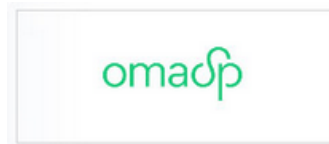


OMA SÄÄSTÖPANKIN VERKKOMAKSU KÄYTTÖOHJE JA TIETUEKUVAUKSET



29.9.2015

versio 1.0

Sisällysluettelo

1 Yleistä	1
2 Palvelusopimus	1
3 Maksamisen nimi ja logo	1
4 Turvallisuus	2
5 Tietuekuvaukset	2
5.1 Maksun versio	3
5.2 Maksun tunnus	3
5.3 Myyjän tunnus	3
5.4 Myyjän tili	3
5.5 Myyjän nimi	3
5.6 Maksun kieli	3
5.7 Maksun määrä	4
5.8 Valuuttalaji	4
5.9 Maksun viite	4
5.10 Maksun eräpäivä	4
5.11 Maksun viesti	4
5.12 Paluu-linkki	4
5.13 Peruuta-linkki	4
5.14 Hylätty-linkki	4
5.15 Maksun tarkiste	4
5.15.1 MD5 -algoritmi	4
5.15.2 SHA256 -algoritmi	5
5.16 Maksun vahvistus	6
5.16.1 MD5 -algoritmi	6
5.16.2 SHA256 -algoritmi	7
5.17 Avaimen versio	7
6 Testaus	7
7 Käyttöönotto	8
8 Oma Säästöpankin verkkomaksun kyselytoiminto	8
8.1 Palvelun kuvaus	8
8.2 Palvelusopimus kyselytoiminnosta	9

8.3 Oma Säästöpankin verkkomaksun tietuekuvaukset.....	9
8.3.1 Myyjän antamat tiedot.....	9
MD5 -algoritmi.....	9
SHA256 -algoritmi	10
8.3.2 Oma Säästöpankin verkkomaksun kyselyn vastaussanomien tiedot	11
MD5 -algoritmi.....	11
SHA256 -algoritmi	11
9 Oma Säästöpankin verkkomaksun palautustoiminto	12
9.1 Palvelusopimus palautustoiminnosta	12
9.2 Oma Säästöpankin verkkomaksun palautuksen tietuekuvaukset.....	12
9.3.1 Myyjän antamat tiedot.....	12
MD5 -algoritmi.....	13
SHA256 -algoritmi	14
MD5 -algoritmi.....	15
SHA256 -algoritmi	15
10 Neuvonta.....	15

1 Yleistä

Tämä ohje määrittelee myyjäyryykselle palvelun käyttöönoton edellytykset sekä tietuekuvaukset järjestelmän rakentamiseen.

Kaupankäynti Internetissä kasvaa koko ajan. Oma Säästöpankin verkkomaksulla asiakkaat voivat ostaa tuotteita Internetin kautta vaivattomasti, nopeasti ja turvallisesti.

Käyttöönotto edellyttää myyjäyryyksen järjestelmältä kykyä muodostaa WWW-tekniikalla ostajalle elektroninen lasku sekä Oma Säästöpankin verkkomaksun vaatimat tiedot.

Myyjä saa tarvittaessa tiedon asiakkaan maksusta heti, kun paluusanomaan liitetään varmennetieto maksun onnistumisesta. Myyjä voi tarkistaa suorituksen myös seuraavalta tiliotteelta tai konekieliseltä tapahtumaluettelolta. Tiliotteet ja konekieliset tapahtumaluettelot muodostetaan asiakkaan sopimuksen mukaisesti.

Oma Säästöpankin verkkomaksun verkko-osoite on
<https://verkkomaksu.omasp.fi/vm/login.html>

Oma Säästöpankin verkkomaksu on käytettävissä 24 h/vrk.

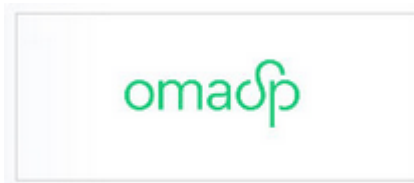
2 Palvelusopimus

Myyjäyryitys tekee kirjallisen sopimuksen palvelun käyttöönotosta Pankin kanssa.

3 Maksamisen nimi ja logo

Pankin verkkomaksamisesta voidaan käyttää joko nimeä Oma Säästöpankin verkkomaksu tai Oma Säästöpankkis nätbetalning. Muita nimityksiä ei saa käyttää.

Oma Säästöpankin verkkomaksun logo on



Myyjäyryitys kopioi logon omalle palvelimellensa Samlinkin palvelimelta osoitteesta
<http://www.omasp.fi/html/OmaSp-painike.png>

Logon kokoa ja värejä ei saa muuttaa.

Logoa/nimeä ei saa luovuttaa tai käyttää muuhun tarkoitukseen kuin Oma Säästöpankin verkkomaksusopimuksessa on sovittu.

Sopimuksen päättymisen jälkeen myyjän on välittömästi poistettava sivuiltaan Oma Säästöpankin verkkomaksun logo.

4 Turvallisuus

Kaikki maksamiseen liittyvä tietoliikenne asiakkaan ja pankin välillä salataan SSL – salausmenettelyllä. Tietoliikenteen salaus suojaa pankin ja asiakkaan väliset sanomat lukemista ja muuttamista vastaan.

5 Tietuekuvaukset

Oma Säästöpankin verkkomaksu, FORM –lomakkeen kentät

	Tieto	Tiedon nimi INPUT NAME=	Esimerkki	Muoto AN=alfanumeerinen A=aakkosellinen N=numeerinen	P=Pakollinen V=Valinnainen
1.	Maksun versio	NET_VERSION	”001” tai ”002” tai ”003”	N 3	P
2.	Maksun tunnus	NET_STAMP		AN 20	P
3.	Myyjän tunnus	NET_SELLER_ID		AN 17	P
4.	Myyjän tili	NET_SELLER_ACC	Ei käytössä		
5.	Myyjän nimi	NET_NAME	Ei käytössä		
6.	Maksun kieli	NET_LANG	Ei käytössä		
7.	Maksun määrä	NET_AMOUNT	”12345,67”	AN 9	P
8.	Valuuttalaji	NET_CUR	EUR	A 3	P
9.	Maksun viite	NET_REF		N 20	P
10.	Maksun eräpäivä	NET_DATE	”EXPRESS”	AN 10	P
11.	Maksun viesti	NET_MSG		AN 210	V
12.	Paluu- linkki	NET_RETURN		AN 160	P
13.	Peruuta- linkki	NET_CANCEL		AN 160	P
14.	Hylätty- linkki	NET_REJECT		AN 160	P
15.	Maksun tarkiste	NET_MAC		AN 64	P
16.	Maksun vahvistus	NET_CONFIRM	YES tai NO	A 3	P
17.	Algoritmi	NET_ALG	03 = SHA256	N 2	P = versiossa ”003”
18.	Avaimen versio	NET_KEYVERS	Ei käytössä		

Uusi kenttä Algoritmi kertoo kumpaa laskentaa käytetään. Algoritmi tiedon puuttuessa, käytetään oletuksena MD5 laskentaa.

Versiossa "001" (NET_VERSION -tieto) hyväksyttiin GET -pyyntö (eli tiedot tulevat URL - parametreina).

Tietoturvasyistä versiosta "002" lähtien on hyväksytty vain POST -pyynnöt (tiedot tulevat FORM - parametreina, ei URLissa).

5.1 Maksun versio

Jatkossa tuetaan kolmea eri versiota

Versio "001"	Versio "002"	Versio "003"
NET_VERSION&	NET_VERSION&	NET_VERSION&
NET_STAMP&	NET_STAMP&	NET_STAMP&
NET_SELLER_ID&	NET_SELLER_ID&	NET_SELLER_ID&
NET_AMOUNT&	NET_AMOUNT&	NET_AMOUNT&
NET_REF&	NET_REF&	NET_REF&
NET_DATE&	NET_DATE&	NET_DATE&
NET_CUR&	NET_CUR&	NET_CUR&
Turvatarckiste&	NET_RETURN&	NET_RETURN&
	NET_CANCEL&	NET_CANCEL&
	NET_REJECT&	NET_REJECT&
	Turvatarckiste&	NET_ALG&
		Turvatarckiste&

5.2 Maksun tunnus

Myyjä antaa maksulle yksilöivän tunnuksen, jonka avulla estetään maksun syntyminen useamman kuin yhden kerran.

5.3 Myyjän tunnus

Tunnuksen perusteella määräytyvät maksulomakkeelle tulevat saajan tilinumero ja saajanimi. 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 myyjän tunnus on 1234567890123.

5.4 Myyjän tili

Ominaisuus ei ole käytössä.

5.5 Myyjän nimi

Ominaisuus ei ole käytössä.

5.6 Maksun kieli

Ominaisuus ei ole käytössä.

5.7 Maksun määrä

Verkkomaksun maksimimäärä määräytyy käyttäjän tilille asettaman maksun ylärajan mukaan. Minimimäärä on 0,01 euroa. Määrä on annettava ilman tuhateroittimia. Desimaalierotin on pakollinen, desimaalierottimena käytetään pilkkua. Maksun määrä esitetään aina kahdella desimaalilla.

5.8 Valuuttalaji

EUR

5.9 Maksun viite

Normaali laskulle merkittävä viite.

5.10 Maksun eräpäivä

Vain HETI –maksut ovat mahdollisia, arvo on EXPRESS.

5.11 Maksun viesti

Mikäli halutaan, voidaan asiakkaan maksulomakkeen viestikenttään liittää mukaan maksua yksilöivää tietoa. Käytössä on 35 merkkiä kuudelle riville.

5.12 Paluu-linkki

Kauppapaikan sivu, jolle palataan onnistuneen maksun teon jälkeen.

Kauppapaikalta lähetettävä paluulinkki voi olla esimerkiksi muodossa *http://ostos.kauppa.fi/cgi-bin/valmis?suoritettu* jolloin pankista kauppapaikalle siirryttäessä paluulinkki on muotoa *http://ostos.kauppa.fi/cgi-bin/valmis&suoritettu&001&01234567890123456789&123&20000101457898I11234&laskettu_mac* mikäli NET_CONFIRM –tietokentän arvo on YES.

5.13 Peruuta-linkki

Kauppapaikan sivu, jolle siirrytään siinä tapauksessa, että asiakas keskeyttää maksutoiminnon Oma Säästöpankin verkkomaksussa.

5.14 Hylätty-linkki

Kauppapaikan sivu, jolle siirrytään mikäli maksu hylkääntyy Oma Säästöpankin verkkomaksussa.

5.15 Maksun tarkiste

5.15.1 MD5 -algoritmi

Maksun tarkiste lasketaan MD5 –algoritmilla siten, että ensin muodostetaan merkkijono seuraavista tietokentistä tässä järjestyksessä:

NET_VERSION&

```
NET_STAMP&  
NET_SELLER_ID&  
NET_AMOUNT&  
NET_REF&  
NET_DATE&  
NET_CUR&  
Turvatarkiste&
```

Versiossa ”002” maksun tarkiste lasketaan MD5 –algoritmillä siten, että ensin muodostetaan merkkijono seuraavista tietokentistä tässä järjestyksessä:

```
NET_VERSION&  
NET_STAMP&  
NET_SELLER_ID&  
NET_AMOUNT&  
NET_REF&  
NET_DATE&  
NET_CUR&  
NET_RETURN&  
NET_CANCEL&  
NET_REJECT&  
Turvatarkiste&
```

Turvatarkiste on kaksiosainen. Tarkisteen ensimmäinen osa postitetaan asiakkaan sopi-muksella nimeämälle avaimen ensimmäisen osan saajalle asiakkaan sopimuksella olevaan osoitteeseen. Toinen osa toimitetaan sähköpostilla avaimen toisen osan saajan sähköpostiosoitteeseen. Turvatarkiste on 16-20 merkkiä pitkä ja sitä käytetään vain maksun tarkisteen laskennassa.

Merkkijonossa ei saa olla tyhjiä merkkejä ja & -merkit ovat mukana laskennassa. Esimerkiksi merkkijonosta *001&01234567890123456789&0000000000&1234,56&123&EXPRESS&EUR&11111111111111111111&* saadaan laskennan tulokseksi *09934B1A4BD21AD47C38ECAF99C9BE24*.

5.15.2 SHA256 -algoritmi

Maksun tarkiste lasketaan SHA256 –algoritmillä siten, että ensin muodostetaan merkkijono seuraavista tietokentistä tässä järjestyksessä:

```
NET_VERSION&  
NET_STAMP&  
NET_SELLER_ID&  
NET_AMOUNT&  
NET_REF&  
NET_DATE&  
NET_CUR&  
NET_RETURN&  
NET_CANCEL&  
NET_REJECT&  
NET_ALG&  
Turvatarkiste&
```


Mikäli asiakas peruuttaa maksun suorittamisen, linkkitieto välitetään NET_CANCEL – tietokentän mukaisena ja jos maksu hylkääntyy, NET_REJECT –tietokentän mukaisena.

Myyjän tunnukset:

- palvelutunnus = 0000000000
- turvatarkiste = 11111111111111111111
- testitili = 448710-126

Testimyyjälle voi maksaa ainoastaan testiostaja eikä maksua suoriteta. Testiostajan tilit ovat 401910-111012 ja 401910-111004. Testikäyttäjälle näytetään virheelliset kentät sellaisenaan, tuotannossa tapahtuvia virhetilanteita varten on omat sivunsa.

7 Käyttöönotto

Palvelu on käytettävissä sopimukseen merkittynä käyttöönottopäivänä.

8 Oma Säästöpankin verkkomaksun kyselytoiminto

Oma Säästöpankin verkkomaksun kysely on järjestelmä niille yritysasiakkaille, jotka käyttävät Oma Säästöpankin verkkomaksunappia omilla verkkokauppasivuillaan. Palvelun avulla yritykset voivat tehdä kyselyjä Oma Säästöpankin verkkomaksunapilla tehdyistä tapahtumilta. Järjestelmän päätarkoituksena on tehdä verkkokaupoille kyselymahdollisuus niistä tapahtumista, jotka ovat maksatuksen yhteydessä jostain syystä epäonnistuneet eli tieto maksatuksen onnistumisesta tai epäonnistumisesta ei tavoita yrityksen verkkokauppajärjestelmää. Palvelun avulla verkkokaupparyitykset voivat varmistua epävarmoista maksatustiedoista välittömästi. Näin verkkokauppa voi onnistuneen maksun myötä myös tarjota verkkokaupassa asioivalle asiakkaalle välittömästi sen palvelun tai tuotteen, jonka asiakas oli verkkokaupassa maksanut ja joka oli myös tarkoitus toimittaa asiakkaalle välittömästi onnistuneen maksatuksen jälkeen.

8.1 Palvelun kuvaus

Asiakas siirtyy takaisin verkkokaupan sivulle onnistuneen maksun kuittaussivulta tai Oma Säästöpankin verkkomaksujärjestelmä siirtää asiakkaan automaattisesti verkkokaupan sivulle. Siirtymisen mukana menee verkkokaupalle tietoa maksun onnistumisesta ja verkkokauppa voi antaa asiakkaalle tuotteen/palvelun välittömästi. Jos siirtymistä ei tapahdu (asiakas toimii toisin kuin pitäisi, järjestelmässä tapahtuu virhe tai tietoliikenteessä tapahtuu virhe), maksun onnistumistietoa ei välity verkkokaupalle.

Verkkokauppaan on yritys itse rakentanut tapahtuman kyselyn, joka käynnistyy automaattisesti tai kysely tehdään manuaalisesti, kun tapahtumaa ei kuulu takaisin verkkokauppaan. Kysely tehdään niin, että verkkokaupan tunnukset toimivat tunnistimina Samlinkiin päin (aivan kuten verkkokaupasta siirtyminen Oma Säästöpankin -maksatukseen). Verkkokauppa antaa tarvittavat yksilöivät tiedot maksusta, jonka perusteella maksu voidaan luotettavasti löytää ja lähettää takaisin verkkokaupalle.

8.2 Palvelusopimus kyselytoiminnosta

Myyjäyrittys tekee kirjallisen sopimuksen palvelun käyttöönotosta Pankin kanssa.

8.3 Oma Säästöpankin verkkomaksun tietuekuvaukset

Myyjäyrittys rakentaa oman kyselyjärjestelmän. Oma Säästöpankin verkkomaksun kyselytoiminnon verkko-osoite on <https://verkkomaksu.omasp.fi/vm/kysely.html>. Oma Säästöpankin verkkomaksu on käytettävissä 24 h/vrk.

8.3.1 Myyjän antamat tiedot

	Tieto	Tiedon nimi INPUT NAME=	Esimerkki	Muoto	P/V	
1.	Maksun versio	NET_VERSION	"001" tai "003"	N 3	P	
2.	Myyjän tunnus	NET_SELLER_ID		AN 17	P	
3.	Maksun tunnus	NET_STAMP	Kauppiaan antama alkuperäisen maksun tunnus	AN 20	V	P
4.	Kyseltävän maksun yksilöivä viite	NET_REF	Standardiviite	N 20	V	
5.	Paluuosoite	NET_RETURN	Paluulinkin osoite	AN199	P	
6.	Algoritmi	NET_ALG	03 = SHA256	N 2	P = versiossa "003"	
7.	Maksun tarkiste	NET_MAC		AN64	P	
8.	Avaimen versio	NET_KEYVERS	Ei käytössä			

Joko maksun tunnus tai viite on annettava. Jos molemmat annetaan, niin molempien on täsmättävä.

MD5 -algoritmi

Maksun tarkiste lasketaan MD5 –algoritmilla siten, että ensin muodostetaan merkkijono seuraavista tietokentistä tässä järjestyksessä:

```
NET_VERSION&
NET_SELLER_ID&
NET_STAMP&
NET_REF&
Turvatarkiste&
```

Turvatarkiste on kaksiosainen. Tarkisteen ensimmäinen osa postitetaan asiakkaan sopimuksella nimeämälle avaimen ensimmäisen osan saajalle asiakkaan sopimuksella olevaan osoitteeseen. Toinen osa toimitetaan sähköpostilla avaimen toisen osan saajan sähköpostiosoitteeseen. Valinnaiset kentät otetaan mukaan vain, jos ne ovat läsnä. Merkkijonossa ei saa olla tyhjiä merkkejä ja & -merkit ovat mukana laskennassa. Saadusta merkkijonosta lasketaan MD5-algoritmilla hash-arvo, joka muutetaan heksadesimaaliseen, 32-merkkiä pitkään esitysmuotoon, jossa käytetään isoja kirjaimia.

Merkkijonossa ei saa olla tyhjiä merkkejä ja & -merkit ovat mukana laskennassa. Esimerkiksi merkkijonosta

8.3.2 Oma Säästöpankin verkkomaksun kyselyn vastaussanomien tiedot

	Tieto	Tiedon nimi INPUT NAME=	Esimerkki	Muoto	P/V
1.	Kyselyn versio	NET_VERSION	"001" tai "003"	N 3	P
2.	Myyjän tunnus	NET_SELLER_ID		AN 17	P
3.	Paluutieto	NET_RESPCODE	"OK": Maksu löytyi ja se on hyväksytty "NOTFOUND": Maksua ei löytynyt "ERROR": Maksussa epäselvää tai virhe kyselytiedoissa tai muu virhe	A 8	P
4.	Maksun tunnus	NET_STAMP		AN 20	V P
5.	Maksun viite	NET_REF		N 20	
6.	Maksupäivä	NET_DATE	"vvvvkkpp"-muodossa	N 10	V
7.	Maksun määrä	NET_AMOUNT	"12345,67"	AN 9	V
8.	Valuuttalaji	NET_CUR	EUR	A 3	V
9.	Maksun arkistointitunnus	NET_PAID	Pankin arkistointitunnus	AN 20	V
10.	Algoritmi	NET_ALG	03 = SHA256	N 2	P = versiossa "003"
11.	Kyselyn tarkiste	NET_RETURN_MAC		AN 64	P
12.	Avaimen versio	NET_KEYVERS	Ei käytössä		V

MD5 -algoritmi

Kyselyvastauksen tarkiste lasketaan MD5 –algoritmilla siten, että ensin muodostetaan merkkijono seuraavista tietokentistä tässä järjestyksessä:

```
NET_VERSION&
NET_SELLER_ID&
NET_RESPCODE&
NET_STAMP&
NET_REF&
NET_DATE&
NET_AMOUNT&
NET_CUR&
NET_PAID&
Turvatarkiste&
```

Saadusta merkkijonosta lasketaan MD5-algoritmilla hash-arvo, joka muutetaan heksadesimaaliseen, 32-merkkiä pitkään esitysmuotoon, jossa käytetään isoja kirjaimia. Valinnaiset kentät otetaan mukaan vain, jos ne ovat läsnä.

Esimerkiksi merkkijonosta

```
001&0000022222000&NOTFOUND&4J5Y1OBYdPSx34567890&
11111111111111111111111111111111& saadaan laskennan tulokseksi
5846A67B2145D01BD70396009AA962E1
```

SHA256 -algoritmi

Kyselyvastauksen tarkiste lasketaan SHA256 –algoritmilla siten, että ensin muodostetaan merkkijono seuraavista tietokentistä tässä järjestyksessä:

```
NET_VERSION&
NET_SELLER_ID&
NET_RESPCODE&
NET_STAMP&
```


	Tieto	Tiedon nimi INPUT NAME=	Esimerkki	Muoto	P/V
1.	Palautuksen versio	NET_VERSION	”001” tai ”003”	N3	P
2.	Myyjän tunnus	NET_SELLER_ID		AN13	P
3.	Palautusmaksun tunnus	NET_STAMP		AN20	P
4.	Palautusmaksun viite	NET_REF		N20	P
5.	Palautusmaksun määrä	NET_AMOUNT	”12345,67”	AN9	P
6.	Valuuttalaji	NET_CUR	”EUR”	A3	P
7.	Palautusmaksun viesti	NET_MSG		AN210	V
8.	Alkuperäisen maksun tunnus	NET_STAMP_ORG		N20	P
9.	Alkuperäisen maksun viite	NET_REF_ORG		N20	P
10.	Paluulinkin osoite	NET_RETURN		AN160	P
11.	Algoritmi	NET_ALG	03 = SHA256	N 2	P = versiossa ”003”
12.	Maksun tarkiste	NET_MAC		AN64	P
13.	Avaimen versio	NET_KEYVERS	Ei käytössä		

MD5 -algoritmi

Tarkiste lasketaan MD5- algoritmilla siten, että ensin muodostetaan merkkijono laskennassa mukana olevista tietokentistä seuraavassa järjestyksessä:

```
NET_VERSION&
NET_SELLER_ID&
NET_STAMP&
NET_REF&
NET_AMOUNT&
NET_CUR&
NET_STAMP_ORG&
NET_REF_ORG&
NET_RETURN&
Turvatarkiste&
```

Turvatarkiste on 16-20 merkkiä pitkä. Merkkijonossa ei saa olla tyhjiä merkkejä ja & -merkit ovat mukana laskennassa. Saadusta merkkijonosta lasketaan MD5 –algoritmilla hash –arvo, joka muutetaan heksadesimaaliseen, 32 –merkkiä pitkään esitysmuotoon, jossa käytetään isoja kirjaimia. Esimerkiksi merkkijonosta

```
”001&0000022222000&4J5YIOBYDPSX34567890&123&25,50&EUR&4J5YIOBYDPSX34567801
&12344&http://www.kauppapaikkax.fi &11111111111111111111&”
```

saadaan laskennan tulokseksi "92D8EFC7DC2349248366AAF6FCF8EA56".

Avaimen versio	NET_KEYVERS	Ei käytössä		
----------------	-------------	-------------	--	--

Palautuksen vastaussanomien MAC –tarkisteen laskennassa käytettävät tietokentät

MD5 -algoritmi

NET_VERSION&
NET_SELLER_ID&
NET_STAMP&
NET_REF&
NET_PAID&
Turvatarkiste&

SHA256 -algoritmi

NET_VERSION&
NET_SELLER_ID&
NET_STAMP&
NET_REF&
NET_PAID&
NET_ALG&
Turvatarkiste&

10 Neuvonta

Asiakasyhteysneuvonta: 0100-4052 (1,1689 €/min + pvm).

Sähköposti: info@samlink.fi