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

Contents

Version

0.1	26.3.2018	Petri Pyöriä
0.2	3.4.2018	Petri Pyöriä
0.3	11.4.2018	Petri Pyöriä
0.4	25.4.2018	Petri Pyöriä
0.5	18.6.2018	Petri Pyöriä
0.6	20.8.2018	Petri Pyöriä
0.8	14.9.2018	Petri Pyöriä

Terms and abbreviations

CA	Certificate Authority
FTN	Finnish Trust Network
(FTN) IDP	Identity Provider within the FTN
(FTN) Broker	Broker that handles authentication requests between Service Providers and IDPs in the FTN.
HTTPS	Hyper Text Transfer Protocol Secure
JWA	JSON Web Algorithms (RFC 7518)
JWE	JSON Web Encryption (RFC 7516)
JWS	JSON Web Signature (RFC 7515)
JWKS	JSON Web Key Set
JWT	JSON Web Token (RFC 7519)
KID	Key Identifier
OIDC	Open ID Connect
PKI	Public Key Infrastructure
SP	Service Provider, provides a service the end-user is trying to access and is being authenticated to, from the viewpoint of the FTN Broker
SSL	Secure Sockets Layer
TLS	Transport Layer Security (updated SSL)
URI	Uniform Resource Identifier

Introduction

In the case of Finnish Trust Network, Service Providers (SP) request identity authentication of end users from the FTN brokers. Brokers then utilize the authentication services of Identity Providers (IDP) to perform the authentication of the user. One broker may be offering identity authentication services of several different identity providers for service providers.

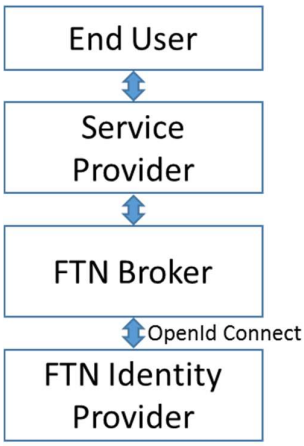

Figure 1: The Service Provider authenticates identity of the end user by requesting the service from an FTN Broker, which utilizes the services of FTN identity providers.

Identity authentication interface of the Finnish Trust Network (FTN) between the IDP and Broker follows either SAML or Open ID Connect protocol. In this document, an assumption is that Open ID Connect protocol is used (Viestintävirasto, 2018) (OpenID Foundation, 2018).

To enable secure communication between identity providers and brokers, as well as brokers and service providers, all security sensitive communication between parties must be digitally signed and encrypted as described in the FTN OIDC Profile –specification of Finnish Communications Regulatory Authority Viestintävirasto (Viestintävirasto, 2018). Encryption and signing of messages requires that communication parties must exchange security keys and client identity information in a secure way before the actual OIDC identity authentication communication starts.

A secure security key and data exchange require that, on the other hand, keys and certificates must be transferred so that third party agents cannot access or change clear content of the data, and, on the other hand, that the correct origin of the keys and certificates can be ensured.

This document describes how FTN IDP and FTN Broker can exchange security keys and Open ID Connect security information and start to communicate over the identity authentication interface in a secure way. If the identity provider acts also in the role of a broker, it is supposed that the same key and data exchange process can be used by service providers. Otherwise, key and data exchange process between service providers and brokers has been left out of scope of this document.

Goals and assumptions of the key and security data exchange process

1. Key and security data exchange process must be secure as described above.

2. The process should be as automatic as possible to minimize the amount of human errors and manual work.

3. If possible, the process should be common for the most parties in the Finnish Trust Network to reduce system implementation and integration work as well as the number of possible error sources.

4. Implementation of the process should be relatively easy. It should be possible to join the identity authentication system even with limited capabilities to design and implement security systems.

5. It is supposed that FTN parties must provide whole service as such – external supporting services will not be available (for example, third party PKI CA service)

6. Keys and certificates must be exchanged beforehand between the FTN IDP and broker. Keys must be explicitly configured/pinned as trusted for OIDC use (Viestintävirasto, 2018).

Key and data exchange process

In this chapter is described a method to exchange security keys safely without an external PKI (CA) service.

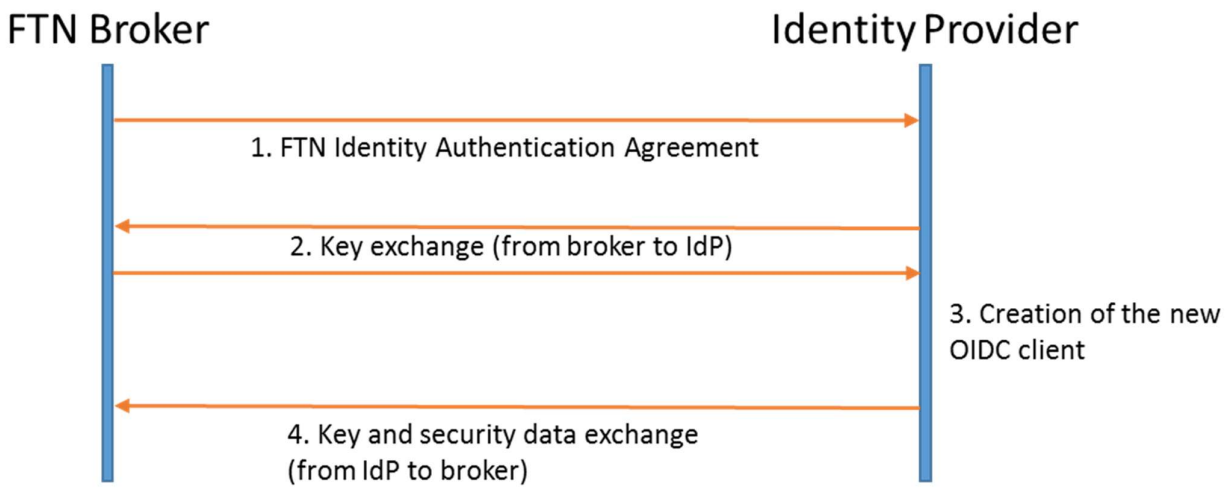

Figure 2: Basic key and data exchange process between the broker and identity provider.

The security key exchange process starts from the creation of the FTN agreement between the broker and provider and ends as the identity provider sends client information and public keys to the broker.

1. When FTN Broker makes an FTN agreement with the identity provider, the identity provider creates a new OIDC client for the broker and the broker delivers required information for the creation of OIDC client (Figure 2, step 1). This information can be provided in a clear format and it contains at least following data fields:

    - Client name
    - Redirect URIs
    - Broker contact information
    - Broker JWKS URI

    In addition, to ensure that broker receives later IDP JWKS URI and OIDC client id from the correct source, the IDP creates a random number (= temporary broker identification code). This random value is given immediately back to the broker. The broker can later check that value matches with the received value (see step 4).

2. When IDP has received the broker information, the identity provider needs to create a new OIDC client. A creation of the OIDC client requires that the identity provider knows the public keys of the broker. Because of that, either the identity provider must attain the keys from the broker or keys must have been got during the agreement creation phase (Figure 2, step 1 or step 2). In this document, it is proposed that the identity provider downloads keys from the JSON Web Key Set -web page of the broker. For that purpose, the broker provides the URL of the JWKS page at the phase 1 of the process when the agreement was created (= Broker JWKS URI).

    Security of the provided JWKS URI page is based on the secure URI messaging through the FTN agreement making process and, on the other hand, encrypted HTTPS communication and SSL/TLS certificates signed by the trusted CA.

3. When public keys of the broker have been received, the identity provider creates a new OIDC client (Picture 2, step 3) and a JWKS page for IDP public keys.

4. When the new client has been created, a new OIDC client id is available and must be delivered to the broker. In addition to the client id, the broker must also receive a public signing key (and optionally encryption key) of the identity provider. The broker signs all authentication messages with the private signing key and optionally encrypts messages with IDP's public encryption key. According to Luottamusverkosto OpenID Connect specification of the Viestintävirasto, signing of messages is mandatory and encryption optional.

    To provide all required information for the new broker (Figure 2, step 4), the identity provider creates an email including IDP JWKS URI, client id, OpenID Connect endpoints and temporary broker identification code created in the phase 1. The email is send to the broker by secure email service. The secure email service sends notification of the message to the broker's email address and message pin code to the broker's phone number as a SMS

message. The broker can read the encrypted email from the web service by entering the given pin code as an authentication input.

The broker can ensure origin and being correct recipient of the message by comparing temporary broker identification codes, received by the secure email and during the FTN agreement making process. As above in the case of broker keys, security of the IDP key exchange is based on the secure way to transfer URI to the broker through the secure email system and, on the other hand, on encrypted HTTPS communication and SSL/TLS certificates signed by the trusted CA.

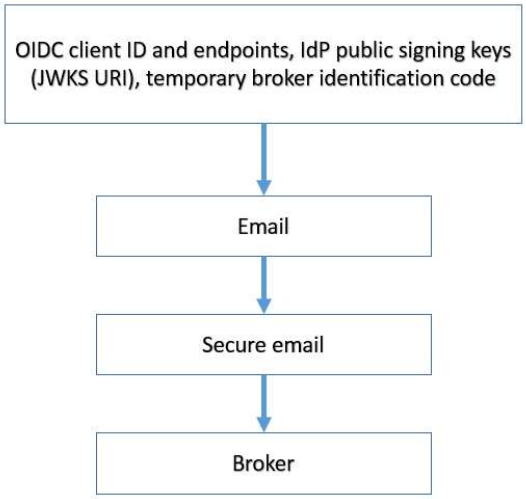

Figure 3: Sending of the sensitive information from the IDP to the Broker. The IDP creates an email and sends itl over the secure email service.

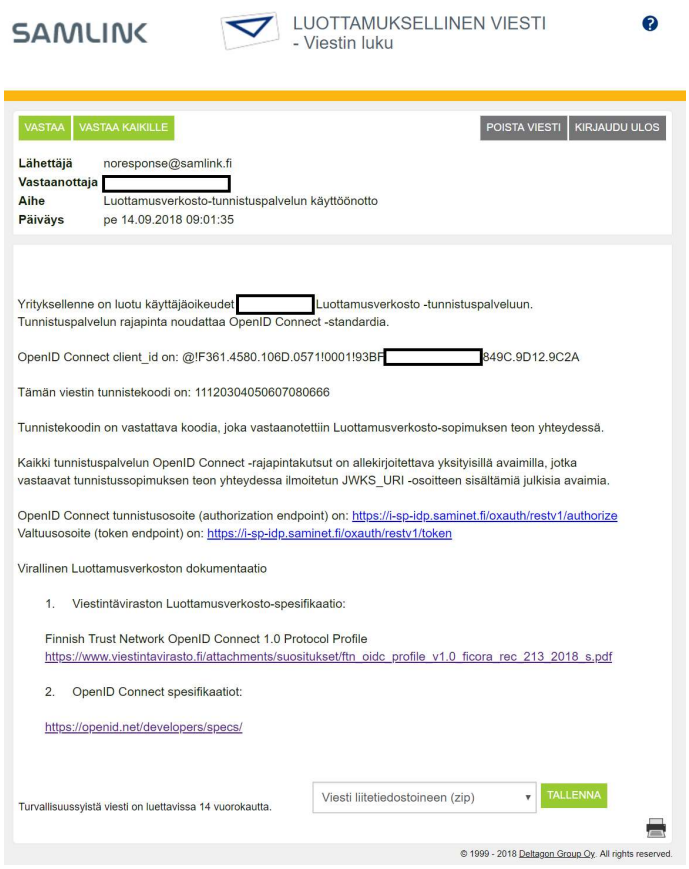

Figure 4: An example of the secure email for the broker

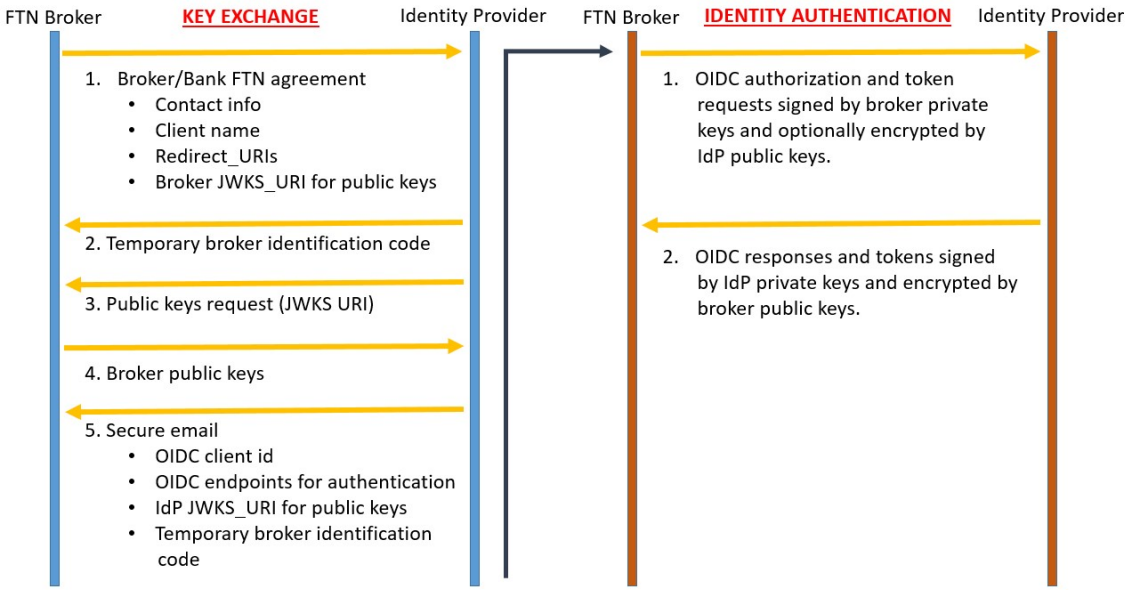

Figure 5: More detailed key exchange process description.

Ensuring correct origin of keys and data

In the secure key or data exchange, correct origin of the data must be ensured. If the receiver accepts wrong data sources for keys and certificates, keys may be compromised and communication channel may not be safe.

A common solution for the problem is to establish a trusted third party Certificate Authority that signs and publishes public keys of the key exchange parties. Each party can ensure that received keys belong to the correct source organization by checking signing of the CA with their public signing key.

In the case of Luottamusverkosto PKI CA services will not be available to FTN service providers except common SSL/TLS CA providers.

In this document, the identity provider receives public keys of the broker from the broker web page. The URI for the page is received when the agreement between the broker and IDP is created. It is the responsibility of IDP check identity of the broker and enter valid Broker JWKS URI to the FTN identity authentication system of the IDP. JWKS URI –pages are read through encrypted HTTPS-connections. Standard SSL/TLS –certificates signed by trusted CA ensure origin of the data. JWKS URI pages without signing certificates must not be accepted by the broker or IDP.

The broker receives OpenID Connect client id and a JWKS URI of the IDP by secure email. Trust for correctness of the data is based on the secure email service and temporary broker identification code included to the email.

It is necessary for both parties to check SSL/TLS certificate of the JWKS URI page every time when the page is read to ensure security of the authentication process.

Key exchange in practice

Broker activities:

1. Create private and public keys for signing and encryption.

2. Save keys to file in the JWKS –format.

3. Create a web page containing JWKS-file content. The web page must have SSL/TLS –certificates signed by trusted CA to ensure origin of data for the IDP.

4. When a new FTN agreement is created, give URI of the JWKS –page for the identity provider. You will receive a temporary broker identification code, which is used to check origin of the client data message received later by a secure email.

5. When client id and IDP JWKS_URI has been received from the IDP, check temporary broker identification code of the email and start usage of the identity authentication service. Attach required parameters (client_id) to OIDC messages, sign them with your own private keys, and optionally encrypt with IDP public keys

(from IDP JWKS URI). Every time when JWKS URI page of the IDP is read, validity of the CA signed SSL/TLS certificates must be checked.

Identity provider activities:

1. Create private and public keys for signing and encryption.
2. Save keys to file in the JWKS –format.
3. Create a web page containing JWKS-file content. The web page must have SSL/TLS –certificates signed by trusted CA to ensure origin of data for the broker.
4. When a new client is created, send OIDC client id, temporary broker identification code and OIDC endpoints by secure email for the broker.
5. Every time when broker JWKS URI page is read during the authentication messaging process, validity of the CA signed SSL/TLS certificates must be checked.

FTN broker and identity provider security key management

Finnish trust network specifications of Viestintävirasto do not address issues of the encryption key management. The key management policy should define the lifecycle of keys, physical and logical access to the key storage and users/roles who can access the keys. In this document, a basic assumption is that both communication parties define their own processes and handle encryption keys safe way. However, some lifecycle issues are common for both parties. Because of that, in next chapters we define a default crypto period for FTN keys and high-level processes for the key renewal and revocation.

Lifecycle of keys

Encryption key lifecycle can be defined to have four different high-level states:

- Pre-operational
- Operational
- Post-operational
- Obsolete/destroyed

Crypto period defines how long key remains in the operational state. In this document, an assumption is that both parties use relatively short time period for operational state of keys – for example, two days.

Key renewal

In this document, it is proposed that both parties, identity provider and broker, will use short key renewal periods – for example, two days. When encryption and signing keys change, corresponding public keys are changed in JWKS URI –pages. After that, key ids (KID) in identity authentication messages are changed and based on them, receiving party can download new keys from updated JWKS URI –pages when previously unknown KID has been detected.

Key revocation

If keys must be revoked, both parties can just renew their keys. If required, the IDP can prevent access of the broker by removing or disabling their OIDC client in the OpenID Connect system.

Changing JWKS URI

Because the correct origin of keys is based on the JWKS URI web pages, it is important that the URI address cannot be changed easily. If it is necessary to change JWKS URIs, information must be delivered to another party secure way. In this document, it is supposed that IDP and broker agrees by themselves how secure URI change is done. Changing of the JWKS URIs should be a rare event, which is made only for compelling reasons.

References

OpenID Foundation. (2018). *OIDC Specifications*. http://openid.net/developers/specs/

Viestintävirasto. (01 2018). *FTN OIDC Profile*. https://www.viestintavirasto.fi/attachments/suositukset/ftn_oidc_profile_v1.0_ficora_rec_213_2018_s.pdf