# VERKKOPANKKILINKKI

## Turvallinen linkki verkkopankista pankin ulkopuoliseen palveluun

## Palvelun kuvaus ja palveluntarjoajan ohje

## v1.3 26.5.2008

FK|Finanssialan Keskusliitto
FC|Finansbranschens Centralförbund
Federation of Finnish Financial Services

**Sisällysluettelo**

# 1 Verkkopankkilinkin kuvaus

Verkkopankkilinkki tarjoaa yrityksille mahdollisuuden vähentää paperilla toimitettavien dokumenttien tulostusta ja jakelua, kun ne liittyvät pankin kautta välitettyihin maksuliiketapahtumiin tai kuluttajan e-laskuun.

Verkkopankkilinkki on pankkien yhteisesti standardoima. Palvelun tarjoaja sopii linkin käyttöönotosta kaikkien niiden pankkien kanssa, joiden verkkopankkia käyttäville asiakkaille linkki halutaan tarjota.

## 1.1 Yleiskuvaus

Verkkopankkilinkki muodostetaan verkkopankissa olevasta tapahtumasta, johon näin voidaan antaa lisätietoja tai tarkempi erittely pankin ulkopuolisessa palvelussa.

Linkki yhdistää verkkopankkia käyttävän asiakkaan palvelun tarjoajan esilläpitopalveluun internetissä. Linkki sisältää tiedot, joiden avulla palvelun tarjoaja voi kohdistaa linkin oikeaan tapahtumaan.

Tietoliikenne on salattua ja välitettävien tietojen eheys turvattu tarkisteella.

## 1.2 Soveltaminen

Verkkopankkilinkki soveltuu käytettäväksi esim. suoraveloitus-, suoralasku-, toistuvaissuoritus- tai kuluttajan e-laskupalvelun yhteydessä.

Suoraveloituspalvelussa linkin avulla voidaan korvata maksajalle toimitettava ennakkoilmoitus. Kun suoraveloitettavan maksun summa vaihtelee, asiakas tarkistaa maksun perusteena olevan laskun tiedot linkin avulla. Laskuttaja voi automatisoida suoraveloitettavien maksujen peruutusten käsittelyä, jos esilläpitopalvelussa on mahdollisuus antaa laskuun liittyvää palautetta.

Suoralaskussa linkkiä voidaan käyttää suoraveloituksen tapaan korvaamaan paperilasku.

Toistuvaissuorituksena maksettuun palkkapanoon liittyvä palkkalaskelma voidaan esittää verkossa. Palkkalaskelmien selauspalveluun voidaan rakentaa toimintoja, joilla helpotetaan palkanlaskentaa ja mahdollisia palkanlaskentaan liittyviä oikaisuja.

Kuluttajan e-laskun liite voi sisältää esimerkiksi laskuerittelyn.

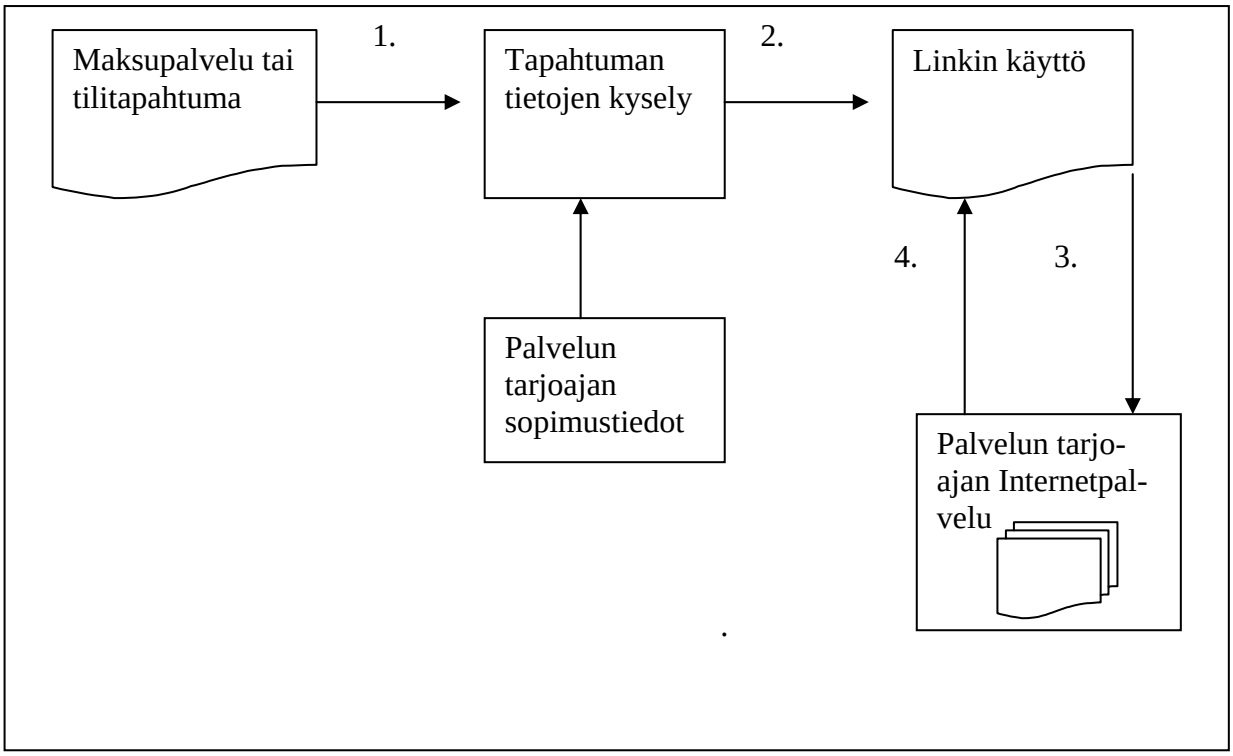
## 1.3 Turvallisuus

Verkkopankin ja esilläpitopalvelun välisessä tietoliikenteessä käytetään SSL-salausprotokollaa, joten ulkopuoliset eivät näe tietoja eivätkä voi muuttaa niitä. Linkin kohteena olevien palvelun tarjoajan tietojen tulee myös olla SSL-suojattuja.

Pankki tunnistaa verkkopankkiasiakkaansa. Verkkopankkilinkissä pankin tarjoajalle tulevat tiedot perustuvat pankin maksutapahtuman ja verkkopankkiasiakkaan tietoihin. Linkin tie-

dot on lisäksi suojattu tiedon eheyden turvaavalla tarkisteella, joten linkkiä käyttävä verkkopankin asiakas ei voi muuttaa tietoja palvelun tarjoajan sitä havaitsematta.

## 2 Verkkopankkilinkin toiminnallinen kuvaus




1 Verkkopankin asiakas kirjoittautuu verkkopankkiinsa ja valitsee maksuluettelosta tai tilitapahtumista maksun tai e-laskun.
2 Maksussa tai laskussa voi olla verkkopankkilinkki.
3 Linkin käyttö yhdistää verkkopankin asiakkaan palvelun tarjoajan Internetpalveluun ja siellä maksusta esitettyihin tietoihin, jotka voidaan esittää esim. erillisenä selainikkunana.
4 Verkkopankin asiakas selaa ja tarkistaa maksun perusteen (esim. laskun) ja voi käyttää myös muita palvelun tarjoajan toimintoja, esim. paperilaskun peruutusta.
Kun verkkopankin asiakas lopettaa palvelun tarjoajan Internetpalvelun käytön (esim. sulkemalla selainikkunan), hän palautuu verkkopankkiin ja voi hyväksyä maksamisen. Jos verkkopankin timeout -aika on täyttynyt verkkopankin asiakkaan asioidessa palvelun tarjoajan verkkosivuilla, täytyy asiakkaan kirjoittautua uudelleen verkkopankkiinsa.

## 3 Verkkopankkilinkin käyttöönotto

Palvelun tarjoaja sopii verkkopankkilinkin käyttöönotosta kunkin pankin kanssa erikseen. Palvelun käyttöönottopäivä sovitaan sopimuksen teon yhteydessä. Palveluntarjoajan tiedot rekisteröidään kussakin pankissa ja palveluntarjoaja ilmoittaan kullekin pankille erikseen, kun hänen sopimustietoihinsa tulee muutoksia.

Pankki toimittaa palveluntarjoajalle sopimuksen teon jälkeen palvelussa käytettävän tunnuksen ja tarkisteavaimen. Tiedot toimitetaan palveluntarjoajalle pankkikohtaisella menettelyllä joko sähköisessä muodossa tai paperitulosteena. Toimitettavat tiedot on suojattu kuljetuksen aikana siten, että vastaanottaja voi havaita, jos toimituksen suojakuori on avattu kuljetuksen aikana.

Testausmenettelyt ovat pankkikohtaisia ja niistä löytyy lisää tietoa pankkien omista palvelukuvauksista.

## 4 Verkkopankkilinkin parametrit

Merkkijono muodostuu parametrikenttien sisällöistä ja &-merkeistä kenttien välissä. Kentän nimi yhdistetään arvoon = merkillä. Merkkijonon loppuun liitetään salainen avaintieto ja &-merkki. Merkkijonot eivät sisällä tyhjä-merkkejä.

| **Kentän nimi** | **Arvo** | **Pituus** | **Kuvaus** |
|---|---|---|---|
| | https://<br>www.yritys.fi<br>aaaa/bbbbbb/ccccccc<br>? | | - protokolla, SSL-salaus<br>- palvelimen nimi<br>- esilläpitopalvelun nimi ko. palvelimella |
| **VERSION** | 0001 | 4 merkkiä | Linkin versionumero, käytössä olevat arvot pankkien omissa kuvauksissa |
| **PMTREFNB** | | | Linkin kohteena olevan tapahtuman yksilöintitieto<br>- suoralaskussa maksun viitenumero<br>- palkkapanossa palkansaajan henkilötunnus (123456-789X) ja palkan maksupäivä<br>-kuluttajan e-laskussa<br>o pituus max. 60 merkkiä<br>o laskuun liittyvän lisätiedon arkistointitunnus (esimerkiksi laskun viite, laskuttaja syöttää tiedon Finvoice verkkolaskulle kenttään InvoiceUrlText)<br>PMTREFNB voidaan myös salata ks. kohta 4.2, mutta Kuluttajan e-laskussa ei salata |

| | | | |
|---|---|---|---|
| **RCVID** | | enintään 20 merkkiä | Laskuttajan tai palkanmaksajan tunnus pankissa<br>Kuluttajan e-laskussa ei käytössä |
| **TIMESTMP** | VVVV-KK-PP-HHMMSS+HH<br>tai<br>VVVV-KK-PP-HHMMSS%2BHH | 22 tai 24 merkkiä | Linkin muodostushetki, aikavyöhykkeen esitysmuoto voi olla pankista riippuen joko +HH tai %2BHH,<br>+02 = %2B02 = normaali aika Suomessa<br>+03 = %2B03 = kesäaika Suomessa |
| **KEYVERS** | | 4 merkkiä | MAC-Avaimen versio.<br>Linkin MAC tarkisteen laskentaan käytetään salattua PMTREFNB kenttää |
| **ALG** | 0001= MD5<br>0002= SHA-1 | 4 merkkiä | MAC-avaimen laskenta-algoritmi, joko MD5 tai SHA-1 |
| **LANGCODE** | 1= suomi,<br>2= ruotsi,<br>3= englanti | 1 merkki | Asiakkaan kielikoodi verkkopankissa |
| **SESSIONID** | | enintään 20 merkkiä | Lokitieto |
| **SENDID** | | enintään 20 merkkiä | Linkin muodostajan tunnus.<br>Kuluttajan e-laskun sisältämässä pankin muodostamassa linkissä SENDID -kentässä on linkin muodostaneen pankin BIC. OP:n tunnus on "OSUUSPANKKI" kaikissa verkkopankkilinkeissä<br>Käytössä olevat muut arvot pankkien omissa kuvauksissa. |
| *Valinnaiset tiedot:* | | | |
| **STATUS** | Prod = tuotantolinkki<br>Test = testilinkki | 4 merkkiä | Linkin tila |
| **PMTORIG** | 1 = Suoralasku, suoraveloitus tai kuluttajan e-lasku<br>2 = Toistuvaissuoritus | 1 merkki | Maksun syöttötapa |
| **USERMAC** | | 32 merkkiä | Maksajan henkilötunnuksesta muodostettu tarkiste.<br>Katso lisäselvitystä 4.3 |

| | | | |
|---|---|---|---|
| **MAC** | | | Linkin MAC-tarkiste<br>Kaikista käytössä olevista parametreista laskettu tarkiste. Linkin muodostava palvelin laskee parametritiedoista kentän MAC. Tarkenne sijoitetaan näkyvässä muodossa ascii-merkkeinä parametrikentän MAC arvoksi. |

### 4.1 Lisäselvitys TIMESTMP-parametrin käytöstä

Vastaanottavan palvelun on tarkistettava, että timestampia on käytetty tietyssä aikaikkunassa. Lisäksi linkki voidaan käyttää vain kerran. Tarkistus tehdään vertaamalla TIMESTMP- ja PMTREFNB- parametrien arvoja.

### 4.2 Lisäselvitys PMTREFNB-kentän salauksesta

Algoritmi sovitaan pankin kanssa. Vaihtoehtoina DES ja AES.

DESiä käytettäessä, käytetään 8 merkin (56 bittiä) salausavainta ja EBC moodia.

AESia käytettäessä, käytetään ECB-menetelmää. Merkkikoodisto on ISO 8859-1 (latin-1). Avaimen pituus on 256 bittiä. Salattu lohko on 32 merkkiä pitkä. Lohkon alussa (vasemmassa reunassa) on henkilötunnus 123456-789X), jonka jälkeen on palkan maksupäivä (00000000). Loppuosa lohkosta on täytetty tyhjämerkeillä. Salauksen tulos muutetaan heksadesimaaliseen esitysmuotoon, jossa A-F esitetään isoilla kirjaimilla.

Linkin MAC tarkisteen laskentaan käytetään salattua PMTREFNB kenttää.

### 4.3 Lisäselvitys USERMAC-parametrin käytöstä

Joissain tilanteissa saattaa esilläpitopalvelussa olla tarvetta verrata, onko verkkopankin käyttäjä sama kuin se, jolla on oikeus katsella tiettyjä tietoja tai tehdä jotain toimintoja.

Vertailu tehdään verkkopankin käyttäjän henkilötunnuksesta muodostetun tarkisteen USERMAC avulla.

USERMAC muodostetaan koko linkin tarkisteen tapaan seuraavasti:

- Muodostetaan merkkijono aikaleimasta, henkilötunnuksesta ja avaimesta &-merkillä eroteltuina, esimerkiksi TIMESTMP&HENKILÖTUNNUS&AVAIN&
- Henkilötunnuksessa on merkkijonossa mukana välimerkki ja mahdollinen kirjain on isolla.
- Lasketaan merkkijonolle tarkiste, joka sijoitetaan kentän USERMAC arvoksi näkyvässä, ascii-muodossa.

Jos esilläpitopalvelussa on rekisteröitynä niiden henkilöiden tunnukset, jotka saavat selailla tiettyjä tietoja, voidaan oikeus tarkistaa muodostamalla vastaava

merkkijono laskuttajan tiedoista, laskemalla siitä tarkiste ja vertaamalla näin saatua tarkistetta parametrikenttään USERMAC.

**HUOM:** Tarkistus edellyttää, että esilläpitopalvelun tarjoajan järjestelmässä on rekisteröitynä henkilötunnukset, sillä sitä ei välitetä missään, eikä henkilötunnusta voi laskea parametritiedosta USERMAC, vaikka käytössä olisi jopa tarkisteen muodostuksessa käytettävä salainen avain.

### 4.4 Suoralaskuun muodostettava linkki

Verkkopankissa linkki muodostetaan pankkikohtaisten sääntöjen mukaisesti suoralaskuna toimitettuun maksuun, jota verkkopankin asiakas katsoo omassa verkkopankissaan.

Myös suoraveloitukseen voidaan muodostaa linkki samaan tapaan.

Linkissä on parametrina laskuttajan tunnus ja kyseisen suoralasku- tai suoraveloitustapahtuman viite. Näiden tietojen avulla linkki voidaan kohdistaa laskujen esilläpitopalvelussa oikeaan laskuun.

**Esimerkki**:

https://www.yritys.fi/aaaa/bbbbbb/cccccccc?VERSION=0001&PMTREFNB=12345678901234567890&RCVID=12345678&TIMESTMP=1999-06-21-102030+02&KEYVERS=0001&ALG=0001&MAC=12345678901234567890123456789012&LANGCODE=1&SESSIONID=1234567890123456789&SENDID=Pankki&STATUS=Prod& PMTORIG=1&USERMAC=12345678901234567890123456789012

### 4.5 Kuluttajan e-laskuun muodostettava linkki

Linkki muodostetaan kuten kohdassa 4.4, paitsi:

- SENDID:nä käytetään pankin BIC:iä.
- PMTREFNB-kentässä on kuluttajan e-laskussa laskuun liittyvän lisätiedon arkistointitunnus (esimerkiksi laskun viite, laskuttaja syöttää tiedon Finvoice verkkolaskulle kenttään InvoiceUrlText).

**Esimerkki:**

https://www.yritys.fi/aaaa/bbbbbb/cccccccc?VERSION=0001&PMTREFNB=12345678901234567890&TIMESTMP=2008-03-16-102030%2B02&KEYVERS=0001&ALG=0001&LANGCODE=1&SESSIONID=12345&STATUS=Prod&SENDID=NDEAFIHH&PMTORIG=1&USERMAC=1234567890123456789012345678901234567890123456789012&MAC=12345678901234567890123456789012

#### 4.5.1 Esimerkki Kuluttajan e-laskun MAC laskennasta:

Esimerkki linkki:

https://www.yritys.fi/aaaa/bbbbbb/cccccccc?VERSION=0001&PMTREFNB=12345678901234567890&TIMESTMP=2008-03-16-102030%2B02&KEYVERS=0001&ALG=0001&LANGCODE=1&SESSIONID=12345&STATUS=Prod&SENDID=NDEAFIHH&PMTORIG=1&USERMAC=12345678901234567890123456789012&MAC=12345678901234567890123456789012

Mac laskennassa käytettävä merkkijono muodostuu parametrikenttien sisällöistä ja &-merkeistä seuraavasti:

VERSION&PMTREFNB&TIMESTMP&KEYVERS&ALG&LANGCODE&SESSIONID&STATUS&SENDID&PMTORIG&USERMAC&

Merkkijonon loppuun liitetään MAC avain ja &-merkki. Merkkijonot eivät sisällä tyhjämerkkejä. Lopputulos on:

VERSION&PMTREFNB&TIMESTMP&KEYVERS&ALG&LANGCODE&SESSIONID&STATUS&SENDID&PMTORIG&USERMAC&MAC AVAIN&

Esimerkki linkin tapauksessa:

0001&12345678901234567890&2008-03-16-102030+02&0001&01&1&12345&Prod&NDEAFIHH&1&12345678901234567890123456789012&[MAC avain]&

HUOM! Kentän TIMESTMP enkoodaus on laskennassa muutettu takaisin +-merkiksi:

2008-03-16-102030%2B02 on laskennassa siis muodossa 2008-03-16-102030+02

Tälle merkkijonolle lasketaan MD5-tarkenne, joka sijoitetaan näkyvässä muodossa, asciimerkkeinä, parametrikentän MAC arvoksi. HUOM! MAC arvon mahdolliset pienet kirjaimet ovat linkille muutettu isoiksi.

### 4.6 Toistuvaissuoritukseen muodostettava linkki

Verkkopankissa linkki muodostetaan pankkikohtaisten sääntöjen mukaisesti toistuvaissuorituksena toimitettuun panoon, esimerkiksi palkkaan, jota verkkopankin asiakas katsoo omassa verkkopankissaan.

Linkissä on parametrina palkanmaksajan tunnus ja kyseisen palkkatapahtuman saajan henkilötunnus ja palkan maksupäivä. Näiden tietojen avulla linkki voidaan kohdistaa palkkalaskelmien esilläpitopalvelussa oikeaan palkkaan.

**Esimerkki**:

https://www.yritys.fi/aaaa/bbbbbb/cccccccc?VERSION=0001&PMTREFNB=12345678901234567890&RCVID=12345678&TIMESTMP=1999-06-21-102030+02&KEYVERS=0001&ALG=0001&MAC=12345678901234567890123456789012&LANGCODE=1&SESSIONID=12345678901234567890&SENDID=Pankki&STATUS=Prod& PMTORIG=1&USERMAC=12345678901234567890123456789012