LUOTTAMUSVERKOSTON PALVELUKUVAUS

22 May 2019

Aktia

Sisällysluettelo

Aktia Pankki Oyj • PL 207 • 00101 Helsinki
Puh. 010 247 5000 • Faksi 010 247 6356
Y-tunnus 2181702-8 • www.aktia.fi

1. Yleiskuvaus

Vahva sähköisen tunnistamisen **Luottamusverkosto** (myöhemmin myös FTN) koostuu tunnistukseen luottavista **asiointipalveluista**, vahvan tunnistusvälineen tarjoajista ja **tunnistusvälityspalvelun tarjoajista** (Broker). Aktia toimii Luottamusverkostossa vahvojen tunnistusvälineiden liikkeellelaskijana eli tunnistuspalvelun tarjoajana, mutta ei toimi tunnistusvälityspalveluna. Tunnistamista tarvitseva asiointipalvelu voi hankkia valitsemansa tunnistusvälityspalvelun tarjoajan kautta eri tunnistuspalvelun tarjoajien tuottamat vahvat tunnistusvälineet yhdellä sopimuksella. Pääsääntöisesti Aktia tarjoaa tunnistuspalveluita ainoastaan tunnistuksen välityspalveluille. Tupas-rajapinta ei 30.9.2019 täytä lain vaatimuksia vahvasta sähköisestä tunnistamisesta, mikä on takaraja Luottamusverkoston palveluille. Palveluissa ja rajapinnoissa noudatetaan Liikenne- ja viestintäviraston määräystä M 72 sähköisistä tunnistus- ja luottamuspalveluista.

Aktian **tunnistuspalvelu** (FTN IdP) toteuttaa Traficomin (Liikenne- ja viestintäviraston) suosituksen (myöhemmin FTN OIDC-profiili) mukaisen OpenID Connect (myöhemmin OIDC Core) tunnistusrajapinnan (OP / IdP). Toteutus poikkeaa OIDC-määrityksestä siten, kuin FTN OIDC -profiilissa määritetään ja siten, kuin Brokerin kanssa erikseen sovitaan. Tunnistuspalveluun viitataan OIDC Core -määrityksestä poiketen termillä Identity Provider (IdP) silloin, kun OIDC Core -määrityksessä käytetään termiä OpenID Provider (OP).

Brokerin välityspalvelusta käytetään asiakirjassa myös termiä Broker Service Provider (SP). Mikäli viitataan tunnistamiseen luottavaan tunnistusvälineen haltijan käyttämään asiointipalveluun, tarkennetaan asia aina erikseen. Aktian tunnistuspalveluun ja tunnistusvälityspalveluun viitataan myöhemmin myös termeillä **osapuoli** (viitatessa toiseen) ja **osapuolet** (viitatessa molempiin).

Tunnistuspalvelun teknisiä yksityiskohtia tarkennetaan myöhemmin tässä Palvelukuvauksessa.

Aktia **ei toteuta** tunnistuspalvelussaan Traficomin määrittämää **SAML-rajapintaa**.

Aktia käsittelee palvelussa ainoastaan suomalaisia tunnistusvälineitä. Aktia Tunnistuspalvelun käyttö edellyttää tunnistuksen välityspalvelun ja Aktian välistä sopimusta. Sopimisen jälkeen tunnistuspalvelun käyttöönotto tapahtuu tämän kuvauksen mukaisesti.

Tämä palvelukuvaus koskee Luottamusverkosto tunnistuksen välityspalvelun (FTN Broker - asiakas) ja tunnistusvälinen tarjoajan (FTN IdP / Aktian tunnistuspalvelu - palveluntarjoaja) välistä toimintaa.

Aktialla ei ole kesällä 2019 käytössä tunnistusvälineeseen liittyviä rajoituksia ja estoja, jotka kuvataan tunnistuslain 18§:ssä.

1.1. Palvelun kohderyhmä

Aktian tunnistuspalvelun asiakkaaksi voi liittyä FTN-luottamusverkostossa toimiva tunnistusvälityspalvelun tarjoaja (asiakas). Luottamusverkostossa tunnistukseen luottava asiointipalvelu tekee sopimuksen tunnistusvälityspalvelun tarjoajan (palveluntarjoaja) kanssa.

Aktian tunnistuspalvelussa tunnistetaan Aktian henkilöasiakkaita. Loppukäyttäjät käyttävät tunnistusvälineenä verkkopankkitunnuksiaan ja muita kulloinkin voimassa olevia tunnistusvälineitä.

2. Vaatimukset käytettävälle ohjelmistolle

2.1. Käyttöliittymä

Tunnistuspalvelussa on selainpohjainen responsiivinen käyttöliittymä. Käyttöliittymä tarjotaan kokosivuisena eikä siitä ole toistaiseksi tarjolla välityspalvelusopimukseen upotettavaa versiota. Käyttöliittymä on käytettävissä suomeksi ja ruotsiksi.

2.2. Tuetut selaimet

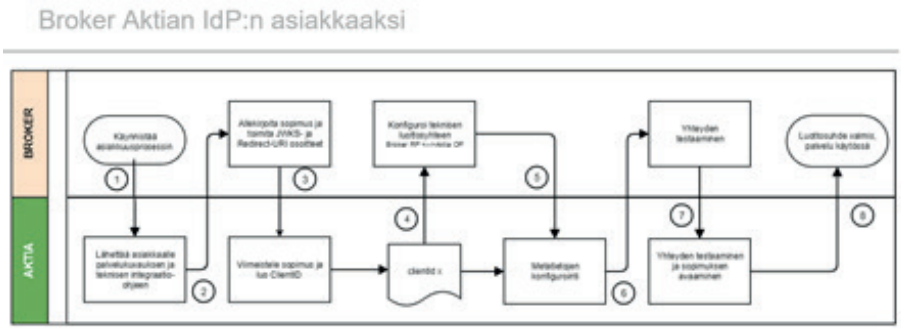
Aktia tunnistuspalvelussa noudatetaan Aktian yleisiä selainsuosituksia. Käytettävän selaimen tulee tukea moderneja yleisesti käytettyjä salausalgoritmeja. Selaimen on ajantasaisesti tuettava kulloinkin markkinoilla olevien selaintoimittajien yleisesti luottamia varmenteita. Suosituksena on käyttää sellaisia luotettavia uusimpia selainversioita, joiden virheet ja tietoturvapuutteet on korjattu. Loppukäyttäjä vastaa itse käyttämänsä laitteiston ja ohjelmistonsa ajantasaisuudesta ja turvallisuudesta. Palvelu vaatii toimiakseen istuntoevästeiden (http session cookies) ja JavaScript-tuen sallimisen selaimessa.

Lisätietoa Aktian yleisistä selainsuosituksista: https://www.aktia.fi/fi/verkkoselain-ja-laitesuositukset

3. Sopiminen

Tunnistuksen välityspalvelun ja Aktian tunnistuspalvelun välisessä sopimuksessa määritetään tunnistuksen vahvuuden tasot ja ehdot.

Jokaisella välityspalvelun tarjoajalla on palvelua käyttääkseen oltava vähintään yksi sopimus. Sopimuksia avataan yksi kappale jokaista teknistä liityntärajapintaa kohden. Jos tunnistuspalvelua käytetään lain tarkoittamaan **ensitunnistamiseen** vahvan tunnistusvälineen luovuttamiseksi **tunnistusvälineen haltijalle** (nk. tunnistamisen ketjuttaminen), on se etukäteen valittava sopimuksen ominaisuudeksi. Aktia tarjoaa lähtökohtaisesti ensitunnistamista vain Luottamusverkostossa tunnistusvälineen tarjoajille. Lisäksi välityspalvelu merkitsee kuhunkin yksittäiseen tunnistuspyyntöön kyseisen tunnistustapahtumatyypin FTN OIDC-profiilin mukaisesti.



Välityspalvelu (Broker) tulee Aktian asiakkaaksi:

1. Välityspalvelun edustaja ottaa yhteyttä Aktiaan tehdäkseen sopimuksen
2. Välityspalvelulle lähetetään sopimusehtojen mukana tämä palvelukuvaus ja tekninen Aktia FTN OIDC-profile supplement määritys
3. Välityspalvelu allekirjoittaa sopimuksen ja sen yhteydessä toimitetaan OIDC-protokollan tarvitsemat metatieto-osoitteet (URIt)
4. Aktia viimeistelee sopimuksen ja välityspalvelulle luodaan ClientID, joka toimii asiakkaan teknisen rajapinnan yksilöivänä tunnisteena
5. Välityspalvelu konfiguroi teknisen luottosuhteen
6. Aktiassa konfiguroidaan saadut metatiedot luottosuhteen aktivoimiseksi, sovitaan integraation testaamisesta
7. Integraatio testataan ja Välityspalvelun (Broker) sopimus avataan
8. Luottosuhde on valmis käyttöön

3.1. Sopimusmuutokset

Seuraavat muutokset vaativat sopimusmuutoksen:

- Sopimukselle halutaan tai sopimukselta halutaan pois vahvojen sähköisten tunnusten ketjuttaminen
- Sopimukselle halutaan lisätä tai poista rajoitus käytetyistä tunnistusvälineistä
- Sopimuksella mainittujen JWKS-URL:n ja/tai Redirect-URL:n muuttuvat tai niiden sijainnit vaihtuvat
  - Toistaiseksi metatietojen vaihtaminen ei ole automatisoitavissa - vrt. Aktia FTN OIDC-profile supplement

3.2. Laskuttaminen

Palvelun laskutus tapahtuu onnistuneesti toteutuneiden tunnistustapahtumien osalta kulloinkin voimassaolevan hinnaston mukaisesti suoraveloittamalla asiakkaan Aktiaan avaamalta pankkitililtä. Muista laskutusjärjestelyistä voidaan sopia tapauskohtaisesti.

3.3. Myötävaikuttamisvelvollisuus

Asiakkaalla on myötävaikuttamisvelvollisuus mm. osallistua ja avustaa oikea-aikaisesti ja viivyttelemättä teknisien ongelmien selvittämisessä. Lisäksi asiakkaan velvollisuutena on ilmoittaa etukäteen yhteystietojensa ja rajapintansa tai käyttämiensä teknisten ominaisuuksien olennaisesta muuttumisesta.

4. Käyttöönottovaiheet

Tekninen luottosuhde osapuolien välille muodostuu FTN OIDC -profiilin mukaisesti osapuolien julkaisemaan tekniseen metatietoon perustuen. Metatieto vaihdetaan ensimmäisen kerran sopimuksen tekemisen yhteydessä siten, että osapuolet tunnistavat toisensa luotettavasti ja varmistuvat metatiedon eheydestä ja että se on vastaanotettu oikealta sopimuksen osapuolen edustajana toimivalta lähettäjältä (**origin validation**). Osapuolet sitoutuvat pitämään toistensa saatavilla ajantasaista ja eheää tietoa sisältävää metatietoa rajapintansa teknisestä toteutuksesta.

4.1. Metatietojen vaihtaminen

Aktian tunnistuspalvelun rajapinnan metatiedot ovat välityspalvelun saatavilla. Tarkempi kuvaus on tämän palvelukuvauksen lopussa. Käytännössä, välityspalvelu toimittaa Aktialle välityspalvelunsa jwks-avainnipun ja redirect_urin. Sopimuksen tekemisen yhteydessä välityspalvelulle toteutetaan ja toimitetaan rajapinnan teknisessä yksilöimisessä käytettävä clientID. ClientID on sidottu sopimukseen ja sen käytössä pätee ne ominaisuudet, joista kussakin sopimuksessa on määritetty.

Välityspalvelun vastuulla on käynnistää avaimiensa vaihto riittävän hyvissä ajoin etukäteen siten, että vaihtoon on mahdollisuus reagoida Aktian tunnistuspalvelussa.

4.2. Tunnistuksen välityspalvelun testaus

Aktian tunnistuspalvelussa on toteutettu tekninen testausmahdollisuus. Välityspalvelulle voidaan luovuttaa erityinen clientID vain rajapinnan teknistä testausta varten. Testausta varten tarkoitetulla clientID:llä ei ole mahdollista tunnistaa todellisia käyttäjiä. Testi clienID:llä voi käyttää vain LoA-tasoa: http://ftn.ficora.fi/2017/loatest2. Testi LoA-tasoa käytettäessä palautetaan aina saman testikäyttäjän kuvitteelliset henkilötiedot. Tunnistusvastauksen acr-kentässä palautetaan testi-LoA -tason tunniste.

Testausmahdollisuus toteutetaan vain tunnistuspalveluun integroituvalle välityspalvelulle, jonka sopimusprosessi on käynnistetty. Testausrajapinnan metadatojen vaihto ja muu tekninen toteutus vastaa tuotannon liitosta ja tapahtuu samankaltaisin prosessein. Rajapinnan testaamista suositellaan ennen varsinaisen tuotantointegraation toteuttamista.

4.3. Tuotannon todentaminen (loppukäyttäjä)

Tuotanto tulee todentaa tunnistautumalla tunnistuksen välityspalvelun läpi Aktian tunnistusvälineen tarjoajan tunnuksilla.

5. Yhteystiedot ja lähteet

Tunnistuspalvelun käyttöä ja sopimuksia koskevat yhteydenotot:

– Asiakasyhteys, Carola Nyman, carola.nyman@aktia.fi

– sähköpostilla **ftn-sd@aktia.fi**

Kaikki yhteyshenkilötiedoissa tapahtuvat muutokset tulee ilmoittaa Aktian ilmoittamalle sopimuksen yhteyshenkilölle hyvissä ajoin ennen muutoksen voimaantuloa.

Aktia ilmoittaa Luottamusverkostolle muutos- ja katko töistä Luottamusverkostossa sovittujen käytänteiden mukaisesti.

5.1. Lähdeluettelo

1. Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 7.8.2009/617
   - https://www.finlex.fi/fi/laki/ajantasa/2009/20090617
2. Traficom, 72A/2018 M, annettu Helsingissä 14 päivänä toukokuuta 2018: Määräys sähköisistä tunnistus- ja luottamuspalveluista
   - https://www.kyberturvallisuuskeskus.fi/fi/sahkoinen-tunnistaminen , kohdasta Säädökset ja muut asiakirjat vahvasta sähköisestä tunnistamisesta.
3. Traficom, 213/2018 S 2018-01-26, Finnish Trust Network OpenID Connect 1.0 Protocol Profile version 1.0
   - https://www.kyberturvallisuuskeskus.fi/fi/sahkoinen-tunnistaminen , kohdasta Ohjeet ja suositukset.
4. N. Sakimura et al., OpenID Connect Core 1.0 incorporating errata set 1
   - https://openid.net/specs/openid-connect-core-1_0.html (Viitattu 7.12.2018)
5. N. Sakimura et al., OpenID Connect Discovery 1.0 incorporating errata set 1
   - https://openid.net/specs/openid-connect-discovery-1_0.html (Viitattu 10.12.2018)
6. Aktia Pankki oyj, Verkkoselain- ja laitesuositukset (Viitattu 8.5.2019)
   - https://www.aktia.fi/fi/verkkoselain-ja-laitesuositukset

6. Tekninen kuvaus – Aktia FTN OIDC-profile supplement

6.1 General

This appendix supplement procedures defined in OIDC Core and FTN OIDC specifications. Procedures enable interoperability between Identity Provider and Broker Service Provider. 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.

This document sites the same sources as the main document.

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

6.2 HTTP-protocol

This documention 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 recognised encryption and signing algorithms.

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

6.3 Metadata exchange

Parties exchange metadata, which is used to form a technical trust between parties. Authentication of the end user is only possible 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 or data in 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 as strong as was done at the time of initial subscription.

The metadata or a detail in it **MAY** be exchanged **by value** or **by reference**.

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

When the metadata is exchanged by value, the recipient **MUST** verify the integrity of the metadata in a manner that is agreed separately between parties (eg. by comparing a value returned by a cryptographic hash function). Verification **MUST** ensure that the metadata hasn't modified in the exchange and that the origin is the other party.

When the metadata is exchanged by reference the recipient **MUST** verify that the metadata is fetched from the HTTPS endpoint address agreed at the time of subcription and that the certificate used to secure the communication is trusted and valid. The recipient **MUST** verify that the domain name resolution service (DNS) used by the recipient in the metadata exchange is trustworthy and secure.

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.

The metadata of the Aktia Identity Provider

Aktia publishes the metadata of its Identity Provider by reference at the HTTPS-endpoint address as is specified regarding to OpenID Connect Discovery [5]. The endpoint address is released at the time of subscrption.

The metadata endpoint address is in form of: https://ftn.aktia.fi/.well-known/openid-configuration. Among other things, the metadata includes the jwks_uri the Broker uses to fetch the keyset of the identity provider.

The metadata of the Broker Service Provider

The Broker Service Provider releases following details for the Aktia Identity Provider:

- redirectUri
  - The endpoint address of the Broker Service Provider that is used to return authentication reply in the form of code and access_token
- jwks_uri
  - The endpoint address of the Broker Service Provider that the Aktia Identity Provider uses to fetch the keyset of the Broker
  - The keyset **MUST** include keys for encryption (**enc**) and signature (**sig**)
  - It is **RECOMMENDED** that separate keys are used for signing and encryption
  - Broker **MUST** publish the keyset on address that resides on public and static IP-address
  - Broker is **REQUIRED** to inform Aktia Identity Provider Service Desk in well advance before changing the IP-address that is used to publish the keyset
  - Unique kid's **MUST** be used

As an alternative to static IP-address of the jwks_uri, the Broker may negotiate alternative method to deliver the jwks. In this case public keys are exchanged by value. It is the responsibility of the broker to re-negotiate the update of the keys in well advance when the keyset changes. Aktia will make changes in keys only in such banking days where both preceding and following days are banking days.

6.4 Signing and encryption algorithms

FTN OIDC profile specifies the algorithms used in the FTN in signing and encryption of messages. Aktia Identity Provider implements following algorithm in signing of messages:

- RSASSA-PKCS1-v1_5 using SHA-256

Aktia Identity Provider implements following algorithm in key exchange:

- RSA-OAEP

Aktia Identity Provider implements following algorithm in encryption of the messages:

- A128GCM

Other algorithms are not implemented if not separately and specifically agreed.

6.4 Credentials used with the service

Aktia provides a clientID that Broker Service Provider uses to uniquely identify itself to Aktia Identity Provider. After signing service subscription the Broker is able to form a technical trust to Aktia Identity Provider. The published keyset specified in previous chapter is **REQUIRED** to form the technical trust between parties.

ClientID is temporary.

Authentication of the end user and fetching the personal data of the authenticated end user is not possible wihout valid clientID. ClientID **WILL BE** changed only on such banking days when both preceding and following days are banking days. Broker is **REQUIRED** to initiate changing of the clientID in well advance by contacting Aktia Identity Provider Service Desk so that new clientID can be instantiated before preceding clientID becomes outdated. While changing the clientID, the new and preceding clientID are valid concurrently so that both parties have reasonable time to react.

If reasonable doubt is expressed that the Broker SP has become compromised, the Aktia Identity Provider service **MAY BE** temporarily suspended from the Broker SP and/or the clientID **MAY BE** invalidated immediately. Taken the gravity of the situation, the clientID change 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.

6.5 Key rollover

The exchange of changed encryption and signing keys happens as is specified in Metadata Exchange chapter.

The change of signing and encryption keys is done by adding the new key to published keyset in advance of its usage. Both the new and the old keys are concurrently present in the keyset at the time of key change. The new key **MUST** be published at least n(cache) minutes before starting the use of the key. The old key **SHOULD** be removed from the keyset when the new key has been taken in to use.

A key **SHOULD** be in use at least n(cache) minutes unless reasonable doubt has been expressed that the respective private key has been compromised. If reasonable doubt has been expressed that the respective secret key has been compromised, the key **MUST** be removed from the published keyset immediately. Immediate key removal that is done because of security issues can cause disruption in service. The incident **MUST** be communicated according to service disruption processes.

6.6 Authentication Request Signature verification

While Authentication Requests **MAY** be signed, signing of Authentication Requests is **NOT REQUIRED** by Aktia Identity Provider.

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 precedense and override possible unsigned parameters.

Aktia Identity Provider returns code responses only to the redirect_uri endpoint address specified in the metadata of Broker Service Provider.

6.7 Broker authentication

Broker SP **MUST** sign Token Requests with *private_key_jwt* method according to OIDC Core and FTN OIDC Profile. Broker SP **MUST** use the corresponding key in signing the request that has been published in the metadata by type **sig**. Broker is **RECOMMENDED** to use the same signature key to sign both authentication request and Token request. If separate key is used, the metadata chapter and keyrollover chapter applies also on separate keys.

6.8 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.

6.9 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 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.

6.10 Released Personal Data

Only required attributes specified by the FTN OIDC Profile of a **natural person** are relayed and released. The Personal Identifiacation 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 can not 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 Broker Service Provider 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.

6.11 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.

6.12 Validation of Authentication Response signature

The Broker Service Provider is **REQUIRED** to verify the cryptocraphic signature of *id_token* responses. Broker Service Provider **MAY NOT** use such messages or data that cannot be verified by signatures.