# Handelsbankenin tunnistuspalvelun palvelukuvaus

Versio 0.2

Julkaistu 9.12.2018

# Sisällysluettelo

## Versiot

| | | |
|---|---|---|
| 0.1 | 30.10.2018 | Ensimmäinen versio |
| 0.2 | 09.12.2018 | - Kohta 6: päivitetty kuva 3<br>- Kohta 6: muutettu tuotanto-osoite (tunnistus.handelsbanken.fi)<br>- Kohta 6: ”Tunnistuspyyntö allekirjoitetaan aina tunnistusvälityspalvelun tai asiointipalvelun yksityisillä avaimilla ~~ja se voidaan myös salata tunnistuspalvelun julkisilla avaimilla~~.”<br>- Kohta 7: lisätty Samlinkin teknisen tuen yhteystieto |

# 1. YLEISTÄ

Kun pankin myöntämiä tunnistusvälineitä käytetään tunnistamiseen muissa kuin pankin omissa sähköisissä 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.

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

# 2. KESKEISIÄ TERMEJÄ

**Tunnistusvälineen haltija**

Luonnollinen henkilö, jolla on hallussaan vahvan sähköisen tunnistamisen edellyttämät tunnistusvälineet.

**Asiointipalvelu**

Taho, jolle tunnistusvälineen haltija tunnistautuu. Asiointipalvelu tunnistaa tunnistusvälineen haltijan joko tunnistusvälityspalvelun tai suoraan tunnistusvälineen tarjoajalta vastaanotetun tunnistustapahtuman avulla.

**Tunnistusvälityspalvelu**

Palvelu, joka välittää eri tunnistusvälineillä tehtäviä vahvan sähköisen tunnistamisen tunnistustapahtumia asiointipalveluille. Tunnistusvälityspalvelun tarjoajan on kuuluttava vahvan sähköisen tunnistamisen luottamusverkostoon.

**Tunnistusvälineen tarjoaja**

Taho, joka tarjoaa luonnolliselle henkilölle välineet vahvalle sähköiselle tunnistamiselle.

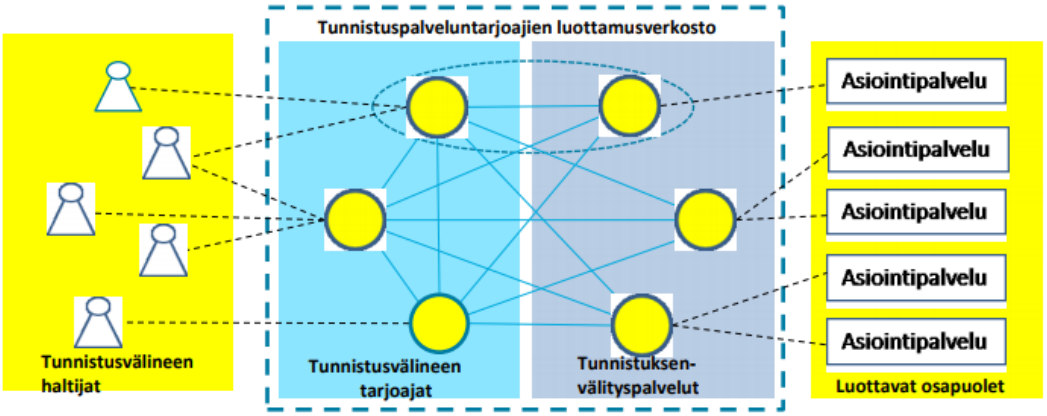
Tunnistusvälineen tarjoajalla on hallussaan tunnistusvälineen haltijan identiteettitiedot. Tässä palvelukuvauksessa kuvatussa palvelussa Handelsbanken on tunnistusvälineen tarjoaja.

**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

# 3. HANDELSBANKENIN TUNNISTUSPALVELU

Tunnistuspalvelu vahvistaa asiakkaan identiteetin tunnistuksenvälityspalveluille tai asiointipalveluille. Tunnistuspalvelun käyttö edellyttää sopimusta Handelsbankenin kanssa.

Handelsbankenin tunnistuspalvelun palvelun tuottaa Oy Samlink Ab.

Tunnistuspalvelu perustuu Viestintäviraston OpenID Connect -pohjaiseen Luottamusverkosto-kuvaukseen. Se on tarkoitettu sähköisen tunnistusvälityspalvelun tarjoajille sekä asiointipalveluiden tuottajille.

# 4. PALVELUN TOIMINNALLINEN KUVAUS

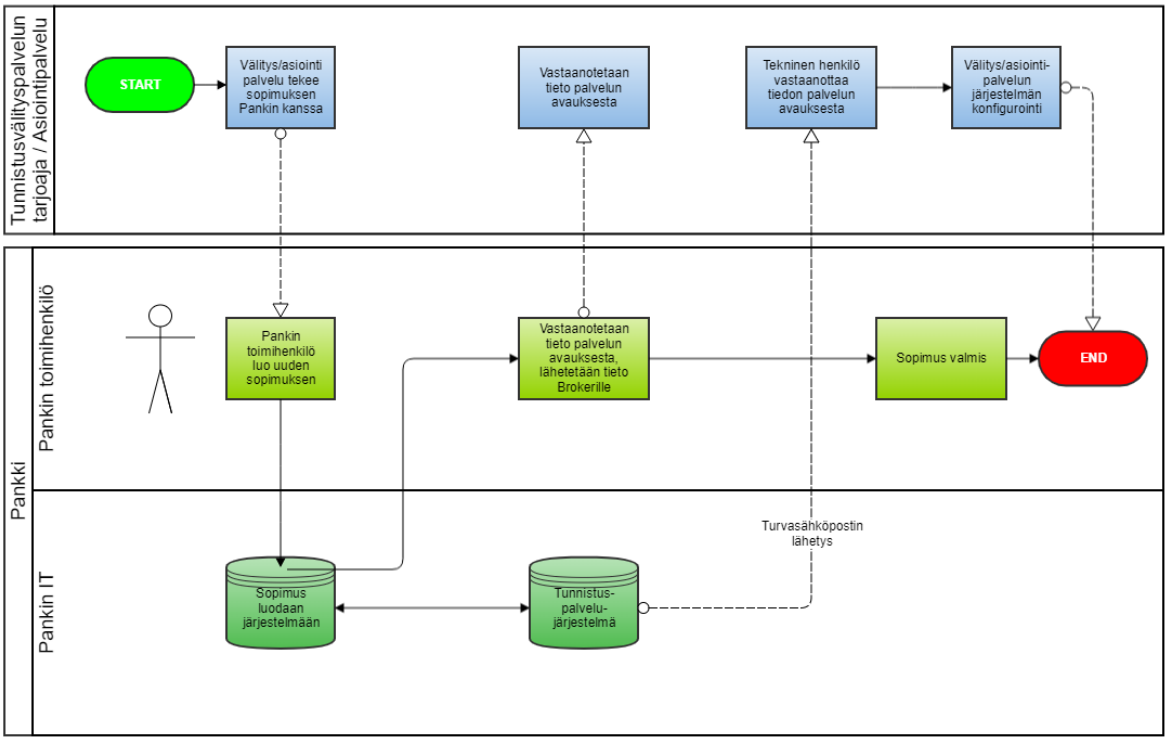
Tässä kappaleessa kuvataan tunnistuspalvelun käyttöönotto.

Palvelun käyttöönoton vaiheet ovat:

- palvelusopimuksen teko Handelsbankenin kanssa
- julkisten allekirjoitus- ja salausavainten vaihto
- palvelun konfigurointi tunnistusvälityspalvelun tai asiointipalvelun järjestelmiin

Tunnistuspalvelun käyttö tapahtuu OpenID Connect- standardin mukaisesti.

# 5. PALVELUN KÄYTTÖÖNOTTO




Kuva 2. Palvelun käyttöönotto

## PALVELUSOPIMUS HANDELSBANKENIN KANSSA

Ensimmäisessä vaiheessa Handelsbankenin toimihenkilö tekee sopimuksen tunnistuspalvelusta tunnistusvälityspalvelun tai asiointipalvelun kanssa.

Sopimuksen yhteydessä sopimusosapuolelle toimitetaan avaintenvaihtoon liittyvä tunnistuskoodi.

Sopimus käynnistää avaintenvaihtoprosessin, 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 ilmoitetaan Handelsbankenille sopimuksenteon yhteydessä.

Handelsbankenin 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.

Prosessilla varmistetaan JWKS URI -osoitteiden sekä avainten alkuperä.

### Palvelun konfigurointi tunnistusvälityspalvelun tai asiointipalvelun järjestelmiin

Tunnistusvälityspalvelu tai asiointipalvelu vastaanottaa tunnistuspalvelun käyttöön liittyvät OpenID Connect- konfigurointitiedot samassa turvasähköpostissa kuin edellisessä kohdassa mainitut avaimet.

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

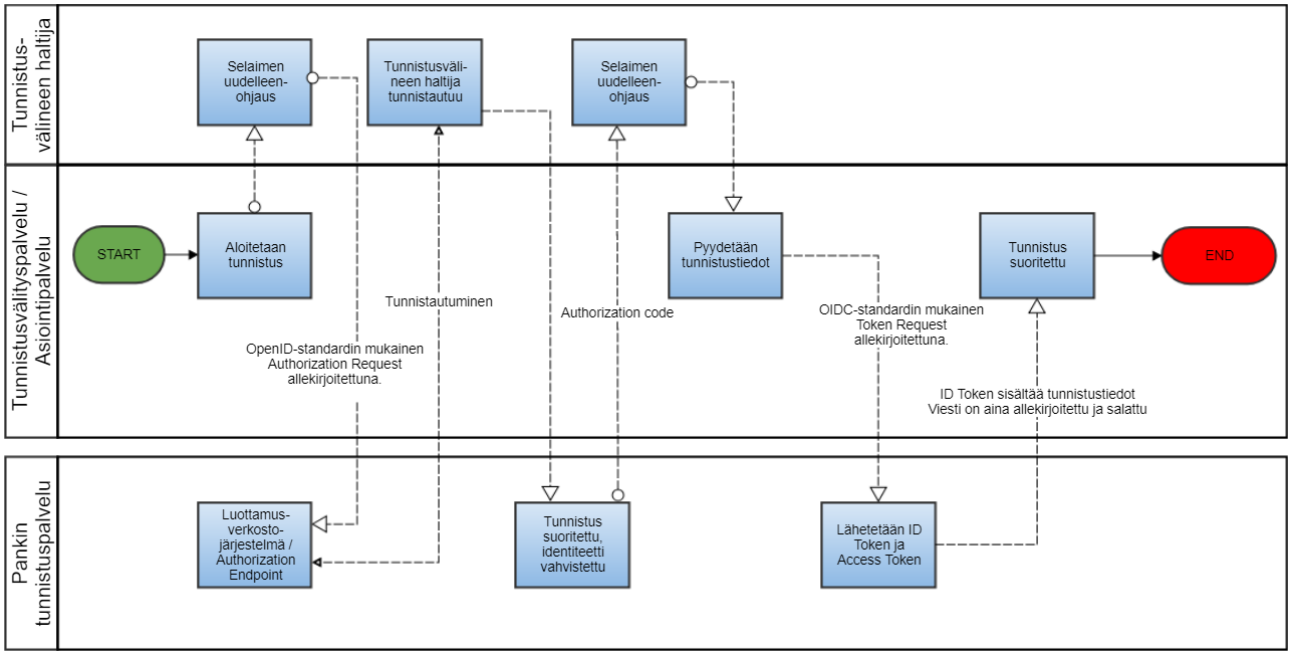
Tunnistusvälityspalvelu tai asiointipalvelu konfiguroi edellä mainitut tiedot tunnistusvälityspalvelun tai Asiointipalvelun järjestelmään. Järjestelmän on noudatettava OpenID Connect -standardia.

### Palvelun testaus

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

# 6. 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 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.handelsbanken.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.

| **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 (http://ftn.ficora.fi/2017/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.handelsbanken.fi/oxauth/restv1/authorize?request=eyJraWQiOiIxIiwidHlwIjoiSldUIiwiYWxnIjoiUlMyNTYifQ.eyJpc3MiOiJAIUYzNjEuNDU4MC4xMDZELjA1NzEhMDAwMSE5M0JGLkY1OEUhMDAwOCE3OEUzLjQ3MzYuMTlDNC5BRUYwIiwicmVzcG9uc2VfdHlwZSI6ImNvZGUiLCJub25jZSI6IkpuTXRLZGtSLVlTd3pZVnRtVzNkSUtKZnAtMUgtLTRvbldoNHZLNGRRbTQiLCJjbGllbnRfaWQiOiJAIUYzNjEuNDU4MC4xMDZELjA1NzEhMDAwMSE5M0JGLkY1OEUhMDAwOCE3OEUzLjQ3MzYuMTlDNC5BRUYwIiwiYXVkIjoiaHR0cHM6XC9cL2ktc3AtaWRwLnNhbWluZXQuZmkiLCJ1aV9sb2NhbGVzIjoiW2ZpXSIsImZ0bl9zcG5hbWUiOiIiLCJzY29wZSI6Im9wZW5pZCBmdG5faGV0dSIsImFjcl92YWx1ZXMiOiJbaHR0cDpcL1wvZnRuLmZpY29yYS5maVwvMjAxN1wvbG9hMl0iLCJyZWRpcmVjdF91cmkiOiJodHRwczpcL1wvaS1taXNjLnNhbWluZXQuZmlcL2dsdXUtYnJva2VyLWNsaWVudFwvdG9rZW4iLCJzdGF0ZSI6IldwdGZaUlBfd3g2Z0VSSWZtaFpxa1AtN0RDSTFBV3RRTjZzaW1zMXk0WlEiLCJleHAiOjE1NDI2MTg5ODMsInByb21wdCI6ImxvZ2luIn0.uqOEJZ49cOCnwU0paQfBjOQvdx7zLmivcm1-9rKztHNbF9GH-PbSOlMPZX2z3SQjIa6dADJRI8WAk37-QQPX6_q9wHwOasCtrUIK00_6LQW8fRdi92JKGe76lLuZZK9XSantsXdE0td_czzRqJYpgV79SbYqoz8hf17SyS_JlMJTNQuloDO5T2m12qTQRiI2gSR2UAjKBJNFGka49Zo5DscMpWReaeiJ4-jBuV0cGbR1DVBssSZjQ6SEp6W8TL3Nh8ELZePrr5Dwn9NeL8DbjTKulZF10vAM8q1AUKsionmU3MU5DvEM4ER-zq6ocNlCX58IaK4myPYAqYm9NTA1vw&ui_locales=fi&ftn_spname=&scope=openid+ftn_hetu&acr_values=http%3A%2F%2Fftn.ficora.fi%2F2017%2Floa2&response_type=code&redirect_uri=https%3A%2F%2Fi-misc.saminet.fi%2Fgluu-broker-client%2Ftoken&state=WptfZRP_wx6gERIfmhZqkP-7DCI1AWtQN6sims1y4ZQ&nonce=JnMtKdkR-YSwzYVtmW3dIKJfp-1H--4onWh4vK4dQm4&prompt=login&client_id=%40%21F361.4580.106D.0571%210001%2193BF.F58E%210008%2178E3.4736.19C4.AEF0

## 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.handelsbanken.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 -määritysten mukaisesti

Valtuuspyyntö allekirjoitetaan aina tunnistusvälityspalvelun tai asiointipalvelun yksityisillä 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). |

# 7. TOIMINNAN JATKUVUUS, HÄIRIÖHALLINTA JA POIKKEUSTAPAUKSIEN KÄSITTELY

Palvelu toimii 24/7, pois lukien suunnitellut huoltokatkokset, joista tiedotetaan Handelsbankenin verkkosivuilla.

Mahdollisissa ongelmatilanteissa tulee ottaa yhteyttä Handelsbankenin asiakastukeen.

**Yritysten maksuliikennepalvelujen asiakaspalvelu**

Palveluaika: arkipäivinä klo 8.00 - 17.00
Puhelin: 010 444 2545
Sähköposti: finhelp@handelsbanken.fi

Samlink Oy:n tekninen tuki myös suoraan: tekninentuki@samlink.fi

# 8. LIITTEET

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