BANK AUTHENTICATION SERVICE
SERVICE DESCRIPTION

POP Pankki

1.3.2019

Version 1.0

Table of contents

General 3

Key terms 3

Bank authentication service 4

Functional description of the service 4

Service deployment 5

Testing the deployed service 6

Using the service 6

Continuity, incident management and processing irregular situations 10

General

When online banking identifiers are used for authentication in services other than those of the bank that provided the identifiers, requirements set for strong electronic identification apply to them. These requirements are defined in the Act on Strong Electronic Identification and Electronic Signatures and the regulation issued by the Finnish Communications Regulatory Authority (FICORA) based on it. FICORA monitors that these requirements are complied with.
The requirements set out in the act and FICORA's regulation are in line with the EU regulation on strong electronic identification methods.

The service fulfils FICORA's regulation no. 72 on electronic identification.
Strong electronic identification and the transmission of strong electronic authentication can be offered by service providers approved by FICORA. A list of approved service providers is available in a register maintained by FICORA.

Using the bank authentication service, other providers of authentication services can transmit and receive strong electronic identification events made using an authentication device of a bank (*enter name of the bank here*).

Key terms

Authentication device holder

A natural person who possesses the authentication device required for strong electronic identification, such as an authentication code app.

Transaction service

A service in which the authentication device holder is identified. The transaction service authenticates the user using the authentication transmission service or directly using the authentication device provider.
For example, the Social Insurance Institution of Finland and online shops are transaction services.

Authentication transmission service

A service that transmits authentication events based on strong electronic identification made using different authentication devices to transaction services.

Authentication device provider

A party that offers a device for strong electronic authentication.
The authentication device provider holds information about the identity of the authentication device holder.

FICORA

The supervising authority which ensures that authentication service providers comply with the obligations set for them.

Trust network

A network of authentication service providers (authentication device providers and authentication transmission service providers) registered with FICORA, the goal of which is to ensure the safety of electronic identification in cooperation between the parties involved.

Trust network

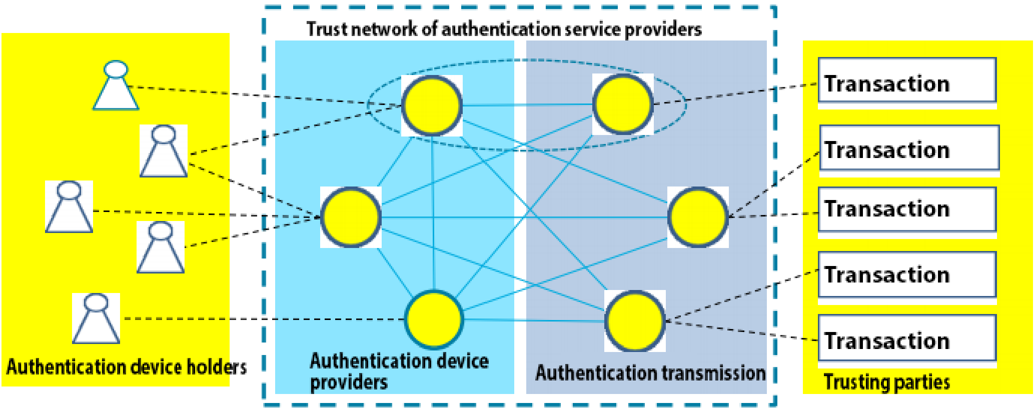
Trust network of authentication service providers
Authentication device holders
Authentication device providers
Authentication transmission
Transaction
Transaction
Transaction
Transaction
Transaction
Trusting parties

Figure 1. Trust network Source: FICORA

Bank authentication service

The authentication service verifies the customer's identity for authentication transmission services or transaction services.
The bank authentication service is produced by Samlink Ltd.

The authentication service is based on an OpenID Connect-based trust network protocol, and it is intended for electronic authentication transmission service providers and transaction service producers.

Functional description of the service

This section describes how the authentication service is deployed and used.
Service deployment phases:
- Entering into a service agreement with the bank
- Exchanging public signature and encryption keys
- Configuring the service in authentication transmission service and transaction service systems

The authentication service is used in accordance with the OpenID Connect standard as described below.

Service deployment

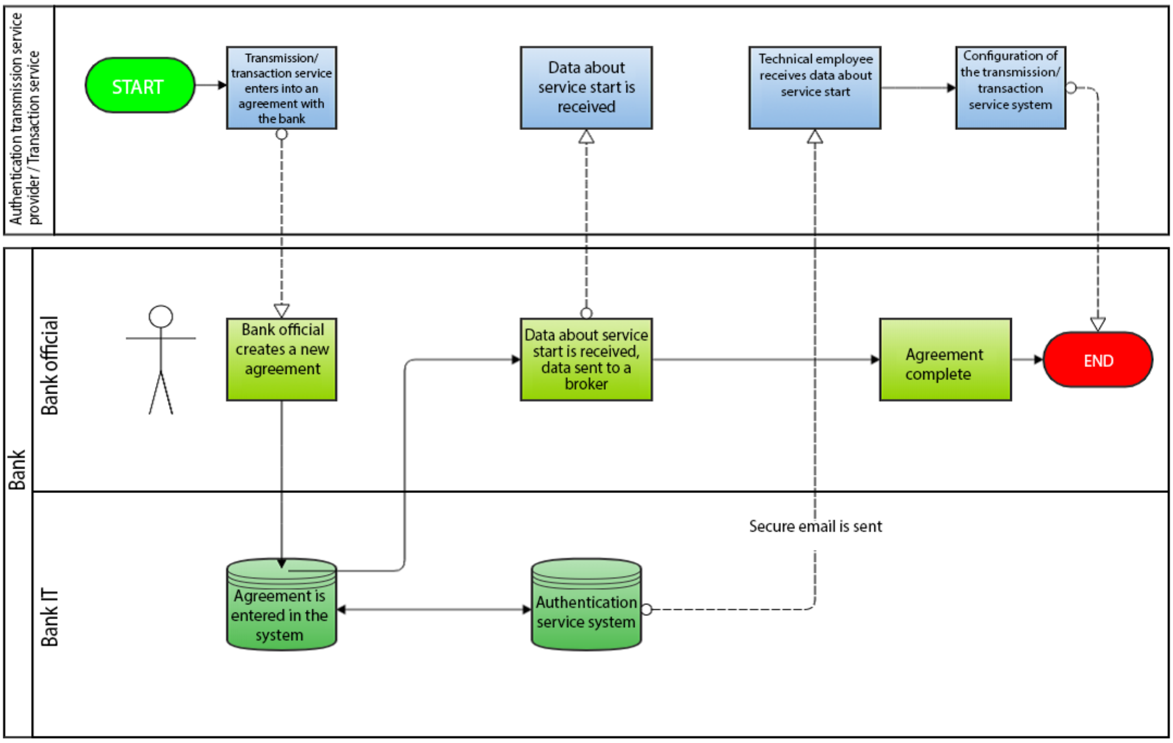
Authentication transmission service provider / Transaction service
START
Transmission/ transaction service enters into an agreement with the bank
Data about service start is received
Technical employee receives data about service start
Configuration of the transmission/ transaction service system
Bank
Bank official
Bank official creates a new agreement
Data about service start is received, data sent to a broker
Agreement complete
END
Bank IT
Secure email is sent
Agreement is entered in the system
Authentication service system

Figure 2. Service deployment

Entering into a service agreement with the bank

In the first phase, a bank official authenticates the other contracting party.
After the authentication, an agreement is created in the bank's system.
Next, the agreement is signed, after which it is sent to the other contracting party. The other contracting party is also provided with an authentication code for the exchange of keys.
Once the agreement has been made, the key exchange process is activated for the exchange of the public keys required for OpenID Connect messaging.

Exchanging OpenID Connect signature and encryption keys

The exchange of keys is based on public JWKS URIs that contain the public signature and encryption keys of both parties.

The JWKS URI of the authentication transmission service or transaction service is given to the bank when entering into an agreement. A bank official identifies the representative of the authentication transmission service or transaction service and enters the URI in the agreement system.

The bank's JWKS URI is given to the authentication transmission service or transaction service via secure email sent after entering into the agreement. The representative of the authentication transmission service or transaction service receives a notification of the secure email via regular email. The notification includes a link to a web page, on which the message can be read. In addition, a code to read the actual message is sent to the recipient as a text message. The message includes basic information about service deployment, including the JWKS URI.

This process verifies the origin of JWKS URIs and keys.

Configuring the service in authentication transmission service and transaction service systems

The authentication transmission service or transaction service receives OpenID Connect configuration data related to the use of the authentication 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 JWKS URI containing the bank's public keys.

This data is configured in the authentication transmission service or transaction service system. The system must follow the OpenID Connection standard in the authentication process.

Testing the deployed service

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

Using the service

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

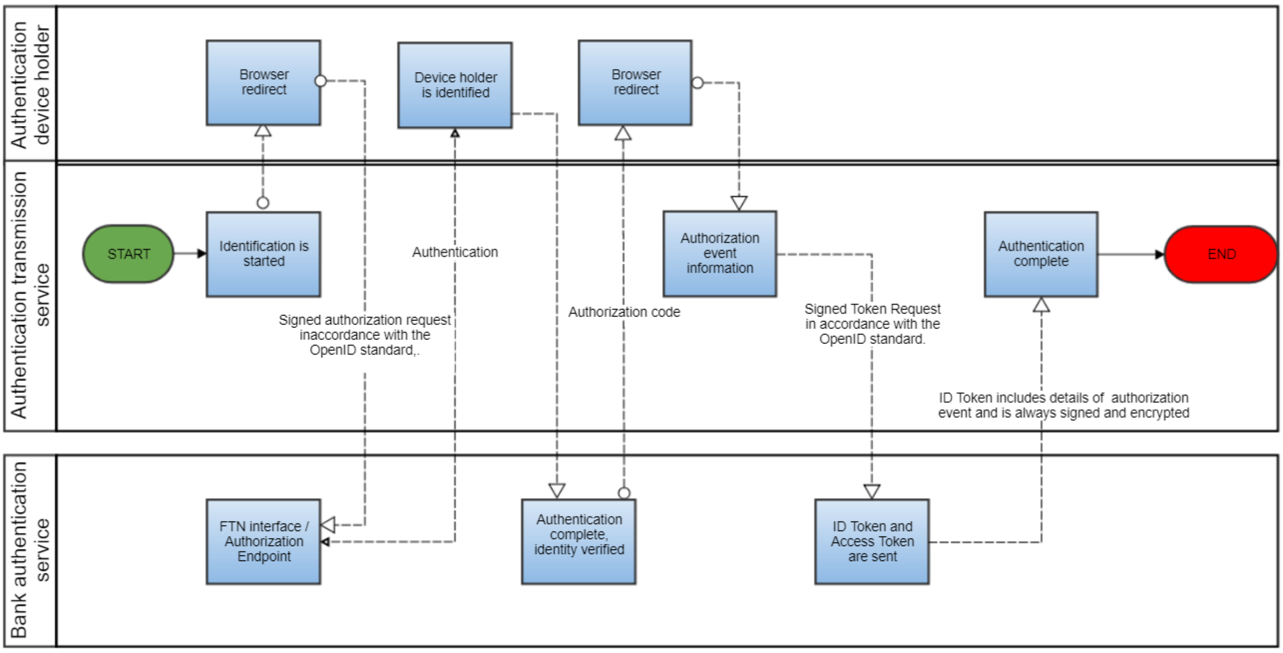
Authentication device holder
Authentication transmission service
Bank authentication service
Browser redirect
Device holder is identified
Browser redirect
START
Identification is started
Authentication
Authorization event information
Authentication complete
END
Signed authorization request inaccordance with the OpenID standard,.
Authorization code
Signed Token Request in accordance with the OpenID standard.
ID Token includes details of authorization event and is always signed and encrypted
FTN interface / Authorization Endpoint
Authentication complete, identity verified
ID Token and Access Token are sent

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 at the following website:

https://openid.net/connect/

In its recommendation, FICORA defines how the OpenID Connect standard applies to trust networks. FICORA'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 authentication device 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.poppankki.fi/oxauth/restv1/authorize

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

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

The authorisation request is always signed using the private keys of the authentication transmission service or transaction service.

An authorisation sent to the redirect URI will always be signed using the private keys of the authentication service and encrypted using the public keys of the authentication transmission 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 authentication service agreement.
ui_locales	The language requested from the service.
ftn_spname	The name of the authentication service provider or transaction service.
scope	The OpenID Connect scope defined by FICORA for the trust network (= openid + ftn_hetu).

acr_values	The level of assurance defined by FICORA for the trust network (= loa2).
response_type	The OIDC authorisation flow defined by FICORA 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 authentication service agreement.
prompt	This defines whether the authentication device holder requires re-authentication or re-authorisation. If the setting is ‘login’, re-authentication is required.
client_id	The OIDC Client ID which the authentication service provider or transaction service receives via secure email after entering into the trust network’s authentication 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.poppankki.fi/oxauth/restv1/authorize?request=eyJraWQiOiIxIiwidHlwIjoiSldUIiwiYWxnIjoiUlMyNTYifQ.eyJpc3MiOiJAIUYzNjEuNDU4MC4xMDZELjA1NzEhMDAwMSE5M0JGLkY1OEUhMDAwOCFDNjNELkVGQ0EuRERDNC4zMDc1IiwicmVzcG9uc2VfdHlwZSI6ImNvZGUiLCJub25jZSI6Ik40Q3pvMTlOUGVLcU9CWUtQYm92Sk90X3BoRzAtYUV6RWVvXzUteHNxcGciLCJjbGllbnRfaWQiOiJAIUYzNjEuNDU4MC4xMDZELjA1NzEhMDAwMSE5M0JGLkY1OEUhMDAwOCFDNjNELkVGQ0EuRERDNC4zMDc1IiwiYXVkIjoiaHR0cHM6XC9cL2ktc3AtaWRwLnNhbWluZXQuZmkiLCJ1aV9sb2NhbGVzIjoiW2ZpXSIsImZ0bl9zcG5hbWUiOiJUZXN0aWthdXBwYSIsInNjb3BlIjoib3BlbmlkIGZ0bl9oZXR1IiwiYWNyX3ZhbHVlcyI6Iltsb2EyXSIsInJlZGlyZWN0X3VyaSI6Imh0dHBzOlwvXC9pLW1pc2Muc2FtaW5ldC5maVwvZ2x1dS1icm9rZXItY2xpZW50XC90b2tlbiIsInN0YXRlIjoiTXhUZVBZMnFrZzB2WVJtcUYzVUdtUnRIWTFWSEktdzd6S3dwSFNydURhOCIsImV4cCI6MTUzNzE4NDM3MywicHJvbXB0IjoibG9naW4ifQ.A5iEDPaQ9XR1jZ3XAPTJpAAgTHnKsGVPR2Gi7Ag_Uz1K8bbEPrbXEN4cs4bc85iQaf6OFsOzSnZl82NcGKBkUL35DzPVbwlwyuTnlSMx4ripp1a45RaaBvQil6lMHWnpvWt7tNnngFmiKQg91iZAQqpUZVlHh6VaVic9pBy0qkXRNFpID79oBK3okoaO3S7DiiL9o19g0caUR_CWJ7DNcsJywAqynsrs36ESzFYn5YC_7cFVdAEx4DbB7G3shJjQQ-BLFNBpTDTrrnyTYNONzBZPNe-bE396GWRT5yOpqzqlSHOWdBPnMM1iZT-rq9W1Q9Uw4NcNUnrWEPfWV6SNSA&ui_locales=fi&ftn_xxname=BrokerOy&scope=openid+ftn_hetu&acr_values=loa2&response_type=code&redirect_uri= https%3A%2F%2Fwww.broker.comi%2Fbroker-oidc-client%2Ftoken&state=MxTePY2qkg0vYRmqF3UGmRtHY1VHI-w7zKwpHSruDa8&nonce=N4Czo19NPeKqOBYKPbovJOt_phG0-aEzEeo_5-xsqpg&prompt=login&client_id=%40%23F361.4580.106D.0171%210001%2163BF.F58E%210558%21C67D.EFCA.DDC4.3075

OIDC token request

The authentication transmission 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.poppankki.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 authentication device holder.

Structure of the signed and encrypted ID token:

JOSE HEADER	JWE ENCRYPTED KEY	INITIALIZATION 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 token request is always signed using the private keys of the authentication transmission service or transaction service.

The response to the token request will always be signed using the private keys of the authentication service and encrypted using the public keys of the authentication transmission 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 authentication service agreement and when carrying out the authorisation request.

PARAMETERS OF A RECEIVED ID TOKEN (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 authentication transmission service or transaction service.
exp	The time when the ID token’s expires.
iat	The time when the ID token was created.
auth_time	The time when the authentication device 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 FICORA for the trust network (= loa2).
amr	Authentication method.
+ CLAIMS	Claims defined in the token request’s scope parameter (ftn_scope in the trust network).

Continuity, incident management and processing irregular situations

The service operates 24/7, apart from planned service breaks that will be announced on the bank’s website.

If there are any problems, please contact Samlink service desk at +358 100 4752 or teknінentuki@samlink.fi.

Attachments

Samlink Finnish Trust Network OIDC security key and data exchange process
between brokers and identity providers