

Pangalingi spetsifikatsioon

Pocopay pangalingilt makse algatamiseks tuleb kasutada teenust 1011. Kaupmees teeb päringu Pocopayle aadressile <https://my.pocopay.com/banklink>. Vastuspäring tehakse makse õnnestumise korral kaupmehe teenusele 1111 ning ebaõnnestumise korral kaupmehe teenusele 1911.

- Päringutes esitatud summades on komakohad ja sendid eristatud punktiga "." Tuhandete eraldajad ei kasutata. Näiteks "20.00" või "1000.00".
- Kuupäev ja kellaaeg esitatakse DATETIME formaadis sekundi täpsusega. Näiteks 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 ± 5 minutit.
- Välja väärtuse pikkus ei tohi ületada spetsifikatsioonis ette nähtut. Pikkuse ületamisel päringut ei töödelda. Välja väärtuse pikkus on sümbolites.
- Välja väärtus võib olla lühem kui maksimaalne pikkus lubab.
- Spetsifikatsioonile mittevastavale päringule vastatakse veateatega.
- Puuduv parameeter arvestatakse tühja väljana ja selle pikkuseks loetakse "000".
- Väljal VK_RETURN ei ole lubatud kasutada pangalingi päringutes kasutatavaid välja nimesid (VK_...).
- URLid VK_RETURN ja VK_CANCEL peavad toetama HTTPS protokollit.
- Andmete vahetamiseks valib klient kodeeringu (VK_ENCODING). Toetatud on UTF-8 (soovitatud kasutada), ISO-8859-1 ja WINDOWS-1257 kodeeringud. Vastus on alati kliendi poolt määratud kodeeringus.

Kontrollkoodi VK_MAC leidmine versiooni 008 alusel

Allkirja MAC008 (VK_MAC) väärtus arvutatakse, kasutades avaliku võtme algoritmi RSA. Räsialgoritm on vaikumisi SHA-256, aga soovi korral võib kasutada ka SHA1. Pocopay vastuses teenustele 1111 ja 1911 kasutatakse alati SHA-256.

$MAC008(x_1, x_2, \dots, x_n) := RSA(SHA-1(p(x_1)||x_1||p(x_2)||x_2||\dots||p(x_n)||x_n), d, n)$

- || - 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 - RSA salajane eksponent;
- n RSA - RSA modulus.

Makseteenused

Teenus 1011

Kaupmees saadab Pocopaysse allkirjastatud maksekorralduse andmed, mida klient Pocopay mobiilipangas makset sooritades muuta ei saa. Pärast edukat makset vastab Pocopay kaupmehele päringuga 1111, ebaõnnestunud makse korral päringuga 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	Soovitatav suhtluskeel (EST, ENG või RUS)
-	INAPP	booleaan	TRUE/FALSE. Näitab, kas pangalinki kasutatakse Pocopay äpis oleva iFrame'i kaudu

Teenus 1111

Pocopay vastus kaupmehele 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. ISO-8859-1 või UTF-8

			(vaikeväärtus) või WINDOWS-1257
-	VK_LANG	3	Soovitatav suhtluskeel (EST, ENG või RUS)
-	VK_AUTO	1	Y = panga poolt automaatselt saadetud vastus N = vastus kliendi liikumisega kaupmehe lehele

Teenus 1911

Pocopay vastus kaupmehele ebaõnnestunud maksekorraldusest teatamiseks.

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 (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	Soovitatav suhtluskeel (EST, ENG või RUS)
-	VK_AUTO	1	Y = panga poolt automaatselt saadetud vastus N = vastus kliendi liikumisega kaupmehe lehele

Self-signed sertifikaadi genereerimine (RSA-SHA256)

1. Privaatvõtme genereerimine
openssl genrsa -out key.pem 2048
2. Sertifikaadi päringu genereerimine
openssl req -new -sha256 -key key.pem -out csr.csr
3. Allkirjastatud sertifikaadi genereerimine
openssl x509 -sha256 -req -days 1825 -in csr.csr -signkey key.pem -out cert.crt

Toodangu sertifikaadi kehtivusaeg on 5 aastat.