1. FTN palvelukuvaus 2024

SISÄLLYSLUETTELO

1. Yleiskuvaus

Vahvan sähköisen tunnistamisen **Luottamusverkosto** (myöhemmin myös FTN) koostuu lailla [1] määritetyistä tunnistukseen luottavista **asiointipalveluista**, vahvan **tunnistusvälineen tarjoajista** ja **tunnistusvälityspalvelun tarjoajista** (Broker). Aktia toimii Luottamusverkostossa vahvojen tunnistusvälineiden liikkeellelaskijana eli tunnistuspalvelun tarjoajana. Tunnistamista tarvitseva asiointipalvelu voi siten hankkia valitsemansa tunnistusvälityspalvelun tarjoajan kautta eri tunnistuspalvelun tarjoajien tuottamat vahvat tunnistusvälineet yhdellä sopimuksella.

Palveluissa ja rajapinnoissa noudatetaan Viestintäviraston määräystä M 72 B / 2022 [2] sähköisistä tunnistus- ja luottamuspalveluista.

Aktian **tunnistuspalvelu** (FTN IdP) toteuttaa Traficomin (Viestintäviraston) suosituksen [3] (myöhemmin FTN OIDC-profiili) mukaisen OpenID Connect (myöhemmin OIDC Core) tunnistusrajapinnan (OP / IdP). Toteutus poikkeaa OIDC-määrityksestä [4] 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).

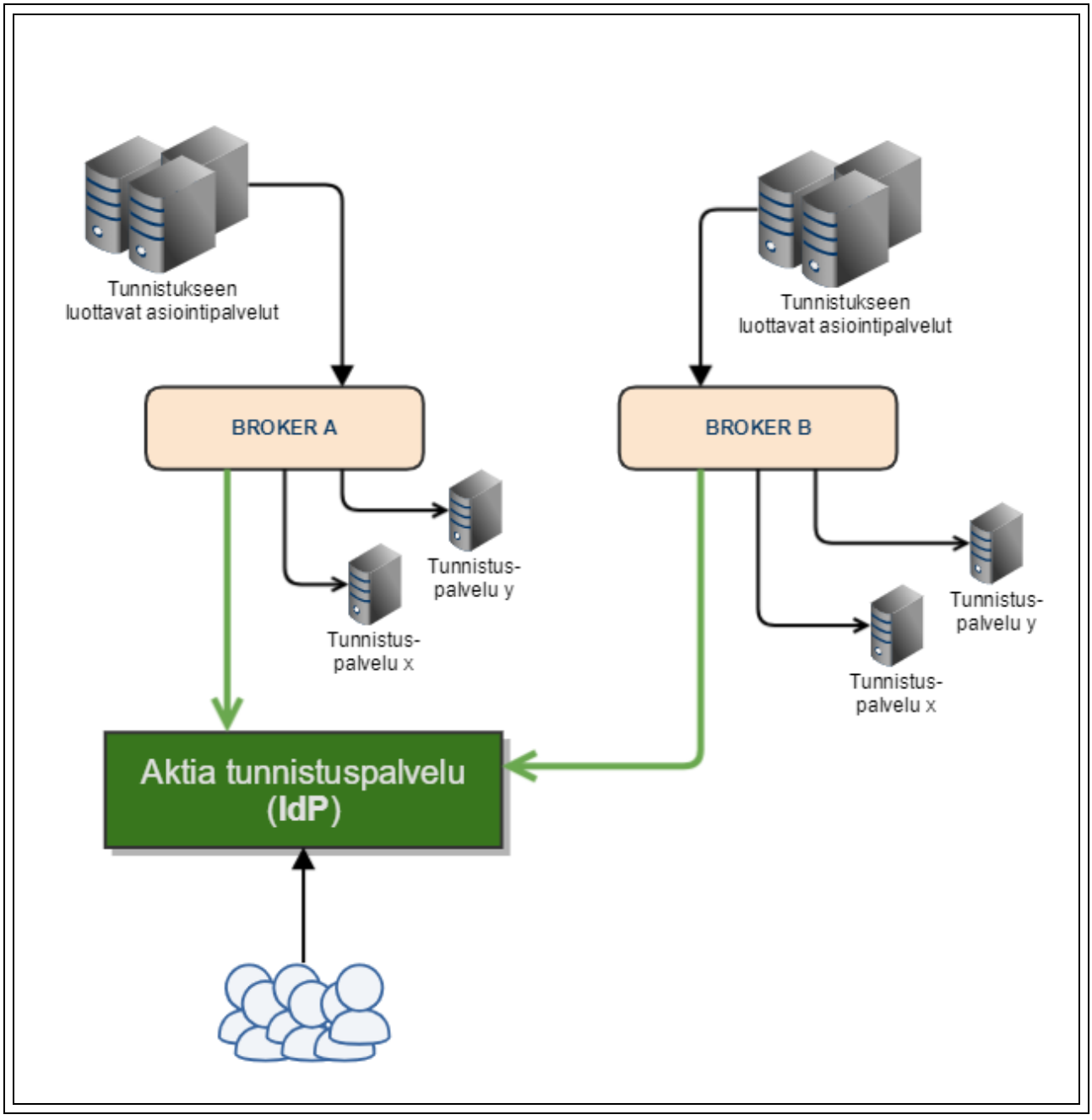
Tunnistuspalvelun teknisiä yksityiskohtia tarkennetaan erikseen tämän asiakirjan **liitteessä 1**.

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

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

Tämä palvelukuvaus koskee Luottamusverkosto tunnistuksen välityspalvelun (Broker tai asiakas) ja tunnistusvälinen tarjoajan (FTN IdP / Aktian tunnistuspalvelu tai palveluntarjoaja) välistä toimintaa, joka on kuvattu kuvassa 1 vihreillä paksuilla viivoilla.

Kuva 1 Brokerin ja Aktian IdP:n välinen yhteys

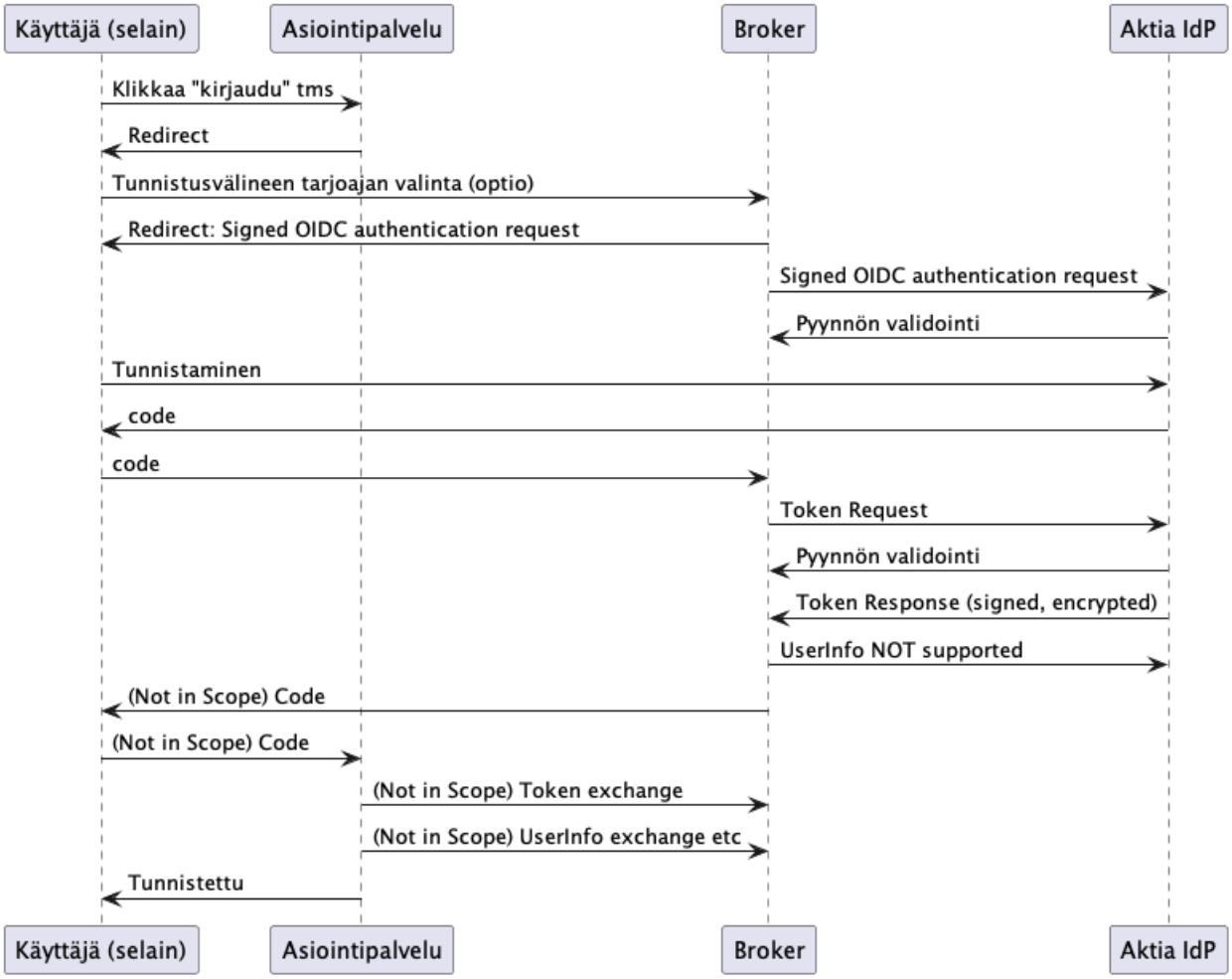


1.1. Palvelun kohderyhmä

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. Kuvassa 2 on havainnoitu tyypillinen tunnistamisen kulku sekvenssikaaviona välityspalvelun ja tunnistuspalvelun tarjoajan näkökulmasta.

Kuva 2 Tyypillinen tunnistamisen kulku FTN luottamusverkostossa



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

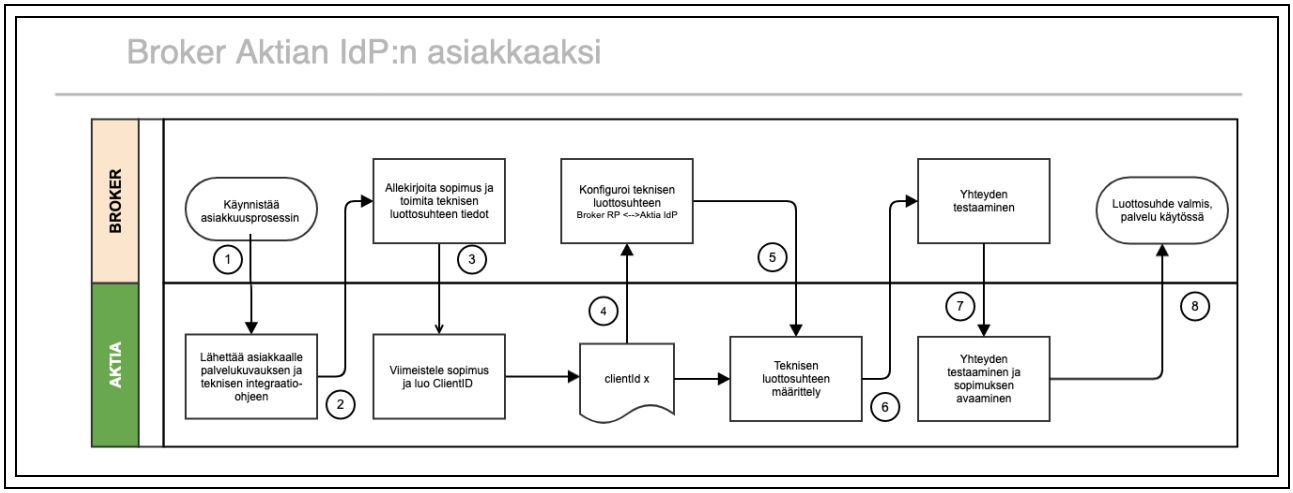
Aktian tunnistuspalvelussa noudatetaan Aktian yleisiä selainsuosituksia [6]. Käytettävän selaimen tulee tukea moderneja yleisesti käytettyjä salausalgoritmeja. Selaimen on ajantasaisesti tuettava tietoliikenteen suojausta perustuen kulloinkin markkinoilla olevien selaintoimittajien yleisesti luottamiin varmenteisiin. 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 [6]

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. Lisäksi välityspalvelu merkitsee kuhunkin yksittäiseen tunnistuspyyntöön kyseisen tunnistustapahtumatyypin FTN OIDC-profiilin mukaisesti.



Broker tulee Aktian asiakkaaksi:

1. Välityspalvelun edustaja ottaa yhteyttä Aktiaan tehdäkseen Broker-sopimuksen.
2. Broker-asiakkaalle lähetetään sopimusehtojen mukana tämä palvelukuvaus ja tekninen Aktia FTN OIDC-profile supplement 2024 määritys.
3. Broker-asiakkaan nimenkirjoitusoikeuden omaava(t) henkilö(t) käy allekirjoittamassa sopimuksen. Sopimuksen allekirjoittamisen yhteydessä vaihdetaan teknisen luottosuhteen määrittämisessä tarvittavat tiedot.
4. Aktia viimeistelee sopimuksen ja broker-asiakkaalle luodaan ClientID, joka toimii asiakkaan teknisen rajapinnan yksilöivänä tunnisteena.
5. Broker-asiakas konfiguroi teknisen luottosuhteen tiedot omaan järjestelmäänsä.
6. Aktiassa konfiguroidaan vastaanotetut teknisen luottosuhteen tiedot ja sovitaan integraation teknisestä testaamisesta.
7. Integraatio testataan ja Broker-sopimus avataan.
8. Luottosuhde on valmis käyttöön.

3.1. Sopimusmuutokset

Seuraavat muutokset vaativat myös sopimusmuutoksen:

- Sopimukselle halutaan tai sopimukselta halutaan pois vahvojen sähköisten tunnusten ketjuttaminen
- Sopimukselle halutaan lisätä tai poistaa rajoitus käytetyistä tunnistusvälineistä
- Sopimuksella mainittujen teknisten luottosuhteen tietojen muuttaminen siten, että tietojen vaihtamiseen tarvitaan luotettavaa asiakkaan todentamista
    - Teknisten luottosuhteen tietojen vaihtaminen toteutetaan profiilitarkennuksen mukaisesti: Aktia FTN OIDC-profile supplement 2024

- Mikäli teknisten luottosuhteiden tietoja ei voida teknisesti luotettavasti todentaa M72B määräyksen mukaisesti, toimitaan kuten ensimmäistä kertaa asiakkuuden luomisen ja sopimuksen allekirjoituksen yhteydessä (edellinen kappale) kohdassa 3.

3.2. Laskuttaminen

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

3.3. Myötävaikuttamisvelvollisuus

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

3.4. Tulkinnat, poikkeamat ja informointivelvoite

Luottamusverkoston toiminnan luonteesta ja viranomaisen toteuttamasta määräysten ja suositusten määrittelytavasta johtuen joitakin tulkintoja on jouduttu tekemään viranomaisen määräyksiin ja suosituksiin liittyen etenkin teknisessä toteutuksessa sekä sen perusteella, miten verkoston osapuolet ovat tehneet omia tulkintojaan määräyksistä ja suosituksista. Siltä osin, kuin tulkintoja on tehty tai poikkeamia on jouduttu toteuttamaan esimerkiksi asiakkaan teknisen toteutuksen vaatimalla tavalla, tulkinnoista ja poikkeamista sovitaan tapauskohtaisesti kirjallisesti osapuolien välillä. Aktia informoi viranomaista ja verkoston osapuolia merkittävistä poikkeamista tunnistuslain edellyttämällä tavalla ja lain edellyttämässä laajuudessa.

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 siitä, että se on vastaanotettu oikealta sopimuksen osapuolen edustajana toimivalta lähettäjältä (**origin validation**). Aktia toteuttaa asiakassuhteen luomisen yhteydessä, tai jos teknisiä luottosuhteen muodostavia tietoja ei voida luotettavalla tavalla todentaa, myös sopimuksen voimassaollessa ja tarvittaessa ajoittain, tavanomaiset asiakkaan tuntemiseen liittyvät toimenpiteet lainsäädännön edellyttämällä tavalla. Osapuolet sitoutuvat pitämään toistensa saatavilla ajantasaista ja eheää tietoa sisältävää metatietoa rajapintansa teknisestä toteutuksesta. Tarkempi rajapintakuvaus esimerkkeineen löytyy dokumentin lopusta liitteestä 1.

4.1. Metatietojen vaihtaminen

Aktian tunnistuspalvelun rajapinnan metatiedot ovat välityspalvelun saatavilla liitteessä 1 kuvatulla tavalla. Välityspalvelu toimittaa vastaavasti Aktialle välityspalvelunsa luotettavaan käyttämiseen tarvittavat tekniset metatiedot. Sopimuksen tekemisen yhteydessä välityspalvelulle toteutetaan ja toimitetaan rajapinnan teknisessä yksilöimisessä käytettävä clientID. ClientID on sidottu sopimukseen ja sen käyttöön liittyvät ne ominaisuudet, jotka kussakin sopimuksessa on määritetty.

Välityspalvelun vastuulla on huolehtia teknisten metatietojensa päivittämisestä siten, että ne voidaan teknisesti todentaa M72B -määräyksen edellyttämällä tavalla luotettavasti. Esimerkiksi protokollaviestien salaamisessa ja allekirjoittamisessa tarvittavien avaimien vaihto tehdään oikea-aikaisesti ja oikeassa järjestyksessä määritysten mukaisesti paitsi julkaistavaan metatietoon, myös asiakkaan järjestelmään.

Silloin, kun metatietoja vaihdetaan asiakkaasta aiheutuvasta tai asiakkaan teknisen toteutuksen aiheuttamasta syystä tai asiakkaan pyynnöstä tavalla, joka edellyttää Aktialta käsin tehtävää työtä ja joka ei mahdollista automaation tai asiakkaan itsepalvelukanavan käyttöä, Aktia voi veloittaa metatietojen tuottamiseen tai sen vaihtamiseen vaadittavan työn tekemisestä hinnastonsa mukaisen tuntiveloituksen.

Mikäli Aktia havaitsee asiakkaan metatiedoissa poikkeamia, jotka edellyttävät Aktialta työtä tilanteen selvittämiseksi ja tilanne aiheutuu asiakkaan laiminlyönnistä tai huolimattomuudesta, Aktia voi veloittaa selvitystyöhön, tilanteen vaatimiin toimenpiteisiin ryhtymiseen ja suorittamiseen sekä asiakkaan ja mahdollisesti viranomaisen informoimiseen käytetystä työajasta hinnastonsa mukaisen tuntiveloituksen.

4.2. Tunnistuksen välityspalvelun testaus

Aktian tunnistuspalvelussa on toteutettu tekninen testausmahdollisuus. Aktia voi toteuttaa testaamista varten erillisen IdP-instanssin erillisessä verkko-osoitteessa (nk. pre-prod instanssi). Välityspalvelulle voidaan luovuttaa erityinen clientID vain rajapinnan teknistä testausta varten.

Testausta varten tarkoitetulla clientID:llä ei ole mahdollista tunnistaa todellisia käyttäjiä. Testi clientID: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. Välityspalvelun velvollisuus on todentaa, että palautettu LoA-tason acr arvo vastaa pyydettyä ja välityspalvelun odottamaa tasoa.

Testausmahdollisuus toteutetaan vain tunnistuspalveluun integroituvalle välityspalvelulle, jonka sopimus on voimassa tai sopimusprosessi on käynnistetty. Testausrajapinnan metatietojen 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:

– Asiakasyhteysneuvonta Aktia Yritysasiakaspalvelussa puh. 010 247 6700

– sähköpostilla **ftn-sd@aktia.fi**

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

5.1. Lähdeluettelo

1. Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 7.8.2009/617
    1. https://www.finlex.fi/fi/laki/ajantasa/2009/20090617
2. Traficom/245890/03.04.05.00/2020, annettu 20.5.2022, Voimaantulopäivä 1.6.2022: *Määräys sähköisistä tunnistus- ja luottamuspalveluista (M72B/2022)*
    1. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen?toggle=Määräys%2072%20sähköisistä%20tunnistus-%20ja%20luottamuspalveluista, kohdasta *Määräys 72 sähköisistä tunnistus- ja luottamuspalveluista,* Viitattu web-sivulle 5.3.2024
3. Traficom/21543/09.02.00/2022, (213/2023 S), Finnish Trust Network OpenID Connect Protocol Profile version 2.2
    1. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen?toggle=Suositus%20213%2F2023%20S%20%28OIDC%29%20Luottamusverkoston%20rajapinnasta, kohdasta *Suositus 213/2023 S (OIDC) Luottamusverkoston rajapinnasta,* Viitattu web-sivulle 5.3.2024
4. N. Sakimura et al., OpenID Connect Core 1.0 incorporating errata set 2
    1. https://openid.net/specs/openid-connect-core-1_0.html, Viitattu web-sivulle 5.3.2024
5. N. Sakimura et al., OpenID Connect Discovery 1.0 incorporating errata set 1
    1. https://openid.net/specs/openid-connect-discovery-1_0.html (Viitattu 10.12.2018)
6. Aktia Pankki oyj, Verkkoselain- ja laitesuositukset (Päivitetty maaliskuu 2021)

1. https://www.aktia.fi/fi/turvallisuus
7. A.Å.Solberg et al., OpenID Federation 1.0 - draft 33
    1. https://openid.net/specs/openid-federation-1_0.html, Viitattu web-sivulle 5.3.2024
8. N.Sakimura et al., OpenID Connect Dynamic Client Registration 1.0 incorporating errata set 2
    1. https://openid.net/specs/openid-connect-registration-1_0.html, Viitattu web-sivulle 5.3.2024

6. LIITE 1 Luottamusverkosto Integration Guide

6.1. OIDC-profile

FTN OIDC PROFILE SUPPLEMENT