PANKKI

TUNNISTUSPALVELUN PALVELUKUVAUS OIDC

PALVELUKUVAUS JA SOVELTAMISOHJE

29.6.2022

SISÄLLYSLUETTELO

1 YLEISTÄ

Tässä palvelukuvauksessa määritellään palveluntarjoajalle tunnistuspalvelun käyttöönoton edellytykset sekä tietuekuvaukset tunnistuspalvelun käyttöönottoon liittyen. S-Pankin tunnistuspalvelussa pankki tunnistaa luotettavasti palveluntarjoajan puolesta sähköisesti asioivat asiakkaat. Tunnistuspalvelu on toteutettu Liikenne- ja Viestintäviraston määrittelemän Luottamusverkosto -protokollan mukaan, joka pohjautuu OpenID Connect -protokollaan ja se on tarkoitettu sähköisen tunnistusvälityspalvelun tarjoajille sekä asiointipalveluiden tuottajille, jatkossa asiakas. Tunnistuspalvelun rajapinta on toteutettu vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain (2009/617) 12 a §:n 2 momentin ja Liikenne- ja Viestintäviraston antamaan OpenID Connect 1.0 rajapintasuositukseen perustuen.

2 YLEISKUVAUS

S-Pankin antama tunniste on ainutlaatuinen ja sidottu sekä palveluntarjoajan kyseiseen palvelutapahtumaan että asiakkaaseen. Asiakkaan tunnistus tapahtuu samoilla pankkitunnisteilla, joita asiakas käyttää S-Pankin omissa palveluissa. Kun palveluntarjoajalla on tarve tunnistaa asiakkaansa, palveluntarjoaja lähettää tunnistuspyynnön asiakkaalle, joka siirtyy S-Pankin tunnistuspalveluun painamalla pankin tunnistuspainiketta.

Palveluntarjoajan tunnistuspyyntö välittyy asiakkaalta S-Pankin tunnistuspalveluun, joka lähettää tunnistamisen jälkeen asiakkaalle vastaussanoman. Asiakas tarkistaa vastaussanoman tiedot, joiden hyväksymisen jälkeen hän palaa takaisin palveluntarjoajan palveluun. Asiakas voi halutessaan peruuttaa tai hylätä tunnistustapahtuman joko ennen tunnistautumista tai vastaussanoman tarkistamisen jälkeen. Asiakkaan keskeyttäessä tunnistustapahtuman asiakkaan tiedot eivät välity palveluntarjoajalle.

Tunnistuspalvelussa välitettäviä tunnistustietoja voidaan käyttää myös osana sähköisen allekirjoituksen muodostamista tunnistautuvan asiakkaan ja palveluntarjoajan niin sopiessa. S-Pankki kuitenkin huolehtii ainoastaan tässä palvelukuvauksessa mainitulla tavalla asiakkaan tunnistamisesta eikä vastaa asiakkaan ja palveluntarjoajan välisen oikeustoimen sitovuudesta tai sisällöstä.

Tunnistuspalvelu on käytettävissä 24 tuntia kaikkina viikonpäivinä, pois lukien huollosta, päivityksestä tms. syystä johtuvista katkoajoista.

Pankkitunnuksilla tunnistautuessa muissa kuin S-Pankin palveluissa, niitä koskevat vahvan sähköisen tunnistamisen vaatimukset lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista sekä Liikenne- ja Viestintäviraston lain nojalla antamista määräyksistä. Liikenne- ja Viestintäviraston tehtävänä on valvoa tämän lain noudattamista.

Palvelun käyttöönoton edellytykset:
1) palvelusopimuksen teko S-Pankin kanssa
2) julkisten allekirjoitus- ja salausavainten vaihto
3) palvelun konfigurointi tunnistusvälityspalvelun tai asiointipalvelun järjestelmiin

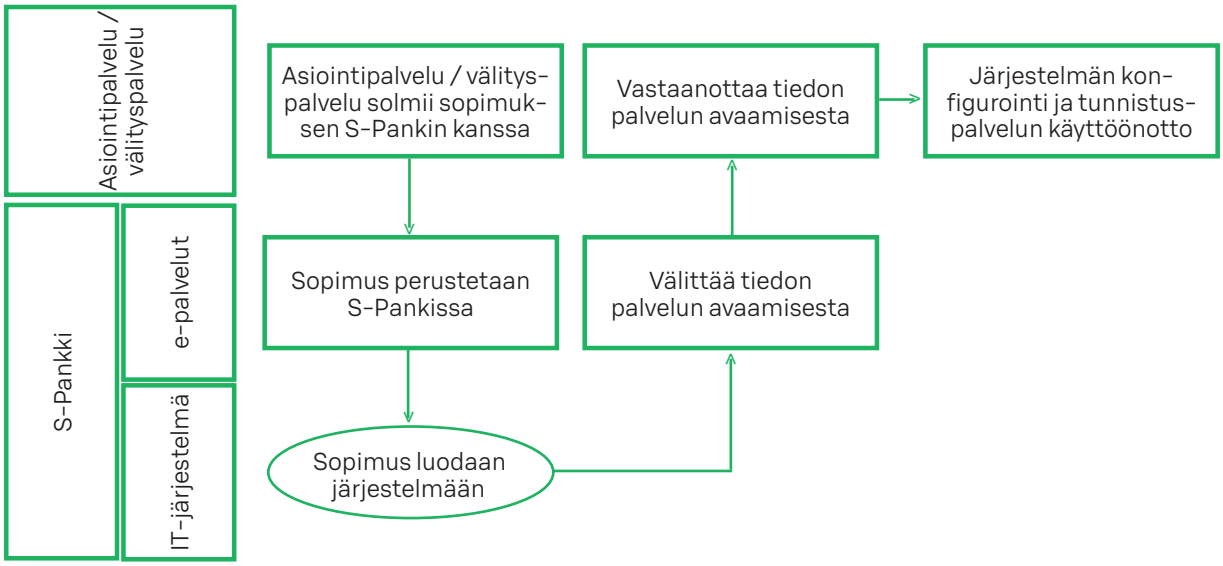
Tunnistuspalvelun käyttö tapahtuu OpenID Connect-standardin mukaisesti.

OpenID Connect –tunnistus tapahtuu vaiheittain:
1. Tunnistuspyyntö, jolla aloitetaan tunnistusprosessi
2. Tunnistusvälineen haltijan tunnistaminen
3. Valtuuspyyntö, jolla pyydetään tunnistustiedot

OpenID Connect-standardin avulla lisätään identiteetti OAuth 2.0 protokollan päälle. OAuth 2.0 protokolla tarjoaa valtuuttamiseen liittyvät palvelut. OpenID Connect –tunnistus tehdään HTTPS REST –rajapinnan kautta.

Lisätietoja teknisen rajapinnan konfiguroinnista e-palvelut@s-pankki.fi

Kuva 1: Tunnistuspalvelun käyttöönotto



3 SOPIMUKSET

Palveluntarjoajan on tehtävä S-Pankin kanssa kirjallinen sopimus tunnistuspalvelun käytöstä. Palveluntarjoajan tiedot rekisteröidään pankissa ja sopimuksessa mainitulle yhteyshenkilölle lähetetään salaus- ja allekirjoitusavaimet salatulla sähköpostilla.

Palveluntarjoaja vastaa siitä, että sillä on EU:n yleisen tietosuoja-asetuksen (GDPR) mukainen peruste käsitellä henkilöiden nimiä, syntymäaikoja ja henkilötunnuksia.

Palveluntarjoajan tulee ilmoittaa S-Pankille, jos hänen palveluunsa tai tietoihinsa tulee muutoksia. S-Pankki täydentää tarvittaessa sopimusta muuttuneilla tiedoilla.

4 TUNNISTUSPALVELUSSA KÄYTETTÄVÄ S-PANKIN PAINIKE

Palveluntarjoajan verkkopalvelussa tunnistuspalvelun käyttö on ilmaistava S-Pankin verkkopalvelutunnuksella ja sen on oltava selvästi näkyvillä. Toimintopainikkeena käytetään kyseistä tunnusta.

S-Pankin tunnistuspalvelupainikkeen kuvatiedosto on noudettavissa S-Pankin internet-sivuilta. Painikkeen kokoa tai värejä ei saa muuttaa, tehdä itse tai muotoilla. Painikkeen kuvaa ei saa käyttää muuhun tarkoitukseen kuin mitä palveluntarjoajan ja S-Pankin välisessä sopimuksessa on sovittu.

S-Pankissa palvelun nimi on tunnistuspalvelu (identifieringstjänst). S-Pankin nimeä ei myöskään saa muokata tai jakaa useammalle riville.

5 OPENID CONNECT SALAUS- JA ALLEKIRJOITUSAVAINTEN VAIHTO

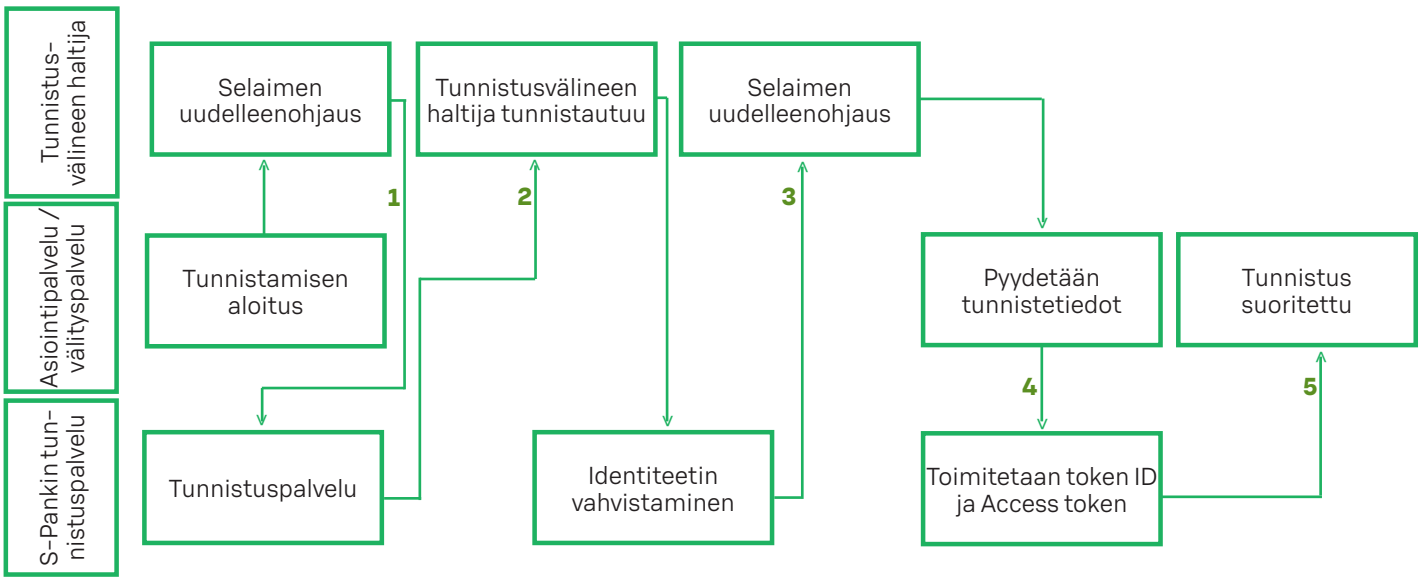
Palveluntarjoajan tulee luoda salausavain ja lähettää avaimen julkinen osa (public key) pem-muodossa salatulla sähköpostilla S-Pankille. S-Pankin viestintä tapahtuu sähköpostiosoitteen e-palvelut@s-pankki.fi kautta. S-Pankki muodostaa allekirjoitusavaimen ja toimittaa palveluntarjoajalle avaimen julkisen osan salatulla sähköpostilla.

6 PALVELUN KONFIGUROINTI TUNNISTUSVÄLITYSPALVELUN TAI ASIOINTI PALVELUN JÄRJESTELMIIN

Asiakas vastaanottaa tunnistuspalvelun käyttöön liittyvät OpenID Connect- konfigurointitiedot samassa salatussa sähköpostissa kuten edellisessä kappaleessa mainitut avaimet tunnistuspalvelun käyttämiseksi. Asiakkaan tulee konfiguroida annetut tiedot omaan järjestelmäänsä S-Pankin tunnistuspalvelun hyödyntämiseksi.

Kuvassa 2 on esitetty tunnistustapahtuman vaiheet:
1. Tunnistuspyyntö allekirjoitettuna (authorization request)
2. Tunnistautuminen
3. Tunnistuskoodi (authorization code)
4. Tunnistustapahtuman koodin pyyntö allekirjoitettuna (token request)
5. ID token tunnistetiedoilla allekirjoitettuna/salattuna

Kuva 2: Tunnistustapahtuma



7 TUNNISTUSPYYNTÖ (OIDC AUTHORIZATION REQUEST)

Tunnistuspyyntö on OpenID Connect –protokollan mukainen HTTPS REST authorization request -viesti, joka lähetetään tunnistusosoitteeseen (authorization endpoint): https://online.s-pankki.fi/ftn/authorize

Asiointipalvelu tai välityspalvelu uudelleenohjaa tunnistusvälineen haltijan selaimen avaamaan tunnistusosoitteen mukaisen osoitteen annetuilla parametreilla. Osoitteen avaaminen käynnistää tunnistusvälineen haltijan tunnistusprosessin S-Pankin tunnistuspalvelussa.

S-Pankin tunnistuspalvelussa tunnistusvälineen haltijan onnistuneen tunnistautumisen jälkeen uudelleenohjataan tunnistusvälineen haltijan selain asiointipalvelun tai välityspalvelun uudelleenohjausosoitteeseen (redirect URI). Uudelleenohjauskutsu sisältää parametrina tunnistuspalvelun myöntämän valtuuskoodin (authorization code), jota käyttäen asiointipalvelu tai välityspalvelu voi hakea tunnistustiedot S-Pankin tunnistuspalvelusta valtuuspyynnön kautta (token request). Tunnistuspyyntö allekirjoitetaan aina asiointipalvelun tai välityspalvelun yksityisillä avaimilla.

8 VALTUUSPYYNTÖ (OIDC TOKEN REQUEST)

Valtuuspyyntö on OpenID Connect –protokollan mukainen token request -viesti, jonka asiointipalvelu tai välityspalvelu lähettää valtuusosoitteeseen (token endpoint) suorana HTTPS REST -viestinä. Viestin parametriksi liitetään 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). Elementit ovat pisteillä erotetut ja base64 koodatut.

Vastaanotettu tunnistuskoodi tulee aina validoida OpenID Connect -spesifikaation mukaisesti. Valtuuspyyntö allekirjoitetaan aina asiointipalvelun tai välityspalvelun yksityisillä avaimilla. Valtuuspyyntö allekirjoitetaan aina S-Pankin tunnistuspalvelun yksityisillä avaimilla ja salataan asiointipalvelun tai välityspalvelun avaimilla.

9 ASIAKASTIEDOT

UserInfo-päätepiste on OAuth 2.0 -suojattu resurssi, joka palauttaa todennettua loppukäyttäjää koskevat vaatimukset. Saadakseen loppukäyttäjää koskevat pyydetyt vaatimukset, asiakas tekee pyynnön UserInfo-päätepisteelle käyttämällä OpenID Connect -todennuksella saatua käyttöoikeustunnusta.

UserInfo-päätepiste ei ole pakollinen toteutus, se on yksi käytettävissä olevista päätepisteistä osana FTN-toteutusta. FTN-toteutusta käyttävien asiakkaiden on päätettävä, haluavatko he käyttää tätä päätepistettä.

10 TUNNISTUSPALVELUN TESTAUS

Sopimuksen teon yhteydessä lähetetyssä turvasähköpostissa asiakas saa ohjeet tunnistuspalvelun testauksesta.

11 POIKKEUSTILANTEET

Palveluntarjoajan on varauduttava poikkeustilanteisiin, joita voivat olla:

1. Asiakas keskeyttää tunnistustapahtuman. Asiakas voi keskeyttää tapahtuman joko ennen tunnisteen välittämistä S-Pankin tunnistuspalveluun tai tunnisteen luonnin jälkeen peruuta-painikkeella.
2. Asiakkaan todennus epäonnistuu, joko asiakkaan antamien tunnistetietojen virheellisyyden takia tai koska asiakas on pyytänyt todennusta väärästä pankista. Asiakas palaa palveluntarjoajan palveluun peruuta-painikkeella.
3. S-Pankki havaitsee virheen tunnistuspyynnössä. S-Pankki havaitsee ennen asiakkaan todennusta tunnistuspyynnössä virheen. Asiakas palaa palveluntarjoajan palveluun.
4. Palveluntarjoaja havaitsee virheen tunnisteessa. Virhe voi johtua sanoman sisällössä olevasta virheestä tai siitä, että tunniste ei vastaa asiakkaan ilmoittamia henkilötietoja. Palveluntarjoajan tulee antaa asiakkaalle tilannetta vastaava ilmoitus.
5. Vastausta ei tule lainkaan. Katkoksen syynä voi olla yhteyskatko, muu tekninen häiriö, asiakas jättää istunnon kesken tai asiakkaan istunnon aikakatkaisu.
6. Sama vastaus tulee useita kertoja.

12 NEUVONTA JA TEKNINEN TUKI

Tunnistuspalvelun tekninen tuki e-palvelut@s-pankki.fi

13 LINKKEJÄ

Finnish Trust Network OpenID Connect 1.0 Protocol Profile version 1.0

https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ftn_oidc_profile_v1.0_ficora_rec_213_2018_s.pdf

OpenID Connect –protokolla

https://openid.net/connect/

OpenID Connect 1.0

https://openid.net/specs/openid-connect-core-1_0.html

JSON Web Tokens

http://jwt.io

6/2022 S-Pankki