

Pankkien TUPAS-varmenne- palvelu palvelun- tarjoajille

Palvelun kuvaus ja palveluntarjoajan ohje

**Versio 2.2
6.2.2007**



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.

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

Sisältö	Sivu
1 Tupas varmennepalvelu	1
1.1 Pankkitunnuksista sopiminen ja asiakkaan tunnistaminen	1
1.1.1 Pankkitunnukset henkilöasiakaskäyttöön	1
1.1.2 Pankkitunnukset yritys-/yhteisöasiakaskäyttöön	2
1.2 Varmennepalvelun käytöstä sopiminen	2
1.3 Varmennepalvelun yleiskuvaus	2
1.4 Palvelun toiminnallisuudet	3
1.5 Palvelun turvallisuus	3
1.6 Vahvan tunnistamisen määritelmä	4
2 Palvelun toiminnallinen kuvaus	5
3 Varmennepalvelun sanomat ja niiden tiedot	7
3.1 Varmennepyyntö	7
3.2 Varmennepyyntön kenttien selitykset	8
3.3 Varmennepyyntön MAC-tarkisteen (A01Y_MAC) muodostaminen	9
3.4 Varmenne ja yksilöintitieto	9
3.5 Vastausanoman kenttien selitykset	10
3.6 Varmenteen tarkisteen laskenta	11
3.7 Yksilöintitiedon tyyppi	11
3.7.1 Selväkielinen yksilöintitieto	12
3.7.2 Salattu yksilöintitieto	12
3.8 Salatun yksilöintitiedon vertailu ja asiakkaan tunnistus	12
3.9 Pankkikohtaiset painikkeet	12
3.10 Poikkeustilanteet	13
4 Tarkisteavaimen vaihto	13
5 Palvelussa käytettävä merkistö	15
LIITE 1 PANKKIKOHTAISET YHTEYSTIEDOT	17
LIITE 2 VARMENNEPYYNNÖN YKSILÖINTITIEDON TYYPPI (A01YIDTYPE)	19
LIITE 3 VARMENTEEN YKSILÖINTITIETO	20

1 TUPAS-varmennepalvelu

Pankkien TUPAS-Varmennepalvelu (jatkossa ”Varmennepalvelu”) mahdollistaa palvelun käyttöönottan, sähköisiä asiointipalveluita internetissä tarjoavan yrityksen tai yhteisön (jatkossa ”palveluntarjoaja”) tunnistaa asiakkaansa Varmennepalvelun välittämien Tupas-varmenteiden (jatkossa ”varmenteiden”) avulla. Varmennepalvelussa pankki tunnistaa asiakkaansa vahvalla tunnistuksella (katso kohta 1.6). Palvelun välittämiä varmenteita voidaan käyttää myös sähköisen allekirjoituksen muodostamiseen tunnistautuvan asiakkaan ja palveluntarjoajan niin sopiessa.

Varmennepalvelu on pankkien yhteisesti määrittelemä. Kukin pankki tunnistaa asiakkaansa samoilla pankkikohtaisilla pankkitunnisteilla, joita asiakas käyttää pankin omissa palveluissa.

1.1 Pankkitunnuksista sopiminen ja asiakkaan tunnistaminen

Varmennepalvelun käyttäminen tapahtuu pankin asiakkaalleen luomillaan ja antamallaan pankkikohtaisilla tunnisteilla, kuten esimerkiksi käyttäjätunnukset ja kertakäyttöisillä tunnusluvuilla, (jatkossa ”pankkitunnukset”). Pankkitunnukset ovat aina henkilökohtaisia riippumatta siitä, onko ne annettu henkilöasiakas- vai yritys-/yhteisöasiakaskäyttöön.

Pankit voivat käyttää toiminnassaan alihankkijoita ja asiamiehiä noudattaen yhteistyössä luottolaitoslain ja Rahoitustarkastuksen sen nojalla antamien standardien mukaisia toimintamalleja.

1.1.1 Pankkitunnukset henkilöasiakaskäyttöön

Asiakas saa henkilökohtaiset pankkitunnukset käyttöönsä kirjallisen sopimuksen perusteella. Sopimus tehdään aina henkilökohtaisesti sen henkilön kanssa, jonka nimiin pankkitunnukset luodaan. Asiakas ei voi valtuuttaa toista tekemään sopimusta puolestaan.

Pankeilla on lakisäätöinen velvollisuus tunnistaa asiakkaansa. Asiakkaan henkilöllisyys varmistetaan Rahoitustarkastuksen hyväksymällä tavalla pankin tai sen asiamiehen toimesta pankkien hyväksymästä virallisesta tunnistamisasiakirjasta, kuten esim. ajokortti, henkilökortti, passi, kuvallinen kelakortti.

Ensimmäiset tunnuks on noudettava henkilökohtaisesti, jolloin asiakas tunnistetaan luotettavasti. Jatkossa kertakäyttöiset tunnuks voidaan lähettää postitse asiakkaalle. Asiakas ei voi valtuuttaa toista noutamaan pankkitunnuksia puolestaan.

1.1.2 Pankkitunnukset yritys-/yhteisöasiakaskäyttöön

Jos pankkitunnukset tulevat yritys/yhteisökäyttöön, pankkitunnuksista sovi-
taan ja ne noudetaan soveltuvin osin kuten henkilöasiakkaan pankkitunnuk-
set noudattaen Rahoitustarkastuksen hyväksymää tapaa.

1.2 Varmennepalvelun käytöstä sopiminen

Palveluntarjoajan tulee sopia Varmennepalvelun käytöstä niiden pankkien
kanssa, joiden tarjoamaa palvelua palveluntarjoaja tahtoo käyttää. Kunkin
pankin kanssa on tehtävä erillinen sopimus. Pankkikohtaiset yhteystiedot
ovat tämän kuvauksen [liitteenä 1](#).

Varmennepalvelun käyttöönottopäivä sovitaan sopimuksen teon yhteydessä.
Palveluntarjoajan tiedot rekisteröidään kussakin pankissa ja palveluntarjoaja
ilmoittaa kullekin pankille erikseen, kun hänen sopimustietoihinsa tulee
muutoksia.

Pankki toimittaa palveluntarjoajalle sopimuksen teon jälkeen palvelussa käy-
tettävän pankkikohtaisen asiakastunnuksen ja tarkisteavaimen. Tiedot toimi-
tetaan palveluntarjoajalle pankkikohtaisella menettelyllä joko sähköisessä
muodossa tai paperitulosteena.

Testausvaiheessa käytettävät pankkikohtaiset tiedot ovat saatavilla pankkien
palvelukuvauksissa. Palveluntarjoaja voi testata palvelua tuotantoympäris-
tössä jo ennen kuin sopimus on tehty käyttämällä pankkikohtaisia testitun-
nuksia.

1.3 Varmennepalvelun yleiskuvaus

Tunnistautuva asiakas on keskeisessä asemassa palvelun käytössä. Asiakas
ohjaa tietojensa välitystä palveluntarjoajan ja pankkinsa välillä. Pankki ja
palveluntarjoaja eivät ole palvelun aikana suorassa yhteydessä keskenään.

Kun palveluntarjoajalla on tarve tunnistaa asiakas, palveluntarjoaja lähettää
varmennepyyntön asiakkaalle, joka siirtyy pankkinsa Varmennepalveluun
painamalla pankkinsa tunnistuslinkkiä. Palveluntarjoajan varmennepyyntö
välittyy asiakkaalta pankin Varmennepalveluun, joka lähettää asiakkaan tun-
nistamisen jälkeen asiakkaalle vastaussanomaa (jatkossa ”varmenne”). Asia-
kas tarkastaa vastaanottamansa varmenteen tiedot. Jos asiakas hyväksyy tie-
dot, hän palaa takaisin palveluntarjoajan palveluun, jolloin Varmenne välit-
tyy palveluntarjoajalle. Asiakas voi halutessaan peruttaa tunnistustapahtuman
ennen tunnistautumistaan pankin palveluun tai hylätä pankin antaman var-
menteen.

Palveluntarjoaja ja asiakas voivat sopia varmenteen käytöstä osana sähköistä
allekirjoitusta asiakkaan ja palveluntarjoajan välisessä oikeustoimessa. Pank-
ki huolehtii kuitenkin ainoastaan tässä palvelukuvauksessa mainitulla tavalla

asiakkaan tunnistamisesta eikä vastaa asiakkaan ja palveluntarjoajan välisen oikeustoimen sitovuudesta tai sisällöstä.

1.4 Palvelun toiminnallisuudet

Pankin antama varmenne on ainutkertainen, ja se on aikaleimalla sidottu sekä palveluntarjoajan kyseiseen palvelutapahtumaan että asiakkaaseen.

Varmennepalvelussa on eri toiminnallisuuksia ja käyttömahdollisuuksia sen mukaan, millaisen varmenteen välittämisestä palveluntarjoaja on palvelusopimuksessaan pankin kanssa sopinut. Pankin antama Varmenne sisältää aina asiakkaan (henkilön ja/tai yrityksen) 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 varmennepyynnön lähettämistä. Tämä toiminnallisuus soveltuu siten asiakkaan ilmoittamien tietojen oikeellisuuden tarkastamiseen pankista.

Varmennepalvelu soveltuu pääasiassa kuluttajille suunnattuihin palveluihin. Eräissä pankeissa on mahdollista tunnistaa myös pankin yritysasiakkaita Y-tunnuksen avulla. Kaikki pankit eivät tarjoa varmennepalvelua, jossa yritysasiakas tunnistetaan. Tunnistettaessa pankin yritysasiakkaita voidaan pankista välittää varmenteen mukana joko asiakkaan Y-tunnus ja yrityksen nimi tai asiakkaan Y-tunnus, yrityksen nimi, henkilön nimi sekä henkilötunnus.

1.5 Palvelun turvallisuus

Varmennepalvelun 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. Varmennepyynnön ja varmenteen tiedot on suojattu tiedon eheyden turvaavalla tarkisteella, joten varmenteen 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.

Palveluntarjoajan on huomautettava asiointipalvelussaan, että palvelussa käytetään Varmennepalvelua, jossa käytetään asiakkaan joko henkilöasiakastai yritysasiakaskäyttöön tarkoitettuja pankkitunnuksia. Palveluntarjoajan tulee muokata asiointipalvelussaan olevaa huomautustekstiä sen mukaisesti haluaako palveluntarjoaja tunnistaa henkilöasiakkaita ja/tai yritysasiakkaita.

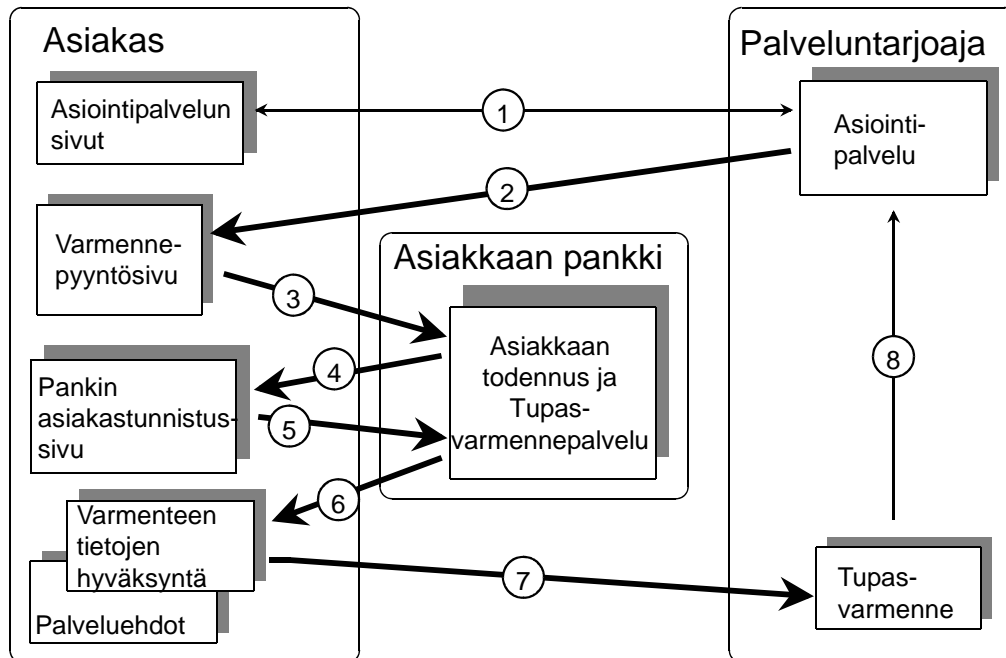
1.6 Vahvan tunnistamisen määritelmä

Henkilön vahva tunnistaminen koostuu jostain, mitä käyttäjä:

- 1) tietää (esim. käyttäjätunnus),
- 2) omistaa (esim. salasanalista),
- 3) on (esim. sormenjälki).

Kahden näistä vaatimuksista on toteuduttava samanaikaisesti, jotta tunnistustapahtuma täyttää vahvan tunnistamisen määritelmän. Vahvan tunnistamisen lisäksi tapahtuman täytyy perustua riittävän turvalliseen menettelyyn. Turvallisen tunnistustapahtuman kriteerit täyttävät vaihtuvat tunnusluvut. Näin ollen esimerkiksi kiinteän salasanan ja käyttäjätunnuksen yhdistelmä ei yksinään täytä Varmennepalvelun määrittämien vahvan tunnistamisen kriteereitä.

2 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 Varmennepalveluun liittyvien tietojen syöttöön. Vaiheiden 2–7 aikana tiedonsiirtoyhteys on aina SSL-suojattu.
2. Palveluntarjoaja lähettää asiakkaalle Varmennepyyntön, 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 Varmennepyyntösivulla ovat Varmennepalveluun johtavat toimintopainikkeet ja peruutuspainike.
3. Asiakas painaa toimintopainiketta, joka johtaa hänen pankkinsa Varmennepalveluun. Pankkiin välittyvä Varmennepyyntö sisältää Varmennepalvelun tarvitsemat tiedot palveluntarjoajasta ja tapahtumasta. Pankki tarkastaa pyynnön eheyden ja tietojen oikeellisuuden.
4. Pankki lähettää asiakkaalle tunnistuspyynnön, jos palveluntarjoajan Varmennepyyntö on virheetön. Pankki antaa asiakkaalle virheilmoituksen, jos pankki havaitsee varmennepyyntönsä virheitä, jolloin asiakas palaa tapahtuman peruutuspainikkeella takaisin palveluntarjoajan palveluun.

5. Asiakas tunnistautuu pankkinsa varmennepalvelussa. Pankki palauttaa asiakkaalle virheilmoituksen, jos tunnistus epäonnistuu, jolloin asiakas palaa peruutuspainikkeella takaisin palveluntarjoajan palveluun.
6. Onnistuneen tunnistuksen jälkeen pankki muodostaa vastaussanoman, ”Varmenteen”. Pankin Varmennepalvelu asettaa asiakkaalle hyväksymis- ja peruutuspainikkeet.
7. Asiakas tarkastaa varmenteen tiedot ja hyväksyy varmenteen välittämisen palveluntarjoajalle. Asiakas voi peruutuspainikkeella keskeyttää tunnistustapahtuman ja palata takaisin palveluntarjoajan palveluun.
8. Palveluntarjoaja varmistaa vastaanottamansa Varmenteen eheyden ja aintukertaisuuden. Palveluntarjoaja liittää Varmenteen asiakkaan palvelutapah-tumaan ja säilyttää sitä yhtä kauan kuin muita palvelutietoja säilytetään. Asiakkaan yksilöintitietoja ei saa rekisteröidä tai käyttää muuhun tarkoitukseen.

3 Varmennepalvelun sanomat ja niiden tiedot

3.1 Varmennepyyntö

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

VARMENNEPYyntÖ			
Kenttä	Tiedon nimi	Pituus	Huomautus
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	kts. Liite 2
7. Paluuosoite	A01Y_RETLINK	199	OK paluuosoite varmenteelle
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
12. Tarkiste	A01Y_MAC	32–40	Pyynnön turvatarkiste

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

```
<FORM METHOD="POST" ACTION="pankin Varmennepalvelun 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>
```

3.2 Varmennepyyntöjen kenttien selitykset

Kenttä 1 Sanoman tyyppi, joka on Varmennepalvelussa vakio "701".

Kenttä 2 Varmennepyyntö-sanoman versionumero, joka on pankkikohtainen.

Kenttä 3 Kentässä on palveluntarjoajan pankkikohtainen asiakastunnus. Pankki tunnistaa palveluntarjoajan asiakastunnuksen perusteella ja liittää rekisterissään olevan palveluntarjoajan nimen varmenteeseen.

Kenttä 4 Palvelun kielikoodi kertoo palveluntarjoajan asiointisivun kielen ja pankin Varmennepalvelu avautuu tällä kielellä.

Kenttä 5 Palveluntarjoajan varmennepyyntölle antama yksilöivä tunnus. Tunnusena voi olla viite, asiakasnumero tai yhdistelmä päivämäärästä, kelloajasta ja juoksevasta tunnuksesta sekä viitteestä.

Kenttä 6 Yksilöintitiedon tyyppi kertoo, minkä yksilöintitiedon palveluntarjoaja tunnistettavasta asiakkaastaan haluaa. Yksilöintitiedon tyyppiin tulee vastata palvelusopimuksessa sovittua toiminnallisuutta.

Kenttä 7 Palveluntarjoajan asiointisivun osoite, joka on OK-tapauksessa jatkokohta. Paluuosoitteen 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 varmenteen välittämisen.

Esimerkki: VALUE="https://tuote.kauppa.fi/tilaus/keskeytykset.htm"

Kenttä 9 Palveluntarjoajan palvelun jatkokohta, jos tunnistuksessa on havaittu tekninen virhe. Paluuosoite voi olla sama kuin kentässä 8.

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.

Kenttä 12 MAC-tarkiste, joka on laskettu Varmennepyyntöjen suojattavista tiedoista ja palveluntarjoajan tarkiste-avaimesta tietokentässä 11 määritellyillä algoritmeilla. Tarkisteen avulla sanoman vastaanottaja voi varmistaa Varmennepyyntöjen eheyden ja lähettäjän.

3.3 Varmennepyyntöön MAC-tarkisteen (A01Y_MAC) muodostaminen

Palveluntarjoaja muodostaa kunkin pankin painiketta varten oman pankki-kohtaisen Varmennepyyntö, 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 Tarkistekenttään.

3.4 Vastauksanoma eli varmenne ja sen yksilöintitiedot

VARMENNE				
Kenttä	Tiedon nimi	Pituus	Pakollisuus¹⁾	Huomautus
1. Versio	B02K_VERS	4	P	Esim. "0002"
2. Varmenteen yksilöinti	B02K_TIMESTMP	23	P	NNNvvvvkkpphhmss xxxxxx
3. Varmenteen numero	B02K_IDNBR	10	P	Pankin varmenteelle antama numero
4. Pyyntöön yksilöinti	B02K_STAMP	20	P	Kyselyn tietokenttä 7 (A01Y_STAMP)
5. Asiakas	B02K_CUSTNAME	-40	P	Pankin tietokannassa oleva tunnistetun henki- lön tai yrityksen nimi
6. Avainversio	B02K_KEYVERS	4	P	Avaimen sukupolvi
7. Algoritmi	B02K_ALG	2	P	01 = MD5 02 = SHA-1

8. Yksilöintitieto	B02K_CUSTID	-40	P	Kts- Liite 3
9. Yksilöintitiedon tyyppi	B02K_CUSTTYPE	2	P	Kts. Liite 3
10. Käyttäjän tunnus	B02K_USERID	-40	V	Yrityskäyttäjän henkilötunnus tai salattu tunnus Kts. Liite 3
11. Käyttäjän nimi	B02K_USERNAME	-40	V	Yrityskäyttäjän nimi Kts Liite 3.
12. Tarkiste	B02K_MAC	32-40	P	Vastauksen turvatarkiste

¹⁾ Tiedon pakollisuus:
P = pakollinen,
V = vain pyydettyessä

Asiakkaan pankki lisää varmenteen 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_USERID&B02K_USERNAME&B02K_MAC

Tiedot *B02K_USERID* ja *B02K_USERNAME* ovat optionaalisia ja ne ovat mukana vain tunnisteiden tyyppien arvoilla "08" ja "09".

3.5 Varmenteen kenttien selitykset:

Kenttä 1 Varmenteen versionumero, joka on pankkikohtainen.

Kenttä 2 Pankin järjestelmän muodostama aikaleima, jossa NNN on pankin numero:

Handelsbanken	= 310
Nordea Pankki Suomi	= 200
Osuuspankkiryhmä	= 500
Sampo Pankki	= 800
Säästöpankit ja paikallisosuuspankit	= 400
Tapiola Pankki	= 360
Ålandsbanken	= 600

Kenttä 3 Pankin tietojärjestelmän varmenteelle antama tieto, joka yksilöi sen pankin järjestelmässä.

Kenttä 4 Varmennepyyntöä yksilöintitieto, joka on poimittu kyseisen Varmennepyyntöä 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 Varmennepyyntöä A01Y_IDTYPE-kentän sisällöstä. Kentän sisältö voi siis vaihtoehtoisesti olla joko salattu tai selväkielinen yksilöintitieto.

Kenttä 9 Yksilöintitiedon tyyppi.

Kenttä 10 Varmenteen tarkiste.

3.6 Varmenteen 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 Varmenteen MAC-tarkisteen palveluntarjoajakohtaisella avaimella. Tarkisteen avulla palveluntarjoaja voi varmistua, että Varmenne on muodostettu asiakkaan pankissa ja sen sisältö on muuttumaton.

Varmenteen tunnisteen tyyppin arvoilla ”00”-”07” tarkiste lasketaan vastausanoman tietokentistä 1–9. Tarkisteen laskennassa tiedot ja tarkisteavain erotetaan toisistaan ”&”-merkillä, joka lisätään myös tarkisteavaimen loppuun. Tarkisteen laskennassa käytetään palveluntuottajakohtaista avainta. Turva-tarkisteen 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&
```

Varmenteen tunnisteen tyyppin arvoilla ”08” ja ”09” tarkiste lasketaan vastausanoman 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_USERID&B02K_USERNAME&tarkisteavain&
```

3.7 Yksilöintitiedon tyyppi

Varmenteen tarkisteen laskentaa vaikuttaa välitettävän yksilöintitiedon tyyppi, joka määritellään Varmennepyyntöä A01Y_IDTYPE-kentässä.

3.7.1 Selväkielinen yksilöintitieto

Varmennepyyynnön A01Y_IDTYPE-kentän arvot ovat ”02” tai ”03”, eli selväkielinen perustunnus tai selväkielinen ty pistetty perustunnus.

Yksilöintitieto on selväkielinen merkkijono, esimerkiksi henkilötunnus tai sen loppuosa pyyntösanoman kentän A01Y_IDTYPE mukaisesti. Yksilöintitieto sijoitetaan sellaisenaan vastaussanoman tiedoksi B02K_CUSTID.

3.7.2 Salattu yksilöintitieto

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

Pankki käyttää yksilöintitiedon salaamisessa samaa tiivistealgoritmia kuin sanomien tarkistelaskennassa. Yksilöintitiedon yksilöllisyys varmistetaan käyttämällä lisätietoina varmenteen tietokentissä 2–4 olevia tietoja ja varmennepyyynnön tietokentän 8 (A01Y_IDTYPE) mukaista 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 varmenteen tiedoksi B02K_CUSTID.

3.8 Salatun yksilöintitiedon vertailu ja asiakkaan tunnistus

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

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

3.9 Pankkikohtaiset painikkeet

Pankkikohtaisten painikkeiden kuvatiedostot on noudettavissa ko. pankin www-sivuilta kunkin pankin erikseen ilmoittamasta osoitteesta. Painikkeiden kokoja tai värejä ei saa muuttaa. Painikkeen kuvaa ei saa käyttää muuhun tarkoitukseen kuin palveluntarjoajan ja pankin välisessä sopimuksessa on sovit tu.

3.10 Poikkeustilanteet

Palveluntarjoajan on varauduttava poikkeustilanteisiin, joita voivat olla:

1. Asiakas keskeyttää tunnistustapahtuman

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

2. Asiakkaan todennus epäonnistuu

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

3. Pankki havaitsee virheen varmennepyynnössä

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

4. Palveluntarjoaja havaitsee virheen varmenteessa.

Palveluntarjoaja havaitsee varmenteen tarkastuksen yhteydessä virheen, joka voi johtua varmenteen 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 varmenteen siirtyessään selaimensa ikkunoissa eteen-/taakse-näppäimillä ruudusta toiseen.

4 Tarkisteavaimen vaihto

Tarkisteiden laskennassa käytettyä MAC-avainta voidaan vaihtaa pankin tai palveluntarjoajan toivomuksesta. Avaimen vaihdossa noudatetaan pankki-

kohtaisia 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 voimaanastumispäivästä. 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 varmenteiden tarkiste on laskettu vanhalla avaimella ja osa uudella.

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

5 Palvelussa käytettävä merkistö

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

æ	%00	0	%30	ˆ	%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	ÿ	%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	%oo	%89	ı	%b9	é	%e9		
*	%2a	Z	%5a	Š	%8a	o	%ba	ê	%ea		
+	%2b	[%5b	<	%8b	»	%bb	ë	%eb		
,	%2c	\	%5c	Œ	%8c	¼	%bc	ì	%ec		
-	%2d]	%5d	ž	%8d	½	%bd	í	%ed		
.	%2e	^	%5e	Ž	%8e	¾	%be	î	%ee		
/	%2f	_	%5f		%8f	ı	%bf	ï	%ef		

LIITE 1

PANKKIKOHTAISET YHTEYSTIEDOT

HANDELSBANKEN

Sopimusasiat:	Oma konttori
Tunnukset ja avaimet:	Noudetaan pankista
Asiakasneuvonta ja tekniset ongelmat:	HelpDesk 010 444 2545 pankkipäivinä klo 8-17
Sähköposti:	finhelp@handelsbanken.fi

NORDEA

Sopimusasiat:	Oma konttori
Tunnukset ja avaimet:	Toimitetaan postitse sopimuksessa mainitulle yhteyshenkilölle.
Asiakasneuvonta ja tekniset ongelmat:	Yritysten Solo-neuvonta <ul style="list-style-type: none">• Suomeksi: 0200 67210 (0,11 €min + pvm/mpm) Pankkipäivinä klo 8 – 18• Ruotsiksi: 0200 67220 (0,11 €min + pvm/mpm) Pankkipäivinä klo 9 - 16.30• Englanniksi: 0200 67230 (0,11 €min + pvm/mpm) Pankkipäivinä klo 9 – 18
Sähköposti:	Solo.tori@nordea.fi

OSUUSPANKIT

Sopimusasiat:	Oma osuuspankki
Tunnukset ja avaimet:	Noudetaan pankin konttorista
Asiakasneuvonta:	Osuuspankin puhelinpalvelu: <ul style="list-style-type: none">• Suomeksi: 0100 0500• Ruotsiksi: 0100 9051
Sähköposti:	verkkopainikkeet@op.fi

SAMPO PANKKI

Sopimusasiat:	Oma konttori tai puh. 0106 6060 (pvm/mpm), ma-pe klo 8–17
Tunnukset ja avaimet:	Toimitetaan levykkeellä postitse sine- töidyssä paketissa
Asiakasneuvonta ja tekniset ongelmat:	<ul style="list-style-type: none">• Henkilöasiakkaat 0200 2589 (pvm/mpm),

Sähköposti ma-pe klo 9–18

- Yritysassiakkaat 0600 122 12 (1,17 €/min +pvm/mpm),
ma-pe klo 8–17
asiakastuki.ml@sampo.fi tai varmennepalvelu@sampo.fi

SÄÄSTÖPANKIT JA PAIKALLISOSUUSPANKIT

Sopimusasiat: Oma pankki
Tunnukset ja avaimet: Noudetaan pankista
Asiakasneuvonta ja tekniset ongelmat:
Sähköposti: info@samlink.fi

- Puh. 0100 4052 (1,17 e/min + pvm)

TAPIOLA PANKKI

Sopimusasiat Tapiola sähköiset palvelut
Tunnukset ja avaimet Toimitetaan sopimuksessa mainitulle palveluntarjoajalle yhteyshenkilölle pankin yhteyshenkilön toimesta.
Asiakasneuvonta ja tekniset ongelmat
Sähköposti: tunnistuspalvelu@tapiola.fi

- Henkilöasiakkaat 0203 45370 (ma-pe)

ÅLANDSBANKEN

Sopimusasiat: Oma konttori
Asiakastunnus: Toimitetaan sopimuksen yhteydessä pankin konttorissa. Tarkisteavain postitetaan sopimuksessa mainitulle yhteyshenkilölle.
Asiakasneuvonta ja tekniset ongelmat: Contact Center
-Asiakaspalvelu
Sähköposti: contactcenter@alandsbanken.fi

- Suomeksi: 0204 292920
- Ruotsiksi: 0204 292910
- Pankkipäivinä ma-to 8.40–16.30, pe 9.30–16.30

LIITE 2

VARMENNEPYYNNÖN YKSILÖINTITIEDON TYYPPI (A01Y_IDTYPE)

Varmennepyyntöä 6 määrittelee pyydetyn yksilöintitiedon tyyppi. Tyyppi on koodattu kahdella merkillä XY seuraavasti.

Kymppit (X) ilmoittavat pyydetyn yksilöintitiedon sisällön:

- 0Y = Perustunnus
- 1Y = Henkilötunnus
- 2Y = Y-tunnus
- 3Y = Henkilötunnus tai y-tunnus
- 4Y = Henkilötunnus ja y-tunnus
- 5Y = Henkilötunnus ja y-tunnus tai pelkkä henkilö
tunnus

Ykköset (Y) ilmoittavat pyydetyn tunnisteiden muodon:

X1 = Salattu tunnus

Asiakkaan yksilöintitiedon perusteella laskettu heksadesimaalimuotoinen MAC-tarkisteluku.

X2 = Selväkielinen tunnus

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

X3 = Typistetty tunnus

Tunnus voi sisältää henkilötunnuksen tarkenneosan ilman vuosisataa ilmoitettavaa välimerkkiä tai kokonaisen Y-tunnuksen.

Huom: koodi 23 ei ole käytössä.

LIITE 3

VARMENTEEN YKSILÖINTITIETO

Vastaussanomien tunnisteen tyyppiin (kenttä 9) tieto on koodattu kahdella merkillä XY siten kymmit (X) ilmoittavat löytyvätkö asiakkaasta pyydyt tiedot pankin asiakastietokannasta.

0Y = Pyydyt tiedot on löydetty.

Sanoma palautetaan kyselyanomien paluuosoite-kentän osoitteeseen.

00 = tunnus ei ole tiedossa

Arvoa "00" käytetään, jos mitään tunnistetta 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 asiakkaan nimi ja kentässä 8 on selväkielinen sähköinen asiointitunnus.

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

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 = Asiakkaasta ei löytynyt pyydettyä tietoa.

11 = Asiakkaasta ei löytynyt henkilötunnusta.

12 = Asiakkaasta ei löytynyt Y-tunnusta.

Esimerkki:

Palveluntarjoaja haluaa tietää asiakkaan henkilötunnuksen, mutta asiakas käyttää tunnuksia, joista löytyy vain Y-tunnus. Pankki lähettää Yksilöintitiedon tyyppi -kentän (B02K_CUSTTYPE) tiedot hylätty osoite -kentän osoitteeseen. Kentässä 9 Yksilöintitiedon tyyppi palautetaan arvo 11.

Bulevardi 28
00120 Helsinki
Puhelin 020 7934 200
Faksi 020 7934 202
etunimi.sukunimi@fkl.fi
<http://www.fkl.fi>



FK|Finanssialan Keskusliitto