

POP PANKIN VERKKOMAKSU
KÄYTTÖOHJE JA TIETUEKUVAUKSET



1.9.2014

versio 1.2

Sisällysluettelo

1 Yleistä	1
2 Palvelusopimus	1
3 Maksamisen nimi ja logo	1
4 Turvallisuus	1
5 Tietuekuvaukset	2
5.1 Maksun versio	2
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	3
5.8 Valuuttalaji	3
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	6
5.17 Avaimen versio	7
6 Testaus	7
7 Käyttöönotto	8
8 POP Pankin verkkomaksun kyselytoiminto	8
8.1 Palvelun kuvaus	8
8.2 Palvelusopimus kyselytoiminnosta	8

8.3 POP Pankin verkkomaksun tietuekuvaukset	8
8.3.1 Myyjän antamat tiedot	9
MD5 -algoritmi	9
SHA256 -algoritmi	9
8.3.2 POP Pankin verkkomaksun kyselyn vastaussanomien tiedot	11
MD5 -algoritmi	11
SHA256 -algoritmi	11
9 POP Pankin verkkomaksun palautustoiminto	12
9.1 Palvelusopimus palautustoiminnosta	12
9.2 POP Pankin 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. POP Pankin verkkomaksulla asiakkaat voivat ostaa tuotteita Internetin kautta vaivattomasti, nopeasti ja turvallisesti.

Käyttöönotto edellyttää myyjäyryyksen järjestelmältä kykyä muodostaa WWW-tekniikalla ostajalle elektroninen lasku sekä POP Pankin 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.

POP Pankin verkkomaksun verkko-osoite on
<https://verkkomaksu.poppankki.fi/vm/login.html>

POP Pankin 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 POP Pankin verkkomaksu tai POP Bankens nätbetalning. Muita nimityksiä ei saa käyttää.

Myyjäyryitys kopioi logon omalle palvelimellensa Samlinkin palvelimelta osoitteesta <http://193.65.156.50/POPmaksunappi.png>

Logon kokoa ja värejä ei saa muuttaa.

Logoa/nimeä ei saa luovuttaa tai käyttää muuhun tarkoitukseen kuin POP Pankin verkkomaksu- sopimuksessa on sovittu.

Sopimuksen päättymisen jälkeen myyjän on välittömästi poistettava sivuiltaan POP Pankin verkkomaksun logo/nimi.

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

POP Pankin 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&
Turvatakiste&	NET_RETURN&	NET_RETURN&
	NET_CANCEL&	NET_CANCEL&
	NET_REJECT&	NET_REJECT&
	Turvatakiste&	NET_ALG&
		Turvatakiste&

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 POP Pankin verkkomaksussa.

5.14 Hylätty-linkki

Kauppapaikan sivu, jolle siirrytään mikäli maksu hylkääntyy POP Pankin 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 –algoritmilla siten, että ensin muodostetaan merkkijono seuraavista tietokentistä tässä järjestyksessä:

```
NET_VERSION&
```


saadaan laskennan tulokseksi

6D6E351D42D2E8C8FFFF6C05B426FAC8FBE31D0177A386D9FA5ECD88EFAAC7C1

5.16 Maksun vahvistus

Mikäli NET_CONFIRM kentän arvo on ”YES”, saa myyjä paluulinkissä tiedon maksun käsittelystä. Paluulinkin muodostuksessa käytetään MAC –tarkistetta, jonka avulla myyjä voi varmistua onnistuneesti suoritetusta POP Pankin verkkomaksusta. Täydellisen varmuuden onnistuneesti tehdystä maksusta myyjä saa kuitenkin vasta tiliote- tai viitesiirtoaineistostaan. Myyjä voi tehdä myös erillisen tilitapahtumakyselyn.

Arvon ollessa ”YES”, liitetään paluulinkin loppuun seuraavat tiedot:

5.16.1 MD5 -algoritmi

NET_RETURN_VERSION	”001”
NET_RETURN_STAMP	Maksun yksilöivä tunnus
NET_RETURN_REF	Maksun alkuperäinen viitenumero
NET_RETURN_PAID	Tapahtuman yksilöivä tunniste pankin järjestelmässä
NET_RETURN_MAC	Paluutietojen tarkiste

NET_RETURN_PAID on uusi AN muotoinen tieto jonka enimmäispituus 20 merkkiä.

NET_RETURN_MAC lasketaan kuten kohdassa 5.15.1 kuvattu hash –arvo:

```
NET_RETURN_VERSION&
NET_RETURN_STAMP&
NET_RETURN_REF&
NET_RETURN_PAID&
Turvatarkiste&
```

MD5 –algoritmillä lasketaan muodostettavasta merkkijonosta hash –arvo, joka muutetaan heksadesimaaliseen 32 merkkiä pitkään esitysmuotoon.

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

001&01234567890123456789&123&2000010145789811234&11111111111111111111&
saadaan laskennan tulokseksi 0A17E03DE34E35C965E96225E59438EA.

5.16.2 SHA256 -algoritmi

NET_RETURN_VERSION	”003”
NET_RETURN_STAMP	Maksun yksilöivä tunnus
NET_RETURN_REF	Maksun alkuperäinen viitenumero
NET_RETURN_PAID	Tapahtuman yksilöivä

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 POP Pankin verkkomaksun kyselytoiminto

POP Pankin verkkomaksun kysely on järjestelmä niille yritysasiakkaille, jotka käyttävät POP Pankin verkkomaksunappia omilla verkkokauppasivuillaan. Palvelun avulla yritykset voivat tehdä kyselyjä POP Pankin 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 POP Pankin 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 välitys 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 POP Pankin -maksatukseen). Verkkokauppa antaa tarvittavat yksilöivät tiedot maksusta, jonka perusteella maksu voidaan luotettavasti löytää ja lähettää takaisin verkkokaupalle.

8.2 Palvelusopimus kyselytoiminnosta

Myyjäyritys tekee kirjallisen sopimuksen palvelun käyttöönotosta Pankin kanssa.

8.3 POP Pankin verkkomaksun tietuekuvaukset

Myyjäyritys rakentaa oman kyselyjärjestelmän. POP Pankin verkkomaksun kyselytoiminnon verkko-osoite on <https://verkkomaksu.poppankki.fi/vm/kysely.html>. POP Pankin 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 –algoritilla 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-algoritilla 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

```
001&01234567890123456789&123&2000010145789811234&11111111111111111111&
saadaan laskennan tulokseksi 0A17E03DE34E35C965E96225E59438EA.
```

SHA256 -algoritmi

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

```
NET_VERSION&
NET_SELLER_ID&
NET_STAMP&
NET_REF&
NET_ALG&
```


	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&4J5Y1OBYDPSX34567890&123&25,50&EUR&4J5Y1OBYDPSX34567801
&12344&http://www.kauppapaikkax.fi &11111111111111111111&”
```

saadaan laskennan tulokseksi "92D8EFC7DC2349248366AAF6FCF8EA56".

SHA256 -algoritmi

Tarkiste lasketaan SHA256- algoritmillä 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&
 NET_ALG&
 Turvatarkiste&

Turvatarkiste on 64 merkkiä pitkä. Merkkijonossa ei saa olla tyhjiä merkkejä ja & -merkit ovat mukana laskennassa. Saadusta merkkijonosta lasketaan SHA256 –algoritmillä hash –arvo, joka muutetaan heksadesimaaliseen, 64 –merkkiä pitkään esitysmuotoon, jossa käytetään isoja kirjaimia. Esimerkiksi merkkijonosta ”

003&0000010014001&12312312&12344&1,20&EUR&12312312&12344&http://auto/kauppa/palautus?ACTION=paluu&03&111&” saadaan laskennan tulokseksi
 "6466FB6144718D253A8998C5BBCDA28A1B3360FF9A04AEE34DCEDAE7D980D451".

9.3.2 POP Pankin verkkomaksun palautuksen vastaussanomien tiedot

Tieto	Tiedon nimi INPUT NAME=	Esimerkki	Muoto	P/V
Palautuksen versionumero.	NET_VERSION	”001” tai ”003”	N3	P
Myyjän tunnus.	NET_SELLER_ID		AN13	P
Palautuksen yksilöivä tunnus.	NET_STAMP		AN20	P
Palautuksen yksilöivä viite.	NET_REF		N20	P
Vastauskoodi	NET_RESPCODE	”OK”: palautus onnistui ”NOTFOUND”: alkuperäistä maksua ei löytynyt ”ERROR”: palautus ei onnistunut	A8	P
Palautuksen arkistointitunnus	NET_PAID		AN20	P
Virheselitys	NET_ERRO_MSG	Virheen lisäselitys jos vastauskoodi on ”ERROR”.	A512	V
Algoritmi	NET_ALG	03 = SHA256	N 2	P = versiossa ”003”
Maksun tarkiste	NET_MAC		AN64	P

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