NET BANKING LINK

A secure link from net banking to external services

Service description and service provider's guidelines

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

Table of contents

1 Net banking link description

The Net banking link provides a company with the opportunity of reducing the printing and distribution of paper documents when they are connected to payment transactions or consumers' e-invoices transmitted through the bank.

The Net banking link has a standard agreed jointly by the banks. The service provider agrees on the implementation of the link with all of the banks whose Web customers are to be provided with the link.

1.1 General description

The Net banking link is formed from a Net banking transaction for which by this means it is possible to provide additional information or a more detailed specification in a service external to the bank.

The link connects the Net banking customer to the service provider's presentation service on the Internet. The link contains all of the information the service provide needs to target the link to the right transaction.

The data transmission is encrypted and the integrity of the transferred data is secured using a message authentication code.

1.2 Application

The Net banking link is applicable for use in connection with direct debiting, direct billing, periodic payments, or consumer's e-invoice services, for example.

In a direct debiting service, the link can replace the advance notification sent to the payer. When the sum to be direct debited varies, the customer can use the link to check the information on the invoice upon which the payment is based. If the presentation service allows feedback concerning the invoice, the invoicer can automate the handling of direct debit cancellations.

In direct billing, the link can be used to replace the paper bill, similarly to direct debiting.

The wage slip connected to a periodically paid wage payment can be presented on the Internet. Features can be built into the wage slip browsing service which makes payroll computation and possible corrections to it easier.

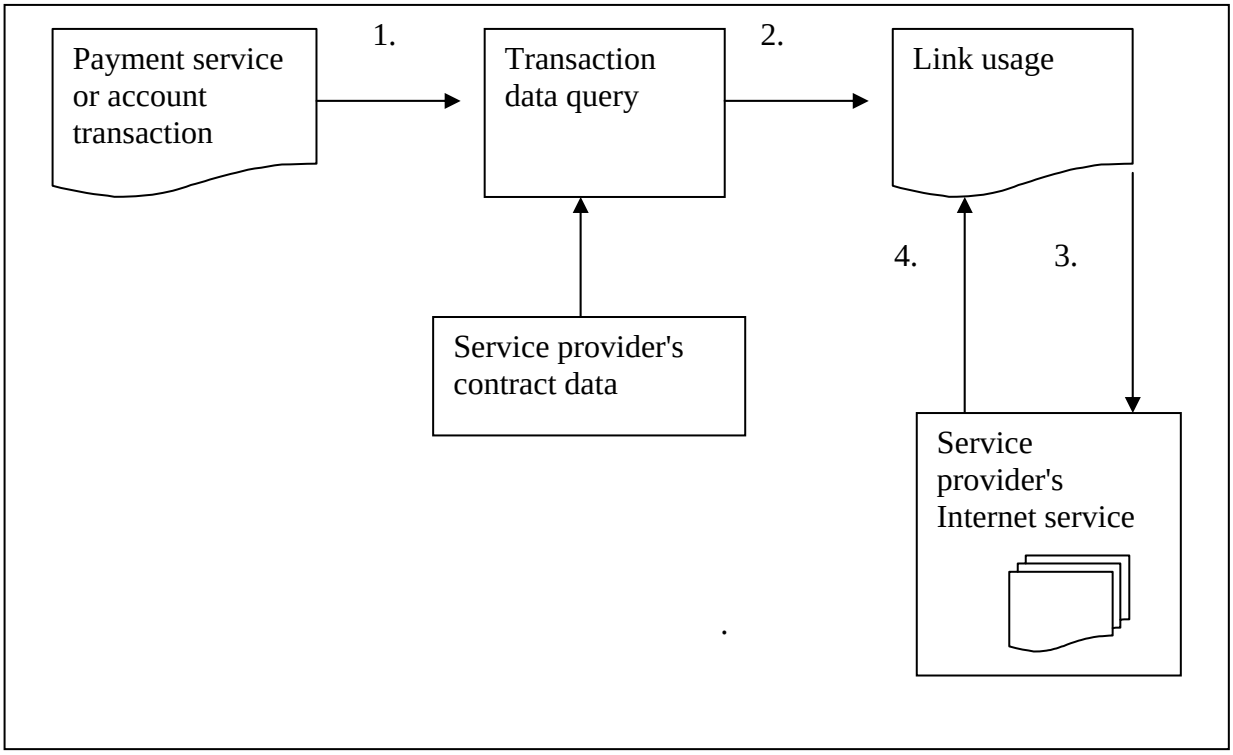
The consumer's e-invoice attachment may contain an itemised invoice, for example.

1.3 Security

The data traffic between the Net banking service and the presentation service uses SSL encryption protocol so outside parties cannot see or change the data. The data of the service provider that is the target of the link must also be SSL encrypted.

The bank authenticates its Net banking customers. In the Net banking link, the data received by the banking service provider are based on the data of the bank's payment transaction and Net banking customer. The data in the link are also secured using a message authentication code that ensures the integrity of the data so that a Net bank customer using the link cannot change the data without the service provider noticing it.

2 Functional description of the Net banking link



1 The Net banking customer logs into the Net banking service and chooses the payment or e-invoice from the list of payments or account transactions.
2 The payment or invoice can have a Net banking link.
3 Using the link connects the Net banking customer to the service provider's Internet service and from there to the data presented about the payment which can be presented in a separate browser window, for example.
4 The Net banking customer browses and verifies the basis for the payment (e.g. the invoice) and may also use other functions enabled by the service, such as the cancellation of a paper invoice.
When the Net banking customer stops using the service provider's Internet service (e.g. by closing the browser window), he or she returns to the Net banking service and can accept the payment.
If the Net banking service has timed out while the Net banking customer was carrying out transactions on the service provider's Web pages, the customer must log back into the Net banking service.

3 Implementation of the Net banking link

The service provider shall agree on the introduction of the Net banking link separately with each bank. The start-up date of the service is agreed when the contract is concluded. The service provider's data are registered in each bank and the service provider notifies each bank separately when there are changes in the service provider's contractual data.

Once the contract is signed, the bank delivers the service identifier and verification key used in the service to the service provider. The data are delivered to the service provider through a bank-specific procedure either electronically or in paper format. The data delivered are secured during transmission so that the recipient can detect if the protective cover of the delivery has been opened during transmission.

The testing procedures are specific to each bank and more information about them is available in the bank's own service descriptions.

4 Net banking link parameters

The character string consists of the contents of the parameter fields with "&" signs in between the fields. The name of the field is connected to the value using the "=" sign. The secret key data and an "&" sign are attached to the end of the character string. The character strings do not contain empty space characters.

Field name	Value	Length	Description
	https:// www.yritys.fi aaaa/bbbbbb/ccccccc ?		- protocol, SSL encryption - server name - name of the presentation service on the server in question
VERSION	0001	4 characters	Version number of the link, available values listed in bank-specific descriptions

PMTREFNB			Unique identification of the transaction corresponding to the link - reference number of the payment in direct billing - in wage payment, the wage recipient's identity number (123456-789X) and the date of payment - in a consumer's e-invoice o length max. 60 characters o archiving identifier of additional data connected to the invoice (for example the invoice's reference; the invoicer feeds the data for the Finvoice e-invoice into the field InvoiceUrlText) PMTREFNB can also be hidden cf. section 4.2, but cannot be hidden in the consumer's e-invoice
RCVID		max. 20 characters	The ID of the invoicer or paymaster in the bank Not used in the consumer's e-invoice
TIMESTMP	VVVV-KK-PP-HHMMSS+HH or VVVV-KK-PP-HHMMSS%2BHH	22 or 24 characters	Time when the link was generated, the form of presentation of the time zone can be +HH or %2BHH depending on the bank +02 = %2B02 = normal time in Finland +03 = %2B03 = daylight saving time in Finland
KEYVERS		4 characters	MAC Key version. The hidden PMTREFNB field is used to calculate the link's MAC message authentication code
ALG	0001= MD5 0002= SHA-1	4 characters	The MAC key calculation algorithm, either MD5 or SHA-1
LANGCODE	1= Finnish 2= Swedish 3 = English	1 character	Customer's language code in the Net banking service
SESSIONID		max. 20 characters	Log data

SENDID		max. 20 characters	The ID of the party forming the link. The BIC of the bank that formed the link is in the SENDID field in the link formed by the bank in the consumer's e-invoice. OP's ID is "OSUUSPANKKI" in all Net banking links Other available values are listed in bank-specific descriptions.
Optional data:			
STATUS	Prod = production link Test = testing link	4 characters	Status of link
PMTORIG	1 = Direct billing, direct debiting or consumer's e-invoice 2 = Periodic payment	1 character	Payment input method
USERMAC		32 characters	Authentication code generated from the payer's identity number For more information see section 4.3.
MAC			The link's MAC authentication code An authentication code generated from all parameters used. The server that forms the link calculates the MAC field based on the parameter data. The authentication code is set as the MAC value of the parameter field in the form of printable ASCII characters.

4.1 Detailed description of the TIMESTMP parameter

The receiving service must check that the time stamp has been used within a certain time window. In addition, the link can only be used once. The verification is carried out by comparing the values of the TIMESTMP and PMTREFNB parameters.

4.2 Detailed description of the encryption of the PMTREFNB field

The algorithm is agreed with the bank. The alternatives are DES and AES.

When using DES, an 8 character (56 bit) encryption key and EBC mode are used.

When using AES, the ECB method is used. The character set is ISO 8859-1 (latin-1). The length of the key is 256 bits. The hidden segment is 32 characters long. At the beginning of the segment (at the left edge) is the personal identification number 123456-789X, and after

that is the payment date of the wage (00000000). The rest of the segment is filled with empty characters. The result of the encryption process is presented in hexadecimal format, with the letters A–F in upper case.

The hidden PMTREFNB field is used to calculate the link's MAC authentication code.

4.3 Detailed description of the use of the TIMESTMP parameter

In some situations, there may be a need in the presentation service to compare whether the user of the Net banking service is the same user that has the right to view certain data or perform certain functions.

The comparison is carried out using the authentication code USERMAC, which is formed from the personal identification number of the Net banking user.

USERMAC is generated as follows (similarly to the authentication code for the whole link):

- A character string is formed from the time stamp, personal identification number and key, separated by & signs, for example TIMESTMP&PERSONALIDNUMBER&KEY&
- In the character string, the personal identification number includes a dash and if there is a letter, it is in upper case.
- An authentication code is generated for the character string, which is set as the value of the field USERMAC in the form of printable ASCII characters.

If the personal identification numbers of the persons who are permitted to browse certain data are registered in the presentation service, the right can be checked by generating the corresponding character string from the invoicer's data, generating an authentication code based upon it and comparing the resulting authentication code with the parameter field USERMAC.

N.B.: To carry out the checking, the personal identification numbers must be registered in the system of the provider of the presentation service because they are not transmitted at any point, and the personal identification numbers cannot be calculated from the USERMAC parameter data even if one had the secret key used to generate the authentication code available.

4.4 Direct billing link

In the Net banking service, the link to the invoice delivered through direct billing is generated in accordance with bank-specific rules, which the Net banking customer can view in the Net banking service.

It is also possible to generate a link to direct debiting in the same way.

In the link, the parameters are the invoicer's ID and the reference for the direct billing or direct debiting transaction in question. Using these data, the link can be associated with the right invoice in the invoice presentation service.

Example:

https://www.yritys.fi/aaaa/bbbbbb/cccccccc?VERSION=0001&PMTREFNB=123456789012345678 90&RCVID=12345678&TIMESTMP=1999-06-21-102030+02&KEYVERS=0001&ALG=0001&MAC=12345678901234567890123456789012&LANGCODE=1&SESSIONID=1234567890123456789 0&SENDID=Pankki&STATUS=Prod& PMTORIG=1&USERMAC=12345678901234567890123456789012

4.5 Consumer's e-invoice link

The link is generated as described in section 4.4, with the following differences:

- the bank's BIC is used as the SENDID
- In the PMTREFNB field, there is an archiving identifier for additional data in the consumer's e-invoice that are associated with the invoice (for example the invoice's reference; the invoicer feeds the data for the Finvoice e-invoice into the field InvoiceUrlText).

Example:

https://www.yritys.fi/aaaa/bbbbbb/cccccccc?VERSION=0001&PMTREFNB=123456789012345678 90&TIMESTMP=2008-03-16-102030%2B02&KEYVERS=0001&ALG=0001&LANGCODE=1&SESSIONID=12345&STATUS=Prod&SENDID=NDEAFIHH&PMTORIG=1&USERMAC=12345678901234567890123456789012&MAC=12345678901234567890123456789012

4.5.1 Example of the MAC calculation of a consumer's e-invoice:

Example link:

https://www.yritys.fi/aaaa/bbbbbb/cccccccc?VERSION=0001&PMTREFNB=123456789012345678 90&TIMESTMP=2008-03-16-102030%2B02&KEYVERS=0001&ALG=0001&LANGCODE=1&SESSIONID=12345&STATUS=Prod&SENDID=NDEAFIHH&PMTORIG=1&USERMAC=12345678901234567890123456789012&MAC=12345678901234567890123456789012

The character string used in MAC calculation is composed of the contents of parameter fields and "&" signs as follows:

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

The MAC key and an "&" sign are attached to the end of the character string. The character strings do not contain empty space characters. The end result is:

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

Example in the case of a link:

0001&12345678901234567890&2008-03-16-102030+02&0001&01&1&12345&Prod&NDEAFIHH&1&12345678901234567890123456789012345&[MAC key]&

N.B.!: In the calculation, the encoding of the field TIMESTMP has been changed back to the "+" sign:

Thus in the calculation, 2008-03-16-102030%2B02 is in the form 2008-03-16-102030+02

An MD5 hash value is calculated from this character string and this value is placed in the MAC parameter field in the form of printable ASCII characters. N.B.!: Any letters in lower case in the MAC value are changed in the link into upper case.

4.6 Periodic payment link

In the Net banking service, the link to a deposit made as a periodic payment, for example a wage, is formed in accordance with bank-specific rules, which the Net banking customer can view in the Net banking service.

The link has, as parameters, the paymaster's ID, the personal identification number of the recipient of the wage payment transaction in question and the date of the payment of the wage. Using these data, the link can be associated with the right wage in the wage slip presentation service.

Example:

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