Technical specification of the bank link

Queries

This document sets out query specifications, whereby each service has a corresponding individual list of parameters. In order to prepare a functioning service, only the parameters which are written in the specification, may be added, following the instructions provided in this document.

- In the amounts presented in queries, decimals and cents are separated with a period "." The thousands separator is not used.
- Date and time is presented in the DATETIME format, e.g. 2018-03-12T09:53:14+0200 with one second precision and together with the time zone. The recipient of a query is obliged to verify the value in the DATETIME field, while the field value may deviate from the time valid at the moment of verification by ± 5 minutes at maximum.
- The length of a field value may not exceed the prescription in the specification. If the length is exceeded, the query is not processed. The lengths of field values are in symbols (not in bites). A field value may be shorter than the permitted maximum value, vacant spaces are not filled in.
- For query-response exchange, the HTTP POST method is used.
- Queries not corresponding to the specification receive an error message.
- In the field VK_RETURN it is not permitted to use the field names used in queries (VK_...).
- Data exchange uses an encoding (VK_ENCODING), from which the Coop bank link supports the UTF-8 (default) and ISO-8859-1 encoding. For a problem-free functioning of the bank link it is necessary to make sure that all the programs connected to the service used the same encoding.

Queries can be divided:
1. based on the initiator:
   - trader or bank queries
2. based on response:
   - requiring response and not requiring response
3. based on purpose:
   - 1xxx – initiation of payments or 4xxx – authentication queries

Finding the verification code VK_MAC based on version 008

Verification of the electronic signature VK_MAC used in queries is performed on the basis of an agreed algorithm VK_VERSION.

Encoding in case of VK_VERSION=008 :

VK_MAC is calculated according to the RSA algorithm and is then turned into the BASE64 encoding. The value of VK_MAC is calculated, using the public key algorithm RSA. The length of empty fields is also taken into account – “000”. Additional fields of queries, which are not arranged in an order, are not signed.

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

where:

|| is the operation of string adding
x1, x2, …, xn are the parameters of the query
p is the parameter length function. Length is a number in the form of a three-digit string.
d is a secret exponent of RSA
n is the RSA modulus

Drawing up a data string, using the service "1012" as an example:
VK_SERVICE="1012"
VK_VERSION="008"
VK_SND_ID ="testvpos"
VK_STAMP ="20011"
VK_AMOUNT="5.00"
VK_CURR ="EUR"
VK_REF ="999"
VK_MSG ="COOP test. OÜ"
VK_RETURN ="https://somehost.ee/returnurl"
VK_CANCEL ="https://somehost.ee/cancelurl"
VK_DATETIME ="2018-03-12T09:53:14+0200"

The signature is calculated from a data string, which comprises the following elements: number of symbols in the parameter value, and the parameter value itself. The data string must include all the fields from the service description, which have an order number; fields without numbers (e.g. VK_LANG) are not included.

004 1012
003 008
008 testvpos
005 20011
004 5.00
003 EUR
003 999
017 COOP test. OÜ
029 https://somehost.ee/returnurl
029 https://somehost.ee/returnurl
024 2018-03-12T09:53:14+0200

In one string: 004101200300800 8testvpos005200110045.00003EUR003999017COOP test. OÜ029https://somehost.ee/returnurl029https://somehost.ee/returnurl0242018-03-12T09:53:14+0200
For example, if the parameter for VK_MSG was empty, it should still be added to the data string, using 000 as the number of symbols.

Query specifications

Payment services

Service 1011

A service assistant sends to the bank the data of a signed payment order, which the client cannot change in the internet bank. After a successful payment, query "1111" is prepared for the trader, and "1911" in case the payment was unsuccessful.

URL: https://i.cooppank.ee/pay

No.	Field name	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 query author (Shop ID)
4	VK_STAMP	20	Query ID
5	VK_AMOUNT	12	Payable amount
6	VK_CURR	3	Name of the currency: EUR
7	VK_ACC	34	Account number of the beneficiary
8	VK_NAME	70	Name of the beneficiary
9	VK_REF	35	Reference number of the payment order
10	VK_MSG	95	Explanation of the payment order
11	VK_RETURN	255	URL for response in case of a successful transaction
12	VK_CANCEL	255	URL for response in case of a transaction failure
13	VK_DATETIME	24	Date and time of query initiation in the DATETIME format
-	VK_MAC	700	Verification code i.e. signature
-	VK_ENCODING	12	Message encoding. UTF-8 or WINDOWS-1257 or ISO-8859-13
-	VK_LANG	3	Language of communication (EST, ENG or RUS)

Service 1012

A service assistant sends to the bank a client's request for a transaction. The name and account number of the beneficiary of the payment is taken from a contract between the bank and the service assistant. After a successful payment, query "1111" is prepared for the trader, and "1911" in case the payment was unsuccessful.

URL: https://i.cooppank.ee/pay

No.	Field name	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 query author (Shop ID)
4	VK_STAMP	20	Query ID
5	VK_AMOUNT	12	Payable amount
6	VK_CURR	3	Name of the currency: EUR
7	VK_REF	35	Reference number of the payment order
8	VK_MSG	95	Explanation of the payment order
9	VK_RETURN	255	URL for response in case of a successful transaction
10	VK_CANCEL	255	URL for response in case of a transaction failure
11	VK_DATETIME	24	Date and time of query initiation in the DATETIME format
-	VK_MAC	700	Verification code i.e. signature
-	VK_ENCODING	12	Message encoding. UTF-8 or WINDOWS-1257 or ISO-8859-13
-	VK_LANG	3	Language of communication (EST, ENG or RUS)

Service 1111

Used for responding about a transaction of a payment order within Estonia.

No.	Field name	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 query author (Shop ID)
4	VK_REC_ID	15	ID of the query recipient (Shop ID)
5	VK_STAMP	20	Query ID
6	VK_T_NO	20	Number of the payment order
7	VK_AMOUNT	12	Paid amount
8	VK_CURR	3	Name of the currency: EUR
9	VK_REC_ACC	34	Account number of the beneficiary
10	VK_REC_NAME	70	Name of the beneficiary
11	VK_SND_ACC	34	Account number of the remitter
12	VK_SND_NAME	70	Name of the remitter
13	VK_REF	35	Reference number of the payment order
14	VK_MSG	95	Explanation of the payment order
15	VK_T_DATETIME	24	Date and time of the payment order in the DATETIME format
-	VK_MAC	700	Verification code i.e. signature
-	VK_ENCODING	12	Message encoding. UTF-8 or WINDOWS-1257 or ISO-8859-13
-	VK_LANG	3	Language of communication (EST, ENG or RUS)
-	VK_AUTO	1	Y = a reply automatically sent by the bank. N = a reply together with moving the client to the website of the trader

Service 1911

Used for informing about a failed transaction.

No.	Field name	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 query author (Bank ID)
4	VK_REC_ID	15	ID of the query recipient (Shop ID)
5	VK_STAMP	20	Query ID
6	VK_REF	35	Reference number of the payment order
7	VK_MSG	95	Explanation of the payment order
-	VK_MAC	700	Verification code i.e. signature
-	VK_ENCODING	12	Message encoding. UTF-8 or WINDOWS-1257 or ISO-8859-13
-	VK_LANG	3	Language of communication (EST, ENG or RUS)
-	VK_AUTO	1	Y = a reply automatically sent by the bank. N = a reply together with moving the client to the website of the trader

If the VK_ENCODING field is missing, then the symbols in all the text fields of the reply that are in the ISO-8859-1 code table at a higher position than code 128, are converted as follows: Estonian special characters are converted into the underlying analogue (e.g. Ä->A and Š->S) and others are removed.

The server of the internet bank always attempts to send the reply from own server in the VK_AUTO='Y' mode, for cases when the session of the client is interrupted or the client does not return correctly to the trader's website.

Authentication services

Service 4011

A package sent by the trader for identification of the user. The service is open for traders, who have concluded the respective contract. Reply package code 3012.
Fields of the authentication query 4011:
URL: https://i.cooppank.ee/auth

No.	Field name	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 message author (partner)
4	VK_REPLY	4	Code of the expected reply package (3012)
5	VK_RETURN	255	Trader URL, where the reply is sent
6	VK_DATETIME	24	Time of generation of the message in the DATETIME format
7	VK_RID	30	Session identifier
-	VK_MAC	700	Verification code i.e. signature
-	VK_ENCODING	12	Message encoding. UTF-8 or WINDOWS-1257 or ISO-8859-13
-	VK_LANG	3	Language of communication (EST, ENG or RUS)

Service 3012

When service 4011 is used, a package with user information and the time of authentication (VK_DATETIME) is sent to the trader, which the trader should verify for security purposes.
Fields of the authentication reply 3012:

No.	Field name	Length	Description
1	VK_SERVICE	4	Service number (3012)
2	VK_VERSION	3	Used encryption algorithm (008)
3	VK_USER	16	Agreed identifier of the user
4	VK_DATETIME	24	Time of generation of the message in the DATETIME format
5	VK_SND_ID	15	ID of the message author (Bank ID)
6	VK_REC_ID	15	ID of the message recipient (partner)
7	VK_USER_NAME	140	Name of the user in the format Familyname, Firstnames
8	VK_USER_ID	20	Personal ID code of the user
9	VK_COUNTRY	2	Country of the ID code (two characters ISO 3166-1)
10	VK_OTHER	150	Other information about the user
11	VK_TOKEN	2	Identifier code of the means of authentication: 1- ID-card; 2- Mobile ID; 5- single-use codes (excl. PIN-calculator); 6- PIN-calculator; 7- password card
12	VK_RID	30	Session identifier
-	VK_MAC	700	Verification code i.e. signature
-	VK_ENCODING	12	Message encoding. UTF-8 or WINDOWS-1257 or ISO-8859-13
-	VK_LANG	3	Language of communication (EST, ENG or RUS)

A user turns to the bank. The bank requests the user to identify himself/herself. After positive entry of user credentials, the user is offered a possibility to use various banking services, including entry into the Portal.

After the user has informed the bank that s/he wishes to use the services of the Portal, the bank produces the message 3012, which is signed and forwarded to the Portal via the browser header of the user.

It should be noted that under this method the verification of the Time Stamp is somewhat different: unlike the previous method, the reference time is not sent in query 4012, but is generated by the bank. If the difference between the server times of the bank and the Portal becomes sufficiently broad, there may occur a situation that all entries, which have originated from the company, are cancelled. In order to avoid this and synchronise time, both the Portal and the Bank select one institution in the Internet, which offers the time standards service, whose core clock is deemed compulsory in compiling the time stamp of messages (VK_TIME and VK_DATE).

Service 4012

A package sent by the trader for identification of a user. The service is open for traders, who have concluded the respective contract. Reply package code 3013.

URL: https://i.cooppank.ee/auth

No.	Field name	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 message author (partner)
4	VK_REC_ID	15	ID of the message recipient (Bank)
5	VK_NONCE	50	Random nonce generated by the author of the query
6	VK_RETURN	255	Trader URL, where the reply is sent
7	VK_DATETIME	24	Time of generation of the message in the DATETIME format
8	VK_RID	30	Session identifier
-	VK_MAC	700	Verification code i.e. signature
-	VK_ENCODING	12	Message encoding. UTF-8 or WINDOWS-1257 or ISO-8859-13
-	VK_LANG	3	Language of communication (EST, ENG or RUS)

Service 3013

A copy of a nonce is forwarded to the trader.

Fields in the authentication reply 3013:

No.	Field name	Length	Description
1	VK_SERVICE	4	Service number (3013)
2	VK_VERSION	3	Used encryption algorithm (008)
3	VK_DATETIME	24	Time of generation of the message in the DATETIME format
4	VK_SND_ID	15	ID of the message author (Bank ID)
5	VK_REC_ID	15	ID of the message recipient (partner)
6	VK_NONCE	50	A copy of the queried nonce
7	VK_USER_NAME	140	Name of the user in the format Familyname, Firstnames
8	VK_USER_ID	20	Personal ID code of the user
9	VK_COUNTRY	2	Country of the ID code (two characters ISO 3166-1)
10	VK_OTHER	150	Other information about the user
11	VK_TOKEN	2	Identifier code of the means of authentication: 1- ID-card; 2- Mobile ID; 5- single-use codes (excl. PIN-calculator); 6- PIN-calculator; 7- password card
12	VK_RID	30	Session identifier
-	VK_MAC	700	Verification code i.e. signature
-	VK_ENCODING	12	Message encoding. UTF-8 or WINDOWS-1257 or ISO-8859-13
-	VK_LANG	3	Language of communication (EST, ENG or RUS)

** If the VK_ENCODING field is missing, then it is presumed that ISO-8859-13 is used for input, also the symbols in all the text fields of the reply that are in the ISO-8859-13 code table at a higher position than code 128, are converted as follows: Estonian special characters are converted into the underlying analogue (e.g. Ä->A and Š->S) and others are removed.

The Portal generates the message 4012 for the bank selected by the user, and signs it. At the same time, the generated message is saved in an interim table.

The generated and signed message 4012 is sent to the waiting user, displaying a button "Autendime", after which the user is guided to the internet bank.

The bank, after having verified the signature, asks the user to log in. When the user has successfully logged into the bank, the bank generated the reply message: 3013. The message is signed, like message 4012, and is sent to the user, after which the latter is guided back to the Portal.

The Portal verifies the signature of the sent message. If the signature is valid, it is checked, if reply 3013 has arrived for the previously sent message (4012) within a set time limit and then it is checked, if the personal ID code of the given user is in use. The Portal uses the personal ID code as the identifier of clients.