# Aktia FTN OIDC-profile supplement 2024

## 1.1. General

This appendix supplement protocols, profiles and procedures defined in OIDC Core and FTN OIDC specifications. Also following OIDC specifications apply to their relevant parts as defined in M72B and FTN OIDC Profile (213/2023 S) and descriptive appendices and amendments in and related to these official specifications and explanations as made available by Traficom:

- OpenID Connect Discovery
- OpenID Connect Dynamic Client Registration
- OpenID Federation

Procedures enable interoperability between Aktia Identity Provider (IdP) and Broker Service Provider (Relying Party). Procedures also ensure availability and information security of the service as well as accuracy, integrity and protection of the personal data of the end user.

When referring to message encryption and signing, this document refers to OIDC protocol messages as described in FTN OIDC profile and OIDC Core specifications. Regarding exchange of technical metadata, OpenID Connect Discovery and OpenID Federation specifications are referred. However, as defined in Chapter 4 of FTN OIDC profile, the OpenID Federation specification is implemented only partially.

This document sites and refers to the same sources as the main document. See references from the main document.

The Aktia Identity Provider implements OpenID Connect **Authorization Code flow** authentication as defined in FTN OIDC Profile.

## 1.2. HTTP-protocol

This documentation describes the form of OIDC messages and procedures in exchanging authentication messages between parties.

All messages are exchanged using HTTPS-protocol. Communication between parties **MUST** use HTTPS-protocol according to well-known best practices and using certificates by commonly trusted root certificate authorities. All communication **MUST** be encrypted using strong TLS-encryption using commonly recognized encryption and signing algorithms as defined in M72B and FTN OIDC Profile.

Aktia Identity Provider doesn't implement HTTP protocol level client authentication. Client certificates and other authentication related HTTP parameters will be ignored.

## 1.3. Metadata exchange

Parties exchange metadata, which is used to form a technical trust between parties. Authentication of the end user is possible only by using endpoint addresses to communicate and the keys specified in the metadata to sign, encrypt, verify and decrypt messages.

Parties **MAY NOT** trust, relay or otherwise use exchanged messages, data in them or data derived from them if messages can't be verified based on to the exchanged metadata.

Aktia Identity Provider doesn't implement dynamic **discovery** [5] of the Service Provider. Technical trust between parties is fixed and it cannot be established using automation.

Parties exchange metadata or address referring to it at the time-of-service subscription or the signing of the service agreement. The parties **MUST** identify each other before signing the subscription. Parties are **REQUIRED** to inform each other in advance about changes in the details of the metadata or the change in representatives of the parties or the contact details of the representatives or in service contact details. If representatives of the parties change, the new representatives **MUST** be identified at least in as strong manner as was done at the time of initial subscription.

Metadata doesn't include secret or confidential information and can be processed as public data. The integrity and the origin of the metadata **MUST** be verified.

If cache is used in the metadata exchange, the original metadata MUST be refreshed from the original endpoint at least once in **240** minutes. This amount of time will be referred as n(cache) in this document.

### 1.3.1. The metadata of the Aktia Identity Provider

Aktia publishes *Entity Statements* as defined in FTN OIDC Profile and specifications it refers to. The entity statement will be published from address:

`https://ftn.aktia.fi/.well-known/openid-federation`

The Entity Statement is signed. Relying Party **MUST** verify the integrity of the Entity Statement based on the signature and to other aspects that are defined in respective specifications. Keys to verify the signature are published inside the Entity Statement itself as defined in FTN OIDC Profile. Relying Party **MUST NOT** trust any data exchanged by or derived from an Entity Statement that can't be verified. Relying Party **MUST** inform Aktia without delay if such anomaly or suspicion of such should be found.

Two (2) separate keys for signature verification are published inside of the Entity Statement.
Keys **MAY** be rolled over without prior notification. Relying Party **MUST** ensure that keys it uses form a chain of trust. Although not necessarily named as such, *Current* and *Next* keys will be published. Relying Party **MUST** identify which of the keys in the keyset is *Current* and which is *Next* based on information exchange with Aktia while parties first initiated the subscription (as defined in main *Palvelukuvaus* document) in trustworthy manner.

Relying Party **MUST NOT** trust a *Current* key it if wasn't published as *Next* in previous properly verified Entity Statements. If it would happen that Relying Party is unable to form a chain of trust between keys while they are rolled over, Relying Party **MUST** ensure the integrity of the key in same manner as was done initially when initiating the subscription of the service (see main *Palvelukuvaus* document).

The actual technical metadata for protocol messaged exchange as defined in *OpenID Connect Discovery* is published inside Entity Statement. Relying Party **MUST NOT** refer to any other technical metadata detail that is not exchanged in the manner described in this document and specifications it refers to. The technical trust formed between parties **MUST** be based only on the data inside of verified Entity Statement or on the data derived from it in trustful manner based on best practices as defined in respective specifications referred in this document.

### 1.3.2. The metadata of the Relying Party

The Broker Service Provider (Relying Party) publishes *Entity Statements* as defined in FTN OIDC Profile and specifications it refers to. Relying Party **MUST** inform Aktia in trustworthy manner of the address where Entity Statements will be published. Also, during the same exchange of data, Relying Party **MUST** inform Aktia about the trust mechanism that is used to form chain of trust between Entity Statements during flow of time.

Aktia has implemented methods for trust mechanisms to Entity Statements according to following list. The list **MAY** be altered based on the implementations of parties.

- Entity Statement URI
    - Technical trust is based on Entity Statements that Relying Party publishes and Aktia reads from an URL. The trust is based on a chain of trusted keys in similar manner as is described above in previous chapter of this document. As deviation from the above, Aktia will formulate the technical metadata of Relying Party as defined in OpenID Federation and OpenID Connect Dynamic Client Registration.
    - Make note that Dynamic Client Registration is NOT supported on Aktia IdP service, but only the technical metadata of the relying party is formulated as described in this specification.
    - If the Entity Statement includes field x5c, it will be used as the base of trust for the Entity Statement. This is the preferred method to establish trust to an Entity Statement. If x5c field is present, Aktia **SHALL** verify the chain of trust of the certificates in chain all the way to the root. In this case, the *modulus* of the key key used to sign the root certificate **SHALL** be pinned in Aktia's configuration. However, as keys of root certificates change very rarely, this is the preferred way of establishing the root trust to Entity Statements. When the keypair of the root certificate changes, it must be exhanged with Aktia in trustworthy manner in same manner as was done initially when initiating the subscription of the service (see main *Palvelukuvaus* document).
- Pinned Entity Statement
    - If Relying Party doesn't publish Entity Statement from an URL, it can be manually pinned to configuration. Trust is formed in similar manner as described above.

- Pinned Protocol JWKS
    - The actual technical metadata for protocol message exchange of the Relying Party is added and pinned to Aktia's configuration manually as hardcoded. Every change in any detail in the configuration **MUST** be exchanged in trustworthy manner in same manner as was done initially when initiating the subscription of the service (see main *Palvelukuvaus* document). Any change in the metadata with this mechanism is always manual. No automation can be applied in exchange of the metadata in this manner.
- JWKS URI
    - This is **deprecated** means of establishing technical trust to a Relying Party. The method is not compliant to current specifications.
    - In this method Aktia **SHALL** read keyset to protect protocol message exchange from URI that Relying Party has informed during initiating the subscription of the service. The technical metadata is configured manually. Refer to previous method on how to change and exchange any data in the metadata.

Relying Parties should prefer to trust mechanisms in the order of the above list, where the first entry has the precedence.

Aktia monitors the published metadata of relying parties. If any errors in verifying the metadata exchange or deviations from specifications should be found, Aktia **SHALL** inform the Relying Party without further delay. In case the deviation is *major* as defined in the specifications, Aktia is obliged to also inform officials from the incident.

## 1.4. Signing and encryption algorithms

FTN OIDC profile specifies the algorithms used in the FTN in signing and encryption of messages. Aktia Identity Provider implements algorithms based on specifications referred in this document. Rest of this chapter has been removed in this version of the document.

## 1.5. Credentials used with the service

Aktia provides a ClientID that Relying Party uses to uniquely identify itself to Aktia Identity Provider. The ClientID is tied to the details that will be used to form the technical trust to exchange metadata with the Relying Party as described above in this document. After signing the service subscription Relying Party is able to form a technical trust to Aktia Identity Provider.

Authentication of the end user and fetching the personal data of the authenticated end user is not possible without valid ClientID.

If reasonable doubt is expressed that the Relying Party or any piece of technical metadata exchange has become compromised, the Aktia Identity Provider service **MAY BE** temporarily suspended from Relying Party and/or the ClientID **MAY BE** revoked immediately. Taken the gravity of the situation, renewal of the ClientID in such case can cause service disruption if the change can't be

coordinated in advance. In such case, the communication between parties **MUST** happen according to service disruption processes.

## 1.6. Key rollover

This chapter has been removed. Please refer to the chapter Metadata Exchange.

## 1.7. Authentication Request Signature verification

Authentication Requests **MUST** be signed.

If verification of Authentication Request signature fails, Aktia Identity Provider **WILL NOT** return authentication response for the requesting party. Instead, an error message is shown to the end user.

Parameters enclosed in signed Authentication Requests take precedence and override possibly unsigned parameters.

Aktia Identity Provider returns *code* responses only to the redirect_uri endpoint address specified in the metadata of the Relying Party.

## 1.8. Broker authentication

Relying Party **MUST** sign Token Requests with *private_key_jwt* method according to OIDC Core and FTN OIDC Profile. Relying Party **MUST** use the corresponding key in signing the request that has been published in the metadata.

## 1.9. Single Sign On (SSO)

Aktia Identity Provider doesn't implement Single Sign On (SSO). An authentication **IS REQUIRED** from the end user on each Authentication Request.

## 1.10. Level of Assurance

Aktia Identity Provider implements following Level of Assurance specified in FTN OIDC Profile:

- Finnish level substantial (korotettu)

Aktia Identity provider doesn't implement cross border eIDAS authentication at the time the service is published to general use. Aktia Identity Provider can be used to identify only **natural persons** in domestic scheme.

## 1.11. Released Personal Data

Only required attributes specified by the FTN OIDC Profile of **a natural person** are relayed and released. The Personal Identification Number is released as unique person identifier.

Aktia Identity Provider releases personal data only when it is requested by specifying the corresponding scope in the authentication request as defined in FTN OIDC Profile.

Aktia Identity Provider doesn't release optional attributes specified by the FTN OIDC Profile. Aktia Identity Provider doesn't release SATU (Sähköinen asiointitunniste) or Eidas Personidentifier.

Aktia Identity Provider cannot be used to identify **legal entities**.

Aktia Identity Provider releases mentioned attributes of the authenticated person enclosed in the encrypted and signed *id_token*. The Relying Party has no need to make separate queries to fetch or validate personal data of the authenticated user. Aktia Identity Provider **does NOT support** userinfo endpoint.

## 1.12. Additional parameters

FTN OIDC Profile defines additional request parameters *ftn_spname* and *ftn_sptype*. While requesting authentication from Aktia Identity Provider, Broker SP **MUST** populate values for *ftn_spname* and *ftn_sptype* as defined in FTN OIDC Profile despite them being defined as optional.