

## Pangalingi päringute tehniline spetsifikatsioon

<b>Makseteenused</b> .....	3
Teenus 1011 .....	3
Teenus 1012 .....	3
Teenus 1111 .....	3
Teenus 1911 .....	4
<b>Autentimisteenused</b> .....	5
Teenus 3013 .....	5
Teenus 4011 .....	5
Teenus 4012 .....	6

## Päringud

- Päringutes esitatud summades on komakohad ja sendid eristatud punktiga "."  
Tuhandete eraldajat ei kasutata.
- Kuupäevad ja kellaajad esitatakse DATETIME formaadis sekundi täpsusega nt  
2013-03-13T07:21:14+0200 Päringu saaja on kohustatud kontrollima DATETIME väljal olevat  
väärtust, kusjuures välja väärtus tohib erineda kontrollimise hetkel kehtivast kellaajast  
maksimaalselt  $\pm 5$  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.
- Spetsifikatsioonile mittevastavatele päringutele vastatakse veateatega.
- Väljal VK\_RETURN ei ole lubatud kasutada pangalingi päringutes kasutatavaid välja nimesid  
(VK\_...)

Päringuid võib jagada:

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

## Kontrollkoodi VK\_MAC leidmine versiooni 008 alusel

Allkiri MAC008 (VK\_MAC) arvutatakse kasutades avaliku võtme algoritmi RSA ning räsialgoritmi SHA1.  
 $MAC008(x_1, x_2, \dots, x_n) := RSA(SHA-1(p(x_1) || x_1 || p(x_2) || x_2 || \dots || p(x_n) || x_n), d, n)$

Selgitused:

|| - stringi liitmise tehe

$x_1, x_2, \dots, x_n$  - päringu parameetrid (spetsifikatsioonis nummerdatud) .

p - funktsioon parameetri pikkusest sümbolites. Pikkus on number kolmekohalise stringi kujul

d RSA - salajane eksponent

n RSA – modulus

# 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 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. ISO-8859-1 või UTF-8 (vaikeväärtus) või WINDOWS-1257
-	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 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. ISO-8859-1 või UTF-8 (vaikeväärtus) või WINDOWS-1257
-	VK_LANG	3	Soovitav suhtluskeel (EST, ENG või RUS)

### Teenus 1111

Kasutatakse vastamiseks eestisesese 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. ISO-8859-1 või UTF-8 (vaikeväärtus) või WINDOWS-1257
-	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. ISO-8859-1 või UTF-8 (vaikeväärtus) või WINDOWS-1257
-	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 3012

Jrk.	Välja nimi	Pikkus	Kirjeldus
1	VK_SERVICE	4	Teenuse number (3012)
2	VK_VERSION	3	Kasutatav krüptoloogiaritm (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
12	VK_RID	30	Sessiooniga seotud identifikaator
-	VK_MAC	700	Kontrollkood e. allkiri
-	VK_ENCODING	12	Sõnumi kodeering. ISO-8859-1 või UTF-8 (vaikeväärtus) või WINDOWS-1257
-	VK_LANG	3	Soovitatav 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 krüptoloogiaritm (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
12	VK_RID	30	Sessiooniga seotud identifikaator
-	VK_MAC	700	Kontrollkood e. allkiri
-	VK_ENCODING	12	Sõnumi kodeering. ISO-8859-1 või UTF-8 (vaikeväärtus) või WINDOWS-1257
-	VK_LANG	3	Soovitatav suhtluskeel (EST, ENG või RUS)

### Teenus 4011

Kaupmehe poolt saadetakse pakett kasutaja tuvastamiseks. Teenus 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 krüptoloogiaritm (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. ISO-8859-1 või UTF-8 (vaikeväärtus) või WINDOWS-1257
-	VK_LANG	3	Soovitav suhtluskeel (EST, ENG või RUS)

#### Teenus 4012

Kaupmehe poolt saadetav pakett kasutaja tuvastamiseks. Teenus 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 krüptoloogiaritm (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. ISO-8859-1 või UTF-8 (vaikeväärtus) või WINDOWS-1257
-	VK_LANG	3	Soovitav suhtluskeel (EST, ENG või RUS)