

**Suomen
julkishallinnon
VETUMA-palvelu
Rajapintakuvaus v1.0**

VETUMA
Verkkotunnistus ja -maksaminen

Sisällysluettelo

1.	Johdanto	3
1.1	VETUMA-palvelu	3
1.2	VETUMA-ympäristö	4
1.3	Loppukäyttäjän ympäristö.....	4
1.3.1	Tuetut selaimet	4
1.3.2	Yleiset vaatimukset ja rajoitukset.....	5
1.3.3	HST-kortin käyttö.....	5
1.4	VETUMA-sovelluksen käyttöliittymä	5
2.	Palvelurajapinta	6
2.1	Palvelun osoitteet	6
2.2	Varmenteet	6
2.3	Palveluiden mukauttaminen.....	6
2.3.1	Peruskonfiguraatio.....	6
2.3.2	Lisäkonfiguraatiot.....	7
2.3.3	VETUMA-palvelua käyttävien sovellusten erottelu	7
2.4	Jaettu salaisuus	7
2.4.1	Jaetun salaisuuden luonti	7
2.5	Rajapinnan viestikentät.....	8
2.5.1	Viestikentät	8
2.5.2	Viestikenttien kuvaus	10
2.6	Kutsuviesti	12
2.7	Vastausviesti.....	13
2.8	Esimerkki Tupas-tunnistuksesta	13
2.9	Tiivisteiden laskeminen	15
2.9.1	Jaettu salaisuus ja algoritmi.....	15
2.9.2	Kutsu	15
2.9.3	Vastaus.....	15
2.10	Käyttäjän Sessio	15
3.	Rajapintakutsut	15
3.1	Tunnistaminen	15
3.1.1	Kutsu- ja vastausparametrit	16
3.1.2	Kutsu	16
3.1.3	Vastaus.....	17
3.2	Hyväksyminen	17
3.2.1	Kutsu- ja vastausparametrit	17
3.2.2	Kutsu	18
3.2.3	Vastaus.....	18
3.3	Kiistämätön allekirjoitus	19
3.3.1	Kutsu- ja vastausparametrit	19
3.3.2	Kutsu	20
3.3.3	Vastaus.....	20
4.	Virhetilanteet	21
4.1	Toistuvat kutsut.....	21
5.	Liitteet	21

Versio: 1.0, 16.2.2006

VETUMA Rajapintakuvaus

1. JOHDANTO

Tämä dokumentti kuvaa Verkkotunnistus- ja maksamispalvelun (VETUMA) teknisen rajapinnan. Fujitsu Services tuottaa palveluntuottajan ominaisuudessa VETUMA-palvelua Valtion ja Kuntien eri organisaatioiden käyttöön. VETUMA-palveluun liittyneet julkishallinnon organisaatiot voivat hyödyntää VETUMA-palvelun toimintoja käyttäen tässä dokumentissa määriteltyä teknistä rajapintaa.

VETUMA-palvelukokonaisuus sisältää tässä dokumentissa kuvatun toiminnallisuuden lisäksi mm. käyttäjähallintaan, laskutukseen ja raportointiin liittyviä toimintoja. Tässä dokumentissa on kuvattu ainoastaan VETUMA-rajapinnan kautta käytettävissä oleva toiminnallisuus.

1.1 VETUMA-palvelu

VETUMA-palvelu tulee sisältämään vaiheittain laajenevan joukon toimintoja. Seuraavassa taulukossa on kuvattu eri vaiheissa toteutettavat toiminnallisuudet, aikataulu yleisellä tasolla sekä rajapintakuvausten versio jossa ko. toiminnallisuudet on määritelty.

Vaihe	Aikataulu	Toiminnallisuudet	Versiossa
Vaihe 1 A	helmikuun 2006 alussa	Tunnistaminen <ul style="list-style-type: none"> • HST-kortti • Tupas v2 • käyttäjätunnus/salasana Hyväksyminen <ul style="list-style-type: none"> • HST-kortti • Tupas v2 • käyttäjätunnus/salasana Kiistämätön sähköinen allekirjoitus (HST)	1.0
Vaihe 1B	maaliskuussa 2006	Verkkomaksaminen	1.5
Vaihe 2	alustavasti vuoden 2006 aikana	Mobiilitunnistaminen Mobiiliallekirjoitus Luottokorttimaksaminen	2.0

Tämä rajapintakuvaus määrittelee eri toiminnallisuudet edellä kuvattujen vaiheiden mukaisesti. Ensimmäisessä vaiheessa kuvaus kattaa eri tunnistamis-, hyväksymis- ja allekirjoitustoiminnallisuudet.

VETUMA-palvelu sisältää tuotantopalvelun lisäksi erillisen testipalvelun. Näille on määritelty omat erilliset osoitteensa (kappale 2.1).

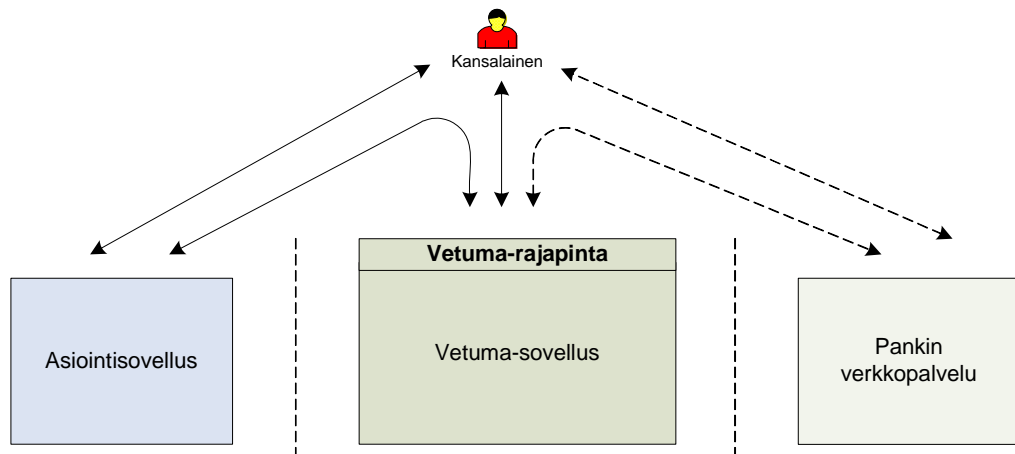
VETUMA-palvelun käyttö rajapinnan mukaisesti edellyttää että sovelluksella on käytössään asiakaskoodi (esim. kunta- / kaupunkikohtainen), sovelluskoodi ja ns. jaettu salaisuus (kappale 2.4). Rajapinnassa käytettävät perustiedot määritellään VETUMA-palveluun liityttäessä. Esim.

Versio: 1.0, 16.2.2006

sovelluskoodeja voidaan määrittellä lisää myös myöhemmin jatkuvan VETUMA-palvelun puitteissa.

1.2 VETUMA-ympäristö

Seuraavassa kuvassa on esitetty VETUMA-rajapinta sekä muut rajapinnan käyttöön vaikuttavat komponentit (Kuva 1).



Kuva 1 VETUMA-ympäristö

Loppukäyttäjä (kansalainen) käyttää selaimella asiointisovellusta. Asiointisovellus kutsuu VETUMA-rajapintaa käyttäen jotain VETUMA-sovelluksen palvelua (esim. tunnistaminen). VETUMA-sovellus itse toteuttaa useimmat eri tunnistus ja allekirjoitus toiminnot. Joissakin toiminnoissa (Tupas-tunnistus, verkkomaksaminen) käyttäjä siirretään VETUMA-palvelusta edelleen valitsemansa pankin verkkopalveluun. Pankin verkkopalvelusta loppukäyttäjä palaa aina VETUMA-sovelluksen kautta takaisin asiointisovellukseen.

Asiointisovelluksen, VETUMA-sovelluksen ja Pankin verkkopalvelun välillä ei ole yhteyksiä vaan kaikki yhteydet ovat suoria yhteyksiä loppukäyttäjän selaimen ja eri web-palvelinten välillä. Kaikki edellä kuvatut yhteydet on suojattu SSL/TLS (HTTPS) protokollaa käyttäen. Lisäksi rajapintakutsuissa eri osapuolet tunnistetaan sekä viestien eheys taataan käyttäen jaettuun salaisuuteen perustuvaa MAC laskentaa.

1.3 Loppukäyttäjän ympäristö

1.3.1 Tuetut selaimet

VETUMA-palvelu tukee seuraavia selaimia:

- Internet Explorer 5 & 6
- Netscape 8
- Firefox 1.0
- Opera 8

Näiden selainten uudemmat versiot testataan 2kk kuluessa selaimen virallisesta versiojulkistuksesta.

Myös muut yleisten standardien mukaiset selaimet todennäköisesti toimivat VETUMA-palvelua käytettäessä. Muita selaimia ei kuitenkaan tueta/testata erikseen.

1.3.2 Yleiset vaatimukset ja rajoitukset

Seuraava lista kuvaa yleisesti selainkäytön asettamia vaatimuksia ja rajoituksia:

- Palvelu tukee http-protokollan versioita 1.0 ja 1.1
- Palvelu vaatii toimiakseen istuntoevästeiden (session cookies) sallimisen selaimessa.
- Palvelu käyttää selainskriptejä mikäli nämä ovat selaimessa käytettävissä. Palvelu toimii myös ilman selainskriptejä, tällöin käyttäjän on itse edettävä palvelussa linkkiä tai painiketta painamalla (esim. siirtyminen VETUMA-palvelusta pankin verkkopalveluun).
- SSL-salausta käytettäessä selaimen tulee tukea SSL-versiota 3.0 tai TLS-versiota 1.0.
- SSL-salausta käytettäessä selaimen tulee tukea 128 bittistä salausta.
- SSL-salausta käytettäessä kaikkiin selaimiin ei välttämättä ole asennettuna palvelinvarmenteen myöntäjän varmennetta, joten selaimen on sallittava SSL yhteyden muodostaminen ko. palvelinvarmennetta hyödyntäen. Tämä saattaa vaatia käyttäjän hyväksynnän. Vaihtoehtoisesti palvelinvarmenteen myöntäjän varmenne voidaan asentaa selaimen luotetuksi varmentajaksi.

1.3.3 HST-kortin käyttö

VETUMA-palvelussa HST-korttia voidaan käyttää tunnistamiseen, hyväksymiseen sekä kiistämättömän allekirjoituksen tekemiseen. HST-korttia käytettäessä käyttäjällä tulee olla tähän tarvittavat laitteet ja ohjelmistot:

- voimassaoleva HST-kortti
- kortinlukija
- kortinlukijaohjelmisto (esim. Fujitsu DigiSign Client, Setec SetWeb, Nexus Personal jne.)
- yhteensopiva selain

Nämä vaatimukset ovat yleisiä HST-kortin käytön vaatimuksia, VETUMA-palvelu ei aseta kortin käytölle lisävaatimuksia tai rajoitteita.

Kiistämättömä allekirjoitusta luotaessa HST-kortilla, käynnistää VETUMA-palvelu loppukäyttäjän selaimessa selain plug-in:n jolla allekirjoituksen luonti suoritetaan. Kyseinen plug-in komponentti asennetaan kortinlukijaohjelmiston asennuksen yhteydessä.

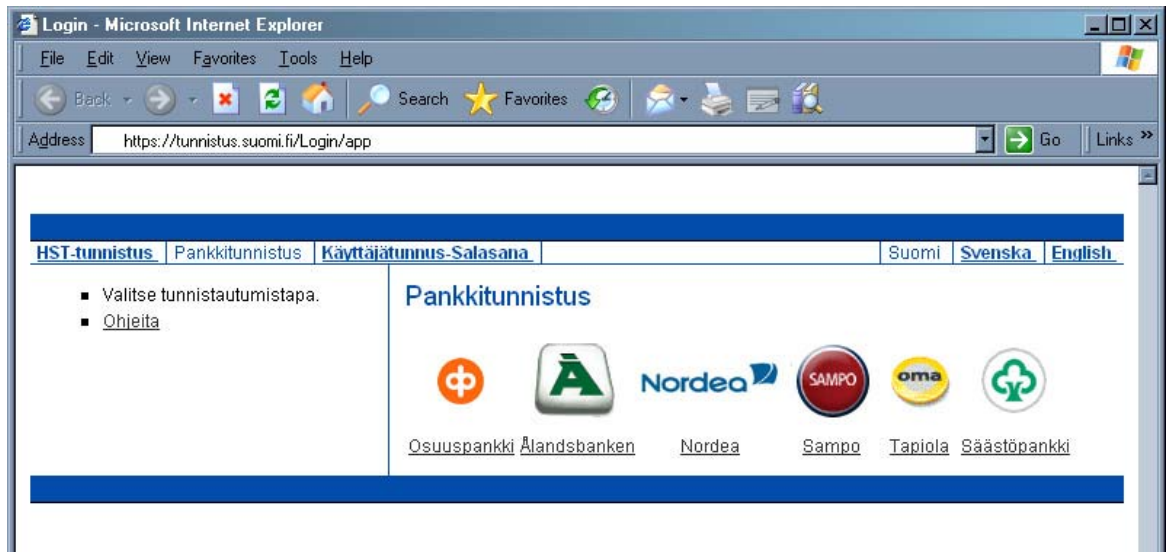
Kortinlukijaohjelmisto ja allekirjoituksen luontiin tarkoitettu plug-in saattavat rajoittaa HST-kortin käyttöä (muut kuin Windows käyttöjärjestelmä yms.). Esimerkiksi Machintosh käyttöjärjestelmässä eivät kaikki kortinlukijaohjelmistot ja plug-init ole tuettuja.

1.4 VETUMA-sovelluksen käyttöliittymä

VETUMA-rajapinnan kautta on mahdollista valita käyttäjälle näytettävät menetelmät (esim. tunnistustavat) sekä käytettävä käyttöliittymäkieli. Loppukäyttäjä voi myös itse vaihtaa esim. kielen toiseksi VETUMA-sovelluksessa.

Kuva 2 esittää esimerkin VETUMA-sovelluksen käyttöliittymästä. Sovelluksen käyttöliittymän käytössä olevat toiminnot ja valinnat vaihtelevat riippuen käytettävästä toiminnosta (tunnistus, allekirjoittaminen jne.), asiakkaalle käytössä olevista menetelmistä (HST, Tupas jne.) sekä rajapintakutsun parametreista.

Sivun vasemmassa yläreunassa on linkit tunnistus-menetelmän vaihtamiseksi, käyttöliittymäkielen vaihtaminen tapahtuu oikean yläreunan linkeistä.



Kuva 2 VETUMA-sovelluksen käyttöliittymäesimerkki

2. PALVELURAJAPINTA

Palvelurajapinta on viestirajapinta missä viestit on toteutettu käyttäen HTTP POST –viestejä. Vaihdetujen viestien eheys taataan käyttämällä Message Authentication Code (MAC) laskentaa viestien yhteydessä. Viestien ja kommunikoinnin luottamuksellisuus perustuu käytettävän yhteyden suojaukseen HTTPS-protokollalla.

2.1 Palvelun osoitteet

VETUMA- tuotantopalvelun osoite on: <https://tunnistus.suomi.fi/Login/app>

VETUMA- testipalveluun osoite on: <https://testitunnistus.suomi.fi/Login/app>

2.2 Varmenteet

VETUMA-testipalvelun varmenteen myöntäjä on Fujitsun CA (Fujitsu Topsel CA). Kyseinen CA varmenne on käytön helpottamiseksi asennettavissa selaimen testipalvelun info-sivulta.

VETUMA-tuotantopalvelun palvelinvarmenteen varmentajan on Väestörekisterikeskus.

VETUMA-palvelun palvelinvarmenteiden ajantasaiset tiedot (voimassaoloaika, myöntäjä jne.) on kerrottu erillisessä dokumentissa (LIITE 1).

2.3 Palveluiden mukauttaminen

2.3.1 Peruskonfiguraatio

Asiakkaan liittyessä VETUMA-palveluun valitaan käyttöön otettavat tunnistus yms. menetelmät ja käytettävät kielet. Lisäksi määritellään yhteinen jaettu salaisuus (kappale 2.4) sekä VETUMA sovellus ID (rajapinnan AP-parametri). Nämä tiedot määritellään VETUMA-palveluun ja ne muodostavat VETUMAn asiakkaalle ns. peruskonfiguraation.

Asiakas voi rajapintakutsussa edelleen mukauttaa palvelua haluamakseen rajoittaen mm. käytettäviä menetelmiä (SOLIST-parametri) sekä määrätä suoritetaanko VTJ-kysely varmennetta käytettäessä (EXTRADATA-parametri).

Versio: 1.0, 16.2.2006

Rajapinnan kautta ei voida laajentaa VETUMA-palveluun staattisesti määriteltyjä toimintoja tai oikeuksia. Mikäli esimerkiksi VTJ-kyselyä ei ole otettu käyttöön, ei sitä voida myöskään rajapinnan kautta pyytää käytettäväksi.

Asiakas voi käyttää tätä peruskonfiguraatiota rajapintakutsuilla mukautettuna kaikissa haluamissaan sovelluksissa joihin ko. konfiguraatio on soveltuva. Lisäkonfiguraatioita määrittelemällä on mahdollista saada edelleen mukautettua VETUMA-palvelun toimintaa.

2.3.2 Lisäkonfiguraatiot

Mikäli asiakkaalla on tarve saada käyttöönsä peruskonfiguraatiosta poikkeava toiminnallisuus tietyille sovellukselle tai joukolle sovelluksia, voidaan tarvittavat tiedot ja parametrit määrittellä erikseen lisäkonfiguraationa.

Esimerkiksi kunnalla voi olla käytössään VETUMA-palvelun peruskonfiguraatio suurimmalle osalle sovelluksistaan. Yhdelle yksittäiselle sovellukselle tai esimerkiksi tietyn viraston sovelluksille voidaan määrittellä oma jaettu salaisuus, vain tietyt tunnistustavat ja uusi VETUMA sovellus ID.

Tarkemmat VETUMA-palvelun yksityiskohdat ja konfiguraatioiden lisäys- ja muutosprosessi on kuvattu VETUMA-palvelun liittymisdokumentaatioissa.

2.3.3 VETUMA-palvelua käyttävien sovellusten erottelu

VETUMA-palvelun laskutustietojen jaottelu sovelluksittain vaatii palvelua käyttävien sovellusten erottelun. VETUMA-palvelua käyttävät sovellukset erotellaan rajapinnan APPID parametrin perusteella.

2.4 Jaettu salaisuus

Jaettua salaisuutta käytetään välitettävän datan suojaamiseen ja eri osapuolten tunnistamiseen. Välitettäviin viesteihin lasketaan MAC-tarkiste jaetun salaisuuden avulla (kappale 2.9).

Oletusarvoisesti asiakkaan (esim. kunnan) kaikki sovellukset käyttävät samaa jaettua salaisuutta kommunikoidessaan VETUMA-palvelun kanssa. Mikäli tarpeen, on myös mahdollista määrittellä tietyille joukolle sovelluksia tai yksittäiselle sovellukselle oma erillinen jaettu salaisuutensa. Rajapinnan kenttä RCVID yksilöi käytettävän jaetun salaisuuden.

Käytettävä jaettu salaisuus ei ole riippuvainen asiakkaan käyttämästä VETUMA-palvelun sovellus ID:stä. Asiakkaalla voi olla käytössään useampi jaettu salaisuus ja vain yksi VETUMAn sovellus ID tai toisaalta vain yksi jaettu salaisuus mutta useampia VETUMA sovellus ID:tä.

Jaetun salaisuuden jakelumenetelmät ja uusimisprosessi on kuvattu VETUMA-palvelun liittymisdokumentaatioissa.

2.4.1 Jaetun salaisuuden luonti

Jaettu salaisuus luodaan uudelle asiakkaalle asiakaskohtaisten konfiguraatioiden määrittelyn yhteydessä. Seuraavassa on kuvattu jaetun salaisuuden luonnin periaatteet:

- alustetaan käyttöön ohjelmistopohjainen kryptografisesti turvallinen satunnaislukugeneraattori sekä symmetrisen avaimen luontifunktio
- näiden avulla luodaan salainen avain (256 bittiä) joka esitetään hex-muodossa (64 merkkiä)
- avaimen käsittelyn helpottamiseksi alkuun lisätään jaetun salaisuuden / asiakkaan ID erotinmerkillä '-' erotettuna (Kuva 3).

Versio: 1.0, 16.2.2006

RCVID (5-15 merkkiä)	-	AVAIN (64 merkkiä)
Jaettu salaisuus (70-80 merkkiä)		

Kuva 3 Jaettu salaisuus

Jaetun salaisuuden suojaamiseen tulee kiinnittää erityistä huomiota koko jaetun salaisuuden elinkaaren ajan.

2.5 Rajapinnan viestikentät

2.5.1 Viestikentät

VETUMA-rajapinnan arvot välitetään HTML FORM rakenteen kentissä. Oheinen taulukko kuvaa

- VETUMA-rajapinnan kentät
- kenttien arvon/tyypin
- kentässä välitettävän datan pituuden
- onko kyseessä kutsu/vastaus viestin kenttä
- onko kenttä mukana MAC-laskennassa (P = pakollinen, V = valinnainen)
- kentän kuvauksen

Versio: 1.0, 16.2.2006

Taulukko 1 Rajapinnan kentät

Nro	Nimi	Arvo / Tyyppi	Pituus	Kutsu / Vastaus	MAC P/V	Kuvaus
1	RCVID	Merkkijono	5-15	K/V	P	Kutsuvan asiakkaan ja käytetyn jaetun salaisuuden ID
2	APPID	Merkkijono	5-10	K/-	P	Kutsuvan asiakassovelluksen ID
3	TIMESTMP	YYYYMMDDHHMMSSsss	17	K/V	P	Aikaleima
4	SO	Merkkijono	1-2	K/V	P	Oletusmenetelmä
5	SOLIST	Merkkijonolista	1-10	K/-	V	Käytössä olevat menetelmät
6	TYPE	Merkkijono	5-10	K/-	V	VETUMA-palvelun tyyppi
7	AU	Merkkijono	5-10	K/-	V	Toimintokoodi
8	USERID	Merkkijono	1-20	K/V	V	Käyttäjän yksilöinti
9	LG	ISO 639: 2-kirjainta (pienillä)	2	K/V	V	Kielikoodi
10	RETURL	URL	250	K/V	V	Paluu URL onnistuneen tapahtuman jälkeen
11	CANURL	URL	250	K/V	V	Paluu URL peruutetun tapahtuman jälkeen
12	ERRURL	URL	250	K/V	V	Paluu URL virhetilanteessa
13	AP	Merkkijono	10-20	K/-	V	VETUMA sovellus ID
14	TTS	Merkkijono	1-2000	K/V	V	Kiistämättömän allekirjoituksen teksti
15	MAC	Merkkijono	32-64	K/V	-	MAC
16	SIGNATURE	Merkkijono	0-5000	-/V	V	PKCS#7 allekirjoitus base64 muodossa
17	SIGNATURESTATUS	Merkkijono	2-6	-/V	V	Allekirjoituksen tarkistuksen tulos
18	SUBJECTDATA	Merkkijono	100	-/V	V	Käyttäjän nimitiedot
19	EXTRADATA	Merkkijono	0-50	K/V	V	VTJ-kyselyn suoritus ja vastaus

Versio: 1.0, 16.2.2006

2.5.2 Viestikenttien kuvaus

Seuraavassa on kuvattu tarkemmin täsmennystä vaativat rajapinnan kentät.

RCVID - VETUMA-palvelua käyttävän asiakkaan ja käytetyn jaetun salaisuuden ID. Mikäli yhdellä asiakkaalla on käytössään useampi jaettu salaisuus, käytössä on myös vastaavat RCVID arvot.

APPID - VETUMA-palvelua käyttävän asiakkaan sovelluksen ID. APPID arvon perusteella VETUMA-palvelussa erotellaan asiakassovellukset raportointia varten.

TIMESTMP - kutsun aikaleima.

TYPE - määrittelee VETUMA-palvelun tyyppin. Ensivaiheessa käytössä on ainoastaan tyyppi "LOGIN".

AU - määrittelee käytettävän toiminnon seuraavan taulukon mukaisesti. Mahdolliset menetelmät –sarake kuvaa menetelmät joita voidaan käyttää kyseisen toiminnon yhteydessä (SO ja SOLIST parametrit).

Toiminto	Arvo	Mahdolliset menetelmät (SO, SOLIST)
Tunnistus	"EXTAUTH"	"2", "3", "6"
Hyväksyntä	"CONFIRM"	"2", "3", "6"
Kiistämätön allekirjoitus	"SIGNATURE"	"2"

SO - määrittelee käyttäjälle oletuksena näytettävän menetelmän. Käyttäjä voi vaihtaa menetelmän toiseksi, mikäli useampi kuin yksi menetelmä on käytettävissä. SO parametrin arvon on oltava mukana SOLIST listalla.

Tupas-tapauksessa paluuviestin SO-parametrissa palautetaan käytetyn Pankin ID (esim. SO = "64", missä "6" on Tupas menetelmä ja "4" on käytetyn pankin ID.).

Menetelmä	Arvo	Mahdolliset toiminnot (AU)
HST	"2"	"EXTAUTH", "CONFIRM", "SIGNATURE"
Käyttäjätunnus-salasana	"3"	"EXTAUTH", "CONFIRM"
Tupas	"6"	"EXTAUTH", "CONFIRM"

SOLIST - määrittelee listan käytössä olevista menetelmistä. Lista on pilkulla eroteltu lista menetelmistä, esim. "2, 3, 6" (kts. SO -parametri).

USERID - määrittelee käyttäjän yksilöivän tunnisteen. (kts. myös EXTRADATA parametri).

Menetelmä	Kutsu / Vastaus	Arvo
-----------	-----------------	------

Versio: 1.0, 16.2.2006

HST-tunnistus	-/V	SATU
Käyttäjätunnus-salasana tunnistus	-/V	Käyttäjätunnus
Tupas-tunnistus	-/V	HETU
Tupas-hyväksyminen	K/V	HETU
HST-hyväksyminen	K/V	SATU
HST kiistämätön allekirjoitus	K/V	SATU

LG - määrittelee käyttäjälle oletuksena näytettävän käyttöliittymän kielen.

Kieli	Arvo
suomi	”fi”
ruotsi	”sv”
englanti	”en”

RETURL - sovelluksen osoite johon käyttäjä ohjataan VETUMA-palvelusta. RETURL parametrin URL:n on oltava HTTPS-URL (https://...).

CANURL - osoite johon käyttäjä ohjataan käyttäjän perueissa toiminnon. CANURL parametrin URL:n on oltava HTTPS-URL (https://...).

ERRURL - osoite johon käyttäjä ohjataan virhetilanteessa. ERRURL parametrin URL:n on oltava HTTPS-URL (https://...).

AP - käytettävä VETUMA sovellus ID (kappale 2.3).

TTS - HST-kortilla allekirjoitettava teksti (toiminto ”SIGNATURE”).

MAC - viestin tiiviste (kappale 2.9).

SIGNATURE - HST-kortilla luotu allekirjoitus (PKCS#7) base64 muodossa.

SIGNATURESTATUS - paluuarvo sisältää allekirjoituksen luonnin tuloksen.

Paluuarvo	Selite
”Valid”	Käyttäjän luoma allekirjoitus on

Versio: 1.0, 16.2.2006

	tarkistettu onnistuneesti
"Invalid"	Virhe käyttäjän luomassa allekirjoituksessa
"Not checked"	Käyttäjän allekirjoitusta ei tarkistettu

SUBJECTDATA - arvona palautetaan käyttäjän nimitiedot mikäli ne ovat saatavilla kyseiseen tapahtumaan liittyen. Nimitiedot koostuvat etunimestä ja sukunimestä (esimerkki: "ETUNIMI=MATTI PEKKA, SUKUNIMI=MEIKÄLÄINEN"). Tiedot muodostetaan seuraavasti:

Menetelmä	Nimitiedot
HST-tunnistus	Varmenteen 'Subject' -kentän nimitiedot
Tupas-tunnistus	Pankin palauttamien nimitiedot
Käyttäjätunnus-salasana tunnustus	Käyttäjän tietoihin tallennetut nimitiedot

EXTRADATA - kutsuviestissä EXTRADATA määrittelee suoritetaanko VTJ-kysely ja asetettu arvo kertoo suoritettavan VTJ-kyselyn tyypin. Toistaiseksi käytössä on vain "VTJ1" kysely, joka palauttaa varmenteen SATU tietoa vastaavan HETU:n. VTJ-kysely voidaan pyytää vain HST-tunnistuksen ja – allekirjoituksen yhteydessä.

Vastausviestissä EXTRADATA kenttä sisältää aina HETU:n Tupas- ja Käyttäjätunnus-tapauksissa sekä HST-tapauksessa mikäli VTJ-kysely on suoritettu.

Mikäli VTJ-kyselyssä tapahtuu virhe, EXTRADATA-kentässä palautetaan VTJ:n palauttama virheilmoitus.

Viesti	Arvo
Kutsuviesti	"VTJ1"
Vastausviesti	"HETU=ARVO", esim: "HETU=123456-7890"

2.6 Kutsuviesti

Seuraavassa taulukossa on esitetty esimerkki VETUMA-rajapinnan kutsusta. Kutsu muodostetaan HTML FORM -rakenteesta jossa on tarvittavat kentät sekä kentillä arvot. Lisää esimerkkiviestejä on kuvattu erillisessä dokumentissa (LIITE 2).

```
<form method="POST" action="https://tunnistus.suomi.fi/Login/app">
  <input name="RCVID" type="hidden" value="RCVID1">
  <input name="APPID" type="hidden" value="APP1">
  <input name="TIMESTAMP" type="hidden" value="20051028120232152472">
  <input name="SO" type="hidden" value="3">
  <input name="SOLIST" type="hidden" value="3">
  <input name="TYPE" type="hidden" value="LOGIN">
  <input name="AU" type="hidden" value="EXTAUTH">
```

Versio: 1.0, 16.2.2006

```
<input name="LG" type="hidden" value="fi">
<input name="RETURL" type="hidden"
value="https://www.kunta.fi/Sovellus/ret">
<input name="CANURL" type="hidden"
value="https://www.kunta.fi/Sovellus/can">
<input name="ERRURL" type="hidden"
value="https://www.kunta.fi/Sovellus/err">
<input name="AP" type="hidden" value="VAPP1">
<input name="MAC" type="hidden"
value="0D951095739D4D5D4704A0AC1C299AD6">
</form>
```

2.7 Vastausviesti

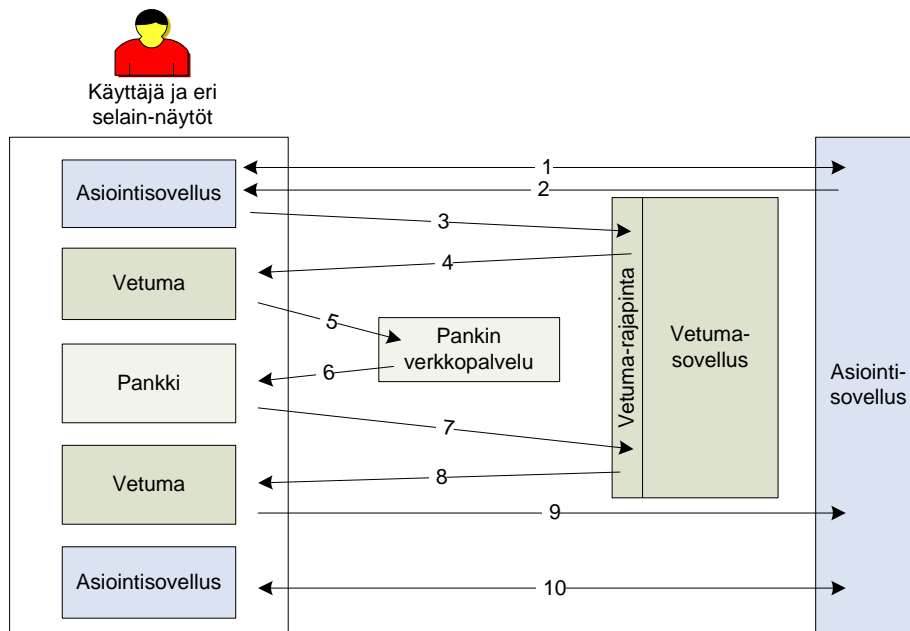
Seuraavassa taulukossa on esitetty esimerkki VETUMA-rajapinnan kutsusta. Kutsu muodostetaan HTML FORM –rakenteesta jossa on tarvittavat kentät sekä kentillä arvot.

```
<form method="POST" action="https://www.kunta.fi/Sovellus/ret">
  <input type="hidden" name="RCVID" value="RCVID1">
  <input type="hidden" name="TIMESTAMP" value="20051028120232152472">
  <input type="hidden" name="SO" value="3">
  <input type="hidden" name="USERID" value="username1">
  <input type="hidden" name="RETURL"
value="https://www.kunta.fi/Sovellus/ret">
  <input type="hidden" name="CANNURL"
value="https://www.kunta.fi/Sovellus/cann">
  <input type="hidden" name="ERRURL"
value="https://www.kunta.fi/Sovellus/err">
  <input type="hidden" name="MAC"
value="839CA6911FDD159811A073A0C8C1352A">
  <input type="hidden" name="SUBJECTDATA" value="ETUNIMI=Teemu,
SUKUNIMI=Testaaja">
</form>
```

2.8 Esimerkki Tupas-tunnistuksesta

Seuraavassa kuvassa on esitetty esimerkki tilanteesta jossa asiointisovellus pyytää VETUMA-rajapintaa käyttäen tunnistusta ja loppukäyttäjää tunnistetaan Tupas-menetelmällä.

Versio: 1.0, 16.2.2006



Kuva 4 Esimerkki Tupas-tunnistuksesta

Tapahtumien kuvaus vaiheittain:

1. Käyttäjä käyttää asiontisovellusta selaimella. Ennen VETUMA-palvelun käyttöä yhteys käyttäjän ja asiontisovelluksen välillä voi olla suojaamaton (HTTP) yhteys. Asiakkaan ja asiontisovelluksen välillä on muodostettava suojattu (HTTPS) yhteys siten että VETUMA-rajapintakutsu (vaihe 2) välitetään suojatun yhteyden kautta.
2. Asiointisovellus muodostaa VETUMA-rajapintakutsun joka sisältää kaikki tarvittavat kutsuviestin kentät sekä oikein lasketun tiivisteen.
3. Rajapintakutsu välitetään käyttäjän selaimelta VETUMA-palvelulle. Käyttäjälle näytetään käyttöliittymä josta hän valitsee Pankkitunnistamisen ja valitsee käyttämänsä pankin.
4. Asiakkaan valittua oman pankkinsa, tekee VETUMA-palvelu tarvittavan Tupas-kutsun kyseisen pankin verkkopalveluun.
5. Tupas-kutsu välittyy asiakkaan selaimelta pankin verkkopalveluun ja käyttäjälle näytetään pankin verkkopalvelun sivu. Käyttäjä syöttää pyydettyt pankin tunnistetiedot.
6. Pankin hyväksytyt tunnistetiedot, suorittaa pankin verkkopalvelu Tupas-paluu-kutsun takaisin VETUMA-palveluun.
7. Paluuviesti välitetään käyttäjän selaimen kautta VETUMA-palveluun. Käyttäjälle näytetään VETUMA-palvelussa tieto tapahtumasta sekä tapahtuman lopputuloksesta.
8. Käyttäjän valitessa paluu-toiminnon takaisin asiontisovellukseen, suorittaa VETUMA-palvelu kutsun, jossa välitetään VETUMA-vastaussanoma takaisin asiontisovellukseen.
9. Käyttäjän selaimen kautta välittyy VETUMA-vastaussanoma asiontisovellukseen. Asiointisovellus tarkistaa sanoman oikeellisuuden laskemalla viestin tiivisteen.

Versio: 1.0, 16.2.2006

Muut asiointitapahtumat VETUMA-palvelussa etenevät edellä kuvatun kaltaisesti. Muissa kuin Tupas- ja verkkomaksamistapahtumissa käyttäjä ei siirry VETUMA-palvelusta pankin verkkopalveluun vaan toiminnot suoritetaan VETUMA-palvelussa.

Edellisen esimerkin rajapintaviestit sekä muita lisäesimerkkejä on kuvattu erillisessä dokumentissa (LIITE 2).

2.9 Tiivisteiden laskeminen

2.9.1 Jaettu salaisuus ja algoritmi

Jaettu salaisuus ja algoritmi määräytyvät RCVID-kentän perusteella. Asiakaskohtaisissa liittymistiedoissa ovat RCVID, jaettu salaisuus ja käytetty hash algoritmi.

Tällä hetkellä tuettuja hash algorimeja ovat **MD5, SHA-1 ja SHA-256**. Algoritmeja suositellaan käytettäväksi seuraavassa järjestyksessä: SHA-256, SHA-1, MD5 siten että mikäli mahdollista, käytetään SHA-256 –algoritmia ja MD5 –algoritmia ainoastaan jos muut algoritmit eivät ole käytettävissä.

2.9.2 Kutsu

Kutsuviestin MAC lasketaan taulukossa (Taulukko 1) merkityistä kentistä ja jaetusta salaisuudesta. Kentät yhdistetään peräkkäin käyttäen erotinmerkkiä (&-merkki). Erotinmerkin tulee olla myös yhdistetyn merkkijonon viimeisenä kirjaimena. Merkintä P tarkoittaa että kenttä on aina mukana MAC-laskennassa, V että kenttä on mukana MAC laskennassa mikäli ko. kenttä on viestissä mukana sekä '-' että kenttä ei ole MAC laskennassa mukana. Mikäli kenttä on asetettu mutta arvo on tyhjä, on kyseinen parametri mukana MAC laskennassa.

Tästä merkkijonosta lasketaan MAC käyttäen valittua tiiviste-funktiota (hash-algoritmi).

Esimerkki:

```
100&20051028120232152472&LOGIN&EXTAUTH&3&username1&en&SharedSecret&
MD5 Hash → 0D951095739D4D5D4704A0AC1C299AD6
```

2.9.3 Vastaus

Vastausviestin tiiviste lasketaan samoin kuin kutsuviestistä.

2.10 Käyttäjän Sessio

Loppukäyttäjälle luodaan nk. istunto (sessio) hänen asioidessaan VETUMA-palvelussa. Istunnon avulla käyttäjän istunnonaikainen tila ylläpidetään VETUMA-palvelussa. Istunto pysyy voimassa käyttäjän käyttäessä palvelua ja käytön lakattua, määritellyn ajan.

VETUMA-palvelun istunnon voimassaoloaika on 10 min. VETUMA-palvelun istuntoa ei tarvita onnistuneen VETUMA-tapahtuman jälkeen. Mikäli käyttäjä tulee uudelleen VETUMA-palveluun vanhentuneella istunnolla (esim. tunnistamisen jälkeen hyväksyminen) luodaan käyttäjälle automaattisesti uusi istunto.

3. RAJAPINTAKUTSUT

Seuraavissa kappaleissa on kuvattu VETUMA-palvelun eri toimintojen kutsu- ja vastausviestit.

3.1 Tunnistaminen

Tunnistamiskutsulla voidaan VETUMA-palvelun avulla tunnistaa käyttäjä käyttäen eri tunnistamismenetelmiä.

Versio: 1.0, 16.2.2006

3.1.1 Kutsu- ja vastausparametrit

Seuraavassa taulukossa on kuvattu tunnistamisen kutsu- ja vastausviestien parametrien käyttö.

Nro	Nimi	Kutsuviesti	Vastausviesti	Huom
1	RCVID	X	X	
2	APPID	X	-	
3	TIMESTMP	X	X	
4	SO	X	X	
5	SOLIST	X	-	
6	TYPE	X	-	"LOGIN"
7	AU	X	-	"EXTAUTH"
8	USERID	-	X	
9	LG	X	X	
10	RETURL	X	X	
11	CANURL	X	X	
12	ERRURL	X	X	
13	AP	X	-	
15	MAC	X	X	
18	SUBJECTDATA	-	X	
19	EXTRADATA	- / X	X	"VTJ1" kutsuviestissä, mikäli halutaan suorittaa VTJ-kysely (vain HST)

3.1.2 Kutsu

Seuraavassa on esimerkki tunnistamiskutsusta (HST-tunnistus).

```
<form method="POST" action="https://tunnistus.suomi.fi/Login/app">
  <input name="RCVID" type="hidden" value="RCVID1">
  <input name="APPID" type="hidden" value="APP1">
  <input name="TIMESTMP" type="hidden" value="20051028120232152472">
  <input name="SO" type="hidden" value="2">
  <input name="SOLIST" type="hidden" value="2,6">
  <input name="TYPE" type="hidden" value="LOGIN">
  <input name="AU" type="hidden" value="EXTAUTH">
  <input name="LG" type="hidden" value="en">
  <input name="RETURL" type="hidden" value=
  "https://www.kunta.fi/Sovellus/ret">
  <input name="CANURL" type="hidden" value=
  "https://www.kunta.fi/Sovellus/can">
  <input name="ERRURL" type="hidden" value=
  "https://www.kunta.fi/Sovellus/err">
```

Versio: 1.0, 16.2.2006

```
<input name="AP" type="hidden" value="VAPP1">
<input name="MAC" type="hidden" value="0D951095739D4D5D4704A0AC1C299AD6">
</form>
```

3.1.3 Vastaus

Seuraavassa esimerkki VETUMA-palvelun lähettämästä vastausviestistä tunnistamistapahtuman jälkeen (HST-tunnistus).

```
<form method="POST" action="https://www.kunta.fi/Sovellus/ret">
<input type="hidden" name="RCVID" value="RCVID1">
<input type="hidden" name="TIMESTAMP" value="20051028120232152472">
<input type="hidden" name="SO" value="64">
<input type="hidden" name="USERID" value="010101-123N">
<input type="hidden" name="LG" value="fi">
<input type="hidden" name="RETURL" value=
"https://www.kunta.fi/Sovellus/ret">
<input type="hidden" name="CANURL" value=
"https://www.kunta.fi/Sovellus/can">
<input type="hidden" name="ERRURL" value=
"https://www.kunta.fi/Sovellus/err">
<input type="hidden" name="MAC" value="839CA6911FDD159811A073A0C8C1352A">
<input type="hidden" name="SUBJECTDATA" value="ETUNIMI=Teemu, SUKUNIMI=
Testaaja">
<input type="hidden" name="EXTRADATA" value="HETU=123456-123A">
</form>
```

3.2 Hyväksyminen

Hyväksyminen -kutsulla VETUMA-palvelu pyytää hyväksynnän loppukäyttäjältä. Käyttäjä suorittaa hyväksynnän tekemällä onnistuneen tunnistustapahtuman HST-kortilla, Tupas-tunnuksilla tai käyttäjätunnus-salasana -menetelmällä.

Hyväksyntää suoritettaessa käyttäjä ei voi itse käyttöliittymässä vaihtaa rajapinnassa määriteltyä hyväksymistapaa (SO), vaan hyväksyntä on suoritettava rajapintakutsun mukaisella menetelmällä.

3.2.1 Kutsu- ja vastausparametrit

Seuraavassa taulukossa on kuvattu hyväksymisen kutsu- ja vastausviestien parametrien käyttö.

Nro	Nimi	Kutsuviesti	Vastausviesti	Huom
1	RCVID	X	X	
2	APPID	X	-	
3	TIMESTAMP	X	X	
4	SO	X	X	
5	SOLIST	X	-	

Versio: 1.0, 16.2.2006

6	TYPE	X	-	"LOGIN"
7	AU	X	-	"CONFIRM"
8	USERID	X	X	
9	LG	X	X	
10	RETURL	X	X	
11	CANURL	X	X	
12	ERRURL	X	X	
13	AP	X	-	
15	MAC	X	X	
18	SUBJECTDATA	-	X	
19	EXTRADATA	- / X	X	"VTJ1" kutsuviestissä, mikäli halutaan suorittaa VTJ-kysely (vain HST)

3.2.2 Kutsu

Seuraavassa esimerkki hyväksyntä-kutsusta.

```
<form method="POST" action="https://tunnistus.suomi.fi/Login/app">
  <input name="RCVID" type="hidden" value="RCVID1">
  <input name="APPID" type="hidden" value="APP1">
  <input name="TIMESTAMP" type="hidden" value="20051028035002802052">
  <input name="SO" type="hidden" value="3">
  <input name="SOLIST" type="hidden" value="3">
  <input name="TYPE" type="hidden" value="LOGIN">
  <input name="AU" type="hidden" value="CONFIRM">
  <input name="USERID" type="hidden" value="username1">
  <input name="LG" type="hidden" value="fi">
  <input name="RETURL" type="hidden" value="https://www.kunta.fi/Sovellus/ret">
  <input name="CANURL" type="hidden" value="https://www.kunta.fi/Sovellus/can">
  <input name="ERRURL" type="hidden" value="https://www.kunta.fi/Sovellus/err">
  <input name="AP" type="hidden" value="VAPP1">
  <input name="MAC" type="hidden" value="9C65620B275FCB00DFA4C8DB52B372D5">
</form>
```

3.2.3 Vastaus

Seuraavassa esimerkki VETUMA-palvelun paluuviestistä hyväksymistapahtuman jälkeen.

```
<form method="POST" action="https://www.kunta.fi/Sovellus/ret">
  <input type="hidden" name="RCVID" value="RCVID1">
  <input type="hidden" name="TIMESTAMP" value="20051028035002802052">
```

Versio: 1.0, 16.2.2006

```

<input type="hidden" name="SO" value="3">
<input type="hidden" name="USERID" value="username1">
<input name="LG" type="hidden" value="fi">
<input type="hidden" name="RETURL" value=
"https://www.kunta.fi/Sovellus/ret">
<input type="hidden" name="CANURL" value=
"https://www.kunta.fi/Sovellus/can">
<input type="hidden" name="ERRURL" value=
"https://www.kunta.fi/Sovellus/err">
<input type="hidden" name="MAC" value="E4EE1CD3BA72206CB39D3A24AA09BCBF">
<input type="hidden" name="SUBJECTDATA" value= "ETUNIMI=Teemu,
SUKUNIMI=Testaaja">
<input type="hidden" name="EXTRADATA" value= "HETU=123456-123A">
</form>

```

3.3 Kiistämätön allekirjoitus

Kiistämätön allekirjoitus –kutsulla VETUMA-palvelun avulla käyttäjä allekirjoittaa HST-kortilla asiointisovelluksen antaman tekstimuotoisen data.

3.3.1 Kutsu- ja vastausparametrit

Seuraavassa taulukossa on kuvattu allekirjoittamisen kutsu- ja vastausviestien parametrien käyttö.

Nro	Nimi	Kutsuviesti	Vastausviesti	Huom
1	RCVID	X	X	
2	APPID	X	-	
3	TIMESTMP	X	X	
4	SO	X	X	"2"
5	SOLIST	X	-	"2"
6	TYPE	X	-	"LOGIN"
7	AU	X	-	"SIGNATURE"
8	USERID	-	X	
9	LG	X	X	
10	RETURL	X	X	
11	CANURL	X	X	
12	ERRURL	X	X	
13	AP	X	-	
14	TTS	X	X	
15	MAC	X	X	
16	SIGNATURE	-	X	

Versio: 1.0, 16.2.2006

17	SIGNATURESTATUS	-	X	
18	SUBJECTDATA	-	X	
19	EXTRADATA	- / X	X	"VTJ1" kutsuviestissä, mikäli halutaan suorittaa VTJ-kysely

3.3.2 Kutsu

Seuraavassa esimerkki Kiistämätön allekirjoitus –kutsusta.

```
<form method="POST" action="https://tunnistus.suomi.fi/Login/app">
  <input name="RCVID" type="hidden" value=" RCVID1">
  <input name="APPID" type="hidden" value="APP1">
  <input name="TIMESTAMP" type="hidden" value="20051028014114074072">
  <input name="SO" type="hidden" value="2">
  <input name="SOLIST" type="hidden" value="2">
  <input name="TYPE" type="hidden" value="LOGIN">
  <input name="AU" type="hidden" value="SIGNATURE">
  <input name="LG" type="hidden" value="fi">
  <input name="REURL" type="hidden" value=
"https://www.kunta.fi/Sovellus/ret">
  <input name="CANURL" type="hidden" value=
"https://www.kunta.fi/Sovellus/can">
  <input name="ERRURL" type="hidden" value=
"https://www.kunta.fi/Sovellus/err">
  <input name="TTS" type="hidden" value="Text to be signed digitally">
  <input name="AP" type="hidden" value="VAPP1">
  <input name="MAC" type="hidden" value="BBFE4DDD8A932C8E86620DBD8E0E1920">
  <input type="hidden" name="EXTRADATA" value="VTJ1">
</form>
```

3.3.3 Vastaus

Seuraavassa esimerkki VETUMA-palvelun lähettämästä paluuviestistä allekirjoituksen jälkeen.

```
<form method="POST" action="https://www.kunta.fi/Sovellus/ret">
  <input type="hidden" name="RCVID" value=" RCVID1">
  <input type="hidden" name="TIMESTAMP" value="20051028014114074072">
  <input type="hidden" name="SO" value="2">
  <input type="hidden" name="USERID" value="0102030405">
  <input name="LG" type="hidden" value="fi">
  <input type="hidden" name="REURL" value=
"https://www.kunta.fi/Sovellus/ret">
  <input type="hidden" name="CANURL" value=
"https://www.kunta.fi/Sovellus/can">
  <input type="hidden" name="ERRURL" value=
"https://www.kunta.fi/Sovellus/err">
  <input type="hidden" name="TTS" value="Data to be signed digitally">
```

Versio: 1.0, 16.2.2006

```
<input type="hidden" name="MAC"
value="0FFE9B547EC021D52F97DBB56E51EF12">
<input type="hidden" name="SIGNATURE" value="MIIFcgYJKoZIhvc... ">
<input type="hidden" name="SIGNATURESTATUS" value="Valid">
<input type="hidden" name="SUBJECTDATA" value=
"ETUNIMI=Teemu, SUKUNIMI=Testaaaja">
<input type="hidden" name="EXTRADATA" value="HETU=123456-7890">
</form>
```

4. VIRHETILANTEET

VETUMA-palvelusta palataan aina CANURL parametrin osoittamaan osoitteeseen käyttäjän keskeyttäessä / peruuttaessa toiminnon.

Mikäli käyttäjä vain sulkee selaimen, VETUMA-palvelu ei koskaan palauta tietoa kutsuvalle asiointisovellukselle.

Kaikissa virhetilanteissa kuten virheellisissä rajapintakutsuissa, epäonnistuneissa tunnistuksissa jne. palataan ERRURL parametrin osoittamaan osoitteeseen.

4.1 Toistuvat kutsut

Yleisesti selainpohjaisissa sovelluksissa on mahdollista käyttäjän toimesta aiheuttaa useampi kuin yksi peräkkäinen identtinen palvelupyyntö. Tätä ei voida jokaisessa tilanteessa ohjelmallisesti estää. VETUMA-palvelussa tällaisia toiminnallisuuksia on pyritty välttämään.

5. LIITTEET

1. VETUMA_palvelinvarmenteet.doc
2. VETUMA_sanomaesimerkit.doc