

OP Tunnistuksen välityspalvelu

Sisällys

1	Yleiskuvaus	2
2	Vaatimukset käytettävälle ohjelmistolle	3
2.1	Käyttöliittymä	3
2.2	Tuetut selaimet	3
3	Sopiminen.....	4
3.1	Sopimusmuutokset	4
4	Käyttöönoton vaiheet.....	4
4.1	Teknisten tietojen ilmoittaminen	5
4.2	Salasavainten vaihtaminen.....	6
4.3	Tunnistuksen välityspalvelun testaus.....	6
4.4	Tuotannon todentaminen	6
5	Yhteystiedot.....	6

Voit käyttää OP Tunnistuksen välityspalvelua henkilön vahvaan sähköiseen tunnistamiseen verkkopalvelussasi tai sovelluksessasi. Saat OP:sta eri tunnistuspalveluiden vahvat tunnistusvälineet yhdellä sopimuksella ja teknisellä integraatiolla.

Palvelu on osa kansallista luottamusverkostoa, joka koostuu Tunnistuspalvelun tarjoajina toimivista vahvojen tunnistusvälineiden liikkeellelaskijoista ja tunnistuksen välityspalvelun tarjoajina toimivista osapuolista. OP toimii Luottamusverkostossa tunnistuksen välityspalvelun tarjoajana.



Lisää asiointipalveluusi linkki, joka johtaa OP Tunnistuksen välityspalveluun. Linkkiin on rakennettava OIDC-rajapintakutsu integraatio-ohjeen mukaisesti.

Asiointipalvelun käyttäjä klikkaa valitsemansa tunnistuspalvelun painiketta. Tarjolla ovat ne Luottamusverkostossa mukana olevat tunnistuspalvelut, jotka on kuvattu op.fi:ssä OP Tunnistuksen välityspalvelu –sivulla.

Tunnistautuminen tapahtuu käyttäjän valitsemassa tunnistuspalvelussa, joka uudelleenohjaa käyttäjän takaisin välityspalveluun.

Välityspalvelu uudelleenohjaa käyttäjän tunnistuspalvelusta takaisin asiointipalveluun.

Tunnistautuneen käyttäjän tunnistetiedot välittyvät asiointipalveluun. Virhetapauksessa välittyy tieto virheestä.

Noudatamme palveluissa ja rajapinnoissa Traficomien määräystä 72 sähköisistä tunnistus- ja luottamuspalveluista. Määräyksen yksityiskohdat <https://www.finlex.fi/data/normit/42947/M72A-2018-M.pdf>.

OP Tunnistuksen välityspalvelu perustuu OIDC-rajapintamääritykseen (Open ID Connect). Käsittelemme palvelussa ainoastaan suomalaisia tunnistusvälineitä. Tunnistustapahtuma, joka sisältää valinnaisia attribuutteja käsitellään kuten siinä ei olisi mukana valinnaisia attribuutteja. Valinnaiset attribuutit on lueteltu Traficomien määräyksessä.

OP Tunnistuksen välityspalvelun käyttö edellyttää, että teet käytöstä sopimuksen Osuuspankin kanssa ja hyväksyt käyttöehdot. Voit ottaa välityspalvelun käyttöön sopimuksen tekemisen jälkeen. Käyttöönotto tapahtuu tämän palvelukuvausten mukaisesti.

2 Vaatimukset käytettävälle ohjelmistolle

2.1 Käyttöliittymä

Voit integroida OP Tunnistuksen välityspalvelun asiointipalveluusi kahdella eri tavalla.

1) OP:n tarjoama käyttöliittymä

Lisää asiointipalveluusi linkki, joka tekee OIDC-rajapintakutsun ja ohjaa käyttäjän OP:n tarjoamaan selainpohjaiseen responsiiviseen käyttöliittymään. Käyttöliittymä on käytettävissä suomeksi, ruotsiksi ja englanniksi. Käyttäjä valitsee tunnistuspalvelun, jossa tunnistautuu ja josta hänet uudelleenohjataan takaisin asiointipalveluun tunnistautuneena. Tunnistuspalvelussa tapahtuvissa virhetilanteissa käyttäjä ohjataan takaisin OP:n tarjoamaan käyttöliittymään.

Käyttäjälle on myös mahdollista näyttää välityspalvelussa näkymä, josta hän voi tarkistaa omat henkilötietonsa ennen uudelleenohjausta takaisin asiointipalveluun.

2) Asiointipalveluun upotettu käyttöliittymä

Asiointipalvelu tekee OIDC-rajapintakutsun ja saa vastauksena OP Tunnistuksen välityspalvelulta tunnistuspainikkeet (linkit ja kuvat) tunnistuspalveluihin, jotka asiointipalvelu upottaa omaan käyttöliittymäänsä. Tunnistuspalvelussa tapahtuvissa virhetilanteissa käyttäjä ohjataan takaisin asiointipalvelun käyttöliittymään.

Kun toteutat upotetun käyttöliittymän, tulee asiointipalvelussa mainita, että tunnistuksen välityspalvelun tuottaa OP. Ja lisäksi käyttöliittymään on lisättävä linkki välityspalvelun tietosuojaselosteeseen.

Tiedot on laitettava asiointipalveluun tässä muodossa:

OP Tunnistuksen välityspalvelun tarjoaa OP Ryhmän osuuspankit ja OP Yrityspankki Oyj.

Tietosuojaseloste (linkki osoittaa: <https://www.op.fi/tietosuoja/tietosuojaselosteet-ja-yhteystiedot/op-tunnistuksen-valityspalvelun-asiakasrekisterin-tietosuojaseloste>)

2.2 Tuetut selaimet

OP Tunnistuksen välityspalvelu toimii kaikilla yleisimmillä selainohjelmilla. Suosituksena on käyttää uusimpia selainversioita. Palvelu vaatii toimiakseen istuntoevästeiden (http session cookies) ja JavaScript -selainkriptien sallimisen selaimessa.

OP:n tarjoama käyttöliittymä on toteutettu siten, että se on mahdollisimman laajan asiakasjoukon saavutettavissa ja käytettävissä mm. avustavien teknologioiden avulla.

Tiedot tuetuista selaimista ja ohjeet evästeiden ja JavaScriptin käytöstä löydät op.fi:stä verkkopalveluiden käyttö -sivulta.

3 Sopiminen

Kun sovit OP Tunnistuksen välityspalvelun käytöstä, sinun tulee valita, mihin tarkoitukseen tulet käyttämään vahvaa sähköistä tunnistamista. Tunnistamisen lisäksi palvelua voi käyttää tunnusten ketjuttamiseen eli joko vahvojen sähköisten tunnusten myöntämiseen (saatavilla vain Luottamusverkoston jäsenille) tai asiointipalvelun omien heikkojen tunnusten myöntämiseen. Näistä kolmesta eri käyttötarkoituksesta puhutaan tässä kuvauksessa sopimustyyppinä: tunnistaminen, vahvojen tunnusten ketjuttaminen ja heikkojen tunnusten ketjuttaminen.

3.1 Sopimusmuutokset

Seuraavat muutokset vaativat sopimusmuutoksen. Jos haluat:

- lisätä tai poistaa vahvojen sähköisten tunnusten ketjuttamisen tai heikkojen tunnusten ketjuttamisen.
- rajata käytettävissä olevia tunnistusvälineitä.
- poistaa rajoituksen käytetyistä tunnistusvälineistä.

Ajantasaiset tiedot Tunnistuksen välityspalvelussa tarjolla olevista tunnistusvälineistä on op.fi:ssä.

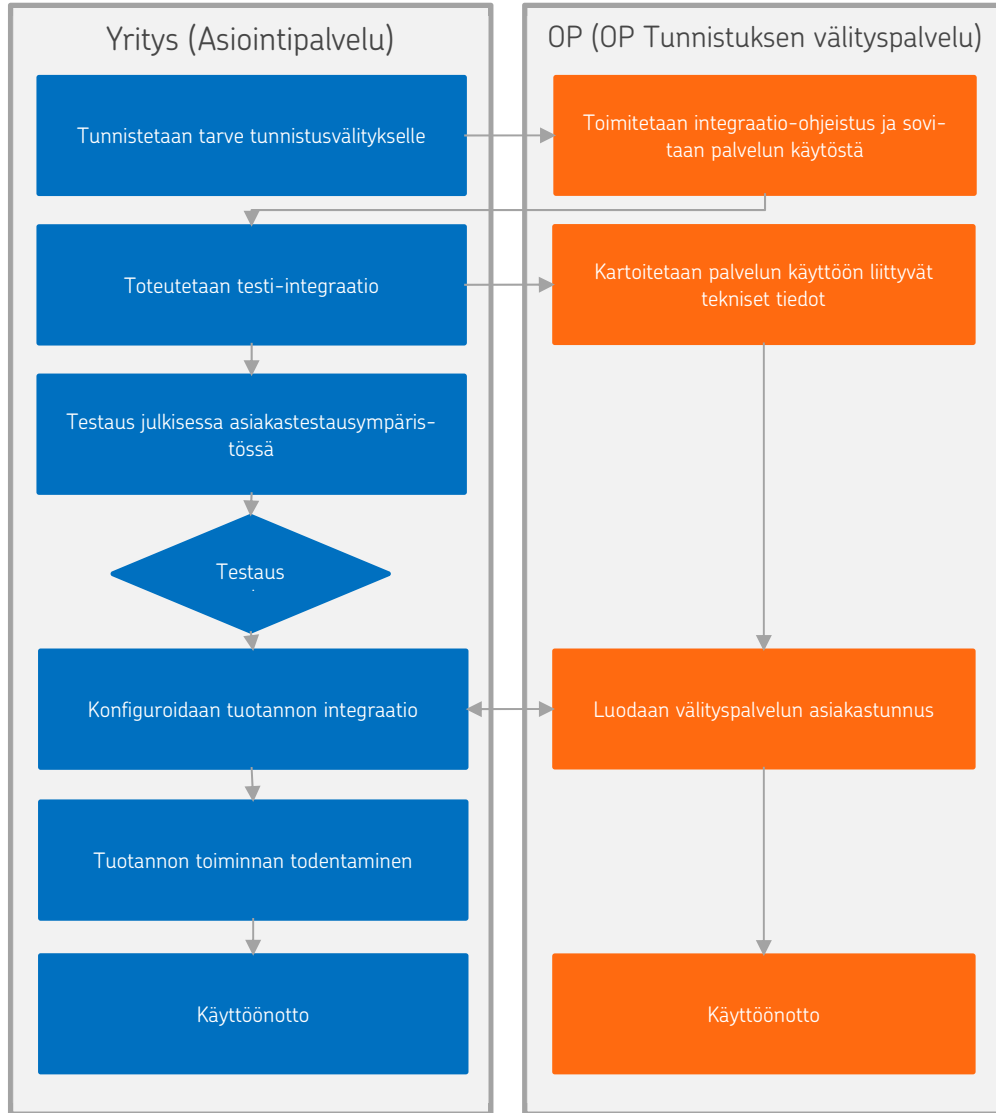
4 Käyttöönoton vaiheet

Toteuta asiointipalvelun ja OP Tunnistuksen välityspalvelun integraation julkista integraatio-ohjetta noudattamalla. Ennen integraation aloittamista, sinun kannattaa ottaa yhteyttä Osuuspankkiin sopimuksen tekoa varten.

Voit testata asiointipalvelun ja OP Tunnistuksen välityspalvelun integraatiota julkisessa asiakastestausympäristössä (Sandbox), johon kaikki asiointipalvelut integroidaan samalla julkisella testitunnuksella.

Tee sopimus palvelun käytöstä ennen tuotantokäytön aloitusta. Kartoitamme palvelun käyttöön liittyvät tekniset tiedot ja annamme asiointipalvelulle asiakastunnuksen (Client ID), jolla asiointipalvelu yksilöidään integraation rajapintakutsuissa.

Tarkempi rajapintakuvaus esimerkkeineen löytyy OP Developer sivustolta (<https://op-developer.fi/docs#Identity>).



4.1 Teknisten tietojen ilmoittaminen

Käyttöönottoa varten tarvitsemme seuraavat tiedot:

- Yrityksen nimi
- Yrityksen y-tunnus
- Asiointipalvelun OIDC JWKS end-pointin
- Listan asiointipalvelun Redirect URL:sta

Ilmoita meille asiointipalvelun tekninen yhteyshenkilö, jolle voimme lähettää lomakkeen tietojen antamista varten. Lähetämme lomakkeen suojatulla sähköpostilla. Sähköisesti täytetty lomake tulee palauttaa vastaamalla suojattuun sähköpostiin.

Tietojen toimittamisen jälkeen annamme tekniselle yhteyshenkilölle välityspalvelun asiakastunnuksen (Client ID), jolla asiointipalvelu yksilöidään integraation rajapintakutsuissa.

4.2 Salausavainten vaihtaminen

OP Tunnistuksen välityspalvelu vaihtaa rajapinnan salausavaimia säännöllisesti. Asiointipalvelu saa voimassa olevat salausavaimet OIDC JWKS-rajapinnasta automaattisesti ja sen tarkistus tulee tehdä vähintään kerran vuorokaudessa. Tarkistuksen yhteydessä asiointipalvelun tulee myös tarkistaa OP Tunnistuksen välityspalvelun TLS-varmenne.

Asiointipalvelun omat OIDC-avaimet tulee vaihtaa säännöllisesti. OP Tunnistuksen välityspalvelu saa voimassa olevat salausavaimet asiointipalvelun OIDC JWKS-rajapinnasta automaattisesti. Kun vanha avain poistetaan käytöstä, se tulee poistaa ensin asiointipalvelun JWKS-rajapinnasta vähintään vuorokautta ennen kuin avain lakkaa toimimasta.

Yrityksesi vastuulla on havaita asiointipalvelun TLS-varmenteen vanheneminen ja uusia varmenne ajoissa. Varmenteen suositeltu voimassaoloaika on kaksi vuotta ja yrityksesi vastaa sen uusimisesta. Varmenteen tulee olla yleisesti luotetun varmennepalveluntarjoajan myöntämä.

4.3 Tunnistuksen välityspalvelun testaus

OP Tunnistuksen välityspalvelun ja asiointipalvelun välistä integraatiota pääset testaamaan ensin julkisessa asiakastestausympäristössä (Sandbox). Asiakastestausympäristöön on integroitu tunnistuspalveluiden testiympäristöt eikä niissä voi tunnistautua oikeilla tunnistusvälineillä.

4.4 Tuotannon todentaminen

Tuotantoon siirryttäessä integraation toiminnan todentaminen tapahtuu tuotantoympäristössä oikeilla tunnistuspalveluilla ja -välineillä.

5 Yhteystiedot

OP Tunnistuksen välityspalvelun käyttöä koskevat yhteydenotot:

- Yritys- ja maksuliikepalvelut 0100 05151 tai
- sähköpostilla verkkopainikkeet@op.fi

Sopimusasioissa ota yhteys omaan Osuuspankkiisi.

Jos yrityksesi yhteyshenkilöt tai tiedot muuttuvat, ilmoita muutoksista OP:n yhteyshenkilölle.