

E-tunniste

Palvelukuvaus

Sisällys

1.1 E-tunnisteen edut.....	2
1.2 E-tunnisteen yleiskuvaus	2
1.3 E-tunnisteen toiminnot	3
1.4 Soveltuvuus ja käytettävyys	3
1.5 E-tunnisteen turvallisuus	4
2 E-tunnisteen toiminnallinen kuvaus	5
2.1 Palvelun etenemistä kuvaava kaavio	5
2.2 Palvelun etenemistä kuvaavan kaavion selite:	6
3 E-tunnisteen sanomakuvaukset.....	6
3.1 Tunnistepyyntö	6
3.2 Tunnistepyyntöä koskevien kenttien selitykset:	7
3.3 Tunnistepyyntöä koskevien MAC-tarkisteen muodostaminen.....	8
3.4 Vastausanoma ja tunniste	9
3.5 Vastausanomien kenttien selitykset	10
3.6 Vastausanomien tarkisteen laskenta	10
3.7 Tunnisteen tyyppi.....	10
3.8 Sanoman tarkisteen tarkastus ja asiakkaan tunnistus	11
4 Poikkeustilanteet.....	11
5 Tarkisteavaimen vaihto ja säilytys.....	12
5.1 MAC-tarkisteavaimen sulkeminen	12
6 Toiminnot ja Nordea-painike	12
7 E-tunnisteen käyttöönotto.....	12
7.1 Edellytykset	12
7.2 Sopimukset	13
7.3 Testaus.....	13
8 Neuvonta & tekninen tuki.....	14
Yritysten maksuliikeneuvonta	14
9 Palvelussa käytettävä merkistö	15

E-tunniste

E-tunnisteen avulla palveluntarjoaja tunnistaa luotettavasti asiakkaitaan Nordean tunnistamismenetelmiä hyväksikäyttäen. E-tunniste-palvelussa Nordea tunnistaa asiakkaan palveluntarjoajan puolesta. E-tunnistepalvelussa välitettäviä tunnistamistietoja voidaan käyttää myös osana sähköisen allekirjoituksen muodostamista tunnistautuvan asiakkaan ja palveluntarjoajan niin sopiessa.

Nordea laskee liikkeelle e-tunnistepalvelussa tarvittavat tunnistusvälineet. Palveluntarjoajalle Nordea toimittaa MAC-avaimet ja tunnistautuvalle asiakkaalle verkkopankkitunnukset.

Nordean e-tunniste perustuu Finanssialan keskusliitossa laadittuun Tupas-standardiin. Yhdessä muiden pankkien vastaavien palvelujen kanssa, palveluntarjoaja voi tavoittaa useita miljoonia suomalaisia yksityishenkilöitä verkkopalvelunsa asiakkaiksi. Lisätietoa standardista Finanssialan Keskusliiton sivuilta www.fkl.fi.

Nordea on Viestintäviraston Vahvan sähköisen tunnistamisen rekisterissä. Nordean e-tunnistepalvelu on lain tarkoittama vahvan sähköisen tunnistamisen palvelu silloin, kun tunnistus tehdään suomalaisen henkilötunnuksen omaavalle luonnolliselle henkilölle. Yritystunnistamisen ollessa kyseessä tarjottava palvelu ei ole lain määrittämää vahvaa sähköistä tunnistamista, sillä tunnistaminen tapahtuu yrityksen tasolla, eikä tunnistaminen siten kohdistu lain edellyttämällä tavalla luonnollisen henkilön henkilöllisyyteen.

Nordea tarjoaa kahta erillistä e-tunniste palvelua.

Perinteinen e-tunniste

- Yksi tunnistautumistapa per asiointikerta.
- Ei salli omien tunnusten luomista.
- Pankki vastaa tunnistustapahtuman oikeellisuudesta.

E-tunniste omien tunnusten luojille:

- Asiakas tunnistautuu e-tunnisteella kerran.
- Palveluntarjoaja voi myöntää omat tunnisteet asiakkaalle, eikä jatkossa e-tunnistetta enää tarvita.
- Pankki vastaa tunnistustapahtuman oikeellisuudesta e-tunnistetta käytettäessä.
- Omilla tunnuksilla tehdyt tunnistustapahtuman oikeellisuudesta vastaa palveluntarjoaja.

1.1 E-tunnisteen edut

Internetissä olevien palveluiden teho perustuu helppokäyttöisyyteen. Palvelun helppokäyttöisyyteen vaikuttaa mm. mahdollisuus käyttää omia tuttuja tunnistamismenetelmiä. Nordean e-tunnisteen avulla palveluntarjoaja voi hyödyntää samoja tunnistamismenetelmiä kuin Nordean verkkopankkipalveluissa. E-tunnisteella palveluntarjoaja tavoittaa kaikki Nordean verkkopalvelujen asiakkaat potentiaalisina asiakkaina.

E-tunnisteen avulla palveluntarjoaja voi luotettavasti tunnistaa asiakkaansa ilman erillisiä asiakasnumeroita ja salasanoja. Tämä mahdollistaa palveluntarjoajalle huomattavia säästöjä kehittämis- ja ylläpito-kustannuksissa.

Palveluntarjoaja voi sopia tunnistautuvan asiakkaan kanssa palvelun käyttämisestä osana sähköisen allekirjoituksen muodostamista heidän välisessään oikeustoimessa, mikä mahdollistaa erilaisten hakemusten vastaanottamisen sekä sopimusten tekemisen verkossa. Pankki huolehtii kuitenkin tällöin e-tunnistepalvelussaan ainoastaan asiakkaan tunnistamisesta. Palveluntarjoaja tulee huolehtia muista sähköisen allekirjoituksen edellyttämistä seikoista, kuten esim. tietojen kokonaisuuden hallinnasta, vastaussanomien tallentamisesta ja oman palvelunsa muuttumattomuudesta.

E-tunniste tuo lisäturvaa myös maksamiseen verkkokaupassa. E-tunnisteen avulla palveluntarjoaja ja asiakas voivat esimerkiksi sopia tilauksesta tai laskutuksesta. Lisäksi e-tunnisteella voi myös parantaa e-maksun turvallisuutta, sillä eräpäivämaksujen käyttö on huolettomampaa mikäli tilaajan henkilöllisyys on varmennettu ja tilaus päivätty.

1.2 E-tunnisteen yleiskuvaus

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

Nordean antama tunniste on ainutkertainen ja se on sidottu sekä palveluntarjoajan kyseiseen palvelutapahtumaan että asiakkaaseen.

Kun palveluntarjoajalla on tarve tunnistaa asiakkaansa, palveluntarjoaja lähettää tunnistepyynnön asiakkaalle, joka siirtyy Nordean tunnistepalveluun painamalla Nordean toimintopainiketta.

Palveluntarjoajan tunnistepyyntö välittyy asiakkaalta Nordean tunnistepalveluun, joka lähettää tunnistamisen jälkeen asiakkaalle vastaussanomaa. Asiakas tarkastaa vastaanottamansa vastaussanomaa tiedot, joiden hyväksymisen jälkeen hän palaa takaisin palveluntarjoajan palveluun ja jatkaa siellä palveluun liittyviä toimintoja. Asiakas voi halutessaan peruttaa tai hylätä tunnistustapahtuman joko ennen tunnistautumista tai vastaussanomaa tarkastamisen jälkeen, jolloin asiakkaan tiedot eivät välity palveluntarjoajalle.

Mahdollisuus käyttää palvelun tietoja osana sähköistä allekirjoitusta perustuu palveluntarjoajan ja asiakkaan keskinäiseen sopimukseen siitä, että tunnistetietoja voidaan käyttää osana sähköistä allekirjoitusta heidän välisessään oikeustoimessa. E-tunnisteen käyttämistä sähköisenä allekirjoituksena tukevat lisäksi Nordean verkkopankkisopimuksen ehdot, vastaussanomien aikaleimat sekä Nordean lokitiedot. Jos palvelua halutaan käyttää hyväksi osana sopimuksen tai hakemuksen tekemistä, tulee palveluntarjoajan kuitenkin huolehtia muista sähköisen allekirjoituksen edellyttämistä seikoista, kuten tietojen kokonaisuuden hallinnasta, vastaussanomaa tallentamisesta ja oman palvelunsa muuttumattomuudesta. Nordea ei vastaa palveluntarjoajan ja tunnistautuvan asiakkaan välisen sopimuksen tai muun oikeustoimen pätevydestä tai sisällöstä eikä yrityksen tunnistautumistietoja käyttävän henkilön kelpoisuudesta tai toimivallasta edustaa yritystä tai yhteisöä.

1.3 E-tunnisteen toiminnot

E-tunniste-palvelussa on eri toimintoja ja käyttömahdollisuuksia sen mukaan, millaisen vastaussanomaa välittämistä on palvelusopimuksessa sovittu. Nordean antama vastaussanomaa tunnistetieto sisältää aina asiakkaan nimen. Tämän lisäksi välitettävä tunnistetieto voi olla joko selväkielinen tai salattu.

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

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

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

1.4 Soveltuvuus ja saatavuus

E-tunniste-palvelu on tarkoitettu suomalaisille yksityishenkilöille suunnattuihin sähköisiin palveluihin, joissa tarvitaan vahvaa tunnistautumista. Vahva sähköinen tunnistaminen perustuu henkilökohtaisiin pankkitunnuksiin. Tämän johdosta esimerkiksi muiden kuin suomalaisen henkilötunnuksen omaavan, keino-tunnuksen omaavan tai kuolinpesän tunnistaminen e-tunniste-palvelussa ei ole mahdollista.

E-tunnistepalvelua voidaan käyttää myös yritys- ja yhteisöasiakkaiden tunnistamiseen. Kun pankki toimittaa yksilöintitietona yrityksen Y-tunnuksen tai muun yrityksen yksilöintitiedon, kyseessä ei ole vahva sähköinen tunnistaminen.

E-tunniste-palvelu on käytettävissä 24 tuntia kaikkina viikonpäivinä, pois lukien huollosta, päivityksestä tms. syystä johtuvista katkoajoista.

1.5 E-tunnisteen turvallisuus

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

Tunnistepyyntöön ja vastaussanomien tiedot on suojattu tiedon eheyden turvaavalla tarkisteella, joten tunnistetietojen välitystä ohjaavalla asiakkaalla ei ole mahdollisuutta muuttaa tietoja palveluntarjoajan ja Nordean sitä havaitsematta.

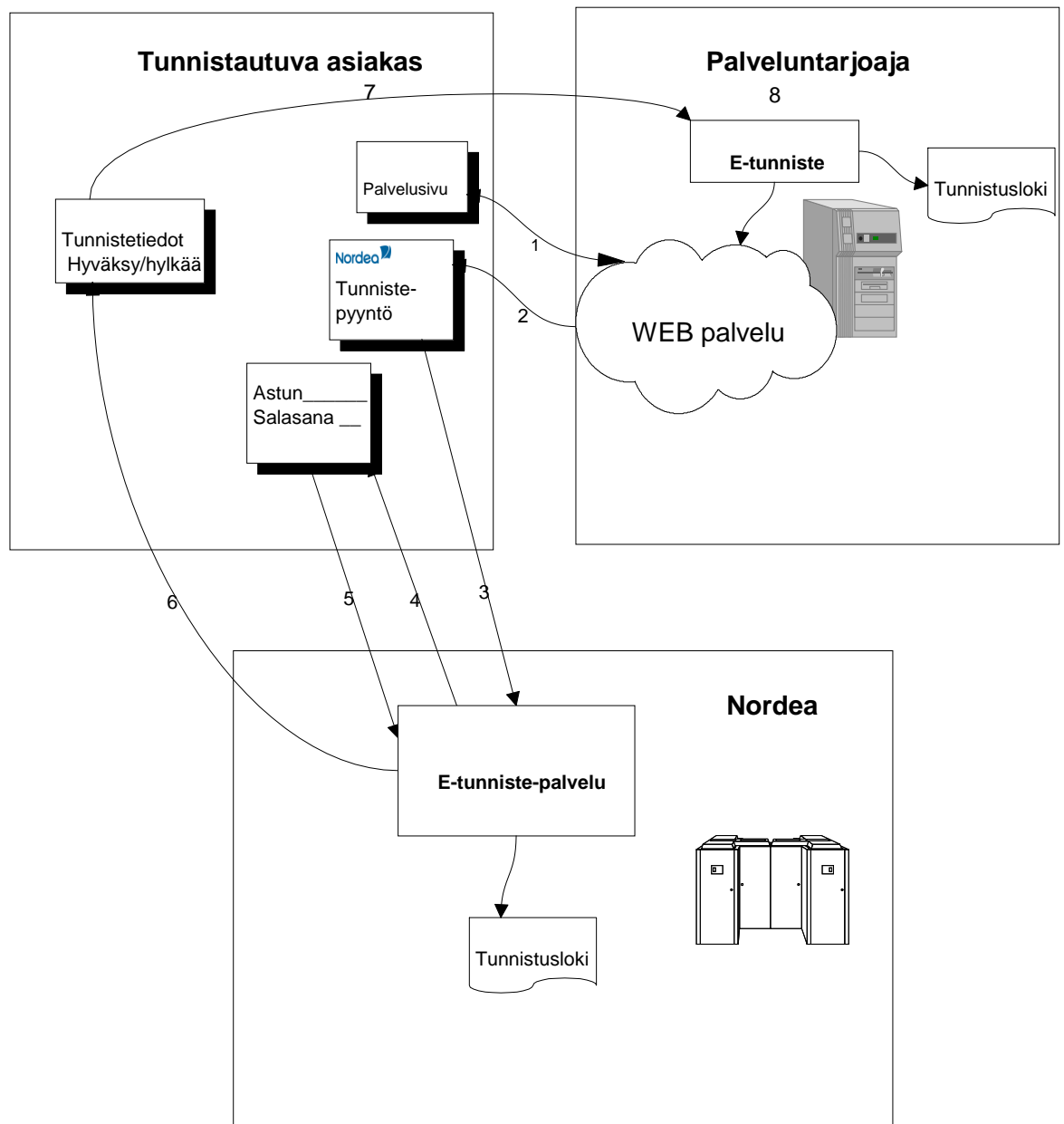
Kukin osapuoli vastaa omien palveluittensa suojauksesta, turvallisuudesta ja säilyttämiensä tietojen oikeellisuudesta. Tunnistautuva asiakas vastaa siitä, että Nordean antamat tunnuksot tai muut todennusvälineet eivät joudu ulkopuolisten haltuun.

Palvelun käyttäjä vastaa siitä, että hänen pankkitunnuksensa eivät joudu ulkopuolisten haltuun ja että tunnuksot annetaan vain Nordean tunnistuspalvelua hoitavalle tietokoneelle. Palvelun käyttäjä myös varmistaa Nordean palauttamista tunnistetiedoista palveluntarjoajan ja hyväksyy e-tunnisteen välittämisen.

2 E-tunnisteen toiminnallinen kuvaus

2.1 Palvelun etenemistä kuvaava kaavio

E - tunnisteen periaate



2.2 Palvelun etenemistä kuvaavan kaavion selite:

1. Tunnistautuva asiakas on yhteydessä palveluntarjoajan palveluun. Asiakkaan ja palveluntarjoajan välisen tietoliikenteen tulee olla SSL/TLS-suojattua, kun asiakas siirtyy tunnistepalveluun liittyvien tietojen syöttöön. Vaiheiden 2 - 7 aikana tiedonsiirtoyhteys on aina SSL/TLS-suojattu.
2. Palveluntarjoaja lähettää asiakkaalle tunnistepyyntön, joka sisältää tapahtumaan liittyvät yksilöinti-tiedot. Palveluntarjoajan tunnistuspyyntö asettaa tunnistautuvan asiakkaan näytölle Nordea-painikkeen sekä tapahtuman peruutuspainikkeen.
3. Asiakas painaa toimintopainiketta, joka johtaa hänen Nordean tunnistuspalveluun. Nordeaan välit-tyvä tunnistuspyyntö sisältää tunnistepalvelun tarvitsemat tiedot palveluntarjoajasta ja tapahtumas-ta. Nordea tarkastaa tunnistepyyntön eheyden ja tietojen oikeellisuuden.
4. Nordea lähettää asiakkaalle tunnistuspyyntön, jos palveluntarjoajalta toimitettu pyyntö on virhee-tön. Nordea antaa asiakkaalle virheilmoituksen, jos Nordea havaitsee tunnistepyyntönsä virheitä.
5. Asiakas tunnistautuu Nordeaan. Nordea palauttaa asiakkaalle virheilmoituksen, jos tunnistus epä-onnistuu.
6. Onnistuneen todennuksen jälkeen Nordea muodostaa vastaussanoman. Nordean tunnistuspalvelu asettaa tunnistautuvalle asiakkaalle hyväksymis- ja peruutuspainikkeet ja lähettää vastaussanoman tämän selaimelle.
7. Asiakas tarkastaa tunnisteen tiedot ja hyväksyy tunnisteen välittämisen palveluntarjoajalle. Asiakas voi peruutuspainikkeella hylätä tunnisteen ja palata takaisin palveluntarjoajan palveluun.
8. Palveluntarjoaja varmistaa vastaanottamansa vastaussanoman eheyden ja ainutkertaisuuden. Palve-luntarjoaja liittää tunnisteen asiakkaan palvelutapahtumaan ja säilyttää sitä yhtä kauan kuin muita palvelutietoja säilytetään. Tunnisteita ei saa rekisteröidä tai käyttää muuhun tarkoitukseen.

3 E-tunnisteen sanomakuvaukset

3.1 Tunnistepyyntö

Tunnistepyyntön tiedot ovat Nordean kuvakkeen takana FORM-tietoryhmässä piilomuuttujina.

Tietoryhmän rakenne on HTML-kielellä:

```
<FORM  
METHOD="POST"  
ACTION="https://tupas.nordea.fi/cgi-bin/SOLO3011">  
<INPUT NAME="..." TYPE="..." VALUE="...">  
<INPUT NAME="..." TYPE="..." VALUE="...">  
</FORM>
```

FORM-TIETORYHMÄ				
Kenttä	Tiedon nimi	Pituus	Pakollisuus	Huomaus
1. Sanomatyyppi	A01Y_ACTION_ID	3 - 4	P	Vakio, "701"
2. Versio	A01Y_VERS	4	P	0002
3. Palveluntarjoaja	A01Y_RCVID	10 -15	P	Asiakastunnus
4. 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 = SHA-256
12. Tarkiste	A01Y_MAC	32-64	P	Kyselyn turvatarkiste

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

```
<FORM METHOD="POST" ACTION="Nordean E-tunniste-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>
```

3.2 Tunnistepyyntöjen kenttien selitykset:

1. Sanoman tyyppi, joka on vakio 701.
2. Tunnistepyyntö-sanoman versionumero, joka on 0002.
3. Palveluntarjoajan asiakastunnus. Nordea tunnistaa palveluntarjoajan asiakastunnuksen perusteella ja liittää rekisterissään olevan palveluntarjoajan nimen tunnistesanomaa.

4. Palvelun kielikoodi kertoo palveluntarjoajan asiointisivun kielen ja Nordean palvelu avautuu tällä kielellä, mikäli kyseinen kieli kuuluu Nordean e-tunnisteessa kulloinkin käytössä olevaan kielivalikoimaan.
5. Palveluntarjoajan tunnistepyyntöille antama yksilöivä tunnus. Tunnuksena voi olla viite, asiakasnumero tai yhdistelmä päivämäärästä, kellonajasta ja juoksevasta tunnuksesta sekä viitteestä.
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. Sisältää asiakkaan täydellisen henkilötunnuksen tai Y-tunnuksen.

02 = Selväkielinen perustunnus. Sisältää asiakkaan täydellisen henkilötunnuksen tai Y-tunnuksen.

03 = Selväkielinen tyhistetty tunnus. Sisältää henkilötunnuksen tarkenteen osan ilman vuosisataa ilmoittavaa välimerkkiä tai kokonaisen Y-tunnuksen.

7. Palveluntarjoajan palvelusivun osoite, joka on OK-tapauksessa jatkokohta. Paluuosoitteen tulee olla https-alkuinen, eli SSL/TLS-suojattu sivu.

Esimerkki: VALUE="<https://tuote.kauppa.fi/tilaus/vahvistus.htm>"

8. Palveluntarjoajan palvelun jatkokohta, jos asiakas peruuttaa tunnisteen välittämisen.

Esimerkki: VALUE="<https://tuote.kauppa.fi/tilaus/keskeytyk.htm>"

9. Palveluntarjoajan palvelun jatkokohta, jos tunnistuksessa on havaittu tekninen virhe. Paluuosoite voi olla sama kuin kentässä 10.

Esimerkki: VALUE="<https://tuote.kauppa.fi/tilaus/virhe.htm>"

10. MAC-tarkisteen laskennassa käytetyn avaimen versio.
11. MAC-tarkisteen laskennassa käytettävän algoritmin tyyppikoodi. Nordean e-tunnisteessa on käytössä tällä hetkellä 03= SHA-256 algoritmi.
12. MAC-tarkiste, joka on laskettu tunnistepyyntönsuojattavista tiedoista ja palveluntarjoajan tarkisteavaimesta tietokentässä 11 määritellyillä algoritmeilla. Vastaanottaja tarkistaa tarkisteesta tunnistepyyntönsuojattavien tietojen eheyden ja lähettäjän.

3.3 Tunnistepyyntönsuojattavien MAC-tarkisteen muodostaminen

Palveluntarjoaja muodostaa Nordea-painiketta varten tunnistepyyntönsuojattavan, joka suojataan MAC-tarkisteella. Tarkiste lasketaan tunnistepyyntönsuojattavien FORM-tietoryhmästä Nordean 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 12) ja tarkisteavaimen väliin sekä tarkisteavaimen loppuun laitetaan "&"-merkki. "&"-merkit otetaan sanoman MAC-tarkisteen laskentaan mukaan. Tieto on yhtenä rivinä. "\n" -merkki näyttää tässä dokumentissa olevan rivinvaihdon.

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

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

3.4 Vastaussanoma ja tunniste

Nordea 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.

Nordea laskee vastaussanomien MAC-tarkisteen palveluntarjoajakohtaisella avaimella. Tarkisteen avulla palveluntarjoaja voi varmistua, että tunniste on muodostettu asiakkaan pankissa ja tunnistesanomien tiedot eivät ole muuttuneet. Palveluntarjoajan tulee varmistaa MAC-tarkisteen oikeellisuus tunnistamistapah-tuman saatuaan.

VASTAUSSANOMA				
Kenttä	Tiedon nimi	Pituus	Pakol-lisuus	Huomautus
1. Versio	B02K_VERS	4	P	0002
2. Tunnisteen yksilöinti	B02K_TIMESTMP	23	P	NNNvvvvkkpphmmssxxxxxx
3. Tunnisteen numero	B02K_IDNBR	10	P	Nordean tunnisteelle antama numero
4. Kyselyn yksilöinti	B02K_STAMP	20	P	Kyselyn tietokenttä 7 (A01Y_STAMP)
5. Asiakas	B02K_CUSTNAM E	40	P	Asiakkaan nimi
6. Avainversio	B02K_KEYVERS	4	P	Avaimen sukupolvi
7. Algoritmi	B02K_ALG	2	P	03 = SHA-256
8. Tunniste	B02K_CUSTID	-64	P	Salattu tarkiste tai selväkielinen asiakastunnus
9. Tunnisteen tyyppi	B02K_CUSTTYPE	2	P	01 = selväkielinen henkilötun-nus 02 = selväkielinen hetun tar-kenne 03 = selväkielinen Y-tunnus 05 = salattu henkilötunnus 06 = salattu Y-tunnus
10. Tarkiste	B02K_MAC	AN 32-64	P	Vastauksen turvatarkiste

3.5 Vastaussanomien kenttien selitykset

1. Vastaussanomien versionumero, joka on 0002.
2. Nordean järjestelmän muodostama aikaleima, jossa NNN on aina 200 ja ilmaisee, että kyseessä on Nordea. Tällä hetkellä Nordea palauttaa 19 merkkiä muotoa NNNvvvvkkpphhmssxx missä aikaleiman perässä olevat xx merkitsevät sadasosasekunteja.
3. Nordean tietojärjestelmän tunnisteelle antama tieto, joka yksilöi tunnisteiden Nordean järjestelmässä.
4. Tunnistepyyntöjen yksilöintitieto, joka on poimittu kyseisen tunnistepyyntöjen tietokentästä 7 (A01Y_STAMP)
5. Nordean asiakastietokannassa oleva asiakkaan nimi.
6. MAC-tarkisteavaimen sukupolvitieto.
7. MAC-tarkistealgoritmin tunnus.
8. Asiakkaan tunnistetieto. Selväkielinen tunnus tai salattu tarkiste riippuen tunnistepyyntöjen A01Y_IDTYPE-kentän sisällöstä. Selväkielinen y-tunnus välitetään väliviivan kanssa muodossa xxxxxxx-x.
9. Tunnisteen tyyppi. Tämä kenttä kertoo, mikä kentän 8 tunnistetieto on. Mahdolliset arvot ovat:
00 = ei tiedossa (ei käytössä Nordeassa)
01 = selväkielinen henkilötunnus
02 = selväkielinen hetun tarkenne
03 = selväkielinen Y-tunnus.
04 = selväkielinen sähköinen asiointitunnus. Ei käytössä Nordeassa
05 = suojattu henkilötunnus
06 = suojattu Y-tunnus.
07 = salattu sähköinen asiointitunnus. Ei käytössä Nordeassa
10. Vastaussanomien tarkiste.

3.6 Vastaussanomien tarkisteen laskenta

Vastaanotetun vastaussanomien eheys tarkistetaan laskemalla siitä aluksi tarkiste, jota verrataan sanomien tarkisteeseen. Tarkiste lasketaan vastaussanomien tietokentistä 1-9. Kentän B02K_CUSTID sisältö määrittäytyy sen mukaan, mitä tunnusta tunnistepyyntöissä on pyydetty ja on siis vaihtoehtoisesti joko salattu tarkiste tai selväkielinen asiakastunnus. Tarkisteen laskennassa tiedot ja tarkisteavaimen erotetaan toisistaan &-merkillä, joka lisätään myös tarkisteavaimen loppuun. Tarkisteen laskennassa käytetään palveluntarjoajakohtaista avainta.

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

3.7 Tunnisteen tyyppi

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

1. Asiakkaan tunnisteena selväkielinen asiakastunnus

Tunnistepyyntöä A01Y_IDTYPE-kentän arvot ”02” ja ”03”: Selväkielinen perustunnus tai tyypistetty perustunnus.

Asiakkaan tunnus on selväkielinen merkkijono, esimerkiksi henkilötunnus tai sen loppuosa tunniste-
pyyntöä A01Y_IDTYPE mukaisesti. Tunnus sijoitetaan sellaisenaan vastaussanomana tiedoksi
B02K_CUSTID.

2. Asiakkaan tunnisteena salattu tarkiste

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

Pankki käyttää asiakastunnuksen salaamisessa samaa tiivistealgoritmia kuin sanomien tarkistelaskennas-
sa. Tunnistetieto salataan käyttämällä vastaussanomana tietokentissä 2-4 olevia tietoja ja pankissa rekis-
teröityä asiakkaan tunnusta (henkilötunnus tai Y-tunnus). Salatun tunnuksen laskennassa tiedot ja
tarkisteavain erotetaan toisistaan &-merkillä, joka lisätään myös tarkisteavaimen loppuun. Salaamisessa
käytetään palveluntarjoajakohtaista avainta.

*B02K_TIMESTMP&B02K_IDNBR&B02K_STAMP&_/
asiakastunnus&tarkisteavain&*

Salattu tunnus muutetaan heksadesimaaliseen esitysmuotoon, jossa arvot A-F esitetään isoilla kirjaimil-
la. Lopputuloksena saadaan asiakkaan tunnisteeksi merkkijono, joka sijoitetaan vastaussanomana tie-
doksi B02K_CUSTID.

3.8 Sanoman tarkisteen tarkastus ja asiakkaan tunnistus

Palveluntarjoaja laskee vastaanottamastaan sanomasta kohdassa 3.6 kuvatulla tavalla vastaanotetun sa-
nomana MAC-tarkisteen. Mikäli se on sama kuin vastaussanomassa pankista tullut vastaussanomana tar-
kiste, on vastaussanomana välittynyt muuttumattomana.

Jos vastaussanomassa on käytetty salattua tunnusta, tarkistaa palveluntarjoaja käytössään olevan asiak-
kaan tunnuksen oikeellisuuden laskemalla tarkisteen vastaussanomana tietokentistä ja käytössään olevas-
ta tunnuksesta kohdassa 3.7 esitetyllä tavalla. Mikäli saatu tarkiste vastaa vastaussanomana
tunnistekentän (B02K_CUSTID) sisältöä, palveluntarjoajalla käytössä oleva asiakkaan tunniste oikea.

4 Poikkeustilanteet

Palveluntarjoajan on varauduttava poikkeustilanteisiin, joita voivat olla:

1. Asiakas keskeyttää tunnistustapahtuman. Asiakas voi keskeyttää tapahtuman joko ennen tun-
nisteä välittämistä Nordeaan tai tunnisteä luonnin jälkeen peruuta-painikkeella, jossa osoit-
teena on tunnisteäpyyntöä FORM-tietokentässä 10 oleva Peruuta-osoite.
2. Asiakkaan todennus epäonnistuu joko asiakkaan antamien tunnistetietojen virheellisuuden takia
tai koska asiakas on pyytänyt todennusta väärästä pankista.
3. Nordea havaitsee virheen tunnisteäpyyntöäsanomassa
4. Palveluntarjoaja havaitsee virheen vastaussanomassa, joka voi johtua sanomana sisällössä ole-
vasta virheestä tai siitä, että tunniste ei vastaa asiakkaan ilmoittamia henkilötietoja. Palvelun-
tarjoajan 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 vastaussanomaa siirtyessään selaimensa ikkunoissa eteen / taakse -näppäimillä ruudusta toiseen.

5 Tarkisteavaimen vaihto ja säilytys

Tarkisteiden laskennassa käytettyä MAC-avainta voidaan vaihtaa Nordean tai palveluntarjoajan toivomuksesta.

Tarkisteavain toimitetaan sopimuksessa mainitulle yhteyshenkilölle. Samalla toimitetaan myös tietoa uuden avaimen versionumerosta ja voimaantulospäivästä. 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 tunnisteista tarkiste on laskettu vanhalla avaimella ja osa uudella.

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

5.1 MAC-tarkisteavaimen sulkeminen

Palveluntarjoajan tulee säilyttää MAC-tarkisteavain huolellisesti ja turvassa oikeudettomalta käytöltä. Jos MAC-tarkisteavaimen epäillään joutuneen väärin käsiin, tulee avain sulkea välittömästi Yritysten Maksuliikeneuvonnan kautta.

Pankkiaikojen ulkopuolella tulee ottaa yhteys sulkupalveluun +358 20 333.

6 Toiminnot ja Nordea-painike

Palveluntarjoajan verkkopalvelussa saa käyttää Nordeasta ainoastaan seuraavia nimiä:

Nordea

Nordea Pankki

Nordea Pankki Suomi Oyj

Palveluntarjoajan Internet-palvelussa e-tunnisteen käyttö on ilmaistava Nordea-painikkeella tai tekstillä Nordea e-tunniste ja sen on oltava selvästi näkyvillä.

Nordea-painikkeen esitystapa ja ohjeet sekä edellytykset niiden käytölle kerrotaan palvelusopimuksen ehtoissa. Nordea-painikkeen saa käyttöön sopimuksen tekemisen jälkeen Nordean palvelimelta osoitteesta www.nordea.fi/nordeapainike. Painiketta ei saa luovuttaa tai käyttää muuhun tarkoitukseen kuin palvelusopimuksessa on sovittu. Nordea-painiketta ei saa itse tehdä eikä muotoilla.

7 E-tunnisteen käyttöönotto

7.1 Edellytykset

Palveluntarjoajan järjestelmän on kyettävä muodostamaan WWW-tekniikalla palvelun käyttäjälle tunnistepyyntö. Kun käyttäjä on hyväksynyt tunnisteen välittämisen palveluntarjoajalle, pitää tunniste liittää käyttäjän antamaan toimeksiantoon ja säilyttää yhtä kauan kuin toimeksianto. Tunnisteita ei saa rekisteröidä tai käyttää muuhun tarkoitukseen. Palveluntarjoajan on kirjoitettava lokia, josta selviää tunniste-
pyynnön yksilöinti mahdollisten ongelma-/selvitystilanteiden varalta.

E-tunniste ei edellytä mitään tiettyä WWW-palvelinohjelmistoa, mutta sen tulee tukea 128 bittistä SSL/TLS-salausta.

7.2 Sopimukset

Palveluntarjoaja tekee kirjallisen sopimuksen e-tunnisteen käytöstä Nordean kanssa. Palveluntarjoajan tiedot rekisteröidään pankissa ja sopimuksessa mainitulle yhteys henkilölle lähetetään MAC-tarkisteavain.

Kustakin eri palvelusta tulee tehdä palvelusopimus. Samoin jokaisesta toiminnallisuudesta. Yhdessä palvelussa voi kuitenkin olla käytössä useita toiminnallisuksia. Nordea tekee sopimuksen henkilötunnuksen välittämistä 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.

7.3 Testaus

Palvelun käyttöönottopäivä sovitaan sopimuksen teon yhteydessä.

Palveluntarjoaja voi testata palvelua tuotantoympäristössä jo ennen kuin sopimus on tehty käyttämällä Nordean testitunnuksia. Mikäli palveluntarjoaja haluaa testata palvelua oikeilla pankkitunnuksilla ja/tai sopimuksensa toimivuutta, tulee palvelusta tehdä Nordean kanssa sopimus, joka tehdään suoraan tuotantotilaan. Sopimukselle voidaan kuitenkin määrittää palveluntarjoajan testiosoite testiajaksi.

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

Palveluntarjoaja: 87654321
Tarkisteavain: LEHTI

Tunnistusnäytössä asiakkaan käyttämät pankkitunnukset
Asiakasnumero: 123456
Tunnusluku: 1111

TUNNISTEPYYNTÖ -TESTISANOMA	
Form-tietokenttä	
A01Y_ACTION_ID	701
A01Y_VERS	0002
A01Y_RCVID	87654321
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	
B02K_VERS	0002
B02K_TIMESTAMP	kts. kuvaus
B02K_IDNBR	kts. kuvaus
B02K_STAMP	Kyselyn tietokenttä A01Y_STAMP
B02K_CUSTNAM	SOLO DEMO
B02K_KEYVERS	0001
B02K_ALG	03
B02K_CUSTID	Perustunnus: 210281-9988 Typistetty tunnus: 9988
	Salattu tunnus: Laskettu tunnuksesta 210281-9988
B02K_CUSTTYPE	kts kuvaus
B02K_MAC	kts kuvaus

8 Neuvonta & tekninen tuki

Yritysten maksuliikeneuvonta

Ongelmatilanteissa apua saa Yritysten maksuliikeneuvonnasta pankkipäivisin (varmistu aukioloajat aina pankin Internet-sivuilta tai konttorista):

Suomeksi: 0200 67210 (klo 8-18), (pvm/ mpm tai ulkomaanpuhelun hinta)

Ruotsiksi: 0200 67220 (klo 9-16.30), (pvm/ mpm tai ulkomaanpuhelun hinta)

Englanniksi: (+358) 200 67230 (klo 9-18), (pvm/ mpm tai ulkomaanpuhelun hinta)

Palveluntarjoajan tunnuksen ilmoittaminen nopeuttaa asiointia.

9 Palvelussa käytettävä merkistö

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

æ	%00	0	%30	`	%60	ˆ	%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	š	%93	Ã	%c3	ó	%f3
	%04	4	%34	d	%64	›	%94	Ä	%c4	ô	%f4
	%05	5	%35	e	%65	œ	%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	Ï	%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	ı	%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	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	%	%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	Ž	%8d	½	%bd	í	%ed		
.	%2e	^	%5e		%8e	¾	%be	î	%ee		
/	%2f	_	%5f		%8f	¿	%bf	ï	%ef		