POP PANKIN TUNNISTUSPALVELUN PALVELUKUVAUS

1.3.2019

Versio 1.0

Sisällysluettelo

Yleistä

Kun pankkitunnuksia käytetään tunnistamiseen muissa kuin tunnuksen myöntäneen pankin palveluissa, niitä koskevat vahvan sähköisen tunnistamisen vaatimukset. Näistä vaatimuksista säädetään laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista sekä Viestintäviraston sen nojalla antamassa määräyksessä. Viestintävirasto valvoo vaatimusten noudattamista.
Tunnistus- ja luottamuspalvelulain ja Viestintäviraston määräyksen vaatimukset ovat yhdenmukaisia vahvoja sähköisiä tunnistusmenetelmiä koskevan EU-sääntelyn kanssa.

Palvelu toteuttaa Viestintäviraston määräyksen 72 vahvasta sähköisestä tunnistamisesta.
Vahvaa sähköistä tunnistamista ja vahvan sähköisen tunnistamisen välitystä voivat tarjota Viestintäviraston hyväksymät palveluntarjoajat. Lista toimijoista löytyy Viestintäviraston ylläpitämästä rekisteristä.

POP Pankin tunnistuspalvelun avulla muut tunnistuspalvelun tarjoajat ja asiointipalvelut voivat välittää ja vastaanottaa POP Pankin tunnistusvälineellä tehtyjä vahvoja sähköisiä tunnistustapahtumia.

Keskeisiä termejä

Tunnistusvälineen haltija

Luonnollinen henkilö, jolla on hallussaan vahvan sähköisen tunnistamisen edellyttämä tunnistusväline, esimerkiksi tunnuslukusovellus.

Asiointipalvelu

Taho, jolle tunnistusvälineen haltija tunnistautuu. Asiointipalvelu tunnistaa käyttäjän joko tunnistusvälityspalvelun tai suoraan tunnistusvälineen tarjoajan avulla.
Esimerkiksi KELA ja verkkokaupat ovat asiointipalveluita.

Tunnistusvälityspalvelu

Palvelu, joka välittää eri tunnistusvälineillä tehtäviä vahvan sähköisen tunnistamisen tunnistustapahtumia asiointipalveluille.

Tunnistusvälineen tarjoaja

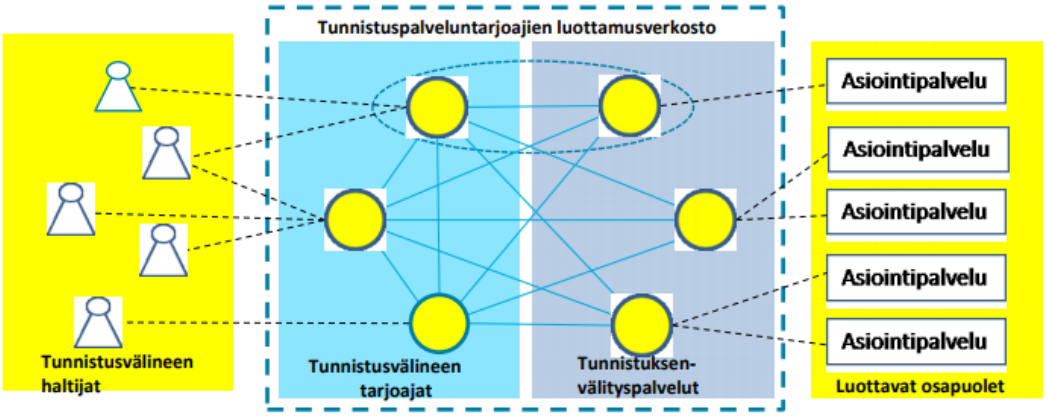
Taho, joka tarjoaa välineen vahvalle sähköiselle tunnistamiselle.
Tunnistusvälineen tarjoajalla on hallussaan tunnistusvälineen haltijan identiteettitiedot.

Viestintävirasto

Toimii valvovana viranomaisena ja valvoo, että tunnistuspalvelun tarjoajat noudattavat niille asetettuja velvollisuuksia.

Luottamusverkosto

Viestintävirastoon rekisteröityneiden tunnistuspalveluntarjoajien (tunnistusvälineen tarjoajat ja tunnistusvälityspalveluntarjoajat) verkosto, jonka tavoitteena on yhteistyössä varmistaa turvallinen sähköinen tunnistaminen.



Kuva 1. Luottamusverkosto. Lähde: Viestintävirasto

POP Pankin tunnistuspalvelu

Tunnistuspalvelu vahvistaa asiakkaan identiteetin tunnistuksenvälityspalveluille tai asiointipalveluille. POP Pankin tunnistuspalvelun tuottaa Oy Samlink Ab.

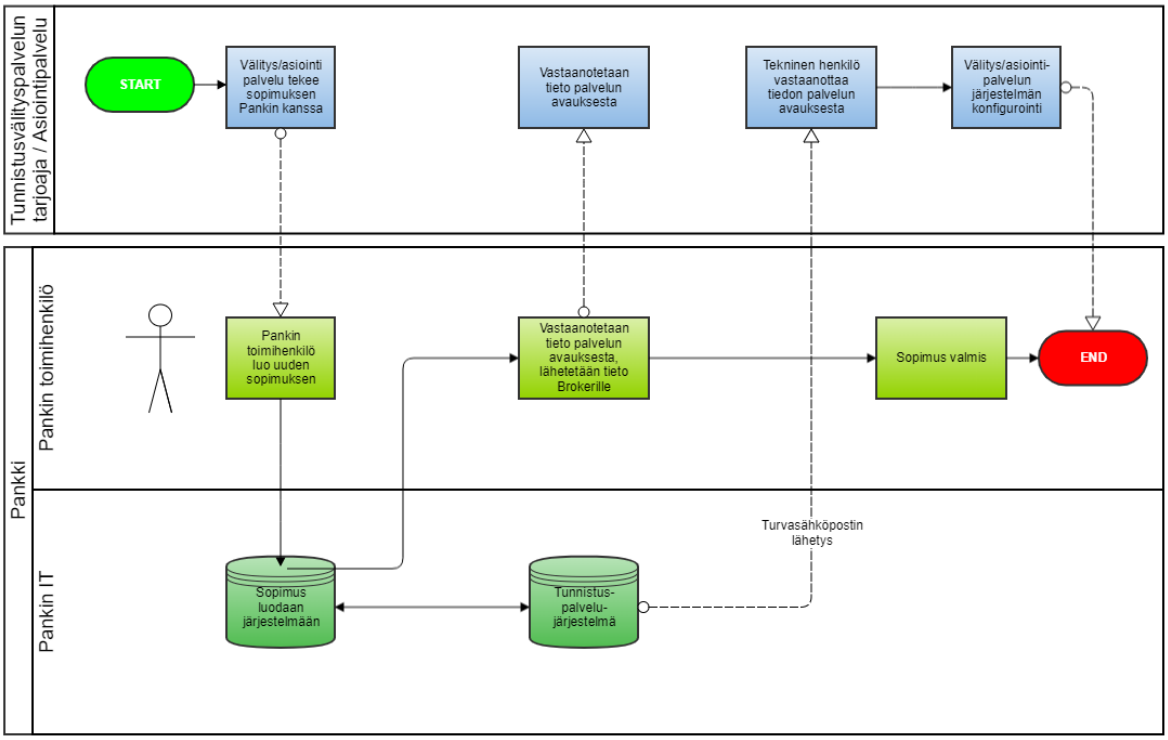
Tunnistuspalvelu perustuu OpenID Connect –pohjaiseen Luottamusverkosto- protokollaan ja se on tarkoitettu sähköisen tunnistusvälityspalvelun tarjoajille sekä asiointipalveluiden tuottajille.

Palvelun toiminnallinen kuvaus

Tässä kappaleessa kuvataan, miten tunnistuspalvelun käyttöönotto ja varsinaisen palvelun käyttö tapahtuvat.
Palvelun käyttöönoton vaiheet ovat:
- palvelusopimuksen teko POP Pankin kanssa
- julkisten allekirjoitus- ja salausavainten vaihto
- palvelun konfigurointi tunnistusvälityspalvelun tai asiointipalvelun järjestelmiin

Tunnistuspalvelun käyttö tapahtuu OpenID Connect- standardin mukaisesti, kuten alla kuvataan.

Palvelun käyttöönotto



Kuva 2. Palvelun käyttöönotto

Palvelusopimuksen teko POP Pankin kanssa

Ensimmäisessä vaiheessa v toimihenkilö tunnistaa sopimusosapuolen.
Tunnistamisen jälkeen sopimus luodaan POP Pankin järjestelmään.
Sopimus allekirjoitetaan. Sen jälkeen se toimitetaan sopimusosapuolelle. Tässä yhteydessä sopimusosapuolelle toimitetaan myös avaintenvaihtoon liittyvä tunnistuskoodi.
Sopimuksen teon myötä aktivoituu avaintenvaihtoprosessi, jossa vaihdetaan OpenID Connect- viestintään tarvittavat julkiset avaimet.

OpenID Connect salaus- ja allekirjoitusavainten vaihto

Avaintenvaihto perustuu julkisiin JWKS URI –sivuihin, jotka sisältävät molempien osapuolten julkiset allekirjoitus- ja salausavaimet.

Tunnistusvälityspalvelun tai asiointipalvelun JWKS URI –osoite luovutetaan POP Pankille sopimuksenteon yhteydessä. POP Pankin toimihenkilö tunnistaa tunnistusvälityspalvelun tai asiointipalvelun edustajan ja syöttää osoitteen sopimusjärjestelmään.

POP Pankin JWKS URI –osoite luovutetaan tunnistusvälityspalvelulle tai asiointipalvelulle sopimuksen teon jälkeen lähetetyllä turvasähköpostilla. Tunnistusvälityspalvelun tai asiointipalvelun edustaja vastaanottaa ilmoituksen turvasähköpostista tavallisena sähköpostina. Ilmoitus sisältää linkin web-sivulle, jossa viesti on luettavissa. Lisäksi vastaanottajalle lähetetään SMS-viestillä avauskoodi, jolla varsinaisen viestin pääsee lukemaan. Viesti sisältää perustiedot palvelun käyttöönottoon – JWKS URI mukaan lukien.

Tämä prosessi varmistaa JWKS URI –osoitteiden sekä avainten alkuperän.

Palvelun konfigurointi tunnistusvälityspalvelun tai asiointipalvelun järjestelmiin

Tunnistusvälityspalvelu / Asiointipalvelu vastaanottaa tunnistuspalvelun käyttöön liittyvät OpenID Connect-konfigurointitiedot samassa turvasähköpostissa kuin edellisessä kappaleessa mainitut avaimet.

Nämä tiedot sisältävät OpenID Connect Client ID:n, tunnistuksessa käytettävien kutsurajapintojen osoitteet sekä POP Pankin julkiset avaimet sisältävän JWKS URI- osoitteen.

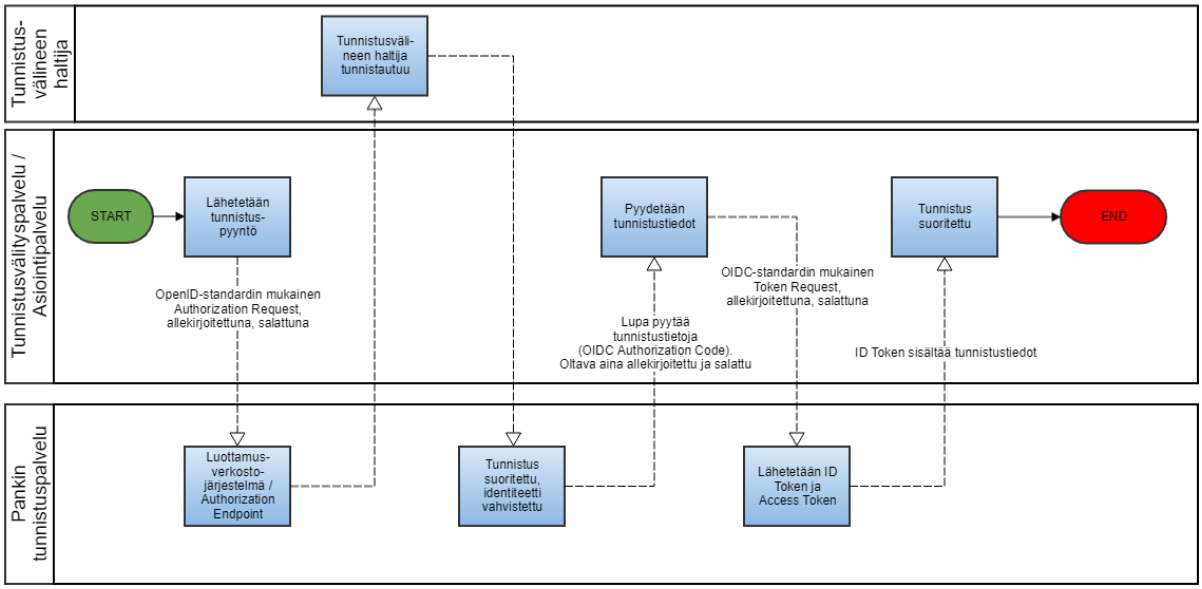
Edellämainitut tiedot konfiguroidaan Tunnistusvälityspalvelun / Asiointipalvelun järjestelmään. Järjestelmän on noudatettava OpenID Connect- standardia tunnistuksessa.

Käyttöönotetun palvelun testaus

Palvelun käyttöönottava tunnistusvälityspalvelu tai asiointipalvelu saa ohjeet tunnistuspalvelun testauksesta sopimuksen teon yhteydessä vastaanotetussa turvasähköpostissa.

Palvelun käyttö

Alla on kuvattu OpenID Connect- tunnistusprosessin eteneminen.



Kuva 3. Tunnistaminen

Palvelun sanomat ja niiden tiedot

OpenID Connect-standardi lisää identiteetin tunnistuskerroksen OAuth 2.0 protokollan päälle. OAuth 2.0 itsessään tarjoaa valtuuttamiseen liittyvät palvelut. OpenID Connect –tunnistus suoritetaan yksinkertaisen HTTPS REST –rajapinnan kautta. Kattava kuvaus OpenID Connect –protokollan toiminnasta löytyy verkkosivulta:

https://openid.net/connect/

Viestintävirasto on antamassaan suosituksessa määritellyt, kuinka Luottamusverkostossa sovelletaan OpenID Connect –standardin mukaista tunnistusta. Viestintäviraston dokumentissa määritellään Luottamusverkoston OpenID Connect –profiili ja viestinnässä käytettävät salausalgoritmit ja -avaimet.

OpenID Connect –tunnistus koostuu kolmesta vaiheesta:

1. Tunnistuspyyntö, jolla aloitetaan tunnistusprosessi
2. Tunnistusvälineen haltijan tunnistaminen
3. Valtuuspyyntö, jolla pyydetään tunnistustiedot

Seuraavissa kappaleissa kuvataan vaiheissa yksi ja kolme lähetettävät tunnistuspyyntö- ja valtuuspyyntösanomat.

Tunnistuspyyntö (OIDC authorization request)

Tunnistuspyyntö –viesti on OpenID Connect –protokollan mukainen HTTPS REST authorization request –viesti, joka lähetetään tunnistusosoitteeseen (authorization endpoint):

https://tunnistus.poppankki.fi/oxauth/restv1/authorize

Tunnistusvälityspalvelu tai asiointipalvelu uudelleenohjaa tunnistusvälineen haltijan selaimen avaamaan tunnistusosoitteen mukaisen osoitteen annetuilla parametreilla.
Osoitteen avaaminen käynnistää tunnistusvälineen haltijan tunnistusprosessin.

Kun tunnistusprosessi on suoritettu onnistuneesti tunnistusvälineen haltijan ja tunnistuspalvelun kesken, tunnistuspalvelu uudelleenohjaa tunnistusvälineen haltijan selaimen tunnistusvälityspalvelun tai asiointipalvelun uudelleenohjausosoitteeseen (redirect URI).
Tämä uudelleenohjauskutsu sisältää parametrina tunnistuspalvelun myöntämän valtuuskoodin (authorization code), jota käyttäen tunnistusvälityspalvelu tai asiointipalvelu voi hakea tunnistustiedot tunnistuspalvelusta seuraavassa kappaleessa kuvatun valtuuspyynnön kautta (token request).

Tunnistuspyyntö allekirjoitetaan aina tunnistusvälityspalvelun tai asiointipalvelun yksityisillä avaimilla ja se voidaan myös salata tunnistuspalvelun julkisilla avaimilla.

Uudelleenohjausosoitteeseen saapuva valtuutus on aina allekirjoitettu tunnistuspalvelun yksityisillä avaimilla ja salattu tunnistusvälityspalvelun tai asiointipalvelun julkisilla avaimilla.

TUNNISTUSPYYNNÖN PARAMETRIT	
request	Viestin allekirjoitus. Allekirjoitus sisältää kaksi objektia: JWTClaimsSet sekä JWSHeader. Allekirjoitus muodostetaan yksityisillä avaimilla, jotka vastaavat Luottamusverkosto-tunnistuspalvelusopimuksen luonnin yhteydessä annetun JWKS URI –sivun julkisia avaimia.
ui_locales	Palvelulta pyydetty kieli.
ftn_spname	Tunnistuspalvelujen tarjoajan tai asiointipalvelun nimi.
scope	Viestintäviraston määrittelemä OpenID Connect scope Luottamusverkostolle (= openid+ftn_hetu).
acr_values	Viestintäviraston määrittelemä Level of Assurance –asetus Luottamusverkostolle (=loa2)

response_type	Viestintäviraston määrittelemä OIDC tunnistusmetodi (authorization flow) Luottamusverkostolle (= code).
redirect_uri	Uudelleenohjausosoite, johon palataan, kun tunnistus on suoritettu. Tämän täytyy vastata osoitetta, jota käytettiin Luottamusverkosto-tunnistuspalvelusopimuksen luonnin yhteydessä.
prompt	Määrittelee, vaaditaanko tunnistusvälineen haltijalta uudelleentunnistautumista ja –valtuuttamista. Asetus 'login' edellyttää uudelleentunnistautumista.
client_id	OIDC client ID, jonka tunnistuspalvelujen tarjoaja tai asiointipalvelu vastaanottaa turvasähköpostilla Luottamusverkosto-tunnistuspalvelusopimuksen luonnin jälkeen.
Nonce	Merkkijono, joka yhdistää istunnon ja tunnistuspyynnön replay-hyökkäysten torjumiseksi.
State	Arvo, joka kytkee pyynnön ja vastauksen yhteen.

Tunnistuspyyntö -esimerkki:

https://tunnistus.poppankki.fi/oxauth/restv1/authorize?request=eyJraWQiOiIxIiwidHlwIjoiSldUIiwiYWxnIjoiUlMyNTYifQ.eyJpc3MiOiJAIUYzNjEuNDU4MC4xMDZELjA1NzEhMDAwMSE5M0JGLkY1OEUhMDAwOCFDNjNELkVGQ0EuRERDNC4zMDc1IiwicmVzcG9uc2VfdHlwZSI6ImNvZGUiLCJub25jZSI6Ik40Q3pvMTlOUGVLcU9CWUtQYm92Sk90X3BoRzAtYUV6RWVvXzUteHNxcGciLCJjbGllbnRfaWQiOiJAIUYzNjEuNDU4MC4xMDZELjA1NzEhMDAwMSE5M0JGLkY1OEUhMDAwOCFDNjNELkVGQ0EuRERDNC4zMDc1IiwiYXVkIjoiaHR0cHM6XC9cL2ktc3AtaWRwLnNhbWluZXQuZmkiLCJ1aV9sb2NhbGVzIjoiW2ZpXSIsImZ0bl9zcG5hbWUiOiJUZXN0aWthdXBwYSIsInNjb3BlIjoib3BlbmlkIGZ0bl9oZXR1IiwiYWNyX3ZhbHVlcyI6Iltsb2EyXSIsInJlZGlyZWN0X3VyaSI6Imh0dHBzOlwvXC9pLW1pc2Muc2FtaW5ldC5maVwvZ2x1dS1icm9rZXItY2xpZW50XC90b2tlbiIsInN0YXRlIjoiTXhUZVBZMnFrZzB2WVJtcUYzVUdtUnRIWTFWSEktdzd6S3dwSFNydURhOCIsImV4cCI6MTUzNzE4NDM3MywicHJvbXB0IjoibG9naW4ifQ.A5iEDPaQ9XR1jZ3XAPTJpAAgTHnKsGVPR2Gi7Ag_Uz1K8bbEPrbXEN4cs4bc85iQaf6OFsOzSnZl82NcGKBkUL35DzPVbwlwyuTnlSMx4ripp1a45RaaBvQil6lMHWnpvWt7tNnngFmiKQg91iZAQqpUZVlHh6VaVic9pBy0qkXRNFpID79oBK3okoaO3S7DiiL9o19g0caUR_CWJ7DNcsJywAqynsrs36ESzFYn5YC_7cFVdAEx4DbB7G3shJjQQ-BLFNBpTDTrrnyTYNONzBZPNe-bE396GWRT5yOpqzqlSHOWdBPnMM1iZT-rq9W1Q9Uw4NcNUnrWEPfWV6SNSA&ui_locales=fi&ftn_spname=BrokerOy&scope=openid+ftn_hetu&acr_values=loa2&response_type=code&redirect_uri= https%3A%2F%2Fwww.broker.comi%2Fbroker-oidc-client%2Ftoken&state=MxTePY2qkg0vYRmqF3UGmRtHY1VHI-w7zKwpHSruDa8&nonce=N4Czo19NPeKqOBYKPbovJOt_phG0-aEzEeo_5-xsqpg&prompt=login&client_id=%40%23F361.4580.106D.0171%210001%2163BF.F58E%210558%21C67D.EFCA.DDC4.3075

Valtuuspyyntö (OIDC token request)

Valtuuspyyntö –viesti on OpenID Connect –protokollan mukainen token request –viesti, jonka tunnistusvälityspalvelu tai asiointipalvelu lähettää valtuusosoitteeseen (token endpoint) suorana HTTPS REST –viestinä:

https://tunnistus.poppankki.fi/oxauth/restv1/token

Viestiin liitetään parametriksi tunnistuspyynnön seurauksena vastaanotettu valtuuskoodi (authorization code) ja vastauksena vastaanotetaan tunnistuskoodi (ID token) ja pääsykoodi (access token).

Viestit välitetään JSON Web Token –standardin (IETF RFC 7519) mukaisesti. JWT määrittelee JSON –tiedonsiirtomenetelmän kahden toimijan välille.

Tunnistuskoodi (ID token) on base64-koodattu, allekirjoitettu ja salattu JWE (JSON Web Encryption), joka sisältää tunnistusvälineen haltijan tunnistustiedot (claims).

Salatun ja allekirjoitetun tunnistuskoodin rakenne on:

JOSE HEADER	JWE ENCRYPTED KEY	INITIALIZATION VECTOR	CIPHERTEXT	AUTHENTICATION TAG

Jokainen elementti on pisteellä erotettu ja base64-koodattu.
JOSE lyhenne tulee sanoista Javascript Object Signing and Encryption ja viittaa IETF:n työryhmään, joka määrittelee tietoturvallista tiedonsiirtoa JWT –standardiin.

JOSE HEADER: sisältää viestin allekirjoitukseen ja salaukseen liittyvää tietoa.

JWE ENCRYPTED KEY: sisältää salatun symmetrisen avaimen varsinaisen viestin sisällön purkamiseen.

INITIALIZATION VECTOR: satunnainen numerosarja, jonka jotkin käytetyt salausalgoritmit vaativat.

CIPHERTEXT: Salattu viestin sisältö.

AUTHENTICATION TAG: Arvo, joka luodaan salausprosessin aikana ja joka varmistaa tiedon integriteetin.

Vastaanotettu tunnistuskoodi täytyy aina validoida OpenID Connect –spesifikaation mukaisesti

Valtuuspyyntö allekirjoitetaan aina tunnistusvälityspalvelun tai asiointipalvelun yksityisillä avaimilla ja se voidaan myös salata tunnistuspalvelun julkisilla avaimilla.

Valtuuspyynnön vastaus allekirjoitetaan aina tunnistuspalvelun yksityisillä avaimilla ja salataan tunnistusvälityspalvelun tai asiointipalvelun julkisilla avaimilla.

VALTUUSPYYNNÖN PARAMETRIT	
grant_type	Valtuutuksen tyyppi (= authorization code).
code	Aiemmin tunnistuspyynnön vastauksena vastaanotettu valtuuskoodi (authorization code).
redirect_uri	Uudelleenohjausosoite, johon palataan, kun valtuuspyyntö on suoritettu. Tämän täytyy vastata osoitetta, jota käytettiin Luottamusverkosto-tunnistuspalvelusopimuksen luonnin yhteydessä sekä tunnistuspyynnön yhteydessä.

VASTAANOTETUN TUNNISTUSKOODIN PARAMETRIT (ID token sisältö, payload)	
iss	Liikkeellelaskijan tunniste (issuer identifier).
sub	Yksilöllinen tunniste, joka yhdistää liikkeellelaskijan ja loppukäyttäjän (subject identifier).
aud	Toimija, jolle tämä tunnistuskoodi on luotu (audience). Tunnistusvälityspalvelun tai asiointipalvelun OIDC client id.
exp	Erääntymisaika tunnistuskoodille.
iat	Ajankohta, jolloin tunnistuskoodi luotiin.
auth_time	Tunnistusvälineen haltijan tunnistamisen ajankohta.
nonce	Merkkijono, joka yhdistää istunnon ja tunnistuskoodin replay-hyökkäysten torjumiseksi.
acr	Viestintäviraston määrittelemä Level of Assurance –asetus Luottamusverkostolle (=loa2)
amr	Tunnistusmenetelmä.
+ TUNNISTUSTIEDOT	Tunnistuspyynnön scope-parametrissa (ftn_scope Luottamusverkostossa) määritellyt tunnistustiedot (claims).

Toiminnan jatkuvuus, häiriöhallinta ja poikkeustapauksien käsittely

Palvelu toimii 24/7, poislukien suunnitellut huoltokatkokset, joista tiedotetaan POP Pankin verkkosivuilla.

Mahdollisissa ongelmatilanteissa tulee ottaa yhteyttä Samlinkin verkkopalveluiden tukeen numerossa 0100 4752 (1,17€/min+pvm) tai sähköpostilla tekninentuki@samlink.fi.

Liitteet

Samlink Finnish Trust Network OIDC security key and data exchange process between brokers and identity providers