Description of *BankLink*

1. Introduction

BankLink is a system by the help of which traders in the Internet (hereinafter in the text – the Traders), clients of the Internetbank of Swedbank (hereinafter in the text – the Clients) and the Internetbank of Swedbank may exchange the data, provide services and start transactions. BankLink offers convenience of starting transactions and receiving reply from the Internetbank in a stipulated way.

- Traders may send their clients to the Internetbank with already prepared payment order and receive confirmation from the Bank on successful/unsuccessful accomplishment of payment;
- Clients may start a session of the Internetbank with transaction that is suitable for them;
- In the Internet, where all users are anonymous, the Traders may identify the Clients using *BankLink*;
- Clients may provide confirmation for Traders on the transactions they have made at the Bank;
- Administration of transactions of the Internetbank may take place in form of confirm. A list of their succession is provided in item "Specifications of requests".

2. General information

In order to choose services or goods in the homepage of the Trader and make payments via the Internetbank, the Client needs a browser. The Client starts the process by surfing in Internet shop. The Client selects certain goods and wishes to purchase them. The Trader offers him the opportunity to pay via the Internetbank of Swedbank. If the Client has a contract on the connection of the Internetbank and wishes to pay for goods this way, the Trader develops HTML page containing payment order data, the integrity of which is ensured by digital signature. This web page readdresses the Client's browser to the Internetbank. There the Trader's signature is verified and the Client is offered to enter user's name and password of the Internetbank. After connection to the Internetbank, the Client will see a prepared payment order. The Client may confirm the prepared payment order or return to the Trader's page. The Bank, on the turn, in reply prepares HTML page that contains information on the result of accomplished payment order, the integrity of which is ensured by electronic signature of the Bank. Then, the Client may return to the Trader's page and continue work in the Internetbank or close the browser. In order to ensure reply of the Bank to the Trader when the Client after transaction does not return to the Trader's page, the server of the Internetbank sends reply from the Bank, the Trader verifies the Bank's signature and acts respectively, for example, delivers goods to the Client.

3. Security

Communication between the Client and Trader takes place in accordance with security requirements of the Trader, which may include use of SSL technology. The data forwarded from the Internetbank to the Trader and vice versa contains digital signature, thus, it allows the second party to make sure about the integrity of forwarded data.
Data of the very payment order is not codified.

Queries

Queries are HTTP GET or POST queries with specified parameters. Each query contains a service number. Each service has a unique list of parameters and its own algorithm for handling the query. By content, the service number is the algorithm number of query handling. All parameters whose field names do not begin with VK_ must be ignored.

- Parameters that are requested by the service but are missing are counted as empty fields.
- In the amount parameters dot "." Is used as decimal separator. Thousands separator is not used.
- Dates are presented in the format "DD.MM.YYYY," e.g. 17.02.2001
- The time is indicated in the format "hh24:min:sec," e.g. 17:02:59
- The length of the value of the parameter must not exceed that which is prescribed in the specifications. Upon exceeding the length, a query is not processed.
- The values of parameters can be shorter than the permitted maximum length. Missing places are not filled in. The spaces at the beginning and at the end of the value of a parameter are removed.
- An error message is sent in reply to queries that do not match the specifications and are invalid.
- Operations to be performed on the basis of a query are carried out pursuant to the general requirements of the service (requirements of payment orders, etc.).

- Merchant specifies the query encoding using VK_ENCODING parameter, supported encodings are UTF-8 and ISO-8859-13. Bank always replies using the encoding specified by merchant. If encoding is not explicitly specified, ISO-8859-13 is used by default.

Queries can be divided into merchant or bank queries according to their originator. Queries can be divided into those that require a reply and that do not require a reply.

According to the purpose, queries are divided as follows:

- 1xxx – initiation of transactions
- 3xxx – identification queries

Queries from the merchant to the bank

Queries from the merchant to the bank are meant for the direction and/or assistance of the customer in the performance of an operation, e.g. a payment order. Each query corresponds to one service. The presented parameters are verified according to the service. The list of parameters of a query and the order depends on the service used. The bank replies to the queries that require a reply after having completed the customer's operation. As a rule, a reply contains the details of the operation and a notice about whether it was successful.

Queries from the merchant to the bank are directed to the URL:

https://ib.swedbank.lv/banklink/

Queries from the bank to the merchant

As a rule, queries from the bank to the merchant are replies to the previous queries of the merchant. At the same time the client may initiate a query from the Bank to a merchant by entering the merchant's page through the E-services page on the Internet bank.

5. Finding the VK_MAC control code

Verification of the electronic signature used in queries, **VK_MAC**, takes place on the basis of the agreed algorithm **VK_VERSION**. Only version 008 is currently used.

VK_MAC is given as the query's parameter value in the BASE64 encoding.

Version 008

The value of the **MAC008** function is calculated using the public key algorithm **RSA**. Values of empty fields are taken into account as well – "000".

$MAC008(x_1,x_2,\ldots,x_n) := RSA(SHA\text{-}1(p(x_1)|| x_1|| p(x_2)|| x_2 || \ldots ||p(x_n)||x_n),d,n)$

Where:

- **||** is an operation of adding the string
- $\mathbf{x_1, x_2, \ldots, x_n}$ are the query parameters
- **p** is a function of the parameter length. The length is a number in the form of a three-digit string
- **d** is the RSA secret exponent
- **n** is the RSA modulus

The signature is calculated in accordance with the PKCS1 standard (RFC 2437).

Example
Let us take a query with the following parameters:
VK_SERVICE="1002"
VK_VERSION="008"
VK_SND_ID="TRADER"
VK_STAMP="1234567890"
VK_AMOUNT="1.99"
VK_CURR="LVL"
VK_REF="01012001-001"
VK_MSG="Payment for a good XXXXXX"

The signature is calculated from the following data row which comprises the following elements (the number of the symbols of the parameter values and the value of the parameter itself):
"0041002"
"003008"
"006TRADER"
"0101234567890"
"0041.99"
"003LVL"
"01201012001-001"
"025Payment for a good XXXXXX"

in one row:
"0041002003008006TRADER01012345678900041.99003LVL01201012001-001025Payment for a good XXXXXX"

or if the VK_MSG parameter is empty, the result:
"0041002003008006TRADER01012345678900041.99003LVL01201012001-001000"

6. Query specifications

NB! A URL with parameters cannot be used in the VK_RETURN field.

Query "1002"

The merchant sends to the Bank the details of a signed payment order which the client cannot change on the Internet bank. After a successful payment the query "1101" is made for the merchant, in the case of a failed payment the "1901" package. The details of the recipient are taken from a bank link agreement.

No.	Field	Length	Description
1	VK_SERVICE	4	Service number (1002)
2	VK_VERSION	3	Used encryption algorithm (008)
3	VK_SND_ID	10	ID of the author of the query (merchant's ID)
4	VK_STAMP	20	Query ID
5	VK_AMOUNT	17	Amount payable
6	VK_CURR	3	Name of the currency in the ISO 4217 format (LVL/EUR, etc.)
7	VK_REF	20	Payment order reference number
8	VK_MSG	300	Description of payment order
-	VK_MAC	700	Control code or signature
-	VK_RETURN	150	URL where the transaction response query is sent (1101, 1901)
-	VK_LANG	3	Preferable language of communication (LAT, ENG or RUS)
-	VK_ENCODING	30	Message encoding. ISO- 8859-13 (by default) or UTF-8

Query "1101"

Used for replying about the execution of a domestic payment order.

No.	Field	Length	Description
1	VK_SERVICE	4	Service number (1101)
2	VK_VERSION	3	Used encryption algorithm (008)
3	VK_SND_ID	10	ID of the author of the query (Bank's ID)
4	VK_REC_ID	10	ID of the author of the query (merchant's ID)
5	VK_STAMP	20	Query ID
6	VK_T_NO	5	Payment order number
7	VK_AMOUNT	17	Amount paid
8	VK_CURR	3	Name of the currency in the ISO 4217 format (LVL/EUR, etc.)
9	VK_REC_ACC	34	Recipient's invoice number
10	VK_REC_NAME	70	Recipient's name
11	VK_SND_ACC	34	Remitter's account number
12	VK_SND_NAME	40	Remitter's name
13	VK_REF	20	Payment order reference number
14	VK_MSG	300	Description of payment order
15	VK_T_DATE	10	Payment order date
-	VK_MAC	700	Control code or signature
-	VK_LANG	3	Preferable language of communication (LAT, ENG or RUS)
-	VK_AUTO	1	Y= reply automatically sent by the Bank. N= reply by moving the customer to the merchant's page.
-	VK_ENCODING	-	Message encoding. ISO- 8859-13 (by default) or UTF-8

Query "1901"

Used for notifying of a failed transaction.

No.	Field	Length	Description
1	VK_SERVICE	4	Service number (1901)
2	VK_VERSION	3	Used encryption algorithm (008)
3	VK_SND_ID	10	ID of the author of the query (Bank's ID)
4	VK_REC_ID	10	ID of the author of the query (merchant's ID)
5	VK_STAMP	20	Query ID
6	VK_REF	20	Payment order reference number
7	VK_MSG	300	Description of payment order
-	VK_MAC	700	Control code or signature
-	VK_LANG	3	Preferable language of communication (LAT, ENG or RUS)
-	VK_AUTO	1	N=reply by moving the customer to the merchant's page.
-	VK_ENCODING	-	Message encoding. ISO- 8859-13 (by default) or UTF-8

7. Exchange with public keys

Exchange of public keys (certificates) takes place in X.509 format.

Notes. Reply's requests "1101" and "1901", which are send directly from the Bank's server to the address specified by the Trader are sent by "HTTPGET".