25 November 2022

OP Identity Service Broker

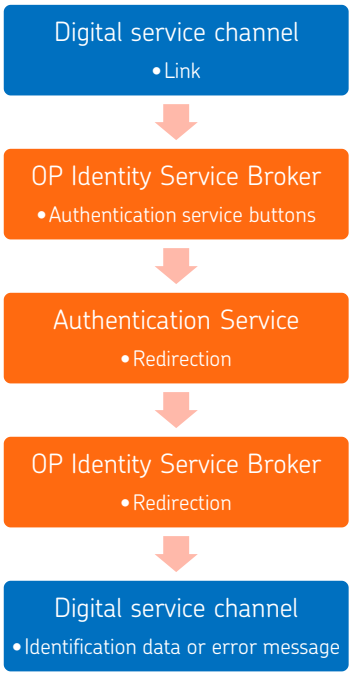
Contents

25 November 2022

1 Overview

You can use OP Identity Service Broker for strong electronic identification of persons using your online service or application. From OP, you can get strong authentication credentials for various identification services with a single contract and technical integration.

The service forms part of the Finnish Trust Network (FTN), which consists of identification service providers issuing strong means of identification that are used to provide the Authentication Service, and parties acting as identification broker service providers. OP operates in the Finnish Trust Network as an identification broker service provider.



Add a link to OP Identity Service Broker in your digital service channel. An OIDC interface call must be built into the link as specified in the integration instructions.

The user of the digital service channel chooses an authentication service by clicking its button. The user can choose between authentication service providers that are members of the Finnish Trust Network (FTN). These are described in op.fi under the OP Identity Service Broker page.

Authentication takes places in the authentication service chosen by the user. The service then redirects the user to OP Identity Service Broker.

OP Identity Service Broker redirects the user back to the digital service channel.

Our services and APIs conform to regulation no. 72b by Traficom about electronic identification and trust services. For details of the regulation, see https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/electronic-identification.

OP Identity Service Broker is based on the OIDC (Open ID Connect) API specification. We handle only Finnish authentication credentials on the service. An identification event that contains optional attributes is handled as if no optional attributes are involved. The optional attributes are listed in the regulation issued by Traficom.

The use of OP Identity Service Broker requires that you make a contract at an OP cooperative bank and accept the terms of use. Once the contract has been made, you can implement OP Identity Service Broker as explained in this service description.

2 Software requirements

2.1 User interface

You can integrate OP Identity Service Broker in your digital service channel in two alternative ways.

1) User interface provided by OP

Add in your digital service channel a link that calls the OIDC API and redirects the user to the web-based responsive user interface provided by OP. The user interface is available in Finnish, Swedish and English. The user selects an identification service in which they identify themselves. From there, they will be redirected to the digital service channel as an authenticated customer. In case of any errors that may occur in the identification service, the user will be redirected back to the user interface provided by OP.

It is also possible to display to the user a view in the Identity Service Broker in which they can check their personal data before they will be redirected to the digital service channel.

2) User interface embedded into the digital service channel

The digital service channel calls the OIDC API. OP Identity Service Broker responds by providing authentication buttons (links and images) for identification services, which the digital service channel embeds into its user interface. In case of any errors that may occur in the identification service, the user will be redirected back to the digital service channel's user interface.

When implementing an embedded user interface, the digital service channel must state that the Identity Service Broker is provided by OP. It also necessary to let customers know that when they identify themselves that a personal ID and name will be forwarded to the service provider. In addition, a link must be added to the Privacy Notice of the Identity Service Broker. All this information also comes from the API.

The information in the digital service channel must be as follows:

During identification, your personal ID and name are forwarded to the service provider. Privacy Notice OP Identity Service Broker is provided by OP Financial Group member cooperative banks and OP Cor-porate Bank plc.

Link to the Privacy Notice: https://isb.op.fi/privacy-info?lang=en. Supported languages are fi, sv and en.

2.2 Supported browsers

OP Identity Service Broker works with the most commonly used browsers. We recommend that you use the latest browser version. In order for the service to work, you must allow http session cookies and JavaScript browser scripts.

The user interface provided by OP has been designed in such a manner that it is accessible to as many customers as possible, and it can be used by means of assistive technologies.

You can find information on supported browsers and instructions for the use of cookies and JavaScript at op.fi under Use of OP's digital services.

3 Settlement

When you agree on the use of OP Identity Service Broker, you must specify the purpose for which you will use strong electronic identification. The service can be used not only for authentication but also to chain credentials, that is, either to grant strong electronic credentials (available to FTN members only) or the digital service channel's weak credentials.

These three types of use are discussed below as contract types: identity verification, chaining of strong credentials, and chaining of weak credentials.

3.1 Contractual changes

The following changes require a change in the contract: If you want to:

- add or remove the chaining of strong electronic credentials or weak electronic credentials
- add a restriction on the means of identification
- remove a restriction on the means of identification.

We will publish an announcement on op.fi if new providers of strong authentication providers are added to OP Identity Service Broker.

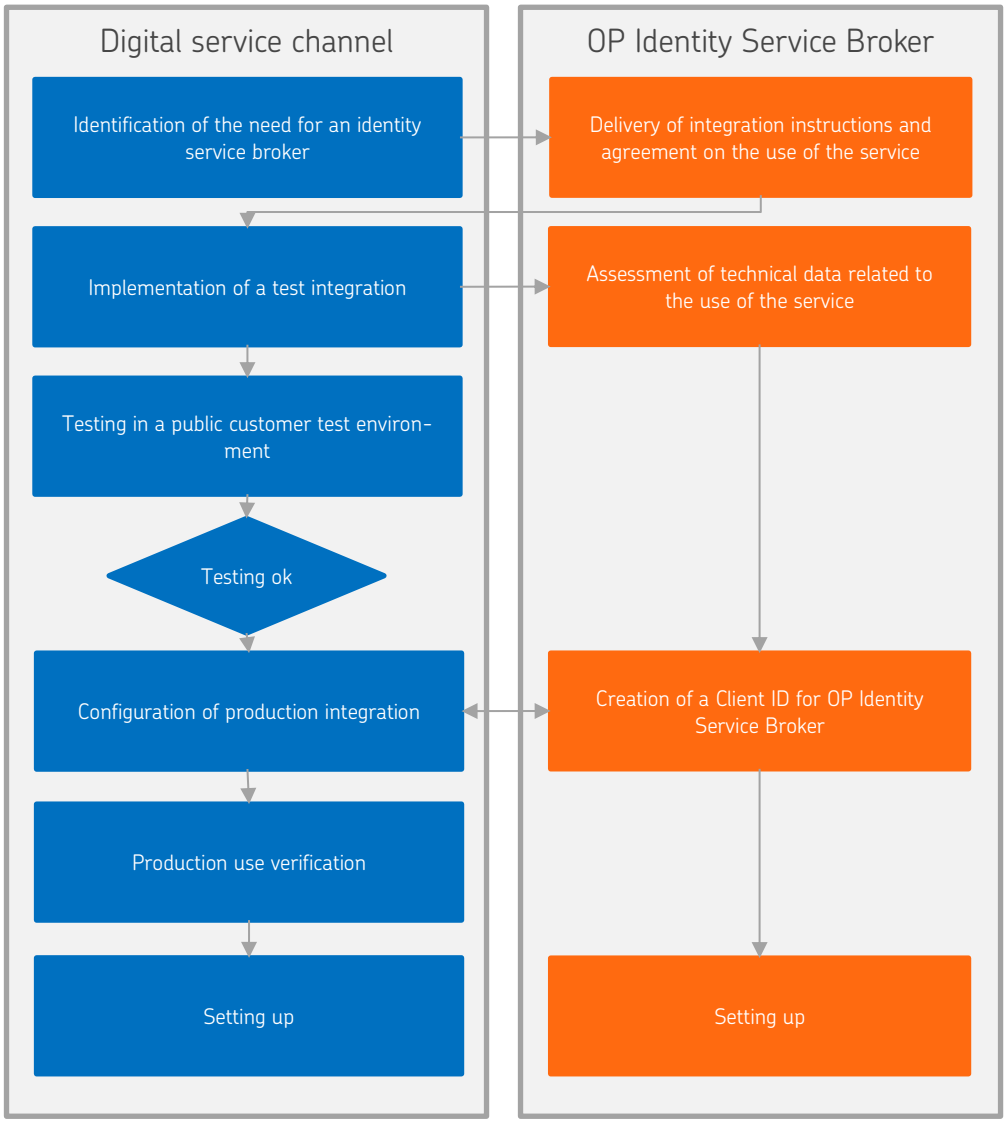
4 Deployment

To integrate your eService with OP Identity Service Broker, follow the integration instructions that are publicly available. We recommend that you contact OP for making a contract before beginning the integration.

You can test the integration between your digital service channel and OP Identity Service Broker in a public customer test environment (Sandbox) into which all digital service channels can be integrated by using a public test ID.

Make a contract on the use of the service before putting it into production use. We will assess the technical details related to the use of the service and provide your digital service channel with a Client ID by which it will be identified in the integration API calls.

For a more detailed description of the API, including examples, see OP Developer below:
https://github.com/op-developer/Identity-Service-Broker-API



4.1 Notification of technical data

We need the following information for the implementation:

- Company name
- Company's business ID
- OpenID entity statement
- As additional information, we require other optional names used for the service (SP name in the technical description)

Please give us the email address of the digital service channel's technical contact person to whom we can send a form for providing such information. We will send the form by using encrypted email. Fill in the form electronically and return it by replying to the encrypted email.

At the same time, we will provide the technical contact person with a Client ID for OP Identity Service Broker. The Client ID is the digital service channel's unique identifier for integration interface calls.

4.2 Changing the cryptographic key

OP Identity Service Broker changes the API encryption key on a regular basis. The digital service channel will automatically receive the cryptographic keys in force from the signed_jwks API, and this should be verified at least once a day. In connection with the verification, the eService should also verify the TLS certificate of OP Identity Service Broker and the signature in the signed_jwks API.

The digital service channel's OIDC keys must be changed on a regular basis and message-level keys at least every two years. OP Identity Service Broker will automatically receive the cryptographic keys in force from the digital service channel's signed_jwks API. Whenever you discontinue the use of an old key, you must remove it from the digital service channel's signed_jwks API at least 24 hours before the key becomes disabled.

It is your company's duty to keep track of the validity of the digital service channel's TLS certificate and to get a new one in time. The recommended period of validity for a certificate is two years, and your company is responsible for renewing it. The certificate must be issued by a trusted certification service provider.

4.3 Testing the OP Identity Service Broker

You can first test the integration between your digital service channel and OP Identity Service Broker in a public customer test environment (Sandbox). The identification services' test environments have been integrated into the customer test environment. The use of real authentication credentials is not possible in this environment.

4.4 Production verification

When migrating into production, the functioning of the integration is verified in production environment by using real identification services and authentication credentials.

5 Contact information

For questions regarding OP Identity Service Broker, please contact:

- OP Corporate and Payment Services, tel. 0100 05151 or
- send email to verkkopainikkeet@op.fi

In contractual matters, please contact your own OP cooperative bank.

Please report any changes in your company's contact persons or other details to your OP contact person.