SERVICE DESCRIPTION FOR IDENTIFICATION SERVICE OIDC

SERVICE DESCRIPTION AND APPLICATION INSTRUCTIONS

29.6.2022

CONTENTS

1 General 3

2 General description 3

3 Agreements 4

4 S-Bank's button used in the identification service 4

5 Exchanging OpenID Connect encryption and signature keys 4

6 Configuring the service with the systems of the identification transmission service or transaction service 4

7 Identification request (OIDC authorisation request) 5

8 Authorisation request (OIDC token request) 5

9 Customer information 5

10 Testing the identification service 5

11 Exceptional situations 5

12 Advice and technical support 6

13 Links 6

1 GENERAL

This service description specifies the requirements for the service provider to take the identification service into use and describes the records related to the implementation of the identification service. In S-Bank's identification service, the bank reliably identifies customers using the electronic service on behalf of the service provider. The identification service has been implemented in line with the trust network protocol determined by the Ministry of Transport and Communications. The protocol is based on the OpenID Connect protocol and is intended for providers of electronic identification transmission services and providers of transaction services. The identification service interface has been implemented in line with Section 12a, Subsection 2 of the Act on Strong Electronic Identification and Electronic Signatures (617/2009) and the OpenID Connect 1.0 interface recommendation issued by the Ministry of Transport and Communications.

2 GENERAL DESCRIPTION

The identifier issued by S-Bank is unique and tied to both the service transaction provided by the service provider and the customer. The customer is identified using the same online banking codes that the customer uses when using S-Bank's own services. If a service provider needs to identify a customer, the service provider sends an identification request to the customer, who is then transferred to S-Bank's identification service by pressing the bank's identification button.

The service provider's identification request is forwarded from the customer to S-Bank's identification service, which sends a reply message to the customer after the customer has been identified. The customer checks the information included in the reply message and returns to the service provider's service once they have confirmed the information. The customer may cancel or reject the identification event either before identification or after checking the reply message.

If the customer aborts the identification event, their information is not forwarded to the service provider.

The identification data transmitted in the identification service can be also be used in the formation of an electronic signature, if so agreed between the customer being identified and the service provider. However, S-Bank will only identify the customer in the manner described in this service description and is not responsible for the validity or content of any legal transaction between the customer and the service provider.

The identification service is available 24 hours a day, seven days a week, excluding any downtime due to maintenance, updates or similar reasons.

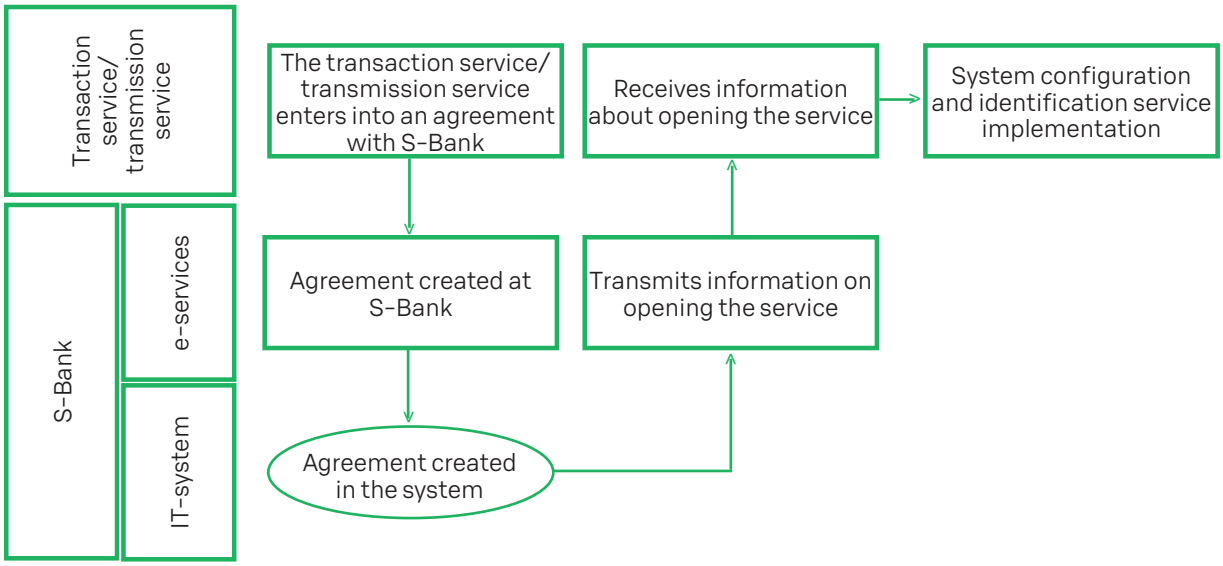
When using online banking codes for identification in services other than S-Bank's services, such services are subject to the requirements for strong electronic identification in line with the Act on Strong Electronic Identification and Electronic Trust Services and regulations issued by the Ministry of Transport and Communications based on the Act. The Ministry of Transport and Communications is responsible for monitoring compliance with the Act.

Requirements for taking the service into use:
1) Entering into a service agreement with S-Bank
2) Exchanging public signature and encryption keys
3) Configuring the service with the systems of the identification transmission service or transaction service

The identification service is taken into use in line with the OpenID Connect standard.

OpenID Connect identification takes place in stages:
1. Identification request to start the identification process
2. Identification of the holder of the identification medium
3. Authorisation request to receive identification information

Figure 1. Taking the identification service into use



The OpenID Connect standard is used to add an identity onto the OAuth 2.0 protocol. The OAuth 2.0 protocol provides services related to authorisation. The OpenID Connect identification takes place through the HTTPS REST interface.

More information on the configuration of the technical interface is available at e-palvelut@s-pankki.fi

3 AGREEMENTS

The service provider must sign a written agreement with S-Bank about the use of the identification service. The service provider's information is registered at the bank, and encryption and signature keys are sent via encrypted email to the contact person specified in the agreement.

The service provider is responsible for ensuring that it has grounds for the processing of people's names, dates of birth and personal identity codes in accordance with the EU General Data Protection Regulation (GDPR).

The service provider must inform S-Bank if any changes are made to its service or information. S-Bank will supplement the agreement with the amended information, if necessary.

4 S-BANK'S BUTTON USED IN THE IDENTIFICATION SERVICE

In the service provider's online service, the use of the identification service must be expressed with S-Bank's online service logo, which must be clearly visible. This logo is used as the function button.

The image file for S-Bank's identification service button can be downloaded from S-Bank's website. The size or colours of the button must not be changed, recreated or redesigned. The button image must not be used for any other purpose than that agreed upon between the service provider and S-Bank.

Within S-Bank, the name of the service is 'identification service' (tunnistuspalvelu or identifieringstjänst). S-Bank's name must not be edited or split across more than one line.

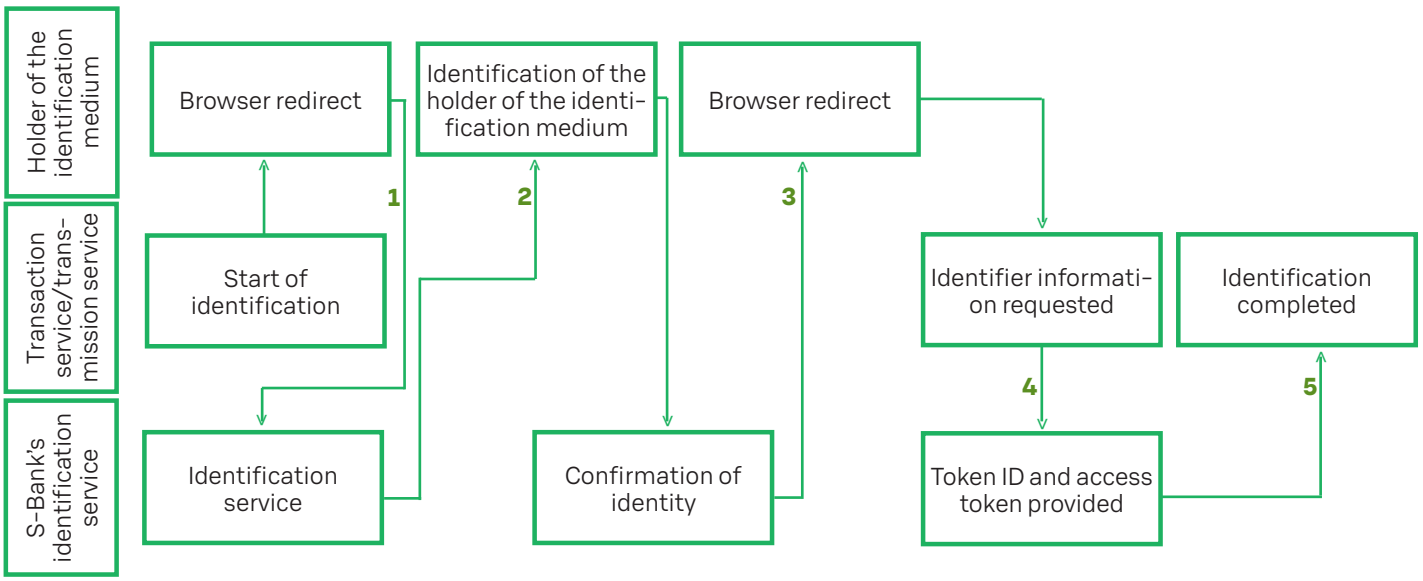
5 EXCHANGING OPENID CONNECT ENCRYPTION AND SIGNATURE KEYS

The service provider must create an encryption key and send the public key in the PEM format via an encrypted email to S-Bank. Communication with S-Bank takes place via the email address e-palvelut@s-pankki.fi. S-Bank generates the signature key and delivers the public key to the service provider via an encrypted email.

6 CONFIGURING THE SERVICE WITH THE SYSTEMS OF THE IDENTIFICATION TRANSMISSION SERVICE OR TRANSACTION SERVICE

The customer receives the OpenID Connect information related to using the identification service in the same encrypted email message as the keys for using the identification service that were mentioned in the previous section. The customer must configure this information with their own system in order to be able to use S-Bank's identification service.

Figure 2. Identification event



The stages of the identification event are presented in image 2:

1. Signed identification request (authorisation request)
2. Identification
3. Identification code (authorisation code)
4. Signed code request for the identification event (token request)
5. Signed/encrypted ID token with identification information

7 IDENTIFICATION REQUEST (OIDC AUTHORISATION REQUEST)

The identification request is an HTTPS REST authorisation request message in line with the OpenID Connect protocol. The message is sent to the identification address (authorisation endpoint): https://online.s-pankki.fi/ftn/authorize

The transaction service or transmission service redirects the browser of the holder of the identification medium to open the identification address with the parameters provided. The opening of the address starts the process of identifying the holder of the identification medium in S-Bank's identification service.

After the holder of the identification medium has been successfully identified in S-Bank's identification service, their browser is redirected to the redirect address (redirect URI) of the transaction service or transmission service. The parameters of the redirect request include the authorisation code issued by the identification service. The transaction service or transmission service uses the authorisation code to retrieve the identification information from S-Bank's identification service through the authorisation request (token request). The identification request is always signed by using the private keys of the transaction service or transmission service.

8 AUTHORISATION REQUEST (OIDC TOKEN REQUEST)

The authorisation request is a token request message in line with the OpenID Connect protocol. The transaction service or transmission service sends the message to the authorisation address (token endpoint) as a direct HTTPS REST message: The authorisation code received in response to the identification request is included as a parameter in the message, and the identification code (ID token) and access code (access token) are received as the response.

The messages are transmitted in accordance with the JSON Web Token standard (IETF RFC 7519). JWT determines the JSON data transfer method between two operators. The identification code (ID token) is base64-coded, signed and JWE-encrypted (JSON Web Encryption) and includes the identification information (claims) of the holder of the identification medium. The elements are separated by periods and base64-coded.

The identification code received must always be validated in accordance with the OpenID Connect specification. The authorisation request is always signed by using the private keys of the transaction service or transmission service. The authorisation request is always signed by using the private keys of S-Bank's identification service and encrypted by using the keys of the transaction service of the transmission service.

9 CUSTOMER INFORMATION

The UserInfo endpoint is a protected OAuth 2.0 resource that restores the claims about the authenticated end user. To obtain the requested claims about the end user, the customer makes a request to the UserInfo endpoint by using the access token provided by the OpenID Connect authentication.

The UserInfo endpoint is not a compulsory execution: it is one of the endpoints available for FTN implementation. Customers using the FTN implementation must decide whether they wish to use this endpoint.

10 TESTING THE IDENTIFICATION SERVICE

The customer receives instructions for testing the identification service in the encrypted email message sent in connection with entering into the agreement.

11 EXCEPTIONAL SITUATIONS

The service provider must prepare for exceptional situations, which may include the following:

1. The customer aborts the identification process. The customer may abort the event, either before the identifier is transmitted to S-Bank's identification service or by using the 'Cancel' button after the identifier has been created.
2. Customer verification fails either due to incorrect identifier data being provided by the customer or because the customer has requested verification from the wrong bank. The customer returns to the service provider's service by using the 'Cancel' button.
3. S-Bank detects an error in the identification request. S-Bank detects an error in the identification request before the customer is verified. The customer returns to the service provider's service.
4. The service provider detects an error in the identifier. An error can be caused by an error in the message content, or if an identifier does not correspond to the personal data issued by the customer. The service provider must issue the customer with a notification corresponding to the situation.
5. No response at all. An interruption can be caused by a break in the connection, another technical disturbance, a customer dropping a session, or a customer's session expiring.
6. The same response is sent many times.

12 ADVICE AND TECHNICAL SUPPORT

Technical support for the identification service:
e-palvelut@s-pankki.fi

13 LINKS

Finnish Trust Network OpenID Connect 1.0 Protocol Profile version 1.0
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ftn_oidc_profile_v1.0_ficora_rec_213_2018_s.pdf

OpenID Connect –protokolla
https://openid.net/connect/

OpenID Connect 1.0
https://openid.net/specs/openid-connect-core-1_0.html

JSON Web Tokens
http://jwt.io

6/2022 S-Bank