

POP PANKIN TUNNISTUSPALVELU
KÄYTTÖOHJE JA TIETUEKUVAUKSET



1.4.2014

versio 1.1

Sisällysluettelo

1. Yleistä.....	3
2. Turvallisuus.....	4
3. Toiminnallinen kuvaus	4
3.1. Kaavio	6
3.2. Kaavion selite.....	6
4. POP Pankin tunnistuspalvelun sanomakuvaukset	8
4.1. Tunnistepyyntö	8
4.2. Tunnistuspyynnön kenttien selitykset	8
4.3. Tunnistuspyynnön MAC-tarkisteen muodostaminen	9
4.4. Vastaussanoma ja tunniste	10
4.5. Vastaussanomien kenttien selitykset	11
4.6. Vastaussanomien tarkisteen laskenta.....	11
4.7. Tunnisteen tyyppi	12
4.8. Sanomien tarkisteen tarkastus ja asiakkaan tunnistus	12
5. Poikkeustilanteet	13
6. Tarkisteavaimen vaihto ja säilytys.....	13
7. POP Pankin tunnistuspalvelun nimi ja logo	13
8. POP Pankin tunnistuspalvelun käyttöönotto.....	14
8.1. Edellytykset	14
8.2. Sopimukset.....	14
8.3. Testaus	14
9. Neuvonta ja tekninen tuki.....	16

POP Pankin tunnistuspalvelu

POP Pankin tunnistuspalvelun avulla palveluntuottaja voi tunnistaa luotettavasti verkkoasiakkaitaan pankin tunnistamismenetelmiä hyväksikäyttäen. POP Pankin tunnistuspalvelussa pankki tunnistaa asiakkaan palveluntuottajan puolesta. POP Pankin tunnistuspalvelu on käytettävissä 24 tuntia kaikkina viikonpäivinä, pois lukien huollosta, päivityksestä tms. syystä johtuvista katkoajoista. POP Pankin tunnistuspalvelun POP Pankille tuottaa Oy Samlink Ab.

POP Pankin tunnistuspalvelu perustuu Suomen pankkiyhdistyksessä laadittuun Tupas-standardiin ja se on tarkoitettu sähköisten asiointi- ja maksamispalveluiden tuottajille. POP Pankin tunnistuspalvelussa välitettäviä tunnistustietoja voidaan käyttää myös osana sähköisen allekirjoituksen muodostamista tunnistuvan asiakkaan ja palveluntuottajan niin sopiessa.

Lisätietoa standardista saa Finanssialan Keskusliiton Internet-sivuilta www.fkl.fi.

1. Yleistä

Tunnistautuva asiakas on keskeisessä asemassa palvelun käytössä. Asiakas ohjaa tietojensa välitystä palveluntuottajan ja pankin välillä. Pankki ja palveluntuottaja eivät ole palvelun aikana suorassa yhteydessä keskenään.

Tuotettu tunniste on ainutkertainen ja se on sidottu sekä palveluntuottajan kyseiseen palvelutapahtumaan että asiakkaaseen. Kun palveluntuottajalla on tarve tunnistaa asiakkaansa, palveluntuottaja lähettää tunnistepyyntön asiakkaalle, joka siirtyy Samlinkin tunnistuspalveluun painamalla POP Pankin tunnistuspainiketta. Palveluntuottajan tunnistuspyyntö välittyy asiakkaalta pankin tunnistuspalveluun, joka lähettää tunnistamisen jälkeen asiakkaalle vastaussanoman. Asiakas tarkastaa vastaanottamansa vastaussanoman tiedot, joiden hyväksymisen jälkeen hän palaa takaisin palveluntuottajan palveluun ja jatkaa siellä palveluun liittyviä toimintoja. Asiakas voi halutessaan peruttaa tai hylätä tunnistustapahtuman joko ennen tunnistautumista tai vastaussanoman tarkastamisen jälkeen, jolloin asiakkaan tiedot eivät välity palveluntuottajalle.

Mahdollisuus käyttää palvelun tietoja osana sähköistä allekirjoitusta perustuu palveluntuottajan ja asiakkaan keskinäiseen sopimukseen siitä, että tunnistustietoja voidaan käyttää osana sähköistä allekirjoitusta heidän välisessään oikeustoimessa. POP Pankin tunnistuspalvelun käyttämistä sähköisenä allekirjoituksena tukevat lisäksi vastaussanomien aikaleimat ja Samlinkin lokitiedot. Jos palvelua halutaan käyttää hyväksi osana sopimuksen tai hakemuksen tekemistä, tulee palveluntuottajan kuitenkin huolehtia muista sähköisen allekirjoituksen edellyttämistä seikoista, kuten tietojen kokonaisuuden hallinnasta, vastaussanoman tallentamisesta ja oman palvelunsa muuttumattomuudesta. POP Pankki tai Oy Samlink Ab eivät vastaa palveluntarjoajan ja tunnistautuvan asiakkaan välisen sopimuksen tai muun oikeustoimen pätevyydestä tai sisällöstä.

Internet-palvelun osoite on <https://tupas.poppankki.fi>
POP Pankin tunnistuspalvelu on käytettävissä 24 h/vrk.

2. Turvallisuus

Tunnistuspalvelun osapuolten välinen tietoliikenteessä käytetään SSL-salausprotokollaa, joten ulkopuoliset eivät näe tietoja eivätkä voi muuttaa niitä. Palveluntuottajan palvelinohjelmiston on tuettava 128 bitin SSL-salausta. Yhteydellä käytettävä avainpituus määräytyy kuitenkin asiakkaan käyttämän selaimen ominaisuuksien perusteella. Tunnistuspyynnön ja vastaussanomien tiedot on suojattu tiedon eheyden turvaavalla tarkisteella, joten tunnistustietojen välitystä ohjaavalla asiakkaalla ei ole mahdollisuutta muuttaa tietoja palveluntuottajan ja POP Pankin tunnistuspalvelun sitä havaitsematta.

Kukin osapuoli vastaa omien palveluittensa suojauksesta, turvallisuudesta ja säilyttämiensä tietojen oikeellisuudesta. Tunnistautuva asiakas vastaa siitä, että pankkien antamat tunnukset tai muut todennusvälineet eivät joudu ulkopuolisten haltuun.

Palvelun käyttäjä vastaa siitä, että hänen verkkopankkitunnuksensa eivät joudu ulkopuolisten haltuun ja että tunnukset annetaan vain POP Pankin tunnistuspalvelua hoitavalle tietokoneelle. Palvelun käyttäjä myös varmistaa POP Pankin tunnistuspalvelun palauttamista tunnistustiedoista palveluntarjoajan ja hyväksyy POP Pankin tunnistuksen välittämisen.

3. Toiminnallinen kuvaus

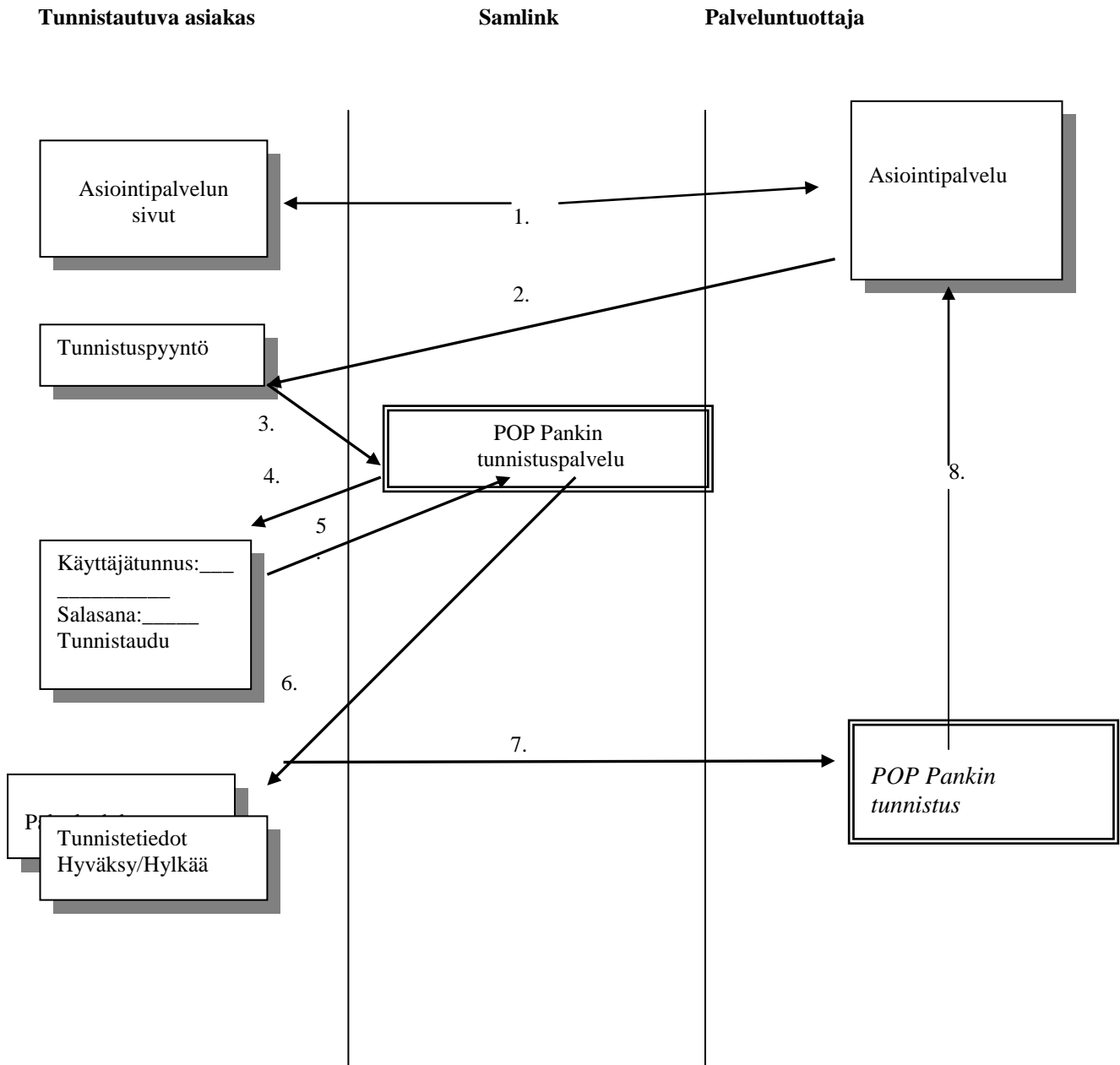
POP Pankin tunnistuspalvelussa on eri toimintoja ja käyttömahdollisuuksia sen mukaan, millaisen vastaussanomien välittämistä on palvelusopimuksessa sovittu. Vastaussanomien tunnistustieto sisältää aina asiakkaan nimen. Tämän lisäksi välitettävä tunnistustieto voi olla joko selväkielinen tai salattu.

Vastaussanomien ollessa selväkielinen, välittää POP Pankin tunnistuspalvelu joko asiakkaan henkilötunnuksen, henkilötunnuksen tarkisteosan tai Y-tunnuksen sen mukaan, mistä on sovittu palvelusopimuksessa. Selväkielisen henkilötunnuksen POP Pankin tunnistuspalvelu välittää vain palveluntuottajille, joilla on oikeus sitä käsitellä.

Vastaussanomien tunnistustiedon ollessa salattu, välittää POP Pankin tunnistuspalvelu palveluntuottajalle tarkisteen, joka perustuu asiakkaan henkilötunnuksen tai Y-tunnuksen. Itse tunnus ei kuitenkaan välity vastaussanomien mukana. Palveluntuottajalla tulee olla käytössään asiakkaan henkilötunnus tai Y-tunnus, jotta hän voi varmistua POP Pankin tunnistuspalvelun antaman vastaussanomien tietojen avulla asiakkaan oikeasta todennuksesta. Jos palveluntuottajalla ei ole asiakkaan tunnusta, hänen tulee kysyä se ennen tunnistuspyynnön lähettämistä. Tämä toiminnallisuus soveltuu siten asiakkaan ilmoittamien tietojen oikeellisuuden tarkastamiseen pankista.

Toiminnallisuudet, joissa käytetään asiakkaan henkilötunnusta soveltuvat mm. asiakkaan tunnistamiseen, palveluun sisäänkirjautumiseen ja sitovien sopimusten tekemiseen. Henkilötunnuksen tarkisteosaa voidaan käyttää esimerkiksi palveluun rekisteröitymisen jälkeiseen sisäänkirjautumiseen.

3.1. Kaavio



3.2. Kaavion selite

1. Tunnistautuva asiakas on yhteydessä palveluntuottajan palveluun. Asiakkaan ja palveluntuottajan välinen tietoliikenne on SSL-suojattua, kun asiakas siirtyy tunnistuspalveluun liittyvien tietojen syöttöön (aina vaiheiden 2-7 aikana).
2. Palveluntuottajalla on tarve tunnistaa asiakkaansa. Tunnistuspyyntö sisältää tapahtumaan liittyvät yksilöintitiedot. Asiakas tarkastaa vastaanottamansa tunnistuspyynnön tiedot, mutta hän ei voi muuttaa niitä. Asiakas voi halutessaan

keskeyttää tunnistuksen ja palata takaisin asiointipalveluun. Palveluntuottaja antaa asiakkaalleen vahvistamissivun, jossa on tapahtuman hyväksymis- ja peruutuspainikkeet.

3. Asiakas painaa painiketta, ja lähtevä sanoma johtaa hänet POP Pankin tunnistuspalveluun. Sanoma sisältää tunnistuspalvelun tarvitsemat tiedot palveluntuottajasta ja tapahtumasta. POP Pankin tunnistuspalvelu tarkastaa tunnistuspyynnön eheyden ja tietojen oikeellisuuden.
4. POP Pankin tunnistuspalvelu lähettää asiakkaalle tunnistuspyynnön, jos palveluntuottajalta toimitettu pyyntö on virheetön. Pankki antaa asiakkaalle virheilmoituksen, jos POP Pankin tunnistuspalvelu havaitsee tunnistuspyynnössä virheitä. Asiakas palaa tapahtuman peruutuspainikkeella takaisin palveluntuottajan palveluun.
5. Asiakas tunnistautuu pankkiin. Pankki palauttaa asiakkaalle virheilmoituksen, jos tunnistus epäonnistuu. Asiakas palaa peruutuspainikkeella takaisin palveluntuottajan palveluun.
6. Onnistuneen todennuksen jälkeen POP Pankin tunnistuspalvelu muodostaa vastaussanomaa. POP Pankin tunnistuspalvelu asettaa tunnistautuvalle asiakkaalle hyväksymis- ja peruutuspainikkeet ja lähettää vastaussanomaa tämän selaimelle.
7. Asiakas tarkastaa tunnisteen tiedot ja hyväksyy tunnisteen välittämisen palveluntuottajalle. Asiakas voi peruutuspainikkeella hylätä tunnisteen ja palata takaisin palveluntuottajan palveluun.
8. Palveluntuottaja varmistaa vastaanottamansa vastaussanomaa eheyden ja ainutkertaisuuden. Palveluntuottaja liittää tunnisteen asiakkaan palvelutapahtumaan ja säilyttää sitä yhtä kauan kuin muita palvelutietoja säilytetään. Tunnisteita ei saa rekisteröidä tai käyttää muuhun tarkoitukseen.

4. POP Pankin tunnistuspalvelun sanomakuvaukset

4.1. Tunnistepyyntö

Tunnistuspyynnön tiedot ovat POP Pankin tunnistuskuvakkeen takana FORM-tietoryhmässä piilomuuttujina.

Tietoryhmän rakenne on HTML-kielillä:

<code><FORM METHOD="POST" ACTION="https://tupas.poppankki.fi"> <INPUT NAME="..." TYPE="..." VALUE="..."> <INPUT NAME="..." TYPE="..." VALUE="..."> </FORM></code>				
FORM-TIETORYHMÄ				
Kenttä	Tiedon nimi	Pituus	Pakollisuus	Huomautus
1. Sanomatyyppi	A01Y_ACTION_ID	3 - 4	P	Vakio, "701"
2. Versio	A01Y_VERS	4	P	0002
3. Palveluntuottaja	A01Y_RCVID	10 -15	P	Palvelutunnus
4. Palvelun kieli	A01Y_LANGCODE	2	P	FI = Suomi SV = Ruotsi EN = Englanti
5. Kyselyn yksilöinti	A01Y_STAMP	20	P	Vvvvkkpphhmmssxxxxxx
6. Tunnisteen tyyppi	A01Y_IDTYPE	2	P	01 = Salattu perustunnus 02 = Selväkielinen perustunnus 03 = Selväkielinen typistetty tunnus
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	Avaimen sukupolvitieto
11. Algoritmi	A01Y_ALG	2	P	03 = SHA256
12. Tarkiste	A01Y_MAC	64	P	Kyselyn turvatarkiste

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

```
<FORM METHOD="POST" ACTION="POP Pankin tunnistuspalvelun URL">
<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>
```

4.2. Tunnistuspyynnön kenttien selitykset

1. Sanoman tyyppi, joka on vakio 701.

2. Tunnistuspyyntö-sanoman versionumero, joka on 0002.
3. Palveluntuottajan asiakastunnus. POP Pankin tunnistuspalvelu tunnistaa palveluntuottajan asiakastunnuksen perusteella ja liittää rekisterissään olevan palveluntuottajan nimen tunnistussanomaan.
4. Palvelun kielikoodi kertoo palveluntuottajan asiointisivun kielen ja POP Pankin tunnistuspalvelu avautuu tällä kielellä, mikäli kyseinen kieli kuuluu POP Pankin tunnistuksessa kulloinkin käytössä olevaan kielivalikoimaan.
5. Palveluntuottajan tunnistuspyynnölle antama yksilöivä tunnus. Tunnuksena voi olla viite, asiakas-numero tai yhdistelmä päivämäärästä, kellonajasta ja juoksevasta tunnuksesta sekä viitteestä.
6. Tunnisteen tyyppi kertoo, minkä yksilöintitiedon palveluntuottaja tunnistettavasta asiakkaastaan haluaa. Tunnisteen tyyppin tulee vastata palvelusopimuksessa sovittua toiminnallisuutta.
 - 01 = Salattu perustunnus. Asiakkaan tunnistetiedon perusteella laskettu heksadesimaalimuotoinen MAC-tarkisteluku. Voi sisältää asiakkaan täydellisen henkilötunnuksen tai Y-tunnuksen.
 - 02 = Selväkielinen perustunnus. Voi sisältää asiakkaan täydellisen henkilötunnuksen tai Y-tunnuksen.
 - 03 = Selväkielinen tyypistetty tunnus. Voi sisältää henkilötunnuksen tarkenneosan ilman vuosisataa ilmoittavaa välimerkkiä tai kokonaisen Y-tunnuksen.
7. Palveluntuottajan palvelusivun osoite, joka on OK-tapauksessa jatkokohta. Paluuosoitteen tulee olla https-alkuinen, eli SSL-suojattu sivu.

Esimerkki: VALUE=<https://www.verkkokauppa.fi/tilaus/vahvistus.html>
8. Palveluntuottajan palvelun jatkokohta, jos asiakas peruu tunnisteen välittämisen.

Esimerkki: VALUE=<https://www.verkkokauppa.fi/tilaus/keskeytys.html>
9. Palveluntuottajan palvelun jatkokohta, jos tunnistuksessa on havaittu tekninen virhe.

Esimerkki: VALUE=<https://www.verkkokauppa.fi/tilaus/virhe.html>
10. MAC-tarkisteen laskennassa käytetyn avaimen versio.
11. MAC-tarkisteen laskennassa käytettävän algoritmin tyyppikoodi. POP Pankin tunnisteissa on käytössä 03 = SHA-256 algoritmi, joka tuottaa 64 merkkisen MACin.
12. MAC-tarkiste, joka on laskettu tunnistuspyynnön suojattavista tiedoista ja palveluntuottajan tarkisteavaimesta tietokentässä 11 määritellyillä algoritmeilla. Vastaanottaja tarkistaa tarkisteesta tunnistuspyynnön eheyden ja lähettäjän.

4.3. Tunnistuspyynnön MAC-tarkisteen muodostaminen

Palveluntuottaja muodostaa pankin toimintopainiketta varten tunnistuspyynnön, joka suojataan MAC-tarkisteella. Tarkiste lasketaan tunnistuspyynnön FORM-tietoryhmästä POP Pankin tunnistuspalvelun palveluntuottajalle antamalla tarkisteavaimella.

Laskennan aluksi muodostetaan merkkijono FORM-tietoryhmän kaikkien tarkistetta edeltävien tieto-kenttien (kentät 1 - 11) VALUE-arvoista ja palveluntuottajan tarkisteavaimesta. 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 tiiviste arvo viedään MAC-tarkiste-kenttään.

4.4. Vastaussanoma ja tunniste

POP Pankin tunnistuspalvelu lisää vastaussanomien 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.

POP Pankin tunnistuspalvelu laskee vastaussanomien MAC-tarkisteen palveluntuottajakohtaisella avaimella. Tarkisteen avulla palveluntuottaja voi varmistua, että tunniste on muodostettu asiakkaan pankissa ja tunnistesanomien tiedot eivät ole muuttuneet.

VASTAUSSANOMA				
Kenttä	Tiedon nimi	Pituus	Pakollisuus	Huomautus
1. Versio	B02K_VERS	4	P	0002
2. Tunnisteen yksilöinti	B02K_TIMESTMP	23	P	NNNvvvkkpphhmssxxx xxx
3. Tunnisteen numero	B02K_IDNBR	10	P	POP Pankin tunnistuspalvelun tunnisteelle antama numero
4. Kyselyn yksilöinti	B02K_STAMP	20	P	Kyselyn tietokenttä 7 (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 = SHA256
8. Tunniste	B02K_CUSTID	40	P	Salattu tarkiste tai selväkielinen palvelutunnus
9. Tunnisteen tyyppi	B02K_CUSTTYPE	2	P	00 = ei tiedossa 01 = selväkielinen

				henkilötunnus 02 = selväkielinen hetun tarkenne 03 = selväkielinen Y-tunnus 04 = selväkielinen sähköinen asiointitunnus 05 = salattu henkilötunnus 06 = salattu Y-tunnus 07 = salattu sähköinen asiointitunnus
10. Tarkiste	B02K_MAC	AN 64	P	Vastauksen turvatarkiste

4.5. Vastaussanomien kenttien selitykset

1. Vastaussanomien versionumero, joka on 0002.
2. Pankin järjestelmän muodostama aikaleima, jossa NNN on aina 430 ja ilmaisee, että kyseessä on POP Pankin tunnistuspalvelu.
3. Pankin tietojärjestelmän tunnisteelle antama tieto, joka yksilöi tunnisteiden pankin järjestelmässä.
4. Tunnistuspyynnön yksilöintitieto, joka on poimittu kyseisen tunnisteiden pyynnön tietokentästä 7 (A01Y_STAMP)
5. Pankin asiakastietokannassa oleva asiakkaan nimi.
6. MAC-tarkisteavaimen sukupolvitieto.
7. MAC-tarkistealgoritmin tunnus.
8. Asiakkaan tunnistetieto. Selväkielinen tunnus tai salattu tarkiste riippuen tunnisteiden pyynnön A01Y_IDTYPE-kentän sisällöstä.
9. Tunnisteiden tyyppi. Tämä kenttä kertoo, mikä kentän 8 tunnistetieto on. Mahdolliset arvot ovat:
01 = selväkielinen henkilötunnus
02 = selväkielinen hetun tarkenne
03 = selväkielinen Y-tunnus
04 = selväkielinen sähköinen asiointitunnus. POP Pankin tunnistuspalvelussa ei käytössä.
05 = suojattu henkilötunnus
06 = suojattu Y-tunnus
07 = salattu sähköinen asiointitunnus. POP Pankin tunnistuspalvelussa ei käytössä.
10. Vastaussanomien tarkiste.

4.6. Vastaussanomien tarkisteiden laskenta

Vastaanotetun vastaussanomien eheys tarkistetaan laskemalla siitä aluksi tarkiste, jota verrataan sanomien tarkisteeseen. Tarkiste lasketaan vastaussanomien tietokentistä 1-9. Kentän B02K_CUSTID sisältö määräytyy sen mukaan, mitä tunnusta tunnisteiden pyynnössä on pyydetty ja on siis vaihtoehtoisesti joko salattu tarkiste tai selväkielinen asiakastunnus. Tarkisteiden laskennassa tiedot ja tarkisteavaimen erotetaan toisistaan &-merkillä, joka lisätään myös tarkisteavaimen loppuun. Tarkisteiden laskennassa käytetään palveluntuottajakohtaista avainta. "+" -merkki näyttää tässä dokumentissa olevan rivinvaihdon.

B02K_CUSTNAME&B02K_KEYVERS&B02K_ALG&+
B02K_CUSTID&B02K_CUSTTYPE&tarkisteavain&

4.7. Tunnisteen tyyppi

Vastaussanomien tarkisteen laskentaan vaikuttaa välitettävän asiakastunnisteen tyyppi, joka määrittää tunnistepyyntöä A01Y_IDTYPE-kentässä. Asiakkaan tunniste on joko 1) selväkielinen asiakastunnus tai 2) salattu tarkiste

1. Asiakkaan tunnisteena selväkielinen asiakastunnus

Tunnistuspyynnön A01Y_IDTYPE-kentän arvot ”02” ja ”03”: Selväkielinen perustunnus tai työstetty perustunnus.

Asiakkaan tunnus on selväkielinen merkkijono, esimerkiksi henkilötunnus tai sen loppuosa tunnistepyyntöä A01Y_IDTYPE mukaisesti. Tunnus sijoitetaan sellaisenaan vastaussanomien tiedoksi B02K_CUSTID.

2. Asiakkaan tunnisteena salattu tarkiste

Tunnistuspyynnön A01Y_IDTYPE-kentän arvo on ”01” eli salattu perustunnus.

Pankki käyttää asiakastunnuksen salaamisessa samaa tiivistealgoritmia kuin sanomien tarkistelaskennassa. Tunnistetieto salataan käyttämällä vastaussanomien tietokentissä 2-4 olevia tietoja ja pankissa rekisteröityä asiakkaan tunnusta (henkilötunnus tai Y-tunnus). Salattun tunnuksen laskennassa tiedot ja tarkisteavain erotetaan toisistaan &-merkillä, joka lisätään myös tarkisteavaimen loppuun. Salaamisessa käytetään palveluntuottajakohtaista avainta. "+" -merkki näyttää tässä dokumentissa olevan rivinvaihdon.

B02K_TIMESTAMP&B02K_IDNBR&B02K_STAMP&+
asiakastunnus&tarkisteavain&

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

4.8. Sanoman tarkisteen tarkastus ja asiakkaan tunnistus

Palveluntuottaja laskee vastaanottamastaan sanomasta kohdassa 4.6 kuvatulla tavalla vastaanotetun sanoman MAC-tarkisteen. Mikäli se on sama kuin vastaussanomassa pankista tullut vastaussanomien tarkiste, on vastaussanoma välittynyt muuttumattomana.

Jos vastaussanomassa on käytetty salattua tunnusta, tarkistaa palveluntuottaja käytössään olevan asiakkaan tunnuksen oikeellisuuden laskemalla tarkisteen vastaussanomien tietokentistä ja käytössään olevasta tunnuksesta kohdassa 4.7 esitetyllä tavalla. Mikäli saatu tarkiste vastaa vastaussanomien tunnistekentän (B02K_CUSTID) sisältöä, palveluntuottajalla käytössä oleva asiakkaan tunniste oikea.

5. Poikkeustilanteet

Palveluntuottajan on varauduttava poikkeustilanteisiin, joita voivat olla:

1. Asiakas keskeyttää tunnistustapahtuman. Asiakas voi keskeyttää tapahtuman joko ennen tunnisteen välittämistä POP Pankin tunnistuspalveluun tai tunnisteen luonnin jälkeen peruuta-painikkeella, jossa osoitteena on tunnistepyyynnön FORM-tietokentässä 8 oleva Peruuta-osoite.
2. Asiakkaan todennus epäonnistuu joko asiakkaan antamien tunnistetietojen virheellisyyden takia tai koska asiakas on pyytänyt todennusta väärästä pankista.
3. POP Pankin tunnistuspalvelu havaitsee virheen tunnistepyyntösanomassa.
4. Palveluntuottaja havaitsee virheen vastaussanomassa, joka voi johtua sanoman sisällössä olevasta virheestä tai siitä, että tunniste ei vastaa asiakkaan ilmoittamia henkilötietoja. Palveluntuottajan tulee antaa asiakkaalle tilannetta vastaava ilmoitus.
5. Vastausta ei tule lainkaan. Katkoksen syynä voi olla yhteyskatko tai muu tekninen häiriö, tai asiakas jättää istunnon kesken.
6. Sama vastaus tulee useita kertoja. Palveluntuottajan on varauduttava, että asiakas voi lähettää saman vastauksen useaan kertaan tai asiakas voi lähettää vanhan vastaussanoma siirtyessään selaimensa ikkunoissa eteen / taakse -näppäimillä ruudusta toiseen.

6. Tarkisteavaimen vaihto ja säilytys

Tarkisteiden laskennassa käytettyä MAC-avainta voidaan vaihtaa POP Pankin tunnistuspalvelun tai palveluntuottajan toivomuksesta.

Tarkisteavain toimitetaan sopimuksessa mainitulle yhteyshenkilölle. Samalla toimitetaan myös tieto uuden avaimen versionumerosta ja voimaantumispäivästä. Ko. päivästä lähtien tarkisteet lasketaan kyseisellä avaimella.

Joustavan avainvaihdon takaamiseksi on palveluntuottajan järjestelmän mahdollistettava uuden avaimen syöttö järjestelmään etukäteen, eli vähintään kahden tarkisteavaimen yhtäaikainen käyttö. Vaihtohetkellä, n. 15 minuutin ajan, on mahdollista, että osassa palveluntuottajalle tulevista tunnisteista tarkiste on laskettu vanhalla avaimella ja osa uudella.

Kun uutta tarkisteavainta on käytetty onnistuneesti, voidaan vanha avain poistaa tai sen käyttö estää palveluntuottajan järjestelmässä.

Palveluntarjoajan tulee säilyttää MAC-tarkisteavain huolellisesti ja turvassa oikeudettomalta käytöltä.

7. POP Pankin tunnistuspalvelun nimi ja logo

Pankin verkkotunnistuksesta voidaan käyttää joko nimeä POP Pankin tunnistus tai POP Bankens identifiering. Muita nimityksiä ei saa käyttää.

POP Pankin tunnistuksen logona on POP Pankin liikemerkki.

Palvelua tarjoava yritys kopioi logon omalle palvelimellensa Samlinkin palvelimelta osoitteesta <http://193.65.156.50/POPmaksunappi.png>

Logon kokoa ja värejä ei saa muuttaa.

Logoa/nimeä ei saa luovuttaa tai käyttää muuhun tarkoitukseen kuin POP Pankin tunnistuspalvelun sopimuksessa on sovittu.

Sopimuksen päättymisen jälkeen palveluntarjoajan on välittömästi poistettava sivuiltaan POP Pankin tunnistuspalvelun logo/nimi.

8. POP Pankin tunnistuspalvelun käyttöönotto

8.1. Edellytykset

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

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

8.2. Sopimukset

Palveluntarjoaja tekee kirjallisen sopimuksen POP Pankin tunnistuspalvelun käytöstä pankin kanssa. Palveluntarjoajan tiedot rekisteröidään pankissa ja sopimuksessa mainitulle yhteyshenkilölle lähetetään Turvatarkiste kahdessa osassa. Turvatarkisteen jälkimmäinen osa lähetetään sähköpostilla Pankin kanssa sovitulle vastaanottajalle.

Kustakin eri palvelusta tulee tehdä palvelusopimus, samoin jokaisesta toiminnallisuudesta. Yhdessä palvelussa voi kuitenkin olla käytössä useita toiminnallisuuksia. Pankki tekee sopimuksen henkilötunnuksen välittämisestä vain silloin kuin palveluntarjoajalla on oikeus rekisteröidä se.

Palvelussa käytettävän tarkisteavaimen pituus ja palveluntarjoajan oikeus henkilötunnuksen rekisteröintiin merkitään sopimukseen.

Palveluntarjoajan tulee ilmoittaa pankin konttoriin, jos hänen palveluunsa tai tietoihinsa tulee muutoksia. Konttori täydentää tarvittaessa sopimusta muuttuneilla tiedoilla.

8.3. Testaus

Palvelun käyttöönottopäivä sovitaan sopimuksen teon yhteydessä.

Palveluntuottaja voi testata palvelua tuotantoympäristössä jo ennen kuin sopimus on tehty käyttämällä testitunnuksia.

Internet-palvelun osoite: <https://tupas.poppankki.fi>

Palveluntuottaja: 11111111111111
Tarkisteavain: 11111111111111111111
Tunnisteen tyyppi: 02

Tunnistusnäytössä asiakkaan käyttämät tunnukset
Käyttäjätunnus: 11111111
Salasana: 123456

TUNNISTEPYYNTÖ –TESTISANOMA	
Form-tietokenttä	
A01Y ACTION_ID	701
A01Y VERS	0002
A01Y RCVID	111111111111
A01Y LANGCODE	kts. kuvaus
A01Y STAMP	kts. kuvaus
A01Y IDTYPE	kts. kuvaus
A01Y RETLINK	kts. kuvaus
A01Y CANLINK	kts. kuvaus
A01Y REJLINK	kts. kuvaus
A01Y KEYVERS	0001
A01Y ALG	03
A01Y MAC	kts. kuvaus

VASTAUSSANOMA	
B01Y VERS	0002
B02K TIMESTMP	kts. kuvaus
B02K IDNBR	kts. kuvaus
B01Y_STAMP	Kyselyn tietokenttä A01Y_STAMP
B02K_CUSTNAM	Teemu Testaaja
B01Y KEYVERS	0001
B01Y ALG	03
B02K_CUSTID	Perustunnus: 010101-123N Typistetty tunnus: 123N Salattu tunnus: Laskettu tunnuksesta 010100-123N
B02K_CUSTTYPE	kts. kuvaus
B01Y_MAC	kts. kuvaus

9. Neuvonta ja tekninen tuki

Ongelmatilanteissa auttaa

Asiakasyhteysneuvonta	0100 4752 (1,17€/min+ pvm).
Sähköposti	info@samlink.fi

Palveluntarjoajan tunnuksen ilmoittaminen nopeuttaa asiointia.

Palvelu käyttää 8 bittistä ISO 8859-1 (Latin1) merkistöä, joiden koodit on lueteltu ohisessa taulukossa.

æ	%00	0	%30	`	%60	‘	%90	À	%c0	ð	%f0
	%01	1	%31	a	%61	’	%91	Á	%c1	ñ	%f1
	%02	2	%32	b	%62	“	%92	Â	%c2	ò	%f2
	%03	3	%33	c	%63	”	%93	Ã	%c3	ó	%f3
	%04	4	%34	d	%64	•	%94	Ä	%c4	ô	%f4
	%05	5	%35	e	%65	—	%95	Å	%c5	õ	%f5
	%06	6	%36	f	%66	—	%96	Æ	%c6	ö	%f6
	%07	7	%37	g	%67		%97	Ç	%c7	÷	%f7
Backspace	%08	8	%38	h	%68	~	%98	È	%c8	ø	%f8
Tab	%09	9	%39	i	%69	™	%99	É	%c9	ù	%f9
Linefeed	%0a	:	%3a	j	%6a	š	%9a	Ê	%ca	ú	%fa
	%0b	;	%3b	k	%6b	›	%9b	Ë	%cb	û	%fb
	%0c	<	%3c	l	%6c	œ	%9c	Ì	%cc	ü	%fc
C return	%0d	=	%3d	m	%6d		%9d	Í	%cd	ý	%fd
	%0e	>	%3e	n	%6e		%9e	Î	%ce	þ	%fe
	%0f	?	%3f	o	%6f	ÿ	%9f	Ï	%cf	ÿ	%ff
	%10	@	%40	p	%70		%a0	Ð	%d0		
	%11	A	%41	q	%71	ı	%a1	Ñ	%d1		
	%12	B	%42	r	%72	ç	%a2	Ò	%d2		
	%13	C	%43	s	%73	£	%a3	Ó	%d3		
	%14	D	%44	t	%74		%a4	Ô	%d4		
	%15	E	%45	u	%75	¥	%a5	Õ	%d5		
	%16	F	%46	v	%76		%a6	Ö	%d6		
	%17	G	%47	w	%77	§	%a7		%d7		
	%18	H	%48	x	%78	¨	%a8	Ø	%d8		
	%19	I	%49	y	%79	©	%a9	Ù	%d9		
	%1a	J	%4a	z	%7a	ª	%aa	Ú	%da		
	%1b	K	%4b	{	%7b	«	%ab	Û	%db		
	%1c	L	%4c		%7c	¬	%ac	Ü	%dc		
	%1d	M	%4d	}	%7d	—	%ad	Ý	%dd		
	%1e	N	%4e	~	%7e	®	%ae	Þ	%de		
	%1f	O	%4f		%7f	—	%af	ß	%df		
Space	%20	P	%50	€	%80	°	%b0	à	%e0		
!	%21	Q	%51		%81	±	%b1	á	%e1		
”	%22	R	%52	,	%82	²	%b2	â	%e2		
#	%23	S	%53	f	%83	³	%b3	ã	%e3		
\$	%24	T	%54	”	%84	´	%b4	ä	%e4		
%	%25	U	%55	...	%85	µ	%b5	å	%e5		
&	%26	V	%56	†	%86	¶	%b6	æ	%e6		
’	%27	W	%57	‡	%87	·	%b7	ç	%e7		
(%28	X	%58	^	%88	,	%b8	È	%e8		
)	%29	Y	%59	%o	%89	ı	%b9	É	%e9		
*	%2a	Z	%5a	Š	%8a	°	%ba	Ê	%ea		
+	%2b	[%5b	‹	%8b	»	%bb	Ë	%eb		
,	%2c	\	%5c	OE	%8c	¼	%bc	Ì	%ec		
-	%2d]	%5d	Ž	%8d	½	%bd	Í	%ed		
.	%2e	^	%5e		%8e	¾	%be	Î	%ee		
/	%2f	_	%5f		%8f	¿	%bf	Ï	%ef		