

**Pankkien TUPAS-tunnistuspalvelu  
palveluntarjoajille**

**Palvelukuvaus ja palveluntarjoajan ohje**

**Versio 2.3c  
28.3.2011**





28.3.2011

## MUUTOSLUETTELO

<u>Versio</u>	<u>Sivu</u>	<u>Huomautus</u>
V2.0	Kaikki	Sanomarakenteet muuttuneet
V2.1		Lisätty uusia pankkeja, sanontoja muutettu
V2.2		Uusia sanomakenttiä sekä sanomakenttien piirteitä Tarkista pankista, ovatko uudet piirteet otettu käyttöön.
V2.3		Nimi muutettu tunnistuspalveluksi ja luovuttu termin "varmenne" käytöstä. Yhteystiedot ja yleiskuvaus siirretty tunnistusperiaatteisiin. Lisätty SHA-256 algoritmi.
V2.3b	7-9	Korjattu SHA-256 algoritmin tarkisteen pituus
V2.3c	8	Tarkennettu SHA-256 algoritmin käyttöönoton aikataulu ja korjattu kenttien B02K_CUSTID ja B02K_USERID enimmäispituus

## HYVÄKSYMINEN

<u>Versiotunnus</u>	<u>Päivämäärä</u>	<u>Hyväksyjä</u>
V2.0	13.6.2002	Maksuliikennetoimikunta
V2.1	3.10.2005	Maksuliikennetoimikunta
V2.2	17.10.2006	Maksuliikennetoimikunta
V2.3	15.3.2010	Maksuliiketoimikunta
V2.3c	20.1.2011	Maksuliiketoimikunta



28.3.2011

## Sisällysluettelo

1 Tupas-palvelun toiminnallisuudet.....	4
2 Palvelun turvallisuus.....	4
3 Palvelun toiminnallinen kuvaus.....	5
4 Tupas-palvelun sanomat ja niiden tiedot.....	7
4.1 Tunnistuspyyntö.....	7
4.2 Tunnistuspyynnön kenttien selitykset:.....	8
4.3 Tunnistuspyynnön MAC-tarkisteen (A01Y_MAC) muodostaminen.....	9
4.4 Vastaussanoma eli Tupas-tunniste ja sen yksilöintitiedot.....	9
4.5 Vastaussanomien kenttien selitykset:.....	10
4.6 Tunnisteen tarkisteen laskenta.....	11
4.7 Yksilöintitiedon tyyppi.....	11
4.7.1 Selväkielinen yksilöintitieto.....	11
4.7.2 Salattu yksilöintitieto.....	11
4.8 Salatun yksilöintitiedon vertailu ja asiakkaan tunnistus.....	12
4.9 Poikkeustilanteet.....	12
5 Tarkisteavaimen vaihto.....	13
6 Palvelussa käytettävä merkistö.....	13
LIITE 1 TUNNISTUSPYYNNÖN YKSILÖINTITIEDON TYYPPI (A01Y_IDTYPE).....	14
LIITE 2 TUPAS-TUNNISTEEN YKSILÖINTITIETO.....	15



28.3.2011

## 1 Tupas-palvelun toiminnallisuudet

Tupas-palvelun yleiskuvaus, hallinnolliset tiedot, palvelusta sopiminen ja palvelun käyttö ovat kuvattu tunnistusperiaatteissa "Pankkien Tupas-tunnistuspalvelun tunnistusperiaatteet".

Tupas-palvelussa on eri toiminnallisuuksia ja käyttömahdollisuuksia sen mukaan, millaisen tunnisteiden välittämisestä palveluntarjoaja on palvelusopimuksessaan pankin kanssa sopinut. Pankin antama tunniste sisältää aina asiakkaan nimen. Tämän lisäksi välitettävä asiakkaan yksilöintitieto voi olla joko selväkielinen tai salattu.

Yksilöintitiedon ollessa selväkielinen, pankki voi välittää asiakkaan henkilötunnuksen, henkilötunnuksen tarkisteosan, Y-tunnuksen tai muun sähköisen asiointitunnuksen sen mukaan, mistä on sovittu palvelusopimuksessa. Selväkielisen henkilötunnuksen pankki välittää vain palveluntarjoajille, joilla on oikeus rekisteröidä se.

Kun yksilöintitieto on salattu, pankki välittää palveluntarjoajalle tiedon, joka perustuu asiakkaan henkilötunnukseen, Y-tunnukseen tai muuhun sähköiseen asiointitunnukseen. Itse tunnus ei kuitenkaan välity vastaussanomana mukana. Siksi palveluntarjoajalla tulee olla käytössään asiakkaan henkilötunnus, Y-tunnus tai muu sähköinen asiointitunnus, jotta hän voi varmistua pankin antaman vastaussanomien tietojen avulla asiakkaan henkilöllisyyden oikeasta todennuksesta. Jos palveluntarjoajalla ei ole asiakkaan tunnusta, hänen tulee kysyä se ennen tunnustuspyynnön lähettämistä. Tämä toiminnallisuus soveltuu siten asiakkaan ilmoittamien tietojen oikeellisuuden tarkastamiseen pankista.

Tupas-palvelu soveltuu pääasiassa kuluttajille suunnattuihin palveluihin. Eräissä pankeissa on mahdollista tunnistaa myös pankin yritysasiakkaita Y-tunnuksen avulla, mutta kaikki pankit eivät rekisteröi yrityksiä verkkopankkien asiakkaita. Kaikki pankit eivät tarjoa tunnustuspalvelua, jossa yritysasiakas tunnustetaan. Tunnistettaessa pankin yritysasiakkaita voidaan pankista välittää tunnisteiden mukana joko asiakkaan Y-tunnus ja yrityksen nimi tai asiakkaan Y-tunnus, yrityksen nimi, henkilön nimi sekä henkilötunnus.

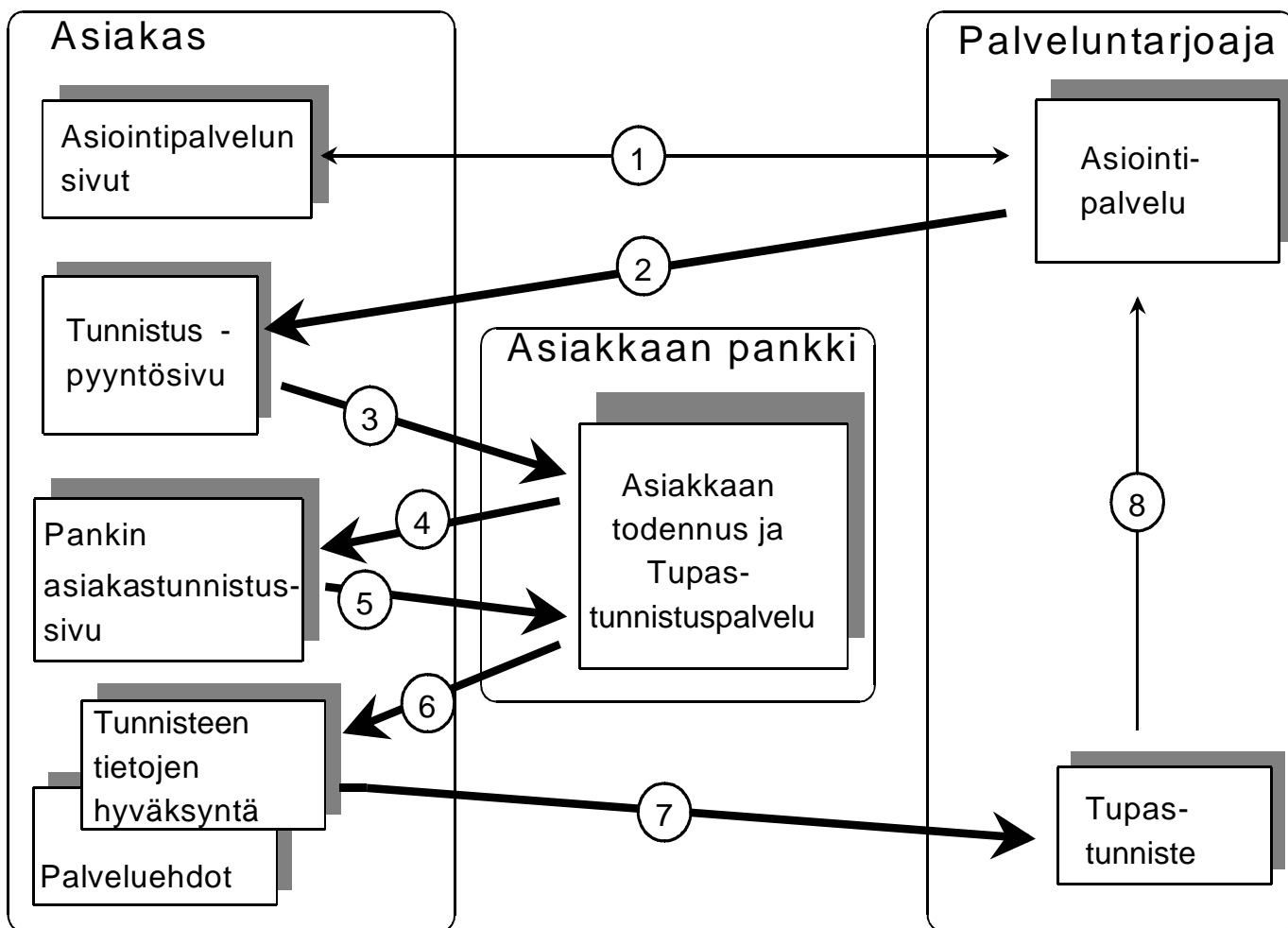
## 2 Palvelun turvallisuus

Tupas-palvelun osapuolten välisessä tietoliikenteessä käytetään SSL-siirtokäytäntöä, joten ulkopuoliset eivät näe tietoja eivätkä voi muuttaa niitä. Palveluntarjoajan palvelinohjelmiston on tuettava 128 bitin avaimilla toteutettua SSL-salausta. Yhteydellä käytettävä avainpituus määräytyy kuitenkin asiakkaan käyttämän selaimen ominaisuuksien perusteella. Tunnustuspyynnön ja tunnisteiden tiedot on suojattu tiedon eheyden turvaavalla tarkisteella, joten tunnisteiden välitystä ohjaavalla asiakkaalla ei ole mahdollisuutta muuttaa tietoja palveluntarjoajan tai pankin sitä havaitsematta.

Kukin osapuoli vastaa omien palveluittensa suojauksesta, turvallisuudesta ja säilyttämiensä tietojen oikeellisuudesta. Tunnistautuva asiakas vastaa siitä, että pankin antamat pankkitunnukset eivät joudu ulkopuolisten haltuun.

28.3.2011

### 3 Palvelun toiminnallinen kuvaus



Palvelun etenemistä kuvaavan kaavion selite:

1. Tunnistautuva asiakas on yhteydessä palveluntarjoajan palveluun. Asiakkaan ja palveluntarjoajan välisen tietoliikenteen tulee olla SSL-suojattu, kun asiakas siirtyy tunnistuspalveluun liittyvien tietojen syöttöön. Vaiheiden 2 - 7 aikana tiedonsiirtoyhteys on aina SSL-suojattu.
2. Palveluntarjoaja lähettää asiakkaalle tunnistuspyynnön, joka sisältää tapahtumaan liittyvät yksilöintitiedot. Asiakas tarkastaa vastaanottamansa pyynnön tiedot, mutta hän ei voi muuttaa niitä. Asiakas voi halutessaan keskeyttää tunnistuksen ja palata takaisin asiointipalveluun. Asiakkaan selaimen tunnistuspyyntösivulla ovat Tupas-palveluun johtavat toimintopainikkeet ja peruutuspainike.
3. Asiakas painaa toimintopainiketta, joka johtaa hänen pankkinsa tunnistuspalveluun. Pankkiin välittyvä tunnistuspyyntö sisältää tunnistuspalvelun tarvitsemat tiedot palveluntarjoajasta ja tapahtumasta. Pankki tarkastaa pyynnön eheyden ja tietojen oikeellisuuden.



28.3.2011

4. Pankki lähettää asiakkaalle tunnistuspyynnön, jos palveluntarjoajan tunnistuspyyntö on virheetön. Pankki antaa asiakkaalle virheilmoituksen, jos pankki havaitsee tunnistuspyynnössä virheitä, jolloin asiakas palaa tapahtuman peruutuspainikkeella takaisin palveluntarjoajan palveluun.
5. Asiakas tunnistautuu pankkiinsa. Pankki palauttaa asiakkaalle virheilmoituksen, jos tunnistus epäonnistuu, jolloin asiakas palaa peruutuspainikkeella takaisin palveluntarjoajan palveluun.
6. Onnistuneen tunnistuksen jälkeen pankki muodostaa vastaussanomana, ”Tupas-tunnisteen”. Pankin Tupas-palvelu asettaa asiakkaalle hyväksymis- ja peruutuspainikkeet.
7. Asiakas tarkastaa tunnisteiden tiedot ja hyväksyy tunnisteiden välittämisen palveluntarjoajalle. Asiakas voi peruutuspainikkeella keskeyttää tunnistustapahtuman ja palata takaisin palveluntarjoajan palveluun.
8. Palveluntarjoaja varmistaa vastaanottamansa Tupas-tunnisteiden eheyden ja ainutkertaisuuden. Palveluntarjoaja liittää tunnisteiden asiakkaan palvelutapahtumaan ja säilyttää sitä yhtä kauan kuin muita palvelutietoja säilytetään. Asiakkaan yksilöintitietoja ei saa rekisteröidä tai käyttää muuhun tarkoitukseen.



28.3.2011

## 4 Tupas-palvelun sanomat ja niiden tiedot

### 4.1 Tunnistuspyyntö

Tunnistuspyynnön tiedot ovat pankkikohtaisen painikkeen tai kuvakkeen takana FORM-tietoryhmässä piilomuuttujina.

FORM-TIETORYHMÄ			
Kenttä	Tiedon nimi	Pituus	Huomaus
1. Sanomatyyppi	A01Y_ACTION_ID	3 - 4	Vakio, "701"
2. Versio	A01Y_VERS	4	Esim. "0002"
3. Palveluntarjoaja	A01Y_RCVID	10 -15	Asiakastunnus
4. Palvelun kieli	A01Y_LANGCODE	2	ISO 639:n mukainen tunnus: FI = Suomi SV = Ruotsi EN = Englanti
5. Pyynnön yksilöinti	A01Y_STAMP	20	Vvvvkkpphhmssxxxxxx
6. Yksilöintitiedon tyyppi	A01Y_IDTYPE	2	ks. liite 1
7. Paluuosoite	A01Y_RETLINK	199	OK paluuosoite tunnisteelle
8. Peruuta-osoite	A01Y_CANLINK	199	Paluuosoite peruutuksessa
9. Hylätty-osoite	A01Y_REJLINK	199	Paluuosoite virhetilanteessa
10. Avainversio	A01Y_KEYVERS	4	Avaimen sukupolvitieto
11. Algoritmi	A01Y_ALG	2	01 = MD5 02 = SHA-1 03 = SHA-256
12. Tarkiste	A01Y_MAC	32 - 64	Pyynnön turvatarkiste

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

```
<FORM METHOD="POST" ACTION="pankin Tupas-palvelun 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>
```



28.3.2011

#### 4.2 Tunnistuspyynnön kenttien selitykset:

- Kenttä 1 Sanoman tyyppi, joka on Tupas-palvelussa vakio "701".
- Kenttä 2 Tunnistuspyyntö-sanoman versionumero, joka on pankkikohtainen.
- Kenttä 3 Kentässä on palveluntarjoajan pankkikohtainen asiakastunnus. Pankki tunnistaa palveluntarjoajan asiakastunnuksen perusteella ja liittää rekisterissään olevan palveluntarjoajan nimen Tupas-tunnisteeseen.
- Kenttä 4 Palvelun kielikoodi kertoo palveluntarjoajan asiointisivun kielen ja pankin palvelu 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 Yksilöintitiedon tyyppi kertoo, minkä yksilöintitiedon palveluntarjoaja tunnistettavasta asiakkaastaan haluaa. Yksilöintitiedon tyyppin tulee vastata palvelusopimuksessa sovittua toiminnallisuutta.
- Kenttä 7 Palveluntarjoajan asiointisivun osoite, joka on OK-tapauksessa jatkokohta. Paluusoitteen tulee olla https-alkuinen, eli SSL-suojattu sivu.  
Esimerkki: VALUE="https://tuote.kauppa.fi/tilaus/vahvistus.htm"
- Kenttä 8 Palveluntarjoajan palvelun jatkokohta, jos asiakas peruu tunnisteiden välittämisen.  
Esimerkki: VALUE="https://tuote.kauppa.fi/tilaus/keskeytyk.htm"
- Kenttä 9 Palveluntarjoajan palvelun jatkokohta, jos tunnistuksessa on havaittu tekninen virhe. Paluusoite voi olla sama kuin kentässä 9.  
Esimerkki: VALUE="https://tuote.kauppa.fi/tilaus/virhe.htm"
- Kenttä 10 MAC-tarkisteen laskennassa käytetyn avaimen versio.
- Kenttä 11 MAC-tarkisteen laskennassa käytettävän algoritmin tyyppikoodi.  
01 = MD5 algoritmi, joka tuottaa 32 merkkisen MACin  
02 = SHA-1 algoritmi, joka tuottaa 40 merkkisen MACin.  
03 = SHA-256 algoritmi, joka tuottaa 64 merkkisen MACin.
- Siirtymäaikana 1.4-31.12.2011 otetaan käyttöön SHA-256 algoritmi (tyyppikoodi 03) ja luovutaan tyyppikoodeista 01 ja 02.
- Kenttä 12 MAC-tarkiste, joka on laskettu tunnistuspyynnön suojattavista tiedoista ja palveluntarjoajan tarkisteavaimesta tietokentässä 11 määritellyillä algoritmeilla. Tarkisteen avulla sanoman vastaanottaja voi varmistaa tunnisteiden eheyden ja lähettäjän.



28.3.2011

### 4.3 Tunnistuspyynnön MAC-tarkisteen (A01Y\_MAC) muodostaminen

Palveluntarjoaja muodostaa kunkin pankin painiketta varten oman pankkikohtaisen tunnistuspyynnön, joka suojataan MAC-tarkisteella. Tarkiste lasketaan pankkikohtaisen pyynnön FORM-tietoryhmästä ko. pankin palveluntarjoajalle antamalla tarkisteavaimella.

Laskennan aluksi muodostetaan merkkijono FORM-tietoryhmän kaikkien tarkistetta edeltävien tietokenttien (kentät 1 - 11) VALUE-arvoista ja palveluntarjoajan tarkisteavaimesta. Tiedot yhdistetään merkkijonoksi järjestyksessä niin, että kenttien täytemerkkeinä olevat blankot jätetään pois. Merkkijonon tietoryhmät erotetaan toisistaan "&" -merkillä. Viimeisen tiedon (kenttä 11) 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 Tarkiste-kenttään.

### 4.4 Vastaussanoma eli Tupas-tunniste ja sen yksilöintitiedot

VASTAUSSANOMA				
Kenttä	Tiedon nimi	Pituus	Pakollisuus <sup>1)</sup>	Huomaus
1. Versio	B02K_VERS	4	P	Esim. "0002"
2. Tunnisteen yksilöinti	B02K_TIMESTMP	23	P	NNNvvvkkpphhmmssxxxxx x
3. Tunnisteen numero	B02K_IDNBR	10	P	Pankin tunnisteelle antama numero
4. Pyynnön yksilöinti	B02K_STAMP	20	P	Kyselyn tietokenttä 7 ( A01Y_STAMP)
5. Asiakas	B02K_CUSTNAME	-40	P	Pankin tietokannassa oleva tunnistetun henkilön tai yrityksen nimi
6. Avainversio	B02K_KEYVERS	4	P	Avaimen sukupolvi
7. Algoritmi	B02K_ALG	2	P	01 = MD5 02 = SHA-1 03 = SHA-256
8. Yksilöintitieto	B02K_CUSTID	-64	P	ks. liite 2
9. Yksilöintitiedon tyyppi	B02K_CUSTTYPE	2	P	ks. liite 2
10. Käyttäjän tunnus	B02K_USERID	-64	V	Yrityskäyttäjän henkilötunnus tai salattu tunnus , ks. liite 2
11. Käyttäjän nimi	B02K_USERNAME	-40	V	Yrityskäyttäjän nimi ks. liite 2
12. Tarkiste	B02K_MAC	32 - 64	P	Vastauksen turvatarkiste



28.3.2011

<sup>1)</sup> Tiedon pakollisuus:

P = pakollinen,  
V = vain pyydettyessä

Asiakkaan pankki lisää Tupas-tunnisteen tiedot OK-paluulinkkiin ns. query-string muodossa.

```
http://A01Y_RETLINK?↵  
B02K_VERS&B02K_TIMESTMP&B02K_IDNBR&B02K_STAMP&↵  
B02K_CUSTNAME&B02K_KEYVERS&B02K_ALG&B02K_CUSTID&↵  
B02K_CUSTTYPE&B02K_USRID&B02K_USERNAME&B02K_MAC
```

Tiedot *B02K\_USRID* ja *B02K\_USERNAME* ovat optionaalisia ja ne ovat mukana vain tunnisteiden tyypin arvoilla ”08” ja ”09”.

#### 4.5 Vastaussanomien kenttien selitykset:

- |           |  |
|-----------|--|
| Kenttä 1  | Tupas-tunnisteen versionumero, joka on pankkikohtainen.  |
| Kenttä 2  | Pankin järjestelmän muodostama aikaleima, jossa NNN on pankin numero:<br><br>Handelsbanken = 310<br>Nordea Pankki Suomi = 200<br>Osuuspankkiryhmä = 500<br>S-Pankki = 390<br>Sampo Pankki = 800<br>Aktia, Säästöpankit ja Paikallisosuuspankit = 400<br>Tapiola Pankki = 360<br>Ålandsbanken = 600 |
| Kenttä 3  | Pankin tietojärjestelmän tunnisteelle antama tieto, joka yksilöi sen pankin järjestelmässä.  |
| Kenttä 4  | Tunnistuspyynnön yksilöintitieto, joka on poimittu kyseisen tunnistuspyynnön tietokentästä 7 (A01Y_STAMP)  |
| Kenttä 5  | Pankin asiakastietokannassa oleva tunnistetun asiakkaan nimi.  |
| Kenttä 6  | MAC-tarkisteavaimen sukupolvitieto.  |
| Kenttä 7  | MAC-tarkistealgoritmin tunnus.   |
| Kenttä 8  | Asiakkaan yksilöintitieto, jonka sisältö riippuu tunnistuspyynnön A01Y_IDTYPE-kentän sisällöstä. Kentän sisältö voi siis vaihtoehtoisesti joko salattu yksilöintitieto tai selväkielinen asiakastunnus.  |
| Kenttä 9  | Yksilöintitiedon tyyppi.   |
| Kenttä 10 | Tupas-tunnisteen tarkiste.   |



28.3.2011

## 4.6 Tunnisteen tarkisteen laskenta

Tarkiste (*B02K\_MAC*) lasketaan alkuperäisestä sanomasta, jonka jälkeen skandinaaviset merkit ja eräät erikoismerkit (esim. tyhjämerkit, yhtäläisyys- ja lainausmerkit) korvataan vastaavalla heksadesimaalimerkillä (esim. %20) tietoliikennesanomassa.

Pankki laskee Tupas-tunnisteen MAC-tarkisteen palveluntarjoajakohtaisella avaimella. Tarkisteen avulla palveluntarjoaja voi varmistua, että tunniste on muodostettu asiakkaan pankissa ja sen sisältö on muuttumaton.

Vastaussanomien yksilöintitiedon tyyppien arvoilla ”00”-”07” tarkiste lasketaan vastaussanomien tietokentistä 1-9. Tarkisteen laskennassa tiedot ja tarkisteavain erotetaan toisistaan ”&”-merkillä, joka lisätään myös tarkisteavaimen loppuun. Tarkisteen laskennassa käytetään palveluntuottajakohtaista avainta. Turvatarkisteen laskentaa optiokenttien 10 ja 11 osalta ei tehdä, mikäli ne ovat molemmat tyhjiä eikä kenttiä silloin palauteta takaisin palveluntuottajalle.

```
B02K_VERS&B02K_TIMESTMP&B02K_IDNBR&B02K_STAMP&␣  
B02K_CUSTNAME&B02K_KEYVERS&B02K_ALG&B02K_CUSTID&␣  
B02K_CUSTTYPE&tarkisteavain&
```

Vastaussanomien yksilöintitiedon tyyppien arvoilla ”08” ja ”09” tarkiste lasketaan vastaussanomien tietokentistä 1-11. Tarkisteen laskennassa tiedot ja tarkisteavain erotetaan toisistaan ”&”-merkillä, joka lisätään myös tarkisteavaimen loppuun. Tarkisteen laskennassa käytetään palveluntuottajakohtaista avainta.

```
B02K_VERS&B02K_TIMESTMP&B02K_IDNBR&B02K_STAMP&␣  
B02K_CUSTNAME&B02K_KEYVERS&B02K_ALG&B02K_CUSTID&␣  
B02K_CUSTTYPE&B02K_USRID&B02K_USERNAME&tarkisteavain&
```

## 4.7 Yksilöintitiedon tyyppi

Tupas-tunnisteen tarkisteen laskentaan vaikuttaa välitettävän yksilöintitiedon tyyppi, joka määritellään tunnistuspyynnön *A01Y\_IDTYPE*-kentässä.

### 4.7.1 Selväkielinen yksilöintitieto

Tunnistuspyynnön *A01Y\_IDTYPE*-kentän arvot ovat ”02” tai ”03”, eli selväkielinen perustunnus tai selväkielinen työstetty perustunnus.

Yksilöintitieto on selväkielinen merkkijono, esimerkiksi henkilötunnus tai sen loppuosa pyyntösanoman kentän *A01Y\_IDTYPE* mukaisesti. Yksilöintitieto sijoitetaan sellaisenaan vastaussanomien tiedoksi *B02K\_CUSTID*.

### 4.7.2 Salattu yksilöintitieto

Tunnistuspyynnön *A01Y\_IDTYPE*-kentän arvo on ”01” eli salattu perustunnus.

Pankki käyttää yksilöintitiedon salaamisessa samaa tiivistealgoritmia kuin sanomien tarkistelaskennassa. Yksilöintitiedon yksilöllisyys varmistetaan käyttämällä lisätietoina tunnisteiden



28.3.2011

tietokentissä 2-4 olevia tietoja ja tunnistuspyynnön tietokentän 8 (A01Y\_IDTYPE) mukaisia asiakkaan tunnusta (henkilötunnus tai Y-tunnus). Salatun yksilöintitiedon laskennassa tiedot ja tarkisteavain erotetaan toisistaan "&"-merkillä, joka lisätään myös tarkisteavaimen loppuun. Salaamisessa käytetään palveluntarjoajakohtaista avainta.

```
B02K_TIMESTAMP&B02K_IDNBR&B02K_STAMP&/  
asiakkaan_tunnus&tarkisteavain&
```

Laskennan lopputulos muutetaan heksadesimaaliseen esitysmuotoon, jossa arvot A-F esitetään isoilla kirjaimilla. Lopputuloksena saadaan asiakkaan yksilöintitiedoksi merkkijono, joka sijoitetaan tunnisteiden tiedoksi B02K\_CUSTID.

#### 4.8 Salatun yksilöintitiedon vertailu ja asiakkaan tunnistus

Jos yksilöintitieto on salattu, niin palveluntarjoaja tarkastaa aluksi vastaanottamansa Tupas-tunnisteen eheyden. Seuraavaksi hän laskee rekisteröimästään asiakkaan tunnuksesta kohdassa 3.7.2 kuvatun asiakkaan yksilöintitiedon vertailutiedon.

Kun laskettu vertailutieto ja vastaanotetun tunnisteiden yksilöintitieto ovat identtiset sekä sanna on ehyt, niin pankin tunnistaman asiakkaan tiedot vastaavat palveluntarjoajan rekisteröimän asiakkaan tietoja.

#### 4.9 Poikkeustilanteet

Palveluntarjoajan on varauduttava poikkeustilanteisiin, joita voivat olla:

1. Asiakas keskeyttää tunnistustapahtuman

Asiakas voi keskeyttää tapahtuman joko ennen tunnistuspyynnön välittämistä pankkiin tai vastaanottamansa Tupas-tunnisteen jälkeen peruuta-painikkeella, jossa osoitteena on tunnistuspyynnön FORM-tietokentässä 8 oleva Peruuta-osoite.

2. Asiakkaan todennus epäonnistuu

Asiakkaan todennus voi epäonnistua joko asiakkaan yksilöintitietojen virheellisuuden takia tai asiakas on pyytänyt todennusta väärästä pankista. Asiakas palaa palveluntarjoajan palveluun peruuta-painikkeella, jossa osoitteena on tunnistuspyynnön FORM-tietokentässä 8 oleva Peruuta-osoite.

3. Pankki havaitsee virheen tunnistuspyynnössä

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



28.3.2011

4. Palveluntarjoaja havaitsee virheen Tupas-tunnisteessa.

Palveluntarjoaja havaitsee tunnisteiden tarkastuksen yhteydessä virheen, joka voi johtua tunnisteiden sisällössä olevasta virheestä tai asiakkaan palveluntarjoajalle ilmoittamat tiedot eivät vastaa pankin tietojärjestelmään talletettuja tietoja.

Palveluntarjoajan 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

Palveluntarjoajan on varauduttava, että asiakas voi lähettää saman vastauksen useaan kertaan tai asiakas voi lähettää vanhan Tupas-tunnisteen siirtyessään selaimensa ikkunoissa eteen / taakse -näppäimillä ruudusta toiseen.

## 5 Tarkisteavaimen vaihto

Tarkisteiden laskennassa käytettyä MAC-avainta voidaan vaihtaa pankin tai palveluntarjoajan toivomuksesta. Avaimen vaihdossa noudatetaan pankkikohtaisia menettelyjä, jotka on kuvattu pankkikohtaisissa järjestelmäkuvauksissa.

Avaimen vaihdossa on käytössä kaksi pankkikohtaista menettelyä:

- Vain tarkisteavain vaihdetaan ja palveluntarjoajan asiakastunnus pysyy entisenä.
- Sekä tarkisteavain että asiakastunnus vaihdetaan.

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

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

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

## 6 Palvelussa käytettävä merkistö

Palvelu käyttää 8 bittistä ISO 8859-1 (Latin1) merkistöä.



28.3.2011

## LIITE 1 TUNNISTUSPYYNNÖN YKSILÖINTITIEDON TYYPPI (A01Y\_IDTYPE)

Tunnistuspyynnön tietokenttä 6 määrittelee pyydetyn yksilöintitiedon tyyppin. Tyyppi on koodattu kahdella merkillä XY seuraavasti.

Kympit (X) ilmoittavat pyydetyn yksilöintitiedon sisällön:

- 0Y = perustunnus
- 1Y = Henkilötunnus
- 2Y = Y-tunnus
- 3Y = Henkilötunnus tai y-tunnus
- 4Y = Henkilötunnus ja y-tunnus

Ykköset (Y) ilmoittavat pyydetyn tunnisteiden muodon:

X1 = Salattu tunnus

Asiakkaan yksilöintitiedon perusteella laskettu heksadesimaali-  
muotoinen MAC-tarkisteluku.

X2 = Selväkielinen tunnus

Tunnus voi olla asiakkaan täydellinen tunnus, joka voi olla hen-  
kilötunnus, sähköinen asiointitunnus tai Y-tunnus.

X3 = Typistetty tunnus

Tunnus voi sisältää henkilötunnuksen tarkenneosan ilman vuosi-  
sataa ilmoittavaa välimerkkiä tai kokonaisen Y-tunnuksen.

Huom. Koodi 43 ei ole käytössä.



28.3.2011

## LIITE 2 TUPAS-TUNNISTEEN YKSILÖINTITIETO

Vastaussanomien yksilöintitiedon tyyppien (kenttä 9) tieto on koodattu kahdella merkillä XY siten kymmit (X) ilmoittavat löytyvätkö asiakkaasta pyydettyt tiedot pankin asiakastietokannasta.

OY = Pyydettyt tiedot on löydetty.

Sanoma palautetaan kyselysanoman paluunosoite-kentän osoitteeseen.

00 = tunnus ei ole tiedossa

Arvoa ”00” käytetään, jos mitään tunnustetta ei löydy.

01 = selväkielinen henkilötunnus

Arvoa ”01” käytetään, mikäli on pyydetty selväkielistä tunnusta ja palautetaan vain henkilötunnus.

Kentässä 5 on henkilön nimi ja kentässä 8 on selväkielinen henkilötunnus.

02 = selväkielinen henkilötunnuksen tarkenne

Arvoa ”02” käytetään, mikäli on pyydetty tyypistettyä tunnusta ja palautetaan vain henkilötunnuksen tarkenne.

Kentässä 5 on henkilön nimi ja kentässä 8 on selväkielisen henkilötunnuksen loppuosa.

03 = selväkielinen Y-tunnus

Arvoa ”03” käytetään, mikäli on pyydetty selväkielistä tunnusta ja palautetaan vain y-tunnus.

Kentässä 5 on yrityksen nimi ja kentässä 8 on selväkielinen y-tunnus.

04 = selväkielinen sähköinen asiointitunnus

Arvoa ”04” käytetään, mikäli on pyydetty selväkielistä tunnusta ja palautetaan vain sähköinen asiointitunnus.

Kentässä 5 on yrityksen nimi ja kentässä 8 on selväkielinen asiointitunnus.



28.3.2011

05 = salattu henkilötunnus

Arvoa ”05” käytetään, mikäli on pyydetty salattua tunnusta ja palautetaan vain henkilötunnus.

Kentässä 5 on henkilön nimi ja kentässä 8 on salattu henkilötunnus.

06 = salattu Y-tunnus

Arvoa ”06” käytetään, mikäli on pyydetty salattua tunnusta ja palautetaan vain y-tunnus.

Kentässä 5 on yrityksen nimi ja kentässä 8 on salattu y-tunnus.

07 = salattu sähköinen asiointitunnus

Arvoa ”07” käytetään, mikäli on pyydetty salattua tunnusta ja palautetaan vain sähköinen asiointitunnus (ei käytössä Sammossa).

Kentässä 5 on asiakkaan nimi ja kentässä 8 on salattu sähköinen asiointitunnus.

08 = selväkielinen Y-tunnus ja selväkielinen yrityskäyttäjän henkilötunnus, tai pankin ja palveluntuottajan keskenään sopima muu tunnus

Arvoa ”08” käytetään mikäli on pyydetty selväkielisiä tunnuksia.

Kentässä 5 on yrityksen nimi,  
kentässä 8 on selväkielinen y-tunnus,  
kentässä 10 on selväkielinen yrityskäyttäjän henkilötunnus ja  
kentässä 11 on yrityskäyttäjän nimi

09 = salattu Y-tunnus ja salattu yrityskäyttäjän henkilötunnus, tai pankin ja palveluntuottajan keskenään sopima salattu muu tunnus

Arvoa ”09” käytetään mikäli on pyydetty salattuja tunnuksia.

kentässä 5 on yrityksen nimi,  
kentässä 8 on salattu y-tunnus,  
kentässä 10 on salattu yrityskäyttäjän henkilötunnus ja  
kentässä 11 on yrityskäyttäjän nimi



28.3.2011

1Y = Kaikkia tai osaa pyydettyistä tiedoista ei ole löytynyt.

Kentän Yksilöintitiedon tyyppi (B02K\_CUSTTYPE) tiedot palautetaan kyselysanoman hylätty-osoite-kentässä olevaan osoitteeseen. Yksilöintitiedon tyyppin toinen numero (Y) ilmoittaa, mitä tietoja asiakkaasta ei löydy. Tällöin palveluntarjoaja pystyy automatisoimaan virhevastauksensa asiakkaalle eri tilanteissa.

10 = Ei pyydettyjä tietoja asiakkaasta.

11 = Yritysassiakkaan käyttäjästä ei henkilötunnusta.

12 = Yritysassiakkaasta ei Y-tunnusta.

**Esimerkki:** Palveluntarjoaja haluaa tietää asiakkaan henkilötunnuksen, mutta asiakas käyttää tunnuksia, joista löytyy vain Y-tunnus. Pankki lähettää vastaussanoman hylätty-osoite-kentän osoitteeseen. Vastaussanoman kentässä tunnisteen tyyppi (kenttä 9) palautetaan arvo 11.