



VERKKOTUNNISTUSPALVELU
Palvelukuvaus ja ohje yrityksille

SISÄLLYSLUETTELO

1 Yleistä.....	3
2 Tunnistuspalvelun kuvaus	3
2.1 Yleiskuvaus.....	3
2.2 Palvelun toiminnallinen kuvaus.....	4
2.3 Palvelun turvallisuus	4
3 Palvelun toiminnallinen kuvaus	5
4 Verkkotunnistuspalvelun käyttöönotto	6
4.1 Käyttöönoton edellytykset.....	6
4.2 Sopimukset	6
5 Tapiolan verkkotunnistuspalvelun tunnus.....	6
6 Verkkotunnistuspalvelun sanomat ja niiden tiedot.....	7
6.1 Tunnistepyyntö.....	7
6.2 Tunnistepyyntöön kenttien selitykset	8
6.3 Vastausanoma ja tunniste.....	10
6.4 Vastausanoman kenttien selitykset.....	10
6.5 Vastausanoman tarkisteen laskenta	11
6.6 Tunnisteen tyyppi.....	12
6.6.1 Selväkielinen asiakastunnus	12
6.6.2 Salattu tarkiste.....	12
6.7 Poikkeustilanteet.....	12
7 Testaus.....	13
8 Neuvonta ja tekninen tuki	14
9 Palvelussa käytettävä merkistö	14

1 Yleistä

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

Tapiolan verkkotunnistuspalvelun avulla palveluntarjoaja voi tunnistaa luotettavasti asiakkaitaan Tapiola Pankin tunnistamismenetelmiä hyväksikäyttäen. Tunnistuspalvelussa Tapiola Pankki tunnistaa asiakkaan palveluntarjoajan puolesta. Palvelun välittämiä tunnistamistietoja voidaan käyttää myös osana sähköisen allekirjoituksen muodostamista tunnistautuvan asiakkaan ja palveluntarjoajan niin sopiessa. Palvelu on pankkien yhteisesti standardoima ja tarkoitettu sähköisten asiointi- tai maksamispalvelujen tarjoajille.

Tapiolan antama tunniste on ainutkertainen ja se on sidottu sekä palveluntarjoajan kyseiseen palvelutapahtumaan että asiakkaaseen. Tapiola tunnistaa asiakkaansa samoilla tunnistamismenetelmillä, joita asiakas käyttää pankin omissa palveluissa.

Finanssialan Keskusliiton antaman ohjeistuksen mukaisesti Tapiola Pankki tulee vuoden 2011 aikana siirtymään verkkotunnistuspalvelun viestiliikenteen tarkistelaskennassa nykyisestä MD5 – salausalgoritmistä SHA-256 -salausalgoritmin käyttöön. SHA-256 -salausalgoritmi on Tapiola Pankin verkkotunnistuspalvelua käyttävien palveluntarjoajien käytettävissä maaliskuun 2011 alusta lukien. Finanssialan keskusliitto edellyttää, että Suomessa toimivat pankit ovat siirtyneet verkkotunnistuksessa SHA-256 –salausalgoritmin käyttöön kaikilta osin vuoden 2011 loppuun mennessä. SHA-256 -salausalgoritmin käytön viestiliikenteen tarkistelaskennassa mahdollistavat muutokset on huomioitu tässä palvelukuvauksessa.

2 Tunnistuspalvelun kuvaus

2.1 Yleiskuvaus

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

Kun palveluntarjoajalla on tarve tunnistaa asiakkaansa, palveluntarjoaja lähettää tunnistepepyynnön asiakkaalle, joka siirtyy Tapiolan verkkotunnistuspalveluun painamalla Tapiolan verkkopalvelun tunnistuslinkkiä. Palveluntarjoajan tunnistepepyyntö välittyy asiakkaalta Tapiolan verkkotunnistuspalveluun, joka lähettää tunnistamisen jälkeen asiakkaalle vastaussanoman. Asiakas tarkastaa vastaanottamansa vastaussanoman tiedot, joiden hyväksymisen jälkeen hän palaa takaisin palveluntarjoajan palveluun, jolloin Tapiolan tunnistussanoman tiedot välittyvät palveluntarjoajalle. Asiakas voi halutessaan peruuttaa tai hylätä tunnistustapahtuman joko ennen tunnistautumista tai vastaussanoman tarkastamisen jälkeen.

Palveluntarjoaja ja asiakas voivat sopia verkkotunnistuspalvelussa välitettävän vastaussanoman käytöstä osana sähköistä allekirjoitusta asiakkaan ja palveluntarjoajan välisessä oikeustoimessa. Tapiola huolehtii kuitenkin ainoastaan tässä palvelukuvauksessa mainitulla tavalla asiakkaan tunnistamisesta eikä vastaa asiakkaan ja palveluntarjoajan välisen oikeustoimen sitovuudesta tai sisälöstä.

Tapiola Pankin verkkotunnistuspalvelun www-osoite on <https://pankki.tapiola.fi/service/identify>.

Verkkotunnistuspalvelu on käytettävissä 24 h/vrk pois lukien huollosta, päivityksestä tms. syystä johtuvat katkoajat.

2.2 Palvelun toiminnallinen kuvaus

Tapiolan antama vastaussanomien tunnistustieto sisältää aina asiakkaan nimen. Tämän lisäksi välitettävä tunnistustieto voi olla joko selväkielinen tai salattu. Tunnistustiedon ollessa selväkielinen, pankki voi välittää asiakkaan henkilötunnuksen, henkilötunnuksen tarkisteosan tai Y-tunnuksen sen mukaan, mistä on sovittu palvelusopimuksessa. Selväkielisen henkilötunnuksen Tapiola välittää vain palveluntarjoajille, joilla on oikeus rekisteröidä se.

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

Tunnistuspalvelu soveltuu pääasiassa kuluttajille suunnattuihin palveluihin.

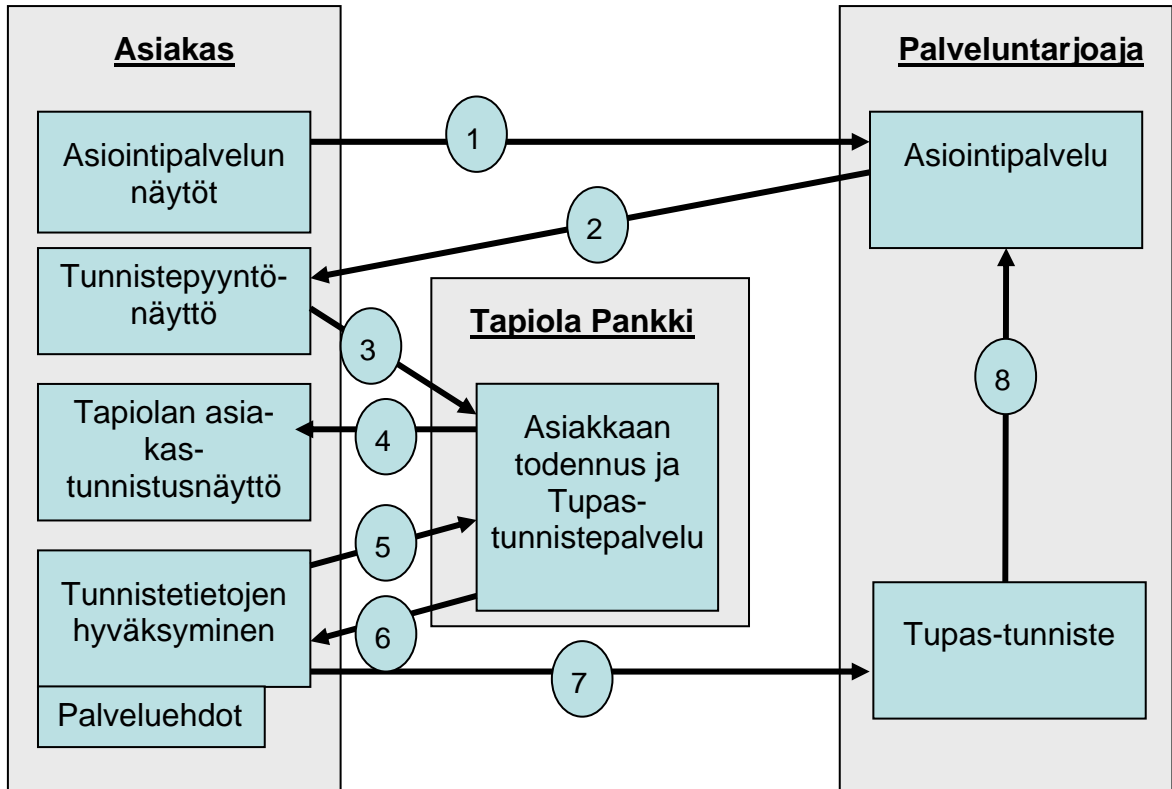
2.3 Palvelun turvallisuus

Verkkotunnistuspalvelun osapuolten välisessä tietoliikenteessä käytetään SSL-salausprotokollaa, 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 vastaussanomien tiedot on suojattu tiedon eheyden turvaavalla tarkisteella, joten tunnistetietojen välitystä ohjaavalla asiakkaalla ei ole mahdollisuutta muuttaa tietoja palveluntarjoajan ja pankin sitä havaitsematta. Tarkisteen lasketaan käytettävä tarkisteavain vaihdetaan määräajoin. Pankki vastaa tarkisteavaimen määräajoin tapahtuvasta vaihdoista ja ottaa palveluntarjoajaan yhteyttä avaimen vaihdon tullessa ajankohtaiseksi.

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

3 Palvelun toiminnallinen kuvaus



1. Tunnistautuva asiakas on yhteydessä palveluntarjoajan palveluun. Asiakkaan ja palveluntarjoajan välisen tietoliikenteen tulee olla SSL-suojattua, kun asiakas siirtyy tunnistepalveluun liittymisen tietojen syöttöön. Vaiheiden 2 – 7 aikana tiedonsiirtoyhteys on aina SSL-suojattu.
2. Palveluntarjoaja lähettää asiakkaalle tunnistepyyntön, joka sisältää tapahtumaan liittyvät yksilöintitiedot. Asiakas tarkastaa vastaanottamansa tunnistepyyntön tiedot, mutta hän ei voi muuttaa niitä. Asiakas voi halutessaan keskeyttää tunnistuksen ja palata takaisin asiointipalveluun. Palveluntarjoajan tunnistepyyntö asettaa käyttäjän näytölle Tapiolan toimintopainikkeen sekä tapahtuman peruutuspainikkeen.
3. Asiakas painaa toimintopainiketta, joka johtaa Tapiolan verkkotunnistuspalveluun. Tapiolaan välittyvä tunnistepyyntö sisältää tunnistuspalvelun tarvitsemat tiedot palveluntarjoajasta ja tapahtumasta. Tapiola tarkastaa tunnistepyyntön eheyden ja tietojen oikeellisuuden.
4. Tapiola lähettää asiakkaalle tunnistuspyynnön, jos palveluntarjoajan tunnistepyyntö on virheellinen. Tapiola antaa asiakkaalle virheilmoituksen, jos Tapiola havaitsee tunnistepyyntöä virheitä, jolloin asiakas palaa tapahtuman peruutuspainikkeella takaisin palveluntarjoajan palveluun.
5. Asiakas tunnistautuu Tapiolan verkkotunnistuspalvelussa. Tapiola palauttaa asiakkaalle virheilmoituksen jos tunnistus epäonnistuu, jolloin asiakas palaa peruutuspainikkeella takaisin palveluntarjoajan palveluun.

6. Onnistuneen tunnituksen jälkeen Tapiola muodostaa vastaussanoman. Tapiolan verkkotunnistuspalvelu asettaa käyttäjälle hyväksymis- ja peruutuspainikkeet, ja lähettää vastaussanoman tämän selaimelle.
7. Asiakas tarkastaa tunnisteiden tiedot ja hyväksyy tunnisteiden välittämisen palveluntarjoajalle. Asiakas voi peruutuspainikkeella hylätä tunnisteiden ja palata takaisin palveluntarjoajan palveluun.
8. Palveluntarjoaja varmistaa vastaanottamansa vastaussanoman eheyden ja ainutkertaisuuden. Palveluntarjoaja liittää tunnisteiden asiakkaan palvelutapahtumaan ja säilyttää sitä yhtä kauan kuin muita palvelutietoja säilytetään. Tunnisteita ei saa rekisteröidä tai käyttää muuhun tarkoitukseen.

4 Verkkotunnistuspalvelun käyttöönotto

4.1 Käyttöönoton edellytykset

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

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

4.2 Sopimukset

Palveluntarjoaja tekee kirjallisen sopimuksen verkkotunnistuspalvelun käytöstä Tapiolan kanssa. Palveluntarjoajan tiedot rekisteröidään pankissa ja sopimuksessa mainitulle yhteyshenkilölle lähetetään MAC-tarkisteavain paperitulosteena. Asiakkaille, jotka ovat siirtyneet uuden SHA-256-salausalgoritmin käyttöön lähetetään tarkistelaskentaan käytettävä tarkisteavain heksaadesimaalimuodossa esitettynä kahdessa osassa erillisinä paperitulosteina (PART 1 ja PART 2).

Kustakin eri palvelusta tulee tehdä palvelusopimus. Tapiola tekee sopimuksen henkilötunnuksen välittämisestä vain silloin kun palveluntarjoajalla on oikeus rekisteröidä se.

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

Mikäli palvelun käyttöönotto viivästyy, tulee asiakkaan ilmoittaa viivästyksestä Tapiola Pankille.

5 Tapiolan verkkotunnistuspalvelun tunnus

Palveluntarjoajan Internet-palvelussa verkkotunnistuspalvelun käyttö on ilmaistava Tapiolan verkkopalvelun logolla ja sen on oltava selvästi näkyvillä. Toimintopainikkeena käytetään kyseistä logoa.

Tapiolan verkkotunnistuspalvelupainikkeen kuvatiedosto on noudettavissa Tapiolan www-sivuilta osoitteesta <http://www.tapiola.fi/painike>.

Painikkeen kokoa tai värejä ei saa muuttaa tai muuten muotoilla. Painikkeen kuvaa ei saa käyttää muuhun tarkoitukseen kuin mitä palveluntarjoajan ja Tapiolan välisessä sopimuksessa on sovittu.

Palveluntarjoajan verkkopalvelussa saa käyttää Tapiola Pankista ainoastaan seuraavia nimiä: Tapiola, Tapiola Pankki tai Tapiola Pankki Oy.

Sopimuksen päätyttyä palveluntarjoajan on viipymättä poistettava sivuiltaan Tapiolan verkkotunnistuspalvelun logo / nimi.

6 Verkkotunnistuspalvelun sanomat ja niiden tiedot

6.1 Tunnistepyyntö

Tunnistepyyntöön tiedot ovat Tapiolan verkkopalvelukuvakkeen takana FORM -tietoryhmässä piilomuuttujina.

Kenttä	Tiedon nimi	Pituus	P/V	Arvo
1. Sanomatyyppi	A01Y_ACTION_ID	3	P	' 701'
2. Versio	A01Y_VERS	4	P	' 0002'
3. Palveluntarjoajan tunnus	A01Y_RCVID	8-15	P	Palveluntarjoajan tunnus
4. Palvelun kieli	A01Y_LANGCODE	2	P	FI = suomi SV = ruotsi
5. Kyselyn yksilöinti	A01Y_STAMP	20	P	vvvkkpphhmssxxxxx
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	' 0001'
11. Algoritmi	A01Y_ALG	2	P	01 = MD5 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://pankki.tapiola.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 Tunnistepyyntö-kenttien selitykset

Kenttä 1

Sanoman tyyppi, joka on Tupas-palvelussa vakio 701.

Kenttä 2

Tunnistepyyntö-sanoman versionumero on 0002.

Kenttä 3

Tapiola Pankin palveluntarjoajalle antama asiakastunnus. Tapiola tunnistaa palveluntarjoajan asiakastunnuksen perusteella ja liittää rekisterissään olevan palveluntarjoajan nimen vastaussanomaa. Palveluntarjoajan tunnus löytyy palvelusopimuksesta ja turvatarkistekirjeestä.

Kenttä 4

Palvelun kielikoodi kertoo palveluntarjoajan asiointisivun kielen ja Tapiolan verkkotunnistuspalvelu avautuu tällä kielellä.

Kenttä 5

Palveluntarjoajan tunnistepyyntöä 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 tyyppin tulee vastata palvelusopimuksessa sovittua toiminnallisuutta.

- 01 = Salattu perustunnus. Asiakkaan tunnistetiedon perusteella laskettu heksadesimaalimuotoinen MAC-tarkisteluku. Tunnus voi olla asiakkaan täydellinen henkilötunnus tai Y-tunnus
- 02 = Selväkielinen perustunnus. Tunnus voi olla asiakkaan täydellinen henkilötunnus tai kokonainen Y-tunnus
- 03 = Selväkielinen typistetty tunnus. Tunnus voi olla henkilötunnuksen tarkenneosa ilman vuosisataa ilmoittavaa välimerkkiä tai kokonainen Y-tunnus.

Kenttä 7

Palveluntarjoajan palvelusivun 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 tunnisteen välittämisen.

- Esimerkki: VALUE="https://tuote.kauppa.fi/tilaus/keskeytys.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 on 0001.

Kenttä 11

MAC-tarkisteen laskennassa käytettävän algoritmin tyyppikoodi. Tapiolan verkkotunnistuspalvelussa ovat käytössä **01 = MD5-algoritmi**, joka tuottaa 32-merkkisen MAC-tarkisteen sekä **03 = SHA-256 -algoritmi**, joka tuottaa 64-merkkisen MAC-tarkisteen.

Mahdollisuus MD5-algoritmin käyttöön tulee Finanssialan Keskusliiton ohjeistuksen mukaisesti **päättymään vuoden 2011 loppuun** mennessä.

Kenttä 12

MAC -tarkiste, joka on laskettu tunnistepeynnön suojattavista tiedoista ja palveluntarjoajan tarkisteavaimesta tietokentässä 11 määritellyillä algoritmeilla. Tarkisteen avulla sanoman vastaanottaja voi tarkistaa tunnistepeynnön eheyden ja lähettäjän.

Tunnistepeynnön MAC-tarkisteen (A01Y_MAC) muodostaminen:

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

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. "α" -merkki näyttää tässä dokumentissa olevan rivinvaihdon.

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

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

Palveluntarjoajan tekemässä verkkotunnistussopimuksessa nimetty yhteyshenkilö saa tarkisteavaimen pankista suljetussa kuoressa (MD5-salausalgoritmi). Mikäli asiakasyritys on siirtynyt SHA-256-salausalgoritmin käyttöön, toimittaa pankki tarkisteavaimen kahdessa osassa kahtena erillisenä suljettuna kuorena.

6.3 Vastaussanoma ja tunniste

Kenttä	Tiedon nimi	Pituus	P/V	Arvo
1. Versio	B02K_VERS	4	P	' 0002'
2. Tunnisteen yksilöinti	B02K_TIMESTAMP	23	P	360vvvkkpphmmssxxxxx
3. Tunnisteen numero	B02K_IDNBR	10	P	Tapiolan 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	' 0001'
7. Algoritmi	B02K_ALG	2	P	01 = MD5 03 = SHA-256
8. Tunniste	B02K_CUSTID	-64	P	Selväkielinen asiakastunnus tai salattu yksilöintitieto
9. Tunnisteen tyyppi	B02K_CUSTTYPE	2	P	01 = selväkielinen henkilötunnus 02 = selväkielinen henkilötunnuksen tarkenne 03 = selväkielinen Y-tunnus 05 = salattu henkilötunnus 06 = salattu Y-tunnus
10. Tarkiste	B02K_MAC	32-64	P	Vastauksen turvatarkiste

P / V = Tieto on pakollinen / valinnainen

Tapiola lisää vastaussanomien tiedot OK-paluu-linkkiin ns. query-string muodossa.

```
http://A01Y_RETLINK?&
B02K_VERS&B02K_TIMESTAMP&B02K_IDNBR&B02K_STAMP&
B02K_CUSTNAME&B02K_KEYVERS&B02K_ALG&B02K_CUSTID&
B02K_CUSTTYPE&B02K_MAC
```

Tarkiste (B02K_MAC) lasketaan alkuperäisestä sanomasta, jonka jälkeen skandinaaviset merkit ja eräät erikoismerkit (esim. tyhjämärkit, yhtäläisyys- ja lainausmerkit) korvataan vastaavalla heksadesimaalimerkillä (esim. %20) tietoliikennesanomassa.

Tapiola laskee vastaussanomien MAC-tarkisteen palveluntarjoajakohtaisella avaimella. Tarkisteen avulla palveluntarjoaja voi varmistua, että tunniste on muodostettu asiakkaan pankissa ja tunniste-sanomien tiedot eivät ole muuttuneet.

6.4 Vastaussanomien kenttien selitykset

Kenttä 1

Vastaussanomien versionumero on 0002.

Kenttä 2

Tapiolan tietojärjestelmän muodostama aikaleima, jossa kolme ensimmäistä merkkiä on pankin numero. 360 = Tapiola Pankki.

Kenttä 3

Tapiolan tietojärjestelmän tunnisteelle antama tieto, joka yksilöi tunnisteen Tapiolan järjestelmässä.

Kenttä 4

Tunnistepyyynnön yksilöintitieto, joka on poimittu kyseisen tunnistepyyynnön tietokentästä 5 (A01Y_STAMP)

Kenttä 5

Tapiolan asiakastietokannassa oleva tunnistetun asiakkaan nimi.

Kenttä 6

MAC-tarkisteavaimen laskennassa käytetyn avaimen version on 0001.

Kenttä 7

MAC-tarkistealgoritmin tyyppi: 01 = MD5 tai 03 = SHA-256.

Kenttä 8

Asiakkaan tunnistetieto, jonka sisältö riippuu tunnistepyyynnön A01Y_IDTYPEkentän sisällöstä. Kentän sisältö voi siis vaihtoehtoisesti olla joko salattu tai selväkielinen yksilöintitieto.

Kenttä 9

Tunnisteen tyyppi. Tämä kenttä kertoo, mikä kentän 8 tunnistetieto on. Mahdollisia arvoja ovat:

01 = selväkielinen henkilötunnus
02 = selväkielinen henkilötunnuksen tarkenne
03 = selväkielinen Y-tunnus
05 = salattu henkilötunnus
06 = salattu Y-tunnus

Kenttä 10

Vastaussanomien tarkiste.

6.5 Vastaussanomien tarkisteen laskenta

Palveluntarjoaja tarkastaa vastaanottamansa vastaussanomien eheyden laskemalla siitä aluksi MAC-tarkisteen, jota verrataan sanomien tarkisteeseen. Tarkiste lasketaan vastaussanomien tietokentistä 1 – 9. Kentän B02K_CUSTID sisältö määräytyy sen mukaan, mitä tunnusta tunnistepyyntöön on pyydetty. Se on siis vaihtoehtoisesti joko salattu tarkiste tai selväkielinen asiakastunnus. Tarkisteen laskennassa tiedot ja tarkisteavain erotetaan toisistaan ”&” –merkillä, joka lisätään myös tarkisteavaimen loppuun. Tieto on yhtenä rivinä. ”☐” –merkki näyttää tässä dokumentissa olevan rivinvaihdon. Tarkisteen laskennassa käytetään palveluntarjoajakohtaista avainta:

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

Kuten tunnistepyyntöjen tarkisteen laskennassa, tulee myös vastaussanomien tarkisteen laskennassa käytettäessä SHA-256-salausalgoritmiä palveluntarjoajan ennen tarkisteavaimen käyttöönottoa konvertoida PART1 ja PART2 muodostuva 64-merkkinen heksadesimaalimuotoinen avain string-muotoon. String-muodossa esitettyä tarkisteavainta on 32 merkin mittainen.

6.6 Tunnisteen tyyppi

Vastaussanomien tarkisteen laskentaan vaikuttaa välitettävän asiakastunnisteen tyyppi, joka määritellään pyyntösanoman A01Y_IDTYPE-kentässä. Asiakkaan tunniste on joko selväkielinen asiakastunnus tai salattu tarkiste

6.6.1 Selväkielinen asiakastunnus

Tunnistepyyntö A01Y_IDTYPE-kentän arvot ovat "02" tai "03", eli selväkielinen perustunnus tai selväkielinen työstetty perustunnus.

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

6.6.2 Salattu tarkiste

Tunnistepyyntö A01Y_IDTYPE-kentän arvo on "01" eli salattu perustunnus.

Pankki käyttää asiakastunnuksen salaamisessa samaa tiivistealgoritmia kuin sanomien tarkistelas-kennassa. Tunnistetieto salataan käyttämällä vastaussanomien tietokentissä 2-4 olevia tietoja ja pankissa rekisteröityä asiakkaan tunnusta (henkilötunnus tai Y-tunnus). Salatun tunnuksen lasken-nassa tiedot ja tarkisteavain erotetaan toisistaan &-merkillä, joka lisätään myös tarkisteavaimen lop-puun. Salaamisessa käytetään palvelutarjoajakohtaista tarkisteavainta.

B02K_TIMESTAMP&B02K_IDNBR&B02K_STAMP&asiakastunnus&tarkisteavain&

Salattu tunnus muutetaan heksadesimaaliseen esitysmuotoon, jossa arvot A-F esitetään isoilla kir-jaimilla. Lopputuloksena saadaan asiakkaan tunnisteksi merkkijono, joka sijoitetaan vastaussano-maan tiedoksi B02K_CUSTID.

6.7 Poikkeustilanteet

Palveluntarjoajan on varauduttava poikkeustilanteisiin, joita voivat olla:

1. Asiakas keskeyttää tunnistustapahtuman

Asiakas voi keskeyttää tapahtuman joko ennen tunnistepyyntöä välittämistä Tapiolaan tai tun-nisteen luonnin jälkeen Peruuta -painikkeella, jossa osoitteena on tunnistepyyntöä FORM-tietokentässä 8 oleva Peruuta -osoite.

2. Asiakkaan todennus epäonnistuu

Asiakkaan todennus voi epäonnistua joko asiakkaan tunnistetietojen virheellisyyden takia tai mikäli asiakas on pyytänyt todennusta väärästä pankista. Asiakas palaa palveluntarjoajan pal-veluun peruuta-painikkeella, jossa osoitteena on tunnistepyyntöä FORM -tietokentässä 8 oleva Peruuta -osoite.

3. Tapiola havaitsee virheen tunnistepepyyntösanomassa

Tapiola havaitsee virheen tunnistepepyynnössä ennen asiakkaan todennusta. Asiakas palaa palveluntarjoajan palveluun FORM -tietokentässä 9 olevaan Hylätty –osoitteeseen.

4. Palveluntarjoaja havaitsee virheen vastaussanomassa

Palveluntarjoaja havaitsee vastaussanomien tarkastuksen yhteydessä virheen, joka 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 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 vastaussanomien siirtyessään selaimensa ikkunoissa eteen/taakse –näppäimillä ruudusta toiseen.

7 Testaus

Palveluntarjoaja voi testata palvelua tuotantoympäristössä milloin tahansa käyttämällä Tapiolan testitunnuksia.

Osoite: <https://pankki.tapiola.fi/service/identify>

Testikäyttäjätunnus 12345678
Testialasana 123TAP
Testitunnusluku 9999

FORM-TIETORYHMÄ

Kenttä	Tiedon nimi	Pituus	P/V	Arvo
1. Sanomatyyppi	A01Y_ACTION_ID	3	P	' 701'
2. Versio	A01Y_VERS	4	P	' 0002'
3. Palveluntuottajan tunnus	A01Y_RCVID	8-15	P	' TAPTUPASID'
4. Palvelun kieli	A01Y_LANGCODE	2	P	FI = suomi SV = ruotsi
5. Kyselyn yksilöinti	A01Y_STAMP	20	P	vvvkkpphhmmssxxxxxx
6. Tunnisteen tyyppi	A01Y_IDTYPE	2	P	01 = salattu perustunnus 02 = selväkielinen perustunnus 03 = selväkielinen tyypistetty 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	' 0001'
11. Algoritmi	A01Y_ALG	2	P	01 = MD5 03 = SHA-256
12. Tarkiste	A01Y_MAC	32-64	P	PAPAKAIJU

VASTAUSSANOMA

Kenttä	Tiedon nimi	Muoto	P/V	Arvo
1. Versio	B02K_VERS	4	P	' 0002'
2. Tunnisteen yksilöinti	B02K_TIMESTMP	23	P	360vvvvkkpphhmssxxxxxx
3. Tunnisteen numero	B02K_IDNBR	10	P	Tapiolan tunnisteelle antama numero
4. Kyselyn yksilöinti	B02K_STAMP	20	P	Kyselyn tietokenttä 5 (A01Y_STAMP)
5. Asiakas	B02K_CUSTNAME	40	P	Testi Tapio
6. Avainversio	B02K_KEYVERS	4	P	' 0001'
7. Algoritmi	B02K_ALG	2	P	01 = MD5 03 = SHA-256
8. Tunniste	B02K_CUSTID	-64	P	' 010170-960F'
9. Tunnisteen tyyppi	B02K_CUSTTYPE	2	P	' 08' = selväkielinen muu tunnus ' 09' = salattu muu tunnus
10. Tarkiste	B02K_MAC	32-64	P	Vastauksen turvatarkiste

8 Neuvonta ja tekninen tuki

Ongelmatilanteissa ota yhteyttä sähköpostiosoitteeseen tunnistuspalvelu@tapiola.fi.

9 Palvelussa käytettävä merkistö

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

Verkkotunnistuspalvelu

æ	%00	0	%30	`	%60		%90	À	%c0	ó	%f0
	%01	1	%31	a	%61	´	%91	Á	%c1	õ	%f1
	%02	2	%32	b	%62	ˆ	%92	Â	%c2	ö	%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	§	%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	¢	%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	Ø	%d7		
	%18	H	%48	x	%78	˘	%a8	Ù	%d8		
	%19	I	%49	y	%79	©	%a9	Ú	%d9		
	%1a	J	%4a	z	%7a	ª	%aa	Û	%da		
	%1b	K	%4b	{	%7b	«	%ab	Ü	%db		
	%1c	L	%4c		%7c	¬	%ac	Ý	%dc		
	%1d	M	%4d	}	%7d	ˆ	%ad	Þ	%dd		
	%1e	N	%4e	~	%7e	@	%ae	ß	%de		
	%1f	O	%4f		%7f	—	%af		%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	ˆ	%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	ˆ	%88	¸	%b8	è	%e8		
)	%29	Y	%59	%o	%89	¹	%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		%8d	½	%bd	í	%ed		
.	%2e	^	%5e	Ž	%8e	¾	%be	î	%ee		
/	%2f	_	%5f		%8f	¿	%bf	ï	%ef		