Bank Link Technical Description
Document version: 1.4

Queries

Queries are exchanged as parameters with HTTP GET or POST methods. Each query contains a service number. Each service has a unique list of parameters and its own algorithm for handling the query. All parameters, which are not described in the specification, must be ignored.

- Parameters that are requested by the service but are missing, are counted as empty fields.
- In the queries, dot is used as decimal separator in the amounts. Thousands separator is not used.
- Date and time are presented in the DATETIME format according to the ISO 8601 standard, with the precision of second, together with time zone, e.g. 2013-03-13T07:21:14+0200. The receiver of the query must check the value in the DATETIME field, whereby the value of the field may not differ from the current time at the moment of checking more than ± 5 minutes. The merchant is responsible for the correctness of the time of their server.
- The length of the value of the parameter is in symbols. 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.
- 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.).
- Fields VK_RETURN and VK_CANCEL must include the address until the end of the hierarchical part (e.g. https://www.company-name.ee/pangalink.php) and it is not allowed to use the name of the fields (VK_...) in the query parameters.
- For data exchange merchant specifies the encoding (VK_ENCODING), the bank link supports UTF-8 (by default), ISO-8859-1 and WINDOWS-1257 encoding. Bank always replies using the encoding specified by the merchant. We suggest using UTF-8.

Queries can be divided as follows:

1. on the basis of originator: queries of merchant or queries of bank
2. on the basis of reply: requiring reply, not requiring reply
3. on the basis of purpose:
   - 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://www.swedbank.ee/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. Reply query from the bank to the merchant "1111", where VK_AUTO=Y, is sent using the "GET" method. The queries sent from client's browser use the "POST" method ("1011", where VK_AUTO=N and all other reply packages).

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($x_{1,x2,...,xn}$) := RSA(SHA-1(p(x1)|| x1|| p(x2)|| x2 || ... ||p(xn)||xn),d,n) Where:
|| is an operation of adding the string
x_1, x_2, ..., 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="1012"
VK_VERSION="008" VK_SND_ID="TRADER" VK_STAMP="1234567890" VK_AMOUNT="1.99" VK_CURR="EUR"
VK_REF="123"
VK_MSG="Payment for a good XXXXXX"
VK_RETURN="https://testtest.ee/banklinkreturn.php" VK_CANCEL="https://testtest.ee/banklinkcancel.php"
VK_DATETIME="2014-10-10T09:25:52+0300"

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" "003EUR"
"025Payment for a good XXXXXX"
038https://testtest.ee/banklinkreturn.php" „038https://testtest.ee/banklinkcancel.php" „0242014-10-10T09:25:52+0300"

in one row:
"00410120030080006TRADER01012345678900041.99003EUR003123025Payment for a good XXXXXX038http://testtest.ee/banklinkreturn.php 038http://testtest.ee/banklinkcancel.php0242014-10-10T09:25:52+0300"

or if the VK_MSG parameter is empty, the result is: "00410120030080006TRADER01012345678900041.99003EUR003123000038https://testtest.ee/banklinkreturn.php038https://testtest.ee/banklinkcancel.php0242014-10-10T09:25:52+0300"

NB! If the merchant is using the UTF-8 encoding (VK_ENCODING=UTF-8) in its package and there are two-byte symbols (e.g. accented characters), the length of the parameter value in the signature data string is the number of symbols in the string, not the number of bytes. E.g. 003ÕUN, not 004ÕUN.

Query specifications
Payment Services

Service “1011”

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 “1111” is made for the merchant and, in the case of a failed payment, the query “1911”.

No.	Field	Length	Description
1	VK_SERVICE	4	Service number (1011)
2	VK_VERSION	3	Used encryption algorithm (008)
3	VK_SND_ID	15	ID of the author of the query (Merchant's ID)
4	VK_STAMP	20	Query ID
5	VK_AMOUNT	12	Amount payable
6	VK_CURR	3	Name of the currency: EUR
7	VK_ACC	34	Recipient's invoice number
8	VK_NAME	70	Recipient's name
9	VK_REF	35	Payment order reference number
10	VK_MSG	95	Description of payment order
11	VK_RETURN	255	URL where reply of successful transaction is sent
12	VK_CANCEL	255	URL where reply of failed transaction is sent
13	VK_DATETIME	24	Date and time of the initiation of the query in DATETIME format
-	VK_MAC	700	Control code / signature
-	VK_ENCODING	12	Message encoding. UTF-8 (by default), ISO-8859-1 or WINDOWS-1257
-	VK_LANG	3	Preferable language of communication (EST, ENG or RUS)

Service “1012“

The merchant sends to the Bank the details of a signed payment order, which the client cannot change on the Internet bank. The name and account number of the payment recipient are taken from the agreement between the Bank and the Service Provider. After a successful payment the query “1111” is made for the merchant, in the case of a failed payment the “1911” query.

No.	Field	Length	Description
1	VK_SERVICE	4	Service number (1012)
2	VK_VERSION	3	Used encryption algorithm (008)
3	VK_SND_ID	15	ID of the author of the query (Merchant's ID)
4	VK_STAMP	20	Query ID
5	VK_AMOUNT	12	Amount payable
6	VK_CURR	3	Name of the currency: EUR
7	VK_REF	35	Payment order reference number
8	VK_MSG	95	Description of payment order
9	VK_RETURN	255	URL where reply of successful transaction is sent
10	VK_CANCEL	255	URL where reply of failed transaction is sent
11	VK_DATETIME	24	Date and time of the initiation of the query in DATETIME format
-	VK_MAC	700	Control code / signature
-	VK_ENCODING	12	Message encoding. UTF-8 (by default), ISO-8859-1 or WINDOWS-1257
-	VK_LANG	3	Preferable language of communication (EST, ENG or RUS)

Query “1111”

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

No.	Field	Length	Description
1	VK_SERVICE	4	Service number (1111)
2	VK_VERSION	3	Used encryption algorithm (008)
3	VK_SND_ID	15	ID of the author of the query (Bank’s ID)
4	VK_REC_ID	15	ID of the author of the query (Store ID)
5	VK_STAMP	20	Query ID
6	VK_T_NO	20	Payment order number
7	VK_AMOUNT	12	Amount paid
8	VK_CURR	3	Name of the currency: EUR
9	VK_REC_ACC	34	Recipient’s account number
10	VK_REC_NAME	70	Recipient’s name
11	VK_SND_ACC	34	Remitter’s account number
12	VK_SND_NAME	70	Remitter’s name
13	VK_REF	35	Payment order reference number
14	VK_MSG	95	Description of payment order
15	VK_T_DATETIME	24	Payment order date and time in DATETIME format
-	VK_MAC	700	Control code / signature
-	VK_ENCODING	12	Message encoding. UTF-8 (by default), ISO-8859-1 or WINDOWS-1257
-	VK_LANG	3	Preferable language of communication (EST, ENG or RUS)
-	VK_AUTO	1	Y= reply automatically sent by the Bank. N= reply by moving the customer to the merchant’s page.

Service “1911”

Used for notifying of a failed transaction.

No.	Field	Length	Description
1	VK_SERVICE	4	Service number (1911)
2	VK_VERSION	3	Used encryption algorithm (008)
3	VK_SND_ID	15	ID of the author of the query (Bank’s ID)
4	VK_REC_ID	15	ID of the recipient of the query (Merchant’s ID)
5	VK_STAMP	20	Query ID
6	VK_REF	35	Payment order reference number
7	VK_MSG	95	Description of payment order
-	VK_MAC	700	Control code / signature
-	VK_ENCODING	12	Message encoding. UTF-8 (by default), ISO-8859-1 or WINDOWS-1257
-	VK_LANG	3	Preferable language of communication (EST, ENG or RUS)
-	VK_AUTO	1	N=reply by moving the customer to the merchant’s page.

Identification Services

Service “4011”

A package sent by the merchant for identification of the user. The service is available to merchants who have entered into a respective agreement. The code of the reply package is 3012.

No.	Field	Length	Description
1	VK_SERVICE	4	Service number (4011)
2	VK_VERSION	3	Used encryption algorithm (008)
3	VK_SND_ID	15	ID of the author of the query (Partner ID)
4	VK_REPLY	4	Code of the expected reply package (3012)
5	VK_RETURN	255	Merchant's URL where to reply
6	VK_DATETIME	24	Message generation time in DATETIME format
7	VK_RID	30	Identifier related to the session, empty value in case of Swedbank
-	VK_MAC	700	Control code / signature
-	VK_ENCODING	12	Message encoding. UTF-8 (by default), ISO-8859-1 or WINDOWS-1257
-	VK_LANG	3	Preferable language of communication (EST, ENG or RUS)

Service “3012”

The data about the user and the date and time of generation of the package are sent to the merchant. For the security reasons, the merchant must check the forwarding time (VK_DATETIME) of the package. The VK_USER_NAME field contains the name of the user in the following format: “lastname,firstname” (e.g. SAAR,JAAN).

No.	Field	Length	Description
1	VK_SERVICE	4	Service number (3012)
2	VK_VERSION	3	Used encryption algorithm (008)
3	VK_USER	16	Agreed user identifier
4	VK_DATETIME	24	Message generation time in DATETIME format
5	VK_SND_ID	15	ID of the author of the message (Bank's ID)
6	VK_REC_ID	15	ID of the message recipient (Partner ID)
7	VK_USER_NAME	140	Name of the user
8	VK_USER_ID	20	Personal Identification Code of the user
9	VK_COUNTRY	2	Country of the Personal Identification Code (two-letter code according to the ISO 3166-1 standard)
10	VK_OTHER	150	Other data about the user
11	VK_TOKEN	2	Identifier Code of the identification device: 1- ID card; 2- Mobile ID; 5- one-time codes, except PIN calculator (Swedbank is currently not using the one-time passwords); 6- PIN-calculator; 7- reusable password card
12	VK_RID	30	Identifier related to the session, empty value in case of Swedbank
-	VK_MAC	300	Control code / signature
-	VK_ENCODING	-	Message encoding. UTF-8 (by default), ISO-8859-1 or WINDOWS-1257
-	VK_LANG	3	Preferable language of communication (EST, ENG or RUS)

Service “4012”

A package sent by the merchant for identification of the user. The service is available to merchants who have entered into a respective agreement. Response package code is 3013.

No.	Field	Length	Description
1	VK_SERVICE	4	Service number (4012)
2	VK_VERSION	3	Used encryption algorithm (008)
3	VK_SND_ID	15	ID of the author of the message (Partner ID)
4	VK_REC_ID	15	ID of the receiver of the message (Bank ID)
5	VK_NONCE	50	Unique nonce generated by query author
6	VK_RETURN	255	Merchant's URL where to reply
7	VK_DATETIME	24	Query generation time in DATETIME format
8	VK_RID	30	Identifier related to the session, empty value in case of Swedbank
-	VK_MAC	700	Control code / signature
-	VK_ENCODING	12	Message encoding. UTF-8 (by default), ISO-8859-1 or WINDOWS-1257
-	VK_LANG	3	Preferable language of communication (EST, ENG or RUS)

Service “3013”

The nonce copy is sent to the merchant.

No.	Field	Length	Description
1	VK_SERVICE	4	Service number (3013)
2	VK_VERSION	3	Used encryption algorithm (008)
3	VK_DATETIME	24	Query generation time in DATETIME format
4	VK_SND_ID	15	ID of the author of the message (Bank ID)
5	VK_REC_ID	15	ID of the receiver of the message (Partner ID)
6	VK_NONCE	50	A copy of the nonce from the query
7	VK_USER_NAME	140	Name of the user
8	VK_USER_ID	20	Personal Identification Code of the user
9	VK_COUNTRY	2	Country of the Personal Identification Code (two-letter code according to the ISO 3166-1 standard)
10	VKJOTHER	150	Other data about the user
11	VK_TOKEN	2	Identifier Code of the authentication device: 1- ID card; 2- Mobile ID; 5- one-time codes, except PIN calculator; 6- PIN-calculator; 7- reusable password card
12	VK_RID	30	Identifier related to the session
-	VK_MAC	700	Control code / signature
-	VK_ENCODING	-	Message encoding. UTF-8 (by default), ISO-8859-1 or WINDOWS- 1257
-	VKJLANG	3	Preferable language of communication (EST, ENG or RUS)

Exchange of public keys

Public keys are exchanged upon entry into the agreement.
We use PEM keys/certificates corresponding to the X.509 standard. We support 2048 bytes for the length of the secret key generated by the client.

Document History

Version	Date	Amendments
1.4	09.10.2014	Removed descriptions of the queries 1001, 1002, 1101, 1901, 4001, 3002, 4002, 3003 and 3004. Added descriptions of queries 1011, 1012, 1111, 1911, 4011, 3012, 4012 and 3013. Added responsibility to check DATETIME value, which may not differ from the current time at the moment of checking more than ± 5 minutes.
1.3	06.12.2012	Added description of query 3004
1.2	18.05.2010	Added description of queries 4002 and 3003
1.1	24.03.2010	Maximum length of the query parameter VK_MAC was extended to 700 units, we support maximum of 4096 bytes for the length of the secret key. Added document history.
1.0	2009	UTF-8 coding support was added to the queries. Added new bank link URL: https://www.swedbank.ee/banklink