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 2016-10-13T07:21:14+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. Välja väärtus võib olla lühem kui maksimaalne pikkus lubab, puuduvaid kohti ei täideta.
- Päring-vastuse vahetamiseks kasutatakse HTTP POST meetodit.
- Jättes teenuse spetsifikatsioonis nõutud parameetri kirjeldamata, arvestatakse seda tühja väljana.
- Spetsifikatsioonile mittevastavatele päringutele vastatakse veateatega.
- Väljal VK_RETURN ei ole lubatud kasutada päringutes kasutatavaid välja nimesid (VK_...).
- Andmete vahetamiseks kasutatakse kodeeringut (VK_ENCODING), millest SEB pangalink toetab UTF-8 (vaikimisi) ja ISO-8859-1 kodeeringut. Pank vastab alati kliendi poolt määratud kodeeringus. Pangalingi probleemideta toimimiseks tuleb veenduda, et kõik teenusega seotud programmid kasutaks sama kodeeringut. Soovitame kasutada UTF-8.

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

Võtmete/sertifikaatide vahetamine

Pangalingi aktiveerimiseks SEB reaalsüsteemis tuleb eservice@seb.ee aadressile saata kaupmehe avalik võti, millele vastuseks saadetakse panga avalik võti ja vastava kaupmehe VK_SND_ID väärtus. Salajast võtit ei tohi teistele osapooltele (sh SEB-le) avaldada. Kasutame x.509 standardile vastavaid .PEM formaadis sertifikaate, salajase võtme pikkusena toetame 2048 bitti. Täpsema juhise võtmete genereerimiseks leiate „Testpaketis“ olevate dokumentide hulgast.

Kontrollkoodi VK_MAC leidmine versiooni 008 alusel

Allkiri MAC008 (VK_MAC) arvutatakse kasutades avaliku võtme algoritmi RSA ning räsialgoritmi SHA1. Arvestatakse ka tühjade väljade pikkusi – „000“.

MAC008(x1,x2,..., xn):= RSA (SHA-1(p(x1) || x1 || p(x2) || x2 || ... || p(xn) || xn),d,n)

Selgitused:

|| - stringi liitmise tehe

x1, x2, ..., xn - päringu parameetrid (spetsifikatsioonis nummerdatud) .
p - funktsioon parameetri pikkusest sümbolites. Pikkus on number kolmekohalise stringi kujul
d RSA - salajane eksponent
n RSA – modulus

Andmerea koostamine teenuse „1012“ näitel:
VK_SERVICE="1012"
VK_VERSION="008"
VK_SND_ID ="testvpos"
VK_STAMP ="20011"
VK_AMOUNT="1.00"
VK_CURR ="EUR"
VK_REF ="999"
VK_MSG ="UPOS testikas. ÕÜ"
VK_RETURN ="https://somehost.ee/returnurl"
VK_CANCEL ="https://somehost.ee/cancelurl"
VK_DATETIME ="2016-09-26T07:21:14+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 1.00
003 EUR
003 999
017 UPOS testikas. ÕÜ
029 https://somehost.ee/returnurl
029 https://somehost.ee/returnurl
024 2016-09-26T07:21:14+0200

Ühes reas: 0041012003008008testvpos005200110041.00003EUR003999017UPOS testikas. ÕÜ029https://somehost.ee/returnurl029https://somehost.ee/returnurl0242016-09-26T07:21:14+0200
Kui näiteks VK_MSG parameeter oleks tühi, siis tuleb see ikkagi lisada andmeritta, kasutades sümbolite arvuna 000.

NB! Kui kasutada kodeeringut UTF-8 ja parameetris sisalduvad kahebaidised sümbolid (näiteks täpitähed), siis andmereas on parameetri väärtuste pikkuseks sümbolite arv stringis, mitte baitide arv. Näiteks 002OÜ, mitte 003OÜ.

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”.

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 seletus
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 ehk allkiri
-	VK_ENCODING	12	Sõnumi kodeering. ISO-8859-1 või UTF-8 (vaikeväärtus)
-	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”.

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 seletus
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 ehk allkiri
-	VK_ENCODING	12	Sõnumi kodeering. ISO-8859-1 või UTF-8 (vaikeväärtus)
-	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 (Kella 22:00-24:00 vahelisel ajal teostatud maksed võivad pärast süsteemisisest pangapäeva vahetust kajastuda järgmise päeva väljavõttes)
-	VK_MAC	700	Kontrollkood ehk allkiri
-	VK_ENCODING	12	Sõnumi kodeering. ISO-8859-1 või UTF-8 (vaikeväärtus)
-	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 ehk allkiri
-	VK_ENCODING	12	Sõnumi kodeering. ISO-8859-1 või UTF-8 (vaikeväärtus)
-	VK_LANG	3	Soovitav suhtluskeel (EST, ENG või RUS)
-	VK_AUTO	1	Y = panga poolt automaatselt saadetud vastus. N = vastus kliendi liikumisega kaupmehe lehele

Autentimisteenused

Teenus 4011

Kaupmehe poolt saadetav pakett kasutaja tuvastamiseks. Teenus on avatud vastava lepingu sõlminud kaupmeestele. Vastuspaketi kood 3012.

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 Vabatahtlik väli, võib jääda täitmata
-	VK_MAC	700	Kontrollkood ehk allkiri
-	VK_ENCODING	12	Sõnumi kodeering, ISO-8859-1 või UTF-8 (vaikeväärtus)
-	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.

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
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 Vabatahtlik väli, võib jääda täitmata
12	VK_RID	30	Sessiooniga seotud identifikaator Vabatahtlik väli, võib jääda täitmata
-	VK_MAC	700	Kontrollkood ehk allkiri
-	VK_ENCODING	12	Sõnumi kodeering. ISO-8859-1 või UTF-8 (vaikeväärtus)
-	VK_LANG	3	Soovitav suhtluskeel (EST, ENG või RUS)

Teenus 4012

Kaupmehe poolt saadetav pakett kasutaja tuvastamiseks. Teenus on avatud vastava lepingu sõlminud kaupmeestele. Vastuspaketi kood 3013.

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 Vabatahtlik väli, võib jääda täitmata
-	VK_MAC	700	Kontrollkood ehk allkiri
-	VK_ENCODING	12	Sõnumi kodeering. ISO-8859-1 või UTF-8 (vaikeväärtus).
-	VK_LANG	3	Soovitav suhtluskeel (EST, ENG või RUS)

Teenus 3013

Kaupmehele edastatakse nonssi koopia.

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
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 Vabatahtlik väli, võib jääda täitmata
12	VK_RID	30	Sessiooniga seotud identifikaator Vabatahtlik väli, võib jääda täitmata
-	VK_MAC	700	Kontrollkood ehk allkiri
-	VK_ENCODING	12	Sõnumi kodeering. ISO-8859-1 või UTF-8 (vaikeväärtus)
-	VK_LANG	3	Soovitav suhtluskeel (EST, ENG või RUS)