Järelmaksulingi tehniline spetsifikatsioon

1. ÜLDINE

1.1. Järelmaksulingi päringute all on mõeldud HTTP POST päringut spetsifitseeritud parameetritega. Iga päring sisaldab endas teenuse numbrit. Igale teenusele vastab oma loetelu parameetritest ja päringu käsitlemise algoritm. Päringud Kaupmehelt LHV Finance'ile (LHVF) suunatakse URLile: https://www.lhv.ee/coflink.

2. COFLINK PÄRINGUD

2.1. Päring 5011

Kaupmees saadab LHVF-i allkirjastatud ostukorvi andmed, mida Klient internetipangas muuta ei saa. Peale edukat makset koostatakse Kaupmehele vastuspäring "5111". Kui Kliendile ei ole võimalik limiiti väljastada, saadetakse Kaupmehele vastusepäring „5113".

Kohustuslikud väljad on märgitud järjekorranumbriga.

JRK	VÄLJA NIMI	PIKKUS	KIRJELDUS
1	VK_SERVICE	4	Teenuse number (5011)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_SND_ID	15	Päringu koostaja (Kaupmehe) ID
4	VK_REC_ID	15	Päringu vastuvõtja ID = „LHV"
5	VK_STAMP	20	Päringu koostaja genereeritud tempel
6	VK_DATA	4096	Päringu lisainfo XML-na <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	URL, kuhu saadetakse vastuspäring 5111 või 5113 ja kuhu suunatakse kasutaja brauser
8	VK_ RETURN	255	URL, kuhu suunatakse kasutaja, kes on klikkinud linki „Tagasi kaupmehe juurde"
9	VK_DATETIME	25	Päringu algatamise kuupäev ja kellaaeg ISO 8601 formaadis sekundi täpsusega koos ajatsooni infoga. Nt. 2015-02-05T07:18:11+02:00. Päringu saaja on kohustatud kontrollima VK_DATETIME väljal olevat väärtust, kusjuures välja väärtus tohib erineda kontrollimise hetkel kehtivast kellaajast maksimaalselt ± 5 minutit. Kaupmees vastutab oma serveri kellaaja õigsuse eest.
10	VK_MAC	700	Kontrollkood e. allkiri
-	VK_ENCODING	12	Sõnumi kodeering. UTF-8 (vaikeväärtus), ISO 8859-1 või WINDOWS-1257

-	VK_LANG	3	Soovitav suhtluskeel (EST, RUS)
-	VK_EMAIL	255	Kliendi e-mail
-	VK_PHONE	25	Kliendi telefoninumber (kujul: +<riigi suunakood><telefoninumber> - nt +37255667788)

Päringu „5011“ VK_DATA välja XMLi tagide kirjeldused

XML field name	Kirjeldused
<CofContractProductList>	Ostukorvi toodete nimekiri
<CofContractProduct>	Ostukorvi toode
<Name>	Toote nimi (maks. 250 tähemärki)
<Code>	Tootekood (maks. 50 tähemärki)
<Currency>	Lepingus kasutatav valuuta (3-kohaline ISO 4217 standard). Hetkel toetatud ainult Eurod.
<CostInclVatAmount>	Toote maksumus koos käibemaksuga (peab olema suurem kui 0 ja arvu murdosa tähistatakse punktiga ja murdosa pikkuseks võib olla kuni 2 numbrit)
<CostVatPercent>	Toote käibemaksu protsent
<ValidToDtime>	Ostukorvi kehtivusaeg ja -kuupäev ISO 8601 standardi formaadis sekundi täpsusega ja ajatsooni infoga. Kui ostukorvil puudub kehtivusaeg võib sisestada tänasele lisatud suvalise pika ajaintervalli. „Kehtib kuni“ aeg peab olema tulevikus. Nt. 2015-02-05T07:18:11+02:00

2.2. Vastuspäring 5111
Vastatakse juhul, kui leping on sõlmitud.
Kohustuslikud väljad on märgitud järjekorranumbriga.

JRK	VÄLJA NIMI	PIKKUS	KIRJELDUS
1	VK_SERVICE	4	Teenuse number (5111)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_SND_ID	15	Päringu koostaja (LHVF) ID
4	VK_REC_ID	15	Päringu vastuvõtja (Kaupmehe) ID
5	VK_STAMP	20	Päringus olnud templi koopia
6	VK_DATA	4096	Lepingu ja kliendi lisainfo XMLina <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	Maksekorralduse kuupäev ja kellaaeg ISO 8601 formaadis sekundi täpsusega koos ajatsooni infoga. Nt. 2015-02-05T07:18:11+02:00
8	VK_MAC	700	Kontrollkood e. allkiri
-	VK_ENCODING	12	Sõnumi kodeering. UTF-8 (vaikeväärtus), ISO 8859-1 või WINDOWS-1257
-	VK_LANG	3	Soovitav suhtluskeel (EST, RUS)

Päringute „5111 VK_DATA välja XMLi tagide kirjeldused

XML field name	Kirjeldus
<CofContract>	Kliendi ja LHVF-i vaheline leping
<IdCode>	Taotleja isikukood

<IdCodeIssuer>	Taotleja isikukoodi väljastajariigi 2-kohaline kood (ISO 3166-1 alpha-2)
<FullName>	Taotleja täisnimi
<ContractStatusCode>	Lepingu staatus: READY_FOR_CONTRACT_SIGNING, CONTRACT_SIGNED
<ContractNumber>	Lepingu number
<ContractDownPaymentAmount>	Lepingu sissemakse
<ContractFeeAmount>	Lepingutasu
<CustomerEmail>	Taotleja e-mailiaadress
<CustomerPhone>	Taotleja telefoninumber
<CustomerCountryCode>	Taotleja riigi 2-kohaline kood (ISO 3166-1 alpha-2)
<CustomerCity>	Taotleja linn
<CustomerStreetAddress>	Taotleja aadress
<CustomerPostalCode>	Taotleja aadressi postiindeks
<SigningDtime>	Lepingu allkirjastamise kellaaeg ja kuupäev ISO 8601 standardi formaadis sekundi täpsusega ja ajatsooni infoga. Nt. 2015-02-05T07:18:11+02:00

2.3. Vastupäring 5113

Vastatakse juhul, Kui Kliendile ei ole võimalik limiiti väljastada.

Kohustuslikud väljad on märgitud järjekorranumbriga.

JRK	VÄLJA NIMI	PIKKUS	KIRJELDUS
1	VK_SERVICE	4	Teenuse number (5113)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_SND_ID	15	Päringu koostaja (LHVF) ID
4	VK_REC_ID	15	Päringu vastuvõtja (Kaupmehe) ID
5	VK_STAMP	20	Päringus olnud templi koopia
6	VK_DATA	4096	Lepingu ja kliendi lisainfo XMLina

			<CoflinkContract> <Message>Application was rejected</Message> </CoflinkContract>
7	VK_DATETIME	25	Maksekorralduse kuupäev ja kellaaeg ISO 8601 formaadis sekundi täpsusega koos ajatsooni infoga. Nt. 2015-02-05T07:18:11+02:00
8	VK_MAC	700	Kontrollkood e. allkiri
-	VK_ENCODING	12	Sõnumi kodeering. UTF-8 (vaikeväärtus), ISO 8859-1 või WINDOWS-1257
-	VK_LANG	3	Soovitav suhtluskeel (EST, RUS)

Päringu „5113“ VK_DATA välja XMLi tagide kirjeldused

XML field name	Kirjeldus
<CoflinkContract>	Kliendi ja LHVF-i vaheline leping
<Message>	Sõnum lepingu staatuse kohta. Antud päringu puhul ainuvõimalik: „Application was rejected“

3. AVALIKUD VÕTMED

3.1. LHV aktsepteerib avaliku võtme alusel loodud sertifikaadipäringut või *self-signed* sertifikaati. Sertifikaatide/päringute vahetamine toimub lepingu sõlmimisel. Kasutame X.509 standardile vastavaid .PEM formaadis sertifikaate/päringuid st. sisu on BASE64 kodeeringus ning märgendite:

—BEGIN CERTIFICATE REQUEST/CERTIFICATE — ja *—END CERTIFICATE REQUEST/CERTIFICATE —* vahel.

Kliendi poolt genereeritud salajase võtme minimaalne pikkus peab olema 1024 bitti.

3.2. Sertifikaate saab luua kasutades openssl utiliiti. Sertifikaadi loomisel soovitame lähtuda järgmistest tingimustest:

i Sertifikaadi signatuuri algoritm: sha256 (eelistatud) või sha1

ii Salajane ja avalik võti: RSA (min 1024 bits)

iii Sertifikaadi kehtivusaeg: mitte üle 10 aasta

4. KONTROLLKOODI VK_MAC LEIDMINE

4.1. Päringutes kasutatava elektroonse allkirja VK_MAC arvutus toimub kokkuleppelise algoritmi alusel. Algoritmi versiooni määrab päringu parameeter VK_VERSION. Hetkel on kasutusel ainult versioon 008. Allkiri VK_MAC edastatakse päringutes BASE64 kodeerituna, VK_MAC(MAC008) arvutatakse kasutades avaliku võtme algoritmi RSA ning räsialgoritmi SHA-1. MAC008(x1,x2,…,xn) := RSA(SHA-1(p(x1)|| x1|| p(x2)|| x2 || … ||p(xn)||xn), d, n)

i x1, x2, …, xn on päringu kohustuslikud parameetrid, v.a. VK_MAC, VK_ENCODING, VK_LANG

ii p on funktsioon parameetri pikkusest sümbolites. Pikkus on formeeritud kolme- või enama kohalisena: 0-999 - kolm kohta, ning üle 999 - nii nagu on stringi kujul. Ehk siis pikkus 1 - "001", 12625 – “ 12625“. Tühjade väljade pikkus on "000".

iii d on RSA salajane eksponent

iv n on RSA modulus

v || - stringide liitmistehe

Näiteks, võtame päringu järgmiste parameetritega:

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=““ – (Vabatahtlik väli. Jätame hetkel näitena tühjaks)
VK_PHONE=“+37255667788“ – (vabatahtlik väli)

Allkiri arvutatakse andmereast, mis koosneb järgmistest elementidest (parameetri väärtuse sümbolite arv ja

parameetri väärtus ise).

NB! Päringu stringi koostamisel ei arvestata järgmiste parameetritega: VK_MAC, VK_ENCODING, VK_LANG, ning tühjade väljade pikkus on "000".

NB! Kui kaupmees kasutab paketis kodeeringut UTF-8 (VK_ENCODING=UTF-8) ja paketis sisalduvad kahebaidised

sümbolid (näiteks täpitähed), siis allkirja arvutamise andmereas (data string) on parameetri väärtuse pikkuseks

sümbolite arv stringis, mitte baitide arv. Näiteks 003ÕUN, mitte 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

Ühes reas:
0045011003008004TEST003LHV0101234567890293<CofContractProductList><CofContractProduct><Name>Product Name</Name><Code>12345abcde</Code><Currency>EUR</Currency><CostInclVatAmount>400</C

ostInclVatAmount><CostVatPercent>20</CostVatPercent></CofContractProduct><ValidToDtime>2015
-07-
11T23:59:59+03:00</ValidToDtime></CofContractProductList>037https://testtest.ee/coflinkreturn.php0
37https://testtest.ee/coflinkreturn.php0252015-07-10T12:08:13+03:00000012+37255667788

5. TESTIMINE

i Integratsiooni testimiseks Coflinkiga tuleb VK_SERVICE 5011 POST päringu URL-le lisada parameeter „testRequest=true“.

Nt. https://www.lhv.ee/coflink?testRequest=true

ii Kasutaja päring valideeritakse ja suunatakse testlehele https://www.lhv.ee/coflink/testrequest, kus saab nupuvajutusega valida testvastuseks saadetava response’i: 5111 või 5113.

iii Vastupäring saadetakse URL-le, mis on võetud esialgse Coflinki päringu VK_ RESPONSE parameetrist.