in messaging.

The OpenID Connect authentication process consists of three phases:

1. An authorisation request to start the authentication process
2. Authentication of the identification means holder
3. A token request to obtain authentication data

The following sections describe the authorisation and token request messages sent in the first and third phases.

OIDC AUTHORISATION REQUEST

An HTTPS REST authorisation request message in accordance with the OpenID Connect protocol is sent to the authorisation endpoint:

https://tunnistus.handelsbanken.fi/oxauth/restv1/authorize

The identification brokering service or transaction service redirects the identification means holder's browser to open the page in accordance with the authorisation endpoint using the parameters given. When this URI is opened, the identification means holder's authentication process starts.

Once the authentication process has been completed successfully between the identification means holder and the identification service, the identification service redirects the identification means holder's browser to the redirect URI of the identification brokering service or transaction service.
This redirection invitation includes the authorisation code granted by the identification service as a parameter. Using this code, the identification brokering service or transaction service can retrieve claims from the identification service using the token request described in the following section.

The authentication request is always signed with the private keys of the identification brokering service or transaction service.

AUTHENTICATION REQUEST PARAMETERS	
request	Message signature. The signature contains two objects: JWTClaimsSet and JWSHeader. The signature is made using private keys that correspond to the public keys of the JWKS URI given when entering into the trust network's identification service agreement.
ui_locales	The language requested from the service.
ftn_spname	The name of the identification service provider or transaction service.
scope	The OpenID Connect scope defined by Traficom for the trust network (= openid + ftn_hetu).
acr_values	Traficom-defined Level of Assurance Regulation for the Trust Network (http://ftn.ficora.fi/2017/loa2)

response_type	The OIDC authorisation flow defined by Traficom for the trust network (= code).
redirect_uri	The redirect URI returned to after a successful authentication. This must correspond to the URI used when entering into the trust network's identification service agreement.
prompt	This defines whether the identification means holder requires re-authentication or re-authorisation. If the setting is 'login', re-authentication is required.
client_id	The OIDC Client ID which the identification service provider or transaction service receives via secure email after entering into the trust network's identification service agreement.
nonce	A character set which combines the session and authorisation request to prevent any replay attacks.
state	A value that connects a request and response together.

Example of an authorisation request:

https://tunnistus.handelsbanken.fi/oxauth/restv1/authorize?request=eyJraWQiOiIxIiwidHlwIjoiSldUIiwiYWxnIjoiUlMyNTYifQ.eyJpc3MiOiJAIUYzNjEuNDU4MC4xMDZELjA1NzEhMDAwMSE5M0JGLkY1OEUhMDAwOCE3OEUzLjQ3MzYuMTlDNC5BRUYwIiwicmVzcG9uc2VfdHlwZSI6ImNvZGUiLCJub25jZSI6IkpuTXRLZGtSLVlTd3pZVnRtVzNkSUtKZnAtMUgtLTRvbldoNHZLNGRRbTQiLCJjbGllbnRfaWQiOiJAIUYzNjEuNDU4MC4xMDZELjA1NzEhMDAwMSE5M0JGLkY1OEUhMDAwOCE3OEUzLjQ3MzYuMTlDNC5BRUYwIiwiYXVkIjoiaHR0cHM6XC9cL2ktc3AtaWRwLnNhbWluZXQuZmkiLCJ1aV9sb2NhbGVzIjoiW2ZpXSIsImZ0bl9zcG5hbWUiOiIiLCJzY29wZSI6Im9wZW5pZCBmdG5faGV0dSIsImFjcl92YWx1ZXMiOiJbaHR0cDpcL1wvZnRuLmZpY29yYS5maVwvMjAxN1wvbG9hMl0iLCJyZWRpcmVjdF91cmkiOiJodHRwczpcL1wvaS1taXNjLnNhbWluZXQuZmlcL2dsdXUtYnJva2VyLWNsaWVudFwvdG9rZW4iLCJzdGF0ZSI6IldwdGZaUlBfd3g2Z0VSSWZtaFpxa1AtN0RDSTFBV3RRTjZzaW1zMXk0WlEiLCJleHAiOjE1NDI2MTg5ODMsInByb21wdCI6ImxvZ2luIn0.uqOEJZ49cOCnwU0paQfBjOQvdx7zLmivcm1-9rKztHNbF9GH-PbSOlMPZX2z3SQjIa6dADJRI8WAk37-QQPX6_q9wHwOasCtrUIK00_6LQW8fRdi92JKGe76lLuZZK9XSantsXdE0td_czzRqJYpgV79SbYqoz8hf17SyS_JlMJTNQuloDO5T2m12qTQRiI2gSR2UAjKBJNFGka49Zo5DscMpWReaeiJ4-jBuV0cGbR1DVBssSZjQ6SEp6W8TL3Nh8ELZePrr5Dwn9NeL8DbjTKulZF10vAM8q1AUKsionmU3MU5DvEM4ER-zq6ocNlCX58IaK4myPYAqYm9NTA1vw&ui_locales=fi&ftn_spname=&scope=openid+ftn_hetu&acr_values=http%3A%2F%2Fftn.ficora.fi%2F2017%2Floa2&response_type=code&redirect_uri=https%3A%2F%2Fi-misc.saminet.fi%2Fgluu-broker-client%2Ftoken&state=WptfZRP_wx6gERIfmhZqkP-7DCI1AWtQN6sims1y4ZQ&nonce=JnMtKdkR-YSwzYVtmW3dIKJfp-1H--4onWh4vK4dQm4&prompt=login&client_id=%40%21F361.4580.106D.0571%210001%2193BF.F58E%210008%2178E3.4736.19C4.AEF0

OIDC TOKEN REQUEST

The identification brokering service or transaction service sends a token request message in accordance with the OpenID Connect protocol to the token endpoint as a direct HTTPS REST message:

https://tunnistus.handelsbanken.fi/oxauth/restv1/token

The message includes the authorisation code received in response to the authorisation request as a parameter, and the ID token and access token are received as a response.

The messages are sent in accordance with the JSON Web Token standard (IETF RFC 7519). JWT defines the JSON data transfer method between two parties.

The ID token is a signed and encrypted base64-coded JSON Web Encryption (JWE) message which includes claims of the identification means holder.

Structure of the signed and encrypted ID token:

JOSE HEADER	JWE ENCRYPTED KEY	INITIALISATION VECTOR	CIPHERTEXT	AUTHENTICATION TAG

Each element is separated by a dot and is base64-coded.
JOSE stands for Javascript Object Signing and Encryption and refers to the IETF working group which defines secure data transfers in the JWT standard.

JOSE HEADER includes data related to the message signature and encryption.

JWE ENCRYPTED KEY includes an encrypted symmetrical key for decoding the content of the actual message.

INITIALISATION VECTOR is a random set of numbers required by certain encryption algorithms used.

CIPHERTEXT includes the content of the encrypted message.

AUTHENTICATION TAG is a value which is created during the encryption process and ensures the integrity of data.

The received ID token must always be validated in accordance with the OpenID Connect specification.

The authorisation request is always signed with the private keys of the identification brokering service or transaction service.

The response to the token request will always be signed using the private keys of the identification service and encrypted using the public keys of the identification brokering service or transaction service.

TOKEN REQUEST PARAMETERS	
grant_type	Token type (= authorisation code).
code	Previously received authorisation code in response to an authorisation request.
redirect_uri	The redirect URI returned to after a successful token request. This must correspond to the URI used when entering into the trust network's identification service agreement and when carrying out the authorisation request.

RECEIVED IDENTIFICATION TOKEN PARAMETERS (ID token content, payload)	
iss	Issuer identifier.
sub	A unique identifier which connects the issuer and end user (subject identifier).
aud	The party for which this ID code was created (audience). The OIDC Client ID of the identification brokering service or transaction service.
exp	The time when the ID token expires.
iat	The time when the ID token was created.
auth_time	The time when the identification means holder was authenticated.
nonce	A character set which combines the session and ID token to prevent any replay attacks.
acr	The level of assurance defined by Traficom for the trust network (= loa2).
amr	Authentication method.
+ CLAIMS	Claims defined in the token request's scope parameter (ftn_scope in the trust network).

7. CONTINUITY, INCIDENT MANAGEMENT AND HANDLING OF IRREGULAR SITUATIONS

The service operates 24/7, with the exception of planned maintenance outages, which will be announced on the Handelsbanken website.

If you encounter any problems, please contact Handelsbanken's customer support.

Customer service for corporate payment services

Service hours: 8:00 am – 5:00 pm on business days
Tel.: +358 10 444 2545
E-mail: finhelp@handelsbanken.fi

Samlink Ltd.'s technical support directly: tekninentuki@samlink.fi