Lisa 1: Pangalingi tehniline spetsifikatsioon

Kehtivad alates
16.01.2015.

1. ÜLDINE

1.1 Pangalingi 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 Pangale suunatakse URLile: https://www.lhv.ee/banklink.

1.2 Alates 2014. aasta oktoobrist võetakse kasutusele uuendatud tehniline spetsifikatsioon. Uuele spetsifikatsioonile vastavad maksepäringud on välja toodud punktis 2 ja autentimispäringud punktis 3. Vanade päringute kasutamist toetatakse kuni 2015. aasta lõpuni.

2. MAKSEPÄRINGUD (vastavuses uuendatud tehnilise spetsifikatsiooniga**)**

2.1 Päring 1011 (asendab päringu 1001)

Kaupmees saadab Panka allkirjastatud maksekorralduse andmed, mida Klient internetipangas muuta ei saa. Peale edukat makset koostatakse Kaupmehele päring “1111”, ebaõnnestunud makse puhul “1911”.

JRK	VÄLJANIMI	PIKKUS	KIRJELDUS
1	VK_SERVICE	4	Teenuse number (1011)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_SND_ID	15	Päringu koostaja (Kaupmehe) ID
4	VK_STAMP	20	Päringu ID
5	VK_AMOUNT	12	Maksmisele kuuluv summa. Komakohad ja sendid eristatud punktiga ".". Tuhandete eraldajat ei kasutata.
6	VK_CURR	3	Makse valuuta (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 ISO 8601 formaadis sekundi täpsusega koos ajatsooni infoga. Nt 2013-03-13T07:21:14+0200
-	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)

2.2 Päring 1012 (asendab päringu 1002)

Kaupmees saadab panka Kliendi sooviavalduse Tehingu tegemiseks. Makse saaja nimi ja konto number võetakse Panga ja Kaupmehe vahelisest lepingust. Peale edukat makset koostatakse Kaupmehele päring “1111”, ebaõnnestunud makse puhul “1911”

JRK	VÄLJANIMI	PIKKUS	KIRJELDUS
1	VK_SERVICE	4	Teenuse number (1012)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_SND_ID	15	Päringu koostaja (Kaupmehe) ID
4	VK_STAMP	20	Päringu ID
5	VK_AMOUNT	12	Maksmisele kuuluv summa. Komakohad ja sendid eristatud punktiga ".". Tuhandete eraldajat ei kasutata.
6	VK_CURR	3	Makse valuuta (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 ISO 8601 formaadis sekundi täpsusega koos ajatsooni infoga. Nt 2013-03-13T07:21:14+0200
-	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)

2.3 Vastuspäring 1111 (asendab päringu 1101)

Kasutatakse vastamiseks maksekorralduse toimumisest.

JRK	VÄLJANIMI	PIKKUS	KIRJELDUS
1	VK_SERVICE	4	Teenuse number (1111)
2	VK_VERSION	3	Kasutatav krüptoalgoritm 008
3	VK_SND_ID	15	Päringu koostaja (Panga) ID
4	VK_REC_ID	15	Päringu vastuvõtja (Kaupmehe) ID
5	VK_STAMP	20	Päringu ID
6	VK_T_NO	20	Maksekorralduse number
7	VK_AMOUNT	12	Makstud summa. Komakohad ja sendid eristatud punktiga ".". Tuhandete eraldajat ei kasutata.
8	VK_CURR	3	Makse valuuta (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 ISO 8601 formaadis sekundi täpsusega koos ajatsooni infoga. Nt 2013-03-13T07:21:14+0200
-	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

2.4 Vastuspäring 1911 (asendab päringu 1901)

Kasutatakse ebaõnnestunud tehingust teatamiseks.

JRK	VÄLJANIMI	PIKKUS	KIRJELDUS
1	VK_SERVICE	4	Teenuse number (1911)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_SND_ID	15	Päringu koostaja (Panga) ID
4	VK_REC_ID	15	Päringu vastuvõtja (Kaupmehe) 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

3. AUTENTIMISPÄRINGUD (vastavuses uuendatud tehnilise spetsifikatsiooniga**)**

3.1 Vastuspäring 3012 (asendab päringu 3002)

Kaupmehele edastatakse Panga poolt tuvastatud kasutaja andmed.

Turvalisuse huvides peab sõnumi saaja lisaks allkirjale (VK_MAC) kontrollima ka sõnumi saaja ID-d (VK_REC_ID) ning sõnumi genereerimise kuupäeva ja

kellaaega (VK_DATETIME), mis tohib erineda kontrollimise hetkel kehtivast maksimaalselt ±5 minutit.

JRK	VÄLJANIMI	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 kuupäev ja kellaaeg ISO 8601 formaadis sekundi täpsusega koos ajatsooni infoga. Nt 2013-03-13T07:21:14+0200
5	VK_SND_ID	15	Sõnumi koostaja (Panga) ID
6	VK_REC_ID	15	Sõnumi saaja (Kaupmehe) 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	Soovitav suhtluskeel (EST, ENG või RUS)

3.2 Vastuspäring 3013

Kaupmehele edastatakse vastusena päringule 4012 Panga poolt tuvastatud kasutaja andmed ja nonssi koopia.

Turvalisuse huvides peab sõnumi saaja lisaks allkirjale (VK_MAC) ja nonssile (VK_NONCE) kontrollima ka sõnumi saaja ID-d (VK_REC_ID) ning sõnumi genereerimise kuupäeva ja kellaaega (VK_DATETIME), mis tohib erineda kontrollimise hetkel kehtivast maksimaalselt ±5 minutit.

JRK	VÄLJANIMI	PIKKUS	KIRJELDUS
1	VK_SERVICE	4	Teenuse number (3013)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_DATETIME	24	Sõnumi genereerimise kuupäev ja kellaaeg ISO 8601 formaadis sekundi täpsusega koos ajatsooni infoga. Nt 2013-03-13T07:21:14+0200
4	VK_SND_ID	15	Sõnumi koostaja (Panga) ID
5	VK_REC_ID	15	Sõnumi saaja (Kaupmehe) 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	Soovitav suhtluskeel (EST, ENG või RUS)

3.3 Päring 4011 (asendab 4001)

Kaupmehe poolt Pangale saadetav päring kasutaja tuvastamiseks. Teenus avatud vastava lepingu sõlminud kaupmeestele. Vastuspäringu kood 3012.

JRK	VÄLJANIMI	PIKKUS	KIRJELDUS
1	VK_SERVICE	4	Teenuse number (4011)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_SND_ID	15	Sõnumi koostaja (Kaupmehe) ID
4	VK_REPLY	4	Oodatava vastuspaketi kood (3012)
5	VK_RETURN	255	Kaupmehe URL, kuhu vastatakse
6	VK_DATETIME	24	Sõnumi genereerimise kuupäev ja kellaaeg ISO 8601 formaadis sekundi täpsusega koos ajatsooni infoga. Nt 2013-03-13T07:21:14+0200
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)

3.4 Autentimispäring 4012 (asendab päringu 4002)

Kaupmehe poolt Pangale saadetav päring kasutaja tuvastamiseks. Teenus avatud vastava lepingu sõlminud kaupmeestele. Vastuspäringu kood 3013.

JRK	VÄLJANIMI	PIKKUS	KIRJELDUS
1	VK_SERVICE	4	Teenuse number (4012)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_SND_ID	15	Sõnumi koostaja (Kaupmehe) 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 kuupäev ja kellaaeg ISO 8601 formaadis sekundi täpsusega koos ajatsooni infoga. Nt 2013-03-13T07:21:14+0200
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)

4. MAKSEPÄRINGUD (toetatud kuni 31.12.2015)

4.1 Päring 1001.

Kaupmees saadab panka kliendi sooviavalduse tehingu tegemiseks. Peale edukat makset edastatakse kaupmehele vastuspäring „1101“. Ebaõnnestunud makse puhul vastuspäring „1901“.

JRK	VÄLJANIMI	PIKKUS	KIRJELDUS
1	VK_SERVICE	4	Teenuse number (1001)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_SND_ID	15	Päringu koostaja ID (kaupmehe ID)
4	VK_STAMP	20	Päringu ID
5	VK_AMOUNT	17	Maksmisele kuuluv summa. Komakohad ja sendid eristatud punktiga ".". Tuhandete eraldajat ei kasutata.
6	VK_CURR	3	Valuuta lühend (EUR)
7	VK_ACC	16	Saaja arve number
8	VK_NAME	70	Saaja nimi
9	VK_REF	20	Maksekorralduse viitenumber
10	VK_MSG	210	Maksekorralduse selgitus
-	VK_MAC	700	Kontrollkood e. allkiri
-	VK_RETURN	60	URL, kuhu saadetakse tehingu vastuse päring
-	VK_LANG	3	Soovitav suhtluskeel
-	VK_CHARSET	12	ISO-8859-1 (vaikeväärtus), UTF-8 või WINDOWS-1257

4.2 Päring 1002

Kaupmees saadab panka kliendi sooviavalduse tehingu tegemiseks. Makse saaja ja konto number võetakse pangalingi lepingust.

JRK	VÄLJANIMI	PIKKUS	KIRJELDUS
1	VK_SERVICE	4	Teenuse number (1002)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_SND_ID	15	Päringu koostaja ID (kaupmehe ID)
4	VK_STAMP	20	Päringu ID
5	VK_AMOUNT	17	Maksmisele kuuluv summa. Komakohad ja sendid eristatud punktiga ".". Tuhandete eraldajat ei kasutata.
6	VK_CURR	3	Valuuta lühend (EUR)
7	VK_REF	20	Maksekorralduse viitenumber
8	VK_MSG	210	Maksekorralduse selgitus
-	VK_MAC	700	Kontrollkood e.allkiri

-	VK_RETURN	200	URL, kuhu saadetakse tehingu vastuse päring
-	VK_LANG	3	Soovitav suhtluskeel
-	VK_CHARSET	12	ISO-8859-1 (vaikeväärtus), UTF-8 või WINDOWS-1257

4.3 Vastuspäring 1101

Kasutatakse vastamiseks eestisisese maksekorralduse toimumisest.

JRK	VÄLJANIMI	PIKKUS	KIRJELDUS
1	VK_SERVICE	4	Teenuse number (1101)
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 (Kaupmehe ID)
5	VK_STAMP	20	Päringu ID
6	VK_T_NO	20	Maksekorralduse number
7	VK_AMOUNT	17	Makstud summa
8	VK_CURR	3	Valuuta lühend (EUR)
9	VK_REC_ACC	16	Saaja konto number
10	VK_REC_NAME	100	Saaja nimi
11	VK_SND_ACC	16	Maksja konto number
12	VK_SND_NAME	100	Maksja nimi
13	VK_REF	20	Maksekorralduse viitenumber
14	VK_MSG	210	Maksekorralduse selgitus
15	VK_T_DATE	10	Maksekorralduse kuupäev (DD.MM.YYYY)
-	VK_MAC	700	Kontrollkood e. Allkiri
-	VK_LANG	3	Soovitav suhtluskeel
-	VK_CHARSET	12	ISO-8859-1 (vaikeväärtus), UTF-8 või WINDOWS-1257
-	VK_AUTO		Y = panga poolt automaatselt saadetud vastus.

4.4 Vastuspäring 1901

Kasutatakse ebaõnnestunud tehingust teatamiseks.

JRK	VÄLJANIMI	PIKKUS	KIRJELDUS
1	VK_SERVICE	4	Teenuse number (1901)
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 (Kaupmehe ID)
5	VK_STAMP	20	Päringu ID
6	VK_REF	20	Maksekorralduse viitenumber
7	VK_MSG	255	Maksekorralduse selgitus
-	VK_MAC	700	Kontrollkood e. Allkiri
-	VK_LANG	3	Soovitav suhtluskeel
-	VK_AUTO		Y = panga poolt automaatselt saadetud vastus.

5. AUTENTIMISPÄRINGUD (toetatud kuni 31.12.2015)

5.1 Päring 4001

Kaupmehe poolt saadetav päring internetipanga kasutaja identifitseerimiseks. Portaali looja peab arvestama, et pank teostab VK_DATE/VK_TIME väljade kontrolli vastu serverikellaaega. Juhul kui panga ja Portaali serverikellaaegade erinevus läheb piisavalt suureks, siis tühistatakse kõik sisenemised. Panga serveri kell on sünkroniseeritud vastu ntp.estpak.ee serverit.

JRK	VÄLJANIMI	PIKKUS	KIRJELDUS
1	VK_SERVICE	4	Teenuse number (4001)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_SND_ID	15	Päringu koostaja ID (kaupmeheID)
4	VK_REPLY	4	Oodatava vastuspaketi kood (3001,3002)
5	VK_RETURN	200	URL, kuhu saadetakse tehingu vastuse päring
6	VK_DATE	10	Paketi genereerimise kuupäev (DD.MM.YYYY)
7	VK_TIME	8	Paketi genereerimise kellaaeg (HH24:MM:SS)
-	VK_CHARSET	12	ISO-8859-1 (vaikeväärtus), UTF-8 või WINDOWS-1257
-	VK_MAC	700	Kontrollkood e. allkiri

5.2 Vastuspäring 3001

Kaupmehele edastatakse kasutaja identifikaator ning paketi genereerimise kuupäev ja kellaaeg. Turvalisuse huvides peab kaupmees kontrollima paketis olevat saatmise aega (VK_DATE ja VK_TIME).

JRK	VÄLJANIMI	PIKKUS	KIRJELDUS
1	VK_SERVICE	4	Teenuse number (3001)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_USER	16	Ei ole kasutusel
4	VK_DATE	10	Paketi genereerimise kuupäev (DD.MM.YYYY)
5	VK_TIME	8	Paketi genereerimise kellaaeg (HH24:MM:SS)
6	VK_SND_ID	15	Päringu koostaja ID (Panga ID)
-	VK_CHARSET	12	ISO-8859-1 (vaikeväärtus), UTF-8 või WINDOWS-1257
-	VK_MAC	700	Kontrollkood e. allkiri

5.3 Vastuspäring 3002

Kaupmehele edastatakse kasutaja identifikaator ning paketi genereerimise kuupäev ja kellaaeg. Väli VK_INFO sisaldab semikoolonitega eraldatud nimi-väärtus paare kujul "NIMI:väärtus". Näiteks "ISIK:37508166516;NIMI:JAAN SAAR". Turvalisuse huvides peaks kaupmees kontrollima paketis olevat saatmise aega (VK_DATE ja VK_TIME).

JRK	VÄLJANIMI	PIKKUS	KIRJELDUS
1	VK_SERVICE	4	Teenuse number (3002)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_USER	16	Ei ole kasutusel
4	VK_DATE	10	Paketi genereerimise kuupäev (DD.MM.YYYY)
5	VK_TIME	8	Paketi genereerimise kellaaeg (HH24:MM:SS)
6	VK_SND_ID	15	Päringu koostaja ID (Panga ID)
7	VK_INFO	300	Kasutaja isikuandmeid sisaldav väli
-	VK_CHARSET	12	ISO-8859-1 (vaikeväärtus), UTF-8 või WINDOWS-1257
-	VK_MAC	700	Kontrollkood e. allkiri

5.4 Autentimispäring 4002

Kaupmehe poolt saadetav pakett kasutaja tuvastamiseks koos juhusliku nonssiga.

JRK	VÄLJANIMI	PIKKUS	KIRJELDUS
1	VK_SERVICE	4	Teenuse number (4002)
2	VK_VERSION	3	Kasutatav krüptoalgoritm (008)
3	VK_SND_ID	15	Päringu koostaja ID (kaupmehe ID)
4	VK_REC_ID	15	Päringu koostaja ID (Panga ID)
5	VK_NONCE	50	Päringu koostaja poolt genereeritud juhuslik nonss
6	VK_RETURN	60	URL, kuhu saadetakse tehingu vastuse päring
-	VK_CHARSET	12	ISO-8859-1 (vaikeväärtus), UTF-8 või WINDOWS-1257
-	VK_MAC	700	Kontrollkood e. allkiri

6. AVALIKUD VÕTMED

6.1 LHV aktsepteerib sertifikaadipäringut või *self-signed* sertifikaati. Avalike võtmete vahetamine toimub lepingu sõlmimisel. Kasutame X.509 standardile vastavaid .PEM formaadis võtmeid/sertifikaate st. sisu on BASE64 kodeeringus ning märgendite —BEGIN… — ja —END… — vahel. Kliendi poolt genereeritud salajase võtme minimaalne pikkus peab olema 1024 bitti.

6.2 Võtmeid saab luua kasutades openssl utiliiti. Võtme loomisel soovitame lähtuda järgmistest tingimustest:

(i) Signature algorithm - sha1RSA

(ii) Public key - RSA(1024 Bits)

(iii) Kehtivusaeg mitte üle 10 aasta

7. KONTROLLKOODI VK_MAC LEIDMINE

7.1 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 parameetrid

(ii) p on uuele spetsifikatsioonile vastavate päringute puhul (1011, 1012, 1111, 1911, 3012, 3013, 4011, 4012) funktsioon parameetri pikkusest sümbolites. Vanade päringute puhul (1001, 1002, 1101, 1901, 4001, 3001, 3002, 4002) on p funktsioon parameetri pikkusest baitides. Pikkus on formateeritud kolmekohalise stringi kujul. Ehk siis pikkus 1 ' "001". Tühjade väljade pikkus on "000".

(iii) d on RSA salajane eksponent

(iv) n on RSA modulus

(v) || - stringide liitmistehe