25.11.2022

OP Tunnistuksen välityspalvelu

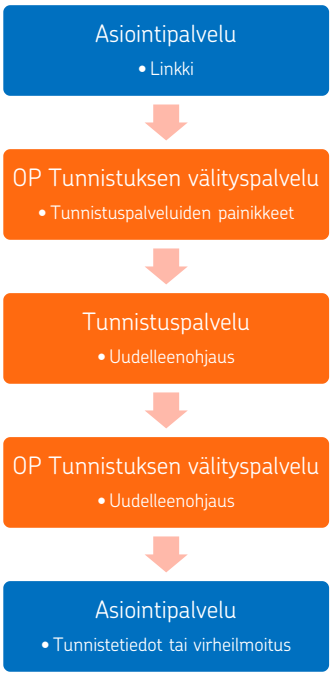
Sisällys

25.11.2022

1 Yleiskuvaus

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 Traficomin määräystä 72b sähköisistä tunnistus- ja luottamuspalveluista. Määräyksen yksityiskohdat https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen.

OP Tunnistuksen välityspalvelu perustuu OIDC-rajapintamäritykseen (OpenID Connect). Käsittelemme palvelussa ainoastaan suomalaisia tunnistusvälineitä. Tunnistustapahtuma, joka sisältää valinnaisia attribuutteja käsitellään kuten siinä ei olisi mukana valinnaisia attribuutteja. Valinnaiset attribuutit lueteltu Traficomin 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 palvelukuvauksen mukaisesti.

2 Vaatimukset käytettävälle ohjelmistolle

2.1 Käyttöliittymä

Voit integroida OP Tunnistuksen välityspalvelun asiointipalveluusi kahdella eri tavalla.

25.11.2022

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.

Toteuttaessaan upotetun käyttöliittymän tulee asiointipalvelun mainita, että tunnistuksen välityspalvelun tuottaa OP. Asiakkaalle pitää myös kertoa, että tunnistautumisen yhteydessä palveluntarjoalle välitetään henkilötunnus ja nimi, lisäksi on lisättävä linkki tunnistuksen välityspalvelun tietosuojaselosteeseen. Nämä kaikki tiedot tulevat myös rajapinnasta.

Tiedot on laitettava asiointipalveluun tässä muodossa:

Tunnistautumisen yhteydessä palveluntarjoajalle välitetään: henkilötunnus, nimi. Tietosuojaseloste OP Tunnistuksen välityspalvelun tarjoaa OP Ryhmän osuuspankit ja OP Yrityspankki Oyj.

Tietosuojaselosteen hyperlinkki osoittaa: https://isb.op.fi/privacy-info?lang=fi. Tuetut kielikoodit ovat fi, sv ja en.

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 -selainskriptien 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 sopimustyyppeinä: 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.

Ilmoitamme op.fi:ssä, jos OP Tunnistuksen välityspalveluun otetaan mukaan uusia vahvoja sähköisen tunnistuksen tarjoajia.

4 Käyttöönoton vaiheet

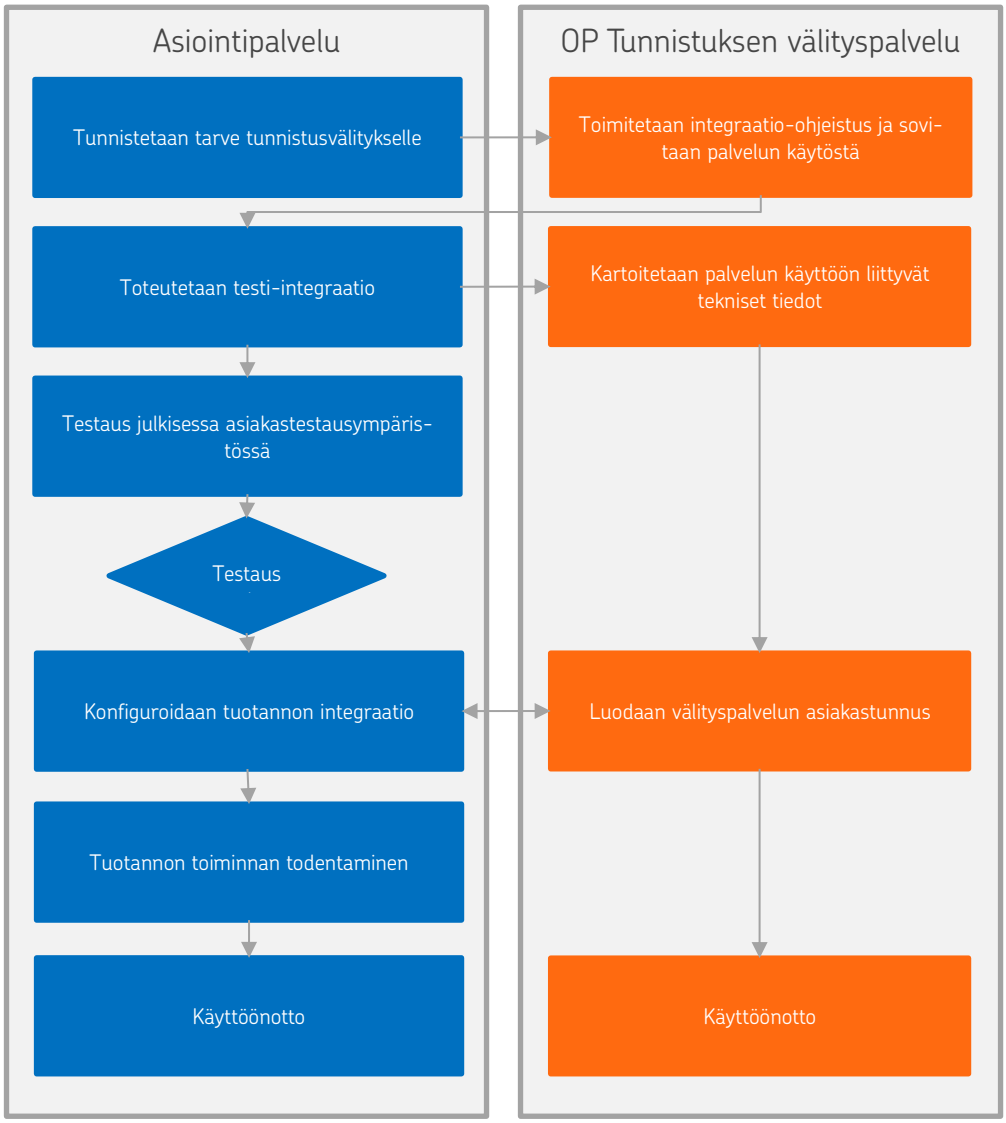
Toteuta asiointipalvelun ja OP Tunnistuksen välityspalvelun integraation julkista integraatio-ohjetta noudattamalla. Ennen integraation aloittamista, sinun kannattaa ottaa yhteyttä Osuuspankkiin sopimuksen tekoa varten.

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 alta:
https://github.com/op-developer/Identity-Service-Broker-API

25.11.2022



4.1 Teknisten tietojen ilmoittaminen

Käyttöönottoa varten tarvitsemme seuraavat tiedot:

- Yrityksen nimi
- Yrityksen y-tunnus
- OpenID entity statement
- Lisätietona tarvitsemme valinnaiset palvelusta käytettävät muut nimet (SP name teknisessä kuvauksessa)

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

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

25.11.2022

4.2 Salausavainten vaihtaminen

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

Asiointipalvelun omat OIDC-avaimet tulee vaihtaa säännöllisesti, sanomatason avaimet vähintään kahden vuoden välein. OP Tunnistuksen välityspalvelu saa voimassa olevat salausavaimet asiointipalvelun signed_jwks -rajapinnasta automaattisesti. Kun vanha avain poistetaan käytöstä, se tulee poistaa ensin asiointipalvelun signed_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 yksi vuosi 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 tunnistuspalveuiden 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.