TUNNISTUSPALVELU

Palvelukuvaus ja soveltamisohje

PANKKI

SISÄLLYSLUETTELO

1 YLEISTÄ

Tämä ohje määrittelee palveluntarjoajalle tunnistuspalvelun käyttöönoton edellytykset sekä tietuekuvaukset järjestelmän rakentamiseen.

S-Pankin tunnistuspalvelun avulla palveluntarjoaja voi luotettavasti tunnistaa verkkoasiakkaitaan. Tunnistuspalvelussa pankki tunnistaa asiakkaan palveluntarjoajan puolesta.

Palvelu perustuu Finanssialan Keskusliiton hallinnoimaan Tupas-standardiin ja on tarkoitettu sähköisten asiointipalveluiden tarjoajille.

2 TUNNISTUSPALVELUN KUVAUS

2.1. YLEISKUVAUS

Tunnistautuva asiakas on keskeisessä asemassa palvelun käytössä. Asiakas ohjaa tietojensa välitystä palveluntarjoajan ja S-Pankin välillä. Palveluntarjoaja ja S-Pankki eivät ole palvelun aikana suorassa yhteydessä keskenään.

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. Tässä tapauksessa 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.

2.2. PALVELUN TOIMINNALLISUUS

Tunnistuspalvelussa on eri toimintoja ja käyttömahdollisuuksia sen mukaan, millaisen vastaussanoman välittämisestä on liittymissopimuksessa sovittu. S-Pankin antama vastaussanoman tunnistetieto sisältää aina asiakkaan nimen. Tämän lisäksi välitettävä tunnistetieto voi olla joko selväkielinen tai salattu.

Vastaussanoman ollessa selväkielinen, välittää S-Pankki joko asiakkaan henkilötunnuksen tai henkilötunnuksen tarkisteosan sen mukaan, mistä on sovittu liittymissopimuksessa. Selväkielisen henkilötunnuksen S-Pankki välittää vain palveluntuottajille, joilla on oikeus sitä käsitellä.

Vastaussanoman tunnistetiedon ollessa salattu, välittää S-Pankki palveluntarjoajalle tarkisteen, joka perustuu asiakkaan henkilötunnukseen. Itse tunnus ei kuitenkaan välity vastaussanoman mukana. Palveluntarjoajalla tulee olla käytössään asiakkaan henkilötunnus, jotta hän voi varmistua S-Pankin antaman vastaussanoman tietojen avulla asiakkaan oikeasta todennuksesta. Jos palveluntarjoajalla ei ole asiakkaan tunnusta, hänen tulee kysyä se ennen tunnistuspyynnön lähettämistä. Tämä toiminnallisuus soveltuu siten asiakkaan ilmoittamien tietojen oikeellisuuden tarkastamiseen pankista.

Tunnistuspalvelu soveltuu pääasiassa kuluttajille suunnattuihin palveluihin. Toiminnallisuudet, joissa käytetään asiakkaan henkilötunnusta soveltuvat mm. asiakkaan tunnistamiseen, palveluun sisäänkirjautumiseen ja sitovien sopimusten tekemiseen. Henkilötunnuksen tarkisteosaa voidaan käyttää esimerkiksi palveluun rekisteröitymisen jälkeiseen sisäänkirjautumiseen.

2.3. PALVELUN TURVALLISUUS

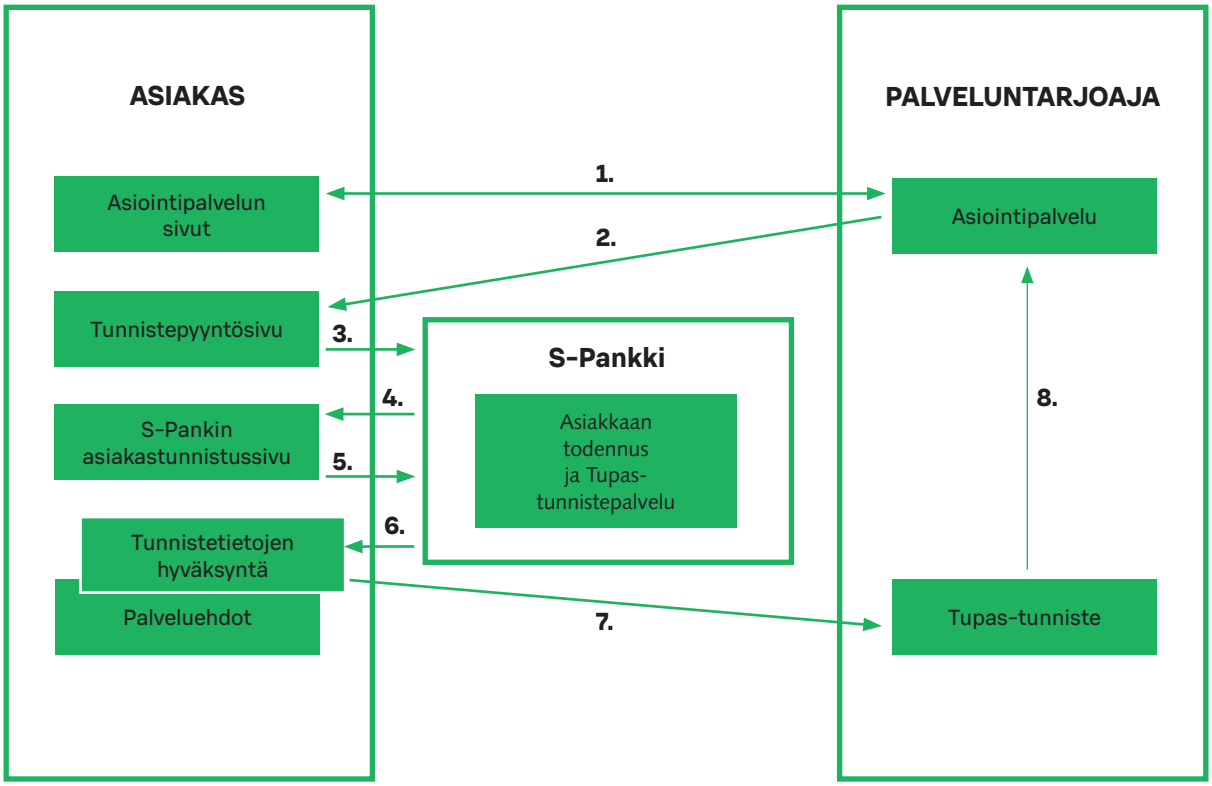
Tunnistuspalvelun osapuolten välisessä tietoliikenteessä käytetään SSL-salausta, joten ulkopuoliset eivät näe tietoja eivätkä voi muuttaa niitä. Palveluntarjoajan palvelinohjelmiston on tuettava 128 bitin SSL-salausta. Yhteydellä käytettävä avainpituus määräytyy kuitenkin asiakkaan käyttämän selaimen ominaisuuksien perusteella.

Tunnistuspyynnön ja tunnisteen tiedot on suojattu tiedon eheyden turvaavalla tarkisteella, joten tunnisteen välitystä ohjaavalla asiakkaalla ei ole mahdollisuutta muuttaa tietoja palveluntarjoajan tai S-Pankin sitä havaitsematta.

Kukin osapuoli vastaa omien palveluidensa suojauksesta, turvallisuudesta ja säilyttämiensä tietojen oikeellisuudesta. Palveluntarjoajan tulee säilyttää S-Pankin antamat palveluntarjoajan asiakastunnukset ja tarkisteavaimet huolellisesti ja oikeudettomalta käytöltä.

Tunnistautuva asiakas vastaa siitä, että pankin antamat pankkitunnukset eivät joudu ulkopuolisten haltuun sekä varmistaa S-Pankin tunnistuspalvelun palauttamista tunnistetiedoista palveluntarjoajan ja hyväksyy tunnisteen välittämisen.

3 TOIMINNALLINEN KUVAUS



Palvelun etenemistä kuvaavan kaavion selite:

1. Tunnistautuva asiakas on yhteydessä palveluntarjoajan palveluun. Asiakkaan ja palveluntarjoajan välinen tietoliikenne on SSL-suojattua heti kun asiakas siirtyy S-Pankin tunnistuspalveluun liittyvien tietojen syöttöön (vaiheet 2–7).

2. Palveluntarjoaja lähettää asiakkaalle tunnistuspyynnön, joka sisältää tapahtumaan liittyvät yksilöintitiedot. Asiakas tarkastaa vastaanottamansa tunnistuspyynnön tiedot, mutta hän ei voi muuttaa niitä. Asiakas voi halutessaan keskeyttää tunnistuksen ja palata takaisin asiointipalveluun. Palveluntarjoaja palauttaa asiakkaalleen vahvistamissivun, jossa on tapahtuman hyväksymis- ja peruutuspainikkeet.

3. Asiakas painaa toimintopainiketta, joka johtaa S-Pankin tunnistuspalveluun. S-Pankkiin välittyvä tunnistuspyyntö sisältää tunnistuspalvelun tarvitsemat tiedot palveluntarjoajasta ja tapahtumasta. S-Pankki tarkastaa tunnistuspyynnön eheyden ja tietojen oikeellisuuden.

4. S-Pankki lähettää asiakkaalle tunnistuspyynnön, jos palveluntarjoajan tunnistepyyntö on virheetön.

5. Asiakas tunnistautuu S-Pankin tunnistuspalvelussa. Jos tunnistus epäonnistuu, S-Pankki palauttaa asiakkaalle virheilmoituksen, jolloin asiakas palaa peruutuspainikkeella takaisin palveluntarjoajan palveluun.

6. Onnistuneen tunnistuksen jälkeen S-Pankki muodostaa vastaussanoman (Tupas-tunnisteen). S-Pankin tunnistuspalvelu asettaa tunnistautuvalle asiakkaalle hyväksymis- ja peruutuspainikkeet ja lähettää vastaussanoman tämän selaimelle.

7. Asiakas tarkastaa tunnisteen tiedot ja hyväksyy tunnisteen välittämisen palveluntarjoajalle. Asiakas voi peruutuspainikkeella keskeyttää tunnistustapahtuman ja palata palveluntarjoajan palveluun.

8. Palveluntarjoaja varmistaa vastaanottamansa vastaussanoman eheyden ja ainutkertaisuuden. Palveluntarjoaja liittää tunnisteen asiakkaan palvelutapahtumaan ja säilyttää sitä yhtä kauan kuin muita palvelutietoja säilytetään. Tunnisteita ei saa rekisteröidä tai käyttää muuhun tarkoitukseen.

4 TUNNISTUSPALVELUN KÄYTTÖÖNOTTO

4.1. KÄYTTÖÖNOTON EDELLYTYKSET

Palveluntarjoajan järjestelmän on kyettävä muodostamaan WWW-tekniikalla palvelun käyttäjälle tunnistepyyntö. Kun käyttäjä on hyväksynyt tunnisteen välittämisen palveluntarjoajalle, pitää tunniste liittää käyttäjän antamaan toimeksiantoon ja säilyttää yhtä kauan kuin toimeksianto. Tunnisteita ei saa rekisteröidä tai käyttää muuhun tarkoitukseen.

Tunnistuspalvelu ei edellytä mitään tiettyä WWW-palvelinohjelmistoa, mutta sen tulee tukea 128 bittistä SSL-salausta.

4.2. SOPIMUKSET

Palveluntarjoajan on tehtävä S-Pankin kanssa kirjallinen sopimus tunnistuspalvelun käytöstä. Palveluntarjoajan tiedot rekisteröidään pankissa ja sopimuksessa mainitulle yhteyshenkilölle lähetetään MAC-tarkisteavain. Palveluntarjoajille, jotka ovat siirtyneet SHA-256-salausalgoritmin käyttöön lähetetään tarkistelaskentaan käytettävä tarkisteavain heksadesimaalimuodossa esitettynä kahdessa eri osassa (PART 1 ja PART 2).

Kustakin eri palvelusta ja toiminnallisuudesta tulee tehdä pankin kanssa sopimus. Yhdessä palvelussa voi kuitenkin olla käytössä useita toiminnallisuuksia. Pankki tekee sopimuksen henkilötunnuksen välittämisestä vain silloin kuin palveluntarjoajalla on oikeus rekisteröidä se.

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

Palveluntarjoaja on myös velvollinen informoimaan S-Pankkia asiakasvolyymeistään vähintään neljännesvuosittain.

5 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.

6 TUNNISTUSPALVELUN SANOMAT JA NIIDEN TIEDOT

6.1. TUNNISTUSPYYNTÖ

Tunnistuspyynnön tiedot ovat S-Pankin verkkopalvelupainikkeen takana FORM-tietoryhmässä piilomuuttujina.

FORM-TIETORYHMÄ				
Kenttä	**Tiedon nimi**	**Pituus**	**P/V**	**Huomautus**
1. Sanomatyyppi	A01Y_ACTION_ID	3-4	P	Vakio, ”701”
2. Versio	A01Y_VERS	4	P	0002
3. Palveluntarjoaja	A01Y_RCVID	10-15	P	Asiakastunnus
4. Palvelukieli	A01Y_LANGCODE	2	P	FI = Suomi SV = Ruotsi
5. Kyselyn yksilöinti	A01Y_STAMP	20	P	yyyymmddhhmmssxxxxxx
6. Tunnisteen tyyppi	A01Y_IDTYPE	2	P	01 = Salattu henkilötunnus 02 = Selväkielinen henkilötunnus 03 = Henkilötunnuksen loppuosa
7. Paluuosoite	A01Y_RETLINK	199	P	OK paluuosoite tunnisteelle
8. Peruuta-osoite	A01Y_CANLINK	199	P	Paluuosoite peruutuksessa
9. Hylätty-osoite	A01Y_REJLINK	199	P	Paluuosoite virhetilanteessa
10. Avainversio	A01Y_KEYVERS	4	P	0001
11. Algoritmi	A01Y_ALG	2	P	03 = SHA-256
12. Tarkiste	A01Y_MAC	32-64	P	Kyselyn turvatarkiste

P/V = Tieto on pakollinen / valinnainen

Tietokenttien tiedon nimet kirjoitetaan isoilla kirjaimilla. FORM-tietoryhmän HTML-kielinen rakenne on seuraava:

```
<FORM METHOD="POST" ACTION="https://online.s-pankki.fi/service/identify">
<INPUT NAME="A01Y_ACTION_ID" TYPE="hidden" VALUE="701">
<INPUT NAME="A01Y_VERS" TYPE="hidden" VALUE="...">
<INPUT NAME="A01Y_RCVID" TYPE="hidden" VALUE="...">
<INPUT NAME="A01Y_LANGCODE" TYPE="hidden" VALUE="...">
<INPUT NAME="A01Y_STAMP" TYPE="hidden" VALUE="...">
<INPUT NAME="A01Y_IDTYPE" TYPE="hidden" VALUE="...">
<INPUT NAME="A01Y_RETLINK" TYPE="hidden" VALUE="...">
<INPUT NAME="A01Y_CANLINK" TYPE="hidden" VALUE="...">
<INPUT NAME="A01Y_REJLINK" TYPE="hidden" VALUE="...">
<INPUT NAME="A01Y_KEYVERS" TYPE="hidden" VALUE="...">
<INPUT NAME="A01Y_ALG" TYPE="hidden" VALUE="...">
<INPUT NAME="A01Y_MAC" TYPE="hidden" VALUE="...">
</FORM>
```

6.2. TUNNISTUSPYYNTÖKENTTIEN SELITYKSET

Kenttä 1
Sanoman tyyppi, joka on Tupas-palvelussa vakio "701".

Kenttä 2
Tunnistuspyyntö-sanoman versionumero on 0002.

Kenttä 3
S-Pankin palveluntarjoajalle antama asiakastunnus. S-Pankki tunnistaa palveluntarjoajan asiakastunnuksen perusteella ja liittää rekisterissään olevan palveluntarjoajan nimen vastaussanomaan.

Kenttä 4
Palvelun kielikoodi kertoo palveluntarjoajan asiointisivun kielen ja S-Pankin tunnistuspalvelu avautuu tällä kielellä.

Kenttä 5
Palveluntarjoajan tunnistuspyynnölle antama yksilöivä tunnus. Tunnuksena voi olla viite, asiakasnumero tai yhdistelmä päivämäärästä, kellonajasta ja juoksevasta tunnuksesta sekä viitteestä.

Kenttä 6
Tunnisteen tyyppi kertoo, minkä yksilöintitiedon palveluntarjoaja tunnistettavasta asiakkaastaan haluaa.
Tunnisteen tyypin tulee vastata palvelusopimuksessa sovittua toiminnallisuutta.
01 = Salattu henkilötunnus. Asiakkaan tunnistetiedon perusteella laskettu heksadesimaalimuotoinen MAC-tarkisteluku.
02 = Selväkielinen henkilötunnus.
03 = Henkilötunnuksen loppuosa. Sisältää henkilötunnuksen tarkenneosan ilman vuosisataa ilmoittavaa välimerkkiä.

Kenttä 7
Palveluntarjoajan palvelusivun osoite, joka on OK-tapauksessa jatkokohta.
Paluuosoitteen tulee olla https-alkuinen eli SSL-suojattu sivu, ja parametrien tulee olla URL-enkoodattuja.
Esimerkki: VALUE=https://www.verkkokauppa.fi/tilaus/vahvistus.do

Kenttä 8
Palveluntarjoajan palvelun jatkokohta, jos asiakas peruu tunnisteen välittämisen.
Esimerkki: VALUE=https://www.verkkokauppa.fi/tilaus/keskeytys.do

Kenttä 9
Palveluntarjoajan palvelun jatkokohta, jos tunnistuksessa on havaittu tekninen virhe.
Esimerkki: VALUE=https://www.verkkokauppa.fi/tilaus/virhe.do

Kenttä 10
MAC-tarkisteen laskennassa käytetyn avaimen versio.

Kenttä 11
MAC-tarkisteen laskennassa käytettävän algoritmin tyyppikoodi. S-Pankin tunnistuspalvelussa käytössä on SHA-256-algoritmi.
SHA-256 tyyppikoodi on 03, ja se tuottaa 64-merkkiä pitkän MAC-tarkisteen.

Kenttä 12
MAC-tarkiste, joka on laskettu tunnistuspyynnön suojattavista tiedoista ja palveluntarjoajan tarkisteavaimesta tietokentässä 11 määritellyllä algoritmilla. Tarkisteen avulla sanoman vastaanottaja tarkistaa tunnistuspyynnön eheyden ja lähettäjän. Tarkisteen pituus riippuu sen laskentaan käytettävästä algoritmista.

6.3. TUNNISTUSPYYNNÖN MAC-TARKISTEEN (A01Y_MAC) MUODOSTUMINEN

Palveluntarjoaja muodostaa pankin toimintopainiketta varten tunnistuspyynnön, joka suojataan MAC-tarkisteella. Tarkiste lasketaan tunnistuspyynnön FORM-tietoryhmästä S-Pankin palveluntarjoajalle antamalla tarkisteavaimella. Käytettäessä SHA-256-salausalgoritmia tulee palveluntarjoajan ennen tarkisteavaimen käyttöönottoa konvertoida PART1 ja PART2 -osista muodostuva 64-merkkinen heksadesimaalimuotoinen avain string-muotoon. String-muodossa esitettynä tarkisteavain on 32 merkin mittainen.

Laskennan aluksi muodostetaan merkkijono FORM-tietoryhmän kaikkien tarkastetta edeltävien tieto-kenttien (kentät 1-11) VALUE-arvoista ja palveluntarjoajan tarkisteavaimista. Tiedot yhdistetään merkkijonoksi järjestyksessä niin, että kenttien täytemerkkeinä olevat blankot jätetään pois. Merkkijonon tietoryhmät erotetaan toisistaan "&" -merkillä. Viimeisen tiedon (kenttä 12) ja tarkisteavaimen väliin sekä tarkisteavaimen loppuun laitetaan "&" -merkki. "&" -merkit otetaan sanoman MAC-tarkisteen laskentaan mukaan. Tieto on yhtenä rivinä "+" -merkki näyttää tässä dokumentissa olevan rivinvaihdon.

A01Y_ACTION_ID&A01Y_VERS&A01Y_RCVID&A01Y_LANGCODE&A01Y_STAMP&+
A01Y_IDTYPE&A01Y_RETLINK&A01Y_CANLINK&A01Y_REJLINK&A01Y_KEYVERS&+
A01Y_ALG&tarkisteavain&

Laskettu MAC muutetaan heksadesimaaliseen esitysmuotoon, jossa A-F esitetään isoilla kirjaimilla. Heksadesimaalinen tiivisteen arvo viedään MAC-tarkiste-kenttään.

6.4. VASTAUSSANOMA JA TUNNISTE

S-Pankki lisää vastaussanoman tiedot OK-paluulinkkiin query-string muodossa.

Tarkiste lasketaan alkuperäisestä sanomasta, jonka jälkeen skandinaaviset merkit ja eräät erikoismerkit (esim. tyhjämerkit, yhtäläisyys- ja lainausmerkit) korvataan vastaavalla heksadesimaalimerkillä (esim. %20) tietoliikennesanomassa.

S-Pankin tunnistuspalvelu laskee vastaussanoman MAC-tarkisteen palveluntarjoajakohtaisella avaimella. Tarkisteen avulla palveluntarjoaja voi varmistua, että tunniste on muodostettu asiakkaan pankissa ja tunnistesanoman tiedot eivät ole muuttuneet.

VASTAUSSANOMA				
Kenttä	**Tiedon nimi**	**Pituus**	**P/V**	**Huomautus**
1. Versio	B02K_VERS	2	P	0002
2. Tunnisteen yksilöinti	B02K_TIMESTMP	23	P	NNNvvvvkkpphhmmssxxxxxx
3. Tunnisteen numero	B02K_IDNBR	10	P	S-Pankin tunnistuspalvelun tunnisteelle antama numero
4. Kyselyn yksilöinti	B02K_STAMP	20	P	Kyselyn tietokenttä 5 (A01Y_STAMP)
5. Asiakas	B02K_CUSTNAME	40	P	Asiakkaan nimi
6. Avainversio	B02K_KEYVERS	4	P	Avaimen sukupolvi
7. Algoritmi	B02K_ALG	2	P	03 = SHA-256
8. Tunniste	B02K_CUSTID	64	P	Pyydetyn mukainen asiakastunniste (salattu henkilötunnus, selväkielinen henkilötunnus tai henkilötunnuksen loppuosa)
9. Tunnisteen tyyppi	B02K_CUSTTYPE	2	P	01 = Selväkielinen henkilötunnus 02 = Selväkielinen henkilötunnuksen loppuosa 05 = Salattu henkilötunnus
10. Tarkiste	B02K_MAC	AN 32-64	P	Vastauksen turvatarkiste

P/V = Tieto on pakollinen / valinnainen

6.5. VASTAUSSANOMAN KENTTIEN SELITYKSET

Kenttä 1
Vastaussanoman versionumero, joka on 0002.
Kenttä 2
S-Pankin tietojärjestelmän muodostama aikaleima, jossa NNN on aina 390 ja ilmaisee, että kyseessä S-Pankki.
Kenttä 3
S-Pankin tietojärjestelmän tunnisteelle antama tieto, joka yksilöi tunnisteen S-Pankin järjestelmässä.
Kenttä 4
Tunnistepyynnön yksilöintitieto, joka on poimittu kyseisen tunnistepyynnön tietokentästä 5 (A01Y_STAMP)
Kenttä 5
S-Pankin asiakastietokannassa oleva tunnistetun asiakkaan nimi.
Kenttä 6
MAC-tarkisteavaimen sukupolvitieto.
Kenttä 7
MAC-tarkistealgoritmin tunnus.
Kenttä 8
Asiakkaan tunnistetieto. Selväkielinen tunnus tai salattu tarkiste riippuen tunnistepyynnön A01Y_IDTYPE-kentän sisällöstä.
Kenttä 9
Tunnisteen tyyppi. Tämä kenttä kertoo, mikä kentän 8 tunnistetieto on. S-Pankin tietojärjestelmän palauttamat arvot ovat:
01 = Selväkielinen henkilötunnus
02 = Selväkielinen henkilötunnuksen loppuosa
05 = Salattu henkilötunnus
Kenttä 10
Vastaussanoman tarkiste.

6.6. VASTAUSSANOMAN TARKISTEEN LASKENTA

Palveluntarjoaja tarkastaa vastaanottamansa vastaussanoman eheyden laskemalla siitä aluksi MAC-tarkisteen, jota verrataan sanoman tarkisteeseen. Tarkiste lasketaan vastaussanoman tietokentistä 1-9.

Kentän B02K_CUSTID sisältö määräytyy sen mukaan, mitä tunnusta tunnistepyynnössä on pyydetty ja on siis vaihtoehtoisesti joko selväkielinen henkilötunnus, salattu henkilötunnus tai selväkielinen henkilötunnuksen loppuosa.

Tarkisteen laskennassa tiedot ja tarkisteavain erotetaan toisistaan & -merkillä, joka lisätään myös tarkisteavaimen loppuun. Tarkisteen laskennassa käytetään palveluntarjoajakohtaista avainta. ”+” -merkki näyttää tässä dokumentissa olevan rivinvaihdon.
B02K_VERS&B02K_TIMESTMP&B02K_IDNBR&B02K_
STAMP&+
B02K_CUSTNAME&B02K_KEYVERS&B02K_ALG&+
B02K_CUSTID&B02K_CUSTTYPE&tarkisteavain&

Kuten tunnistuspyynnössäkin, tulee palveluntarjoajan SHA-256-salausalgoritmia käytettäessä konvertoida tarkisteavaimen PART1 ja PART2 -osista muodostuva 64-merkkinen heksadesimaalimuotoinen avain string-muotoon. String-muodossa esitettynä tarkisteavain on 32 merkin mittainen.

6.7. TUNNISTEEN TYYPPI

Vastaussanoman tarkisteen laskentaan vaikuttaa välitettävän asiakastunnisteen tyyppi, joka määritellään tunnistepyynnön A01Y_IDTYPE-kentässä.

6.7.1. ASIAKKAAN TUNNISTEENA SELVÄKIELINEN ASIAKASTUNNUS

Tunnistepyynnön A01Y_IDTYPE-kentän arvot ”02” ja ”03”: Asiakkaan tunnus on selväkielinen merkkijono, joko henkilötunnus tai sen loppuosa tunnistepyynnön kentän A01Y_IDTYPE mukaisesti. Tunnus sijoitetaan sellaisenaan vastaussanoman tiedoksi B02K_CUSTID.

6.7.2. ASIAKKAAN TUNNISTEENA SALATTU TARKISTE

Tunnistepyynnön A01Y_IDTYPE-kentän arvo on ”01” eli salattu henkilötunnus.

Pankki käyttää asiakastunnuksen salaamisessa samaa tiivistealgoritmia kuin sanomien tarkistelaskennassa. Tunnistetieto salataan käyttämällä vastaussanoman tietokentissä 2-4 olevia tietoja ja pankissa rekisteröityä asiakkaan tunnusta (henkilötunnus). Salatun tunnuksen laskennassa tiedot ja tarkisteavain erotetaan toisistaan &-merkillä, joka lisätään myös tarkisteavaimen loppuun. Salaamisessa käytetään palveluntuottajakohtaista avainta.

B02K_TIMESTMP&B02K_IDNBR&B02K_STAMP&asiakastunnus&tarkisteavain&

Salattu tunnus muutetaan heksadesimaaliseen esitysmuotoon, jossa arvot A-F esitetään isoilla kirjaimilla. Lopputuloksena saadaan asiakkaan tunnisteeksi merkkijono, joka sijoitetaan vastaussanomaan tiedoksi B02K_CUSTID.

6.8. SANOMAN TARKISTEEN TARKASTUS JA ASIAKKAAN TUNNISTUS

Palveluntarjoaja laskee vastaanottamastaan sanomasta kohdassa 6.6. kuvatulla tavalla vastaanotetun sanoman MAC-tarkisteen. Mikäli se on sama kuin vastaussanomassa pankista tullut vastaussanoman tarkiste, on vastaussanoma välittynyt muuttumattomana.

7 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, jossa osoitteena on tunnistuspyynnön FORM-tietokentässä 8 oleva Peruuta-osoite.

2. Asiakkaan todennus epäonnistuu joko asiakkaan antamien tunnistetietojen virheellisyyden takia tai koska asiakas on pyytänyt todennusta väärästä pankista. Asiakas palaa palveluntarjoajan palveluun peruuta-painikkeella, jossa osoitteena on tunnistuspyynnön FORM-tietokentässä 8 oleva Peruuta-osoite

3. S-Pankki havaitsee virheen tunnistuspyynnössä. S-Pankki havaitsee ennen asiakkaan todennusta tunnistuspyynnössä virheen. Asiakas palaa palveluntarjoajan palveluun FORM-tietokentässä 9 olevaan Hylätty-osoitteeseen.

4. Palveluntarjoaja havaitsee virheen Tupas-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. Palveluntarjoajan on varauduttava siihen, että asiakas voi lähettää saman vastauksen useampaan kertaan tai asiakas voi lähettää vanhan Tupas-tunnisteen siirtyessään selaimensa ikkunoissa eteen/taakse -näppäimillä ruudusta toiseen.

8 ASIAKASTUNNUKSEN JA TARKISTEAVAIMEN VAIHTO

Palvelun käyttöön liittyvä asiakastunnus ja tarkisteavain voidaan vaihtaa palveluntarjoajan tai S-Pankin toivomuksesta. Pankki vastaa tunnusten ja tarkisteavainten määräajoin tapahtuvasta vaihdosta ja ottaa palveluntarjoajaan yhteyttä vaihdon tullessa ajankohtaiseksi.

9 TESTAUS

Palveluntarjoaja voi testata palvelua tuotantoympäristössä milloin tahansa käyttämällä seuraavia testitunnuksia:
Osoite: https://online.s-pankki.fi/service/identify
Testitarkisteavain MAC-laskentaa varten: SPANKKI
Testikäyttäjätunnus: 12345678
Testisalasana: 123456
Testitunnusluku: 1234
Testatessa on huomioitava, että vastaussanoman kentässä B02K_CUSTTYPE palautettavat arvot poikkeavat siitä, mitä kentässä palautetaan kun palvelua käytetään tuotantotunnuksin.

10 NEUVONTA JA TEKNINEN TUKI

Mikäli tunnistuspalvelun käyttöönotossa tai käytössä esiintyy ongelmia, ota yhteyttä sähköpostiosoitteeseen e-palvelut@s-pankki.fi

TUNNISTEPYYNTÖ – TESTISANOMA	
FORM-tietokenttä	**Huomautus**
A01Y_ACTION_ID 701	Vakio, "701"
A01Y_VERS	0002
A0IY_RCVID	SPANKKITUPAS
A01Y_LANGCODE	FI = Suomi SV = Ruotsi
A01Y_STAMP	vvvvkkpphhmmssxxxxx
A01Y_IDTYPE	01 = Salattu henkilötunnus 02 = Selväkielinen henkilötunnus 03 = Henkilötunnuksen loppuosa
A01Y_RETLINK	OK paluuosoite tunnisteelle
A01Y_CANLINK	Paluuosoite peruutuksessa
A01Y_REJLINK	Paluuosoite virhetilanteessa
A01Y_KEYVERS	0001
A01Y_ALG	03 = SHA-256
A01Y_MAC	Kyselyn turvatarkiste

VASTAUSSANOMA	
FORM-tietokenttä	**Huomautus**
B02K_VERS	0002
B02K_TIMESTMP	390vvvvkkpphhmmssxxxxx
B02K_IDNBR	S-Pankin tunnisteelle antama numero
B02K_STAMP	Kyselyn tietokenttä 5 (A01Y_STAMP)
B02K_CUSTNAM	Meikäläinen Maija
B02K_KEYVERS	0001
B02K_ALG	03 = SHA-256
B02K_CUSTID	Salattu henkilötunnus: 32-64 merkkinen tiiviste Selväkielinen henkilötunnus: 010170-960F Henkilötunnuksen loppuosa: 960F
	Kyselyn turvatarkiste
B02K_CUSTTYPE	08 = Selväkielinen henkilötunnus 08 = Selväkielinen henkilötunnuksen loppuosa 09 = Salattu henkilötunnus
B02K_MAC	Vastauksen turvatarkiste

S-Pankki Oyj, Y-tunnus 2557308-3, kotipaikka Helsinki
4/2022 S-Pankki