

**Suomalaisen
julkishallinnon
VETUMA-palvelu**

**Sovelluksille tarjotun
toiminnallisuuden kuvaus
versio 2.2**

Sisällysluettelo

1.	Johdanto	3
1.1	VETUMA-palvelun toiminnallisuus.....	3
1.2	VETUMA-palvelun toimintaympäristö	5
1.3	VETUMA-loppukäyttäjän ympäristö työasemassa	6
1.3.1	VETUMA-palvelun selainkäyttöliittymä	6
1.3.2	Yleiset vaatimukset ja rajoitukset selaimille	7
1.3.3	Tuetut selaimet	7
1.3.4	HST-kortin käyttö	8
1.3.5	Käyttäjän VETUMA-istunto	8
1.4	VETUMA-loppukäyttäjän ympäristö mobiililaitteessa	8
1.5	Tuotanto- ja testipalvelut.....	9
2.	Asiakkaan tiedot VETUMA-palvelussa	9
2.1	Jaettu salaisuus	9
2.2	VETUMA-asiakskonfiguraatio	10
2.2.1	Konfiguraatitiedot	10
2.2.2	Peruskonfiguraatio ja lisäkonfiguraatit	11
2.3	VETUMA-palvelua käyttävien sovellusten erottelu	12
3.	VETUMA-rajapinnan yleiset ominaisuudet	12
4.	Tunnistus, hyväksyminen ja allekirjoitus (LOGIN-palvelutyyppi)	12
4.1	Käyttäjän tunnistus	13
4.1.1	Salasanatunnistus	13
4.1.2	Kansalaisvarmennetunnistus	14
4.1.3	Tupas-tunnistus (pankkitunnistus)	15
4.1.4	Perustietojen haku VTJstä	16
4.1.5	Esimerkki tunnistuksen kulusta	17
4.2	Käyttäjän suorittama hyväksyminen	18
4.3	Käyttäjän suorittama kiistämätön sähköinen allekirjoitus	18
4.3.1	Sirukortin käyttöön perustuva allekirjoitus	19
4.3.2	Mobiiliallekirjoitus	19
4.3.3	Allekirjoituksen kulku	20
5.	Verkkomaksaminen (PAYMENT-palvelutyyppi)	21
5.1	Maksatus	21
5.1.1	Tuetut maksupalvelut.....	21
5.1.2	Maksatuksen kulku	22
5.1.3	Maksujen seuranta	23
5.1.4	Maksutapahtumien jäljittäminen.....	25
5.1.5	Mahdollisia poikkeustilanteita	28
5.2	Maksunpalautus	28
5.2.1	Tuki verkkomaksupalveluissa	29
5.2.2	Maksunpalautuksen kulku.....	30
5.2.3	Mahdollisia poikkeustilanteita	31
6.	Liitteet	31

1. JOHDANTO

VETUMA-palvelu on verkkotunnistus- ja maksamispalvelu joka on tarkoitettu julkishallinnon organisaatioiden asiointisovelluksien käyttöön. Fujitsu Services OY tuottaa palveluntuottajan ominaisuudessa VETUMA-palvelun julkishallinnon eri organisaatioiden käyttöön.

Tämä dokumentti kuvaa VETUMA-palvelun asiakkaidensa sovellusohjelmille tarjoaman toiminnallisuuden. Sovellukset voivat käyttää tätä toiminnallisuutta kutsurajapinnan kautta, joka on kuvattu erillisessä dokumentissa ”Suomalaisen julkishallinnon VETUMA-palvelu, kutsurajapinnan määrittely”.

VETUMA-palvelukokonaisuus sisältää tässä dokumentissa kuvatun toiminnallisuuden lisäksi mm. käyttäjähallintaan, laskutukseen ja raportointiin liittyviä toimintoja sekä käytön tukipalveluita. Tässä dokumentissa on kuitenkin kuvattu ainoastaan sovelluksille tarjottu, VETUMA-kutsurajapinnan kautta käytettävissä oleva toiminnallisuus.

Tämä dokumentti kuvaa VETUMA-palvelun version 2.2 toiminnallisuuden. Versiossa 2.2 on version 2.1 toiminnallisuuteen lisätty S-Pankin käyttömahdollisuus sekä päivitetty tuettujen selainten lista.

1.1 VETUMA-palvelun toiminnallisuus

VETUMA-palvelun versio 2.2 tarjoaa sovelluksille seuraavat toiminnot:

- Käyttäjän tunnistaminen hänen valitsemallaan menetelmällä.
 - Tuettuja menetelmiä ovat:
 - Kansalaisvarmenteeseen perustuva tunnistus, jossa varmenne voi sijaita sirukortilla tai matkapuhelimen SIM-kortilla. Sovelluksen niin halutessa noudetaan tunnistautuneen käyttäjän varmenteelta saadulla sähköisen asioinnin tunnukseksi (SATU) käyttäjän henkilötunnus (HETU) VTJ:stä.
 - Käyttäjätunnus/salasanaperiaatteeseen perustuvat tunnistusmenetelmät:
 - Selainpohjainen käyttäjätunnus/salasanatunnistus.
 - Tunnistuskoodin kysyminen matkapuhelimella
 - Verkkopankkien tarjoama tunnistuspalvelu (Tupas).
 - Sovelluksen niin halutessa noudetaan VTJstä joukko kansalaisia koskevia perustietoja kuten osoitetiedot ja kuntalaisuus. Tämän edellytyksenä on, että käyttäjä on tunnistautunut kansalaisvarmenteella tai pankkitunnuksilla.
- Toimenpiteen hyväksyttäminen käyttäjällä siten, että käyttäjä suorittaa hyväksymisen tunnistautumalla. Sovelluksen vastuulla on tällöin tallettaa tunnistautumisen tulos todisteena hyväksymisestä. Tuetut menetelmät ovat samat kuin tunnistuksessakin.
- Kansalaisvarmenteeseen perustuvan kiistämättömän sähköisen allekirjoituksen teettäminen käyttäjällä. Käyttäjän varmenne voi sijaita sirukortilla tai matkapuhelimen SIM-kortilla. VETUMA tarkastaa myös käytetyn varmenteen voimossaolon.
- Tietyn maksun maksattaminen käyttäjällä siten, että käyttäjä ohjataan valitsemaansa verkkomaksupalveluun maksua suorittamaan. Tuettuja maksupalveluita ovat:
 - Pankkien verkkomaksupalvelut
 - Luottokunnan verkkomaksupalvelu (Visa ja MasterCard)
- Maksetun maksun palautus kokonaan tai osittain maksajan tilille.

Versio: 2.2 31.12.2008

VETUMA-palvelun käyttö sen rajapinnan kautta edellyttää, että sovelluksella on käytössään asiakkaan VETUMA-asiakskonfiguraatio ja jaettu salaisuus.

- Asiakskonfiguraatio on niiden tietojen joukko joilla kuvataan palvelun mukautus tietyn asiakkaan asiointisovellusten tarpeisiin.
- Jaettua salaisuutta puolestaan käytetään rajapintakutsujen ja -vastausten alkuperän varmistamiseksi sekä suojaamiseksi muutoksilta kutsunvälityksen aikana.

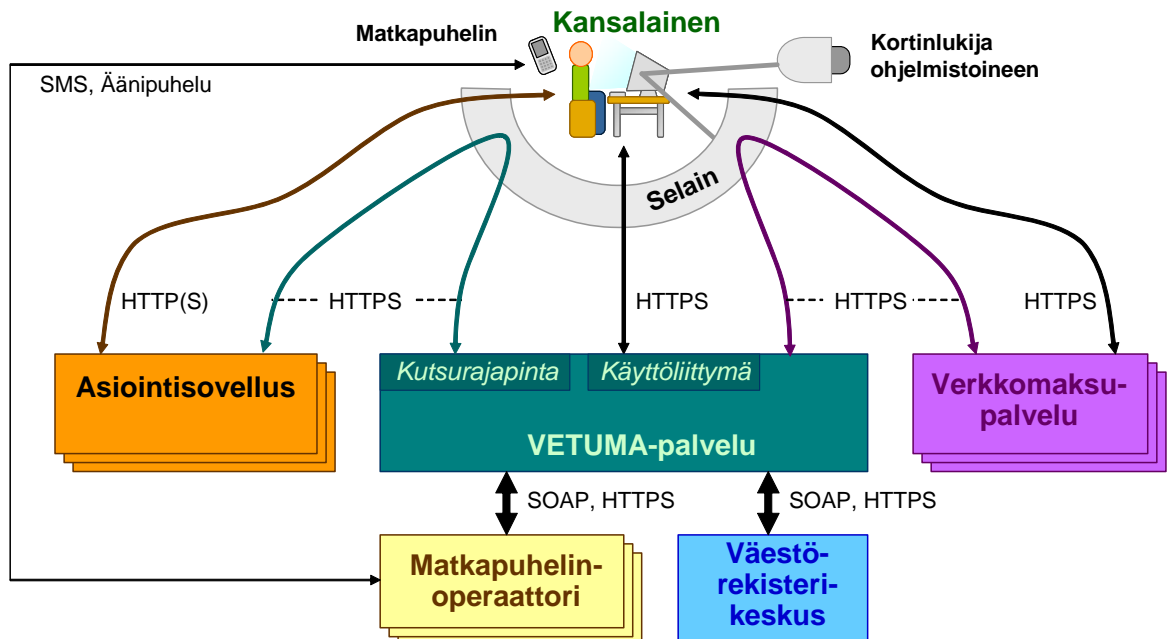
Asiakskonfiguraatio määritetään ja jaetut salaisuudet tunnistus- ja maksatuskäyttöön luodaan organisaation liittyttä VETUMA-palvelun asiakkaaksi. Tarvittaessa voidaan tietylle asiakkaalle määrittää lisää jaettuja salaisuuksia jos asiakas haluaa käyttää eri salaisuuksia eri asiointipalveluissaan.

Asiakskonfiguraatiossa määrätyt valinnat asettavat seuraavia vaatimuksia asiakkaalle:

- Jos asiakskonfiguraatiossa on sallittu käytettäväksi yksi tai useampia käyttäjätunnus/salasanapohjaisia tunnistusmenetelmiä, asiakkaan täytyy ylläpitää VETUMA-palvelussa omaa käyttäjärekisteriä.
- Jos asiakskonfiguraatiossa on sallittu käytettäväksi Tupas-tunnistus, tulee asiakkaalla olla Tupas-käyttöön oikeuttavat sopimukset pankkien kanssa. Tietyn asiakkaan asiointipalveluissa asioiville tarjotaan tunnistautumista varten vain niiden pankkien verkkopalvelut joiden kanssa kyseisellä asiakkaalla on Tupas-tunnistusta koskeva sopimus. Näin ollen teknisesti sopimuksia ei tarvita kaikkien pankkien kanssa, mutta joidenkin pankkien puuttuminen asettaa eri pankkien asiakkaat eriarvoiseen asemaan.
- Jos asiakskonfiguraatiossa on sallittu käytettäväksi maksaminen pankkien verkkopalveluilla, tulee asiakkaalla olla verkkomaksujen vastaanottamiseen oikeuttavat sopimukset pankkien kanssa. Tällöinkin kyseisen asiakkaan asiointipalveluissa asioiville tarjotaan maksamista varten vain niiden pankkien verkkopalvelut joiden kanssa asiakkaalla on VETUMAlle ilmoitettu verkkomaksujen vastaanottamista koskeva sopimus.
- Jos asiakskonfiguraatiossa on sallittu käytettäväksi maksaminen Luottokunnan verkkopalvelulla, tulee asiakkaalla olla verkkomaksujen vastaanottamiseen oikeuttava sopimus Luottokunnan kanssa.
- Jos asiakskonfiguraatiossa on sallittu käytettäväksi HETUn ja perustietojen noutaminen VTJ:stä, tulee asiakkaalla olla tähän oikeuttava sopimus VRK:n kanssa. Perustietojen hakua varten asiakas tarvitsee lisäksi VRKn myöntämän tietoluvan sille tietojoukolle jonka VETUMA-tunnistuksen yhteydessä aikoo hakea.

1.2 VETUMA-palvelun toimintaympäristö

Allaolevassa kuvassa on esitetty VETUMA-palvelun toimintaympäristö.



Kuva 1: VETUMA-palvelun toimintaympäristö

Käyttäjä (asioiva kansalainen) käyttää selaimella asiointisovellusta. Tarpeen tullen asiointisovellus kutsuu VETUMA-palvelua – sen kutsurajapintaa käyttäen – suorittamaan halutun toiminnon (esimerkiksi käyttäjän tunnistamisen). Kutsu välitetään käyttäjän selaimen kautta, jolloin käyttäjä siirtyy käyttämään VETUMA-palvelua sen oman käyttöliittymän kautta. VETUMA-palvelu toteuttaa itse osan sovelluksille tarjoamista toiminnista. Tupas-tunnistuksessa ja verkkomaksamisessa VETUMA-palvelu kuitenkin siirtää käyttäjän edelleen hänen valitsemansa verkkomaksupalveluun kyseisen palvelun rajapintakutsulla, joka myös välitetään käyttäjän selaimen kautta. Verkkomaksupalvelun vastaus jolla palataan sieltä VETUMA-palveluun välitetään myös käyttäjän selaimen kautta. Sovelluksen pyytämän toiminnon suorittamisen jälkeen VETUMA-palvelu palauttaa toiminnon tuloksen kuvaavan vastauksen sovellukselle käyttäjän työaseman kautta. Käyttäjä palautuu tällöin käyttämään asiointisovellusta sen käyttöliittymän kautta.

Sirukortilla sijaitsevaan kansalaisvarmenteeseen perustuvassa tunnistuksessa ja allekirjoituksessa käytetään lisäksi työasemassa olevaa kortinlukijaa ja korttiohjelmistoa käyttöliittymineen. SIM-kortilla sijaitsevaan kansalaisvarmenteeseen perustuvassa tunnistuksessa ja allekirjoituksessa käytetään puolestaan matkapuhelimen varusohjelmiston käyttöliittymän varmennetoimintoja.

Asiointisovelluksen, VETUMA-palvelun ja Pankin verkkopalvelun välillä ei siis ole suoria fyysisiä yhteyksiä vaan kaikki liikennöinti tapahtuu käyttäjän selaimen kautta. Yhteydet selaimen sekä niiden palvelinten välillä joissa asiointisovellus, VETUMA-palvelu ja pankkien verkkopalvelut toimivat suojataan HTTPS -yhteyksikäytäntöä käyttäen. Lisäksi rajapintakutsuissa osapuolten identiteetti varmistetaan ja viestien eheys taataan käyttäen jaettuun salaisuuteen perustuvaa turvatarkisteen laskentaa (Message Authentication Code, lyh. MAC).

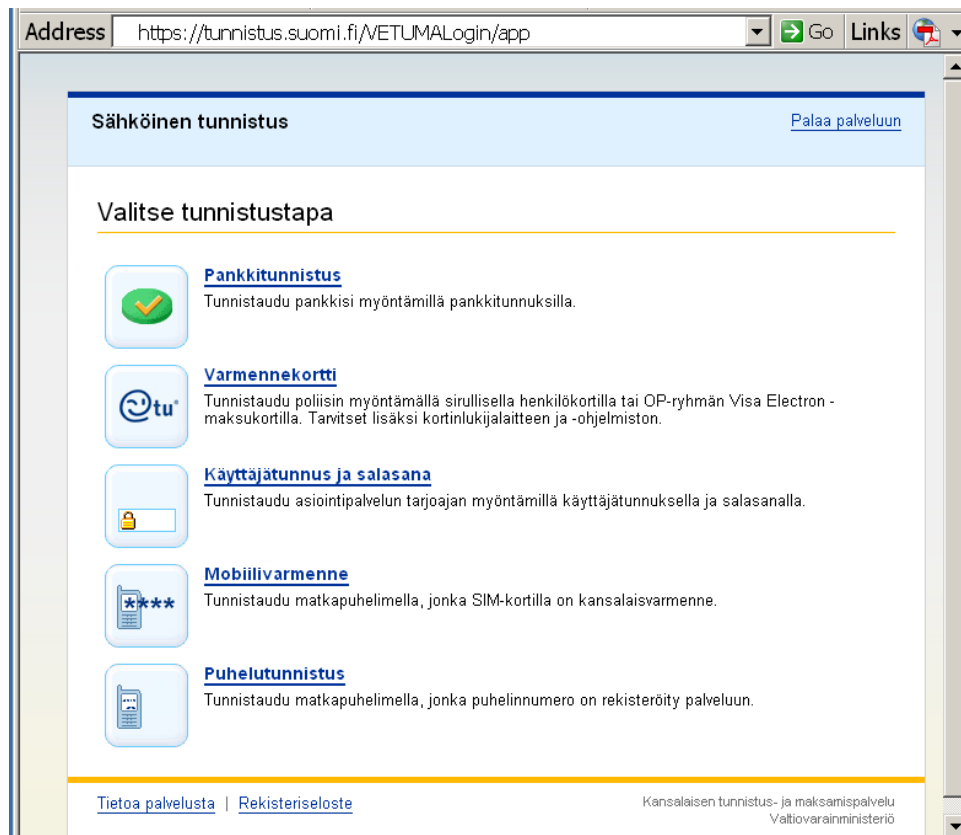
VETUMA-palvelu käyttää toiminnassaan myös Väestörekisterikeskuksen (VRK) tarjoamia palveluita (VTJ-kyselyt ja varmenteiden sulkulistat), mutta käyttäjä ei ole suoraan vuorovaikutuksessa näiden palveluiden kanssa. Mobiilivarmenteella tunnistauduttaessa ja allekirjoitettaessa VETUMA-palvelu käyttää operaattoreiden palveluita komentojen lähettämiseen, mutta käyttäjä ei ole suoraan vuorovaikutuksessa näidenkään palveluiden kanssa.

Käyttäjän tunnistautuessa matkapuhelimella kysyttävällä tunnistuskoodilla soittaa VETUMA normaalin äänipuhelun ja käyttäjä käyttää tällöin matkapuhelimensa tavallista puhelukäyttöliittymää.

1.3 VETUMA-loppukäyttäjän ympäristö työasemassa

1.3.1 VETUMA-palvelun selainkäyttöliittymä

VETUMA-palvelulla on selainkäyttöliittymä jota kansalainen käyttää suorittaessaan asiointisovelluksen pyytämiä toimintoja. Tietyn toiminnon käyttöliittymä säätty automaattisesti sen mukaan mitä menetelmiä sovellus pyytää VETUMA-kutsussa tarjottavaksi käyttäjälle. Allaolevassa kuvassa on esitetty VETUMA-palvelun tunnistuksen aloitussivu esimerkkinä VETUMA:n käyttöliittymästä.



Kuva 2: VETUMA-sovelluksen käyttöliittymäesimerkki

VETUMA-palvelua kutsuva asiointisovellus määrää kutsussa mitä kieltä VETUMA-palvelun käyttöliittymässä tulee käyttää (suomi, ruotsi tai englanti) sekä antaa halutessaan nimensä näytettäväksi VETUMA-palvelun käyttöliittymässä.

VETUMA-palvelu tarjoaa useimpien toimintojensa suorittamiseksi joukon vaihtoehtoisia menetelmiä. Yleisenä periaatteena on, että käyttäjä voi valita haluamansa menetelmän. Asiakas ja sovellus voivat tätä kuitenkin rajoittaa.

- VETUMA-asiakas voi asiakaskonfiguraatiossaan määrätä, mitä toimintojen suoritusmenetelmiä saa käyttää kun VETUMA-palvelua kutsutaan kyseisen asiakkaan sovelluksista.
- Sovellus voi edelleen VETUMA-kutsussa rajoittaa konfiguraatiossa määrättyä menetelmävalikoimaa.

1.3.2 Yleiset vaatimukset ja rajoitukset selaimille

Seuraava lista kuvaa yleisesti VETUMA-käytön asettamia vaatimuksia ja rajoituksia selaimelle ja sen asetuksille:

- VETUMA-palvelu tukee http-protokollan versioita 1.0 ja 1.1, joista jompaakumpaa (tai molempia) selaimen on tuettava.
- VETUMA-palvelun sivut on toteutettu XHTML 1.0 -standardin mukaisiksi. Palvelua voi käyttää myös selainohjelmilla, jotka eivät tue XHTML 1.0 -standardia. Tällöin palvelun ulkoasu on karsitumpi, mutta tekstisisällössä ja toiminnoissa ei ole eroa
- VETUMA-palvelu vaatii toimiakseen istuntoevästeiden (session cookies) käyttömahdollisuuden – ja sallimisen – selaimessa.
- VETUMA-palvelu käyttää JavaScript-selainskriptejä siirtymisessä vuorovaikutteisiin taustapalveluihin ja palaamisessa asiointisovellukseen. Palvelu toimii kuitenkin myös ilman selainskriptejä, mikäli niiden suorittaminen ei ole selaimessa sallittu. Tällöin käyttäjä suorittaa itse siirtymisen hänelle näytettävällä linkillä.
- SSL-salauksen käyttämiseksi selaimen tulee tukea SSL-versiota 3.0 tai TLS-versiota 1.0 ja vähintään 128-bittistä salausta, ja SSL-salauksen käyttö tulee olla sallittu selaimessa.
- SSL-salausta käytettäessä tulee selaimen voida luottaa VETUMA-palvelun palvelinvarmenteeseen.
 - VETUMA-palvelussa käytettävät palvelinvarmenteet on kuvattu liitteessä 1.
 - VETUMA-tuotantopalvelun palvelinvarmenteen myöntäjä (Thawte) on useimmissa selaintuotteissa oletusarvoisesti luotettujen varmentajien joukossa. Mikäli näin ei ole, luottamussuhde voidaan saada aikaan asentamalla selaimen VETUMA-palvelun palvelinvarmenteen myöntäjä luotetuksi varmentajaksi.
 - Jos käyttäjä ei kuitenkaan halua selaimensa jatkuvasti luottavan VETUMA-tuotantopalvelun palvelinvarmenteeseen, tulee selaimen myös sallia SSL-yhteyden muodostaminen siten, että se pyytää joka kerran käyttäjää hyväksymään VETUMA-palvelun palvelinvarmenteen yhteyden muodostamiseksi.
 - VETUMA-palvelun pääkäyttäjien käyttöliittymää käytettäessä sekä VETUMA-testipalvelua käytettäessä palvelinvarmenteen juurivarmenteen myöntäjä on Fujitsu Services (Fujitsu Topsis CA). Joustavaa pääkäyttäjä- ja testikäyttöä varten kannattaa siis lisätä Fujitsun juurivarmenne luotetuksi varmenteeksi. Varmenne on ladattavissa osoitteesta <https://testitunnistus.suomi.fi/info/>.

1.3.3 Tuetut selaimet

VETUMA-palvelu tukee seuraavia selaimia ja niiden versioita:

- Internet Explorer 6 ja 7
- Firefox 3
- Opera 9

VETUMA-palvelun toiminta näiden selainten uudempien versioiden kanssa testataan kahden kuukauden kuluessa uuden version virallisesta versiojulkistuksesta.

Myös muut kuin edellä mainitut yleisten standardien mukaiset selaimet toimivat todennäköisesti VETUMA-palvelua käytettäessä. Muita selaimia ei kuitenkaan testata erikseen.

1.3.4 HST-kortin käyttö

HST-kortilla tarkoitetaan tässä sirukorttia jolla on Väestörekisterikeskuksen (VRK) myöntämä kansalaisvarmenne. Tällaisia kortteja ovat esimerkiksi sirullinen henkilökortti ja tiettyjen pankkien luottokortit. HST-korttia käytettäessä käyttäjällä tulee myös olla kortin käyttöön tarvittavat laitteet ja ohjelmistot.

Tunnistuksessa tarvitaan:

- Kortinlukija joka pystyy lukemaan HST-kortteja.
- Kortinlukijaohjelmisto (esim. Fujitsu DigiSign Client, Setec SetWeb, Nexus Personal jne.) joka pystyy käsittelemään HST-kortteja.
- Kortinlukijaohjelmiston kanssa yhteensopiva selain.

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

Allekirjoituksessa tarvitaan lisäksi allekirjoituskomponentti jolla sähköinen allekirjoitus suoritetaan. Allekirjoituksessa VETUMA on yhteensopiva VRK:n kansalaisille ilmaiseksi jakeleman Fujitsu DigiSign Client-ohjelmiston kanssa.

Kortinlukijaohjelmiston ja allekirjoituskomponentin saatavuus työasemaan saattavat rajoittaa HST-kortin käyttöä. Kaikki kortinlukijaohjelmistot ja allekirjoituskomponentit eivät nimittäin välttämättä toimi kaikissa työasemakäyttöjärjestelmissä. VETUMAn kanssa voidaan käyttää VRK:n ilmaiseksi jakelemaa kortinlukijaohjelmistoa ja allekirjoituskomponenttia. Niiden kohdalla tuetut ympäristöt ja selaimet voi tarkistaa VRK:n sivuilta.

1.3.5 Käyttäjän VETUMA-istunto

Loppukäyttäjälle luodaan VETUMA-istunto (sessio) hänen siirtyessään VETUMA-palvelun käyttöliittymään. Istunnon avulla ylläpidetään käyttäjän VETUMA-toiminnon suorittamisen tilaa. Istunto syntyy kun sovelluksen (käyttäjän työaseman kautta lähettämä) kutsu otetaan vastaan. Istunto pysyy voimassa niin kauan kunnes VETUMA-palvelu palauttaa vastauksen asiointisovellukselle. VETUMA-istunto säilyy voimassa myös sinä aikana kun käyttäjä on siirretty välillä johonkin taustapalveluun. Istunto vanhenee jos käyttäjä ei anna VETUMA-palvelun odottamaa syötettä tai palaa taustapalvelusta 10 minuutissa

VETUMA-palvelun istuntoa ei tarvita suoritettua VETUMA-tapahtuman jälkeen. Mikäli käyttäjä tulee uudelleen VETUMA-palveluun (esimerkiksi tunnistamisen jälkeen hyväksyminen), luodaan käyttäjälle uusi istunto.

1.4 VETUMA-loppukäyttäjän ympäristö mobiililaitteessa

VETUMA-palvelu tukee tunnistusta, hyväksymistä ja kiistämätöntä allekirjoitusta myös mobiililaitteita (matkapuhelimia) käyttäen. Näissä tapauksissa käyttöliittymät mobiililaitteissa ovat seuraavat:

- Puhelinsoitolla kysyttävään tunnistuskoodiin perustuvassa mobiilitunnistuksessa ja -hyväksymisessä VETUMA-palvelu soittaa äänipuhelun käyttäjän mobiililaitteeseen, ja käyttäjä syöttää koodinsa puhelun aikana. Käyttöliittymänä on siis mobiililaitteen äänipuhelukäyttöliittymä.
- Mobiilikansalaisvarmenteeseen (matkapuhelimen SIM-kortilla sijaitsevaan kansalaisvarmenteeseen) perustuvassa tunnistuksessa ja hyväksymisessä sekä kiistämättömässä allekirjoituksessa VETUMA-palvelu lähettää mobiilioperaattorin palvelinohjelmiston kautta toimintoa vastaavan komennon mobiililaitteeseen. Käyttöliittymänä on tällöin mobiililaitteen varmennetta käsittelevän varusohjelmiston käyttöliittymä.

1.5 Tuotanto- ja testipalvelut

VETUMA-palvelu sisältää tuotantopalvelun sekä erillisen – rajapinnaltaan kuitenkin samanlaisen – testipalvelun. Kummallekin on määritelty omat erilliset osoitteensa.

Tuotantopalvelu on nimensä mukaisesti tarkoitettu tuotantokäyttöön. Sellaisella julkishallinnon organisaatiolla, jonka asiointisovellus kutsuu VETUMA-tuotantopalvelua, on oltava voimassaoleva VETUMA-liittymä sekä sopimukset haluamiensa VETUMA-palvelun taustapalveluiden (esimerkiksi pankkien verkkopalvelut) toimittajien kanssa kyseisten palveluiden käytöstä.

Testipalvelu on tarkoitettu VETUMA-liittymissopimuksen tehneiden asiakkaiden asiointisovellusten testaukseen. Se käyttää pankkien testiverkkopalveluita ja VRK:n testipalvelua, eikä sen käyttö vaadi sopimuksia pankkien ja VRK:n kanssa. Testipalvelun käyttöliittymässä annetaan myös virheilmoituksia jotka auttavat sovelluskehittäjiä testauksessa. Testipalvelu on kuvattu dokumentissa joka on saatavilla liittymissopimuksen tehneille asiakkaille. On myös syytä huomioida, että tiettyjen piirteiden testaus edellyttää taustapalveluiden käytön vaatimat välineet kuten HST-testikortti ja testimobiilivarmenne.

Tuotanto- ja testipalveluiden kutsuosoitteet ilmoitetaan asiakkaalle liittymisilmoituksen vastaanottamisen jälkeen. Mikäli osoitteet muuttuvat – esimerkiksi versiomuutosten yhteydessä – ilmoitetaan tästä liittymissopimuksen tehneille asiakkaille.

Tuotanto- ja testipalveluiden palvelinvarmenteiden ajantasaiset tiedot (voimassaoloaika, myöntäjä jne.) on kerrottu erillisessä dokumentissa ”VETUMA PALVELINVARMENTEET” (rajapintadokumentin LIITE 1).

2. ASIAKKAAN TIEDOT VETUMA-PALVELUSSA

Tietyn julkishallinnon organisaation liittyttyä VETUMA-palvelun asiakkaaksi muodostetaan VETUMA-palveluun seuraavat tiedot kyseisestä asiakkaasta:

- Jaetut salaisuudet joilla suojataan VETUMA-rajapinnan kautta välitettävät kutsu- ja vastausviestit siten, että niitä ei voi huomaamatta muuttaa, ja että vastaanottaja voi varmistaa, että viesti tulee oikealta lähettäjältä.
- Asiakaskonfiguraatio, jossa määritetään miten VETUMA-palvelu mukautetaan asiakkaan tarpeisiin (esimerkiksi taustapalveluiden käyttöön oikeuttavat tunnukset ja avaimet). Konfiguraatiolle annetaan tunnus joka on yksilöllinen koko VETUMA-palvelussa. Asiakas voi tarpeen vaatiessa muuttaa konfiguraationsa tietoja.

2.1 Jaettu salaisuus

Jaettua salaisuutta käytetään rajapintakutsuissa ja -vastauksissa lähettäjän identiteetin varmistamiseen sekä niissä välitettävän tiedon suojaamiseen välityksen aikaisia muutoksia vastaan.

- Asiointisovellus muodostaa kutsuviestille turvatarkisteen (Message Authentication Code, MAC) laskemalla tiivisteen (message digest) lähettämänsä kutsun parametrien sekä jaetun salaisuuden arvoista. Sovellus käyttää tiivisteen laskennassa kyseiselle salaisuudelle sovittua yksisuuntaista tiivistealgoritmia. Sovellus lähettää sitten sekä laskennassa käytetyn jaetun salaisuuden tunnuksen että muodostamansa turvatarkisteen kutsuviestin parametreina VETUMA-palvelulle. Kutsun saatuaan VETUMA-palvelu muodostaa turvatarkisteen arvon kutsussa saamistaan parametrien ja kutsussa viitatus jaetun salaisuuden arvoista, käyttäen kyseiselle salaisuudelle sovittua algoritmia. Mikäli tulos poikkeaa kutsussa tulleesta turvatarkisteesta, VETUMA-palvelu hylkää kutsun. Jaetun salaisuuden arvo ja sen yhteydessä käytettävä algoritmi ovat siis sekä sovelluksen että VETUMAN tiedossa.

Versio: 2.2 31.12.2008

- VETUMA-palvelu muodostaa vastausviestin turvatarkisteen samalla tavalla, käyttäen tiivisteiden laskennassa samaa jaettua salaisuutta jota käytettiin kutsussa. VETUMA lähettää sitten turvatarkisteen (sekä laskennassa käytetyn jaetun salaisuuden tunnuksen) vastausviestin parametreina asiointisovellukselle. Asiointisovellus muodostaa turvatarkisteen arvon vastauksen parametrien ja vastauksessa viitatus jaetun salaisuuden arvoista. Mikäli tulos poikkeaa vastauksessa tulleesta turvatarkisteesta, asiointisovelluksen tulee hylätä vastaus.

Jaettu salaisuus luodaan tekemällä satunnaislukugeneraattorilla 256-bittinen avain joka esitetään tekstinä heksadesimaalimuodossa. Siihen liitetään vielä käsittelyn helpottamiseksi kyseisen salaisuuden tunnus. Salaisuuden rakenne on tarkemmin esitetty rajapintamäärittelyssä: ”Suomalaisen julkishallinnon VETUMA-palvelu, kutsurajapinnan määrittely”.

Oletusarvoisesti tietylle VETUMA-asiakkaalle (esim. kunnalle tai valtion virastolle) tehdään kaksi salaisuutta, toinen tunnistustoimintojen käyttöä ja toinen maksatustoimintojen käyttöä varten. Jos asiakkaalla on tarve tämän lisäksi eriyttää salaisuuksien hallintaa eri asiointipalveluissaan, on asiakkaan mahdollista hankkia käyttöönsä tietylle sovellusjoukolla – tai jopa yksittäiselle sovellukselle – oma erillinen jaettu salaisuutensa. Jaettujen salaisuuksien jakelumenettely, salaisuuden arvon uusimismenettely ja lisäsalaisuuksien tilausmenettely on kuvattu VETUMA-palvelun asiakkaan asiointiohjeissa.

Jaettujen salaisuuksien tunnusten, arvojen ja algoritmien lisäksi VETUMA-palvelussa ylläpidetään kutakin salaisuutta kohti seuraavat tiedot:

- Salaisuuden voimassaoloaika.
- Mitä asiakaskonfiguraatioita saa käyttää kyseisen salaisuuden kanssa. Tätä tietoa tarvitaan vain siinä poikkeustapauksessa, että asiakas on tilannut useita konfiguraatioita.

VETUMA-palvelun jaetut salaisuudet ovat asiakaskohtaisia, eli yhden asiakkaan salaisuuden paljastuminen ei vaaranna muiden asiakkaiden VETUMA-käytön turvallisuutta.

2.2 VETUMA-asiakaskonfiguraatio

VETUMA-asiakaskonfiguraation avulla mukautetaan VETUMA-palvelu tietyn asiakkaan tarpeisiin. Asiointisovellus kertoo aina VETUMA-kutsussa mitä asiakaskonfiguraatiota VETUMA-palvelun tulee käyttää kyseisen kutsun palvelemisessa.

2.2.1 Konfiguraatitiedot

Konfiguraatitietoihin sisältyvät seuraavat tiedot:

- Mitä VETUMA-palvelun toimintojen suoritusmenetelmiä on kyseistä konfiguraatiota käyttävien asiointisovellusten käytettävissä. Asiakas voi esimerkiksi määrittellä, että vain Tupas-tunistus ja kansalaisvarmenteeseen perustuvat tunnistustavat ovat kyseisen asiakkaan sovellusten käytettävissä, mutta ei käyttäjätunnus-salasanatunnistus pohjaiset tunnistusmenetelmät.
- Mitä VETUMA-palvelun toiminnoissa käytettäviä lisäpalveluita on kyseistä konfiguraatiota käyttävien asiointisovellusten käytettävissä. Asiakas voi esimerkiksi määrittellä, onko tietojen kysely VTJstä kyseisen asiakkaan sovellusten käytettävissä vai ei.
- Tiedot asiakkaan taustapalvelusopimuksista
 - Tällaisia tietoja ovat ne tunnukset ja salaisuudet joita VETUMA-palvelun tulee käyttää kutsuessaan kyseisiä palveluita asiakkaan sovellusten puolesta.

- Kyseisiä taustapalveluita ovat:
 - Pankkien verkkopalvelut Tupas-tunnistusta, verkkomaksamista ja maksunpalautusta varten. Joillakin pankeilla yksi sopimus kattaa nämä kaikki, kun taas toisilla pankeilla on näille toiminnoille erilliset sopimukset.
 - Luottokunnan verkkopalvelu verkkomaksamista varten.
 - VRK:n VTJ-kyselypalvelu (SoSo).
 - Mobiilioperaattoreiden verkkopalvelut mobiilikansalaisvarmenteen käyttöön perustuvien komentojen (tunnistus ja allekirjoitus) lähettämiseksi
- Asiakas voi vastaanottaa käyttöön oikeuttavat tiedot taustapalveluiden toimittajilta ja luovuttaa ne VETUMA-palvelun toimittajalle (Fujitsu). Vaihtoehtoisesti asiakas voi valtuuttaa VETUMA-palvelun toimittajan vastaanottamaan tiedot suoraan taustapalvelun toimittajalta.
- Jos tietyllä asiakkaalla ei ole talletettuina sopimustietoja tiettyä taustapalvelua varten, ei kyseistä taustapalvelua voi käyttää (esimerkiksi tarjota käyttäjän valittavaksi) silloin, kun kutsut tulevat kyseisen asiakkaan sovelluksilta.

Asiointisovellus voi tunnistus-, hyväksymis- ja allekirjoituskutsussa edelleen rajoittaa käyttäjälle tarjottavia menetelmiä sekä käytettäviä lisäpalveluita. Esimerkiksi jos konfiguraatiossa on sallittu Tupas-tunnistus ja kansalaisvarmenteeseen perustuvat tunnistustavat, voi kyseistä konfiguraatiota käyttävä sovellus tunnistuskutsussa kuitenkin määrätä, että käyttäjälle tarjotaan vain Tupas-tunnistus.

Kutsussa ei voi laajentaa menetelmä- ja lisäpalveluvalikoimaa yli sen mitä sisältyy kutsussa viitattuun konfiguraatioon. Esimerkiksi:

- Mikäli käyttäjätunnus-salasanatunnistusta ei ole mukana konfiguraatiossa, ei sitä voi kyseistä konfiguraatiota käyttävissä rajapintakutsuissa saada käyttäjälle tarjolle.
- Mikäli tietojen kysely VTJstä ei ole mukana konfiguraatiossa, ei sitä voida myöskään kyseistä konfiguraatiota käyttävissä rajapintakutsuissa saada käyttöön.

2.2.2 Peruskonfiguraatio ja lisäkonfiguraatiot

Asiakkaan liittyessä VETUMA-palveluun luodaan asiakkaalle yksi asiakskonfiguraatio jonka tiedot määrätään asiakkaan toiveiden mukaan. VETUMA-palvelun toimittaja (Fujitsu Services OY) määrää konfiguraation tunnuksen. Asiakas voi halutessaan muuttaa tämän peruskonfiguraationsa tietoja pyytämällä sitä VETUMA-palvelun toimittajalta.

Koska kukin sovellus voi VETUMA-kutsuissaan määrätä käyttäjälle tarjottavat menetelmät ja toimintojen lisäpalvelut, ei sovelluskohtaisten toimintovalikoimien määrittelemiseksi tarvita lisäkonfiguraatioita.

Joissain tilanteissa voi kuitenkin olla tarvetta lisäkonfiguraatioille. Esimerkki tällaisesta tilanteesta on maksuliikenteen eriyttäminen asiakkaan eri asiointipalveluiden välillä.

- VETUMAN kautta maksettaessa maksut ohjataan kussakin maksupalvelussa tietylle samalle maksupalvelukohtaiselle tilille (sopimuksessa määritellylle kiinteälle tilille tai sopimuksen oletustilille). VETUMA-maksatuskutsussa ei voi antaa parametrina vastaanottotiliä koska useimmissa verkkomaksupalveluissa tili on kiinteä.
- Tietyille asiakkaalle tulleet maksusuoritukset voidaan erotella viitetietojen perusteella ja siirtää vastaanottotililtä eri asiointipalveluiden tileille.

- Mikäli tällainen siirtomenettely ei jostain syystä ole mahdollista, voi asiakas tehdä kunkin verkkomaksupalvelun kanssa useita maksujen vastaanottosopimuksia ja hankkia useita VETUMA-asiakaskonfiguraatioita joissa kussakin on oma sopimusjoukkonsa.

2.3 VETUMA-palvelua käyttävien sovellusten erottelu

Sovellus antaa VETUMA-palvelun kutsussa merkkijonomuotoisen sovellustunnuksen, joka talletetaan muiden kutsun tietojen kanssa VETUMA-palvelun lokitietoihin. Tätä tunnusta käytetään raportoitaessa kuinka paljon VETUMA-palvelua on missäkin sovelluksessa käytetty. Tiettyä asiakasta koskevassa käyttöraportissa tapahtumat jaotellaan tapahtumatyyppin sekä asiakaskohtaisen sovellustunnuksen perusteella. VETUMA-palvelussa ei kuitenkaan rekisteröidä sovellustunnuksia, eikä niitä tarvitse ilmoittaa liittymisilmoituksessa tai muutosilmoituksissa.

Sovellustunnukset ovat asiakaskohtaisia, ja kukin asiakas päättää mitä tunnuksia kyseisen asiakkaan sovellukset käyttävät. Tietyn asiakkaan kaikki sovellukset voivat käyttää samaa sovellustunnuksia, mutta eri sovelluksilla tai sovellusjoukoilla voi olla kullakin omat tunnuksensa.

3. VETUMA-RAJAPINNAN YLEISET OMINAISUUDET

VETUMA:n palvelurajapinta on viestirajapinta missä viestit on toteutettu käyttäen loppukäyttäjän selaimen kautta välitettäviä http-yhteyksikäytännön POST-komentoja. Viestien ja kommunikoinnin luottamuksellisuus perustuu käytettävien yhteyksien suojaukseen HTTPS-yhteyksikäytännöllä. Vaihdetujen viestien alkuperän varmistus ja eheys puolestaan taataan laskemalla kullekin viestille turvatarkiste (MAC) käyttäen asiakaskohtaista jaettua salaisuutta. Tiettyyn tapahtumaan liittyvän VETUMA-kutsun ja vastauksen yhteenliittämistä tuetaan tapahtumatunnuksella.

VETUMA-palvelu tarjoaa joukon toimintoja jotka on ryhmitelty palvelutyyppeihin. Kullakin toiminnolla on oma kutsu- ja vastaustyyppinsä.

Kun VETUMA-palvelu käsittelee sovellukselta saamaansa kutsua, niin kutsussa pyydetyn toiminnon suoritus voi onnistua tai toiminto voi jäädä eri syistä suorittamatta. VETUMA-palvelu palauttaa vastauksen siihen kutsussa ilmoitettuun paluuositteeseen joka vastaa kutsun käsittelyn jälkeistä tilannetta. Paluuositteet ovat:

- Toiminnon suoritus onnistui.
- Käyttäjä perui toiminnon.
- Toiminnon suorittaminen epäonnistui jostain syystä.

Tämän lisäksi VETUMA-palvelu palauttaa aina vastauksessa statusparametrin jolla kerrotaan onnistuiko suorittaminen vai jäikö toiminto suorittamatta, ja jälkimmäisessä tapauksessa myös syyn suorittamatta jättämiseen.

VETUMA-rajapinnan mekanismit sekä kutsu- ja vastaustyyppien parametrit on kuvattu tarkemmin rajapinnan määrittelydokumentissa ”Suomalaisen julkishallinnon VETUMA-palvelu, kutsurajapinnan määrittely”.

4. TUNNISTUS, HYVÄKSYMINEN JA ALLEKIRJOITUS (LOGIN-PALVELUTYYPPI)

VETUMA-palvelun palvelutyyppi **LOGIN** tarjoaa asiointisovelluksille seuraavat toiminnot: käyttäjän tunnistaminen, käyttäjän suorittama hyväksyminen ja käyttäjän suorittama kiistämätön sähköinen allekirjoitus.

4.1 Käyttäjän tunnistus

Tunnistustoiminto VETUMA-palvelussa tarkoittaa sitä, että VETUMA-palvelu tunnistaa asiointisovelluksen puolesta sovellusistunnon käyttäjän, eli sen henkilön, joka käyttää sitä selainta, jonka kautta sovellus lähetti tunnistuskutsun VETUMA-palvelulle.

4.1.1 Salasanatunnistus

VETUMA-palvelussa tuetaan seuraavia käyttäjätunnus/salasanaperiaatteen käyttöön perustuvia tunnistustapoja:

- Tunnistus käyttäjätunnuksella ja salasanalla selainkäyttöliittymän kautta.
- Tunnistus numeerisella tunnistuskoodilla jonka VETUMA kysyy matkapuhelimeen tekemällään puhelinsoitolla.

Jotta käyttäjän olisi mahdollista tunnistautua tiettyyn asiointipalveluun jollain edellämmainituista salasanapohjaisista tunnistustavoista:

- Sillä VETUMA-asiakkaalla jonka asiointipalveluun käyttäjä tunnistautuu tulee olla VETUMA-palvelussa ylläpidetty oma käyttäjärekisteri.
- Käyttäjän tulee olla rekisteröity mainittuun rekisteriin, siten että rekisterissä on kyseisen tunnistustavan vaatimat tunnistautumistiedot.

Käyttäjärekisterissä ylläpidetään jokaisesta käyttäjästä perustietoina henkilötunnus (HETU) ja nimitiedot (etunimi ja sukunimi), ja VETUMA-palvelu palauttaa ne aina tunnistusvastauksessa riippumatta siitä, minkä salasanapohjaisen tunnistustavan käyttäjä valitsi. Lisäksi rekisterissä ylläpidetään tunnistustapakohtaisia tunnistetietoja kuten käyttäjätunnusta tai puhelinnumeroa joka on rekisteröity tunnistuskoodin kyselyä varten.

4.1.1.1 Selainpohjainen salasanatunnistus

Valittuaan selainpohjaisen salasanatunnistuksen käyttäjä antaa VETUMA-palvelun tunnistuskäyttöliittymän kautta käyttäjätunnuksensa ja salasanansa

- VETUMA-palvelu tarkistaa käyttäjätunnus-salasanaparin vastaavuuden sen VETUMA-asiakkaan käyttäjärekisterissä jonka sovellus pyysi tunnistusta.
- Mikäli tunnistus onnistui, VETUMA-palvelu palauttaa sovellukselle perustietojen lisäksi myös käyttäjätunnuksen.
- Viidennen epäonnistuneen yrityksen jälkeen VETUMA-palvelu keskeyttää tunnistautumisen ja palauttaa vastauksensa sovellukselle kutsussa annettuun ERRURL-osoitteeseen statuksella REJECTED. Tällöin myös käyttäjän tili asiakkaan VETUMA-käyttäjärekisterissä lukittuu selainpohjaisen salasanatunnistuksen osalta, ja se pitää avata asiakkaan pääkäyttäjän toimesta ennen kuin sitä voi taas käyttää selainpohjaiseen salasanatunnistukseen.

4.1.1.2 Matkapuhelimella kysyttävä numeerinen tunnistuskoodi

Matkapuhelimella tehtävää, numeerisen tunnistuskoodin kyselyyn perustuvaa tunnistusta kutsutaan tässä lyhyesti puhelutunnistukseksi. Valittuaan puhelutunnistuksen käyttäjä antaa VETUMA-palvelun tunnistuskäyttöliittymän kautta sen puhelinnumeron joka on rekisteröity hänelle puhelutunnistusta varten, ja määrää tunnistuksen jatkumaan seuraavaan vaiheeseen.

- VETUMA-palvelu soittaa käyttäjän antamaan numeroon ja pyytää tunnistuskoodin. Pyyntö esitetään sovelluksen tunnistuskutsussa määräämällä kielellä (joka on sama jota käytetään myös VETUMA-palvelun selainkäyttöliittymässä kyseistä kutsua palveltaessa).

Versio: 2.2 31.12.2008

- Käyttäjä antaa puhelun kautta sen tunnistuskoodin joka on hänelle rekisteröity sen asiakkaan VETUMA-käyttäjärekisterissä jonka sovellus pyysi tunnistusta.
- VETUMA-palvelu tarkistaa puhelulla saamastaan koodista onko se sama kuin annetulle puhelinnumerolle rekisteröity koodi asiakkaan käyttäjärekisterissä. Sen jälkeen VETUMA-palvelu ilmoittaa puhelussa käyttäjälle – edelleen sovelluksen valitsemalla kielellä – onnistuiko tunnistus vai ei, ja sulkee puhelun.
- Mikäli tunnistus onnistui, VETUMA-palvelu palauttaa sovellukselle perustietojen lisäksi myös puhelutunnistus-puhelinnumeron.
- Viidennen epäonnistuneen yrityksen jälkeen VETUMA-palvelu keskeyttää tunnistautumisen ja palauttaa vastauksensa sovellukselle kutsussa annettuun ERRURL-osoitteeseen statuksella REJECTED. Tällöin myös käyttäjän tili asiakkaan VETUMA-käyttäjärekisterissä lukittuu puhelutunnistuksen osalta, ja se pitää avata asiakkaan pääkäyttäjän toimesta ennen kuin sitä voi taas käyttää puhelutunnistukseen.

4.1.2 Kansalaisvarmennetunnistus

VETUMA-palvelussa tuetaan seuraavia kansalaisvarmenteen käyttöön perustuvia tunnistustapoja:

- Tunnistus sirukortille talletetulla kansalaisvarmenteella.
- Tunnistus mobiililaitteen SIM-kortille talletetulla kansalaisvarmenteella.

Kansalaisvarmennetunnistuksessa ei tarvita käyttäjärekisteriä.

Kansalaisvarmenteelta löytyvät käyttäjän sähköisen asioinnin tunnus (SATU) ja nimitiedot, ja VETUMA-palvelu palauttaa ne aina tunnistusvastauksessa riippumatta siitä, minkä kansalaisvarmennepohjaisen tunnistusmenetelmän käyttäjä valitsi. Lisäksi VETUMA-palvelu noutaa – sovelluksen sitä pyytäessä – käyttäjän HETU:n tai perustiedot VTJ:stä ja palauttaa myös sen/ne tunnistusvastauksessa. Jos VTJ-kyselyssä tapahtuu virhe, palauttaa VETUMA-palvelu kuitenkin VTJ:stä saamansa virhekoodin.

4.1.2.1 Sirukortin käyttöön perustuva kansalaisvarmennetunnistus

Käyttäjän valittua sirukortin käyttöön perustuvan kansalaisvarmennetunnistuksen:

- VETUMA-palvelu pyytää tunnistuskäyttöliittymässään käyttäjää laittamaan kansalaisvarmenteen sisältävän sirukorttinsa kortinlukijaan ja välittää tunnistuspyynnön käyttäjän selaimelle. Selain aktivoi työaseman sirukorttiohjelmiston lukemaan sirukorttia.
- Sirukorttiohjelmisto pyytää käyttäjää antamaan tunnistusta varten tarkoitetun PIN-koodin.
- Sirukorttiohjelmisto tarkistaa PIN-koodin ja jos se on oikea, suorittaa sirukortilta saatavaa, varmenteeseen liittyvää salaista avainta hyväksikäyttäen käyttäjän tunnistamisen. Tieto tunnistuksen tuloksesta – ja onnistuneen tunnistuksen tapauksessa varmenteen sisältö – toimitetaan selaimen kautta VETUMAlle.
- Mikäli tunnistus onnistui, VETUMA-palvelu palauttaa sovellukselle tunnistusvastauksessa varmenteelta saadun SATUn ja nimitiedot sekä sovelluksen pyytäessä myös VTJ:stä hakemansa käyttäjän HETU:n tai perustiedot
- Mikäli tunnistautuminen epäonnistui VETUMA-palvelu palauttaa vastauksensa sovellukselle kutsussa annettuun ERRURL-osoitteeseen statuksella REJECTED.

4.1.2.2 Mobiilikansalaisvarmennetunnistus

Mobiililaitteessa olevalle SIM-kortille tallennettua kansalaisvarmennetta käyttäen tehtävää tunnistusta kutsutaan tässä lyhyesti mobiilikansalaisvarmennetunnistukseksi.

Valittuaan mobiilikansalaisvarmennetunnistuksen käyttäjä antaa VETUMA-palvelun tunnistuskäyttöliittymän kautta sen SIM-kortin puhelinnumeron jolle hänen kansalaisvarmenteensa on tallennettu.

- VETUMA-palvelu lähettää tunnistuspyynnön matkapuhelinoperaattorille, joka välittää pyynnön edelleen annettuun puhelinnumeroon. VETUMA-palvelun kutsuma operaattori suorittaa tarvittaessa tunnistusvierailun (roaming) käyttäjän kotioperaattorin verkkoon (sen operaattorin verkkoon jonka SIM-kortilla käyttäjän kansalaisvarmenne on.)
- Sen mobiililaitteen varusohjelmisto jossa varmenteen sisältävä SIM-kortti on pyytää käyttäjää antamaan varmenteeseen liittyvän, tunnistusta varten tarkoitetun SPIN-koodin (tunnusluvun).
- Mobiililaitteen varusohjelmisto suorittaa tunnistamisen tarkistamalla SPIN-koodin ja palauttaa operaattorin ohjelmistolle tiedon tuloksesta – sekä varmenteen sisällön jos tunnistus onnistui.
- Matkapuhelinoperaattori välittää VETUMA-palvelulle tiedon tunnistuksen onnistumisesta, ja onnistuneen tunnistuksen yhteydessä myös varmenteen sisällön.
- Mikäli tunnistus onnistui, VETUMA-palvelu palauttaa sovellukselle varmenteen sisältämät nimitiedot ja käyttäjän SATU:n. Mikäli sovellus on sitä pyytänyt, VETUMA-palvelu hakee VTJ:stä käyttäjän HETU:n tai perustiedot ja palauttaa myös sen/ne sovellukselle tunnistusvastauksessa.
- Mikäli tunnistautuminen epäonnistui VETUMA-palvelu palauttaa vastauksensa sovellukselle kutsussa annettuun ERRURL-osoitteeseen statuksella REJECTED.

Mobiilikansalaisvarmennetunnistuksessa voidaan käyttää FiCom:in suosittelemia haittakäytön estomekanismeja:

- Istuntotunnus. VETUMA-palvelu luo istuntotunnuksen sovelluksen puolesta ja näyttää sen käyttäjälle mobiilikansalaisvarmennetunnistuksen käyttöliittymässä.
- Käyttäjakohtainen häirinnän estokoodi. Käyttäjä voi sopia häirinnän estokoodin käytöstä kotioperaattorinsa kanssa. Mikäli käyttäjällä on häirinnän estokoodi käytössään, hän antaa kyseisen koodin VETUMA-palvelun tunnistuskäyttöliittymässä puhelinnumeron lisäksi. VETUMA-palvelu välittää häirinnän estokoodin operaattorille jonka toimittaa sen tunnistuskomennon yhteydessä mobiililaitteeseen.

4.1.3 Tupas-tunnistus (pankkitunnistus)

Suomen Pankkiyhdistys on määritellyt yhteisen rajapinnan (Tupas-rajapinnan) jonka kautta eri pankkien verkkopalvelut tarjoavat Internet-palveluiden tarjoajille käyttäjän tunnistusta – kukin oman verkkopankkitunnistuskäytäntönsä mukaan. Tupas-tunnistuksessa VETUMA-palvelu välittää tunnistuspyynnön käyttäjän valitseman pankin verkkopalvelulle käyttäen edellä mainittua Tupas-rajapintaa.

Saatuun tunnistusvastauksen pankin verkkopalvelulta – ja mikäli tunnistus onnistui – VETUMA-palvelu palauttaa sovellukselle verkkopalvelun palauttamien käyttäjän nimitiedot sekä käyttäjän HETUn. VETUMA-palvelu edellyttää tunnisteen olevan nimenomaan HETU. Tästä syystä VETUMA-asiakkaiden ja pankkien välisissä verkkopalvelusopimuksissa on palautettavaksi tunnistetiedoksi määrättävä Tupas-määrittelyn mukainen ”Selväkielinen perustunnus”. VETUMA-palvelu tarkistaa, että pankin palauttama tieto on muodoltaan HETU.

Jos näin ei ole, VETUMA-palvelu palauttaa vastauksensa sovellukselle kutsussa annettuun ERRURL-osoitteeseen statuksella FAILURE..

Tupas-tunnistuksessa ei tarvita VETUMA-käyttäjärekisteriä.

4.1.4 Perustietojen haku VTJstä

VETUMA-tunnistusta käyttävä sovellus voi pyytää VETUMAA noutamaan onnistuneen tunnituksen jälkeen määrättyjä Väestötietojärjestelmässä (VTJ) ylläpidettyjä tietoja tunnistetusta käyttäjästä. Tietyn asiakkaan sovellusten noudettavissa olevat tietojoukot – VRKn terminologiassa tuotteet – määrittellään asiakkaan VRK:lta saamissa tietoluissa, ja sovellus ilmoittaa tunnistuskutsussa minkä VTJ-sovelluskyselytuotteen tiedot haetaan. Tiedot palautetaan samassa esitysmuodossa jossa haussa käytettävä VRKn SoSo-kysely ne palauttaa.

4.1.4.1 Noudettavat tiedot

VETUMAN kautta suoritettavaa VTJ-kyselyä varten määritelty VTJ-kyselytuotteet sisältävät erilaisia yhdistelmiä VETUMAN kautta suoritettaville kyselyille sallitusta tietojoukosta. Nykyisellään on tarjolla kaikille VETUMA-asiakkaille vakiokyselytuote jossa on seuraavat tiedot:

- Henkilötunnus
- Nimitiedot
- Kotikunta
- Osoitetiedot
- Äidinkieli
- Kuolinaika
- Tieto siitä, onko käyttäjä Suomen kansalainen

Laajennetulla VTJ-kyselyllä saatavat tiedot on määritelty VRK:n tarkoitusta varten myöntämässä tietoluissa. VETUMA palauttaa noutamansa henkilötiedot sovellukselle VTJn SoSo-kyselyn vastaussanomana muodossa. Vastaussanomana XML-schemassa viitataan VTJkyselyn henkilötietojen tietotyypimäärittelyn XML-schemaan. Siinä kuvataan kaikki VTJ-henkilötietokyselyiden vastauksissa käytettävät tietotyypit.

- Perustietojen XML-scheman tunnistetiedot ovat:

```
<xs:schema xmlns=http://xml.vrk.fi/schema/vtjkysely
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:vtj="http://xml.vrk.fi/schema/vtj/henkilotiedot/1"
targetNamespace="http://xml.vrk.fi/schema/vtjkysely"
elementFormDefault="qualified"
attributeFormDefault="unqualified">
```

- Tietotyypimäärittelyn XML-scheman tunnistetiedot ovat:

```
<xs:schema
xmlns="http://xml.vrk.fi/schema/vtj/henkilotiedot/1"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://xml.vrk.fi/schema/vtj/henkilotiedo
t/1">
```

VRK toimittaa schemat asiakkaalle Vetuman VTJ-kyselyitä koskevan tietolupaprosessin yhteydessä. Perustietojen vastaussanomana XML-schema on lisäksi saatavissa rajapintamäärittelyn liitteenä Liite3_PERUSJHHS2.xsd.

4.1.4.2 Tunnistustavat

VETUMA-palvelu saa hakea sovellukselle tunnistautuneen käyttäjän perustietoja Väestötietojärjestelmästä mikäli käyttäjä on tunnistautunut riittävän vahvalla tunnistusmenetelmällä. Tällä hetkellä riittävän vahvoiksi tunnistusmenetelmiksi hyväksytyt menetelmät ovat kansalaisvarmenteeseen perustuvat tunnistusmenetelmät sekä pankkitunnistus (Tupas-tunnistus).

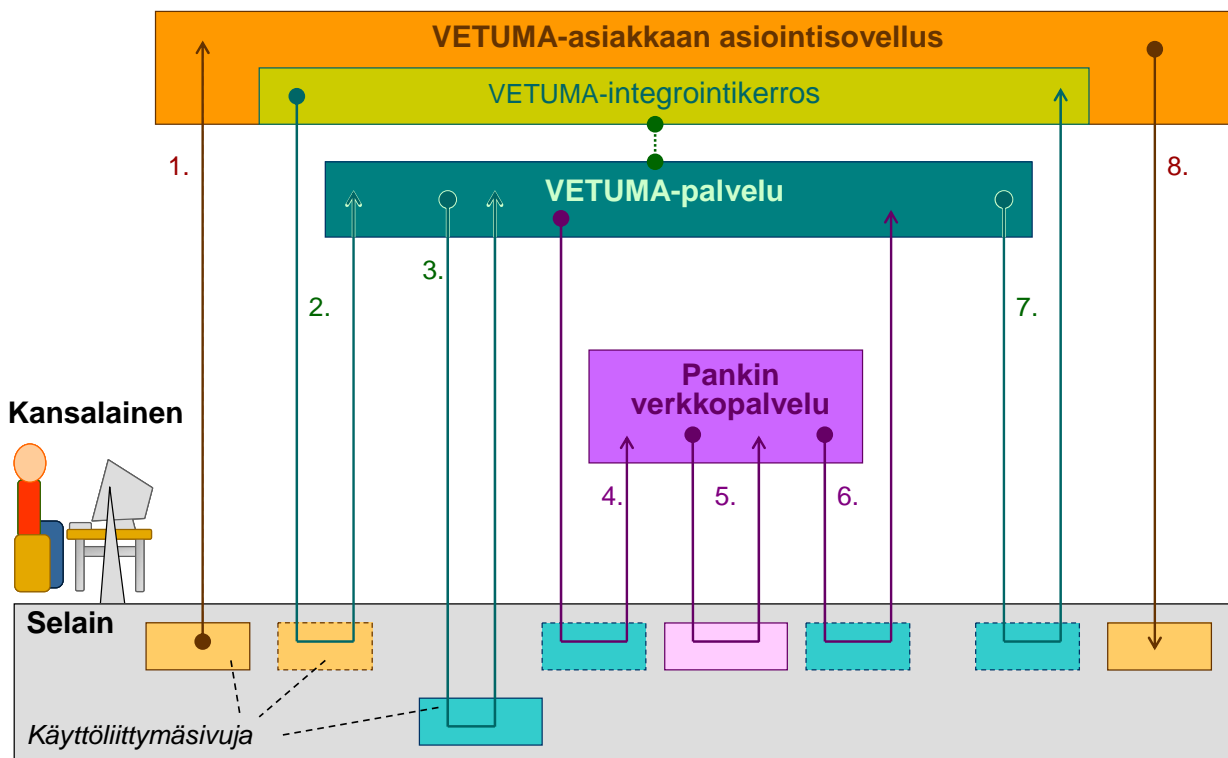
4.1.4.3 Tietolupamenettely

Niiden VETUMA-asiakkaiden jotka haluavat VETUMA-palvelun noutavan asiointipalveluilleen käyttäjän perustiedot VTJ:stä tulee hankkia VRK:lta kyseiselle tietojoukole tietolupa.

- Sopimuksen VRKn kanssa tekevä VETUMA-asiakas ilmoittaa käyttöä ja laskutusta varten tarvittavat tiedot, sitoutuu noudattamaan lupaehtoja, ja saa VRK:lta käyttäjätunnuksen ja salasanan. Asiakas luovuttaa käyttäjätunnuksen ja salasanan VETUMA-palvelulle käytettäväksi kun VETUMA-palvelu suorittaa kyselyitä kyseisen asiakkaan sovelluksilta tulevien tunnistuskutsujen yhteydessä.
- VRK on määritellyt VETUMAn kautta VTJ-kyselyllä saatavissa olevan perustietojen tietojoukon jolle on antanut oman tuotetunnuksen "VTJ-VETUMA-Perus". Asiakas saa näille perustiedoille tietoluvan VRK:lta.
- Asiakkaan sovelluksen pyytäessä tietojen hakua VTJstä VETUMA-tunnistuksen yhteydessä antaa se perustietojoukkoa vastaavan VTJ-tuotteen tuotetunnuksen VETUMA-tunnistuskutsun parametrina. VETUMA tekee tuotetunnuksella VTJ-kyselyn jonka vastauksessa VTJ palauttaa kyselytuotteeseen sisältyvät tiedot. VETUMA välittää tiedot sovellukselle omassa tunnistusvastauksessaan.

4.1.5 Esimerkki tunnistuksen kulusta

Tupas-tunnistuksen eteneminen on esitetty allaolevassa kuvassa esimerkkinä tunnistuksen kulusta:



Kuva 3: Tupas-tunnistuksen kulku

1. Käyttäessään selaimellaan VETUMA-asiakkaan asiointisovellusta käyttäjä (kansalainen) pyytää sellaista toimintoa joka vaatii käyttäjän tunnistamista.
2. Asiointisovellus varmistaa (huolehtii siitä), että yhteys käyttäjän selaimen on SSL/TLS-suojattu, rakentaa VETUMA-tunnistuskutsun, ja toimittaa kutsun käyttäjän selaimen kautta VETUMA-palvelulle (kuten dokumentissa ”Suomalaisen julkishallinnon VETUMA-palvelu, kutsurajapinnan määrittely” on kuvattu).
3. VETUMA-palvelu tarkistaa kutsun oikeellisuuden, ja kelvollisen kutsun tapauksessa avaa oman käyttöliittymänsä käyttäjän selaimen HTTPS-yhteyttä käyttäen, antaen käyttäjän valita tunnistautumismenetelmän.
4. Käyttäjän valittua tunnistautumismenetelmäksi pankkitunnistuksen (Tupas), VETUMA-palvelu rakentaa Tupas-kutsun ja toimittaa sen käyttäjän selaimen kautta valitun pankin verkkopalvelulle (kuten Tupas-määrittelyssä on kuvattu).
5. Valitun pankin verkkopalvelu suorittaa käyttäjän tunnistuksen oman HTTPS-suojatun käyttöliittymänsä kautta.
6. Valitun pankin verkkopalvelu rakentaa Tupas-vastauksen ja toimittaa sen käyttäjän selaimen kautta HTTPS-yhteyttä käyttäen VETUMA-palvelulle (kuten Tupas-määrittelyssä on kuvattu).
7. Käyttäjän tunnistauduttua VETUMA-palvelu rakentaa VETUMA-tunnistusvastauksen ja toimittaa sen käyttäjän selaimen kautta asiointisovellukselle. Vastaus toimitetaan selaimelle VETUMA-palvelun käyttöliittymän tunnistuspaluu-sivulla, jolta se lähtee asiointisovellukselle käyttäjän hyväksytyä paluun.
8. Asiointisovellus tarkistaa vastauksen oikeellisuuden ja jatkaa toimintaansa hyödyntäen tunnistusvastauksessa palautettuja tietoja. Sovellus keskustelee jälleen käyttäjän kanssa oman käyttöliittymänsä kautta.

4.2 Käyttäjän suorittama hyväksyminen

Käyttäjän suorittama hyväksyminen tarkoittaa tässä sitä, että asiointisovellus pyytää aiemmin jo tunnistettua sovellusistunnon käyttäjää hyväksymään tunnistautumalla sellaisen asiointitoiminnon joka vaatii aiemman tunnistuksen lisäksi erillisen hyväksynnän. Asiointisovelluksen vastuulla on tallettaa onnistuneen hyväksymistapahtuman tiedot todistuksena hyväksymisestä. Käyttäjän tällä tavoin suorittama hyväksyminen on kuitenkin siinä mielessä epävirallinen hyväksyminen, että sillä ei ole lain kannalta samanlaista sitovuutta kuin kiistämättömällä sähköisellä allekirjoituksella.

Käytännössä hyväksyminen tehdään siten, että asiointisovellus antaa VETUMA-palvelulle käyttäjän tunnuksen ja pyytää palvelua varmistamaan tunnistamalla, että kyseinen käyttäjä edelleen käyttää sitä selainta, jolta pyyntö hyväksymistä vaativan toiminnon suorittamiseen tuli.

Mikäli käyttäjää ei ole sovelluksessa vielä tunnistettu, voi sovellus suorittaa samantapaisen epävirallisen hyväksyttämisen käyttäen VETUMA-palvelun tunnistustoimintoa. Sovellus voi esimerkiksi antaa käyttäjän tutustua lomakkeeseen ja täyttää sen ilman tunnistusta, mutta täytetyn lomakkeen saatuaan pyytää käyttäjää ilmoittamaan tunnistautumalla henkilöllisyytensä ja samalla vahvistamaan lomakkeessa antamansa tiedot.

4.3 Käyttäjän suorittama kiistämätön sähköinen allekirjoitus

Käyttäjän suorittama kiistämätön sähköinen allekirjoitus tarkoittaa tässä sitä, että sovellusistunnon käyttäjä allekirjoittaa kansalaisvarmenteeseensa liittyvällä salaisella avaimella asiointisovelluksen antaman tekstin.

VETUMA-palvelussa tuetaan seuraavia kansalaisvarmenteeseen perustuvia allekirjoitustapoja:

- Allekirjoitus sirukortille talletetulla kansalaisvarmenteella.

- Allekirjoitus mobiililaitteen SIM-kortille talletetulla kansalaisvarmenteella.

Kansalaisvarmenteeseen perustuvan kiistämättömän allekirjoituksen suorittamisessa ei tarvita VETUMA-käyttäjärekisteriä.

Allekirjoitusta pyytävän sovelluksen vastuulla on muotoilla allekirjoitettava teksti siten, että:

- Käyttäjä ymmärtää tekstin perusteella mihin sitoutuu allekirjoituksellaan.
- Teksti kuvaa aukottomasti sen, mihin allekirjoitus sitoo.

Mikäli allekirjoitus onnistui, VETUMA-palvelu tarkistaa vielä allekirjoitusohjelman lähettämän allekirjoituksen oikeellisuuden. Tähän kuuluu mm. varmenteen voimassaolon tarkistus VRK:n sulkulistaa vasten. Silloinkin kun allekirjoituksen tarkistus epäonnistuu, palauttaa VETUMA palvelu sovellukselle allekirjoituksen sekä lisäksi tilatiedon tarkistuksen epäonnistumisesta.

Asiointisovelluksen vastuulla on tallettaa pysyvästi onnistuneessa allekirjoitustapahtumassa syntynyt kiistämätön allekirjoitus mahdollista myöhempää selvittelyä varten, sillä VETUMA-palvelussa ei talleteta sen kautta suoritettuja allekirjoituksia.

4.3.1 Sirukortin käyttöön perustuva allekirjoitus

Käyttäjän valittua sirukortin käyttöön perustuvan allekirjoituksen:

- VETUMA-palvelu pyytää käyttäjää laittamaan kansalaisvarmenteen sisältävän sirukorttinsa kortinlukijaan ja välittää allekirjoitettavan tekstin allekirjoituspyynnössä käyttäjän selaimelle. Selain aktivoi työaseman allekirjoitusohjelmiston tekemään allekirjoituksen.
- Allekirjoitusohjelmisto näyttää käyttäjälle allekirjoitettavan tekstin ja pyytää käyttäjää antamaan allekirjoitusta varten tarkoitetun PIN-koodin.
- Sirukorttiohjelmisto tarkistaa PIN-koodin ja jos se on oikea, tekee allekirjoituksen ja lähettää sen VETUMA-palvelulle.

4.3.2 Mobiiliallekirjoitus

Mobiililaitteella SIM-kortille tallennettua kansalaisvarmennetta käyttäen tehtävää allekirjoitusta kutsutaan tässä lyhyesti mobiiliallekirjoitukseksi.

Valittuaan mobiiliallekirjoituksen käyttäjä antaa VETUMA-palvelun allekirjoituskäyttöliittymän kautta sen SIM-kortin puhelinnumeron jolle hänen kansalaisvarmenteensa on tallennettu.

- VETUMA-palvelu lähettää allekirjoituspyynnön matkapuhelinoperaattorille, joka välittää pyynnön edelleen annettuun puhelinnumeroon. VETUMA-palvelun kutsuma operaattori suorittaa tarvittaessa allekirjoitusvierailun (roaming) käyttäjän kotioperaattorin verkkoon (sen operaattorin verkkoon jonka SIM-kortilla käyttäjän kansalaisvarmenne on.)
- Sen mobiililaitteen varusohjelmisto jolla varmenteen sisältävä SIM-kortti on pyytää käyttäjää antamaan allekirjoitusta varten tarkoitetun SPIN-koodin (tunnusluvun).
- Varusohjelmisto tarkistaa SPIN-koodin ja jos se on oikea, tekee allekirjoituksen ja toimittaa sen matkapuhelinoperaattorin palvelinohjelmiston kautta VETUMA-palvelulle.

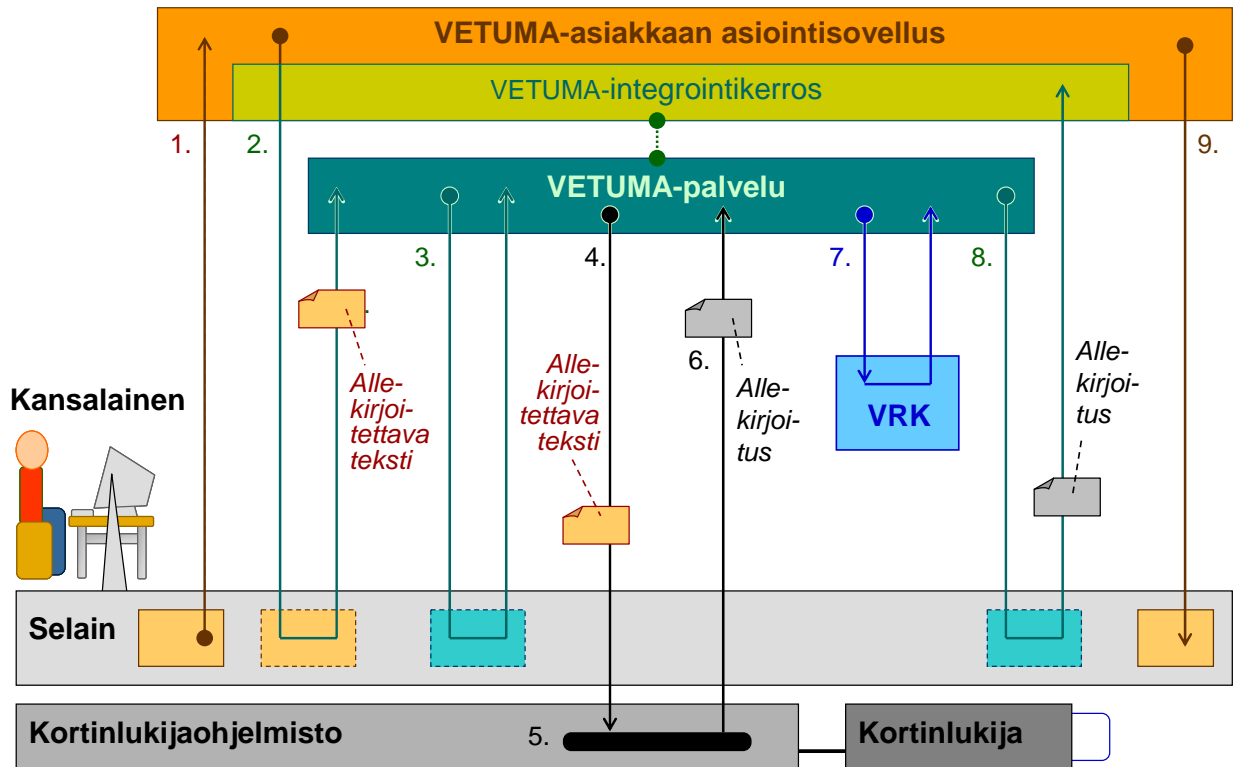
Mobiiliallekirjoituksessakin voidaan käyttää FiCom:in suosittelemia haittakäytön estomekanismeja:

- Istuntotunnus. VETUMA-palvelu luo istuntotunnuksen sovelluksen puolesta ja näyttää sen käyttäjälle mobiiliallekirjoituksen käyttöliittymässä.
- Käyttäjakohtainen häirinnän estokoodi. Mikäli käyttäjällä on häirinnän estokoodi käytössään, hän antaa sen – puhelinnumeron lisäksi – VETUMA-palvelun

mobiiliallekirjoituksen käyttöliittymässä. VETUMA-palvelu välittää häirinnän estokoodin operaattorille jonka toimittaa sen allekirjoituskomennon yhteydessä mobiililaitteeseen.

4.3.3 Allekirjoituksen kulku

Sirukortilla suoritettavan kiistämättömän allekirjoituksen eteneminen on esitetty allaolevassa kuvassa esimerkkinä VETUMA-palvelun avulla suoritettavasta allekirjoituksesta:



Kuva 4: Allekirjoituksen kulku

1. Käyttäessään selaimellaan VETUMA-asiakkaan asiointisovellusta käyttäjä (kansalainen) pyytää sellaista toimintaa johon liittyvää sitouttamista varten tarvitaan kiistämätön sähköinen allekirjoitus.
2. Asiointisovellus varmistaa (huolehtii siitä), että yhteys käyttäjän selaimen on SSL/TLS-suojattu, rakentaa VETUMA-allekirjoituskutsun (johon sisältyy allekirjoitettava teksti), ja toimittaa kutsun käyttäjän selaimen kautta VETUMA-palvelulle (kuten dokumentissa ”Suomalaisen julkishallinnon VETUMA-palvelu, kutsurajapinnan määrittely” on kuvattu).
3. VETUMA-palvelu tarkistaa kutsun oikeellisuuden, ja kelvollisen kutsun tapauksessa avaa käyttöliittymänsä käyttäjän selaimen HTTPS-yhteyttä käyttäen, pyytäen käyttäjää käynnistämään allekirjoittamisen.
4. Käyttäjän käynnistettyä allekirjoittamisen VETUMA-palvelu palauttaa selaimelle HTTPS-yhteyttä käyttäen HTTP-vastauksen joka sisältää allekirjoitettavan tekstin ja aktivoi työaseman selaimen kytketyn allekirjoituskomponentin.
5. Allekirjoituskomponentti pyytää käyttäjää syöttämään allekirjoituksessa tarvittavan PIN-koodin (PIN2). Tämän jälkeen allekirjoituskomponentti suorittaa allekirjoituksen.
6. Allekirjoitus toimitetaan työasemasta selaimen välityksellä VETUMA-palvelulle.

7. Saatuaan allekirjoituksen työaseman allekirjoituskomponentilta VETUMA-palvelu tarkistaa Väestörekisterikeskukselta että allekirjoituksessa käytetyt varmenteet ovat voimassa.
8. VETUMA-palvelu rakentaa VETUMA-allekirjoitusvastauksen (johon sisältyy allekirjoitus) ja toimittaa sen käyttäjän selaimen kautta HTTPS-yhteyden välityksellä asiointisovellukselle (kuten dokumentissa ”Suomalaisen julkishallinnon VETUMA-palvelu, kutsurajapinnan määrittely” luvun on kuvattu).
9. Asiointisovellus tarkistaa vastauksen oikeellisuuden, tallettaa saamansa allekirjoituksen, ja jatkaa toimintaansa. Sovellus keskustelee jälleen käyttäjän kanssa oman käyttöliittymänsä kautta.

5. VERKKOMAKSAMINEN (PAYMENT-PALVELUTYYPPI)

5.1 Maksatus

Maksatus tarkoittaa tässä sitä, että asiointisovellus pyytää sovellusistunnon käyttäjää maksamaan sovelluksen määräämän maksun asiointitapahtuman yhteydessä. Käytännössä maksatus tehdään siten, että asiointisovellus antaa maksatuskutsussa VETUMA-palvelulle maksua koskevat tiedot. VETUMA-palvelu ohjaa sitten käyttäjän hänen valitsemaansa verkkomaksupalveluun, välittäen sille maksua koskevat tiedot. Käyttäjä suorittaa maksamisen valitsemansa verkkomaksupalvelun käyttöliittymän kautta. VETUMA-palvelu palauttaa verkkomaksupalvelulta saamansa tiedot maksamisesta asiointisovellukselle.

Asiointisovellus voidaan toki suunnitella siten, että se antaa käyttäjän valita, käyttääkö hän maksamiseen verkkomaksupalvelua vai haluaako hän itseään laskutettavaksi erikseen lähetettävällä tavanomaisella laskulla. Joka tapauksessa sovelluksen vastuulla on huolehtia siitä, että tieto sovellusistunnon aikana suoritetusta maksamisesta kirjataan siten, että käyttäjää ei laskuteta hänen maksamaansa maksua enää muulla keinoin.

Asiointisovellus tulee myös suunnitella siten, että maksatukset tulevat kirjatuiksi asianmukaisesti asiakkaan kirjanpitoon.

5.1.1 Tuetut maksupalvelut

VETUMA-palvelun vaiheessa 2 tuetaan maksamista pankkien verkkopalveluilla sekä Luottokunnan verkkopalvelulla. Muista maksumenetelmistä ei toistaiseksi ole toteutus päätöstä. VETUMA-palvelun maksatusrajapintamäärittelyssä on kuitenkin myös huomioitu Digiraha (koska se on mainittu VETUMA-palvelun tarvekartoituksessa).

Verkkomaksamisessa ei ole samanlaista kaikkien maksupalveluiden noudattamaa yhteistä standardia kuin tunnistuksessa (Tupas), vaan eri palveluntarjoajilla on maksatuskutsuissaan ja -vastauksissaan jossain määrin erilainen valikoima parametreja sekä erilaisia muotovaatimuksia tietyn merkityksen omaavalle parametrille. VETUMA-palvelu tarjoaa yleisen, eri maksupalveluiden eroista riippumattoman rajapinnan ”pienimmän yhteisen nimittäjän” periaatteella. Esimerkiksi:

- Jos tietyn merkityksen omaavalla viestillä on erilainen enimmäispituus eri verkkomaksupalveluissa, käytetään VETUMA-kutsurajapinnassa pienintä enimmäispituutta (jotta VETUMA-palvelu ei joudu katkaisemaan viestiä kutsuessaan käyttäjän valitsemaa verkkomaksupalvelua).
- Jos tietyn merkityksen omaava parametri on tarjottu joissain maksupalveluissa mutta puuttuu toisilta, kyseinen parametri on mukana VETUMA-kutsurajapinnassa. VETUMA-palvelu jättää tällöin kyseisen parametrin pois kutsusta kutsuessaan sellaista käyttäjän valitsemaa maksupalvelua jossa kyseistä parametria ei käytetä.

Maksun viitetiedossa Luottokunnan ja muiden maksupalveluiden välisiä eroja ei kuitenkaan voi täysin piilottaa.

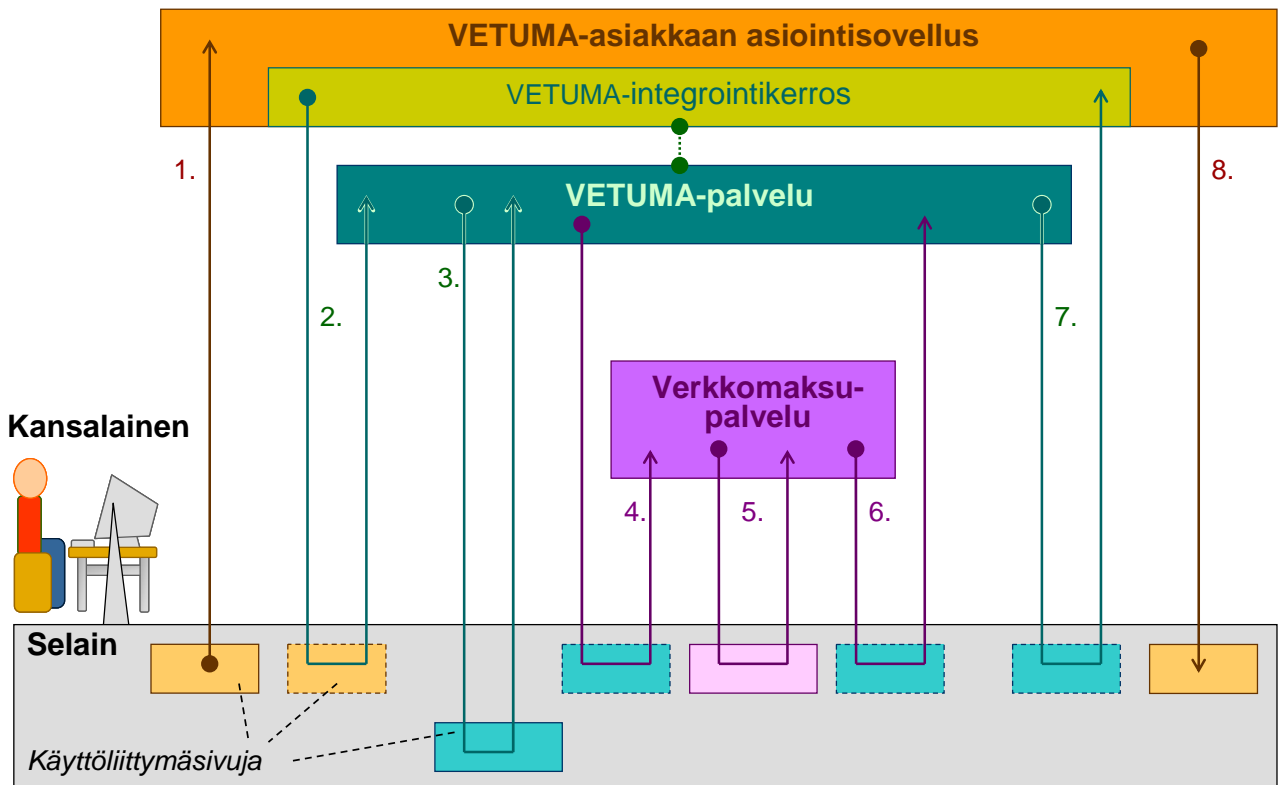
- Luottokunta käyttää tilausnumeroa ja muut maksupalvelut viitenumeroa.
- Tilausnumeron enimmäispituus on 9 merkkiä, kun taas viitenumeron enimmäispituus on 20 merkkiä (19 merkin perusviitenumero ja tietyllä kaavalla laskettava tarkistenumero).
- Käytettäessä yli 9-merkkistä perusviitenumeroa ei sitä voi yksikäsitteisesti muuntaa 9-numeroiseksi tilausnumeroksi.
- Koska VETUMA-palvelu ei halua rajoittaa viitenumeroita enintään 10-merkkisiksi, se tarjoaa kutsurajapinnassaan mahdollisuuden antaa molemmat viitetiedot. Sovelluksen vastuulle jää tällöin huolehtia siitä, että maksu voidaan yksikäsitteisesti tunnistaa kummallakin viitetiedolla asiakkaan maksatusten seurantajärjestelmässä.

VETUMA-palvelu tarjoaa käyttäjän valittavaksi vain ne maksupalvelut joiden kanssa maksatusta pyytäneellä asiakkaalla (siis sillä organisaatiolla jonka sovellus lähetti maksatuskutsun) on VETUMA-palvelun tiedossa oleva maksujen vastaanottosopimus. Tiedot sopimuksista on talletettu asiakkaan asiakskonfiguraatioon. Sopimusten puuttumisen lisäksi käyttäjälle tarjottavien maksupalveluiden joukkoa voivat rajoittaa:

- Tilausnumeron puuttuminen kutsusta (tällöin ei tarjota Luottokuntaa maksamisvaihtoehtoksi).
- Maksupalvelun enimmäissumman ylittäminen (esimerkiksi Digirahalla ei voi maksaa yli 250 €suuruisia maksuja).

5.1.2 Maksatuksen kulku

VETUMA-palvelun kautta suoritetun maksatuksen kulku on esitetty allaolevassa kuvassa:



Kuva 5: Maksamisen kulku

Versio: 2.2 31.12.2008

1. Käyttäessään selaimellaan VETUMA-asiakkaan asiointisovellusta käyttäjä (kansalainen) valitsee sellaisen toiminnon josta aiheutuu hänelle maksu.
2. Asiointisovellus varmistaa (huolehtii siitä), että yhteys käyttäjän selaimen on SSL/TLS-suojattu, rakentaa VETUMA-maksatuskutsun, ja toimittaa kutsun käyttäjän selaimen kautta VETUMA-palvelulle (kuten dokumentissa ”Suomalaisen julkishallinnon VETUMA-palvelu, kutsurajapinnan määrittely” on kuvattu).
3. VETUMA-palvelu tarkistaa kutsun oikeellisuuden, ja kelvollisen kutsun tapauksessa avaa käyttöliittymänsä käyttäjän selaimen HTTPS-yhteyttä käyttäen antaakseen käyttäjän valita verkkomaksupalvelun.
4. VETUMA-palvelu rakentaa käyttäjän valitsemalle verkkomaksupalvelulle sen edellyttämän maksatuskutsun ja toimittaa sen käyttäjän selaimen kautta valitulle palvelulle.
5. Valittu verkkomaksupalvelu suorittaa maksatuksen oman käyttöliittymänsä kautta.
6. Verkkomaksupalvelu rakentaa maksatusvastauksen ja toimittaa sen käyttäjän selaimen kautta HTTPS-yhteyden välityksellä VETUMA-palvelulle.
7. Onnistuneen maksamisen jälkeen VETUMA-palvelu rakentaa VETUMA-maksatusvastauksen ja toimittaa sen käyttäjän selaimelle HTTPS-yhteyttä käyttäen, toimitettavaksi edelleen asiointisovellukselle. Vastaus toimitetaan selaimelle VETUMA-palvelun käyttöliittymän ”paluu maksamisesta”-sivulla, jolta se lähtee asiointisovellukselle käyttäjän hyväksytyä paluun.
8. Asiointisovellus tarkistaa vastauksen oikeellisuuden ja jatkaa toimintaansa. Sovellus keskustelee jälleen käyttäjän kanssa oman käyttöliittymänsä kautta.

5.1.3 Maksujen seuranta

Tietyn asiakkaan – ja kyseisen asiakkaan asiointisovellusten – tapa seurata maksuja ja täsmäyttää saadut maksusuoritukset ei näy VETUMA-palvelulle. VETUMA-palvelu tarjoaa ainoastaan mahdollisuuden välittää seurantaan käytettävät tiedot maksatuskutsun ja -vastauksen parametreina. Asiointisovelluksen vastuulla on siis pitää huoli siitä, että suoritettut maksut – sen lisäksi, että ne huomioidaan sovelluksen toiminnassa – merkitään asianmukaisesti asiakkaan taloushallinnon järjestelmiin (kirjanpito, reskontra tms.) ja kirjataan asianmukaiseen lokiin mahdollista myöhempää selvitystarvetta varten.

5.1.3.1 Maksujen seurannan tuki maksatuskutsussa

Maksatuskutsussa voi antaa seuranta varten seuraavat tiedot:

- Suomen Pankkiyhdistyksen vahvistaman kuvauksen mukaisen viitenumeron.
 - Viitenumeroa käytetään pankkien verkkomaksupalveluissa ja Digirahassa, ja se on niille pakollinen kutsuparametri.
 - Viitenumeroa ei käytetä Luottokunnan verkkomaksupalvelussa, eikä se ole mukana Luottokunnan maksatuskutsuissa.
- Luottokunnan käyttämän tilausnumeron.
 - Tilausnumero on Luottokunnan verkkomaksupalvelussa pakollinen kutsuparametri.
 - Tilausnumeroa ei käytetä muissa verkkomaksupalveluissa, eikä se ole mukana niiden maksatuskutsuissa.
- Sanalliset viestit maksajan ja maksun saajan tilitietoihin. Kaikki verkkomaksupalvelut eivät tue näitä viestejä, ja viestit ovat niitä tukeville palveluillekin valinnaisia kutsuparametreja.

Versio: 2.2 31.12.2008

Asiointisovelluksen vastuulla on muodostaa tai hankkia viitenumerot ja mahdolliset tilausnumerot joilla sovelluksen tekemät maksatukset tarvittaessa yhdistetään asiakkaan saatavien seurantaan, sekä muodostaa seurantaan käytettävät viestit.

- Suomen Pankkiyhdistyksen vahvistama kuvaus viitenumerosta löytyy osoitteesta: (<http://www.pankkiyhdistys.fi/sisalto/upload/pdf/viitenumero.pdf>). Sen mukaan:
 - Maksattaja voi yksilöidä maksun viitenumerolla.
 - Kun maksua suoritettaessa annetaan viitenumero, välittyy maksu maksattajan viitteellisten suoritusten vastaanottamiseen tarkoitettulle tilille.
 - Viitenumeron vähimmäispituus on 4 numeroa (3 + tarkiste) ja sallittu enimmäispituus 20 numeroa (19 + tarkiste).
 - Laskuttaja voi edellä mainittujen pituusrajojen puitteissa vapaasti muodostaa perusviitenumeron.
 - Tarkisteen tarkoituksena on tallennusvirheiden estäminen. Se lasketaan perusviitenumerosta tietyllä laskukaavalla.
- Mikäli asiakas voi käyttää maksujen yksilöinnissä 3..19 numeron mittaista numeerista tunnusta, on siitä siis helppoa muodostaa viitenumero lisäämällä vain sen loppuun tarkistenumero Suomen Pankkiyhdistyksen määrittelemällä tavalla.
- Mikäli asiakkaan saamien maksujen seurannassa ei kuitenkaan voida käyttää 3..19 numeron mittaista numeerista tunnusta, niin sovellus voi esimerkiksi käyttää kuvaustaulua jossa jokaista maksutapahtumalle annettua viitenumeroa kohden on tieto vastaavasta, asiakkaan omassa maksujen seurannassa käytettävästä saatavan tunnuksesta.
- Koska viitenumeroilta ei vaadita yksilöllisyyttä, asiakas voi halutessaan pidättäytyä yksittäisten maksutapahtumien seurannasta ja käyttää viitenumeroa vain esimerkiksi asiointisovelluksen tai palvelutapahtumatyyppin osoittamiseen.

Mikäli asiointisovellus haluaa antaa mahdollisuuden maksaa myös Luottokunnan kautta, asiointisovelluksen vastuulla on myös muodostaa tai hankkia tilausnumerot joilla sovelluksen tekemät maksatukset tarvittaessa yhdistetään asiakkaan saatavien seurantaan.

- Tilausnumeron enimmäispituus on 9 numeroa ja se ei voi alkaa nolllalla.
- Tilausnumeron pitää olla tietyn maksattajan maksatustapahtumien kesken yksilöllinen, eli maksatuskutsussa annettu tilausnumero ei saa esiintyä missään muussa kyseisen maksattajan Luottokunnan kautta maksattamassa maksussa.
- Mikäli asiakkaan saamien maksujen seurannassa ei kuitenkaan voida käyttää 1..9 numeron mittaista numeerista tunnusta, niin esimerkiksi:
 - Voidaan käyttää kuvaustaulua jossa jokaista maksutapahtumalle annettua tilausnumeroa kohden on tieto vastaavasta, seurannassa käytettävästä saatavan tunnuksesta (esimerkiksi viitenumerosta).
 - Tai voidaan jättää tilausnumeroparametri pois maksatuskutsusta. VETUMA-palvelu ei tällöin tarjoa käyttäjälle mahdollisuutta valita Luottokunnan verkkopalvelua maksun suorittamiseksi.

Kuten jo aiemmin on mainittu, tilaus- ja viitenumeroiden käytössä on huomioitava, että vähintään 3- ja enintään 9-merkkistä tilausnumeroa voidaan käyttää myös viitenumeron perusviitetietona ja lisätä siihen viitenumerokuvauksen mukainen tarkistenumero. Yli 9-merkkisistä viitenumeroista ei kuitenkaan voi yksikäsitteisesti muodostaa enintään 9-merkkisiä tilausnumeroita. Mikäli asiakkaalla on tarve käyttää seurannassa yli 9-merkkisiä viitenumeroita ja toisaalta mahdollistaa maksaminen myös luottokunnan kautta, jää asiointisovelluksen vastuulle muodostaa – tai hankkia – yhteys tietyn maksutapahtuman viitenumeron ja tilausnumeron välille.

VETUMA-palvelulle ei näy se, mikä järjestelmä antaa perusviitenumerot ja tilausnumerot, ja mikä on niiden sisäinen rakenne. Asiointisovellus voi antaa perusviitenumerot ja tilausnumerot itse asiakkaan määrittämien sääntöjen mukaisesti, tai se voi hankkia ne joltain sopivalta asiakkaan taustajärjestelmältä (esimerkiksi laskutus- ja maksunseurantajärjestelmältä).

Maksajan ja maksun saajan tilitapahtumatietoihin talletettavien viestien käytöstä on huomioitava, että kaikki VETUMA-palvelussa tuetut verkkomaksupalvelut eivät tue näitä viestejä.

5.1.3.2 Kaksoismaksatuksen estäminen

Useat verkkomaksupalvelut vaativat maksatuskutsussaan sellaisen maksun yksilöivän tunnuksen jolla estetään kaksoismaksatus. Käyttäjän valitessa tällaisen verkkomaksupalvelun VETUMA-palvelu muodostaa kyseisen tunnuksen asiointisovelluksen puolesta, eli asiointisovelluksen ei tarvitse itse muodostaa tätä tunnusta. VETUMA-palvelu palauttaa muodostamansa tunnuksen asiointisovellukselle maksatusvastauksessa.

5.1.3.3 Maksujen seurannan tuki maksatusvastauksessa

Maksatusvastauksessa VETUMA-palvelu palauttaa:

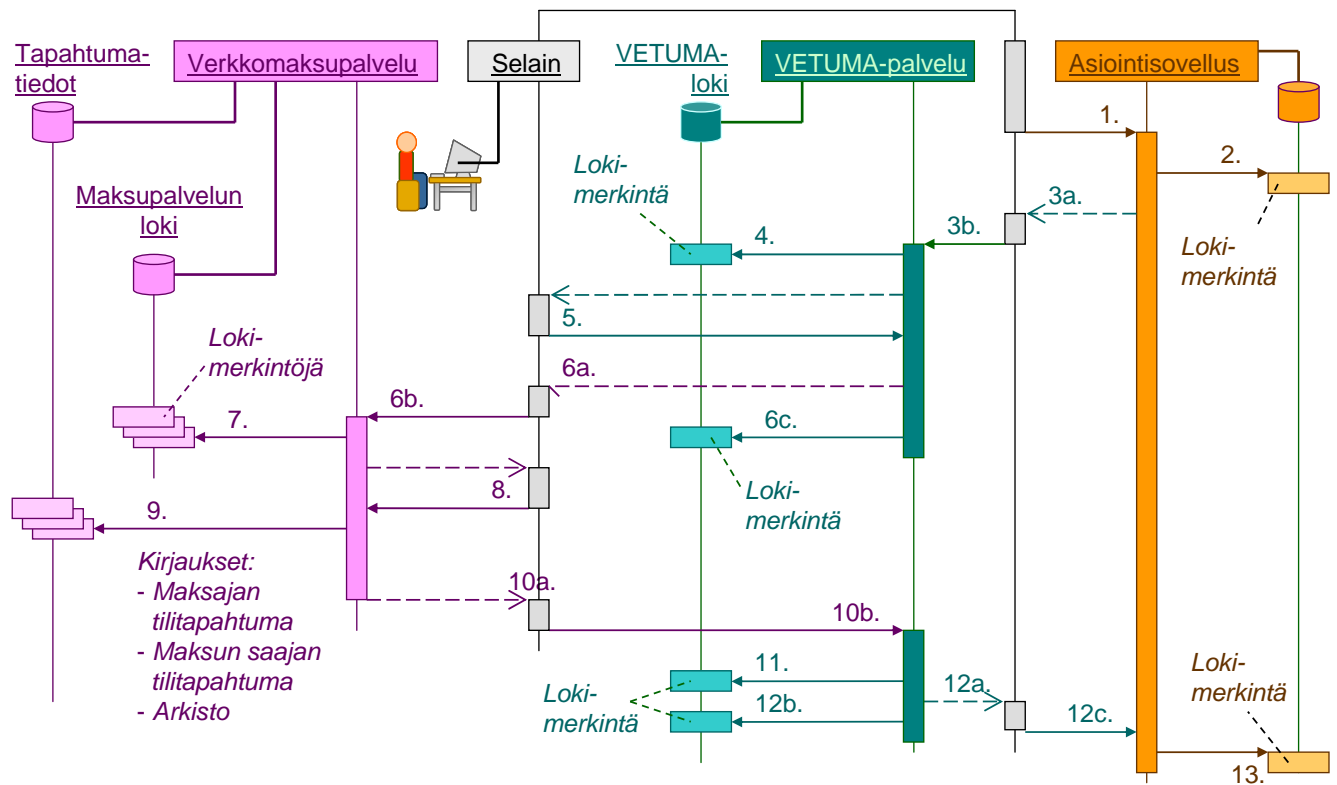
- Tiedon siitä, millä maksupalvelulla käyttäjä suoritti maksun.
- Kutsussa saamansa viitenumeron tai tilausnumero, riippuen siitä maksoiko käyttäjä pankin verkkopalvelulla vai Luottokunnan verkkopalvelulla.
- Kaksoismaksatuksen estävän yksilöllisen tunnuksen jonka se muodosti sovelluksen puolesta maksutapahtumaa varten.
- Verkkomaksupalvelun muodostaman arkistointitunnuksen – mikäli valittu palvelu sellaisen muodostaa ja palauttaa maksatusvastauksessaan VETUMA-palvelulle.
 - Useat verkkomaksupalvelut antavat maksutapahtumalle arkistointitunnuksen jota voidaan käyttää muun muassa epäselvien maksutapahtumien selvittelyssä.
 - Kutsuttuaan sellaista verkkomaksupalvelua VETUMA-palvelu välittää saamansa arkistointitunnuksen asiointisovellukselle.

VETUMA-palvelulle ei näy se, miten VETUMA-palvelun kautta suoritettuja maksatuksia seurataan ja täsmäytetään. Asiointisovellus voi esimerkiksi vain kirjata omiin tietoihinsa maksun suoritetuksi, tai välittää tiedot jollekin sopivalle asiakkaan taustajärjestelmälle (esimerkiksi laskutus- tai reskontrajärjestelmälle) seurantaa ja täsmäytystä varten.

5.1.4 Maksutapahtumien jäljittäminen

Maksatuksen yhteydessä välitetään viestejä asiointisovelluksen, VETUMA-palvelun ja käyttäjän valitseman verkkomaksupalvelun välillä, ja viestit kulkevat käyttäjän selaimen kautta. Maksutapahtuman kulun yhteydessä talletetaan eri paikkoihin tietoa joka mahdollistaa maksutapahtumien jäljitettävyyden. VETUMA-palvelun kannalta tämä on kuvattu allaolevassa kuvassa. Maininnat asiointisovelluksen tekemistä merkinnöistä ovat esimerkkejä, eli kunkin asiointisovelluksen suunnittelija päättää, millaista maksatukseen liittyvää lokitusta sovellus tekee.

Versio: 2.2 31.12.2008



Kuva 6: Maksustapahtuman kulku jäljittämisen kannalta

1. Käyttäjän selaimelta tulee asiointisovellukselle kutsu, jota palvellessaan sovellus toteaa maksustarpeen.
2. Asiointisovellus valmistelelee maksutapahtuman: määrää maksettavan summan, laatii maksutapahtuman viestit, ja luo tai hankkii maksun seurannassa tarvittavat tiedot (viitenumeron ja halutessaan tilausnumeron). Asiointisovellus kirjaa tällöin tietoja maksusta asiakkaan maksulokiin ja voi olla yhteydessä asiakkaan maksujärjestelmiin (laskutus, reskontra). Se ei kuitenkaan näy VETUMA-palvelulle.
3. Asiointisovellus kutsuu VETUMA-palvelua suorittamaan maksatuksen:
 - a. Sovellus rakentaa VETUMA-maksatuskutsun sisältävän HTML-sivun ja palauttaa sen HTTP-vastauksena käyttäjän selaimelle. Kutsun parametrina annetaan muun muassa summa, viestit, seurantatiedot ja kutsuaika.
 - b. Käyttäjän selain toimittaa VETUMA-maksatuskutsun edelleen HTTP-kutsulla (POST-komennolla) VETUMA-palvelulle.
4. **VETUMA-palvelu tallettaa lokitietoihinsa tiedon maksatuskutsun vastaanottamisesta ja sen parametreista (muun muassa summa ja seurantatiedot).**
5. VETUMA-palvelu antaa käyttäjän valita haluamansa verkkomaksupalvelun tai perua maksamisen.
6. VETUMA-palvelu välittää maksatuspyynnön valitulle verkkomaksupalvelulle:
 - a. VETUMA-palvelu rakentaa käyttäjän valitseman verkkomaksupalvelun vaatiman maksatuskutsun sisältävän HTML-sivun ja palauttaa sen HTTP-vastauksena käyttäjän selaimelle. Kutsun parametrina annetaan muun muassa summa, viestit, seurantatiedot ja kutsuaika.
 - b. Käyttäjän selain toimittaa maksatuskutsun edelleen HTTP-kutsulla (POST-komennolla) käyttäjän valitsemalle verkkomaksupalvelulle.

Versio: 2.2 31.12.2008

c. VETUMA-palvelu tallettaa lokitietoihinsa tiedon kutsun lähettamisestä ja sen parametreista (muun muassa seurantatiedot) sekä lähettamisajasta.

7. Verkkomaksupalvelu tekee maksatuskutsun vastaanottamisesta omat lokimerkintänsä, ja saattaa tehdä myös muita lokimerkintöjä maksatuksen suorittamisen yhteydessä. Se, mitä lokimerkintöjä kukin maksupalvelu tekee, ei näy VETUMA-palvelulle.
8. Verkkomaksupalvelu suorittaa maksatuksen, keskustellen käyttäjän kanssa selaimen välityksellä oman käyttöliittymänsä kautta. Tämä keskustelu käyttäjän kanssa koostuu useasta HTTP-vastaus- ja -kutsuparista.
9. Onnistuneen maksatuksen jälkeen verkkomaksupalvelu kirjaa maksun suorittamisen (aika, määrä, viestit, seurantatiedot) maksajan ja maksun vastaanottajan tilitapahtumatietoihin. Eräät verkkomaksupalvelut antavat lisäksi seurantaan varten maksutapahtumalle yksilöllisen arkistointitunnuksen.
10. Verkkomaksupalvelu palauttaa maksatusvastauksen VETUMA-palvelulle:
 - a. Verkkomaksupalvelu rakentaa maksatusvastauksensa sisältävän HTML-sivun ja palauttaa sen HTTP-vastauksena käyttäjän selaimelle. Vastauksen parametreina ovat muun muassa maksupalvelun luoma arkistointitunnuksen, seurantatiedot ja vastausaika.
 - b. Käyttäjän selain toimittaa verkkomaksupalvelun maksatusvastauksen edelleen HTTP-kutsulla (POST-komennolla) VETUMA-palvelulle.
11. **VETUMA-palvelu tallettaa lokitietoihinsa tiedon maksatusvastauksen vastaanottamisesta verkkomaksupalvelulta.** Lokiin talletetaan muun muassa maksutapahtuman arkistointitunnus, seurantatiedot, ja aika jolloin vastaus tuli verkkomaksupalvelulta.
12. VETUMA-palvelu palauttaa maksatusvastauksen asiointisovellukselle:
 - a. VETUMA-palvelu rakentaa maksatusvastauksen sisältävän HTML-sivun ja palauttaa sen HTTP-vastauksena käyttäjän selaimelle.
 - b. **VETUMA-palvelu tallettaa lokitietoihinsa tiedon maksatusvastauksen lähettamisestä asiointisovellukselle.** Lokiin talletetaan muun muassa maksutapahtuman arkistointitunnus, seurantatiedot, ja aika jolloin vastaus lähti VETUMA-palvelulta asiointisovellukselle.
 - c. Käyttäjän selain toimittaa VETUMA-palvelun maksatusvastauksen edelleen HTTP-kutsulla (POST-komennolla) asiointisovellukselle.
13. **Maksatusvastauksen saatuaan asiointisovelluksen edellytetään vielä tekevän lokimerkinnän asiakkaan lokiin.** Tämä vaaditaan VETUMA-pelisäännöissä jotka asiakas hyväksyy liittyessään VETUMA-palvelun asiakkaaksi. Maksatusvastauksen saatuaan asiointisovellus saattaa lisäksi kirjata tiedon maksamisesta asiakkaan maksujärjestelmiin (laskutus, reskontra), mutta sekään ei näy VETUMA-palvelulle.

Tämän jälkeen asiointitapahtuman suoritus asiointisovelluksessa jatkuu tietoisena maksatuksesta (tai maksamisen perumisesta tai epäonnistumisesta).

VETUMA-palvelun lokitiedot on tarkoitettu käytettäväksi yksinomaan palvelun käyttöön liittyvässä, palvelun toimittajan suorittamassa ongelmanselvityksessä. Ne eivät siis ole asiakkaan käytettävissä maksujen seurantaan.

5.1.5 Mahdollisia poikkeustilanteita

Maksatustapahtuman aikana voi ilmetä seuraavanlaisia poikkeustilanteita:

- Mikäli maksatuskutsu asiointisovellukselta (vaihe 3.) on virheellinen, VETUMA-palvelu tallettaa lokitietoihinsa tiedon virheestä ja palauttaa maksatusvastauksen kyseisessä kutsussa annettuun virhepaluusoitteeseen.
- Mikäli käyttäjä peruu maksamisen VETUMA-palvelun käyttöliittymässä (vaihe 5.), VETUMA-palvelu tallettaa lokitietoihinsa tiedon peruutuksesta ja palauttaa maksatusvastauksen palvelemassaan maksatuskutsussa annettuun peruutuspaluusoitteeseen.
- Mikäli verkkomaksupalvelu hylkää maksatuskutsun virheellisenä, se tallettaa tästä tiedon omaan lokiinsa ja palauttaa VETUMA-palvelulle virhevastauksen (vaihe 10.) VETUMA-palvelu tallettaa tästä tiedon omaan lokiinsa (vaihe 11.), ja palauttaa maksatusvastauksen sovellukselle kutsussa annettuun virhepaluusoitteeseen (vaihe 12.)
- Mikäli maksaminen epäonnistuu – esimerkiksi jos käyttäjän tilillä ei ole katetta tai käyttäjän luottoraja ylittyisi – verkkomaksupalvelu tallettaa tästä tiedon omaan lokiinsa ja palauttaa VETUMA-palvelulle virhevastauksen (vaihe 10.) VETUMA-palvelu tallettaa tästä tiedon omaan lokiinsa (vaihe 11.), ja palauttaa maksatusvastauksen sovellukselle kutsussa annettuun virhepaluusoitteeseen (vaihe 12.)
- Mikäli käyttäjä peruu maksamisen verkkomaksupalvelun käyttöliittymässä, tallettaa palvelu tästä tiedon omaan lokiinsa (vaihe 9.) ja palauttaa VETUMA-palvelulle peruutusvastauksen (vaihe 10.) VETUMA-palvelu tallettaa tästä tiedon omaan lokiinsa (vaihe 11.), ja palauttaa maksatusvastauksen sovellukselle kutsussa annettuun peruutuspaluusoitteeseen (vaihe 12.)

Lisäksi maksatustapahtumaa suoritettaessa saattaa esiintyä virheitä viestinvälityksessä. Näitä on tarkemmin käsitelty luvussa YLEINEN POIKKEUSTILANTEIDEN KÄSITTELY.

5.2 Maksunpalautus

VETUMA-asiakkaan sovellus voi pyytää VETUMA-palvelua palauttamaan tietyssä maksutapahtumassa maksetun summan joko kokonaan tai osittain. Maksunpalautusta tukevilla verkkomaksupalveluissa on kussakin omat sääntönsä palautuksen suorittamisesta. Palautusta pyytävän sovelluksen ei tarvitse olla sama sovellus joka aikanaan pyysi maksatusta.

VETUMA-palvelu sovittaa saamansa palautuskutsun kutsussa annetun verkkomaksupalvelun rajapinnan mukaiseksi, ja välittää pyynnön sille. Kutsuttu palvelu suorittaa sääntöjensä mukaiset tarkistukset ja joko suorittaa tai hylkää palautuksen. VETUMA-palvelu välittää tästä tiedon sitä kutsuneelle palautussovellukselle.

Jotta tietty verkkomaksupalvelulla suoritettu maksu voitaisiin palauttaa VETUMA-palvelun maksunpalautustoiminnon kautta, maksunpalautusta pyytävän sovelluksen vastuulla on hankkia tietoonsa (tai säilyttää tiedossaan) maksutapahtumasta ne tiedot, joita tarvitaan palautuksessa:

- Millä verkkomaksupalvelulla maksu suoritettiin. Mikäli maksatus suoritettiin VETUMA-palvelun kautta, palautti VETUMA-palvelu maksatusvastauksessa sovellukselle tiedon siitä, millä verkkomaksupalvelulla käyttäjä maksoi (kts. maksatusvastauksen kuvaus rajapintamäärittelyssä). Tätä tietoa tarvitaan jotta sovellus:
 - E turhaan yrittäisi palautusta VETUMA-palvelun kautta mikäli kyseinen verkkomaksupalvelu ei maksunpalautuksia tue.
 - Osaisi pyytää VETUMA-palvelua välittämään palautuspyynnön kyseiselle verkkomaksupalvelulle,

- Maksettu summa (jotta sovellus tietäisi, kuinka paljon se voi palauttaa)
- Maksamisaika (koska palautuksen voi tehdä vain tietyn ajan kuluessa maksamisesta)
- Tieto jolla voi viitata alkuperäiseen maksutapahtumaan. Siinä tapauksessa, että maksatus suoritettiin VETUMA-palvelun kautta, sovellus sai alkuperäisen maksun tunnisteiden seuraavasti:
 - Jos sovellus aikoo käyttää palautuksessa alkuperäisen maksun yksilöintiin viitenumeroa, sovellus itse hankki tai muodosti viitenumeron jonka antoi maksatuskutsussa VETUMA-palvelulle.
 - Jos sovellus aikoo käyttää alkuperäisen maksun yksilöintiin sen kaksoismaksatuksen estävää tunnusta, sovellus sai sen maksatusvastauksessa VETUMA-palvelulta joka muodosti kyseisen tunnuksen.

Maksunpalautusta tukevilla eri verkkomaksupalveluilla on erilaiset rajapinnat maksunpalautusta varten. VETUMA-palvelu tarjoaa kuitenkin yhtenäisen palautusrajapinnan joka peittää maksupalveluiden väliset erot samoin kuin maksatuksessakin.

VETUMA-palvelun maksunpalautuskutsussa sovellus antaa (yhteyshälytysparametrien lisäksi):

- Verkkomaksupalvelun jolle palautuspyyntö tulee välittää.
- Kyseisessä maksupalvelussa aiemmin suoritettua maksutapahtuman yksilöintitiedon.
- Yksilöintitiedon (esimerkiksi viitenumeron) palautustapahtumalle.
- Palautettavan summan.

Koska VETUMA-palvelu ei tiedä palautuskutsussa annetusta maksutapahtumasta niitä tietoja jotka vaikuttavat palautuksen onnistumiseen (kuten maksamisaika ja alun perin maksettu summa), se välittää aina maksunpalautuskutsussa siinä mainitulle maksupalvelulle. Vaikka palautuspyyntö olisikin siis sisällöltään virheellinen (esim. summa ylittää maksetun määrän tai palautusaika on mennyt umpeen), käy VETUMA joka tapauksessa siinä verkkomaksupalvelussa joka palautuskutsussa annettiin. Kyseinen verkkomaksupalvelu tutkii, voidaanko palautus suorittaa. Jos ei voida, niin verkkomaksupalvelu palauttaa hylkäyksensä VETUMA-palvelulle, joka puolestaan välittää tiedon hylkäyksestä asiointipalvelulle maksunpalautusvastauksessaan.

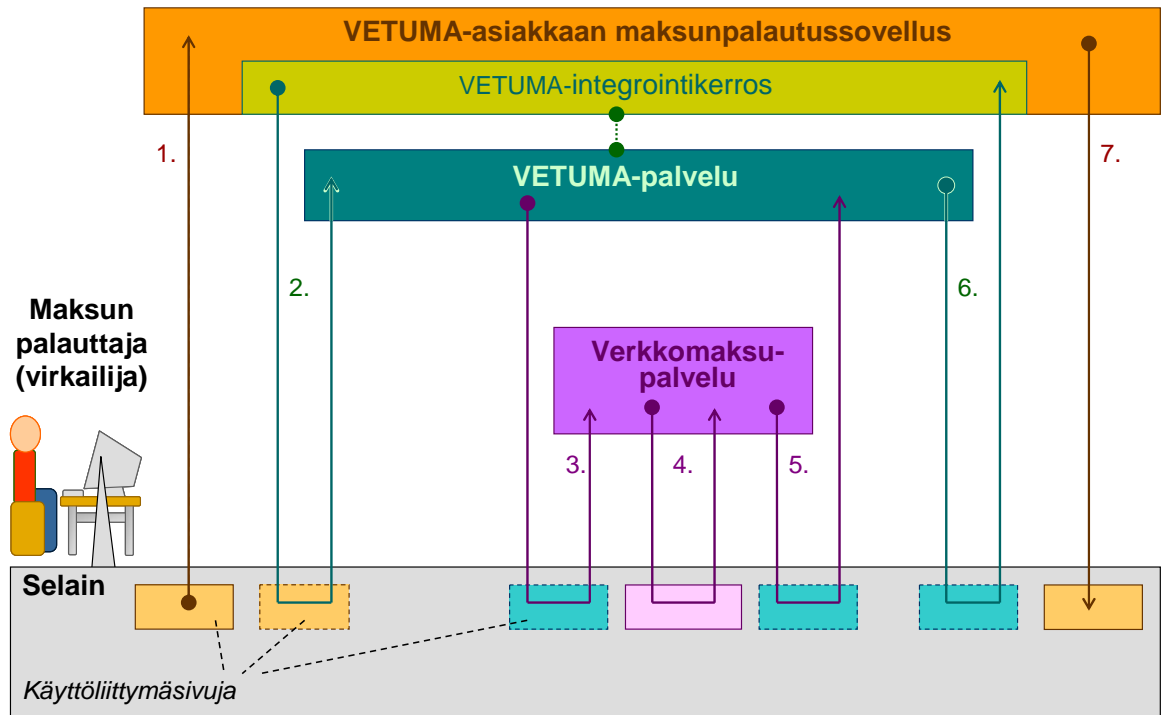
Maksunpalautus on VETUMA-asiakkaan palautuksiin oikeutetulle henkilökunnalle tarkoitettu toiminto. Kansalainen ei siis osallistu maksun palautukseen. Siksi maksunpalautuksessa ei ole mitään VETUMA-käyttöliittymää loppukäyttäjille, eikä palautuksen saajan tarvitse olla yhteydessä VETUMA-palveluun palautuksen saamiseksi. Koska palautustapahtumassa ei ole palauttajalle mitään VETUMA-palvelun toimintaan vaikuttavia valintoja, niin – palautusprosessin sujuvuuden vuoksi – VETUMA-palvelussa ei ole käyttöliittymää myöskään maksun palauttajalle. Palauttaja siirretään siis suoraan palautussovelluksen käyttöliittymästä palautuksen suorittavan maksupalvelun käyttöliittymään.

5.2.1 Tuki verkkomaksupalveluissa

Kaikissa verkkomaksupalveluissa ei vielä tueta maksunpalautusta, ja verkkomaksupalveluiden palautusta koskevien hankkeiden aikataulut eroavat verkkomaksupalveluiden välillä. VETUMA-palvelun tietyn version rajapintamäärittelyssä kerrotaan, missä verkkomaksupalveluissa kyseinen versio tukee maksunpalautusta.

5.2.2 Maksunpalautuksen kulku

Maksunpalautuksen eteneminen on esitetty allaolevassa kuvassa:



Kuva 7: Maksunpalautuksen kulku

1. Käyttäessään selaimellaan asiakkaan henkilökunnalle (ei siis loppukäyttäjille) tarkoitettua maksunpalautussovellusta, palauttaja (palautuksen suorittava virkailija) syöttää tiedot palautuksesta (kuten käytettävä maksupalvelu, palautettava summa, alkuperäisen maksun tunniste ja palautuksen viitetieto). Kehittyneemmät palautussovellukset osaavat ottaa nämä tiedot esimerkiksi asiointipalvelusta.
2. Maksunpalautussovellus varmistaa (huolehtii siitä), että yhteys palauttajan selaimen on SSL/TLS-suojattu, rakentaa VETUMA-maksunpalautuskutsun, ja toimittaa kutsun palauttajan selaimen kautta VETUMA-palvelulle (kuten dokumentissa ”Suomalaisen julkishallinnon VETUMA-palvelu, kutsurajapinnan määrittely” on kuvattu).
3. VETUMA-palvelu tarkistaa kutsun oikeellisuuden. Kelvollisen kutsun tapauksessa VETUMA-palvelu muodostaa kutsussa määrätyle verkkomaksupalvelulle sen rajapinnan mukaisen palautuskutsun ja toimittaa kutsun palauttajan selaimen kautta kyseiselle verkkomaksupalvelulle.
4. Verkkomaksupalvelu suorittaa palautuksen, keskustellen oman käyttöliittymänsä kautta palauttajan kanssa (esimerkiksi pyytäen vahvistusta palautukselle).
5. Verkkomaksupalvelu muodostaa oman rajapintansa mukaisen palautusvastauksen ja toimittaa sen palauttajan selaimen kautta VETUMA-palvelulle.
6. VETUMA-palvelu rakentaa VETUMA-maksunpalautusvastauksen ja toimittaa sen palauttajan selaimen kautta HTTPS-yhteyden välityksellä maksunpalautussovellukselle (kuten dokumentissa ”Suomalaisen julkishallinnon VETUMA-palvelu, kutsurajapinnan määrittely” luvun on kuvattu).
7. Maksunpalautussovellus tarkistaa vastauksen oikeellisuuden, tallettaa tiedon palautuksesta, ja jatkaa toimintaansa. Sovellus keskustelee jälleen palauttajan kanssa oman käyttöliittymänsä kautta.

VETUMA-palvelulla ei siis ole mitään maksunpalautuksen käyttöliittymää jolla palauttaja hyväksyisi palautuksen – koska tällaisen hyväksynnän tarjoaminen on palautuksen suorittavan verkkomaksupalvelun vastuulla. VETUMA-palvelu siis välittää palautuspyynnön palautussovellukselta verkkomaksupalvelulle ja palautusvastauksen verkkomaksupalvelulta palautussovellukselle vaivaamatta palauttajaa.

Maksunpalautussovellus on tarkoitettu VETUMA-asiakkaan henkilökunnan (virkailijoiden) käyttöön. Maksunpalautussovellus vastaa palauttajan tunnistuksesta asiakkaan sisäisen tunnistuskäytännön mukaisesti.

- VETUMA-palvelun muut toiminnot kuin maksunpalautus on tarkoitettu asioivien kansalaisten, ei virkailijoiden tunnistamiseen.
- Sisäiset tunnistuskäytännöt saattavat perustua sellaisiin menetelmiin (esimerkiksi organisaatiokortteihin) joita ei edes tueta VETUMA-palvelussa.

Kehittyneempi maksunpalautussovellus saattaa tukea sellaisia massapalautuksia joissa tietty maksu palautetaan usealle kansalaiselle. Esimerkiksi tietyn kurssin peruuttaminen saattaa aiheuttaa ennalta maksetun kurssimaksun palauttamisen kaikille ilmoittautuneille. Kehittyneempi maksunpalautussovellus selvittää palautuksen saajat asiointipalvelussa ylläpidettävän tiedon perusteella ja lähettää kutakin palautuksen saajaa kohti palautuskutsun VETUMA-palvelulle. Maksunpalautussovellus saa kustakin palautustapahtumasta vastauksen sen onnistumisesta riippuvaan paluuosoitteeseen (onnistui, palauttaja perui, palauttaminen epäonnistui).

5.2.3 Mahdollisia poikkeustilanteita

Maksunpalautustapahtuman aikana voi ilmetä seuraavanlaisia poikkeustilanteita:

- Mikäli maksunpalautuskutsu palautussovellukselta on VETUMA-yhteyksikäytännön mielessä virheellinen, VETUMA-palvelu tallettaa lokitietoihinsa tiedon virheestä ja palauttaa maksatusvastauksen sovelluksen kutsussa antamaan virhepaluuosoitteeseen.
- Mikäli verkkomaksupalvelu hylkää maksunpalautuskutsun (esimerkiksi jos palautusaika on mennyt umpeen), verkkomaksupalvelu tallettaa tästä tiedon omaan lokiinsa ja palauttaa VETUMA-palvelulle virhevastauksen. VETUMA-palvelu tallettaa tästä tiedon omaan lokiinsa, ja palauttaa maksatusvastauksen palautussovellukselle sen kutsussa antamaan virhepaluuosoitteeseen.
- Mikäli palauttaja peruu palautuksen verkkomaksupalvelun käyttöliittymässä, tallettaa verkkomaksupalvelu tästä tiedon omaan lokiinsa ja palauttaa VETUMA-palvelulle peruutusvastauksen. VETUMA-palvelu tallettaa tästä tiedon omaan lokiinsa ja palauttaa maksatusvastauksen palautussovellukselle sen kutsussa antamaan peruutuspaluuosoitteeseen.

6. LIITTEET

1. Liite1_VETUMA_palvelinvarmenteet (pdf)
2. Liite2_VETUMA_sanomaesimerkit (pdf)
3. Liite3_PERUSJHHS2 (xsd)