Pangalingi tehniline spetsifikatsioon

Päringud

Käesolevas dokumendis on välja toodud päringute spetsifikatsioonid, milles igale teenusele vastab oma loetelu parameetritest. Toimiva teenuse koostamiseks ei tohi lisada ühtegi parameetrit, mida pole spetsifikatsioonis kirjas ja tuleb järgida dokumendis välja toodud juhiseid.

- Päringutes esitatud summades on komakohad ja sendid eristatud punktiga "." Tuhandete eraldajat ei kasutata.
- Kuupäevad ja kellaajad esitatakse DATETIME formaadis nt 2018-03-12T09:53:14+0200 sekundi täpsusega koos ajatsooniga. Päringu saaja on kohustatud kontrollima DATETIME väljal olevat väärtust, kusjuures välja väärtus tohib erineda kontrollimise hetkel kehtivast kellaajast maksimaalselt ± 5 minutit.
- Välja väärtuse pikkus ei tohi ületada spetsifikatsioonis ettenähtut. Pikkuse ületamisel päringut ei töödelda. Välja väärtuse pikkused on sümbolites (mitte baitides). Välja väärtus võib olla lühem kui maksimaalne pikkus lubab, puuduvaid kohti ei täideta.
- Päring-vastuse vahetamiseks kasutatakse HTTP POST meetodit.
- Spetsifikatsioonile mittevastavatele päringutele vastatakse veateatega.
- Väljal VK_RETURN ei ole lubatud kasutada päringutes kasutatavaid välja nimesid (VK_...).
- Andmete vahetamiseks kasutatakse kodeeringut (VK_ENCODING), millest Coop pangalink toetab UTF-8 (vaikimisi) ja ISO-8859-1 kodeeringut. Pangalingi probleemideta toimimiseks tuleb veenduda, et kõik teenusega seotud programmid kasutaks sama kodeeringut.

Päringuid võib jagada:
1. algataja põhjal:
   - kaupmehe või panga päringuteks.
2. vastuse põhjal:
   - vastust nõudvateks või vastust mitte nõudvateks.
3. otstarbe põhjal:
   - 1xxx – maksete algatamine või 4xxx – autentimispäringud

Kontrollkoodi VK_MAC leidmine versiooni 008 alusel

Päringutes kasutatava elektroonse allkirja, VK_MAC, kontroll toimub kokkuleppelise algoritmi, VK_VERSION, alusel.

Kodeerimine VK_VERSION=008 puhul:

VK_MAC arvutatakse vastavalt RSA algoritmile ning viiakse seejärel üle BASE64 kodeeringusse. VK_MAC väärtus arvutatakse kasutades avaliku võtme algoritmi RSA. Arvestatakse ka tühjade väljade pikkusi – “000”. Ei signeerita päringute järjekorrastamata lisaväljasid.

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

kus:

|| on stringi liitmise tehe
x1, x2, …, xn on päringu parameetrid
p on funktsioon parameetri pikkusest. Pikkus on number kolmekohalise stringi kujul
d on RSA salajane eksponent
n on RSA modulus

Andmerea koostamine teenuse „1012“ näitel:
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"

Allkiri arvutatakse andmereast (data string), mis koosneb järgnevatest elementidest – parameetri väärtuse sümbolite arv ja parameetri väärtus ise. Andmereas peavad olema kõik teenuse kirjelduses järjekorranumbrit omavad väljad, numbriteta (nt VK_LANG) sinna ei kuulu.

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

Ühes reas: 0041012003008008testvpos005200110045.00003EUR003999017COOP test. OÜ029https://somehost.ee/returnurl029https://somehost.ee/returnurl0242018-03-12T09:53:14+0200
Kui näiteks VK_MSG parameeter oleks tühi, siis tuleb see ikkagi lisada andmeritta, kasutades sümbolite arvuna 000.

Päringute spetsifikatsioonid

Makseteenused

Teenus 1011

Teenindaja saadab panka allkirjastatud maksekorralduse andmed, mida klient internetipangas muuta ei saa. Peale edukat makset koostatakse kaupmehele päring “1111”, ebaõnnestunud makse puhul “1911”.
URL: https://i.cooppank.ee/pay

Jrk.	Välja nimi	Pikkus	Kirjeldus
1	VK_SERVICE	4	Teenuse number (1011)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_SND_ID	15	Päringu koostaja ID (Kaupluse ID)
4	VK_STAMP	20	Päringu ID
5	VK_AMOUNT	12	Maksmisele kuuluv summa
6	VK_CURR	3	Valuuta nimi: EUR
7	VK_ACC	34	Saaja konto number
8	VK_NAME	70	Saaja nimi
9	VK_REF	35	Maksekorralduse viitenumber
10	VK_MSG	95	Maksekorralduse selgitus
11	VK_RETURN	255	URL, kuhu vastatakse edukal tehingu sooritamisel
12	VK_CANCEL	255	URL, kuhu vastatakse ebaõnnestunud tehingu puhul
13	VK_DATETIME	24	Päringu algatamise kuupäev ja kellaaeg DATETIME formaadis
-	VK_MAC	700	Kontrollkood e. allkiri
-	VK_ENCODING	12	Sõnumi kodeering. UTF-8 või WINDOWS-1257 või ISO-8859-13
-	VK_LANG	3	Soovitav suhtluskeel (EST, ENG või RUS)

Teenus 1012

Teenindaja saadab panka kliendi sooviavalduse tehingu tegemiseks. Makse saaja nimi ja konto number võetakse panga ja teenindaja vahelisest lepingust. Peale edukat makset koostatakse kaupmehele päring “1111”, ebaõnnestunud makse puhul “1911”.
URL: https://i.cooppank.ee/pay

Jrk.	Välja nimi	Pikkus	Kirjeldus
1	VK_SERVICE	4	Teenuse number (1012)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_SND_ID	15	Päringu koostaja ID (Kaupluse ID)
4	VK_STAMP	20	Päringu ID
5	VK_AMOUNT	12	Maksmisele kuuluv summa
6	VK_CURR	3	Valuuta nimi: EUR
7	VK_REF	35	Maksekorralduse viitenumber
8	VK_MSG	95	Maksekorralduse selgitus
9	VK_RETURN	255	URL, kuhu vastatakse edukal tehingu sooritamisel
10	VK_CANCEL	255	URL, kuhu vastatakse ebaõnnestunud tehingu puhul
11	VK_DATETIME	24	Päringu algatamise kuupäev ja kellaaeg DATETIME formaadis
-	VK_MAC	700	Kontrollkood e. allkiri

-	VK_ENCODING	12	Sõnumi kodeering. UTF-8 või WINDOWS-1257 või ISO-8859-13
-	VK_LANG	3	Soovitav suhtluskeel (EST, ENG või RUS)

Teenus 1111
Kasutatakse vastamiseks Eesti-sisese maksekorralduse toimumisest.

Jrk.	Välja nimi	Pikkus	Kirjeldus
1	VK_SERVICE	4	Teenuse number (1111)
2	VK_VERSION	3	Kasutatav krüptoalgoritm 008
3	VK_SND_ID	15	Päringu koostaja ID (Panga ID)
4	VK_REC_ID	15	Päringu vastuvõtja ID (Kaupluse ID)
5	VK_STAMP	20	Päringu ID
6	VK_T_NO	20	Maksekorralduse number
7	VK_AMOUNT	12	Makstud summa
8	VK_CURR	3	Valuuta nimi: EUR
9	VK_REC_ACC	34	Saaja konto number
10	VK_REC_NAME	70	Saaja nimi
11	VK_SND_ACC	34	Maksja konto number
12	VK_SND_NAME	70	Maksja nimi
13	VK_REF	35	Maksekorralduse viitenumber
14	VK_MSG	95	Maksekorralduse selgitus
15	VK_T_DATETIME	24	Maksekorralduse kuupäev ja kellaaeg DATETIME formaadis
-	VK_MAC	700	Kontrollkood e. allkiri
-	VK_ENCODING	12	Sõnumi kodeering. UTF-8 või WINDOWS-1257 või ISO-8859-13
-	VK_LANG	3	Soovitav suhtluskeel (EST, ENG või RUS)
-	VK_AUTO	1	Y = panga poolt automaatselt saadetud vastus. N = vastus kliendi liikumisega kaupmehe lehele

Teenus 1911
Kasutatakse ebaõnnestunud tehingust teatamiseks.

Jrk.	Välja nimi	Pikkus	Kirjeldus
1	VK_SERVICE	4	Teenuse number (1911)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_SND_ID	15	Päringu koostaja ID (Panga ID)
4	VK_REC_ID	15	Päringu vastuvõtja ID (Kaupluse ID)
5	VK_STAMP	20	Päringu ID
6	VK_REF	35	Maksekorralduse viitenumber
7	VK_MSG	95	Maksekorralduse selgitus
-	VK_MAC	700	Kontrollkood e. allkiri
-	VK_ENCODING	12	Sõnumi kodeering. UTF-8 või WINDOWS-1257 või ISO-8859-13
-	VK_LANG	3	Soovitav suhtluskeel (EST, ENG või RUS)
-	VK_AUTO	1	Y = panga poolt automaatselt saadetud vastus. N = vastus kliendi liikumisega kaupmehe lehele

Juhul kui VK_ENCODING väli puudub, siis teisendatakse kõikides vastuse tekstiväljades ISO-8859-1 kooditabelis kõrgemal kui kood 128 olevad sümbolid järgnevalt: eesti keele täpitähed vastavateks täppideta analoogiks (nt Ä->A ja Š->S) ja muud eemaldatakse.

Internetipanga server püüab alati oma serverist saata ka vastuse režiimiga VK_AUTO='Y', seda juhtudeks kui kliendi seanss katkeb või klient ei liigu korrektselt tagasi kaupmehe veebilehekülje.

Autentimisteenused

Teenus 4011

Kaupmehe poolt saadetav pakett kasutaja tuvastamiseks. Teenus on avatud vastava lepingu sõlminud kaupmeestele. Vastuspaketi kood 3012.
Autentimispäringu 4011 väljad:
URL: https://i.cooppank.ee/auth

Jrk.	Välja nimi	Pikkus	Kirjeldus
1	VK_SERVICE	4	Teenuse number (4011)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_SND_ID	15	Sõnumi koostaja (partneri) ID
4	VK_REPLY	4	Oodatava vastuspaketi kood (3012)
5	VK_RETURN	255	Kaupmehe URL, kuhu vastatakse
6	VK_DATETIME	24	Sõnumi genereerimise aeg DATETIME formaadis
7	VK_RID	30	Sessiooniga seotud identifikaator
-	VK_MAC	700	Kontrollkood e. allkiri
-	VK_ENCODING	12	Sõnumi kodeering. UTF-8 või WINDOWS-1257 või ISO-8859-13
-	VK_LANG	3	Soovitav suhtluskeel (EST, ENG või RUS)

Teenus 3012

Teenus 4011 kasutamisel saadetakse kaupmehele pakett kasutaja infoga ning autentimise aeg (VK_DATETIME), mida tuleb kaupmehe poolt turvalisuse kaalutlusel kontrollida.
Autentimisvastuse 3012 väljad:

Jrk.	Välja nimi	Pikkus	Kirjeldus
1	VK_SERVICE	4	Teenuse number (3012)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_USER	16	Kokkuleppeline kasutaja identifikaator
4	VK_DATETIME	24	Sõnumi genereerimise aeg DATETIME formaadis
5	VK_SND_ID	15	Sõnumi koostaja ID (Panga ID)
6	VK_REC_ID	15	Sõnumi saaja (partneri) ID
7	VK_USER_NAME	140	Kasutaja nimi, kujul Perenimi, Eesnimed
8	VK_USER_ID	20	Kasutaja isikukood
9	VK_COUNTRY	2	Isikukoodi riik (kahetäheline ISO 3166-1)
10	VK_OTHER	150	Muu info kasutaja kohta
11	VK_TOKEN	2	Autentimisvahendi identifikaatori kood: 1- ID-kaart; 2- Mobiil-ID; 5- ühekordsed koodid (v.a. PIN-kalkulaator); 6- PIN-kalkulaator; 7- korduvkasutusega kaart

12	VK_RID	30	Sessiooniga seotud identifikaator
-	VK_MAC	700	Kontrollkood e. allkiri
-	VK_ENCODING	12	Sõnumi kodeering. UTF-8 või WINDOWS-1257 või ISO-8859-13
-	VK_LANG	3	Soovitav suhtluskeel (EST, ENG või RUS)

Kasutaja pöördub panka. Pank palub kasutajal ennast identifitseerida. Pärast positiivset kasutajatunnuste sisestamist pakutakse kasutajale võimalust kasutada erinevaid pangateenuseid, millest üks on sisenemine Portaali.

Pärast seda, kui kasutaja on teavitanud panka, et ta soovib kasutada Portaali teenuseid, produtseerib pank sõnumi 3012, mis signeeritakse ja saadetakse kasutaja brauseri päise kaudu edasi Portaali.

Peab siiski märkima, et Ajapitseri kontrollimine käib selles meetodis mõnevõrra teistmoodi: erinevalt eelmisest meetodist, ei saadeta kontrollaega päringuga 4012, vaid selle genereerib pank. Kui panga ja Portaali serverikellaaegade erinevus läheb piisavalt suureks, siis võib tekkida olukord, et tühistatakse kõik sisenemised, mis on saabunud sellest ettevõttest. Et seda vältida, valivad Portaal ja Pank aja sünkroniseerimiseks ühe Internetis ajastandardi teenust pakkuvatest institutsioonidest, kelle tuumakella loetakse sõnumi ajapitseri (VK_TIME ja VK_DATE) koostamisel kohustuslikuks.

Teenus 4012

Kaupmehe poolt saadetav pakett kasutaja tuvastamiseks. Teenus on avatud vastava lepingu sõlminud kaupmeestele. Vastuspaketi kood 3013
URL: https://i.cooppank.ee/auth

Jrk.	Välja nimi	Pikkus	Kirjeldus
1	VK_SERVICE	4	Teenuse number (4012)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_SND_ID	15	Sõnumi koostaja (partneri) ID
4	VK_REC_ID	15	Sõnumi saaja (panga) ID
5	VK_NONCE	50	Päringu koostaja poolt genereeritud juhuslik nonss
6	VK_RETURN	255	Kaupmehe URL, kuhu vastatakse
7	VK_DATETIME	24	Sõnumi genereerimise aeg DATETIME formaadis
8	VK_RID	30	Sessiooniga seotud identifikaator
-	VK_MAC	700	Kontrollkood e. allkiri
-	VK_ENCODING	12	Sõnumi kodeering. UTF-8 või WINDOWS-1257 või ISO-8859-13
-	VK_LANG	3	Soovitav suhtluskeel (EST, ENG või RUS)

Teenus 3013

Kaupmehele edastatakse nonssi koopia
Autentimisvastuse 3013 väljad:

Jrk.	Välja nimi	Pikkus	Kirjeldus
1	VK_SERVICE	4	Teenuse number (3013)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_DATETIME	24	Sõnumi genereerimise aeg DATETIME formaadis
4	VK_SND_ID	15	Sõnumi koostaja ID (Panga ID)
5	VK_REC_ID	15	Sõnumi saaja (partneri) ID
6	VK_NONCE	50	Päringus olnud nonssi koopia
7	VK_USER_NAME	140	Kasutaja nimi, kujul Perenimi, Eesnimed

8	VK_USER_ID	20	Kasutaja isikukood
9	VK_COUNTRY	2	Isikukoodi riik (kahetäheline ISO 3166-1)
10	VK_OTHER	150	Muu info kasutaja kohta
11	VK_TOKEN	2	Autentimisvahendi identifikaatori kood: 1- ID-kaart; 2- Mobiil-ID; 5- ühekordsed koodid (v.a. PIN-kalkulaator); 6- PIN-kalkulaator; 7- korduvkasutusega kaart
12	VK_RID	30	Sessiooniga seotud identifikaator
-	VK_MAC	700	Kontrollkood e. allkiri
-	VK_ENCODING	12	Sõnumi kodeering. UTF-8 või WINDOWS-1257 või ISO-8859-13
-	VK_LANG	3	Soovitav suhtluskeel (EST, ENG või RUS)

** Juhul kui VK_ENCODING väli puudub, siis eeldatakse, et sisendis on ISO-8859-13 lisaks teisendatakse kõikides vastuseväljades ISO-8859-13 kooditabelis kõrgemal kui kood 128 olevad sümbolid järgnevalt: eesti keele täpitähed vastavateks täppideta analoogiks (nt Ä->A ja Š->S) ja muud eemaldatakse.

Portaal genereerib kasutaja poolt valitud panga jaoks sõnumi 4012 ja signeerib selle. Samaaegselt salvestatakse genereeritud sõnum ka vahetabelisse.

Genereeritud ja signeeritud sõnum 4012 saadetakse ootavale kasutajale, kus kuvatakse nupp Autendime, mispeale suunatakse kasutaja edasi internetipanka.

Pank, pärast signatuuri kontrolli palub kasutajal ennast sisse logida. Kui kasutaja on edukalt panka sisenenud, siis koostab pank vastussõnumi: 3013. Sarnaselt sõnumile 4012 see signeeritakse ning edastatakse kasutajale, misjärel viimane suunatakse tagasi Portaali.

Portaal kontrollib edastatud sõnumi signatuuri. Kui signatuur on tõene, siis kontrollitakse, kas vastus 3013 on saabunud eelnevalt saadetud sõnumile (4012) etteantud ajaliimid piires ja seejärel vaadatakse, kas antud kasutaja isikukood on kasutusel. Portaal kasutab klientide identifikaatorina isikukoodi.