Jarkko Nevalainen

REKISTERÖITYMISRATKAISU JULKISHALLINNON SÄHKÖISEN ASIOINNIN PALVELUUN

Opinnäytetyö
Kajaanin ammattikorkeakoulu
Tradenomikoulutus
Tietojenkäsittelyn koulutusohjelma
Syksy 2010

Kajaanin ammattikorkeakoulu

OPINNÄYTETYÖ
TIIVISTELMÄ

Koulutusala Tradenomikoulutus	Koulutusohjelma Tietojenkäsittely
Tekijä(t) Jarkko Nevalainen	
Työn nimi REKISTERÖITYMISRATKAISU JULKISHALLINNON SÄHKÖISEN ASIOINNIN PALVELUUN	
Vaihtoehtoiset ammattiopinnot Ohjelmistosuunnittelu	Ohjaaja(t) Matti Härkönen
	Toimeksiantaja Documenta Oy
Aika Syksy 2010	Sivumäärä ja liitteet 50+2

Tämän opinnäytetyön tarkoituksena oli tutkia käyttäjän tunnistamista julkishallinnon sähköisen asioinnin palvelun kannalta ja toteuttaa ratkaisu, minkä avulla käyttäjä voi rekisteröityä SharePoint-ympäristössä olevan verkkopalvelun käyttäjäksi tunnistauduttuaan ensin tunnistuspalvelussa. Työn toimeksiantajana oli Documenta Oy.

VETUMA-palvelun käyttäjätunnistustoiminnallisuutta hyödyntävä rekisteröitymisratkaisu, Vetuma for SharePoint, toteutettiin Microsoftin SharePoint-alustalle. Ratkaisu on yhteensopiva Windows SharePoint Services 3.0:n, Microsoft Office SharePoint Server 2007, SharePoint Foundation 2010 ja SharePoint Server 2010 kanssa. Ratkaisun avulla henkilö voi rekisteröityä käyttäjäksi SharePoint-ympäristössä toimivaan verkkopalveluun. Ratkaisussa käyttäjälle tarjotaan myös mahdollisuutta kirjautua verkkopalveluun VETUMA-palvelun avulla, jolloin hänen ei tarvitse itse luoda tai muistaa käyttäjätunnusta ja salasanaa. Rekisteröitymis- ja kirjautumistoimintojen lisäksi ratkaisu mahdollistaa unohtuneen salasanan korvaamisen uudella. Ratkaisun toteutuksessa käytettiin C#-ohjelmointikieltä ja ASP.NET-ohjelmointimenetelmää. Kehitystyökaluna toimi Microsoftin Visual Studio 2008 ja Visual Studio 2010. VETUMA-palvelun liittämisessä ratkaisuun hyödynnettiin Vetuma Toolkit –luokkakirjastoa.

Vetuma for SharePoint –ratkaisu toteutettiin avoimen lähdekoodin periaatteella eli lähdekoodi on kaikkien saatavilla Internetissä. Ratkaisun asennuspaketit ja asennusohjeet eri SharePoint-versioille sekä ratkaisun lähdekoodi ovat saatavilla codeplex.com-palvelusta.

Opinnäytetyön teoriaosuudessa tutkittiin käyttäjän tunnistamista Internetissä sekä VETUMA-palvelua ja erityisesti sen tunnistustoimintoa. Teoriaosassa tutustutaan VETUMA-palveluun sekä palvelun toiminnallisuuteen ja rajapintaan.

Kieli	Suomi
Asiasanat	VETUMA, käyttäjän tunnistaminen, SharePoint, avoin lähdekoodi
Säilytyspaikka	☒ Verkkokirjasto Theseus ☒ Kajaanin ammattikorkeakoulun kirjasto

Kajaanin ammattikorkeakoulu
University of Applied Sciences

THESIS
ABSTRACT

School Business	Degree Programme Business Information Technology
Author(s) Jarkko Nevalainen	
Title Registration Solution for Online Service of Public Administration	
Optional Professional Studies Programming	Instructor(s) Matti Härkönen
	Commissioned by Documenta Oy
Date Autumn 2010	Total Number of Pages and Appendices 50+2

The purpose of the thesis was to study eIdentification for online services of public administration and to implement a solution that utilizes the Vetuma service for authenticating users before they register to the online service. The thesis was commissioned by Documenta Oy.

A solution using the identification function of Vetuma was implemented in the SharePoint environment because of its growing popularity. The solution is compatible with Windows SharePoint Services 3.0, Microsoft Office SharePoint Server 2007, SharePoint Foundation 2010 and SharePoint Server 2010. With the solution the users of Internet are able to register themselves to the online service operating in the SharePoint environment. Successful identification at Vetuma service is required before registration. The solution also allows people to login to the online service with Vetuma. The login function of the solution does not require registration to the service, the account is made automatically. If the person is already registered, he or she can login with Vetuma without the user name and password. Additionally, the solution allows users to create a new password to substitute a forgotten one. Before replacing the password successful authentication at Vetuma is required.

The solution was implemented with C# and Asp.Net and the development environments were Microsoft's Visual Studio 2008 and Visual Studio 2010. The solution is an open source solution and anyone can download it with or without source code from http://vetuma.codeplex.com. The installation guide is included in the installation packages.

The theory part of the thesis concentrates on the Vetuma service and especially its identification function. It also contains general information about identifying users at Internet. The part contains general details about the Vetuma service, describes the functionality and the interface of the service.

Language of Thesis	Finnish
Keywords	VETUMA, User Identification, SharePoint, Open Source
Deposited at	☒ Electronic library Theseus ☒ Library of Kajaani University of Applied Sciences

ALKUSANAT

Opinnäytetyöprosessin alkaessa syksyllä 2008 tämä hetki tuntui hyvin kaukaiselta. Hieman yli kaksi vuotta tähän tavoitteeseen pääseminen kestikin. Nyt näytölläni on valmis opinnäytetyö ja olo on melko tyhjä, samoin sanavarasto. Sen vuoksi osoitankin vain kiitokset opinnäytetyöprosessissa mukana olleille tai siihen vaikuttaneille tahoille, erityisesti Documenta Oy:lle aiheen tarjoamisesta opinnäytetyöhöni.

SISÄLLYS

SYMBOLILUETTELO

.NET	Lyhenne Microsoftin ohjelmistokomponenttikirjasto .Net Frameworkista
Asp.Net	Web-sovellusten kehittämiseen tarkoitettu menetelmä .Net Frameworkissa
ASPX	Active Server Page Extended Asp.Net-tekniikan web-sivu, joka koostuu pääsääntöisesti (x)html-kuvauskielestä.
HANSEL	Suomen valtion yhteishankintayhtiö
HST	Henkilön sähköinen tunnistaminen
Jaettu salaisuus	Symmetrinen salausavain Jaettu salaisuus on yleensä pitkäikäinen, kahden eri osapuolen tiedossa oleva salausavain. Esimerkkinä voidaan mainita verkkopalvelun sanasana; käyttäjä tietää oman salasanansa ja verkkopalvelu tietää käyttäjän salasanan.
LOGIN	VETUMA-palvelun palvelutyyppi
MAC	Message Authentication Code, viestien turvatarkiste
MOSS	Microsoft Office SharePoint Server

Query string	Kokoelma parametreja arvoineen
	Käytetään esimerkiksi Asp.Net:ssä url-osoitteessa varsinaisen osoitteen jälkeen ?-merkillä erotettuna, esimerkiksi www.demo.fi/default.aspx?parametri1=abc.
RFC	Request for Comments
	Joukko Internetin erilaisia käytäntöjä kuvaavia asiakirjoja.
SAML	Security Assertion Markup Language, xml-standardi
	Tätä standardia käytetään käyttäjien tunnistamis- ja valtuutustietojen vaihtamiseen turva- ja tunnistuspalveluiden välillä.
SATU	Sähköinen asiointitunnus
SPIN	Allekirjoitus- tai tunnistustapahtuman varmistamiseen tarkoitettu henkilökohtainen koodi
SSL	Secure Socket Layer, tietoturvaprotokolla
TLS	Transport Layer Security (RFC2246), SSL 3.0:n pohjalta luotu tietoturvaprotokolla
Tupas	Tunnistuspalvelu asiointipalveluntuottajille
WSS	Windows SharePoint Services

1 JOHDANTO

Palveluiden siirtyessä entistä enemmän Internetiin, yleistyy sähköinen asiointi myös julkishallinnon palveluissa. Sähköiseen asiointiin liittyy oleellisena osana käyttäjän luotettava tunnistaminen. Suomen kunnille ja julkishallinnon organisaatioille on kehitetty VETUMA-palvelu, joka tarjoaa sähköisille asiointipalveluille käyttäjän luotettavaa tunnistamista. Tässä opinnäytetyössä käsitellään käyttäjän tunnistamista Internetissä sekä VETUMA-palvelua ja erityisesti sen LOGIN-palvelutyyppiä. Lisäksi esitellään toteutettu rekisteröitymisratkaisu, joka hyödyntää VETUMA-palvelua käyttäjän tunnistamisessa rekisteröitymisen yhteydessä.

Opinnäytetyön aluksi tutustutaan käyttäjän Internetissä tunnistamisen menetelmiin. Sen jälkeen esitellään VETUMA-palvelu yleisellä tasolla. Yleisesittelyssä käydään läpi palvelun historia, hyödyt ja palveluun liittyminen. Lisäksi esitellään muutamia VETUMA-palvelua hyödyntäviä tahoja sekä muita Internetin suomalaisia käyttäjätunnistuspalveluita. Yleisesittelyn jälkeen tutustutaan VETUMA-palvelun tarjoamaan toiminnallisuuteen sekä palvelun rajapintaan. Rajapintaa käsittelevässä osiossa selvitetään, kuinka organisaatioiden asiointisovellukset kutsuvat palvelua, miten kutsujen eheys varmistetaan ja mitä parametreja kutsuihin kuuluu. Kun VETUMA-palvelun toiminnallisuus ja rajapinta on esitelty, tutustutaan palvelun LOGIN-palvelutyyppiin. LOGIN-palvelutyypin esittelyssä käsitellään kyseisen palvelutyypin eri toiminnot.

SharePointin suosio on kasvanut viime vuosina. Tänä vuonna esitellyt SharePoint Foundation 2010 ja SharePoint Server 2010 ovat tuoneet SharePointiin lisää ominaisuuksia, jotka varmasti osaltaan vaikuttavat positiivisesti SharePointin suosioon. SharePointin suuren suosion vuoksi tämän opinnäytetyön empiirisessä osuudessa toteutettiin VETUMA-palvelua hyödyntävä rekisteröitymisratkaisu SharePoint-alustalle. Ratkaisu toteutettiin avoimen lähdekoodin periaatteella. Luotu lähdekoodi on vapaasti kaikkien saatavilla Internetissä codeplex.com-palvelussa. Ratkaisuun tutustutaan VETUMA-palvelun esittelyn jälkeen.

Lopuksi tehdään yhteenveto opinnäytetyössä läpikäydyistä asioista sekä arvioidaan toteutettua ratkaisua ja koko opinnäytetyöprosessia.

2 KÄYTTÄJÄN TUNNISTAMINEN INTERNETISSÄ

Tässä luvussa käsitellään käyttäjän tunnistamista Internetissä. Käyttäjän luotettava tunnistaminen on edellytys sähköiselle asioinnille. Asioitaessa esimerkiksi virastossa, asiakas tunnistetaan henkilöllisyystodistuksesta. Internetissä asioitaessa ei ole kuitenkaan ketään, kenelle perinteistä henkilöllisyystodistusta voisi näyttää. Sen vuoksi käyttäjän tunnistamiseksi Internetissä on olemassa seuraavia menetelmiä:

- käyttäjätunnus-salasana -yhdistelmä,
- kansalaisvarmenne ja
- verkkopankkitunnukset. (Korpela 2007, 234.)

Verkkopankkitunnukset ovat pankin asiakkaalleen myöntämät, henkilökohtaiset tunnukset. Myönnettäessä tunnuksia pankki tarkistaa asiakkaansa henkilöllisyyden ja näin ollen verkkopankkitunnuksia voidaan pitää luotettavana tunnistustapana Internetissä. Kansalaisvarmenne puolestaan on Väestörekisterikeskuksen myöntämä, erittäin luotettavana pidetty tunnistusmenetelmä. Sähköisen tunnistautumisen lisäksi kansalaisvarmennetta voidaan käyttää sähköpostiviestien ja tiedostojen salaamiseen sekä sähköisen allekirjoituksen tekemiseen. Käyttäjätunnus-salasana -yhdistelmää käytettäessä käyttäjätunnus ja salasana on ensin toimitettava käyttäjälle luotettavasti. Käyttäjätunnuksen ja salasanan luovutus voidaan tehdä esimerkiksi käyttäjän asioidessa virastossa, jossa hänen henkilöllisyytensä voidaan varmistaa. Seuraavissa alaluvuissa tutustutaan tarkemmin näihin Internetin käyttäjätunnistusmenetelmiin. (Korpela 2007, 234.)

2.1 Käyttäjätunnus-salasana -tunnistaminen

Käyttäjätunnus-salasana -yhdistelmä on yleisin tunnistustapa tietotekniikassa. Käyttäjä tunnistetaan käyttäjätunnuksen perusteella. Salasana puolestaan on järjestelmän ja käyttäjän jakama salaisuus, jolla autentikoidaan käyttäjä. Käyttäjätunnusta ja salasanaa käytetään paljon niiden helpon ja halvan toteutuksen takia. Helppouden ja halvan hinnan lisäksi niissä ei Petteri Järvisen mukaan ole mitään muuta hyvää. Käyttäjätkään eivät pidä suuresta käyttäjätunnusten ja salasanojen määrästä, sillä niitä on vaikea muistaa. Suuri salasanojen määrä johtaa

helposti siihen, että käytetään samaa salasanaa useassa paikassa, luodaan lyhyitä, helposti muistettavia salasanoja tai kirjoitetaan salasanoja paperille. Nämä edellä mainitut toimet heikentävät oleellisesti salasanojen turvallisuutta. (Järvinen 2003, 35 - 36.)

2.2 Kansalaisvarmenteeseen perustuva tunnistaminen

Kansalaisvarmennetta käytetään sähköiseen henkilöllisyyden todistamiseen. Suomi oli ensimmäinen maa, jossa kansalaisvarmenteita eli sähköisiä henkilöllisyyksiä alettiin myöntää. Tämä tapahtui 1.12.1999, jolloin kansalaisvarmenne liitettiin HST- eli sirullisiin henkilökortteihin. Pian Suomen jälkeen muutkin maat, ensimmäisten joukossa Belgia, Italia, Ruotsi ja Viro, alkoivat ottaa käyttöön sirullisia henkilökortteja. Sirullisen henkilökortin suosion kasvua hidastivat tavallista henkilökorttia korkeampi hinta, lyhyempi voimassaoloaika ja kortilla käytettävien palveluiden vähyys. Ensimmäisen kolmen vuoden aikana kansalaisvarmenteella varustettuja HST-kortteja oli hankittu vain 16 000 kappaletta. Vuosina 2002 ja 2003 käynnistettiin erilaisia hankkeita ja ryhmiä vauhdittamaan HST-kortin yleistymistä. Keväällä 2003 eduskunta hyväksyi lait sähköisestä asioinnista ja sähköisestä allekirjoituksesta, jotka osaltaan vauhdittivat HST-kortin suosion kasvua. (Järvinen 2003, 190 - 191.)

Kansalaisvarmenteen avulla henkilö voi todistaa henkilöllisyytensä Internetissä sekä allekirjoittaa tekstejä ja tiedostoja sähköisesti. Ne ovat kansalaisvarmenteen kaksi päätoimintoa. Kansalaisvarmenteella tunnistautumisen jälkeen Internetissä toimiva palveluntarjoaja voi olla varma yhteyden toisessa päässä olevan henkilön henkilöllisyydestä. Sähköinen allekirjoitus puolestaan kertoo muille tekstin tai tiedoston lukijoille, että kyseinen kohde on allekirjoittajan hyväksymä. Lisäksi lukijat voivat olla varmoja siitä, ettei tekstiä tai tiedostoa ole allekirjoituksen jälkeen muutettu. Sähköisen allekirjoittamisen periaate on yksinkertainen; allekirjoitettavasta asiakirjasta lasketaan ensin tiiviste, minkä jälkeen tiiviste salataan henkilön salaisella avaimella. Allekirjoitetun tekstin eheys voidaan tarkistaa allekirjoittajan julkisen avaimen avulla. Kansalaisvarmenteella sähköisesti allekirjoitettu teksti on Suomen lain perusteella oikeudellisesti pätevä. (Järvinen 2003, 154, 194, 209.)

Yksittäinen henkilö voi hankkia itselleen kansalaisvarmenteen Väestörekisterikeskuksesta. Varmenne sisältää omistajansa etu- ja sukunimen, tiedon kotimaasta, myöntämisajankohdan, varmenteen voimassaoloajan ja sähköisen asiointitunnuksen, SATUn. Näiden tietojen lisäksi kansalaisvarmenne sisältää teknistä tietoa ja Väestörekisterin sähköisen allekirjoituksen, jolla

todistetaan varmenteessa olevat tiedot oikeiksi. Kansalaisvarmennetta ei käytetä henkilötietojen säilyttämiseen vaan ainoastaan henkilöllisyyden todistamiseen ja sen vuoksi se ei sisällä esimerkiksi omistajansa syntymäaikaa tai kotiosoitetta. Jos kansalaisvarmenteen omistajasta tarvitaan muita kuin kansalaisvarmenteeseen tallennettuja tietoja, on tiedot haettava muista lähteistä. (Järvinen 2003, 192.)

SATU on henkilön sähköinen asiointitunnus. SATU muodostuu 8-numeroisesta numerosarjasta ja tarkistusmerkistä, joka lasketaan samalla tavalla kuin henkilötunnuksen tarkistusmerkki. SATU ei varsinaisesti kerro mitään henkilöstä, vaan se yksilöi kyseisen henkilön muiden saman nimisten henkilöiden joukosta. Jokainen suomalainen kesäkuussa 2003 tai sen jälkeen syntynyt on saanut heti syntymän jälkeen henkilötunnuksen lisäksi myös SATUn. Aivan kuten henkilötunnus, SATUkin säilyy koko elämän ajan. (Järvinen 2003, 193 - 194.)

Kansalaisvarmenne voidaan tallentaa HST-kortille, OP-ryhmän Visa Electron -kortille tai matkapuhelimen SIM-kortille. HST-kortille tallennettaessa kansalaisvarmenteeseen liittyy kaksi(2) PIN-koodia. PIN1-koodia käytetään tunnistautumisen yhteydessä ja PIN2-koodia sähköisessä allekirjoituksessa. PIN-koodien avulla kortti ja sen oikea haltija sidotaan toisiinsa. Kortti ja PIN1-koodi yhdessä tekevät käyttäjän henkilöllisyyden todistamisesta luotettavan. Sirullisen kortin käyttöä varten tarvitaan tietokoneeseen liitettävä sirukortinlukija ja kortinlukijaohjelmisto. (Järvinen 2003, 192, 197 - 200.)

2.3 Tupas-tunnistus

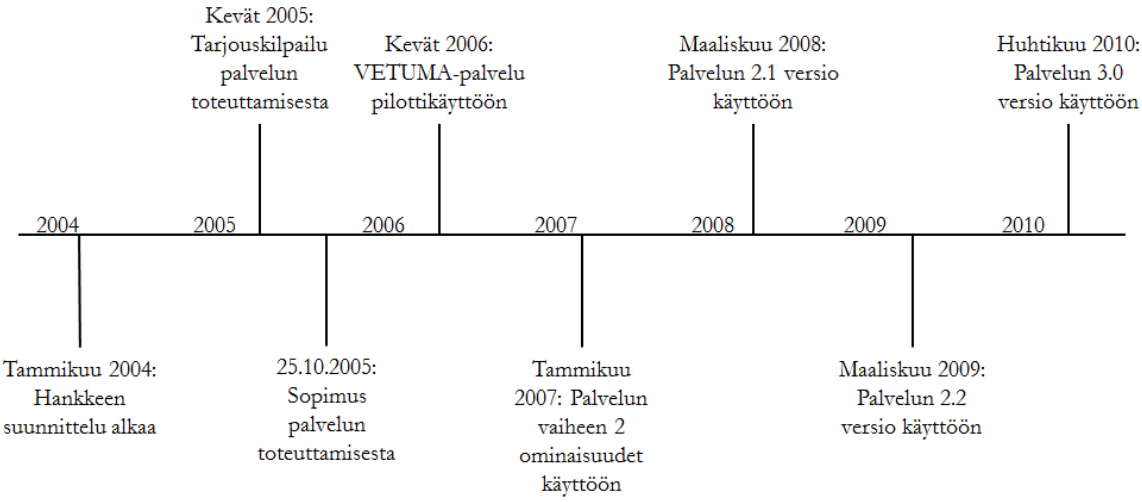
Tupas-rajapinta on Suomen Pankkiyhdistyksen määrittelemä yhteinen rajapinta, jonka kautta eri pankkien verkkopalvelut tarjoavat käyttäjän tunnistusta Internet-palveluiden tarjoajille (Fujitsu Services Oy 2010 a, 15). Ensimmäiset pankit alkoivat jakaa laskujen maksamiseen tarkoitettua DOS-ohjelmaa modeemin omistaville asiakkailleen jo 1980-luvun lopussa. Pankit olivat tuolloin sähköisen asioinnin edelläkävijöitä. Pankissa asioitaessa henkilöltä kysytään aina henkilöllisyystodistusta, sillä pankkitoiminnassa on erittäin tärkeää tunnistaa asioiva henkilö. Sähköisessä pankkiasioinnissa henkilöllä on asiakasnumero tai käyttäjätunnus ja salasana sekä lista kertakäyttöisiä tunnuksia, joilla hänen henkilöllisyytensä voidaan turvallisesti varmistaa. Verkkopankkiasioinnin yleistyessä pankit alkoivat myydä omaa luotettavaa tunnistuspalvelua muidenkin Internetissä toimivien palveluntarjoajien käyttöön. Asiointipalvelut, verkkokaupat ja muut käyttäjän tunnistamista tarvitsevat Internetissä toimivat palvelut voivat

tehdä sopimuksen Tupas-palvelun käytöstä. Koska pankeilla oli oma luotettava tunnistusjärjestelmä, eivät pankit olleet kovin kiinnostuneita HST-kortin käytöstä. OP-ryhmä oli edelläkävijä pankkien saralla HST-kortin käytössä, sillä se alkoi tarjota HST-kortilla tapahtuvaa tunnistusvaihtoehtoa vuonna 2001. (Järvinen 2003, 191 - 192.)

3 VETUMA-PALVELUN ESITTELY

VETUMA-palvelu on julkishallinnon tarjoama, kansalaisille tarkoitettu verkkotunnistus- ja maksamispalvelu. Palveluun voivat liittyä valtion ja kuntien organisaatiot. Palvelun omistaa Suomen valtio ja se maksaa palvelun käyttöönotto- ja tapahtumakustannukset vuoden 2010 loppuun saakka. (Suomi.fi 2010.)

3.1 VETUMA-palvelun historia



Kuvio 1. VETUMA-palvelun historia.

Kuviossa 1 esitetty VETUMA-palvelun historia alkaa tammikuusta 2004, jolloin Espoon kaupunki ja Vantaan kaupunki alkoivat suunnitella yhteisen tunnistus- ja maksamispalvelun hankkimista. Saman vuoden keväällä mukaan hankkeeseen liittyivät Helsingin ja Kauniaisten kaupungit sekä Suomen valtio. Palvelu herätti kiinnostusta muissa kunnissa ja pian mukaan liittyi noin 60 kuntaa ja kuntayhteisöä. Keväällä 2005 Helsingin kaupunki ja Hansel järjestivät tarjouskilpailun palvelun toteuttamisesta. Palvelun toimittajaksi valittiin kesäkuussa 2005 Fujitsu Services Oy ja sopimus palvelun toteuttamisesta solmittiin 25.10.2005. (Valtiovarainministeriö 2009, 2.)

Palvelun toimitus jaettiin alussa kahteen vaiheeseen, joista ensimmäisen vaiheen toimintojen suunniteltiin olevan käytössä maaliskuussa 2006 ja toisen vaiheen toimintojen vuoden 2007 alussa. Ensimmäiseen vaiheeseen kuuluivat seuraavat toiminnot:

- käyttäjän tunnistaminen pankkitunnuksilla, sähköisellä henkilökortilla sekä käyttäjätunnuksella ja salasanalla
- käyttäjän henkilötunnuksen noutaminen Väestötietojärjestelmästä
- asiakirjan tai vastaavan hyväksyminen pankkitunnuksilla ja sähköisellä henkilökortilla
- kiistämätön allekirjoitus sähköisellä henkilökortilla, esimerkiksi hakemuksiin
- verkkomaksaminen pankkien verkkopalveluissa. (Valtiovarainministeriö 2009, 3.)

Kun ensimmäisen vaiheen toiminnot oli saatu valmiiksi, järjestelmä otettiin pilottikäyttöön keväällä 2006 (Valtiovarainministeriö 2009, 2 - 3).

Toukokuussa 2006 VETUMA-palvelu voitti kunniamaininnan kansainvälisessä World Information Technology and Services Alliancen, WITSAn, järjestämässä Global IT Excellence Awards –kilpailussa (Fujitsu 2006). Samana vuonna VETUMA-palvelu valittiin suomalaisessa Julk IT awards –kisassa parhaaksi julkishallinnon yleishankkeeksi. Alan vaikuttajista koostuneen raadin mielestä VETUMA-palvelu oli ainutlaatuinen kisassa ja täytti kriteerit julkishallinnon yhteisinvestoinnista parhaiten. Seuraavassa ote raadin perusteluista:

> "Hanke on osoitus siitä, että julkishallinnon sisällä voidaan aidosti toteuttaa yhteishankkeita. Vetuma näyttää esimerkkiä siitä kuinka useat toimijat eri näkökulmistaan toteuttavat ja hyödyntävät yhteistä projektia. Kyseessä on todellinen tietoyhteiskuntahanke, jossa yhteisten tahtotilojen löytämisessä on onnistuttu." (Tietokone.fi 2006.)

Vuoden 2007 alussa palvelu laajeni suunnitelmien mukaisesti seuraavilla toiminnoilla:

- tunnistaminen ja sähköinen allekirjoittaminen mobiilikansalaisvarmenteella
- luottokorttimaksaminen Luottokunnan luottokorteilla
- maksun palautus sitä tukevissa palveluissa. (Valtiovarainministeriö 2009, 2 - 3.)

Helmikuussa 2008 VETUMA-palvelussa oli käytössä kaikki ensimmäisen ja toisen vaiheen toiminnot. Maaliskuussa 2008 julkaistiin palvelun 2.1 versio, johon oli lisätty aikaisempaa laajempi kysely väestötietojärjestelmästä. Laajennetun kyselyn avulla käyttäjästä saatiin aikaisempaa enemmän tietoa, mm. äidinkieli, kotikunta ja koko nimi pelkän henkilötunnuksen sijasta. Lisäksi 2.1 versiossa otettiin käyttöön uusi DigiSign-kortinlukijaohjelmisto. VETU-

MA-palvelun versio 2.2 otettiin käyttöön maaliskuussa 2009 ja se toi palveluun uutena ominaisuutena SAML 2.0 rajapinnan. (Valtiovarainministeriö 2009, 3.)

VETUMA-palvelun 3.0 versio otettiin käyttöön 30.4.2010. Palvelun uusin versio varmistaa käyttäjän pääsyn asiointitiliin kertakirjautumisella ja mahdollistaa verkkopankkimaksun onnistumisen tarkistamisen VETUMA-palvelun avulla. (Suomi.fi 2010.)

3.2 VETUMA-palvelun tietoturva

Käyttäjien henkilötietoja käsittelevässä järjestelmässä tietoturva on olennaisen tärkeä. Tämän vuoksi VETUMA-palvelun on tietoturva-auditoinut ulkopuolinen auditoija. Auditoinnissa on otettu huomioon kattavasti palvelun eri osa-alueet. Tämän lisäksi VETUMA-palvelun tuottajalle, Fujitsu Services Oy:n palvelutuotannolle, on myönnetty standardoitu tietoturvasertifikaatti. (Valtiovarainministeriö 2009, 7.)

Tekninen tietoturva on toteutettu käyttämällä VETUMA-palvelussa ainoastaan suojattua Internet-yhteyttä, jolla varmistetaan tiedon suojaus tiedon liikkuessa Internetissä. Tämän lisäksi osapuolten identiteetti ja viestien eheys varmistetaan käyttämällä jaettuun salaisuuteen perustuvaa turvatarkisteen (MAC) laskentaa. Palvelun tietoturvaan liittyviin ominaisuuksiin tutustutaan tarkemmin myöhemmissä luvuissa. (Valtiovarainministeriö 2009, 7.)

3.3 VETUMA-palvelun hyödyt

Valtiovarainministeriön Valtion IT-toiminnan johtamisyksikkö on listannut VETUMA-palvelun hyödyiksi muun muassa seuraavia asioita:

- palvelu on kilpailutettu koko julkishallinnon käyttöön ja on näin edullinen käyttää
- palvelu on monipuolinen ja tietoturvallinen
- palvelua kehitetään keskitetysti, mikä tuo uudet palvelut kerralla kaikkien käyttöön
- palveluun löytyy yhtenäinen ohjeistus Internetistä
- mahdollisuus koulutukseen ja konsultointiin

- valmiiksi neuvotellut sopimukset palveluun kuuluvien tahojen välillä
- yhtenäinen toiminnallisuus ja käyttöliittymä kaikkiin julkishallinnon palveluihin tunnistauduttaessa tekee palvelusta helppokäyttöisen kansalaisille. (Valtiovarainministeriö 2009, 8.)

Laki sähköisestä asioinnista määrää viranomaisia käyttämään sähköisessä asioinnissa mahdollisimman helppokäyttöisiä ja yhteensopivia ohjelmistoja (Kuntaliitto 2009, 128). Edellä olleen listauksen mukaan VETUMA-palvelu auttaa osaltaan viranomaisia toteuttamaan tämän vaatimuksen.

3.4 Esimerkkejä VETUMA-palvelun hyödyntämisestä

Elokuussa 2010 VETUMA-palvelun asiakkaana oli yli 70 kuntaa ja valtion organisaatiota. Asiakkaat käyttävät vaihtelevasti tunnistus- ja maksatustoimintoja, joillakin on käytössä molemmat, toisilla vain toinen toiminto. Seuraavassa on esitetty muutamia esimerkkejä VETUMA-palvelun käytöstä. (Fujitsu Services Oy 2010 c, 3.)

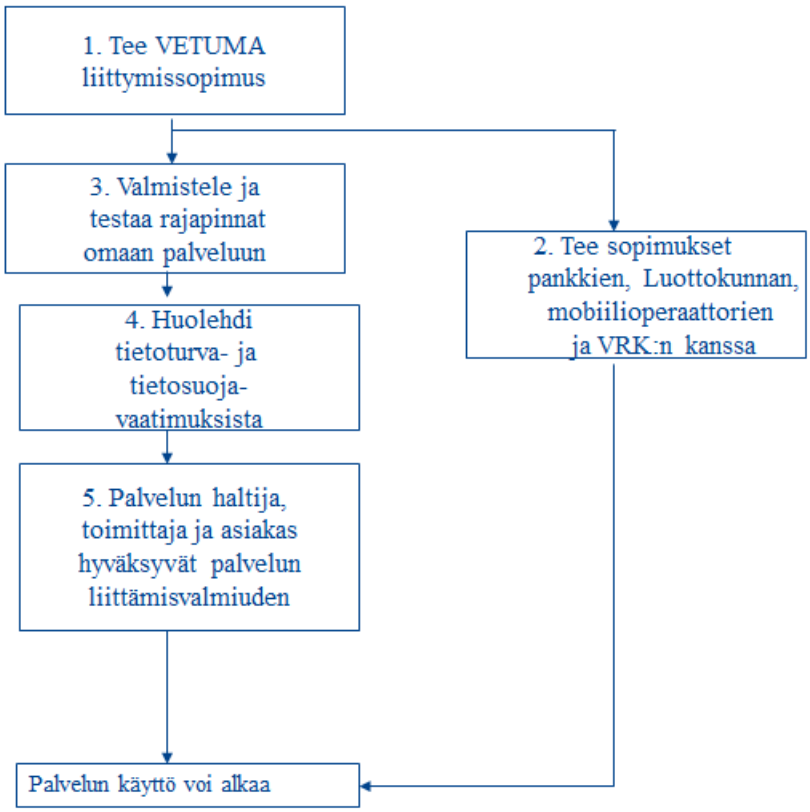
Oulun kaupunki oli ensimmäinen kunta Suomessa, jossa kuntalaiset pystyivät tekemään mobiili- ja verkkokuntalaisaloitteen. VETUMA-tunnistusta hyödyntävä aloitetoiminto otettiin käyttöön Oulun kaupungin nuorisoasiainkeskuksen lasten- ja nuorten osallisuuteen liittyvässä mobiili- ja verkkoaloitekanavassa vuonna 2005. Kyseessä oli pilottihankkeena toteutettu Tee Aloite –palvelu. Hankkeen rahoituksesta vastasivat Oulu Innovaatioympäristö –hanke ja Verkkopalveluiden kehittäminen –hanke. (Kunnat.net 2005.)

Turussa VETUMA-palvelua hyödynnetään mm. yhdistystietojen ylläpidossa. Turun seudulla toimivat yhdistykset, seurat ja järjestöt voivat lisätä yhdistyksen tiedot ja ylläpitää niitä Turun kaupungin verkkopalvelussa. Tietojen lisääminen edellyttää VETUMA-tunnistautumista, minkä jälkeen yhdistyksen edustaja saa tunnukset, joilla hän pääsee lisäämään tai päivittämään yhdistyksen tietoja. (Turku.fi 2008.)

Kotkassa kuntalainen voi selata kaupunkisuunnittelun kiinteistörekisterissä olevia tietojaan Internetissä. Tietojen selailu edellyttää tunnistautumista VETUMA-palvelun avulla. (Kymenlaakson ammattikorkeakoulu 2007.)

Poutapilvi Web Design on toteuttanut Valtiontalouden tarkastusvirastolle vaalirahoitusjärjestelmän, jonka käyttäjätunnistuksessa hyödynnetään VETUMA-palvelun tunnistustoiminnallisuutta. Järjestelmää käyttävän henkilön on ensin tunnistauduttava VETUMA-palvelussa ennen kuin hän voi täyttää vaalirahoitus- tai ennakkoilmoituksen. (Poutapilvi 2009.)

3.5 Liittyminen VETUMA-palveluun



Kuvio 2. VETUMA-palvelun liittymisprosessi (Valtiovarainministeriö 2009, 5).

Kuviossa 2 esitetään VETUMA-palvelun liittymisprosessi. VETUMA-palvelun käyttöönottamiseksi asiakkaan on ensin tehtävä VETUMA-liittymissopimus. Tämän jälkeen on tehtävä erilliset sopimukset pankkien, Luottokunnan, mobiilioperaattorien ja Väestörekisterikeskuksen kanssa sen mukaan, mitä palveluita asiakas haluaa asiointisovellustensa käyttäjille tarjota. Kunta-asiakkaat voivat tehdä VETUMA-liittymissopimuksen sisäasiainministeriön KuntaIT-yksikön ja valtion laitokset valtiovarainministeriön Valtion IT-toiminnan johtamisyksikön kautta. Kun asiakas on tehnyt VETUMA-liittymissopimuksen, tulee tämän valmistella ja testata rajapinnat VETUMA-palveluun sekä huolehtia tietoturva- ja tietosuojavaatimusten täyttymisestä. Asiakkaan tehtyä vaadittavat esivalmistelut hyväksyvät palvelun haltija, toimittaja

ja asiakas valmiuden palvelun käyttöönottoon, minkä jälkeen palvelun käyttö voi alkaa. (Valtiovarainministeriö 2009, 5 - 6.)

3.6 Muita suomalaisia käyttäjäntunnistuspalveluita

VETUMA-palvelu ei ole ainoa sähköisen tunnistamisen tai tunnistukseenohjauksen palvelu Suomessa. Kansaneläkelaitos, työ- ja elinkeinoministeriö sekä verohallitus omistavat tunnistus.fi-palvelun, joka tarjoaa henkilötunnistuksen lisäksi myös yritystunnistuksen. Palvelu otettiin käyttöön tammikuussa 2004 ja se perustuu Ubisecure-yrityksen Ubilogin-valmistuotteeseen. Tunnistus.fi-palvelussa voi tunnistautua verkkopankkitunnuksilla ja sirullisella henkilökortilla. (Kiiski 2004, 6 - 8.)

Työeläkejärjestelmän yhteistä tunnistuspalvelua käyttävät työeläkejärjestelmän verkkopalvelut kuten esimerkiksi Eläke-Fennia, Kuntien eläkevakuutus ja Työeläke.fi. Tunnistuspalvelua hyödynnetään sähköisessä eläkeasioiden käsittelyssä. Palvelussa käyttäjä voi valita tunnistustavakseen verkkopankkitunnukset tai sirullisen henkilökortin. (Työeläkejärjestelmän yhteinen tunnistuspalvelu.)

4 VETUMA-PALVELUN TOIMINNALLISUUS

Tässä luvussa kerrotaan VETUMA-palvelun sovelluksille tarjoamasta toiminnallisuudesta. Toiminnallisuus on sovelluksien käytettävissä yleisen kutsujarajapinnan kautta, joka myös kuvataan tässä luvussa. Luvun lopuksi kerrotaan lyhyesti VETUMA Toolkit -paketista, joka helpottaa asiointisovelluksen liittämistä VETUMA-palveluun.

VETUMA-palvelun versiossa 3.0 sovelluksille on tarjolla käyttäjän tunnistaminen, toimenpiteen hyväksyminen, kiistämätön sähköinen allekirjoitus, maksun maksattaminen ja maksetun maksun palautus. Käyttäjän tunnistamiseen voidaan käyttää verkkopankkien tunnistuspalvelua Tupasta, käyttäjätunnus-salasana tunnistusmenetelmiä tai kansalaisvarmenteeseen perustuvaa tunnistusta. Toimenpiteen hyväksyminen ja kiistämätön sähköinen allekirjoitus perustuvat käyttäjän tunnistamiseen edellä mainituilla menetelmillä, mutta kiistämätön sähköinen allekirjoitus on mahdollista tehdä vain kansalaisvarmennetunnistusta käyttämällä. (Fujitsu Services Oy 2010 a, 3.)

Kuviossa 3 VETUMA-palvelun käyttäjätunnistustoimintoja vertaillaan edellisen luvun lopussa mainittuihin palveluihin. Kuviosta nähdään, kuinka monipuolinen käyttäjäntunnistuspalvelu VETUMA on. Verrattuna tunnistus.fi-palveluun ja Työeläkejärjestelmän yhteiseen tunnistuspalveluun VETUMA-palvelussa on mahdollista tunnistautua mobiilikansalaisvarmenteella sekä selain- ja matkapuhelinpohjaisesti käyttäjätunnuksella ja salasanalla. Tunnistus.fi ja Työeläkejärjestelmän tunnistuspalvelu tarjoavat tunnistautumista vain yleisimmillä menetelmillä eli pankkien Tupas-tunnistuksella ja sirullisella henkilökortilla sijaitsevalla kansalaisvarmenteella.

	VETUMA	**Tunnistus.fi**	**Työeläkejärjestelmän yhteinen tunnistus-palvelu**
Verkkopankkitunnukset	X	X	X
Kansalaisvarmenne	X	X	X
Sirullinen henkilökortti	X	X	X
Mobiilivarmenne	X		
Käyttäjätunnus-salasana	X		
Selainpohjainen	X		
Matkapuhelin	X		

Kuvio 3. VETUMA-palvelun, tunnistus.fi-palvelun ja Työeläkejärjestelmän yhteisen tunnistuspalvelun toimintojen vertailu.

Käyttäjätunnus-salasana –periaatteeseen perustuvat tunnistusmenetelmät vaativat käyttäjältä käyttäjätunnuksen ja salasanan. Tunnus ja salasana voidaan kysyä Internet-selaimessa tai tunnistuskoodia voidaan kysyä matkapuhelimella. Verkkopankkien tunnistuspalvelussa tunnistautumiseen käytetään henkilökohtaisia verkkopankkitunnuksia. Käyttäjän tunnistuksessa käytettävä kansalaisvarmenteeseen perustuva tunnistaminen perustuu varmenteeseen, joka voi sijaita sirukortilla tai matkapuhelimen SIM-kortilla. Tunnistautumisen yhteydessä VETUMA-palvelu voi noutaa Väestötietojärjestelmästä joukon tunnistettavan käyttäjän perustietoja, kuten osoitetiedot ja kuntalaisuuden. Väestötietojärjestelmäkysely edellyttää tunnistautumista kansalaisvarmenteella tai verkkopankkitunnuksilla. (Fujitsu Services Oy 2010 a, 3.)

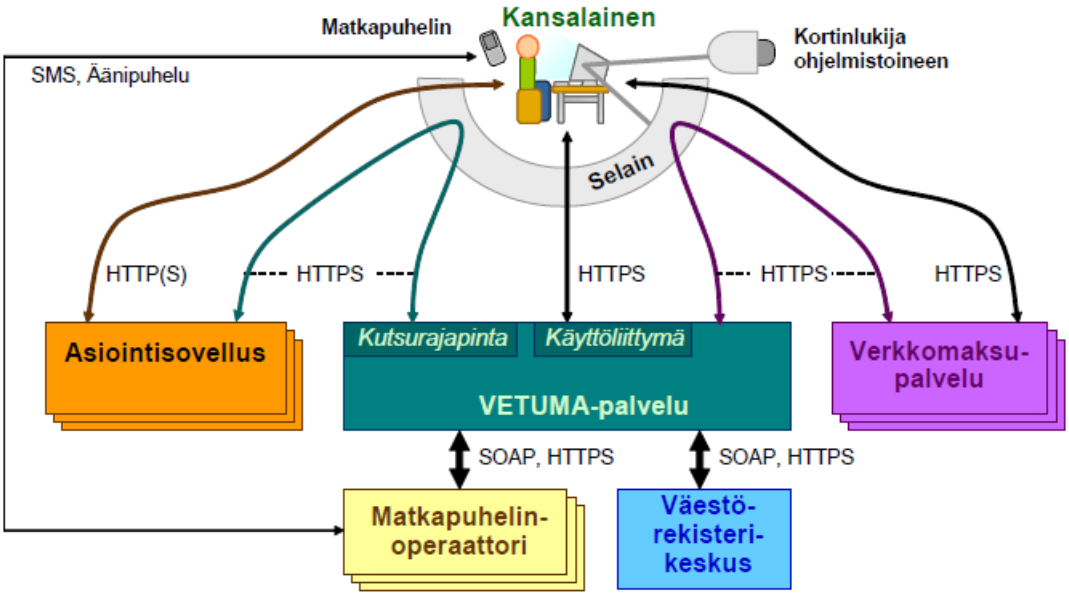
Maksun maksatuksessa tuettuja palveluita ovat pankkien verkkomaksupalvelut sekä Luottokunnan verkkomaksupalvelu. Maksun maksatuksen avulla asiointisovellus voi ohjata käyttäjän suorittamaan maksua VETUMA-palvelun kautta. VETUMA-palvelun kautta voidaan myös palauttaa maksettu maksu takaisin maksajan tilille joko osittain tai kokonaan. (Fujitsu Services Oy 2010 a, 3.)

Jotta sovellus voi hyödyntää VETUMA-palvelun rajapintaa ja edellä mainittuja toimintoja, on sovelluksella oltava käytössään VETUMA-asiakkaan, esimerkiksi kunnan, VETUMA-asiakaskonfiguraatio ja jaettu salaisuus. Asiakaskonfiguraatiossa kuvataan palvelun mukautus asiakkaan sovelluksen tarpeisiin. Asiakaskonfiguraatio määritetään asiakaskohtaisesti silloin, kun organisaatio liittyy VETUMA-palvelun asiakkaaksi. Samalla määritetään myös jaettu salaisuus tunnistus- ja maksatuskäyttöä varten. Jaetun salaisuuden avulla varmistetaan rajapintakutsujen ja -vastausten aitous ja alkuperä sekä osapuolten identiteetti. Jaettu salaisuus myös suojaa kutsuja muutoksilta kutsunvälitysten aikana. (Fujitsu Services Oy 2010 a, 4.)

VETUMA-asiakaskonfiguraatioon määritetyt valinnat asettavat tiettyjä vaatimuksia asiakkaalle. Jos asiakas haluaa käyttää yhtä tai useampaa käyttäjätunnus-salasana –pohjaista tunnistusmenetelmää, on asiakkaan ylläpidettävä omaa käyttäjärekisteriä VETUMA-palvelussa. Asiakkaan hyödyntäessä pankkien tarjoamaa Tupas-tunnistusta VETUMA-palvelussa, on asiakkaalla oltava Tupas-käyttöön oikeuttavat sopimukset pankkien kanssa. Jos jonkin pankin kanssa ei ole solmittu sopimusta Tupas-tunnistuksesta, ei asiakkaan asiointisovelluksen käyttäjille näytetä kyseistä pankkia tunnistautumisvaihtoehtona. Mikäli asiakas haluaa hyödyntää sovelluksissaan VETUMA-palvelun maksatustoimintoa, on asiakkaalla oltava verkkomaksujen vastaanottamiseen oikeuttavat sopimukset pankkien ja Luottokunnan kanssa. Jos sopimusta ei ole jonkin pankin tai Luottokunnan kanssa, asiakkaan asiointisovelluksen

käyttäjille ei näytetä kyseistä vaihtoehtoa maksamisvaihtoehtona VETUMA-palvelun käyttöliittymässä. Asiakkaan halutessa VETUMA-palvelun noutavan tunnistetun käyttäjän tietoja väestötietojärjestelmästä, on asiakkaan tehtävä sopimus asiasta Väestötietorekisterikeskuksen kanssa. Lisäksi asiakas tarvitsee Väestörekisterikeskuksen myöntämän luvan sille tietojoukolle, joka käyttäjään liittyen haetaan VETUMA-tunnistautumisen yhteydessä. (Fujitsu Services Oy 2010 a, 4.)

4.1 VETUMA-palvelun toimintaympäristö



Kuvio 4. Kuvaus VETUMA-palvelun toimintaympäristöstä (Fujitsu Services Oy 2010 a, 5).

VETUMA-palvelun toimintaympäristö on esitetty kuviossa 4, jossa kansalainen käyttää VETUMA-asiakkaan asiointisovellusta Internet-selaimella. Asiointisovellus kutsuu tarvittaessa VETUMA-palvelua, käyttäen palvelun kutsujarajapintaa. Asiointisovelluksen kutsu välitetään kansalaisen selaimen kautta VETUMA-palveluun ja kansalainen ohjautuu käyttämään palvelua. Osa VETUMA-palvelun tarjoamista toiminnoista on toteuttu palvelun yhteyteen ja osa toiminnoista ohjaa käyttäjän edelleen toiseen verkkopalveluun. Pankkien Tupas-tunnistuksessa ja verkkomaksamisessa kansalainen ohjataan VETUMA-palvelusta edelleen hänen valitsemaansa pankin tai Luottokunnan verkkopalveluun, käyttäen kyseisen palvelun rajapintakutsua. Rajapintakutsu välitetään pankin tai Luottokunnan verkkopalvelulle käyttäjän selaimen kautta. Käyttäjän suoritettua tunnistautumisen tai maksun verkkopalvelussa, verkkopalvelun vastaus välitetään VETUMA-palveluun kansalaisen selaimen kautta. Asioin-

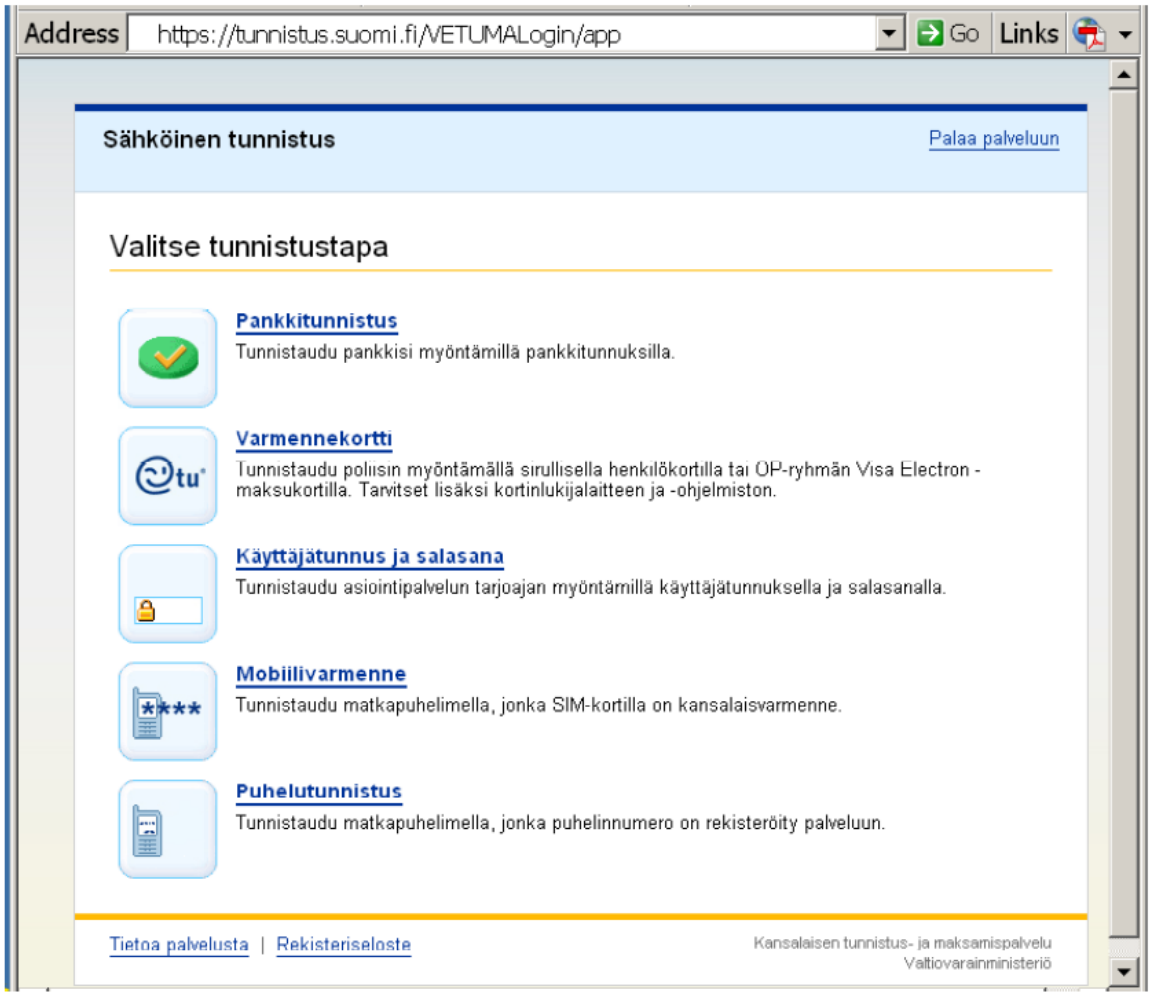
tisovelluksen pyytämän toiminnon suorittamisen jälkeen VETUMA-palvelu palauttaa vastauksen asiointisovellukselle kansalaisen selaimen kautta. Tämän jälkeen kansalainen jatkaa asiointisovelluksen käyttämistä. (Fujitsu Services Oy 2010 a, 5.)

Kaikki VETUMA-palvelun, asiointisovelluksen ja pankkien verkkopalveluiden välinen liikenne kulkee siis kansalaisen Internet-selaimen kautta. Liikenne suojataan käyttämällä https-yhteyskäytäntöä. Rajapintakutsuissa käytetään lisäksi jaettuun salaisuuteen perustuvaa turvatarkisteen laskentaa, jolla varmistetaan osapuolten identiteetti ja viestien eheys. (Fujitsu Services Oy 2010 a, 5.)

Käytettäessä sirukortilla sijaitsevaa kansalaisvarmennetta edellä kuvattuun toimintaympäristöön kuuluu lisäksi työasemassa oleva kortinlukija ja sen ohjelmisto. Mikäli käytetään SIM-kortilla sijaitsevaa kansalaisvarmennetta, toimintaympäristöön kuuluu edellä kuvattujen lisäksi matkapuhelin ja sen varusohjelmiston toimintoja. (Fujitsu Services Oy 2010 a, 5.)

4.1.1 VETUMA-palvelun käyttöliittymä

VETUMA-palvelun käyttöliittymä on selainpohjainen. Kansalainen käyttää sitä suorittaessaan toimintoja, joita asiointipalvelu on pyytänyt VETUMA-palvelulta. Kuviossa 5 esitetään VETUMA-palvelun tunnistuksen aloitussivu. VETUMA-palvelua kutsuva asiointisovellus määrittää VETUMA-palvelun käyttöliittymän kielen kutsussa olevan parametrin arvolla. Kielivaihtoehtoina ovat suomi, ruotsi ja englanti. (Fujitsu Services Oy 2010 a, 6.)



Kuvio 5. VETUMA-palvelun selainkäyttöliittymä (Fujitsu Services Oy 2010 a, 6).

Asiointisovelluksen pyytämällä toiminnolla on VETUMA-palvelussa yleensä vaihtoehtoisia suoritusmenetelmia, kuten kuviossa 5. Kansalainen voi valita näistä vaihtoehdoista haluamansa menetelmän. VETUMA-asiakas voi määrittää asiakaskonfiguraatiossaan, mitä suoritusmenetelmiä kyseisen asiakkaan asiointisovelluksista tulevissa kutsuissa saa käyttää. Tämän lisäksi asiointisovellus voi rajoittaa konfiguraatiossa määritettyä menetelmävalikoimaa VETUMA-kutsussaan. (Fujitsu Services Oy 2010 a, 6.)

4.1.2 Vaatimukset selaimelle

VETUMA-palvelun käyttäminen asettaa vaatimuksia ja rajoituksia käytettävälle selaimelle. Selaimen on tuettava http-protokollan versiota 1.0 tai 1.1. Selaimen on myös tuettava ja sallittava istuntoevästeiden käyttö, sillä ilman niitä VETUMA-palvelua ei voi käyttää. VETU-

MA-palvelun liikenne tapahtuu https-protokollaa käyttäen, joten selaimen tulee tukea SSL 3.0 –versiota tai TLS 1.0 –versiota ja vähintään 128-bittistä salausta. Lisäksi SSL-salauksen käytön tulee olla sallittua. Näiden vaatimusten lisäksi selaimen olisi hyvä voida luottaa VETUMA-palvelun palvelinvarmenteeseen, jotta palvelun käyttö olisi mahdollisimman joustavaa. VETUMA-palvelun käyttämän palvelinvarmeenteen myöntäjä Thawte on useimmissa selaimissa valmiiksi luotettujen varmentajien joukossa. VETUMA-palvelun tukemat selaimet ovat: a) Internet Explorer 6, b) Internet Explorer 7, c) Firefox 3 ja d) Opera 9. Fujitsu Services Oy (Fujitsu) testaa palvelun toiminnan näiden selainten uudempien versioiden kanssa kahden kuukauden kuluessa uuden version julkistamisesta. VETUMA-palvelu toimii todennäköisesti myös muilla uusia standardeja noudattavilla Internet-selaimilla, mutta Fujitsu ei erikseen testaa muita kuin edellä mainitut selaimet. (Fujitsu Services Oy 2010 a, 7.)

4.2 VETUMA-asiakkaan tiedot palvelun käyttöä varten

Julkishallinnon organisaation liittyessä VETUMA-palvelun asiakkaaksi palveluun muodostetaan asiakaskohtaiset jaetut salaisuudet ja asiakaskonfiguraatio. Jaettuja salaisuuksia käytetään VETUMA-rajapinnan kautta välitettävien viestien suojauksessa. VETUMA-asiakkaalle tehdään oletusarvoisesti kaksi jaettua salaisuutta, toinen tunnistustoimintoja ja toinen maksatustoimintoja varten. VETUMA-asiakas voi tarvittaessa hankkia oman erillisen jaetun salaisuuden jokaiselle asiointisovellukselleen. VETUMA-palvelu säilyttää jaettujen salaisuuksien tunnusten, arvojen ja algoritmien lisäksi kunkin jaetun salaisuuden voimassaoloajan ja tiedon siitä, mitä asiakaskonfiguraatioita saa käyttää tietyn jaetun salaisuuden kanssa. Jaetun salaisuuden tarkoitus on varmistaa rajapintakutsujen ja –vastausten lähettäjän identiteetti sekä kutsujen sisältämän tiedon oikeellisuus. Jaetun salaisuuden luomiseen käytetään satunnaislukugeneraattorilla tehtyä 256-bittistä avainta, joka esitetään heksadesimaalimuodossa. Jaettuun salaisuuteen lisätään myös kyseisen salaisuuden tunnus käsittelyn helpottamiseksi. (Fujitsu Services Oy 2010 a, 9 - 10.)

VETUMA-asiakkaan asiointisovelluksen on muodostettava kaikkiin VETUMA-palveluun lähetettäviin viesteihin turvatarkiste, jota kutsutaan MAC:ksi. Turvatarkiste muodostetaan jaetun salaisuuden arvosta ja tiivisteestä, joka lasketaan VETUMA-palveluun lähetettävän kutsuviestin parametrien arvoista. Turvatarkiste ja asiakkaan jaetun salaisuuden arvo lähetetään palveluun kutsuviestin parametreina. VETUMA-palvelun vastaanotettua kutsuviestin se muodostaa turvatarkisteen arvon vastaavalla tavalla kuin asiakkaan asiointisovellus muodosti

sen kutsua lähetettäessään ja vertaa sitä kutsuviestin mukana tulleeseen turvatarkisteeseen. Jos kutsun mukana tulleen turvatarkisteen ja VETUMA-palvelun laskeman turvatarkisteen arvot eivät ole samat, kutsuviesti hylätään, sillä kutsu on muuttunut matkalla asiointisovelluksesta VETUMA-palveluun. Tiivisteen laskennassa asiointisovellus ja VETUMA-palvelu käyttävät VETUMA-asiakkaan jaetulle salaisuudelle sovittua yksisuuntaista tiivistealgoritmia. Käytettävä tiivistealgoritmi on määritetty palveluun liityttäessä. VETUMA-palvelun lähettäessä vastausviestiä asiakkaan asiointisovellukselle VETUMA-palvelu muodostaa turvatarkisteen samalla tavalla kuin asiointisovellus muodosti lähettäessään kutsuviestiä. Asiointisovelluksen on tarkistettava vastausviesti samoin kuin VETUMA-palvelu tarkistaa kutsuviestit, ja hylättävä vastaus mikäli turvatarkisteet eivät täsmää. (Fujitsu Services Oy 2010 a, 9 - 10.)

Asiakaskonfiguraatio määritetään asiakkaan liittyessä VETUMA-palveluun. Asiakaskonfiguraatiota käytetään mukauttamaan VETUMA-palvelu asiakkaan tarpeiden mukaiseksi. Konfiguraatiotietoja voidaan muuttaa myöhemmin asiakkaan niin halutessa. VETUMA-asiakkaan asiointisovellus välittää tiedon käytettävästä asiakaskonfiguraatiosta VETUMA-kutsussaan. Asiakaskonfiguraatioon määritetään seuraavat tiedot:

- Asiointisovellusten käytettävissä olevat VETUMA-palvelun toimintojen suoritusmenetelmät. VETUMA-asiakas voi esimerkiksi määrittää, että tunnistuksessa voi käyttää ainoastaan TUPAS-tunnistusta. (Fujitsu Services Oy 2010 a, 10.)

- Asiointisovellusten käytettävissä olevat VETUMA-palvelun toimintojen lisäpalvelut (Fujitsu Services Oy 2010 a, 10).

- Tiedot VETUMA-asiakkaan taustapalvelutunnuksista. Taustapalvelutunnuksilla tarkoitetaan niitä tunnuksia ja salasanoja, joita VETUMA-palvelu käyttää kutsuessaa taustapalveluita VETUMA-asiakkaan asiointisovelluksen puolesta. Tällaisia taustapalveluita ovat esimerkiksi pankkien verkkopalvelut, Luottokunnan verkkopalvelu ja Väestörekisterikeskuksen Väestötietojärjestelmän kyselypalvelu. (Fujitsu Services Oy 2010 a, 10 - 11.)

VETUMA-asiakkaan asiointisovellus ei voi kutsussaan laajentaa asiakaskonfiguraatiossa määritettyjä menetelmiä ja palveluita, mutta se voi rajoittaa käyttäjälle tarjottavia. Esimerkiksi, jos asiakaskonfiguraatiossa tunnistusmenetelmiksi on määritetty Tupas-tunnistus ja kansalaisvarmenteeseen perustuva tunnistus, voi asiointisovellus rajoittaa tarjottavat tunnistuspalvelut kutsussaan vain Tupas-tunnistukseen. Tämän vuoksi sovelluskohtaisten toimintovali-

koimien rajoittamiseksi ei tarvita erillistä lisäkonfiguraatiota. VETUMA-palvelun käytössä on kuitenkin tilanteita, jolloin on tarpeen tehdä asiakaskohtaisia lisäkonfiguraatioita peruskonfiguraation lisäksi. Esimerkiksi, jos maksuliikenne halutaan eriyttää VETUMA-asiakkaan eri asiointipalveluiden välillä, tarvitaan erillinen lisäkonfiguraatio. (Fujitsu Services Oy 2010 a, 11.)

VETUMA-asiakas voi halutessaan erotella asiointisovellustensa VETUMA-palvelukutsut. VETUMA-palvelua käyttävälle asiointisovellukselle annetaan VETUMA-kutsussa merkkijonomuotoinen sovellustunnus, joka tallennetaan VETUMA-palveluun yhdessä kutsun muiden tietojen kanssa. Sovellustunnusta ei rekisteröidä VETUMA-palveluun liittymisvaiheessa vaan VETUMA-asiakas voi itse päättää tunnuksen. Sovellustunnus voi olla asiointisovellus- tai asiakaskohtainen. Sovellustunnusta käytetään raportoitaessa VETUMA-palvelun käyttöä. Raporteissa tapahtumat jaotellaan tapahtumatyypin ja sovellustunnuksen mukaan. (Fujitsu Services Oy 2010 a, 12.)

4.3 VETUMA-rajapinta

VETUMA-palvelu liitetään asiointisovellukseen VETUMA-rajapinnan kautta. Kommunikointi asiointisovelluksen ja VETUMA-palvelun välillä tapahtuu kutsu- ja vastausviesteillä. Seuraavissa alaluvuissa kerrottavat asiat koskevat pääsääntöisesti VETUMA-palvelun tunnistus-toimintoa. (Fujitsu Services Oy 2010 b, 3.)

4.3.1 Viestien välitys

VETUMA-palvelu käyttää kaikkien viestien välityksessä http-yhteyskäytännön POST-komentoja. Asiointisovellus kutsuu VETUMA-palvelua lähettämällä käyttäjän selaimen kautta POST-komennon, jossa VETUMA-kutsun parametrit on annettu html-lomakkeella. Kutsussa on aina määritettävä ne osoitteet, joihin VETUMA-palvelu palauttaa vastausviestin eri tilanteissa. Näitä osoitteita on kolme: a) onnistunutta toimintoa varten, b) käyttäjän peruuttamaa toimintoa varten ja c) virhetilannetta varten. Kaikkien näiden osoitteiden täytyy olla https-alkuisia eli niissä on käytettävä suojattua yhteyttä. (Fujitsu Services Oy 2010 b, 3.)

Kaikissa VETUMA-kutsuissa parametrit välitetään html-lomakkeen piilokenttinä, jolloin ne eivät näy käyttäjälle. Seuraavassa esimerkki html-lomakkeesta, jossa on parametreja:

```
”<form name=”VETUMA” method=”POST”  acti-
on=https://tunnistus.suomi.fi/Login/app”>
<input type=”hidden” name=”RCVID” value=”Ankkalinna_S1”>
<input type=”hidden” name=”APPID” value=”Portaali”>
<input type=”hidden” name=”TIMESTMP” value=”20060211...”>
...
</form>” (Fujitsu Services Oy 2010 b, 4.)
```

Yllä olevassa esimerkissä *input*-tyyppiset html-kontrollit on määritetty *hidden*-tyyppisiksi eli piilotetuiksi. Näihin html-kontrolleihin sijoitetaan VETUMA-kutsuissa välitettävät parametrit. Kontrollin ominaisuus *name* kertoo parametrin nimen ja ominaisuus *value* kyseisen parametrin arvon.

VETUMA-palvelun ja VETUMA-asiakkaan asiointisovelluksen välillä liikkuvien viestien eheys ja lähettäjän tunnistaminen varmistetaan viestien turvatarkisteita (MAC) käyttämällä. Tämä tunniste saadaan laskemalla parametrien arvoista ja jaetun salaisuuden arvosta tiiviste. Laskenta suoritetaan käyttämällä jaetun salaisuuden luonnin yhteydessä määritettyä tiivistealgoritmia. VETUMA-palvelu tukee tällä hetkellä seuraavia tiivistealgoritmeja: a) SHA-256, b) SHA-1 (RFC-3174) ja c) MD-5 (RFC-1321). Näistä turvallisin on SHA-256, mutta toisaalta se on hidas. MD-5 puolestaan on nopein, mutta ei niin turvallinen. (Fujitsu Services Oy 2010 b, 4 - 6; Järvinen 2003, 123 - 124.)

4.3.2 Parametrit

Jokaisella VETUMA-palvelun kutsu- ja vastausviestityypillä on useita parametrejä, osa kaikille yhteisiä ja osa vain tiettyyn kutsu- tai vastausviestiin kuuluvia. Parametrien on oltava tietyssä järjestyksessä, jotta VETUMA-palvelu ei hylkää tehtyä kutsua. Jokaiselle parametrille on annettu järjestysnumero, jotta ne on helpompi asettaa oikeaan järjestykseen. Kaikki parametrit eivät kuitenkaan ole pakollisia, vaan ne voidaan tilanteen mukaan jättää pois. Tunnistus- ja maksupalveluiden välillä on lisäksi eroja käytettävissä parametreissä. Kuviossa 6 on esitetty parametrit, jotka esiintyvät kaikissa VETUMA-palvelun kutsuviestityypeissä samalla tavalla riippumatta siitä, onko kyseessä tunnistus- vai maksatuskutsu. (Fujitsu Services Oy 2010 b, 4 - 5.)

Nro	Nimi	Merkitys
1	RCVID	Kutsun suojauksessa käytetyn jaetun salaisuuden tunnus
2	APPID	VETUMA-palvelua kutsuvan asiontisovelluksen tunnus
3	TIMESTMP	Kutsun aikaleima
4	SO	Oletusmenetelmä
5	SOLIST	Käyttäjälle tarjottavat menetelmät
6	TYPE	Käytettävän VETUMA-palvelun tyypin tunnus
7	AU	Kutsussa pyydettävän toiminnon koodi.
9	LG	Käyttöliittymäkieli
10	RETURL	Paluuosoite sovellukseen onnistuneen tapahtuman jälkeen
11	CANURL	Paluuosoite sovellukseen käyttäjän peruman tapahtuman jälkeen
12	ERRURL	Virhepaluuosoite sovellukseen
13	AP	Kutsun palvelemisessa käytettävän konfiguraation tunnus
15	MAC	Kutsun turvatarkiste (MAC)
20	APPNAME	Kutsuvan sovelluksen nimi käyttöliittymää varten
34	TRID	Tapahtumatunnus

Kuvio 6. VETUMA-rajapinnan yleiset kutsuparametrit (Fujitsu Services Oy 2010 b, 7).

Kuviossa 6 esitetyistä parametreistä kahteen on hyvä kiinnittää erityistä huomiota. Numero 6, TYPE, kertoo pyydetyn palvelutyypin. VETUMA-palvelun tarjoamia vaihtoehtoja tälle parametrille ovat LOGIN ja PAYMENT. Parametri numero 7, AU, puolestaan määrittää pyydettävän toiminnon. LOGIN-palvelutyypin toiminnot ja niiden tunnukset ovat: a) tunnistus (EXTAUTH), b) hyväksyminen (CONFIRM) ja c) kiistämätön allekirjoitus (SIGNATURE). PAYMENT-palvelutyypin toiminnot ja niiden tunnukset ovat: a) maksaminen verkkomaksupalvelulla (PAY) ja b) maksunpalautus (RETURN). (Fujitsu Services Oy 2010 b, 10.)

Kaikilla VETUMA-palvelun vastaustyypeillä on myös yhteisiä parametrejä, jotka esiintyvät jokaisessa vastausviestityypissä samalla tavalla. Nämä yhteiset parametrit esitetään kuviossa 7 lyhyiden selitysten kera. (Fujitsu Services Oy 2010 b, 14.)

Nro	Nimi	Merkitys
1	RCVID	Vastauksen suojauksessa käytetyn jaetun salaisuuden tunnus
3	TIMESTMP	Vastauksen aikaleima
4	SO	Käytetty menetelmä
9	LG	Käytetty käyttöliittymäkieli.
10	RETURL	Paluuosoite sovellukseen onnistuneen tapahtuman jälkeen
11	CANURL	Paluuosoite sovellukseen käyttäjän peruman tapahtuman jälkeen
12	ERRURL	Virhepaluuosoite sovellukseen
15	MAC	Vastauksen turvatarkiste (MAC)
29	STATUS	Tieto toiminnon suorittamisesta tai suorittamatta jättämisestä.
34	TRID	Tapahtumatunnus.

Kuvio 7. VETUMA-rajapinnan yleiset vastausparametrit (Fujitsu Services Oy 2010 b, 14).

On hyvä huomata, että kaikissa kutsu- ja vastausviesteissä välitetään turvatarkiste (MAC), jota käytetään viestien eheyden varmistamiseen. Myös aikaleima (TIMESTMP) löytyy kaikista kutsu- ja vastausviesteistä.

4.4 VETUMA Toolkit

VETUMA Toolkit on Fujitsu Services Oy:n toteuttama moottori VETUMA-palvelun käyttöön. Toolkitin .Net-versio on luokkakirjasto, joka sijoittuu VETUMA-asiakkaan asiointisovelluksen ja VETUMA-palvelun väliin. VETUMA Toolkit tarkistaa muun muassa VETUMA-palvelusta palautuvien viestien MAC-tunnisteet. Toolkitin avulla asiointisovellus saa tiedon paluuviestin oikeellisuudesta suoraan boolean-tyyppisenä tietona eli kyllä/ei-muodossa eikä sen tarvitse itse muodostaa näitä tunnisteita. Liitteissä 1 ja 2 on koodiesimerkit Vetuma Toolkitin käytöstä Asp.Net-sovelluksessa C#-ohjelmointikielellä toteutettuna. (Fujitsu Services Oy 2007, 2 - 3.)

5 VETUMA-PALVELUN LOGIN-PALVELUTYYPPI

Tässä luvussa tutustutaan VETUMA-palvelun LOGIN-palvelutyyppin. LOGIN-palvelutyyppi sisältää käyttäjän tunnistamisen, käyttäjän suorittaman hyväksymisen ja käyttäjän suorittaman kiistämättömän sähköisen allekirjoituksen (Fujitsu Services Oy 2010 a, 12).

5.1 Käyttäjän tunnistaminen

VETUMA-palvelun käyttäjän tunnistustoiminto tarkoittaa, että VETUMA-palvelu tunnistaa VETUMA-asiakkaan asiointisovellusta käyttävän käyttäjän sovelluksen puolesta. VETUMA-palvelun tukemia tunnistusmenetelmiä ovat salasanatunnistus, kansalaisvarmennetunnistus ja Tupas-tunnistus. (Fujitsu Services Oy 2010 a, 13 - 15.)

Salasanatunnistus

VETUMA-palvelu tukee salasanatunnistamista selaimeen syötettävillä käyttäjätunnuksella ja salasanalla sekä numeerisella tunnistuskoodilla tapahtuvaa salasanatunnistusta, jossa VETUMA-palvelu kysyy tunnistuskoodia matkapuhelimeen tehtävällä puhelinsoitolla. Salasanaperusteista käyttäjätunnistusta käytettäessä VETUMA-asiakkaalla tulee olla VETUMA-palvelussa ylläpidetty oma käyttäjärekisteri. Kyseiseen käyttäjärekisteriin tallennetaan perustietona jokaisen käyttäjän henkilötunnus ja nimitieto. Näiden tietojen lisäksi rekisteriin tallennetaan tunnistustapaan sidottuja tietoja, kuten käyttäjätunnus tai puhelinnumero. (Fujitsu Services Oy 2010 a, 13.)

Selaimessa tapahtuva käyttäjätunnus-salasana -tunnistus alkaa käyttäjän suorittamalla tunnistustavan valinnalla VETUMA-palvelun tunnistustavan valintasivulla. Käyttäjän valittua tunnistustavaksi käyttäjätunnus-salasana -tunnistuksen, hän syöttää tunnistuskäyttöliittymään oman käyttäjätunnuksen ja salasanan. Tämän jälkeen VETUMA-palvelu tarkistaa käyttäjätunnus-salasanaparin vastaavuuden käyttäjärekisteristä. Tarkistus tehdään sen VETUMA-asiakkaan käyttäjärekisteristä, jonka asiointisovellus pyysi tunnistusta. Käyttäjällä on viisi yritystä käyttäjätunnuksen ja salasanan syöttämiseksi. Tunnistuksen onnistuessa VETUMA-palvelu palauttaa VETUMA-asiakkaan asiointisovellukselle käyttäjän perustiedot sekä käyttäjän käyttäjätunnuksen. Viiden epäonnistuneen yrityksen jälkeen VETUMA-palvelu palauttaa

VETUMA-asiakkaan asiointisovelluksen määrittämään ERRURL-osoitteeseen REJECTED-tilatiedon tunnistuksen epäonnistumisesta. Lisäksi VETUMA-asiakkaan asiointisovellusta käyttävän käyttäjän käyttäjätunnus lukkiutuu eikä sitä voida käyttää käyttäjätunnus-salasana -tunnistukseen ennen kuin lukitus on poistettu. Lukituksen voi poistaa VETUMA-asiakkaan pääkäyttäjä. (Fujitsu Services Oy 2010 a, 13.)

Matkapuhelimella tapahtuvaan, numeerisen tunnistuskoodin kyselyyn perustuva tunnistus alkaa käyttäjän valitessa kyseisen tavan tunnistustavakseen VETUMA-palvelun tunnistustavan valintasivulla. Tämän jälkeen käyttäjän on syötettävä se puhelinnumero, joka hänelle on rekisteröity puhelintunnistusta varten VETUMA-palveluun. Syötettyään puhelinnumeron käyttäjä määrää tunnistuksen jatkumaan seuraavaan vaiheeseen, jossa VETUMA-palvelu soittaa käyttäjän antamaan numeroon ja pyytää häneltä tunnistuskoodia. Käyttäjä näppäilee puhelimeen oman tunnistuskoodinsa, minkä jälkeen VETUMA-palvelu tarkistaa koodin vastaavuuden puhelinnumerolle rekisteröityyn koodiin. Tarkistus tehdään sen VETUMA-asiakkaan käyttäjärekisteristä, jonka asiointisovellus pyysi tunnistusta. Tarkistuksen jälkeen VETUMA-palvelu ilmoittaa käyttäjälle puhelimessa, onnistuiko tunnistus. Käyttäjällä on viisi yritystä tunnuksen syöttämiseksi. Tunnistuksen onnistuessa VETUMA-palvelu palauttaa VETUMA-asiakkaan asiointisovellukselle käyttäjän perustiedot ja käyttäjän puhelintunnistuksessa käytetyn puhelinnumeron. Viiden epäonnistuneen yrityksen jälkeen VETUMA-palvelu palauttaa VETUMA-asiakkaan asiointisovelluksen määrittämään ERRURL-osoitteeseen REJECTED-tilatiedon tunnistuksen epäonnistumisesta. Lisäksi VETUMA-asiakkaan asiointisovellusta käyttävän käyttäjän käyttäjätunnus lukkiutuu eikä sitä voida käyttää puhelutunnistukseen ennen kuin lukitus on poistettu. Lukituksen voi poistaa VETUMA-asiakkaan pääkäyttäjä. (Fujitsu Services Oy 2010 a, 13 - 14.)

Kansalaisvarmennetunnistus

VETUMA-palvelu tukee kansalaisvarmennetunnistusta sirukortille tallennetulla kansalaisvarmenteella ja mobiililaitteen SIM-kortille tallennetulla kansalaisvarmenteella. VETUMA-palvelu palauttaa kansalaisvarmenteen sisältämät SATUn ja käyttäjän nimitiedot VETUMA-asiakkaan asiointisovellukselle aina riippumatta siitä, minkä kansalaisvarmenteeseen perustuvan tunnistusmenetelmän käyttäjä valitsi. Kansalaisvarmenteeseen perustuvassa tunnistuksessa ei käytetä käyttäjärekisteriä. (Fujitsu Services Oy 2010 a, 14.)

Sirukortilla sijaitsevaan kansalaisvarmenteeseen perustuva tunnistus alkaa käyttäjän valitessa kyseisen tavan tunnistustavakseen VETUMA-palvelun tunnistustavan valintasivulla. Tämän jälkeen VETUMA-palvelu pyytää käyttäjää laittamaan sirukorttinsa kortinlukijaan ja lähettää tunnistuspyynnön käyttäjän selaimelle. Selain aktivoi työasemassa olevan sirukorttiohjelmiston lukemaan käyttäjän tiedot sirukortilta. Sen jälkeen sirukorttiohjelmisto pyytää käyttäjältä tunnistusta varten tarkoitetun PIN-koodin (PIN1). Sirukorttiohjelmiston todettua PIN-koodin oikeaksi, ohjelmisto suorittaa käyttäjän tunnistamisen. Tieto tunnistuksen onnistumisesta, ja onnistuneen tunnistuksen yhteydessä myös käyttäjän tiedot, välitetään käyttäjän selaimen kautta VETUMA-palveluun. Tunnistuksen onnistuessa VETUMA-palvelu palauttaa VETUMA-asiakkaan asiointisovellukselle käyttäjän varmeessa olleet tiedot, SATUn ja nimitiedot, sekä Väestötietojärjestelmästä haetut tiedot, jos asiointisovellus on niitä pyytänyt. Mikäli tunnistus epäonnistuu, VETUMA-palvelu palauttaa VETUMA-asiakkaan asiointisovelluksen kutsussa määritettyyn ERRURL-osoitteeseen REJECTED-tilatiedon tunnistuksen epäonnistumisesta. (Fujitsu Services Oy 2010 a, 14.)

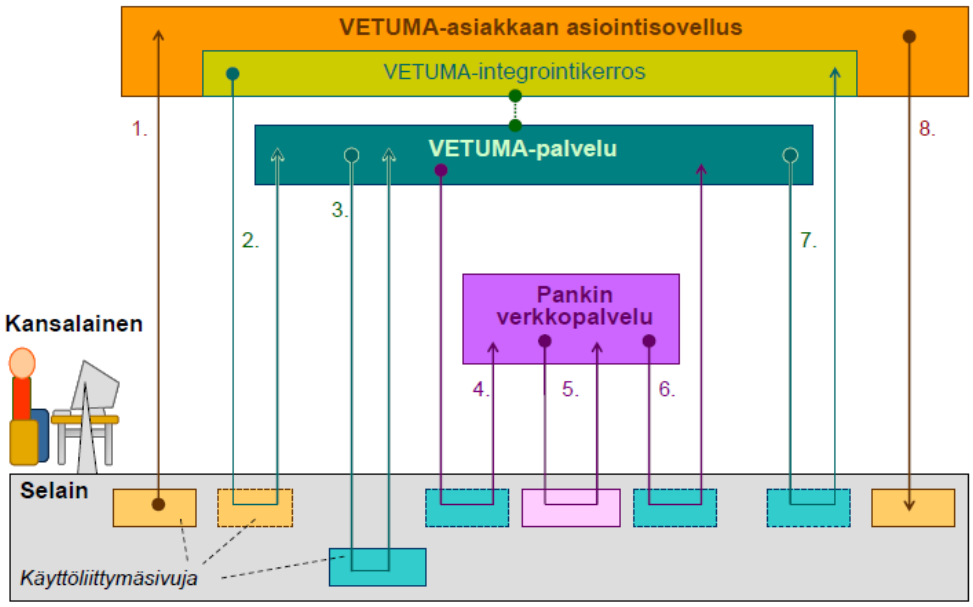
SIM-kortilla sijaitsevaan kansalaisvarmenteeseen perustuva tunnistus alkaa käyttäjän valitessa kyseisen tavan tunnistustavakseen VETUMA-palvelun tunnistustavan valintasivulla. Tämän jälkeen käyttäjää pyydetään syöttämään sen SIM-kortin puhelinnumero, mihin hänen kansalaisvarmenteensa on tallennettu. Käyttäjän syötettyä puhelinnumeron, VETUMA-palvelu lähettää siihen tunnistuspyynnön matkapuhelinoperaattorin välityksellä. Mobiililaitteen varusohjelmisto pyytää käyttäjää syöttämään tunnistusta varten tarkoitetun SPIN-koodin. Varusohjelmiston todettua SPIN-koodin oikeaksi, ohjelmisto suorittaa käyttäjän tunnistamisen. Tieto tunnistuksen onnistumisesta, ja onnistuneen tunnistuksen yhteydessä myös käyttäjän tiedot, välitetään matkapuhelinoperaattorin kautta VETUMA-palveluun. Tunnistuksen onnistuessa VETUMA-palvelu palauttaa VETUMA-asiakkaan asiointisovellukselle käyttäjän varmeessa olleet tiedot, SATUn ja nimitiedot, sekä Väestötietojärjestelmästä haetut tiedot, jos asiointisovellus on niitä pyytänyt. Mikäli tunnistus epäonnistuu, VETUMA-palvelu palauttaa VETUMA-asiakkaan asiointisovelluksen määrittämään ERRURL-osoitteeseen REJECTED-tilatiedon tunnistuksen epäonnistumisesta. (Fujitsu Services Oy 2010 a, 15.)

Mobiililiikenne on altis haittakäytölle ja sen vuoksi mobiilikansalaisvarmennetunnistuksessa voidaan käyttää FiCom:n suosittelemia estomekanismeja, joita ovat istuntotunnus ja käyttäjäkohtainen häirinnän estokoodi. Istustotunnus tarkoittaa, että VETUMA-palvelu luo käyttäjälle istuntotunnuksen sovelluksen puolestaja ja se näytetään käyttäjälle mobiilikansalaisvarmennetunnistuksen käyttöliittymässä. Käyttäjäkohtainen häirinnän estokoodi puolestaan tar-

koittaa, että käyttäjä voi sopia estokoodin käytöstä oman operaattorinsa kanssa. Käyttäjän käyttäessä häirinnän estokoodia, hän antaa kyseisen koodin VETUMA-palvelun tunnistussivulla oman puhelinnumeronsa lisäksi. Estokoodi välittyy mobiililaitteeseen operaattorin kautta tunnistuskutsun yhteydessä. (Fujitsu Services Oy 2010 a, 15.)

Tupas-tunnistus

Käyttäjän valitessa Tupas-tunnistuksen, VETUMA-palvelu välittää tunnistuspyynnön käyttäjän valitseman pankin verkkopalvelulle käyttämällä Tupas-rajapintaa. VETUMA-palvelun saatua tunnistusvastauksen pankin verkkopalvelulta, VETUMA-palvelu palauttaa VETUMA-asiakkaan asiointisovellukselle käyttäjän nimitiedot ja henkilötunnuksen. VETUMA-palvelu edellyttää Tupas-tunnistuksen yhteydessä, että käyttäjän tunniste on nimenomaan henkilötunnus. Tämän vuoksi VETUMA-asiakkaiden ja pankkien välisissä verkkopalvelusopimuksissa tulee määrittää palautettavaksi tunnistetiedoksi Tupas-määrittelyn mukainen ”Selväkielinen perustunnus”. Tupas-tunnistuksessa ei tarvita VETUMA-käyttäjärekisteriä. Kuviossa 8 on esitetty esimerkkinä Tupas-tunnistuksen eteneminen. (Fujitsu Services Oy 2010 a, 15.)



Kuvio 8. VETUMA-palvelun Tupas-tunnistuksen kulku (Fujitsu Services Oy 2010 a, 17).

1. VETUMA-asiakkaan asiointisovellusta käyttävä kansalainen pyytää sellaista toimintoa, joka vaatii käyttäjän tunnistamista (Fujitsu Services Oy 2010 a, 18).

2. Asiointisovellus varmistaa, että yhteys käyttäjän selaimeen on SSL/TLS-suojattu. Sovellus muodostaa VETUMA-tunnistuskutsun ja toimittaa sen käyttäjän selaimen kautta VETUMA-palvelulle. (Fujitsu Services Oy 2010 a, 18.)

3. VETUMA-palvelu tarkistaa kutsun oikeellisuuden. Mikäli kutsu on kelvollinen, VETUMA-palvelu avaa oman käyttöliittymänsä käyttäjän selaimeen HTTPS-yhteyttä käyttäen ja tarjoaa käyttäjän valittavaksi tunnistautumismenetelmän. (Fujitsu Services Oy 2010 a, 18.)

4. Käyttäjä valitsee tunnistautumismenetelmäksi pankkitunnistuksen (Tupas), minkä jälkeen VETUMA-palvelu muodostaa Tupas-kutsun ja toimittaa sen käyttäjän selaimen kautta käyttäjän valitseman pankin verkkopalvelulle (Fujitsu Services Oy 2010 a, 18).

5. Käyttäjän valitseman pankin verkkopalvelu suorittaa käyttäjän tunnistuksen oman HTTPS-suojatun käyttöliittymänsä kautta (Fujitsu Services Oy 2010 a, 18).

6. Käyttäjän valitseman pankin verkkopalvelu muodostaa Tupas-vastauksen ja toimittaa sen käyttäjän selaimen kautta HTTPS-yhteyttä käyttäen VETUMA-palvelulle (Fujitsu Services Oy 2010 a, 18).

7. Kun käyttäjä on tunnistautunut, VETUMA-palvelu muodostaa VETUMA-tunnistusvastauksen ja toimittaa sen käyttäjän selaimen kautta asiointisovellukselle. Vastaus toimitetaan käyttäjän selaimelle VETUMA-palvelun käyttöliittymän tunnistuspaluu-sivulla, jolta se lähtee asiointisovellukselle, kun käyttäjä on hyväksynyt paluun asiointisovellukseen. (Fujitsu Services Oy 2010 a, 18.)

8. Asiointisovellus tarkistaa vastauksen ja jatkaa toimintaansa oman sovelluslogiikkansa mukaan (Fujitsu Services Oy 2010 a, 18).

Perustietojen hakeminen Väestötietojärjestelmästä

VETUMA-asiakkaan asiontisovellus voi pyytää VETUMA-palvelua noutamaan Väestötietojärjestelmästä tietoja VETUMA-palvelussa tunnistetusta käyttäjästä. Tietojen haku Väestötietojärjestelmä edellyttää, että käyttäjä on tunnistettu riittävän vahvalla tunnistusmenetelmällä. Näitä menetelmiä ovat tällä hetkellä kansalaisvarmenteeseen perustuvat tunnistustavat ja pankkien Tupas-tunnistus. Lisäksi VETUMA-asiakkaalla täytyy olla tietolupa Väestötietojärjestelmästä haettavalle tietojoukolle. Väestötietojärjestelmästä noudettavissa olevat tietojoukot (Väestörekisterikeskuksen terminologiassa Tuotteet) riippuvat VETUMA-asiakkaan Väestörekisterikeskukselta saamista tietoluvista. Kaikille VETUMA-asiakkaille tarjolla oleva vakiokyselytuote sisältää seuraavat tiedot käyttäjästä:

- henkilötunnus
- nimitiedot
- kotikunta
- osoitetiedot
- äidinkieli
- mahdollinen kuolinaika
- onko käyttäjä Suomen kansalainen. (Fujitsu Services Oy 2010 a, 16 - 17.)

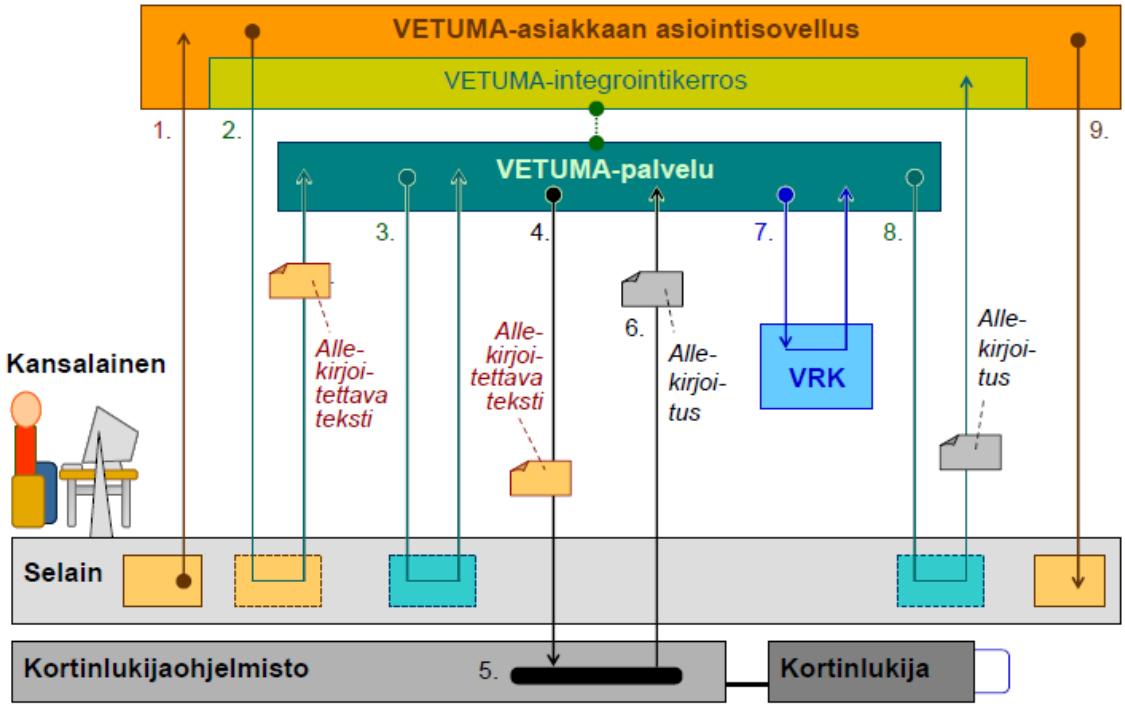
VETUMA-asiakkaan asiointisovellus voi pyytää Väestötietojärjestelmästä myös laajennettua kyselyä, jolla saatavat tiedot on määritetty Väestörekisterikeskuksen myöntämässä tietoluvassa (Fujitsu Services Oy 2010 a, 16).

5.2 Käyttäjän suorittama hyväksyminen

Hyväksymis-toiminto VETUMA-palvelussa tarkoittaa, että VETUMA-asiakkaan asiointisovellus pyytää aiemmin saman istunnon aikana tunnistettua käyttäjää hyväksymään tunnistautumalla sellaisen asiointitoiminnon, joka vaatii hyväksynnän aiemman tunnistuksen lisäksi. Hyväksyminen tapahtuu käytännössä siten, että VETUMA-asiakkaan asiointisovellus lähettää käyttäjän tunnuksen VETUMA-palvelulle ja pyytää palvelua varmistamaan, että käyttäjä on edelleen sama kuin aikaisemmassa tunnistuksessa. Asiointisovellus vastaa hyväksymistiedon pysyvästä tallennuksesta. Hyväksymis-toiminnolla ei ole lain kannalta vastaavaa sitovuutta kuin kiistämättömällä sähköisellä allekirjoituksella. (Fujitsu Services Oy 2010 a, 18.)

5.3 Käyttäjän suorittama kiistämätön sähköinen allekirjoitus

Kiistämätön sähköinen allekirjoitus tarkoittaa, että VETUMA-asiakkaan asiointisovelluksen käyttäjä allekirjoittaa sovelluksen antaman tekstin kansalaisvarmenteeseensa liittyvällä salaisella avaimella. Asiointisovelluksen on muotoiltava allekirjoitettava teksti siten, että käyttäjä ymmärtää, mihin hän sitoutuu allekirjoittamalla sen. Lisäksi tekstin on kuvattava aukottomasti, mihin sen allekirjoittaminen sitoo. VETUMA-palvelu tukee allekirjoitusta sirukortille tallennetulla kansalaisvarmenteella ja mobiililaitteen SIM-kortille tallennetulla kansalaisvarmenteella. Allekirjoituksen onnistuessa VETUMA-palvelu tarkistaa vielä allekirjoituksen oikeellisuuden, mm. tarkistamalla varmenteen voimassaolon Väestörekisterikeskuksen sulkulistalta. Vaikka allekirjoitus epäonnistuu, VETUMA-palvelu palauttaa allekirjoituksen asiointisovellukselle, mukanaan tilatieto tarkistuksen epäonnistumisesta. VETUMA-asiakkaan asiointisovelluksen vastuulla on tallentaa syntynyt kiistämätön sähköinen allekirjoitus mahdollista myöhempää tarvetta varten, koska VETUMA-palvelu ei tallenna tietoja sen kautta suoritetuista allekirjoituksista. Kuviossa 9 kuvataan VETUMA-palvelun avulla tehtävän kiistämättömän sähköisen allekirjoituksen kulku. (Fujitsu Services Oy 2010 a, 18 - 19.)



Kuvio 9. Kiistämättömän sähköisen allekirjoituksen kulku (Fujitsu Services Oy 2010 a, 20).

1. VETUMA-asiakkaan asiointisovellusta selaimellaan käyttävä kansalainen pyytää sellaista toimintoa, johon liittyvää sitouttamista varten tarvitaan kiistämätön sähköinen allekirjoitus (Fujitsu Services Oy 2010 a, 20).

2. Asiointisovellus varmistaa, että yhteys käyttäjän selaimeen on SSL/TLS-suojattu. Sen jälkeen asiointisovellus muodostaa VETUMA-allekirjoituskutsun, johon sisältyy allekirjoitettava teksti, ja toimittaa kutsun käyttäjän selaimen kautta VETUMA-palvelulle. (Fujitsu Services Oy 2010 a, 20.)

3. VETUMA-palvelu tarkistaa kutsun oikeellisuuden. Mikäli kutsu on kelvollinen, palvelu avaa käyttöliittymänsä käyttäjän selaimeen HTTPS-yhteyttä käyttäen ja pyytää käyttäjää käynnistämään allekirjoittamisen. (Fujitsu Services Oy 2010 a, 20.)

4. Kun käyttäjä on käynnistänyt allekirjoittamisen, VETUMA-palvelu palauttaa käyttäjän selaimelle HTTPS-yhteyttä käyttäen HTTP-vastauksen, joka sisältää allekirjoitettavan tekstin ja aktivoi työaseman selaimeen kytketyn allekirjoituskomponentin (Fujitsu Services Oy 2010 a, 20).

5. Selaimeen kytketty allekirjoituskomponentti pyytää käyttäjää syöttämään allekirjoituksessa tarvittavan PIN-koodin (PIN2), minkä jälkeen allekirjoituskomponentti suorittaa allekirjoituksen (Fujitsu Services Oy 2010 a, 20).

6. Allekirjoitus toimitetaan käyttäjän työasemasta selaimen välityksellä VETUMA-palvelulle (Fujitsu Services Oy 2010 a, 20).

7. VETUMA-palvelu vastaanottaa allekirjoituksen käyttäjän työaseman allekirjoituskomponentilta ja tarkistaa Väestörekisterikeskukselta, että allekirjoituksessa käytetyt varmenteet ovat voimassa (Fujitsu Services Oy 2010 a, 21).

8. VETUMA-palvelu muodostaa VETUMA-allekirjoitusvastauksen ja toimittaa sen käyttäjän selaimen kautta HTTPS-yhteyden välityksellä VETUMA-asiakkaan asiointisovellukselle (Fujitsu Services Oy 2010 a, 21).

9. VETUMA-asiakkaan asiointisovellus tarkistaa vastauksen oikeellisuuden, tallettaa saamansa allekirjoituksen ja jatkaa toimintaansa (Fujitsu Services Oy 2010 a, 21).

6 VETUMA-PALVELUA HYÖDYNTÄVÄ REKISTERÖITYMISRATKAISU

VETUMA-palvelua hyödyntävä rekisteröitymisratkaisu, Vetuma for SharePoint, on rekisteröitymissovellus SharePoint 2007 ja 2010 alustoille. Ratkaisu toteutettiin Asp.Net ohjelmointimenetelmällä käyttämällä C#-ohjelmointikieltä. Kehitystyökaluna ratkaisun tekemisessä käytettiin Visual Studio 2008 ja Visual Studio 2010 -ohjelmia. Ratkaisussa hyödynnettiin Vetuma Toolkit –luokkakirjastoa, minkä avulla VETUMA-palvelu saatiin helposti liitettyä osaksi ratkaisua.

6.1 Ratkaisun määrittely

Documentan yhteistyökumppani esitti toiveen avoimen lähdekoodin ratkaisusta, jonka tulisi tarjota SharePoint-ympäristöön VETUMA-palvelua hyödyntävä rekisteröitymistoiminto. VETUMA-palvelun hyödyntäminen oli vaatimuksena ratkaisun toteutuksessa, koska haluttiin tehdä ratkaisu nimenomaan julkishallinnon käyttöön ja VETUMA-palvelu on toteutettu juuri julkishallinnon verkkopalveluita varten. Ratkaisun avulla käyttäjän on pystyttävä rekisteröitymään ja autentikoitumaan SharePoint-ympäristössä olevan verkkopalvelun käyttäjäksi. Rekisteröitymis- ja autentikoitumistoiminnot edellyttävät käyttäjän tunnistautumista VETUMA-palvelussa verkkopankkitunnuksilla. Ratkaisua määriteltäessä teknisiksi vaatimuksiksi todettiin seuraavat asiat:

- toimittava SharePoint 2007 ja 2010 alustoilla
- käytettävä lomakkeet-autentikointi (Forms Based Authentication, FBA) ja toimittava SharePoint 2010 väitteisiin pohjautuvan autentikoinnin (Claims Based Authentication) kanssa
- käyttäjätiedot tallennettava joko Sql Server -tietokantaan tai Active Directoryyn
- VETUMA-tunnistus rekisteröitymisen ja unohtuneen salasanan korvaamisen yhteydessä
- tuettava autentikointia VETUMA-tunnistusta hyödyntäen
- kirjautumissivulta pääsy rekisteröitymään

- rekisteröitymisen yhteydessä käyttäjästä tallennettava käyttäjätunnus, salasana, etunimi, sukunimi ja henkilöturvatunnus

- web.config-osio, jossa määritetään VETUMA-palvelun tarvitsemat tiedot sekä roolit, joihin rekisteröityvä käyttäjä liitetään

- koodin kommentointi englanniksi

- asennus wsp-paketin avulla

- suomenkielinen asennusohjeistus.

Projektin työmääräarvio oli 11 henkilötyöpäivää (htp). Se suunniteltiin toteutettavan 26.4.2010 ja 11.6.2010 välisenä aikana. Kuviosta 10 on nähtävillä projektin tarkempi aikataulutus sekä työmääräarviot.

TEHTÄVÄ	**KESTO htp**	**AIKA**
Projektin aloitus		26.4.2010
Vetuma-palvelun dokumentaatioon tutustuminen	1	26.4. – 28.5.2010
Kehitys:		
SharePoint-kehitysympäristön konfigurointi	0,5	
Rekisteröintitoiminnallisuuden kehitys (FBA)	2	
Rekisteröintitoiminnallisuuden laajennus (AD)	2	
Autentikointitoiminnallisuuden kehitys	2	
Salasanan vaihto -toiminnallisuuden kehitys	1	
Asennuspaketin tekeminen	0,5	
Kehitystyö yhteensä	8	26.4. – 4.6.2010
Testaus ja mahdolliset korjaukset	1	17.5. – 4.6.2010
Dokumentointi	1	31.5. – 9.6.2010
Projektin päättäminen		11.6.2010
Työmääräarvio yhteensä	11	26.4.2010 – 11.6.2010

Kuvio 10. Rekisteröitymisratkaisu SharePoint alustalle -projektin aikataulu ja työmääräarviot.

SharePoint on Microsoftin palvelinohjelmisto, joka on rakennettu Microsoftin omilla tekniikoilla; Sql Serveriä käytetään tietokantaohjelmistona ja itse SharePoint-sovellus on toteutettu Asp.Net-tekniikalla (Roine 2007, 15, 21). Asp.Net tekniikkana mahdollistaa dynaamisen sivuston luonnin sekä erilaisten teemojen ja ulkoasujen käytön sivustoissa.

SharePoint Foundation on Windows Server 2008 palvelinlisenssin mukana tuleva ilmainen ja kevyempi versio SharePointista. Nimi SharePoint Foundation tuli uuden 2010 version myö-

tä, aiemmin ilmaisversio tunnettiin nimellä Windows SharePoint Services (WSS). Vuonna 2007 julkaistu WSS 3.0 on edelleen saatavilla Windows Server 2003 ja 2008 palvelimille. Ilmaisen version lisäksi SharePointista on saatavilla maksullinen SharePoint Server, minkä runkona käytetään SharePoint Foundationia. SharePoint Server nimi tuli toukokuussa julkaistun 2010 version myötä. Aiemmin maksullinen versio tunnettiin nimellä Microsoft Office SharePoint Server (MOSS) 2007. SharePoint Server 2010:stä on tarjolla Standard ja Enterprise -versiot. SharePointin 2010 versiot vaativat 64-bittisen ympäristön. (Microsoft 2010.)

SharePointin tarkoituksena on tehdä ihmisten työnteosta ja yhteistyöstä helpompaa sekä toisaalta tarjota helppo tapa jakaa tietoa. SharePoint Foundation on tarkoitettu yritysten, yhteisöjen ja muiden vastaavien ryhmien yhteistyön tehostamiseen sekä keskitettyyn sisällön hallintaan. SharePoint Serveriä puolestaan voidaan käyttää edellä mainittujen lisäksi mm. Internet-sivustojen, esimerkiksi kunnan sähköisen asiointipalvelun, alustana. SharePointissa on eri käyttötarkoituksiin useita eri sivustomalleja; sivustot voivat keskittyä esimerkiksi dokumenttienhallintaan, kokoushallintaan, julkaisuun tai toimia tiedon jakamiseen tarkoitettuna wikisivustona. SharePointin rakenne on hierarkinen, esimerkiksi sivustolla voi olla useita alisivustoja ja niillä useita alisivustoja jne. SharePointia käytetään myös alustana erilaisille sovelluksille, koska siinä on valmiit integraatiot Microsoftin muihin tuotteisiin, erityisesti Officeen ja sen oliomalli on avoin. (Microsoft 2010; Roine 2007, 15, 21, 117 - 125.)

6.2 Ratkaisu

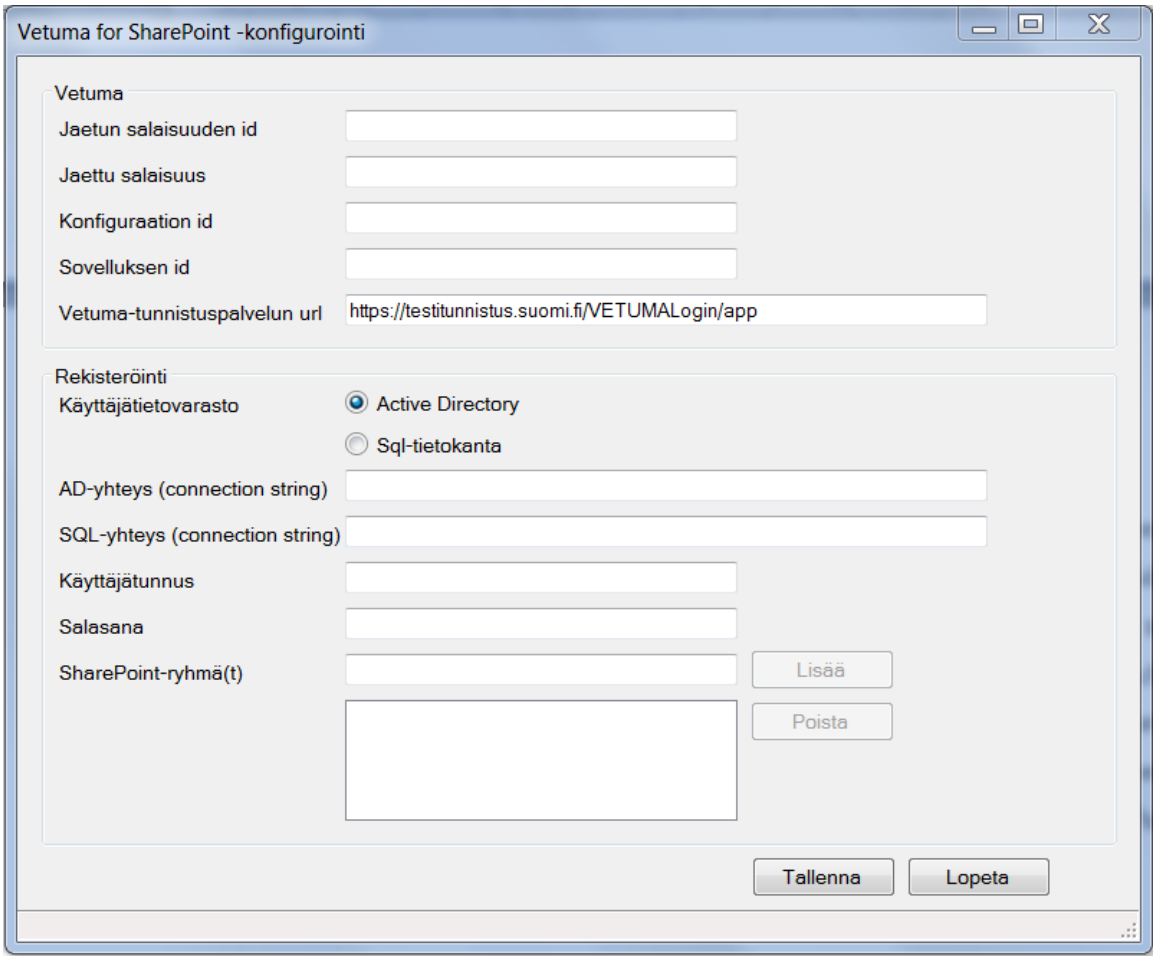
Vetuma for SharePoint –ratkaisua suunniteltaessa tavoitteena oli tehdä yksinkertainen, VETUMA-palvelua hyödyntävä rekisteröitymissovellus SharePoint-alustalle. Ratkaisun avulla organisaatiot voivat tarjota SharePoint-alustalla toimivaan palveluun rekisteröitymistoiminnallisuuden ilman, että heidän tarvitsee itse tutustua VETUMA-palvelun rajapintaan ja VETUMA Toolkitiin. Riittää, että organisaatio on liittynyt VETUMA-palvelun asiakkaaksi ja solminut sopimukset pankkien kanssa käyttäjien Tupas-tunnistamista varten. Ratkaisu koostuu kolmesta aspx-sivusta, kahdesta resurssi- eli kielitiedostosta (.resx) ja kahdesta sovelluslaajennuksesta eli luokkakirjastosta (.dll).

Ratkaisussa käytetään Asp.Netin lomakkeet-autentikointia. Lomakkeet-autentikoinnissa käyttäjän kirjautuessa käyttäjälle luodaan autentikointilippu (Authentication Ticket), joka tallennetaan evästeeseen selaimessa (Microsoft 2005). Jos käyttäjän selain ei salli evästeiden käyt-

töä, voidaan autentikointilippu lisätä query stringiin (Microsoft 2005). Lomakkeet-autentikoinnin käyttäjätunnusten ja salasanojen tietokantana voidaan käyttää joko Active Directoryä, Sql-tietokantaa tai esimerkiksi xml-tiedostoa. Sql-tietokantaan tallennettaessa ratkaisussa hyödynnetään Asp.Net 2.0:n mukana tulevaa Asp.Net-käyttäjätietokantaa, joka on suunniteltu web-sovellusten käyttäjien käyttäjätunnusten ja salasanojen tallentamista varten. Asp.Net-tietokanta sisältää myös profiilitietojen ja roolien hallinnan, mutta niitä ei käytetä Vetuma for SharePoint –ratkaisun yhteydessä. Sovelluksen yhdistämisessä valittuun käyttäjätietokantaan hyödynnetään Asp.Net 2.0:n mukana tulevia SqlMembershipProvideria ja ActiveDirectoryMembershipProvideria. SqlMembershipProvideria käytetään, kun käyttäjätietovarastona on Asp.Netin Sql-käyttäjätietokanta. Vastaavasti ActiveDirectoryMembershipProvideria käytetään, kun käyttäjätietovarastona on Active Directory. Membership provider on jäsenyyden tarjoaja, joka tarjoaa sovellukselle rajapinnan käyttäjätietovarastoon. Jäsenyyden tarjoajalla on useita ominaisuuksia sekä metodeja, joita käytetään tietojen palauttamiseen ja tietojen lisäämiseen/muuttamiseen käyttäjätietokannassa. Tällaisia metodeja ovat mm. GetAllUsers, CreateUser ja UpdateUser. Sovelluskehittäjä voi myös luoda täysin oman jäsenyyden tarjoajan.

Toteutetun ratkaisun avulla käyttäjä voi rekisteröityä käyttäjäksi SharePoint-ympäristöön, korvata unohtuneen salasanan uudella ja kirjautua SharePoint-ympäristöön VETUMA-palvelun avulla. Käyttäjältä kysytään rekisteröitymisen yhteydessä sähköpostiosoite sekä käyttäjän valitsemat käyttäjätunnus ja salasana. Nimitiedot ja henkilötunnus saadaan VETUMA-palvelusta, joten käyttäjän ei tarvitse syöttää niitä. Käyttäjän henkilötunnus ja salasana ovat arkaluonteista tietoja ja sen vuoksi ne tallennetaan salattuna, muut tiedot selväkielisenä tekstinä. Ratkaisun avulla käyttäjä voi myös kirjautua SharePoint-ympäristöön ilman, että hänen tarvitsee rekisteröityä tai jo rekisteröityneen käyttäjän syöttää käyttäjätunnusta ja salasanaa. Jos käyttäjä on rekisteröitynyt aikaisemmin, käyttäjä ohjautuu VETUMA-palvelusta suoraan SharePoint-sivustolle. Mikäli käyttäjä ei ole aikaisemmin rekisteröitynyt ympäristön käyttäjäksi, häneltä kysytään ensimmäisellä kerralla VETUMA-palvelun avulla kirjauduttaessa ainoastaan sähköpostiosoite. Käyttäjän syötettyä sähköpostiosoitteensa, hänelle luodaan automaattisesti etunimi.sukunimi-muotoinen käyttäjätunnus ja generoidaan salasana. Käyttäjätunnus ja salasana tallennetaan valittuun käyttäjätietokantaan, minkä jälkeen käyttäjä ohjataan SharePoint-sivustolle. Seuraavilla kerroilla VETUMA-palvelun avulla kirjauduttaessa käyttäjä ohjautuu VETUMA-palvelusta suoraan SharePoint-sivustolle.

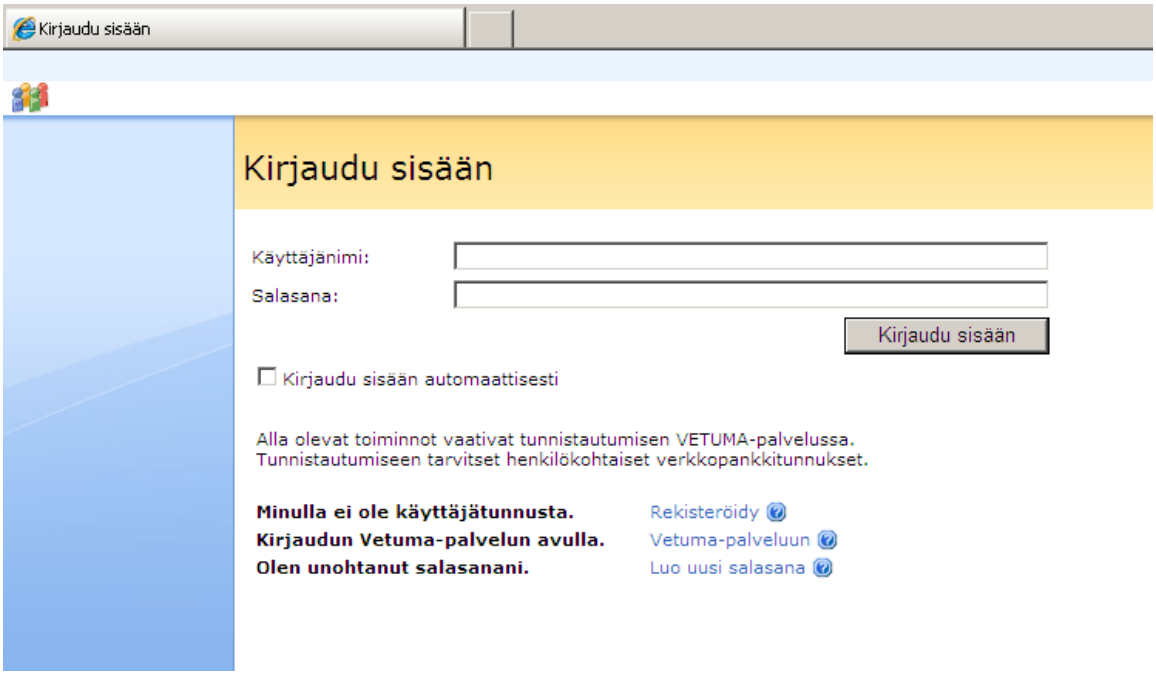
Ratkaisun tarvitsemat konfigurointitiedot lisätään SharePoint-web-sovelluksen web.config-tiedostoon. Lisäys tehdään automaattisesti, kun Vetuma for SharePoint -feature aktivoidaan SharePoint-web-sovellukselle. Featuren aktivoituessa konfigurointitiedot luetaan xml-tiedostosta, jonka luontia varten toteutettiin VetumaForSharePointConfigurationApp-sovellus. Kyseinen sovellus on yksinkertainen Windows-sovellus, jossa on käyttöliittymä tarvittavien konfigurointitietojen syöttämiseen. Sovelluksen käyttöliittymä on esitetty kuviossa 11. Konfiguroinnissa tarvittavia tietoja ovat VETUMA-palvelun tarvitsemat tiedot, käyttäjätunnusten tallennuspaikka, käytettävä jäsenyyden tarjoaja ja niiden SharePoint-ryhmien nimet, joihin rekisteröityvät käyttäjät lisätään.



Kuvio 11. VetumaForSharePointConfigurationApp-sovellus.

6.2.1 Kirjautumissivu

SharePointissa on valmiina lomakkeet-autentikointiin tarkoitettu kirjautumissivu login.aspx, jota käytetään pohjana vetumaLogin.aspx-sivulle, sillä login.aspx sisältää valmiiksi sisäänkirjautumislogiikan. Vetuma for SharePoint –ratkaisun kirjautumissivu SharePoint 2007 -ympäristössä on esitetty kuviossa 12. VetumaLogin.aspx eroaa alkuperäisestä kirjautumissivusta ainoastaan siten, että siihen on lisätty kolme(3) riviä, joissa on Vetuma for SharePoint –ratkaisun toiminnot.



Kuvio 12. Vetuma for SharePoint –ratkaisua hyödyntävän palvelun kirjautumissivu SharePoint 2007 -ympäristössä.

Rekisteröidy-linkki

Käytetään, kun käyttäjä haluaa rekisteröityä käyttäjäksi. Linkki ohjaa käyttäjän VetumaRegister-sivulle, josta tapahtuu jatko-ohjaus VETUMA-palveluun. Linkin url sisältää queryString-parametrin auth=1, joka kertoo VetumaRegister-sivulle, että käyttäjä on ohjattava VETUMA-palveluun tunnistautumaan.

Vetuma-palveluun –linkki

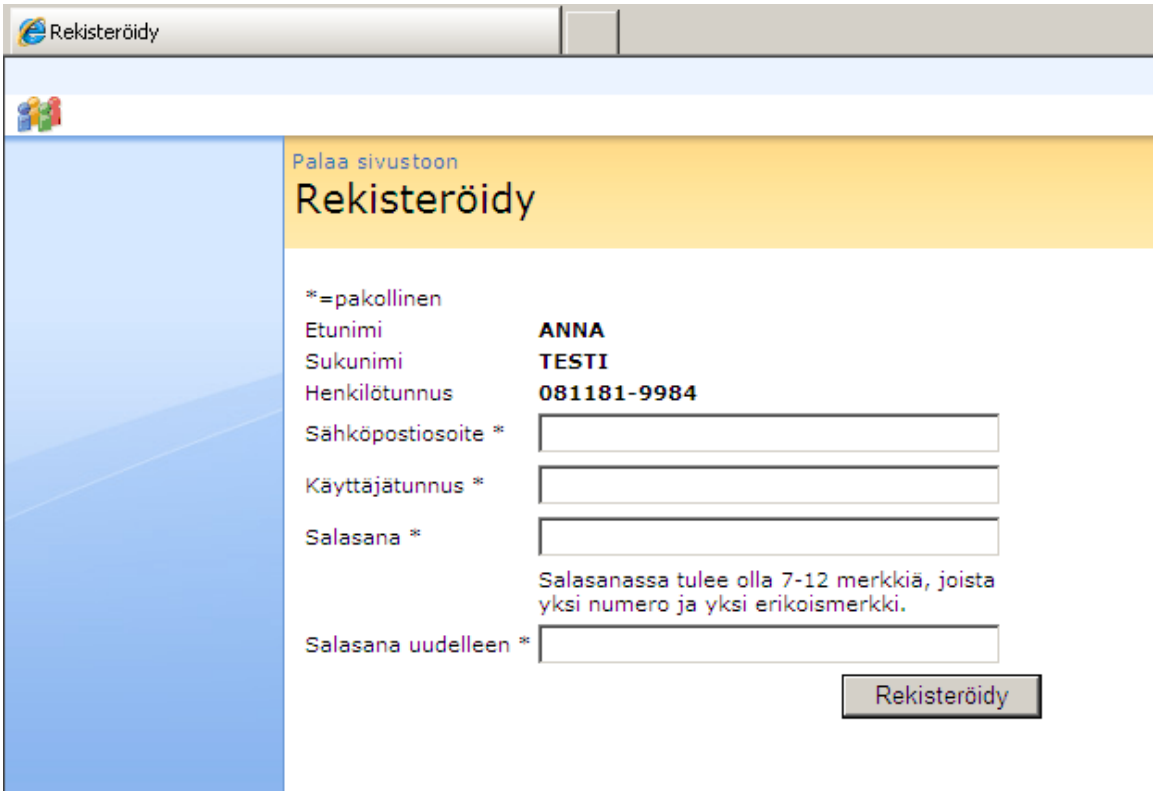
Käytetään, kun käyttäjä haluaa kirjautua SharePoint-ympäristöön VETUMA-palvelun avulla. Linkki ohjaa käyttäjän VetumaRegister-sivulle, josta tapahtuu jatko-ohjaus VETUMA-palveluun. Linkin url sisältää parametrit auth=1 ja loginMethod=1. Auth-parametrin tarkoitus on sama kuin Rekisteröidy-linkin kohdalla. LoginMethod-parametrin arvo 1 kertoo VetumaRegister-sivulle, että käyttäjä haluaa kirjautua VETUMA-palvelua käyttämällä.

Luo uusi salasana –linkki

Linkkiä käytetään, kun käyttäjä on unohtanut salasanansa ja haluaa luoda itselleen uuden salasanan. Linkki ohjaa käyttäjän VetumaPasswordRecovery-sivulle, josta tapahtuu jatko-ohjaus VETUMA-palveluun. Linkin url sisältää parametrit auth=1 ja recoveryCase=1. Auth-parametrin tarkoitus on sama kuin Rekisteröidy-linkin ja Vetuma-palveluun -linkin kohdalla. RecoveryCase-parametrin arvo 1 kertoo VetumaPasswordRecovery-sivulle, että kyseessä on unohtuneen salasanan vaihto.

6.2.2 Rekisteröitymissivu

VetumaRegister-sivu on muokattu sovellussivu (custom application page), jonka master-sivuna käytetään SharePointin simple.master-sivua. SharePointin master-sivun käyttö tuo rekisteröitymissivulle saman ulkoasun kuin muillakin SharePointin sivuilla. Rekisteröitymissivulla käyttäjä rekisteröityy käyttämään SharePoint-ympäristöä. Rekisteröitymissivu sisältää myös logiikan käyttäjän kirjautumiselle VETUMA-palvelun avulla. Vetuma for SharePoint –ratkaisun rekisteröitymissivu esitetään kuviossa 13.



Kuvio 13. Vetuma for SharePoint –ratkaisua hyödyntävän palvelun rekisteröitymissivu SharePoint 2007 -ympäristössä.

Sivun toiminta

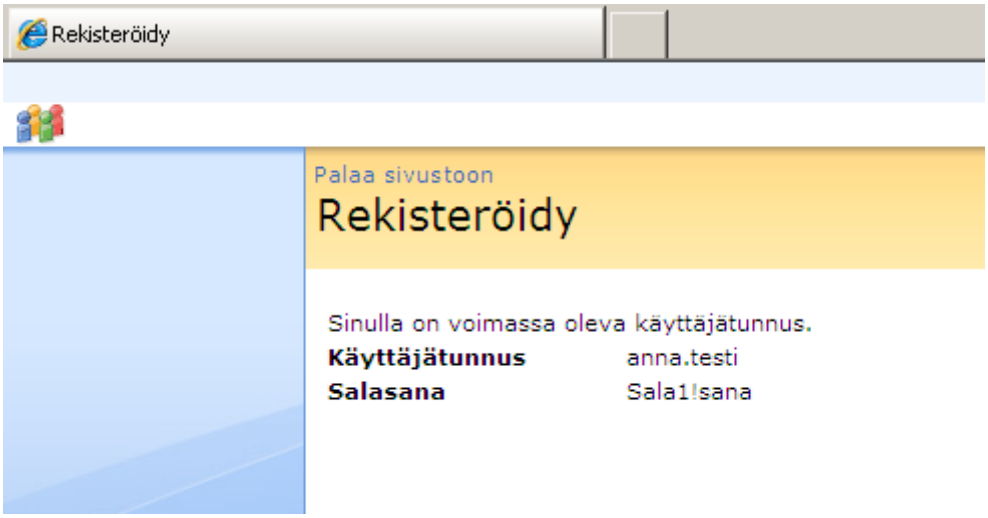
VetumaRegister-sivu tarkistaa saapuneen pyynnön url-parametrit. Jos pyynnössä on parametri auth ja sen arvo on 1, käyttäjä ohjataan VETUMA-palveluun tunnistautumaan. Mikäli pyyntö sisältää auth parametrin lisäksi parametrin loginMethod, jonka arvo on 1, lisätään kyseinen parametri arvoineen VETUMA-palvelun vaatimaan, onnistuneen tunnistautumisen paluu –urliin. Tämä tehdään siksi, että tiedetään käyttäjän pyytämä toiminto tämän palatessa VETUMA-palvelusta.

Pyynnön saapuessa VETUMA-palvelusta, parametreinä on vetumaStatus ja VetumaAction. VetumaStatus-parametri kertoo tunnistautumisen onnistumisesta; 1=onnistunut, 2=käyttäjä on keskeyttänyt tunnistuksen ja 3=virhe tunnistuksen aikana. Parametri VetumaAction puolestaan kertoo toiminnon, joka Vetuma-palvelussa tapahtui. Parametrin arvo on aina 1, koska käytetään tunnistus-toimintoa.

Kun käyttäjä haluaa rekisteröityä ja hän on tunnistautunut onnistuneesti VETUMA-palvelussa, tarkistetaan ensimmäiseksi henkilötunnuksen avulla, onko käyttäjällä ennestään

käyttäjätunnus. Mikäli käyttäjällä on olemassa oleva tunnus, se näytetään hänelle, kuten kuviossa 14, ja rekisteröintilomake piilotetaan. Jos tunnusta ei ennestään ole, näytetään rekisteröitymissivulla kuviossa 13 näkyvä lomake, jonka täyttämällä käyttäjä voi rekisteröityä käyttämään SharePoint-ympäristöä. Lomakkeella kysytään seuraavat tiedot:

- sähköpostiosoite
- käyttäjätunnus
- salasana (kaksi kertaa).



Kuvio 14. Vetuma for SharePoint –rekisteröitymissivu ilmoittaa käyttäjälle, jos hänellä on ennestään käyttäjätunnus.

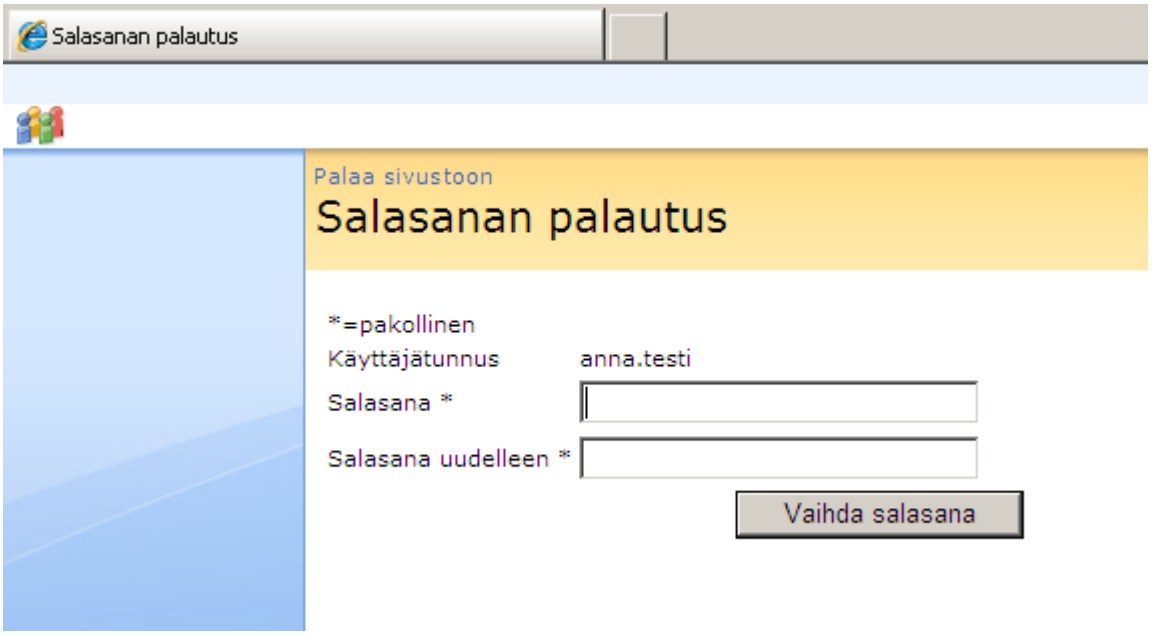
Tilanteessa, jossa käyttäjä haluaa kirjautua SharePoint-ympäristöön VETUMA-palvelun avulla eikä hänellä vielä ole tunnusta ympäristöön, kysytään käyttäjältä sähköpostiosoite. Sovellus luo käyttäjälle käyttäjätunnuksen etunimi.sukunimi-muodossa ja generoi salasanan. Mikäli järjestelmässä on sama etunimi.sukunimi-tunnus, ratkaisu lisää tunnuksen perään luvun 1 ja tarkistaa, löytyykö vastaavaa tunnusta. Jos ei löydy, käyttäjän tunnukseksi tulee etunimi.sukunimi1. Jos vastaava löytyy, kasvatetaan tunnuksen perään lisättävää lukua niin kauan, että löytyy yksilöllinen tunnus. Tunnuksen ja salasanan generoinnin jälkeen käyttäjä kirjataan sisään järjestelmään kyseisillä tunnuksilla. Seuraavilla kerroilla tunnusta ei luoda enää uudestaan vaan käyttäjä kirjataan sisään VetumaRegister-sivulla automaattisesti ja ohjataan pyydetylle SharePoint-sivustolle.

Hyväksyttävät syötteet rekisteröidyttäessä

Kaikki käyttäjän syöttämät tiedot tarkistetaan ennen tallennuksen aloittamista. Sähköpostiosoitteen täytyy olla muodoltaan sähköpostiosoite, muuten rekisteröinti ei onnistu. Salasanan on oltava 7-12 merkkiä pitkä, sisällettävä vähintään yhden(1) numeron ja yhden(1) ei-aakkosnumeerisen merkin eli niin sanotun erikoismerkin, esimerkiksi ! tai ?.

6.2.3 Salasanan vaihto/palautus -sivu

VetumaPasswordRecovery-sivu on muokattu sovellussivu (custom application page), jonka master-sivuna käytetään SharePointin simple.master-sivua. VetumaPasswordRecovery-sivun kautta käyttäjä voi korvata unohtuneen salasanan uudella. Kuviossa 15 esitetään VetumaPasswordRecovery-sivu käyttäjän tunnistauduttua VETUMA-palvelussa.



Kuvio 15. Vetuma for SharePoint –ratkaisun salasanan vaihto sivu.

Sivun toiminta

VetumaPasswordRecovery-sivu tarkistaa saapuneen pyynnön url-parametrit. Jos pyynnössä on parametri auth ja sen arvo on 1, käyttäjä ohjataan VETUMA-palveluun tunnistautumaan. Pyynnössä mukana oleva parametri recoveryCase lisätään arvoineen VETUMA-palvelun

vaatimaan, onnistuneen tunnistautumisen paluu -urliin, jotta tiedetään käyttäjän pyytämä toiminto käyttäjän palatessa VETUMA-palvelusta.

Pyynnön saapuessa VETUMA-palvelusta, parametreinä on vetumaStatus ja VetumaAction. VetumaStatus-parametri kertoo tunnistautumisen onnistumisesta. Parametri VetumaAction puolestaan kertoo toiminnon, joka Vetuma-palvelussa tapahtui, aivan kuten VetumaRegister-sivulla.

Mikäli käyttäjän tunnistautuminen on onnistunut, VetumaPasswordRecovery-sivulla haetaan käyttäjän tiedot henkilötunnuksen avulla. Käyttäjälle näytetään hänen käyttäjätunnuksensa ja pyydetään syöttämään uusi salasana kahteen kertaan. Käyttäjälle kerrotaan viestillä uuden salasanan luonnin onnistumisesta. Active Directory ei tue unohtuneen salasanan palauttamista, jolloin salasanan vaihtaminen ei normaalisti onnistu. Tämä rajoite on ohitettu tallentamalla rekisteröintivaiheessa käyttäjän salasana salattuna piilotettuun SharePointin mukautettuun luetteloon. Salasanan tallennus tehdään vain, kun käyttäjätietokantana on Active Directory.

Vetuma for SharePoint –ratkaisun lähdekoodi on saatavilla osoitteesta http://vetuma.codeplex.com. Samasta osoitteesta löytyy myös ratkaisun asennuspaketit, jotka sisältävät ratkaisun wsp-paketin (SharePointin sovelluspaketti), VetumaForSharePoint-ConfigurationApp-sovelluksen ja asennusohjeistuksen.

6.3 Testaus

Ratkaisu sekä sen asennuspaketti ja -ohjeistus testattiin asentamalla ratkaisu Microsoft Office SharePoint Server 2007 ja SharePoint Server 2010 -ympäristöihin. Molemmissa ympäristöissä testattiin käyttäjätietokantana sekä Active Directoryä että Sql-tietokantaa. Lisäksi Documentan yhteistyökumppani testasi ratkaisua omassa SharePoint-ympäristössään. Toteuttajan suorittamassa testauksessa testattiin kaikki ratkaisun toiminnot sekä uuden käyttäjän että jo rekisteröityneen käyttäjä kannalta.

6.4 Tapahtumien kulku

Tässä luvussa kuvataan Vetuma for SharePoint –sovelluksen tukemien tapahtumien kulut. Tapahtumien kulku voi katketa odottamattoman virheen seurauksena, jolloin käyttäjälle näy-

tetään viesti ’Tapahtui odottamaton virhe’. Odottamattoman virheen voi aiheuttaa esimerkiksi tilapäinen yhteysvirhe yhdistettäessä käyttäjätietokantaan.

Rekisteröityminen

1. Käyttäjä on kirjautumissivulla, jossa hän valitsee ’Rekisteröidy’.

2. Käyttäjä ohjautuu VetumaRegister-sivulle, jossa pyyntö tarkistetaan ja käyttäjä edelleenohjataan VETUMA-palveluun.

3. Käyttäjä suorittaa tunnistautumisen VETUMA-palvelussa, minkä jälkeen hänet ohjataan takaisin VetumaRegister-sivulle.

4. VETUMA-palvelun vastaus tarkistetaan VetumaRegister-sivulla.

    a. Jos tunnistautuminen on onnistunut, käyttäjälle näytetään rekisteröitymislomake. Tapahtumien kulku jatkuu kohdasta 5.

    b. Mikäli tunnistuksessa tapahtui virhe tai käyttäjä peruutti tunnistautumisen, rekisteröitymislomaketta ei näytetä käyttäjälle ja VetumaRegister-sivulle tulee viesti ’Peruutit tunnistautumisen’ tai ’Virhe tunnistautumisen aikana’, VETUMA-vastauksen perusteella. Käyttäjä voi halutessaan siirtyä takaisin kirjautumissivulle ’Palaa sivustoon’-linkistä. Tapahtumien kulku päättyy.

5. Käyttäjä syöttää vaaditut tiedot ja painaa ’Rekisteröidy’-nappia.

6. Käyttäjän syötteiden kelvollisuus tarkistetaan. Syötteiden ollessa kelvolliset, käyttäjälle luodaan käyttäjätunnus. Jos käyttäjän syötteet ovat puutteelliset, näytetään sivulla puutteellisten syötteiden kohdalla punainen tähti. Kohdat 5 ja 6 toistuvat, kunnes syötteet ovat kelvolliset.

7. Sivulla näytetään viesti ’Rekisteröinti onnistui’.

8. Käyttäjä voi siirtyä kirjautumaan sivustolle valitsemalla ’Jatka sivustolle’-linkkiä.

Kirjautuminen VETUMA-palvelun avulla

1. Käyttäjä on kirjautumissivulla, jossa hän valitsee ’Vetuma-palveluun’-linkin ’Kirjaudun Vetuma-palvelun avulla’-tekstin vieressä.

2. Käyttäjä ohjautuu VetumaRegister-sivulle, jossa pyyntö tarkistetaan ja käyttäjä edelleenohjataan VETUMA-palveluun.

3. Käyttäjä suorittaa tunnistautumisen VETUMA-palvelussa, minkä jälkeen hänet ohjataan takaisin VetumaRegister-sivulle.

4. VETUMA-palvelun vastaus tarkistetaan VetumaRegister-sivulla.

    a. Jos tunnistautuminen on onnistunut, tapahtumien kulku jatkuu kohdasta 5.

    b. Jos tunnistuksessa tapahtui virhe tai käyttäjä peruutti tunnistautumisen, VetumaRegister-sivulle tulee viesti ’Peruutit tunnistautumisen’ tai ’Virhe tunnistautumisen aikana’, VETUMA-palvelun vastauksen mukaan. Käyttäjä voi halutessaan siirtyä takaisin kirjautumissivulle ’Palaa sivustoon’-linkistä. Tapahtumien kulku päättyy.

5. VetumaRegister-sivulla tarkistetaan, onko käyttäjällä olemassa oleva käyttäjätunnus järjestelmään.

    a. Jos käyttäjällä on käyttäjätunnus, käyttäjä kirjataan sisään järjestelmään ja ohjataan pyydetylle SharePoint-sivustolle. Tapahtumien kulku päättyy VETUMA for SharePoint -ratkaisun osalta.

    b. Jos käyttäjällä ei ole käyttäjätunnusta, tapahtumien kulku jatkuu kohdasta 6.

6. Käyttäjää pyydetään syöttämään sähköpostiosoite.

7. Käyttäjän syötettyä sähköpostiosoite, syöte tarkistetaan. Jos syöte on kelvollinen, käyttäjälle luodaan tunnus (etunimi.sukunimi) ja generoidaan salasana, joilla käyttäjä kirjataan järjestelmään ja ohjataan pyydetylle SharePoint-sivustolle. Jos käyttäjän syöte on virheellinen, näytetään sivulla punainen tähti sähköpostiosoite-kentän vieressä. Kohdat 6 ja 7 toistuvat, kunnes käyttäjän syöte on muodoltaan sähköpostiosoite.

Salasanan korvaaminen

1. Käyttäjä on kirjautumissivulla, jossa hän valitsee ’Luo uusi salasana’.

2. Käyttäjä ohjautuu VetumaPasswordRecovery-sivulle, jossa pyyntö tarkistetaan ja käyttäjä edelleenohjataan VETUMA-palveluun.

3. Käyttäjä suorittaa tunnistautumisen VETUMA-palvelussa, minkä jälkeen hänet ohjataan takaisin VetumaPasswordRecovery-sivulle.

4. VETUMA-palvelun vastaus tarkistetaan VetumaPasswordRecovery-sivulla.

    a. Jos tunnistautuminen on onnistunut, tapahtumien kulku jatkuu kohdasta 5.

    b. Jos tunnistuksessa tapahtui virhe tai käyttäjä peruutti tunnistautumisen, VetumaPasswordRecovery-sivulle tulee viesti ’Peruutit tunnistautumisen’ tai ’Virhe tunnistautumisen aikana’, VETUMA-palvelun vastauksen mukaan. Käyttäjä voi halutessaan siirtyä takaisin kirjautumissivulle ’Palaa sivustoon’-linkistä. Tapahtumien kulku päättyy.

5. VetumaPasswordRecovery-sivulla tarkistetaan, että käyttäjällä on olemassa oleva tunnus.

    a. Jos tunnus on olemassa, tapahtumien kulku jatkuu kohdasta 6.

    b. Mikäli käyttäjällä ei ole tunnusta, käyttäjälle näytetään viesti, joka kertoo, ettei tunnusta löydynyt. Tapahtumien kulku päättyy.

6. Käyttäjälle näytetään hänen käyttäjätunnuksensa ja pyydetään syöttämään uusi salasana. Syötettyään uuden salasanan kahdesti käyttäjä painaa ’Vaihda salasana’-nappia.

7. Salasanan vahvuus tarkistetaan. Jos käyttäjän syöttämä salasana ei ole tarpeeksi vahva, näytetään sivulla punainen tähti salasana-kentän vieressä. Salasanan ollessa riittävän vahva, käyttäjän salasana vaihdetaan ja hänelle näytetään viesti salasanan vaihdon onnistumisesta. Käyttäjä voi palata kirjautumissivulle ’Palaa sivustoon’-linkistä. Kohdat 6 ja 7 toistuvat, kunnes käyttäjä on syöttänyt riittävän vahvan salasanan.

7 POHDINTA JA YHTEENVETO

Tämän opinnäytetyön tarkoituksena oli tutkia käyttäjän tunnistamista kunnan sähköisen asioinnin palvelun kannalta. Sähköisessä asioinnissa on tärkeää, että käyttäjä voidaan tunnistaa luotettavasti. Tätä tarkoitusta varten on kehitetty VETUMA, kansalaisille tarkoitettu verkkotunnistus- ja maksamispalvelu. Palvelun tarve tuli kunnilta ja kuntien organisaatioilta, myöhemmin mukaan liittyi myös Suomen valtio. Palvelun on toteuttanut Fujitsu Services Oy, joka vastaa palvelun ylläpidosta ja jatkokehityksestä.

VETUMA-palvelu tukee monipuolisesti julkishallinnon verkkopalveluissa tarvittavia käyttäjäntunnistustoimintoja. Palvelun avulla voidaan suorittaa käyttäjän luotettava tunnistaminen, käyttäjän suorittama hyväksyminen ja sähköinen allekirjoitus sekä maksaminen ja maksun palautus. Eri toimintojen suorittamiseksi käyttäjälle on tarjolla useita eri suoritusvaihtoja, joista palvelua höydyntävä organisaatio voi valita käyttäjilleen tarjottavat. Esimerkiksi käyttäjän tunnistamiseen organisaatio voi tarjota pankkien Tupas-tunnistusta, kansalaisvarmenteeseen perustuvaa tunnistusta tai käyttäjätunnus-salasana-tunnistusta. Näistä organisaation verkkopalvelua käyttävä kansalainen voi valita itselleen parhaiten soveltuvan tunnistautumismenetelmän.

VETUMA-palvelun dokumentaatio auttaa organisaatioita liittämään palvelun verkkopalveluihinsa. Mikäli verkkopalvelu on toteutettu Microsoftin .Net-tekniikoilla, on organisaatioilla käytettävissään Vetuma Toolkit, jolloin VETUMA-palvelun liittäminen verkkopalveluun on todella helppoa.

Alunperin opinnäytetyön tarkoituksena oli toteuttaa VETUMA-palvelun liittämistä kunnan verkkopalveluun helpottava .Net-pohjainen palvelu. Työn edetessä todettiin sen olevan tarpeeton, sillä Fujitsun toteuttama Vetuma Toolkit arvioitiin riittävän helppokäyttöiseksi. Documentan yhteistyökumppanin toiveesta päädyttiin toteuttamaan SharePoint-alustalle rekisteröitymisratkaisu, joka hyödyntää VETUMA-palvelua käyttäjän tunnistamisessa rekisteröitymisen yhteydessä. Ratkaisun avulla käyttäjä voi myös kirjautua verkkopalveluun tunnistautumalla VETUMA-palvelussa, jolloin hänen ei tarvitse syöttää käyttäjätunnusta. Vetuma for SharePoint –ratkaisussa hyödynnetään VETUMA-palvelua myös unohtuneen salasanan korvaamisessa; käyttäjän on ensin tunnistauduttava VETUMA-palvelussa ennen kuin hän voi uusia salasanansa.

Toteutettu ratkaisu vastaa määrittelyä ja sitä voidaan sen vuoksi pitää onnistuneena. Ratkaisuun olisi voinut lisätä mahdollisuuden määrittää käyttäjille tarjottavia tunnistusmenetelmiä VetumaForSharePointConfigurationApp-sovelluksen avulla web.config-tiedoston muokkaamisen sijaan. Nyt ratkaisu tukee ainoastaan Tupas- eli verkkopankkitunnistusta. Tosin verkkopankkitunnistus oli ainoana tunnistustapavaatimuksena määrittelyssä. Ratkaisun toteutusaikataulu oli sen hetkiseen työmäärän nähden melko tiukka. Toteutusaikataulussa ei pysytty, vaan ratkaisu valmistui Documentan yhteistyökumppanin testattavaksi syyskuussa 2010 suunnitellun kesäkuun sijaan. Välissä oli kuukauden mittainen kesäloma eli periaatteessa aikataulu ylittyi noin kahdella kuukaudella. Arvioitu työmäärä puolestaan ylittyi lähes 100 %:lla. Suurin osa työmäärän ylittymisestä johtui SharePoint 2010 mukana tulleen Claims Based –autentikoinnin lainalaisuuksien ja konfiguroinnin opettelemisesta. Aikatauluarviota tehtäessä kyseinen uusi tapa hoitaa autentikointi jäi huomioimatta.

Opinnäytetyöprosessi alkoi 6.10.2008 aiheanalyysin palauttamisella. Aiheanalyysin hyväksymisen jälkeen toimeksiantosopimus tehtiin 8.10.2008 Documenta Oy:n kanssa. Prosessi eteni sen jälkeen siten, että 31.3.2009 oli opinnäytetyösuunnitelman esitys. Suunnitelmassa suunniteltiin opinnäytetyön teoriaosuuden valmistuvan kesäkuussa 2009, juuri ennen kyseisen vuoden kesälomia. Suunnitelma ei pitänyt, vaan teoriaosa valmistui marraskuussa 2010, yli vuoden suunnitellusta aikataulusta myöhässä. Opinnäytetyösuunnitelmassa suunniteltiin koko opinnäytetyön olevan valmis huhtikuussa 2010. Koska teoriaosa ei edennyt aikataulun mukaan, myös empiirinen osa viivästyi ja valmistui vasta syyskuun 2010 alussa. Kaiken kaikkiaan opinnäytetyöprosessin suunniteltu aikataulu ylittyi reilulla puolella vuodella. Suurin syy aikataulun venymiseen oli tekijän ajattelutapa ”Onhan tässä vielä aikaa...”. Olisiko opinnäytetyöstä tullut parempi, jos työ olisi tehty suunnitellun aikataulun mukaan? Kyllä ja ei. ’Kyllä’ siksi, että aikataulun mukaan kirjoitettuna opintojen aikana saatu kielioppi- ja kirjoitustaito olisi ollut paremmin muistissa ja sen vuoksi opinnäytetyöstä olisi tullut kieliasultaan parempi. Reilu vuosi ohjelmakoodin ja englanninkielen kirjoittamista ilman suurempia suomenkielisiä tuotoksia ei ole tehnyt hyvää suomenkielen kirjoitustaidolle. Ja ’ei’ sen vuoksi, että vuosi sitten ammatillinen osaaminen ei olisi ollut samalla tasolla kuin nyt ja toteutetusta ratkaisusta ei olisi tullut yhtä hyvä. Tosin tähän voitaisiin vuoden päästä todeta, että ratkaisusta olisi tullut koodin osalta vielä vuoden myöhemmin toteutettuna vieläkin parempi, sillä ammatillista kehittymistä tapahtuu jatkuvasti.

Nyt, marraskuussa 2010, yli kaksi vuotta opinnäytetyöprosessin aloittamisen jälkeen voidaan todeta, että työ valmistui ennen opiskeluajan päättymistä ja aikataulun venymistä lukuunot-

tamatta opinnäytetyöprosessiin voi olla tyytyväinen. Opinnäytetyön kirjallinen osa itsessään olisi voinut paikoin olla parempaa suomenkieltä ja monipuolisemmin lukijan huomioivaa.

LÄHTEET

Fujitsu 2006. Net – Fujitsun asiakaslehti. Saatavilla: http://www.net-lehti.com/netlehtiarkisto/net206/vetuma.htm (Luettu 30.10.2010).

Fujitsu Services Oy 2007. Vetuma Toolkit .Net. Web-dokumentti. Saatavilla: http://www.suomi.fi/suomifi/laatuaverkkoon/asiointi_ja_lomakkeet/sahkoinen_asiointi/verkkotunnistaminen_ja_maksaminen/ (Luettu 19.9.2010).

Fujitsu Services Oy 2010 a. VETUMA-palvelu - Sovelluksille tarjotun toiminnallisuuden kuvaus versio 3.0. Web-dokumentti. Saatavilla: http://www.suomi.fi/suomifi/tyohuone/yhteiset_palvelut/verkkotunnistaminen_ja_-maksaminen_vetuma/tekninen_rajapinta/VETUMA_palvelun_sovelluksille_tarjoaman_toiminnallisuuden_kuvaus_v3_0/VETUMA_palvelun_sovelluksille_tarjoaman_toiminnallisuuden_kuvaus_v2_2.pdf (Luettu 24.10.2010).

Fujitsu Services Oy 2010 b. VETUMA-palvelu - Kutsujarajapinnan määrittely versio 3.0. Web-dokumentti. Saatavilla: http://www.suomi.fi/suomifi/tyohuone/yhteiset_palvelut/verkkotunnistaminen_ja_-maksaminen_vetuma/tekninen_rajapinta/VETUMA_palvelun_kutsurajapinnan_maarittely_v3_0/VETUMA_palvelun_kutsurajapinnan_maarittely_v2_2.pdf (Luettu 24.10.2010).

Fujitsu Services Oy 2010 c. Vetuma-palvelun tilanne 8.2010. Web-dokumentti. Saatavilla: http://www.suomi.fi/suomifi/laatuaverkkoon/asiointi_ja_lomakkeet/sahkoinen_asiasi-oi/verkkotunnistaminen_ja_maksaminen/yleiset_materiaalit/vetuma_palvelun_tiltila_elokuussa_2010/VETUMATransactions_Transactions_20100601-014856.pdf (Luettu 26.9.2010).

Järvinen, P. 2003. Salausmenetelmät. Jyväskylä: Docendo.

Kiiski, M. 2004. Kelan, verohallinnon ja työministeriön yhteinen Katve-hanke ja sen palvelut. Web-dokumentti. Saatavilla: http://www.vaestorekisterikeskus.fi/vrk/files.nsf/files/CC255E41C49B6B2AC2256F09002AC93F/$file/aHST-seminaari+III+-+Markku+Kiiski.ppt (Luettu 17.11.2010).

Korpela, J. 2007. Internet hyöty- & viihdekäytössä. Jyväskylä: Docendo.

Kunnat.net 2005. http://www.kunnat.net/k_perussivu.asp?path=1;29;66354;66364;91446 (Luettu 26.9.2010).

Kuntaliitto 2009. Kuntalaki, hallintolaki ja laki sähköisestä asioinnista. 2009. Helsinki: Hakapaino Oy.

Kymenlaakson ammattikorkeakoulu 2007.
http://www.kyamk.fi/Ajankohtaista/Mediatiedotteet/?news_id=131 (Luettu 26.9.2010).

Microsoft 2005. http://msdn.microsoft.com/en-us/library/ff647070.aspx (Luettu 2.11.2010).

Microsoft 2010. http://sharepoint.microsoft.com/fl-fl/Pages/default.aspx (Luettu 18.11.2010).

Poutapilvi 2009. http://www.poutapilvi.fi/tyonaytteet/tyonaytteita/vtv_-_vaalirahoitusvalvonta/ (Luettu 26.9.2010).

Roine, J. 2007. Microsoft 2007 Office system. Helsinki: Readme.fi.

Suomi.fi 2010.
http://www.suomi.fi/suomifi/laatuaverkkoon/asiointi_ja_lomakkeet/sahkoinen_asiasioi/verkkotunnistaminen_ja_maksaminen/ (Luettu 25.9.2010).

Tietokone.fi 2006. http://www.tietokone.fi/uutiset/2006/paras_julkinen_palvelu_loytyi (Luettu 26.9.2010).

Turku.fi 2008.
http://www.taideakatemia.turkuamk.fi/public/default.aspx/nodeid/Local%20SettinSe/UserControls/default.aspx?contentid=102312 (Luettu 26.9.2010).

Työeläkejärjestelmän yhteinen tunnistuspalvelu. https://tunnistus.etk.fi/ (Luettu 30.10.2010).

Valtiokonttori 2009.
http://www.suomi.fi/suomifi/laatuaverkkoon/asiointi_ja_lomakkeet/sahkoinen_asiointi/vverkkotunnistamine_ja_maksaminen/ (Luettu 12.3.2009).

Valtiovarainministeriö 2009. VETUMA-palvelun yleisesittely. Web-dokumentti. Saatavilla:
http://www.suomi.fi/suomifi/laatuaverkkoon/asiointi_ja_lomakkeet/sahkoinen_asiointi/verkkotunnistaminen_ja_maksaminen/ (Luettu 25.9.2010)

LIITTEET

```
// Set authentication methods
Collection<VetumaLoginMethod> methods = new
Collection<VetumaLoginMethod>(){ VetumaLoginMethod.Tupas };

// Create Vetuma authentication request
VetumaAuthenticationRequest request = new VetumaAuthenticationRequest(
      // Text "next", used if browser does not support javascript and
      user must click himself to Vetuma. Text is loaded from resource
      file.
      VetumaForSP.ResourceManager.GetString("Next"),

      // Text which tells user to click Next to continue to Vetuma.
      Text is loaded from resource file.
      VetumaForSP.ResourceManager.GetString("NoJavascript"),

      "fi", // Vetuma user interface language

      methods, // Authentication methods available for user

      new Uri(successUrl), // Success url

      new Uri(cancelUrl), // Cancel url

      new Uri(errorUrl), // Error url

      // Get from web.config: Vetuma service url
      new Uri(VetumaForSharePointConfig.getConfig().
            VetumaConfig.PostUrl),

      // Get from web.config: Shared secret id
      VetumaForSharePointConfig.getConfig().
            VetumaConfig.SharedSecretId,

      // Get from web.config: Shared secret
      VetumaForSharePointConfig.getConfig().VetumaConfig.SharedSecret,

      // Get from web.config: Id of the application that calls Vetuma
      VetumaForSharePointConfig.getConfig().VetumaConfig.ApplicationId,

      // Get from web.config: Vetuma configuration id
      VetumaForSharePointConfig.getConfig().VetumaConfig.
            ConfigurationId);

// Submit the authentication request to Vetuma.
try
{
    request.Submit();
}
catch (System.Threading.ThreadAbortException)
{
    // This error is caused by redirection in sharepoint. No need to
handle.
}
```

```
int vetumaStatus = 0;

// Get vetumaStatus from http request query string.
int.TryParse(Request["vetumaStatus"].ToString(), out vetumaStatus);

// Create response object.
VetumaAuthenticationResponse response =new
VetumaAuthenticationResponse(
// Get from web.config: Shared secret id
VetumaForSharePointConfig.getConfig().VetumaConfig.SharedSecretId,
// Get from web.config: Shared secret
VetumaForSharePointConfig.getConfig().VetumaConfig.SharedSecret);

// Validate Vetuma response.
bool valid = response.Validate();

if (valid)
{
    switch (vetumaStatus)
    {
         case 1:
            // Authentication succeeded
            // Get user social security number
            string socialSecurityNumber = response.PersonId;
            break;
         case 2:
            // Authentication cancelled by user
            break;
         case 3:
            // Authentication error
            break;
         default:
            break;
     }

}
else
{
      throw new ApplicationException("Vetuma response was not valid.");
}
```