Bank Link's technical specification

Queries

In this document you can find the format of the queries used for either payments or authentication. Each service has its own list of parameters and for functional service the guidelines in this document must be followed.

- Decimal points and cents in the amounts presented in queries are separated with a dot ".". 1000 separator is not used.
- Dates and times are presented in DATETIME format with the accuracy of a second + the time zone, e.g. 2016-10-13T07:21:14+0200. The receiver of the query has to check the value in the DATETIME field, whereas the value of the field may differ from the current checking time by a maximum of ± 5 minutes.
- The length of the field may not exceed the length given in the specification. Query shall not be processed, if the length of the field is exceeded. Field value length is given in symbols. Field value may be shorter than the maximum permitted length.
- Queries are exchanged using HTTP POST method.
- If one of the numbered field for the service isn't sent out, then it's still counted as an empty field.
- An error message is returned to queries not corresponding to the specification.
- Field names, used in the Bank Link queries (VK:...) cannot be used in the field VK_RETURN.
- Encoding is used for the exchanged messages (VK_ENCODING) and SEB's Bank Link supports either UTF-8 (default value) or ISO-8859-1. Bank always answers using the encoding in which the merchant sent its service. For functional service all the involved programs must use the same encoding.

Queries may be divided:

1. Based on the initiator:
   - queries of the merchant or queries of the bank.

2. Based on the answer:
   - answer is requested or answer is not requested.

3. Based on the purpose:
   - 1xxx - initiation of payments or 4xxx - authentication queries

Exchanging the certificates/public keys

For the activation of the bank link in SEB's live system the merchant has to send its public key to eservice@seb.ee. After that SEB replies sending our public key and merchant's VK_SND_ID parameter. Private key must always be kept secret (also from SEB). SEB uses x.509 standard .PEM format certificates and the private key length should be 2048 bits. Certificate generating guide can be found from the documents in "Test package".

Finding the control code VK_MAC on the basis of version 008

The signature MAC008 (VK_MAC) is calculated by using the public key algorithm RSA and hash algorithm SHA1. Values of the empty fields are also counted as "000".

MAC008(x1,x2,..., xn):= RSA (SHA-1(p(x1) || x1 || p(x2) || x2 || ... || p(xn) || xn),d,n)

Descriptions:

|| - string addition operation

x1, x2, ..., xn - query parameters (numbered in the specification).
p - function of the length of parameter in symbols Length is a number in the form of a three digit string
d RSA - secret exponent
n RSA - modulus

Example of the data string composition for service "1012"
VK_SERVICE="1012"
VK_VERSION="008"
VK_SND_ID ="testvpos"
VK_STAMP ="20011"
VK_AMOUNT="1.00"
VK_CURR ="EUR"
VK_REF ="999"
VK_MSG ="UPOS testikas. ÕÜ"
VK_RETURN ="https://somehost.ee/returnurl"
VK_CANCEL ="https://somehost.ee/cancelurl"
VK_DATETIME ="2016-09-26T07:21:14+0200"

The signature (VK_MAC) is calculated from the data string, which consists of the following elements - the number of symbols of the parameter value and of the parameter itself.
Data string must include every field with list numbers (1 to 11 for service "1012") which is described in the service specification.
Fields that don't have the list number (for example VK_LANG) is not included in the data string.

004 1012
003 008
008 testvpos
005 20011
004 1.00
003 EUR
003 999
017 UPOS testikas. ÕÜ
029 https://somehost.ee/returnurl
029 https://somehost.ee/returnurl
024 2016-09-26T07:21:14+0200

In one row:
0041012003008008testvpos005200110041.00003EUR003999017UPOS testikas. ÕÜ029https://somehost.ee/returnurl029https://somehost.ee/returnurl0242016-09-26T07:21:14+0200

If for example VK_MSG parameter would be empty, then it still would be included to the data string with the symbol value of 000.

NB! If the UTF-8 encoding is used and the parameter would include two-byte symbols (e.g. accented characters), the length of the parameter value in the data string is the number of symbols in the string, not the number of bytes. E.g. 002OÜ, not 003OÜ

Query specifications

Payment services

Service 1011

The service provider sends to the bank the signed payment order data, which the client cannot change in Internet Bank. After a successful payment, query “1111” is compiled to the merchant, in case of unsuccessful payment “1911”.

No.	Field name	Length	Description
1	VK_SERVICE	4	Service number (1011)
2	VK_VERSION	3	Encryption algorithm used (008)
3	VK_SND_ID	15	Query compiler’s ID (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	Beneficiary’s account number
8	VK_NAME	70	Beneficiary’s name
9	VK_REF	35	Reference number of payment order
10	VK_MSG	95	Description of payment order
11	VK_RETURN	255	URL where response is sent if the transaction is successful
12	VK_CANCEL	255	URL where response is sent if the transaction fails
13	VK_DATETIME	24	Date and time of the query in DATETIME format
-	VK_MAC	700	Control code / signature
-	VK_ENCODING	12	Encoding of the message. ISO-8859-1 or UTF-8 (default value)
-	VK_LANG	3	Preferred language of communication (EST, ENG or RUS)

Service 1012

The service provider sends to the bank the client’s request for transaction. The beneficiary’s name and account number is taken from the contract signed between the Bank and the service provider. After a successful payment, query “1111” is compiled to the merchant, in case of unsuccessful payment “1911”.

No.	Field name	Length	Description
1	VK_SERVICE	4	Service number (1012)
2	VK_VERSION	3	Encryption algorithm used (008)
3	VK_SND_ID	15	Query compiler’s ID (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	Reference number of payment order
8	VK_MSG	95	Description of payment order
9	VK_RETURN	255	URL where response is sent if the transaction is successful
10	VK_CANCEL	255	URL where response is sent if the transaction fails

11	VK_DATETIME	24	Date and time of the query in DATETIME format
-	VK_MAC	700	Control code / signature
-	VK_ENCODING	12	Encoding of the message. ISO-8859-1 or UTF-8 (default value)
-	VK_LANG	3	Preferred language of communication (EST, ENG or RUS)

Service 1111

Response compiled after a successful domestic payment order.

No.	Field name	Length	Description
1	VK_SERVICE	4	Service number (1111)
2	VK_VERSION	3	Encryption algorithm used (008)
3	VK_SND_ID	15	Query compiler's ID (Bank's ID)
4	VK_REC_ID	15	Query recipient's ID (Merchant's 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	Beneficiary's account number
10	VK_REC_NAME	70	Beneficiary's name
11	VK_SND_ACC	34	Remitter's account number
12	VK_SND_NAME	70	Remitter's name
13	VK_REF	35	Reference number of payment order
14	VK_MSG	95	Description of payment order
15	VK_T_DATETIME	24	Date and time of the payment order in DATETIME format (Payments carried out between 10 PM and 12 PM after the change of the banking day in the system may be presented in the next day's statement)
-	VK_MAC	700	Control code / signature
-	VK_ENCODING	12	Encoding of the message. ISO-8859-1 or UTF-8 (default value)
-	VK_LANG	3	Preferred language of communication (EST, ENG or RUS)
-	VK_AUTO	1	Y = automatically sent response by the bank. N = response compiled if the client proceeds back to the merchant's page after the payment

Service 1911

Compiled if the transaction failed.

No.	Field name	Length	Description
1	VK_SERVICE	4	Service number (1911)
2	VK_VERSION	3	Encryption algorithm used (008)
3	VK_SND_ID	15	Query compiler's ID (Bank's ID)
4	VK_REC_ID	15	Query recipient's ID (Merchant's ID)
5	VK_STAMP	20	Query ID
6	VK_REF	35	Reference number of payment order
7	VK_MSG	95	Description of payment order
-	VK_MAC	700	Control code / signature
-	VK_ENCODING	12	Encoding of the message. ISO-8859-1 or UTF-8 (default value)
-	VK_LANG	3	Preferred language of communication (EST, ENG or RUS)
-	VK_AUTO	1	Y = automatically sent response by the bank. N = response compiled if the client proceeds back to the merchant's page after the payment

Authentication services

Service 4011

Package sent by the merchant to identify the user. Service is available for merchants holding a respective contract. Code of response package (3012).

No.	Field name	Length	Description
1	VK_SERVICE	4	Service number (4011)
2	VK_VERSION	3	Encryption algorithm used (008)
3	VK_SND_ID	15	Query compiler's ID (partner's ID)
4	VK_REPLY	4	Code of expected response package (3012)
5	VK_RETURN	255	Merchant's URL where the response is sent
6	VK_DATETIME	24	Time of generating the message in DATETIME format
7	VK_RID	30	Session-related identifier. Optional field, may be left empty.
-	VK_MAC	700	Control code / signature
-	VK_ENCODING	12	Encoding of message. ISO-8859-1 or UTF-8 (default value)
-	VK_LANG	3	Preferred language of communication (EST, ENG or RUS)

Service 3012

Response to service 4011 which is compiled of the user data and authentication time (VK_DATETIME) which have to be checked for security reasons.

No.	Field name	Length	Description
1	VK_SERVICE	4	Service number (3012)
2	VK_VERSION	3	Encryption algorithm used (008)
3	VK_USER	16	Conventional user ID
4	VK_DATETIME	24	Time of generating the message in DATETIME format
5	VK_SND_ID	15	Query compiler's ID (Bank's ID)
6	VK_REC_ID	15	Query recipient's ID (partner's ID)
7	VK_USER_NAME	140	Name of user
8	VK_USER_ID	20	ID code of user
9	VK_COUNTRY	2	Country of ID code (two-letter ISO 3166-1)
10	VK_OTHER	150	Other user information
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- re-usable card Optional field, may be left empty.
12	VK_RID	30	Session-related identifier. Optional field, may be left empty.
-	VK_MAC	700	Control code / signature
-	VK_ENCODING	12	Encoding of message. ISO-8859-1 or UTF-8 (default value)
-	VK_LANG	3	Preferred language of communication (EST, ENG or RUS)

Service 4012

Package sent by the merchant to identify the user. Service is available for merchants holding a respective contract. Code of response package (3013).

No.	Field name	Length	Description
1	VK_SERVICE	4	Service number (4012)
2	VK_VERSION	3	Encryption algorithm used (008)
3	VK_SND_ID	15	Query compiler's ID (partner's ID)
4	VK_REC_ID	15	Query recipient's ID (Bank's ID)
5	VK_NONCE	50	Random nonce, generated by the compiler of query
6	VK_RETURN	255	Merchant's URL where the response is sent
7	VK_DATETIME	24	Time of generating the message in DATETIME format
8	VK_RID	30	Session-related identifier. Optional field, may be left empty.
-	VK_MAC	700	Control code / signature
-	VK_ENCODING	12	Encoding of message. ISO-8859-1 or UTF-8 (default value)
-	VK_LANG	3	Preferred language of communication (EST, ENG or RUS)

Service 3013

Copy of nonce is sent to the merchant.

No.	Field name	Length	Description
1	VK_SERVICE	4	Service number (3013)
2	VK_VERSION	3	Encryption algorithm used (008)
3	VK_DATETIME	24	Time of generating the message in DATETIME format
4	VK_SND_ID	15	Query compiler's ID (Bank's ID)
5	VK_REC_ID	15	Query recipient's ID (partner's ID)
6	VK_NONCE	50	Copy of nonce in query
7	VK_USER_NAME	140	Name of user
8	VK_USER_ID	20	ID code of user
9	VK_COUNTRY	2	Country of ID code (two-letter ISO 3166-1)
10	VK_OTHER	150	Other user information
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- re-usable card Optional field, may be left empty.
12	VK_RID	30	Session-related identifier. Optional field, may be left empty.
-	VK_MAC	700	Control code / signature
-	VK_ENCODING	12	Encoding of message. ISO-8859-1 or UTF-8 (default value)
-	VK_LANG	3	Preferred language of communication (EST, ENG or RUS)