COFlink Technical Specification

1. GENERAL

1.1. Consumer factoring requests are defined as HTTP POST requests with specified parameters are meant by. Every request contains a service number. Every request has a list of parameters and a processing algorithm. The requests from the Dealer to LHV Finance (LHVF) should be directed at the URL: https://www.lhv.ee/coflink.

2. COFLINK REQUESTS

2.1. Request 5011

NR	FIELD NAME	LENGTH	DESCRIPTION
1	VK_SERVICE	5	Query number (5011)
2	VK_VERSION	3	Encryption algorithm used (008)
3	VK_SND_ID	15	ID of the compiler of the message (Dealer)
4	VK_REC_ID	15	ID of the receiver of the message = “LHV”
5	VK_STAMP	20	A stamp generated by the composer
6	VK_DATA	4096	Contract data XML: <CofContractProductList> <CofContractProduct> <Name>LCD</Name> <Code>1122</Code> <Currency>EUR</Currency> <CostInclVatAmount>120</CostInclVatAmount> <CostVatPercent>20</CostVatPercent> </CofContractProduct> <ValidToDtime>2015-02-05T07:18:11+02:00</ValidToDtime> </CofContractProductList>
7	VK_RESPONSE	255	the URL to which the success response requests 5111 or 5113 will be sent to and user’s browser directed to
8	VK_RETURN	255	the URL where the user will be directed to when he/she has pressed the „Back to the dealer“ button
9	VK_DATETIME	25	Request initialization date and time in the ISO 8601 format in with second precision with the time zone info. Ex. 2015-02-05T07:18:11+02:00. Receiver of the request is ordered to control the value that is added to VK_DATEEIME field. Value can vary from the actual time ± 5 minutes.
10	VK_MAC	700	Check code or signature
-	VK_ENCODING	12	Message encoding. UTF-8 (default value), ISO-8859-1, or WINDOWS-1257
-	VK_LANG	3	Preferred language (EST or RUS)
-	VK_EMAIL	255	The client's e-mail address
-	VK_PHONE	25	The client's phone number (mandatory format: [+][country code][subscriber number], for instance - +37255667788)

The Dealer sends the signed shopping cart data to LHVF, which the client cannot change in the internet bank. After a successful payment the Dealer will receive the responding request “5111”. If it is not possible to give credit limit to customer Dealer will receive request “5113”.

Fields with the sequence number are mandatory.

The VK_DATA field XML descriptions from request “5011”

XML field name	Descrition
<CofContractProductList>	List of products in the shopping car
<CofContractProduct>	An item in the shopping cart
<Name>	Item's name (max 250 characters)
<Code>	Item's code (max 50 characters)
<Currency>	The currency used in the contract (3-digit ISO 4217 standard). Currently only Euros supported.
<CostInclVatAmount>	Item's cost with VAT (must be greater than 0)
<CostVatPercent>	Item cost's VAT percentage
<ValidToDtime>	Shopping cart's date and time of validity in the ISO 8601 format in with second precision with the time zone info. If your shopping cart does not expire you can enter any long time interval from today. Ex. 2015-02-05T07:18:11+02:00

2.2. Response 5111

Sent in case the contract has been signed.

NR	FIELD NAME	LENGTH	DESCRIPTION
1	VK_SERVICE	4	Query number (5111)
2	VK_VERSION	3	Encryption algorithm used (008)
3	VK_SND_ID	15	ID of the compiler of the message (LHVF)
4	VK_REC_ID	15	ID of the receiver of the message (Dealer)
5	VK_STAMP	20	Copy of the stamp from 5011
6	VK_ DATA	4096	Contract and client data as XML: <CoflinkSignedContract> <IdCode>38307070013</IdCode> <IdCodeIssuer>EE</IdCodeIssuer> <FullName></FullName> <ContractStatusCode>CONTRACT_SIGNED</ContractStatusCode> <ContractNumber>524557</ContractNumber> <ContractDownPaymentAmount>99</ContractDownPaymentAmount> <ContractFeeAmount>20</ContractFeeAmount> <CustomerEmail>john.doe@test.com</CustomerEmail> <CustomerPhone>55667788</CustomerPhone> <CustomerCountryCode>EE</CustomerCountryCode> <CustomerCity>Tallinn</CustomerCity> <CustomerStreetAddress>Tartu mnt 2</CustomerStreetAddress> <CustomerPostalCode></CustomerPostalCode> <SigningDtime>2015-02.05T07:18:11+02:00</SigningDtime> </CoflinkSignedContract>
7	VK_DATETIME	25	Request initialization date and time in the ISO 8601 format in with second precision with the time zone info. Ex. 2015-02-05T07:18:11+02:00
8	VK_MAC	700	Check code or signature
-	VK_ENCODING	12	Message encoding. UTF-8 (default value), ISO-8859-1, or WINDOWS-1257
-	VK_LANG	3	Preferred language (EST or RUS)

Fields with the sequence number are mandatory

The VK_DATA field XML descriptions from requests "5111"

XML field name	Description
<CofContract>	The contract between the client and LHVF
<IdCode>	The applicant's ID code
<IdCodeIssuer>	The applicant's ID code's issuer country's 2 digit code (ISO 3166-1 alpha-2)
<FullName>	The applicant's full name
<ContractStatusCode>	The contract's status: READY_FOR_CONTRACT_SIGNING, CONTRACT_SIGNED
<ContractNumber>	Contract number

<ContractDownPaymentAmount>	The down payment amount of the contract
<ContractFeeAmount>	The contract fee amount
<CustomerEmail>	The applicant's e-mail address
<CustomerPhone>	The applicant's phone number
<CustomerCountryCode>	The applicant's country's 2 digit code (ISO 3166-1 alpha-2)
<CustomerCity>	The applicant's city of residence
<CustomerStreetAddress>	The applicant's home address
<CustomerPostalCode>	The applicant's home address' postal code
<SigningDtime>	The date and time of signing in the ISO 8601 format in with second precision with the time zone info. Ex. 2015-02-05T07:18:11+02:00

2.3. Response 5113

This response is given if limit to client is not given.

Fields with the sequence number are mandatory

NR	FIELD NAME	LENGTH	DESCRIPTION
1	VK_SERVICE	4	Query number (5113)
2	VK_VERSION	3	Encryption algorithm used (008)
3	VK_SND_ID	15	ID of the compiler of the message (LHVF)
4	VK_REC_ID	15	ID of the receiver of the message (Dealer)
5	VK_STAMP	20	Copy of the stamp
6	VK_DATA	4096	Contract and client data as XML: <CoflinkContract> <Message>Application was rejected</Message> </CoflinkContract>
7	VK_DATETIME	25	Request initialization date and time in the ISO 8601 format in with second precision with the time zone info. Ex. 2015-02-05T07:18:11+02:00
8	VK_MAC	700	Check code or signature
-	VK_ENCODING	12	Message encoding. UTF-8 (default value), ISO-8859-1, or WINDOWS-1257
-	VK_LANG	3	Preferred language (EST or RUS)

3. PUBLIC KEYS

3.1. LHV accepts certificate requests or self-signed certificates created based on the public key. Certificates/requests will be swapped during the signing of the contract. We use the X.509 standard-compliant .PEM format certificates/requests i.e. the content is in BASE64 and between

—BEGIN CERTIFICATE REQUEST/CERTIFICATE — and *—END CERTIFICATE REQUEST/CERTIFICATE —*

The minimum required length of the private key generated by the client is 1024 bits.

3.2. The keys can be generated using the openssl utility. When creating the key we suggest to follow these criteria:

i Certificate signature algorithm: sha256 (preferred) or sha1

ii Private and public key: RSA (min 1024 bits)

iii Certificate expiration date: not over 10 years

4. FINDING THE VK_MAC SIGNATURE

4.1. The calculations of the electronic signature VK_MAC used in the requests take place with an agreed upon algorithm. The version of the algorithm is set by the parameter VK_VERSION. 008 is the only

currently available version. The signature VK_MAC will be forwarded in a BASE64 encoding, VK_MAC(MAC008) will be calculated using the RSA public key algorithm and the SHA-1 hash algorithm. MAC008(x1,x2,…,xn) := RSA(SHA-1(p(x1)|| x1|| p(x2)|| x2 || … ||p(xn)||xn), d, n)

i x1, x2, …, xn are the request parameters, excluding VK_MAC, VK_ENCODING, VK_LANG

ii p is a function of the length of the parameters in symbols. The length is formatted as a 3-or-more character string. So length 1 is “001” and 12625 is “12625”. Empty fields have a length of "000".

iii d is the secret component of RSA

iv n is an RSA modulus

v || - string addition function

For example if the parameters are:

VK_SERVICE=”5011”

VK_VERSION=”008”

VK_SND_ID=”TEST”

VK_REC_ID=”LHV”

VK_STAMP=”1234567890”

VK_DATA=”<CofContractProductList>

<CofContractProduct>

<Name>Product Name</Name>

<Code>12345abcde</Code>

<Currency>EUR</Currency>

<CostInclVatAmount>500</CostInclVatAmount>

<CostVatPercent>20</CostVatPercent>

</CofContractProduct>

<ValidToDtime>2015-07-11T23:59:59+03:00</ValidToDtime>

</CofContractProductList>”

VK_RESPONSE=”https://testtest.ee/coflinkreturn.php”

VK_RETURN=”https://testtest.ee/coflinkreturn.php”

VK_DATETIME=“2015-07-10T12:08:13+03:00“

VK_EMAIL=““ – (not mandatory, left empty)

VK_PHONE=“+37255667788“ – (not mandatory, left empty)

Signature is calculated form the data which consist the above mentioned elements (parameter name length and value).

NB! When forming the string, these parameters are not taken into account: VK_MAC, VK_ENCODING, VK_LANG, the length of empty fields is “000”.

NB! When forming the string, using UTF-8 encoding (VK_ENCODING=UTF-8) and parameters contain two byte symbols (for example Ä; Ö; Õ; Ü), then we still must take into account the number of symbols as a length, not the number of bytes. For example 003ÕUN, not 004ÕUN.

0045011
003008
004TEST
003LHV
0101234567890
293<CofContractProductList><CofContractProduct><Name>Product Name</Name><Code>12345abcde</Code><Currency>EUR</Currency><CostInclVatAmount>400</CostInclVatAmount><CostVatPercent>20</CostVatPercent></CofContractProduct><ValidToDtime>2015-07-11T23:59:59+03:00</ValidToDtime></CofContractProductList>
037https://testtest.ee/coflinkreturn.php
037https://testtest.ee/coflinkreturn.php
0252015-07-10T12:08:13+03:00
000
012+37255667788

In one row:
0045011003008004TEST003LHV0101234567890293<CofContractProductList><CofContractProduct><Name>Product Name</Name><Code>12345abcde</Code><Currency>EUR</Currency><CostInclVatAmount>400</CostInclVatAmount><CostVatPercent>20</CostVatPercent></CofContractProduct><ValidToDtime>2015-07-11T23:59:59+03:00</ValidToDtime></CofContractProductList>037https://testtest.ee/coflinkreturn.php037https://testtest.ee/coflinkreturn.php0252015-07-10T12:08:13+03:00000012+37255667788

5. TESTING

i To test the integration with Coflink a parameter must be added to the VK_SERVICE 5011 POST request URL: “testRequest=true”. Ex. https://www.lhv.ee/coflink?testRequest=true

ii The user’s request will be validated and she/he will be directed to the test page https://www.lhv.ee/coflink/testrequest, where she/he can choose with a click of a button which testresponse to generate: 5111 or 5113.

iii The response will be sent to the URL taken from the initial 5011 Coflink request’s VK_ RESPONSE parameter.