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 GET 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 the 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 009

Signature MAC009 (VK_MAC) is calculated using public key algorithm RSA and hash algorithm SHA512.

MAC009(x1,x2,..., xn):= RSA (SHA-512(p(x1) || x1 || p(x2) || x2 || ... || p(xn) || xn),d,n)

where:
|| is a string addition operation
x1, x2, …, xn are the query parameters (numbered in the specification)
p is a function of the length of the parameter. The length is a number in the form of a three-digit string
d on RSA salajane ekspone is the secret exponent of RSA nt
n is the RSA modulus

Drawing up a data string, using the service “1012“ as an example:

VK_SERVICE="1012"
VK_VERSION="009"
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
003 009
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:
004101200300900 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 (009)
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
-	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 (009)
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
-	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 (009)
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_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
-	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 (009)
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
-	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

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.

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 (009)
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
-	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.

No.	Field name	Length	Description
1	VK_SERVICE	4	Service number (3012)
2	VK_VERSION	3	Used encryption algorithm (009)
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; 9 - Smart-ID; 12 - Biometrics
12	VK_RID	30	Session identifier
-	VK_MAC	700	Verification code i.e. signature
-	VK_ENCODING	12	Message encoding. UTF-8
-	VK_LANG	3	Language of communication (EST, ENG or RUS)

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 (009)
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
-	VK_LANG	3	Language of communication (EST, ENG or RUS)

Service 3013

A copy of a nonce is forwarded to the trader.

No.	Field name	Length	Description
1	VK_SERVICE	4	Service number (3013)
2	VK_VERSION	3	Used encryption algorithm (009)
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; 9 - Smart-ID; 12 - Biometrics
12	VK_RID	30	Session identifier
-	VK_MAC	700	Verification code i.e. signature
-	VK_ENCODING	12	Message encoding. UTF-8
-	VK_LANG	3	Language of communication (EST, ENG or RUS)