Aktia tunnistuspalvelu

Käyttöohje ja tietuekuvaukset

30.9.2016, versio 1.4

Sisällysluettelo

1. Aktia tunnistuspalvelu

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

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

Lisätietoa standardista saa Finanssialan Keskusliiton verkkosivuilta www.fkl.fi.

2. Yleistä

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

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

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

Verkkopalvelun osoite on https://auth.aktia.fi/tupas
Aktia tunnistuspalvelu on käytettävissä 24 h/vrk.

2.1 Sopimukset

Palveluntarjoaja tekee kirjallisen sopimuksen Aktia tunnistuspalvelun käytöstä pankin kanssa. Palveluntarjoajan tiedot rekisteröidään pankissa ja sopimuksessa mainitulle yhteyshenkilölle lähetetään Tarkisteavaimen jälkimmäinen osa erikseen sovittavalla turvallisella tavalla. Tarkisteavaimen ensimmäinen osa tulostetaan sopimukselle.

Aktian tunnistuspalvelusta on käytössä versio 0003.

Pankki tekee sopimuksen henkilötunnuksen välittämisestä vain silloin kuin palveluntarjoajalla on oikeus rekisteröidä se.

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

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

2.2 Aktia tunnistuspalvelun nimi ja logo

Pankin verkkotunnistuksesta voidaan käyttää joko nimeä Aktia tunnistus tai Aktia identifiering. Muita nimityksiä ei saa käyttää. Aktia tunnistuksen logo on Aktia Pankin liikemerkki.

Palvelua tarjoava yritys kopioi logon omalle palvelimellensa Aktian palvelimelta osoitteesta http://www.aktia.fi/fi/verkkomaksu-tunnistuspalvelu-logo.fi.

Logon kokoa ja värejä ei saa muuttaa.

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

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

3. Turvallisuus

Tunnistuspalvelun osapuolten välisessä tietoliikenteessä käytetään SSL-salausprotokollaa, joten ulkopuoliset eivät näe tietoja eivätkä voi muuttaa niitä. Palveluntuottajan palvelinohjelmiston on tuettava 256 bitin SSL-salausta. Yhteydellä käytettävä avainpituus määräytyy kuitenkin asiakkaan käyttämän selaimen ominaisuuksien perusteella. Tunnistuspyynnön ja vastaussanoman tiedot on suojattu tiedon eheyden turvaavalla tarkisteella, joten tunnistustietojen välitystä ohjaavalla asiakkaalla ei ole mahdollisuutta muuttaa tietoja palveluntuottajan ja Aktia tunnistuspalvelun sitä havaitsematta.

Kukin osapuoli vastaa omien palveluittensa suojauksesta, turvallisuudesta ja säilyttämiensä tietojen oikeellisuudesta.

Palvelun käyttäjä vastaa siitä, että hänen verkkopankkitunnuksensa eivät joudu ulkopuolisten haltuun ja että tunnukset annetaan vain Aktia tunnistuspalvelua hoitavalle tietokoneelle. Palvelun käyttäjä myös varmistaa Aktia tunnistuspalvelun

palauttamista tunnistustiedoista palveluntarjoajan ja hyväksyy Aktia tunnistuksen välittämisen.

3.1 Tarkisteavaimen vaihto ja säilytys

Tarkisteavain on voimassa 2 vuotta ensimmäisestä onnistuneesta tunnistus-tapahtumasta lähtien. Tarkisteavaimen toinen osa lähetetään asiakkaalle siinä vaiheessa kun käytössä olevalla avaimella on 60 päivää voimassaoloaikaa jäljellä.

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

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

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

4. Toiminnallinen kuvaus

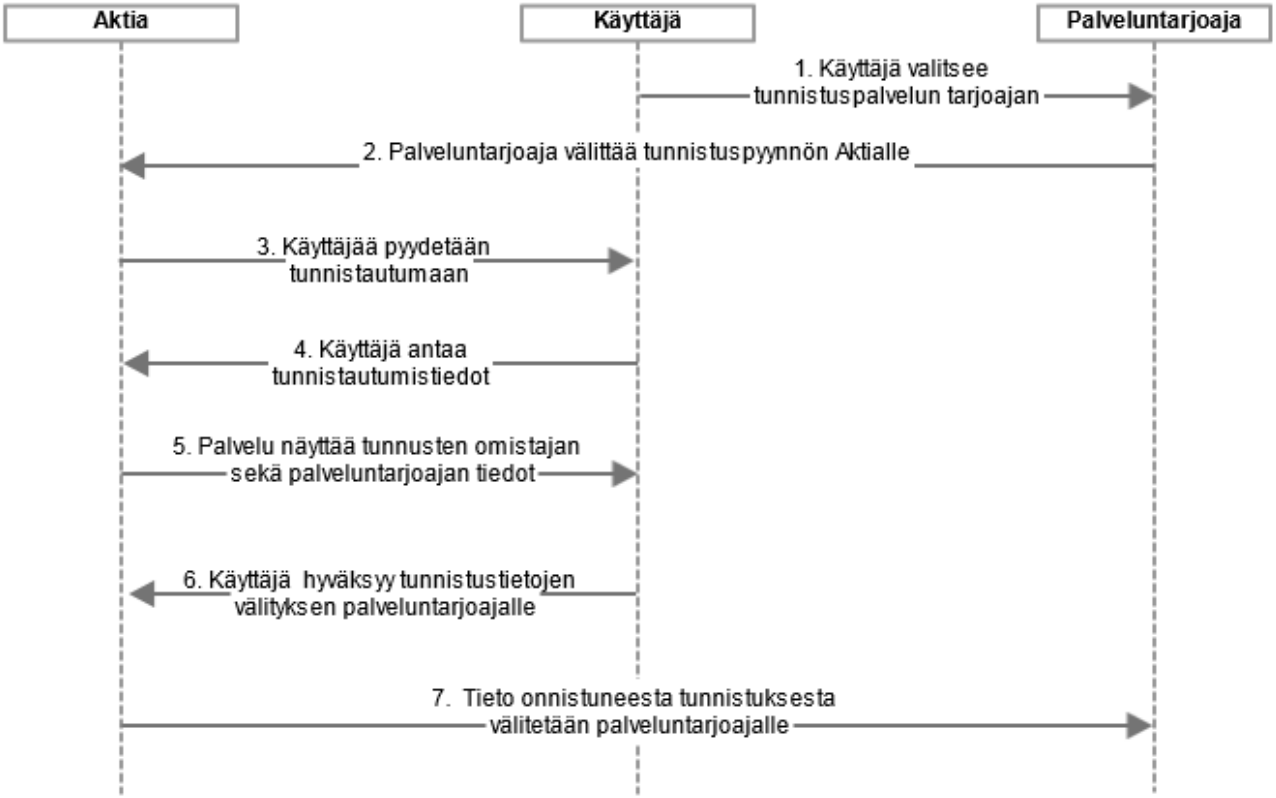
Aktia tunnistuspalvelussa on eri toimintoja ja käyttömahdollisuuksia sen mukaan, millaisen vastaussanoman välittämisestä on palvelusopimuksessa sovittu. Vastaussanoman tunnistustieto sisältää aina asiakkaan nimen. Tämän lisäksi välitettävä tunnistustieto voi olla joko selväkielinen tai salattu.

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

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

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

4.1 Palvelun eteneminen



Kaavion selite

1. Tunnistautuva käyttäjä on yhteydessä palveluntarjoajan palveluun.
2. Palveluntuottajalla on tarve tunnistaa käyttäjänsä. Tunnistuspyyntö sisältää tunnistuspalvelun tarvitsemat tiedot palveluntarjoajasta ja tunnistustapahtumasta. Aktia tarkastaa pyynnön eheyden, tietojen oikeellisuuden ja palveluntarjoajan tunnistuspalvelusopimuksen.
3. Aktia antaa käyttäjälle tunnistuspyynnön, jos palveluntarjoajalta toimitettu pyyntö on virheetön. Aktia antaa käyttäjälle virheilmoituksen, jos havaitsee tunnistepyynnössä virheitä. Käyttäjä voi halutessaan keskeyttää tunnistuksen ja palata takaisin palveluntarjoajan palveluun.
4. Käyttäjä tunnistautuu Aktian verkkopankkitunnuksilla. Käyttäjälle näytetään virheilmoitus, jos tunnistus epäonnistuu.
5. Käyttäjä tarkastaa tunnisteen tiedot. Aktia tunnistaa palveluntarjoajan asiakastunnuksen perusteella ja näyttää rekisterissä olevan palveluntarjoajan nimen käyttäjälle.
6. Käyttäjä hyväksyy tunnisteen välittämisen palveluntarjoajalle. Käyttäjä voi peruutuspainikkeella hylätä tunnisteen ja palata takaisin palveluntarjoajan palveluun.
7. Aktia lähettää palveluntarjoajalle tiedon onnistuneesta tunnistautumisesta palveluntarjoajan kanssa sovituilla käyttäjän tunnistetiedoilla rikastettuna ja lopettaa käyttäjän session Aktian palvelussa.

5. Aktia tunnistuspalvelun sanomakuvaukset

5.1 Tunnistepyyntö

Tunnistuspyynnön tiedot ovat Aktia tunnistuskuvakkeen takana FORM-tietoryhmässä piilomuuttujina.

FORM-TIETORYHMÄ				
Kenttä	Tiedon nimi	Pituus	Pakollisuus	Huomautus
1. Sanomatyyppi	A01Y_ACTION_ID	3 - 4	P	Vakio, "701"
2. Versio	A01Y_VERS	4	P	0003
3. Palveluntuottaja	A01Y_RCVID	10 -15	P	Palvelutunnus
4. Palvelun kieli	A01Y_LANGCODE	2	P	FI = Suomi SV = Ruotsi
5. Kyselyn yksilöinti	A01Y_STAMP	20	P	Vvvvkkpphhmmssxxxxxx
6. Tunnisteen tyyppi	A01Y_IDTYPE	2	P	01 = Salattu perustunnus 02 = Selväkielinen perustunnus 03 = Selväkielinen typistetty tunnus
7. Paluuosoite	A01Y_RETLINK	199	P	OK paluuosoite tunnisteelle
8. Peruuta-osoite	A01Y_CANLINK	199	P	Paluuosoite peruutuksessa
9. Hylätty-osoite	A01Y_REJLINK	199	P	Paluuosoite virhetilanteessa
10. Avainversio	A01Y_KEYVERS	4	P	Avaimen sukupolvitieto
11. Algoritmi	A01Y_ALG	2	P	03 = SHA256
12. Tarkiste	A01Y_MAC	64	P	Kyselyn tarkisteavain

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

```
<FORM METHOD=”POST” ACTION=”https://auth.aktia.fi/tupas”>
<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>
```

5.2 Tunnistuspyynnön kenttien selitykset

1. Sanoman tyyppi, joka on vakio 701.

2. Tunnistuspyyntö-sanoman versionumero 0003 (ISO-8859-1).

3. Palveluntuottajan asiakastunnus. Aktia tunnistuspalvelu tunnistaa palveluntuottajan asiakastunnuksen perusteella ja liittää rekisterissään olevan palveluntuottajan nimen tunnistussanomaan. Tunnus on merkitty pankin kanssa tehtyyn sopimuslomakkeeseen kohtaan ”Palvelutunnus” ja ”Tarkenne”. Tunnus muodostetaan yhtenä merkkijonona ilman välimerkkejä. Esim. palvelutunnus on 1234567890 ja tarkenne on 123, jolloin palveluntuottajan tunnus on 1234567890123.

4. Palvelun kielikoodi kertoo palveluntuottajan asiointisivun kielen ja Aktia tunnistuspalvelu avautuu tällä kielellä, mikäli kyseinen kieli kuuluu Aktia tunnistuksessa kulloinkin käytössä olevaan kielivalikoimaan.

5. Palveluntuottajan tunnistuspyynnölle antama yksilöivä tunnus. Tunnuksena voi olla viite, asiakas-numero tai yhdistelmä päivämäärästä, kellonajasta ja juoksevasta tunnuksesta sekä viitteestä.

6. Tunnisteen tyyppi kertoo, minkä yksilöintitiedon palveluntuottaja tunnistettavasta asiakkaastaan haluaa. Tunnisteen tyypin tulee vastata palvelusopimuksessa sovittua toiminnallisuutta.

i. 01 = Salattu perustunnus. Asiakkaan tunnistetiedon perusteella laskettu heksadesimaalimuotoinen MAC-tarkisteluku. Voi sisältää asiakkaan täydellisen henkilötunnuksen tai Y-tunnuksen.

ii. 02 = Selväkielinen perustunnus. Voi sisältää asiakkaan täydellisen henkilötunnuksen tai Y-tunnuksen.

iii. 03 = Selväkielinen typistetty tunnus. Voi sisältää henkilötunnuksen tarkenneosan ilman vuosisataa ilmoittavaa välimerkkiä tai kokonaisen Y-tunnuksen.

7. Palveluntuottajan palvelusivun osoite, joka on OK-tapauksessa jatkokohta. Paluuosoitteen tulee olla https-alkuinen, eli SSL-suojattu sivu.
   i. Esimerkki: VALUE=https://www.verkkokauppa.fi/tilaus/vahvistus.html

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

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

10. MAC-tarkisteen laskennassa käytetyn avaimen versio.

11. MAC-tarkisteen laskennassa käytettävän algoritmin tyyppikoodi. Aktia tunnisteessa on käytössä 03 = SHA-256 algoritmi, joka tuottaa 64 merkkisen MACin.

12. MAC-tarkiste, joka on laskettu tunnistuspyynnön suojattavista tiedoista ja palveluntuottajan tarkisteavaimesta tietokentässä 11 määritellyllä algoritmilla. Vastaanottaja tarkistaa tarkisteesta tunnistuspyynnön eheyden ja lähettäjän.

5.3 Tunnistuspyynnön MAC-tarkisteen muodostaminen

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

Laskennan aluksi muodostetaan merkkijono FORM-tietoryhmän kaikkien tarkistetta edeltävien tieto-kenttien (kentät 1 - 11) VALUE-arvoista ja palveluntuottajan tarkisteavaimesta. Tiedot yhdistetään merkkijonoksi järjestyksessä niin, että kenttien täytemerkkeinä olevat blankot jätetään pois. Merkkijonon tietoryhmät erotetaan

toisistaan & -merkillä. Viimeisen tiedon (kenttä 12) ja tarkisteavaimen väliin sekä tarkisteavaimen loppuun laitetaan ”&”-merkki. ”&”-merkit otetaan sanoman MAC-tarkisteen laskentaan mukaan. Tieto on yhtenä rivinä. "+" -merkki näyttää tässä dokumentissa olevan rivinvaihdon.

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

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

5.4 Vastaussanoma ja tunniste

Aktia tunnistuspalvelu lisää vastaussanoman 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.

Aktia tunnistuspalvelu laskee vastaussanoman MAC-tarkisteen palveluntuottaja-kohtaisella avaimella. Tarkisteen avulla palveluntuottaja voi varmistua, että tunniste on muodostettu asiakkaan pankissa ja tunnistesanoman tiedot eivät ole muuttuneet.

VASTAUSSANOMA				
Kenttä	Tiedon nimi	Pituus	Pakollisuus	Huomautus
1. Versio	B02K_VERS	4	P	0003
2. Tunnisteen yksilöinti	B02K_TIMESTMP	23	P	NNNvvvvkkppphhmmssxxxxxx
3. Tunnisteen numero	B02K_IDNBR	10	P	Aktia tunnistuspalvelun tunnisteelle antama numero
4. Kyselyn yksilöinti	B02K_STAMP	20	P	Kyselyn tietokenttä 7 (A01Y_STAMP)
5. Asiakas	B02K_CUSTNAME	40	P	Asiakkaan nimi
6. Avainversio	B02K_KEYVERS	4	P	Avaimen sukupolvi
7. Algoritmi	B02K_ALG	2	P	03 = SHA256
8. Tunniste	B02K_CUSTID	40	P	Salattu tarkiste tai selväkielinen palvelutunnus
9. Tunnisteen tyyppi	B02K_CUSTTYPE	2	P	00 = ei tiedossa 01 = selväkielinen henkilötunnus 02 = selväkielinen hetun tarkenne 03 = selväkielinen Y-tunnus 04 = selväkielinen sähköinen asiointitunnus 05 = salattu henkilötunnus 06 = salattu Y-tunnus 07 = salattu sähköinen asiointitunnus
10. Tarkiste	B02K_MAC	AN 64	P	Vastauksen tarkisteavain

5.5 Vastaussanoman kenttien selitykset

1. Vastaussanoman versionumero 0003 (ISO-8859-1).

2. Pankin järjestelmän muodostama aikaleima, jossa NNN on aina 410 ja ilmaisee, että kyseessä on Aktia tunnistuspalvelu.

3. Pankin tietojärjestelmän tunnisteelle antama tieto, joka yksilöi tunnisteen pankin järjestelmässä.

4. Tunnistuspyynnön yksilöintitieto, joka on poimittu kyseisen tunnistepyynnön tietokentästä 7 (A01Y_STAMP)

5. Pankin asiakastietokannassa oleva asiakkaan nimi.

6. MAC-tarkisteavaimen sukupolvitieto.

7. MAC-tarkistealgoritmin tunnus.

8. Asiakkaan tunnistetieto. Selväkielinen tunnus tai salattu tarkiste riippuen tunnistepyynnön A01Y_IDTYPE-kentän sisällöstä.

9. Tunnisteen tyyppi. Tämä kenttä kertoo, mikä kentän 8 tunnistetieto on. Mahdolliset arvot ovat:
   01 = selväkielinen henkilötunnus
   02 = selväkielinen hetun tarkenne
   03 = selväkielinen Y-tunnus
   04 = selväkielinen sähköinen asiointitunnus. Aktia tunnistuspalvelussa ei käytössä.
   05 = suojattu henkilötunnus
   06 = suojattu Y-tunnus
   07 = salattu sähköinen asiointitunnus. Aktia tunnistuspalvelussa ei käytössä.

10. Vastaussanoman tarkiste.

5.6 Vastaussanoman tarkisteen laskenta

Vastaanotetun vastaussanoman eheys tarkistetaan laskemalla siitä aluksi tarkiste, jota verrataan sanoman tarkisteeseen. Tarkiste lasketaan vastaussanoman tietokentistä 1-9. Kentän B02K_CUSTID sisältö määräytyy sen mukaan, mitä tunnusta tunnistepyynnössä on pyydetty ja on siis vaihtoehtoisesti joko salattu tarkiste tai selväkielinen asiakastunnus.

Tarkisteen laskennassa on tärkeää huomioida, että vastaussanoman enkoodaus on ISO-8859-1 (versiossa 0003). Jos vastaussanoman enkoodaus muuttuu palveluntarjoajan käsittelyn aikana, niin tarkisteavain ei välttämättä täsmää. Tiedot ja tarkisteavain erotetaan toisistaan &-merkillä, joka lisätään myös tarkisteavaimen loppuun. Tarkisteen laskennassa käytetään palveluntarjoajakohtaista avainta. "+" -merkki näyttää tässä dokumentissa olevan rivinvaihdon.

B02K_VERS&B02K_TIMESTMP&B02K_IDNBR&B02K_STAMP&+
B02K_CUSTNAME&B02K_KEYVERS&B02K_ALG&+
B02K_CUSTID&B02K_CUSTTYPE&tarkisteavain&

5.7 Tunnisteen tyyppi

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

1. Asiakkaan tunnisteena selväkielinen asiakastunnus

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

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

2. Asiakkaan tunnisteena salattu tarkiste

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

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

B02K_TIMESTMP&B02K_IDNBR&B02K_STAMP&+
asiakastunnus&tarkisteavain&

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

5.8 Sanoman tarkisteen tarkastus ja asiakkaan tunnistus

Palveluntuottaja laskee vastaanottamastaan sanomasta kohdassa 5.6 kuvatulla tavalla vastaanotetun sanoman MAC-tarkisteen. Mikäli se on sama kuin vastaussanomassa pankista tullut vastaussanoman tarkiste, on vastaussanoma välittynyt muuttumattomana.

Jos vastaussanomassa on käytetty salattua tunnusta, tarkistaa palveluntuottaja käytössään olevan asiakkaan tunnuksen oikeellisuuden laskemalla tarkisteen vastaussanoman tietokentistä ja käytössään olevasta tunnuksesta kohdassa 5.7 esitetyllä tavalla. Mikäli saatu tarkiste vastaa vastaussanoman tunnistekentän (B02K_CUSTID) sisältöä, palveluntuottajalla käytössä oleva asiakkaan tunniste on oikea.

6. Poikkeustilanteet

Palveluntuottajan on varauduttava poikkeustilanteisiin, joita voivat olla:

1. Asiakas keskeyttää tunnistustapahtuman. Asiakas voi keskeyttää tapahtuman joko ennen tunnisteen välittämistä Aktia tunnistuspalveluun tai tunnisteen luonnin jälkeen peruuta-painikkeella, jossa osoitteena on tunnistepyynnön FORM-tietokentässä 8 oleva Peruuta-osoite.

2. Asiakkaan todennus epäonnistuu joko asiakkaan antamien tunnistetietojen virheellisyyden takia tai koska asiakas on pyytänyt todennusta väärästä pankista.

3. Aktia tunnistuspalvelu havaitsee virheen tunnistepyyntösanomassa.

4. Palveluntuottaja havaitsee virheen vastaussanomassa, joka voi johtua sanoman sisällössä olevasta virheestä tai siitä, että tunniste ei vastaa asiakkaan ilmoittamia henkilötietoja. Palveluntuottajan tulee antaa asiakkaalle tilannetta vastaava ilmoitus.

5. Vastausta ei tule lainkaan. Katkoksen syynä voi olla yhteyskatko tai muu tekninen häiriö, tai asiakas jättää istunnon kesken.

6. Sama vastaus tulee useita kertoja. Palveluntuottajan on varauduttava, että asiakas voi lähettää saman vastauksen useaan kertaan tai asiakas voi lähettää vanhan vastaussanoma siirtyessään selaimensa ikkunoissa eteen / taakse -näppäimillä ruudusta toiseen.

7. Aktia tunnistuspalvelun 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.

Aktia tunnistuspalvelu ei edellytä mitään tiettyä WWW-palvelinohjelmistoa, mutta sen tulee tukea 256 bittistä SSL-salausta.

7.2 Testaus

Palvelun käyttöönottopäivä sovitaan sopimuksen teon yhteydessä.

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

Verkkopalvelun testiversion osoite: https://auth.aktia.fi/tupastest.

Testiversiossa käytettävät palvelusopimukset

Palvelun-tuottaja (A0IY_RCVID)	Asiakkaan nimi	Tarkisteavain (salainen avain)	Sopimuksen tyyppi (A01Y_IDTYPE)
2222222222222	Testiyritys Oy	12345678901234567890123456789012345678901234567890123456789012345678901234	Salattu perustunnus (01)
3333333333333	Testipalvelu Oy	12345678901234567890123456789012345678901234567890123456789012345678901234	Selväkielinen perustunnus (02)
4444444444444	Testiyhteisö	12345678901234567890123456789012345678901234567890123456789012345678901234	Selväkielinen typistetty tunnus (03)

Avaimen versio on kaikissa 0001.

Testiversiossa käytettävät asiakkaan tunnukset

Asiakkaan tunnus	Asiakkaan nimi	Hetu	Salasana	Turvaluku
12345678	Tero Testi Äyrämö	010170-999R	123456	1234

Esimerkki sanoman kentistä

TUNNISTEPYYNTÖ –TESTISANOMA Form-tietokenttä	
A01Y_ACTION_ID	701
A01Y_VERS	0003
A0IY_RCVID	2222222222222
A01Y_LANGCODE	kts. kuvaus
A01Y_STAMP	kts. kuvaus
A01Y_IDTYPE	kts. kuvaus
A01Y_RETLINK	kts. kuvaus
A01Y_CANLINK	kts. kuvaus
A01Y_REJLINK	kts. kuvaus
A01Y_KEYVERS	0001
A01Y_ALG	03
A01Y_MAC	kts. kuvaus

VASTAUSSANOMA	
B01Y_VERS	0003
B02K_TIMESTMP	kts. kuvaus
B02K_IDNBR	kts. kuvaus
B01Y_STAMP	Kyselyn tietokenttä A01Y_STAMP
B02K_CUSTNAM	Äyrämö Testi Tero
B01Y_KEYVERS	0001
B01Y_ALG	03
B02K_CUSTID	Perustunnus: 010170-999R Typistetty tunnus: 999R Salattu tunnus: Laskettu tunnuksesta 010170-999R
B02K_CUSTTYPE	kts. kuvaus
B01Y_MAC	kts. kuvaus

Tarkisteen laskentaesimerkki

TUNNISTEPYYNTÖ –TESTISANOMA Form-tietokenttä	
A01Y_ACTION_ID	701
A01Y_VERS	0003
A0IY_RCVID	2222222222222
A01Y_LANGCODE	fi
A01Y_STAMP	2342392232323
A01Y_IDTYPE	01
A01Y_RETLINK	https://www.esimerkki.fi/tupasreturn
A01Y_CANLINK	https://www.esimerkki.fi/tupascancel
A01Y_REJLINK	https://www.esimerkki.fi/tupasreject
A01Y_KEYVERS	0001
A01Y_ALG	03
A01Y_MAC	53818C40A8637B4D744DC3E7A7C23FCD0C6F3E6F2F672E B403B3A04284A7E1B8

Tarkiste lasketaan merkkijonosta.

701&0003&2222222222222&fi&2342392232323&01&https://www.esimerkki.fi/tupasreturn&https://www.esimerkki.fi/tupascancel&https://www.esimerkki.fi/tupasreject&0001&03&12345678901234567890123456789012345678901234567890123456789012345678901234&

Mac laskennan ja sen heksadesimaalisen muunnoksen jälkeen tarkiste on:
53818C40A8637B4D744DC3E7A7C23FCD0C6F3E6F2F672EB403B3A04284A7E1B8

8. Neuvonta ja tekninen tuki

Asiakasyhteysneuvonta Aktia Yritysasiakaspalvelussa puh. 010 247 6700 ja sähköposti yritys@aktia.fi. Löydät tarkemmat palveluiden yhteystiedot osoitteesta www.aktia.fi.

Liite

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

æ	%00 %01 %02 %03 %04 %05 %06 %07	0 1 2 3 4 5 6 7	%30 %31 %32 %33 %34 %35 %36 %37	` a b c d e f g	%60 %61 %62 %63 %64 %65 %66 %67	‘ ’ “ ” • – — 	%90 %91 %92 %93 %94 %95 %96 %97	À Á Â Ã Ä Å Æ Ç	%c0 %c1 %c2 %c3 %c4 %c5 %c6 %c7	ð ñ ò ó ô õ ö ÷	%f0 %f1 %f2 %f3 %f4 %f5 %f6 %f7
Backspace Tab Linefeed C return	%08 %09 %0a %0b %0c %0d %0e %0f	8 9 : ; < = > ?	%38 %39 %3a %3b %3c %3d %3e %3f	h i j k l m n o	%68 %69 %6a %6b %6c %6d %6e %6f	˜ ™ š › oe Ÿ	%98 %99 %9a %9b %9c %9d %9e %9f	È É Ê Ë Ì Í Î Ï	%c8 %c9 %ca %cb %cc %cd %ce %cf	ø ù ú û ü ý þ ÿ	%f8 %f9 %fa %fb %fc %fd %fe %ff
	%10 %11 %12 %13 %14 %15 %16 %17	@ A B C D E F G	%40 %41 %42 %43 %44 %45 %46 %47	p q r s t u v w	%70 %71 %72 %73 %74 %75 %76 %77	 ¡ ¢ £ ¥ ¦ §	%a0 %a1 %a2 %a3 %a4 %a5 %a6 %a7	Ð Ñ Ò Ó Ô Õ Ö	%d0 %d1 %d2 %d3 %d4 %d5 %d6 %d7		

	%18
	%19
	%1a
	%1b
	%1c
	%1d
	%1e
	%1f
		H
		I
		J
		K
		L
		M
		N
		O
			%48
			%49
			%4a
			%4b
			%4c
			%4d
			%4e
			%4f
				x
				y
				z
				{
				¦
				}
				~
					%78
					%79
					%7a
					%7b
					%7c
					%7d
					%7e
					%7f
						¨
						©
						ª
						«
						¬
						¯
						®
						¯
							%a8
							%a9
							%aa
							%ab
							%ac
							%ad
							%ae
							%af
								Ø
								Ù
								Ú
								Û
								Ü
								Ý
								Þ
								ß
									%d8
									%d9
									%da
									%db
									%dc
									%dd
									%de
									%df		

Space ! ” # $ % & ’	%20 %21 %22 %23 %24 %25 %26 %27	P Q R S T U V W	%50 %51 %52 %53 %54 %55 %56 %57	€ ‚ ƒ „ … † ‡	%80 %81 %82 %83 %84 %85 %86 %87	° ± ² ³ ´ µ ¶ ·	%b0 %b1 %b2 %b3 %b4 %b5 %b6 %b7	à á â ã ä å æ ç	%e0 %e1 %e2 %e3 %e4 %e5 %e6 %e7		
( ) * + , - . /	%28 %29 %2a %2b %2c %2d %2e %2f	X Y Z [\ ] ^ _	%58 %59 %5a %5b %5c %5d %5e %5f	ˆ ‰ Š ‹ OE Ž 	%88 %89 %8a %8b %8c %8d %8e %8f	¸ ¹ º » ¼ ½ ¾ ¿	%b8 %b9 %ba %bb %bc %bd %be %bf	È É Ê Ë Ì Í Î ï	%e8 %e9 %ea %eb %ec %ed %ee %ef		