Niko Loukola

Käyttäjätunnusten luovutus ja salasanan uusiminen Vetuma-palvelun avulla

WinhaPro, Active Directory ja Luovari

Opinnäytetyö
Syksy 2016
SeAMK Tekniikka
Tietotekniikan tutkinto-ohjelma

SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: SeAMK Tekniikka

Tutkinto-ohjelma: Tietotekniikka

Suuntautumisvaihtoehto: Ohjelmointi

Tekijä: Niko Loukola

Työn nimi: Käyttäjätunnusten luovutus ja salasanan uusiminen Vetuma-palvelun avulla

Ohjaaja: Hilkka Niemelä

Vuosi: 2016 Sivumäärä: 37 Liitteiden lukumäärä: -

Tämän opinnäytetyön tavoitteena oli ohjelmoida digitaalisella tunnistautumisella toimiva käyttäjätunnusten luovutukseen ja salasanan uusimiseen tarkoitettu sovellus Seinäjoen Ammattikorkeakoulun (SeAMK) opiskelijoiden käyttöön. Sovellus kehitettiin myös SeAMKin Opiskelijapalveluiden ja Helpdesk Jelpparin avuksi. Sovellus hyödyntää tunnistautumista Vetuma-palvelussa.

Opinnäytetyössä käsitellään digitaalista tunnistautumista sekä yleisesti että sovellukseen liittyen. Lisäksi opinnäytetyössä esitellään yleisellä tasolla ja SeAMKin näkökulmasta opiskelijajärjestelmiin liittyviä palveluja.

Opinnäytetyössä kuvataan uusi sovelluksen myötä mahdolliseksi tuleva käyttäjätunnusten luovutusprosessi vaiheittain opiskelupaikan vastaanotosta käyttäjätunnusten luovutukseen ja salasanan uusimiseen.

Avainsanat: Vetuma-palvelu, digitaalinen tunnistautuminen, WinhaPro, Active Directory, C#, ASP.NET

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Information Technology

Specialisation: Programming

Author: Niko Loukola

Title of thesis: Handing credentials and resetting a password using the Vetuma service

Supervisor: Hilkka Niemelä

Year: 2016 Number of pages: 37 Number of appendices: -

The goal of this thesis was to program an application using digital identification for handing credentials and resetting a password for the use of the students of Seinäjoki University of Applied Sciences. The application was also developed for the help of the school's Student Services and the Helpdesk Jelppari. The application uses identification in the Vetuma service.

The thesis covers digital identification in general and related to the application. Additionally, the services associated with student systems are presented in general and from the point of view of Seinäjoki University of Applied Sciences.

The thesis describes the new process of handing credentials made possible by the application. It proceeds step by step from accepting a student place to handing credentials and resetting the password.

Keywords: The Vetuma service, digital identification, WinhaPro, Active Directory, C#, ASP.NET

SISÄLTÖ

Opinnäytetyön tiivistelmä 2
Thesis abstract 3
SISÄLTÖ 4
Kuva- ja taulukkoluettelo 6
Käytetyt termit ja lyhenteet 7
1 JOHDANTO 10
1.1 Työn tausta 10
1.2 Työn tavoite 10
1.3 Työn rakenne 11
2 DIGITAALINEN TUNNISTAUTUMINEN 12
2.1 Vetuma-palvelu 12
2.2 Tupas-tunnistuspalvelu 13
2.3 Tunnistautuminen mobiilivarmenteella 13
2.4 Muita tunnistautumispalveluita ja -menetelmiä 14
3 OPISKELIJAJÄRJESTELMIIN LIITTYVIÄ PALVELUJA 16
3.1 WinhaPro 16
3.2 Luovari 16
3.3 Microsoftin tarjoamia palveluja 17
3.4 Valtakunnalliset palvelut 18
4 KÄYTTÄJÄTUNNUSTEN LUOVUTUS KEHITETYLLÄ SOVELLUKSELLA 19
4.1 Käyttäjätunnusten luovutusprosessi 19
4.2 Kehitys- ja palvelinympäristö 21
4.3 Uuden opiskelijan tietojen muodostuminen SeAMKin järjestelmiin 21
4.4 Vetuma-palvelun integroiminen palveluntarjoajan sovellukseen 22
4.5 SeAMKin järjestelmien integroiminen palveluntarjoajan sovellukseen 27
4.5.1 WinhaPro 28
4.5.2 Active Directory 28
4.5.3 Luovari 29
4.5.4 Salasanan uusiminen 29

4.6 Versionhallinta 30
4.7 Tietoturva 30
4.8 Sovelluksen testaus 31
5 POHDINTAA 33
LÄHTEET 35

Kuva- ja taulukkoluettelo

Kuva 1. Siirtyminen tunnistautumaan Vetuma-palveluun. 22

Kuva 2. Tunnistustavan valinta Vetuma-palvelussa. 25

Kuva 3. Pankin valinta Vetuma-palvelussa. 26

Kuva 4. Sovelluksen näyttämät käyttäjätiedot. 27

Kuva 5. Salasanan uusiminen sovelluksella. 30

Taulukko 1. Vetuma-kutsujen yleiset parametrit. 24

Taulukko 2. Vetuma-vastausten yleiset parametrit. 27

Käytetyt termit ja lyhenteet

.NET Framework	Microsoftin kehittämä ohjelmistokehys .NET-teknologioita käyttävien sovellusten ja palveluiden kehittämiseen, käyttöönottamiseen ja suorittamiseen (Beal 2016).
ASP.NET	Avoimen lähdekoodin web-ohjelmistokehys modernien web-sovellusten ja -palveluiden kehittämiseen ja .NET Frameworkin osa (Microsoft 2016b).
C#	Ohjelmointikieli, joka on suunniteltu .NET Frameworkissa suoritettavien sovellusten rakentamiseen (Microsoft 2016a).
FIM	Forefront Identity Manager, Microsoftin kehittämä käyttäjän digitaalisen identiteetin hallintapalvelu yrityksessä (Nordström 2012).
Metaverse	Forefront Identity Managerin osa, johon kaikki informaatio kaikista identiteeteistä on kerätty (Nordström 2012).
Rules extensions	Forefront Identity Manageriin esimerkiksi C#-kielellä ohjelmoituja toiminnallisuuslisäyksiä (Microsoft 2016c).
Active Directory	Microsoftin kehittämä Windows-toimialueen verkkokäyttöjärjestelmä (Desmond ym. 2013, 1).
ADAM	Active Directory Application Mode, Active Directorya vastaava palvelu, joka on erityisesti suunniteltu directory-enabled-sovelluksia varten, kun taas AD on suunniteltu palvelinkäyttöjärjestelmätoimintoja varten (Microsoft 2014).
WinhaPro	CGI:n kehittämä opintohallinnon perusjärjestelmä (CGI Suomi Oy, [viitattu 23.8.2016]).

Luovari SeAMKin itse kehittämä käyttäjätunnusten luovutussovellus, jota on aiemmin käytetty käyttäjätunnusten luovutukseen (Kinnunen 2015).

Vetuma-palvelu Fujitsun Finland Oy:n ylläpitämä digitaaliseen tunnistaumiseen ja verkkomaksamiseen julkishallinnon sovelluksia varten kehitetty palvelu, josta vastaa Valtion tieto- ja viestintätekniikkakeskus Valtori (Valtori 2016).

Tupas-tunnistuspalvelu

Pankkien yhteisesti määrittelemä ja jokaisen pankin itse ylläpitämä verkkopankkitunnistautumispalvelu (Finanssialan keskusliitto 2013, 4).

Jaettu salaisuus Vetuma-palvelun kutsujan identifioimiseen tarkoitettu tunnus ja merkkisarja (Valtori 2015a, 6).

MAC Message Authentication Code, viestin turvatarkiste, jota käytetään Vetuma-palvelussa lähetetyn viestin eheyden ja lähettäjän todentamiseen (Valtori 2015a, 4).

SHA-256 Eräs MAC-turvatarkisteen laskemiseen käytettävistä tiivistystekniikoista Vetuma-palvelussa (Valtori 2015a, 6).

Opintopolku.fi Valtakunnallinen portaali, jossa opiskelijat voivat mm. vastaanottaa opiskelupaikkansa ammattikorkeakouluunsa (Opetushallitus, [viitattu 23.8.2016]).

OILI-palvelu Valtakunnallinen palvelu, jossa opiskelijat voivat ilmoittautua opiskelijaksi ja lukukaudelle ammattikorkeakouluunsa (Mäki & Raatikainen 2016).

Object Manager SeAMKin itse kehittämä palvelu, jolla mm. luodaan data Luovariin WinhaPron luomasta csv-tiedostosta (Mäkelä 2016).

json-tiedosto JavaScript Object Notation, tiedonvälitykseen tarkoitettu standardoitu tiedostomuoto (Ecma International 2013).

csv-tiedosto Comma Separated Value, standardoitu tiedostomuoto, joka voi sisältää pilkuilla erotettuina eri tyyppistä dataa (Shafranovich 2005).

1 JOHDANTO

1.1 Työn tausta

Verkossa on nykyisin saatavilla monenlaisia palveluja, kuten pankkipalvelut, veroilmoituspalvelut, potilastietopalvelut ja KELA:n palvelut. Näissä palveluissa tarvitaan henkilön vahvaa digitaalista tunnistamista. Digitaalisia tunnistustapoja ovat mm. verkkopankkitunnistautuminen, tunnistautuminen mobiilivarmenteella, tunnistautuminen sähköisellä henkilökortilla, sormenjälkitunnistus ja kasvotunnistus (Valtori 2016; Kuusisto 2014, 15, 18).

SeAMKissa digitaalista tunnistautumista tarvitaan mm. oppilaitoksessa käytössä olevien sovellusten käyttäjätunnusten luovutukseen ja hallintaan.

1.2 Työn tavoite

Tämän opinnäytetyön aiheena on SeAMKin järjestelmien vaatima digitaalinen tunnistautuminen ja SeAMKin Tietohallinnon Helpdeskin eli Jelpparin toimeksiannosta ohjelmoitu sovellus, jolla voidaan luovuttaa uusille SeAMKin opiskelijoille käyttäjätunnukset verkkopankkitunnistautumisen ja mobiilivarmenteen avulla. Sovelluksen tarkoituksena on vähentää sekä Jelpparin että SeAMKin Opiskelijapalveluiden työkuormaa. Tunnistautumalla Vetuma-palvelussa uusi opiskelija voi henkilöllisyyden tarkistuksen jälkeen saada mm. käyttäjätunnuksensa ja sähköpostiosoitteensa omatoimisesti käyttöönsä, paperilla toimitettavien ja allekirjoitettavien tunnusten sijaan. Lisäksi opiskelija voi sovelluksella uusia salasanansa.

Työn tavoitteena on rakentaa SeAMKin opiskelijoille käyttäjätunnusten luovutukseen ja salasanan uusimiseen Vetuma-tunnistautumista hyödyntävä, toimiva ja turvallinen web-sovellus, joka on käyttöliittymältään tarpeeksi selkeä ja helppokäyttöinen.

1.3 Työn rakenne

Luvussa 2 käsitellään digitaalista tunnistautumista yleisellä tasolla ja siltä osin kuin se liittyy kehitettyyn sovellukseen. Luvussa 3 esitellään kehitettyyn sovellukseen liittyviä opiskelijajärjestelmiä, niiden yleisiä ominaisuuksia sekä käyttökohteet. Luvussa 4 esitellään koko uusi sovelluksen myötä mahdolliseksi tuleva käyttäjätunnusten luovutusprosessi. Lisäksi luvussa käsitellään sovelluksen versionhallintaa, tietoturvaa ja testausta. Viimeisessä luvussa 5 kuvataan sovelluksen kehitysprosessia ja luodaan yhteenveto sekä kehitysprosessista että sen tuloksista.

2 DIGITAALINEN TUNNISTAUTUMINEN

Verkkopankkitunnistautumista ja tunnistautumista mobiilivarmenteella käytetään, kun halutaan luotettavasti selvittää jonkin internetissä olevan palvelun käyttäjän henkilöllisyys (JUHTA 2012, 3). Tunnistautumista tarvitaan esimerkiksi, kun halutaan sallia käyttäjälle pääsy hänen henkilökohtaisiin tietoihinsa Kansaneläkelaitoksen verkkoasiointipalvelussa ja halutaan luovuttaa joitain henkilökohtaisia tietoja palveluntarjoajan hallusta (Kela 2016).

Pankit voivat toimia verkkopankkitunnistautumisessa henkilökohtaisten tunnistustietojen välittäjinä pankin järjestelmistä palveluntarjoajalle (Finanssialan keskusliitto 2013, 4). Tunnistautumisessa mobiilivarmenteella tunnistustiedot ovat tallessa henkilön SIM-kortilla, jotka välitetään matkapuhelinoperaattorin välityksellä palveluntarjoajalle (Valtori 2015b, 13).

2.1 Vetuma-palvelu

Vetuma-palvelu on verkossa toimiva kansalaisen tunnistus- ja maksamispalvelu, se on tarkoitettu julkishallinnon organisaatioiden asiointisovellusten käyttöön. Siitä vastaa Valtion tieto- ja viestintätekniikkakeskus Valtori ja sitä ylläpitää Fujitsu Finland Oy. Palvelun avulla asiakas voi tunnistautua ja maksaa kaikissa niissä julkishallinnon verkkopalveluissa, joihin se on liitetty. (Valtori 2016.)

Vetuma-palvelussa on mahdollista tunnistautua verkkopankkitunnuksilla pankkien Tupas-tunnistuspalveluissa, mobiilivarmenteella tai sähköiselle henkilökortille tallennetulla kansalaisvarmenteella. Myös mobiilivarmenne on tietyn tyyppinen kansalaisvarmenne. Verkkomaksaminen tapahtuu Vetuma-palvelussa joko pankkien omilla maksusivuilla tai Nets Oy:n korttimaksupalvelussa. (Valtori 2016.) Käytännössä Vetuma-palvelu integroidaan osaksi palveluntarjoajan sovellusta (JUHTA 2012, 7).

2.2 Tupas-tunnistuspalvelu

Pankit ovat yhteisesti määritelleet Tupas-tunnistuspalvelun. Jokainen pankki vastaa itse omasta Tupas-tunnistuspalvelustaan. Verkkopankkitunnistautuminen tapahtuu pankin Tupas-tunnistussivulla ko. pankin tarjoamilla verkkopankkitunnuksilla. Pankin järjestelmiin on tallennettu pankin asiakkaan tunnistustiedot, jotka tunnistuspalvelu välittää tunnistautumisen onnistuttua palveluntarjoajalle, joka hyödyntää vastaanotettuja tunnistustietoja asiakkaan tunnistamisessa omassa palvelussaan. (Finanssialan keskusliitto 2013, 4.)

Eri pankkien Tupas-tunnistautumiset on integroitu Vetuma-palveluun, josta kutsutaan eri pankkien Tupas-tunnistuspalveluja (JUHTA 2012, 3). Tupas-tunnistuksia voi kuitenkin käyttää erikseenkin, eli Tupas-tunnistuspalvelua voi itse kutsua myös suoraan ja sen voi myös sellaisenaan integroida palveluntarjoajan sovellukseen (Finanssialan keskusliitto 2013, 4).

Tupas-tunnistautumisessa tulee käyttää henkilökohtaisia pankkitunnuksia, jotka on hankittu tekemällä sopimus pankin kanssa. Esimerkiksi tunnuksia, jotka ovat yhteyksissä yritys- tai yhdistystoimintaan, ei voi käyttää. Puolisoilla voi olla yhteinen tili, mutta yleensä verkkopankkitunnukset on myönnetty jommankumman nimellä. Näitä tunnuksia voi tässä tapauksessa käyttää se, jonka nimissä ne ovat. Tarvittaessa pankilta voi pyytää tunnukset molemmille. (Valtiokonttori 2015.)

2.3 Tunnistautuminen mobiilivarmenteella

Mobiilivarmenteen hankkiminen tapahtuu esimerkiksi siten, että kirjautuu matkapuhelinoperaattorin sivuille henkilökohtaisilla verkkopankkitunnuksillaan, jolloin tunnistustiedot tallennetaan asiakkaan puhelimen SIM-kortille, joka tukee mobiilivarmennetta. Tässä vaiheessa myös asetetaan henkilökohtainen tunnusluku, jonka puhelimen varusohjelmisto kysyy asiakkaan tunnistautuessa mobiilivarmenteella. Toinen vaihtoehto on hankkia mobiilivarmenne oman operaattorinsa liikkeestä esittämällä kuvallisen henkilöllisyystodistuksen. (TeliaSonera 2016.)

Tunnistautuminen mobiilivarmenteella tapahtuu niin että tunnistuspalvelu, esimerksi Vetuma-palvelu, pyytää antamaan sen SIM-kortin puhelinnumeron, jolle asiakkaan mobiilivarmenne on tallennettu. Vetuma-palvelu lähettää tunnistuspyynnön matkapuhelinoperaattorille, joka välittää tunnistuspyynnön edelleen asiakkaan mobiililaitteeseen, jonka varusohjelmisto näyttää varmistusviestin, jossa pyydetään syöttämään tunnusluku. Tunnistautumisen onnistuttua mobiililaite lähettää varmenteen sisällön matkapuhelinoperaattorille, joka välittää tiedon edelleen Vetuma-palvelulle. Vetuma-palvelu palauttaa palveluntarjoajan sovellukselle varmenteen sisältämät tunnistustiedot. (Valtori 2015b, 13.)

2.4 Muita tunnistautumispalveluita ja -menetelmiä

Paytrail. Suomessa on käytössä verkkomaksamiseen esimerkiksi Paytrail-palvelu, jossa käytetään samoja verkkopankkitunnuksia kuin Tupas-tunnistautumisessa (Paytrail 2016a). Paytraylilla on yli 100 000 Paytrail-tilin käyttäjää ja se hoitaa yli 10 000 verkkokaupan/-palvelun maksuliikenteen (Paytrail 2016c).

Paytrail-palvelua voi palveluntarjoajan sovelluksesta kutsua kuten Vetuma-palvelua webform-tekniikalla, mutta tarjolla on myös REST-pohjainen ratkaisu, joka on tällä hetkellä beta-vaiheessa (Paytrail 2016b).

Kasvotunnistus. Kasvojen tunnistus on biometrinen tunnistustapa, jossa kasvot kuvataan ja järjestelmä tunnistaa kasvot mittaamalla olennaisten kasvonpiirteiden etäisyyksiä toisistaan, jonka jälkeen se etsii vastaavuutta tietokannasta (Kuusisto 2014, 19).

Suomessa esimerkiksi Helsinki-Vantaan lentoasemalla on käytössä kasvojen tunnistusmenetelmä, joka vertaa asiakkaan biometrisen passin sirun sisältämää kuvaa hänen kasvoihinsa (Automatisoitu rajatarkastus 2016).

Sormenjälkitunnistus. Sormenjälkitunnistus on niin ikään biometrinen tunnistustapa. Sormenjäljet voidaan kerätä joko off-line-menetelmillä eli esimerkiksi valokuvaamalla rikospaikalla tai on-line-menetelmillä, jotka tuottavat digitaalisen kuvan sormenjäljestä skannauksen jälkeen. Yleensä on-line-menetelmillä saadaan tarkempia tuloksia. (Kuusisto 2014, 16-17.)

Esimerkiksi kannettavissa tietokoneissa saattaa olla kapea pyyhkäisysensori, joka muodostaa kuvan sormenjäljestä viipaleittain pyyhkäistäessä sormi sensorin läpi. Tunnistus tapahtuu vertaamalla näitä kuvia tietokannassa oleviin sormenjälkiin. (Kuusisto 2014, 16-17.)

3 OPISKELIJAJÄRJESTELMIIN LIITTYVIÄ PALVELUJA

Tässä luvussa on käsitelty SeAMKissa ja muualla käytössä olevia opiskelijajärjestelmiä niiltä osin kuin ne liittyvät kehitettyyn sovellukseen.

3.1 WinhaPro

CGI:n kehittämä WinhaPro on opintohallinnon perusjärjestelmä, joka kattaa opiskelija- ja opetushallinnossa tarvittavat toiminnallisuudet sisältäen toiminnot opetuksen suunnittelusta todistusten tulostamiseen ja tilastoitavien tietojen poimintaan. WinhaProsta saa myös monipuolisia valmisraportteja todistuksineen. WinhaProhon kirjataan opiskelijoista mm. henkilötiedot, läsnäolotieto ja arvosanat. (CGI Suomi Oy, [viitattu 25.5.2016]; Husa, 2016.)

WinhaPron opiskelijakäyttöliittymä on nimeltään WinhaWille ja henkilökunnan käyttöliittymä WinhaWiivi. Nämä ovat web-liittymiä, jotka on ostettu täydentämään WinhaProta. WinhaWillen kautta opiskelijat mm. ilmoittautuvat kursseille ja läsnä- tai poissaolevaksi lukukausille. WinhaWillesta pystyy myös seuraamaan etenemistään mm. suoritettujen kurssien haun kautta. Sieltä näkyvät myös arvosanat, tietoa siitä miksi jokin kurssisuoritus on hylätty ja kurssien perustietoja, esimerkiksi vastuuopettaja ja kurssien alku- ja loppupäivämäärät. WinhaWillen kautta opiskelija pystyy myös muuttamaan joitain käyttäjätietojaan, kuten puhelinnumeronsa, asuinosoitteensa ja ulkoisen sähköpostiosoitteensa. (CGI Suomi Oy, [viitattu 25.5.2016]; Husa, 2016.)

3.2 Luovari

Luovari on SeAMKin itse kehittämä käyttäjätunnusten luovutussovellus, josta voidaan tulostaa opiskelijan käyttäjätunnustiedot sisältävä lomake. Lomakkeen allekirjoittamalla opiskelijat ovat vastaanottaneet käyttäjätunnuksensa. (Kinnunen 2015.)

Luovari kirjoittaa ja hakee tietoja omasta tietokannastaan, jonne uuden opiskelijan data muodostuu käyttäjätunnuksen luonnin yhteydessä. Data poistuu 30 päivän kuluttua käyttäjätunnusten luovutuksesta ja puolen vuoden kuluessa, jos tunnuksia ei ole niiden muodostumisen jälkeen luovutettu. (SeAMK 2009.)

Tämän opinnäytetyön aiheena olevan uusi järjestelmä korvaa käyttäjätunnusten luovutuksen Luovarin kautta syksystä 2016 alkaen.

3.3 Microsoftin tarjoamia palveluja

Active Directory. Active Directory on Microsoftin kehittämä Windows-toimialueen verkkokäyttöjärjestelmä, jota järjestelmänvalvojat hallinnoivat. Verkkokäyttöjärjestelmät tarjoavat palveluja, kuten autentikointia, auktorisointia ja tilimanipulaatioita ja ne voivat koostua yhdestä tai useammasta palvelimesta. Active Directoryssa data on hierarkkisessa järjestyksessä samoin kuin tiedostojärjestelmässä. Active Directoryyn voi lisätä tietoja käyttäjistä, ryhmistä, tietokoneista, tulostimista, sovelluksista ja palveluista. (Desmond ym. 2013, 2, 5.)

Esimerkkinä autentikoinnista ja auktorisoinnista on tilanne, kun opiskelija kirjautuu jollekin SeAMKin toimialueen tietokoneelle. Tällöin otetaan yhteys Active Directoryyn, tarkistetaan salasana ja annetaan opiskelijalle hänelle kuuluvat oikeudet käyttää tietokonetta. (Kinnunen 2015.)

Forefront Identity Manager. Forefront Identity Manager eli FIM on Microsoftin kehittämä käyttäjän digitaalisen identiteetin, käyttäjätunnusten ja ryhmäyksien hallintapalvelu yrityksessä sen koko elinkaaren ajan luonnista poistoon. FIM integroituu mm. Active Directoryn ja ADAM:in kanssa. (Nordström 2012; Kuja-Lipasti 2016.)

Kun SeAMKissa haetaan dataa primäärilähteestä kuten WinhaProsta tai ADAM-järjestelmästä, FIM käy sen läpi ja tarkistaa onko dataan tullut FIM-palvelun omaan Metaverseen verrattuna muutoksia. FIM-palvelua on laajennettu eri tarkoituksiin rules extensioneilla. FIM on itsessään vain identiteetin hallinnan perusmoottori. Data haetaan esimerkiksi WinhaProsta ajastetusti csv-muodossa. Verrattuaan eri lähteistä haettua dataa Metaverseensä, FIM tekee muutoksia tämän jälkeen Active Di-

rectoryyn tai ADAM-järjestelmään. Esimerkiksi, jos opiskelija on ilmoittautunut jollekin kurssille WinhaProssa, FIM lukee tämän tiedon ja lisää opiskelijan kyseisen kurssin jakelulistalle Active Directoryyn. (Kuja-Lipasti 2016.)

3.4 Valtakunnalliset palvelut

Opintopolku.fi. Opintopolku.fi on valtakunnallinen yhteishakujärjestelmä ja portaali, jossa opiskelijat voivat mm. vastaanottaa ammattikorkeakoulun opiskelupaikkansa. Opintopolku.fi-palvelussa voi myös selailla eri aloja ja tutkintoja, saada tietoa opinnoista, etsiä ajankohtaisia koulutuksia, hakea koulutuksiin, tutustua valintaperusteisiin sekä katsoa videoita ja lukea tekstejä opiskelijoiden omista kokemuksista. (Opetushallitus, [viitattu 23.8.2016].)

OILI. OILI-palvelu eli Opiskelijaksi-ilmoittautuminen ja lukukausi-ilmoittautuminen on valtakunnallinen palvelu, jossa opiskelijat voivat saumattomasti ja sähköisesti ilmoittautua opiskelijaksi ja lukukaudelle ammattikorkeakouluunsa (Mäki & Raatikainen 2016).

Palvelu on kaikille ammattikorkeakouluille yhteinen ja se on tarkoitettu sekä ilmoittautuville opiskelijoille että ilmoittautumispalvelua ohjaaville korkeakoulujen ja yliopilaskuntien tai opiskelijakuntien virkailijoille (Mäki & Raatikainen 2016).

4 KÄYTTÄJÄTUNNUSTEN LUOVUTUS KEHITETYLLÄ SOVELLUKSELLA

Käyttäjätunnusten luovutussovellusta varten tarvittiin tarpeeksi laaja, käytännössä kaikilla palvelun käyttäjillä käytössä oleva digitaalinen tunnistautumismenetelmä. Sovelluksen tarpeisiin valittiin verkkopankkitunnistautuminen ja tunnistautuminen mobiilivarmenteella. Nämä ovat tarpeeksi yleisiä digitaalisia tunnistusmuotoja, joiden vahvalla tunnistautumisella voidaan selvittää mm. käyttäjän henkilötunnus, jonka avulla koulun järjestelmistä haetaan tarvittavat tiedot. Tunnistautuminen sähköisellä henkilökortilla jätettiin pois, koska se ei ole yhtä laajassa käytössä.

SeAMKilla oli ennen sovelluksen kehitysprosessiin alkua jo valmiiksi monen pankin kanssa Tupas-sopimus, mistä syystä sovellus päätettiin kehittää nimenomaan Tupas-tunnistautumisiin perustuen. Vetuma-palvelu valittiin kuitenkin erillisten Tupas-tunnistuspalveluiden integroimisen sijaan siksi, että näin sovelluksen tarvitsee kutsua vain Vetuma-palvelua yhdellä jaetulla salaisuudella. Vetuma-palvelusta voidaan taas kutsua kaikkien niiden eri pankkien Tupas-tunnistuspalvelua, joiden kanssa SeAMKilla on Tupas-sopimus. Ilman Vetuma-palvelua sovellukseen olisi pitänyt ohjelmoida kaikille näille pankeille jaettu salaisuus erikseen. Lisäksi eri pankkien Tupas-tunnistautumiset oli jo valmiiksi liitetty aiempien SeAMKin projektien vuoksi Vetuma-palveluun, joten uutta Vetuma-tilaustakaan ei tarvinnut tehdä. Tilausta varten kaikkien liitettävien pankkien Tupas-tunnistautumisten jaetut avaimet olisi pitänyt toimittaa Fujitsulle.

4.1 Käyttäjätunnusten luovutusprosessi

Aiemmin, kun opiskelijalle oli muodostunut SeAMKin järjestelmiin tunnukset, niiden luovutus toteutettiin tulostamalla SeAMKin itse kehittämästä käyttäjätunnusten luovutussovellus Luovarista käyttäjätunnusten luovutuslomake. Allekirjoittamalla ja palauttamalla lomakkeen opiskelija vastaanotti omat käyttäjätunnuksensa.

Nyt kehitetyn sovelluksen myötä opiskelija voi omatoimisesti vastaanottaa tunnuksensa tunnistautumalla ensin verkkopankkitunnuksillaan tai mobiilivarmenteella.

Seuraavassa uusi käyttäjätunnusten luovutusprosessi lyhyesti:

1. Opiskelupaikan vastaanotto valtakunnallisessa yhteishakujärjestelmä Opintopolku.fi:ssä.

2. Ilmoittautuminen opiskelijaksi verkkopankkitunnuksilla valtakunnallisessa OILI-palvelussa. SeAMKin uudelle opiskelijalle luodaan käyttäjätunnukset, jotka on mahdollista luovuttaa parin päivän kuluttua tästä. Parin päivän viive johtuu käyttäjätunnusten muodostumisen viemästä ajasta.

3. Siirrytään osoitteeseen https://tunnukset.seamk.fi. Hyväksytään Seinäjoen Ammattikorkeakoulun tietokoneiden ja tietoverkon käyttösäännöt ja siirrytään Vetuma-palveluun tunnistautumaan.

4. Verkkopankkitunnistautuminen Vetuma-palvelussa, josta on paluu palvelun-tarjoajan sovellukseen. Toinen vaihtoehto on tunnistautuminen mobiilivar-menteella.

5. Sovellus tarkistaa WinhaProsta, onko SeAMKilla kyseisen henkilötunnuksen omaava opiskelija. Jos opiskelijan tiedot löytyvät, sovellus näyttää opiskelija-numeron WinhaProsta.

6. Sovellus hakee käyttäjätunnuksen opiskelijanumeron perusteella Active Di-rectorysta, jos se löytyy, näytetään sekin.

7. Sovellus etsii opiskelijan tietoja Luovarista. Jos käyttäjätunnuksia ei ole vielä luovutettu, sovellus näyttää myös Luovarista haetut tiedot käyttäjälle.

8. Sovelluksella voidaan asettaa käyttäjälle uusi salasana SeAMKin Active Di-rectoryyn. Kun opiskelija kirjautuu käyttäjätunnuksillaan johonkin SeAMKilla käytössä olevaan palveluun, salasana tarkistetaan nimenomaan Active Di-rectorysta.

4.2 Kehitys- ja palvelinympäristö

SeAMKin järjestelmät ovat pääosin toteutettu Microsoftin tuotteilla. Käytössä on mm. Forefront Identity Manager, Active Directory, Outlook Web Server sekä Windows-työasemat ja muita Windows-palvelimia. Käytössä on lisäksi mm. joitain Linux-pohjaisia järjestelmiä.

Sovellusta varten asennettiin oma palvelimensa, jolla sovellusta myös testattiin. Ottaen huomioon jo käytössä olevat SeAMKin järjestelmät, luonnollinen valinta oli, että palvelimen käyttöjärjestelmäksi valittiin Microsoft Windows Server 2012 R2, joka oli valintahetkellä kyseisen palvelinkäyttöjärjestelmän uusin versio. Valittuun käyttöjärjestelmään sisältyy Internet Information Services 8.5 -palvelinohjelmisto, jolle sovellus asennettiin. Myös ohjelmointikieleksi valittiin näin ollen Microsoftin kehittämä ASP.NET/C#.

Sovelluksen kehityksessä käytettiin ohjelmointialustana Microsoftin Visual Studio 2013 Ultimatea. Itse ohjelmointiin käytettiin myös Notepad++-sovellusta keveytensä vuoksi.

4.3 Uuden opiskelijan tietojen muodostuminen SeAMKin järjestelmiin

Perustapauksessa opiskelija vastaanottaa opiskelupaikan sähköisesti valtakunnallisessa Opintopolku.fi-yhteishakujärjestelmästä ja siirtyy ilmoittautumaan läsnä- tai poissaolevaksi niin ikään valtakunnalliseen OILI-palveluun. OILI-palvelusta ladataan manuaalisesti opiskelijan tiedot sisältävä json-muotoinen tiedosto, jonka tiedot hieman ohjelmallisesti muokattuna viedään WinhaProhon. (Husa 2016.)

WinhaProssa luodaan csv-tiedosto, josta tiettyjen FIM-palveluun tehtyjen rules extensioneiden perusteella luodaan käyttäjätunnukset FIM-palvelun kautta Active Directoryyn. FIM-palvelussa säilyvät Metaverse-tiedot opiskelijasta. FIM-palveluun viedään kaikki opiskelijadata ja Active Directoryyn viedään vain osa FIM-palvelun datasta. Lisäksi SeAMKin itse kehittämä Object Manager luo datan opiskelijoille Luovarin tietokantaan samasta WinhaPron luomasta csv-tiedostosta. (Mäkelä 2016.)

4.4 Vetuma-palvelun integroiminen palveluntarjoajan sovellukseen

Vetuma-tunnistautumispyyntö palveluntarjoajan sovelluksesta Vetuma-palveluun tehdään lähettämällä http post -tekniikalla Vetuman tunnistautumisosoitteeseen määritellyt html-lomakkeen input-kenttien attribuutit. Tämän jälkeen siirrytään kyseiseen tunnistautumisosoitteeseen tunnistautumaan. Kutsu tapahtuu sovelluksen ”Siirry Vetuma-palveluun tunnistautumaan”-painekkeesta (kuva 1). Vetuma-palvelu sisältää sekä tuotanto- että testiympäristön, jotka vastaavat käyttöliittymältään toisiaan, mutta joiden kutsuissa käytetään kumpaankin tilanteeseen tarkoitettuja jaettuja salaisuuksia ja internet-osoitteita. Testiympäristössä toimivat testitunnukset ja tuotantoympäristössä oikeat tunnukset.

Kuva 1. Siirtyminen tunnistautumaan Vetuma-palveluun.

Palveluntarjoajan sovellus voi kutsua Vetuma-palvelua esimerkiksi palauttamalla selaimelle seuraavanlaisen html-sivun, jossa on Vetuma-testitunnistautumisen kutsuparametreja html-lomakkeessa piilokenttinä, jotka eivät näy käyttäjälle:

```
...
<form method="post"
action="https://testitunnistus.suomi.fi/VETUMALogin/app">
<input name="RCVID" type="hidden" value="TESTIASIAKAS11" />
<input name="APPID" type="hidden" value="VETUMA-APP2" />
<input name="TIMESTMP" type="hidden" value="20061218151424309" />
<input name="SO" type="hidden" value="6" />
<input name="SOLIST" type="hidden" value="1,6" />
<input name="TYPE" type="hidden" value="LOGIN" />
<input name="AU" type="hidden" value="EXTAUTH" />
<input name="LG" type="hidden" value="fi" />
<input name="RETURL" type="hidden" value="https://localhost/Re-
turn.aspx"/>
<input name="CANURL" type="hidden" value="https://localhost" />
<input name="ERRURL" type="hidden" value="https://localhost" />
<input name="AP" type="hidden" value="TESTIASIAKAS1" />
<input name="MAC" type="hidden"
value="72A72A046BD5561BD1C47F3B77FC9456AD58C9C428CACF44D502834C9F8C
02A3" />
<input name="TRID" type="hidden" value="trid1234567890" />
<input type="submit" value="Siirry Vetuma-palveluun tunnistautu-
maan" />
</form>
...
```

Samalla tavalla kaikissa kutsutyypeissä esiintyvät Vetuma-rajapinnan parametrit on lueteltu taulukossa 1. Turvatarkiste lähetettävästä datasta täytyy ohjelmallisesti laskea muiden parametrien arvoista taulukon indeksin osoittamassa järjestyksessä ilman MAC-arvoa. Viimeisenä annetaan pankilta saatu tai tässä tapauksessa testaukseen tarkoitettu jaettu salaisuus. SHA256-metodilla tiivistettävä turvatarkistelauseke on tässä tapauksessa:

```
TESTIASIAKAS11&
VETUMA-APP2&
20061218151424309&
6&1,6&LOGIN&EXTAUTH&fi&
https://localhost/Return.aspx&
https://localhost&
https://localhost&
TESTIASIAKAS1&
trid1234567890&
TESTIASIAKAS11-
617DC7C1714500BB7837C0B9486B67405FC66B0687C599E2400B57F10F0E1660&
```

Taulukko 1. Vetuma-kutsujen yleiset parametrit.
(Valtori 2015a, 7)

Nro	**Nimi**	**Merkitys**
1	RCVID	Kutsun suojauksessa käytetyn jaetun salaisuuden tunnus
2	APPID	Vetuma-palvelua kutsuvan asiointisovelluksen tunnus
3	TIMESTMP	Kutsun aikaleima
4	SO	Oletusmenetelmä 1)
5	SOLIST	Käyttäjälle tarjottavat menetelmät 1)
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
1) Näiden parametrien käytössä on toimintokohtaisia vivahde-eroja. Ne on kuvattu tarkemmin kunkin toimintokohtaisten kutsutyypin yhteydessä tämän taulukon lähteenä olevassa Vetuman kutsurajapinnan määrittelydokumentissa.		

Kun siirrytään Vetuma-palveluun palveluntarjoajan sovelluksesta, tehdään valinta Tupas-tunnistautumisen ja mobiilivarmenteella toimivan tunnistuksen välillä (kuva 2). Tässä selostuksessa on käytetty Tupas-tunnistautumista.

Kuva 2. Tunnistustavan valinta Vetuma-palvelussa.

Vetuma-palvelua varten tehdään jokaisen pankin kanssa erikseen Tupas-sopimus. Sopimusten teon yhteydessä saadaan pankkikohtaiset jaetut salaisuudet, joilla identifioidaan tunnistusta pyytävä taho. Nämä tunnukset SeAMK on toimittanut Fujitsulle. Vetuma-palvelussa on Tupas-tunnistautumisten päänäkymä, jossa Tupas-tunnistuksen vaihtoehtoina ovat kaikki pankit, joiden kanssa SeAMKilla on sopimus (kuva 3). Tunnistautuminen mobiilivarmenteella tulee mahdolliseksi automaattisesti Vetuma-sopimuksen myötä. Fujitsulla luotiin pyynnöstä sovellusta varten Vetuma-palveluun uusi jaettu salaisuus, jolla identifioidaan, että Vetuma-palvelua kutsuu SeAMK.

Kuva 3. Pankin valinta Vetuma-palvelussa.

Tupas-tunnistautumisen jälkeen Vetuma-palvelusta palataan palveluntarjoajan sovellukseen tunnistustietojen kanssa, jotka Vetuma-palvelu palauttaa sovelluksen paluuosoitteeseen post datana. Vastausviestien turvatarkisteen laskenta tapahtuu samoin kuin kutsujen. Samalla tavalla kaikissa vastaustyypeissä esiintyvät Vetuma-rajapinnan parametrit on lueteltu taulukossa 2.

Taulukko 2. Vetuma-vastausten yleiset parametrit.
(Valtori 2015a, 14)

Nro	Nimi	Merkitys
1	RCVID	Vastauksen suojauksessa käytetyn jaetun salaisuuden tunnus
3	TIMESTMP	Vastauksen aikaleima
4	SO	Käytetty menetelmä 1)
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.
1) Parametrin SO tulkinnoissa on toimintokohtaisia vivahde-eroja. SO-parametri toimintokohtaisine tulkintoineen on kuvattu tarkemmin kunkin toimintokohtaisten vastaustyypin yhteydessä tämän taulukon lähteenä olevassa Vetuman kutsurajapinnan määrittelydokumentissa.		

4.5 SeAMKin järjestelmien integroiminen palveluntarjoajan sovellukseen

Vastaanotetun post datan perusteella palveluntarjoajan sovellus palauttaa kuvan 4 tyyppiset tiedot, jotka se hakee eri lähteistä.

Kuva 4. Sovelluksen näyttämät käyttäjätiedot.

4.5.1 WinhaPro

WinhaProsta tarkistetaan Vetumalta saadulla henkilötunnuksella, onko SeAMKilla kyseisen henkilötunnuksen omaava läsnäoleva opiskelija. Jos opiskelija löytyy, sovellus hakee WinhaPron raporttikannasta henkilön opiskelija- eli roolinumeron. WinhaProssa on sql-tietokantoina tuotantokanta, jonne WinhaPro kirjaa pääasiallisen datan, ja raporttikanta, jonne WinhaPro raportoi uuden datan kerran vuorokaudessa.

Sovellusta varten luotiin tunnus, jolla on lukuoikeudet WinhaPron raporttitietokannan näkymään, joka palauttaa läsnäolevien opiskelijoiden roolinumeron, oppijanumeron, sukunimen, etunimet, kutsumanimen sekä henkilötunnuksen. Roolinumero on opiskelijan senhetkisen opiskelun tunnus ja oppijanumero on opiskelijan valtakunnallinen tunnus.

Sovellus ottaa yhteyden lähiverkon kautta WinhaPron raporttitietokantaan ODBC DSN -tekniikalla. Raporttitietokanta on eri palvelimella kuin kehitetty sovellus. Tämä johtuu siitä, että oli turvallisempaa kehittää sovellusta omalla palvelimellaan kuin esimerkiksi WinhaPron palvelimella. Lisäksi sovelluksen kehitykseen käytetylle palvelimelle oli tehty asetukset jo valmiiksi, joten oli järkevää jättää julkaistukin sovellus samalle palvelimelle.

Samalla henkilötunnuksella voi olla useampi kuin yksi läsnäoleva roolinumero, mutta näitä opiskelijoita on vain vähän. Roolinumeron haku WinhaProsta henkilötunnuksella ohjelmoitiin palauttamaan vanhempi eli numerollisesti pienempi roolinumero. Tämä on toivottavaa, sillä opiskelijalla säilyy käyttäjätunnuksena vanhemmasta roolinumerosta johdettu käyttäjätunnus.

4.5.2 Active Directory

Kehitetty sovellus näyttää opiskelijan käyttäjätunnuksen, jos opiskelijanumeroa vastaava käyttäjätunnus löytyy Active Directorysta. SeAMKin Active Directory, samoin

kuin WinhaPro, sijaitsee eri palvelimella kuin kehitetty sovellus. Tämä johtuu samoista syistä kuin WinhaPron yhteydessä. Active Directoryyn voidaan ohjelmallisesti ottaa yhteys ja hakea tietoja lähiverkon kautta LDAP-tekniikalla.

Active Directorysta haetaan käyttäjätunnuksen lisäksi myös opiskelijan koko nimi, jota käytetään salasanan uusimisen validoinnissa.

4.5.3 Luovari

Luovarin tietokanta, jonne sovellus ottaa yhteyden ja josta se hakee tietoja kuten WinhaPron tietokannasta, sijaitsee myös eri palvelimella kuin kehitetty sovellus.

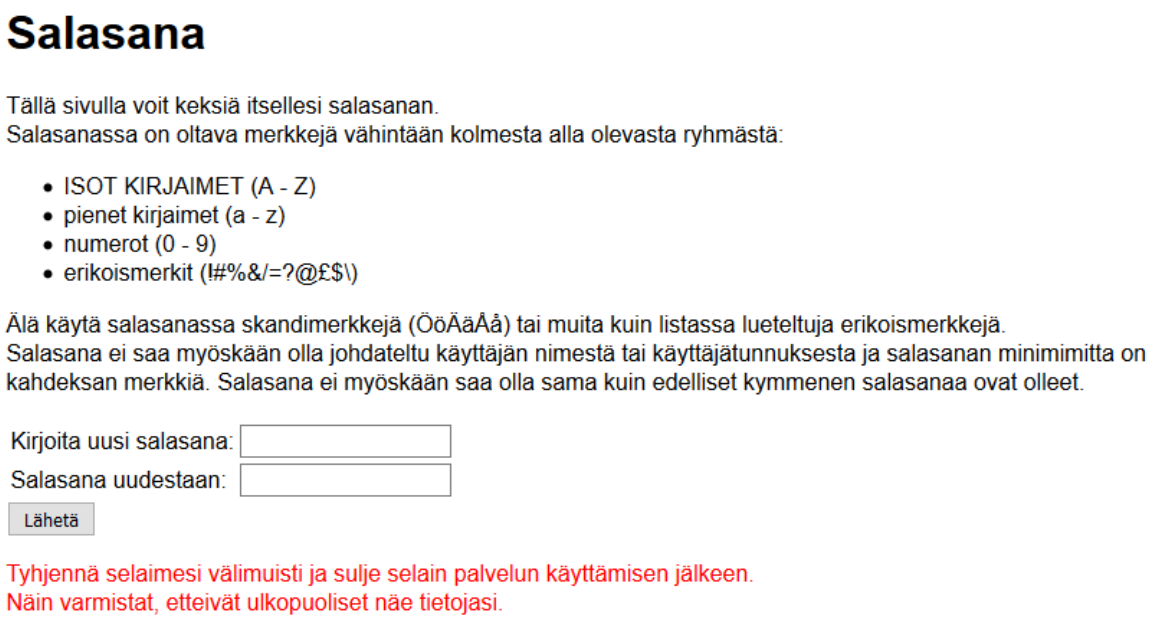
Kun sovellus luovuttaa käyttäjätunnukset opiskelijalle, Luovarin tietokantaan päivitetään kyseisen opiskelijan kohdalle luovutettu-merkintä päivämäärineen ja luovuttajineen. Tässä tapauksessa luovuttaja on opiskelija itse.

Luovarista haetaan loputkin kuvan 4 tiedot, jos Active Directorysta löytyy opiskelijan käyttäjätunnus.

4.5.4 Salasanan uusiminen

Opiskelijan salasanan uusimisessa Active Directoryyn (salasana tarkistetaan Active Directorysta kun opiskelija kirjautuu johonkin SeAMKilla käytössä olevaan järjestelmään käyttäjätunnuksillaan ja salasanallaan) otetaan kuvan 5 ehdot huomioon eikä sovellus suostu etenemään ennen kuin ehdot on täytetty. Tämä tehdään palvelimella muodostettavalla validointilausekkeella.

Jos opiskelija on jo aiemmin vastaanottanut käyttäjätunnuksensa, niitä ei luovuteta uudestaan ja sovellus näyttää opiskelijalle vain hänen käyttäjätunnuksensa ja opiskelijanumeronsa. Erillistä valintaa käyttäjätunnusten luovutuksen ja salasanan uusimisen välillä ei tarvitse tehdä, vaan sovellus ottaa nämä tilanteet huomioon sen mukaan, onko opiskelijalla Luovarin tietokannassa käyttäjätunnusten luovutusmerkintä.



Kuva 5. Salasanan uusiminen sovelluksella.

4.6 Versionhallinta

Sovelluksen kehityskaari tallennettiin SeAMKilla käytössä olevalle TortoiseSVN-versionhallintapalvelimelle. Uuden version siirroissa palvelimelle käytettiin Windowsin resurssienhallintaan integroituvaa TortoiseSVN-asiakasohjelmaa.

Jokaiselle uudelle versiolle kirjoitettiin selventävä otsikko, mitä on lisätty, muutettu tai poistettu. Opinnäytetyön kirjoitushetkellä näitä sovellusversioita oli yli 30. Versiohistoria muodostui lineaariseksi, eli ei ollut tarpeen tehdä esimerkiksi haaraumia mahdollisille eri ohjelmoimissuunnille. Sovelluskehityksessä oli välillä kuitenkin tarpeen palata aiempaan sovellusversioon.

4.7 Tietoturva

Sovellusta varten asennettiin oma palvelimensa, jolle ei asennettu muita sovelluksia. Tämä on tietoturvan kannalta hyvä asia, mm. sen takia, että näin palvelimella ei ole avattuna ylimääräisiä portteja, mikä saattaisi johtaa ulkopuolisten pääsyn palvelimelle.

Lisäksi huolehdittiin, että sovelluksessa on vain tarvittavat ominaisuudet, jotta sovellus ei palauta ylimääräistä dataa. Sovellus konfiguroitiin palauttamaan kustomoitu ilmoitussivu, jos sovellus menee virhetilaan. Näin vältytään paljastamasta koodia ulkopuolisille käyttäjille.

Sovellus käännettiin yhteen DLL-tiedostoon, jotta mahdollisten palvelimelle tunkeutujien olisi hankalampi lukea sovelluksen tiedostoja.

Palvelimeen konfiguroitiin varmenteellinen SSL-salaus. Sovellus ohjaa selaimen käyttämään https-protokollaa, vaikka käyttäjä ei olisi sitä osoiteriville kirjoittanutkaan.

Kun sovellus lähettää http post -kutsun Vetuma-palvelulle, käytetään https-protokollaa. Lisäksi sovellus laskee lähettävistä tiedoista MAC-turvatarkisteen, jonka sovellus lähettää Vetuma-palvelulle lähettäjän todentamiseksi ja lähetettävän datan eheyden tarkistamiseksi. Samoin kun sovellus vastaanottaa Vetuma-palvelulta post datan, lasketaan turvatarkiste. (Valtori 2015b, 5.)

Sovelluksen palvelimen ja SeAMKin järjestelmien välillä käytetään SSL-salausta.

4.8 Sovelluksen testaus

Sovellusta testattiin uusilla SeAMKin opiskelijoilla, joille luovutettiin sovelluksella käyttäjätunnukset sekä opiskelijoilla, joita Jelpparista ohjattiin uusimaan sovelluksella salasanansa. Pääasiassa palaute on ollut positiivista.

Aluksi muutamilla opiskelijoilla oli ongelmia sovelluksen kanssa. Kyseessä oli Vetuma-palvelulta vastaanotettavan post datan MAC-turvatarkisteen laskentaongelma, joka paljastui, kun ongelmaa tutkittiin aidoilla pankkitunnuksilla, joiden omistajan nimi sisältää ä-kirjaimia. Sovelluksesta rakennettiin ongelman vuoksi analysoivampi versio, jonka avulla selvisi, että oli jäänyt huomioimatta, että suomenkielisissä nimissä on skandimerkkejä. Sovellus ei niitä ymmärtänyt, joten se konfiguroitiin käyttämään ISO-8859-1-standardia, joka sisältää mm. skandimerkit.

Sovelluksesta on ollut apua esimerkiksi tilanteessa, jossa opiskelija oli unohtanut salasanansa ja hänen puhelinnumeronsa oli myös vaihtunut. SeAMKissa käytössä

oleva palvelua, jolla salasanan voi uusia tekstiviestillä, ei voinut käyttää. Lisäksi henkilö asui 200 kilometrin päässä Jelpparin toimistosta, eikä voinut tulla esittämään henkilöllisyystodistusta paikan päälle salasanan uusimista varten. Henkilö ohjattiinkin uusimaan salasanansa kehitetyssä sovelluksessa verkkopankkitunnustensa tai mobiilivarmenteen avulla, ja hän sai tunnukset jälleen käyttöönsä.

5 POHDINTAA

Työ aloitettiin etsimällä internetistä ohjeita Tupas-tunnistautumiseen liittyen. Verkosta löytyi Tupas-tunnistautumisen testauksen koodiesimerkkejä php-ohjelmointikielellä (Ohjelmointiputka 2009), joita hieman muokkaamalla saatiin toimimaan tunnistautuminen Nordea-pankkiin heidän omilla testitunnuksillaan. Tässä vaiheessa Tupaksen testaamisessa käytettiin Apache/php-kehitysympäristöä.

Tässä vaiheessa kuitenkin pohdittiin, kannattaisiko sovellus sittenkin toteuttaa ASP.NET-tekniikalla php:n sijaan, sillä SeAMKin sivustot toimivat yleensä Microsoftin Internet Information Services -palvelinohjelmiston päällä ja ne käyttävät laajasti ASP.NET-pohjaisia ratkaisuja. Näin ei myöskään tarvitsisi erikseen huolehtia sovelluksen palvelimelle vähemmän käytössä olevan php:n päivityksistä.

Lisäksi pohdittiin, sisältääkö ASP.NET tarvittavat koodikirjastot. Koska ASP.NET on palvelimella toimiva, esimerkiksi täyttä C#-tukea tarjoava kieli, ASP.NET tarjoaa riittävästi ominaisuuksia web-sovelluksen toteutuspohjaksi, jotta tarvittavat ohjelmointikielen tuottamat edellytykset sovelluksen tekemiseksi ovat olemassa. Sovelluksen jatkokehitys tapahtui ASP.NET/C#-muodossa sen jälkeen, kun sovellus oli käännetty php-kielestä ASP.NET-kielelle.

Jossain vaiheessa mietittiin, voisiko tässä yhteydessä käyttää SeAMKilla käytössä olevan Eduixin E-lomakkeiden Vetuma-tunnistautumista. E-lomakkeet hyödyntävät Vetuma-palvelun tunnistautumista ja maksamista. Tästä kuitenkin luovuttiin, koska palvelua ei pystynyt järkevästi integroimaan palveluntarjoajan sovellukseen.

Sovelluksen kehitys oli mielenkiintoista ja sujui joutuisasti. Ohjelmoinnin edetessä käytiin keskustelua Jelpparin ja muiden SeAMKin ja Koulutuskeskus Sedun työntekijöiden kanssa siitä, miten sovelluksen tulisi toimia. Palautteen mukaan sovellusta muokattiin haluttuun muotoon.

Ohjelmointivaiheen lopputuloksena syntyi toimiva web-sovellus, joka täytti toimeksiannon. Sovellus suorittaa varmatoimisesti käyttäjätunnusten luovutuksen sekä salasanan uusimisen. Sovellus myös esimerkiksi kertoo, jos opiskelijanumeroa ei

löydy WinhaProsta. Tällöin opiskelijalle ei vielä ole ehtinyt muodostua tietoja WinhaProhon tai henkilö ei ole läsnäolevana opiskelijana SeAMKissa. Jos taas opiskelijalle ei löydy käyttäjätunnusta Active Directorysta, sovellus ei siitä erikseen ilmoita sanallisesti, vaan jättää käyttäjätunnusrivin näyttämättä. Tässä tapauksessa ei myöskään etsitä opiskelijan tietoja Luovarista eikä käyttäjätunnuksia voida luovuttaa. Jos käyttäjätunnukset taas on jo luovutettu, sovellus kertoo sen sanallisesti. Silloin kun käyttäjätunnukset luovutetaan, sovellus kehottaa ottamaan tiedot talteen. Sovelluksella pystyy uusimaan salasanansa vain kerran yhden istunnon aikana.

LÄHTEET

Automatisoitu rajatarkastus. 2016. [Verkkosivu]. Helsinki: Rajavartiolaitos. [Viitattu: 5.10.2016]. Saatavana: http://www.raja.fi/ohjeita/automatisoitu_rajatarkastus

Beal, V. 2016. What is .NET Framework? Webopedia Definition. [Verkkosivu]. Foster City: QuinStreet Inc. [Viitattu 23.8.2016]. Saatavana: http://www.webopedia.com/TERM/D/dot_NET_Framework.html

CGI Suomi Oy. Ei päiväystä. WinhaPro – Opintohallinnon kokonaisjärjestelmä. [Verkkosivu]. CGI Suomi Oy - Consultants to Government and Industry. [Viitattu 23.8.2016]. Saatavana: http://www.cgi.fi/tuoteratkaisut/winhapro

Desmond, B., Richards, J., Allen, R. & Lowe-Norris, A. G. 2013. Active Directory: Designing, Deploying, and Running Active Directory. 5. painos. Beijing, Sebastopol: O'Reilly Media, Inc.

Ecma International. 2013. The JSON Data Interchange Format. [Verkkojulkaisu]. Ecma International - European association for standardizing information and communication systems. 10.2013. [Viitattu 10.10.2016]. Saatavana: http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-404.pdf

Finanssialan keskusliitto. 2013. Pankkien Tupas-tunnistuspalvelun tunnistusperiaatteet V2.0c. 2.12.2013. [Verkkojulkaisu]. [Viitattu 5.10.2016]. Saatavana: http://www.finanssiala.fi/maksujenvalitys/dokumentit/Tupas_tunnistusperiaatteet_v20c.pdf

Husa, H. 2016. Järjestelmäsuunnittelija. Seinäjoen Ammattikorkeakoulun Tietohallinto. Haastattelu 25.5.2016.

JUHTA. 2012. JHS 164 Tunnistautuminen ja maksaminen sähköisessä asioinnissa VETUMA-palvelun avulla [Verkkojulkaisu]. JUHTA - Julkisen hallinnon tietohallinnon neuvottelukunta. 5.10.2012. [Viitattu 12.4.2016]. Saatavana: http://docs.jhs-suositukset.fi/jhs-suositukset/JHS164/JHS164.pdf

Kela. 2016. Asiointipalvelun henkilöasiakkaille – kela.fi. [Verkkosivusto]. Kansaneläkelaitos. 6.5.2016. [Viitattu 29.3.2016]. Saatavana: http://www.kela.fi/asiointi

Kinnunen, J. 2015. Atk-tukihenkilö. Seinäjoen Ammattikorkeakoulun Tietohallinnon Helpdesk Jelppari. Haastattelu 1.10.2015.

Kuja-Lipasti, M. 2016. Atk-suunnittelija. Koulutuskeskus Sedu. Haastattelu 29.8.2016.

Kuusisto, H. 2014. Biometrinen Tunnistus. [Verkkojulkaisu]. Pori: Satakunnan ammattikorkeakoulu. Tietojenkäsittelyn koulutusohjelma. Opinnäytetyö. [Viitattu 12.4.2016]. Saatavana: http://urn.fi/URN:NBN:fi:amk-2014112817315

Microsoft. 2014. What Is Active Directory Application Mode? [Verkkosivu]. Microsoft Corporation. 19.11.2014. [Viitattu 5.10.2016]. Saatavana: https://technet.microsoft.com/en-us/library/cc738377(v=ws.10).aspx

Microsoft. 2016a. C#. [Verkkosivu]. Microsoft Corporation. [Viitattu 23.8.2016]. Saatavana: https://msdn.microsoft.com/en-us/library/kx37x362.aspx

Microsoft. 2016b. ASP.NET. [Verkkosivusto]. Microsoft Corporation. [Viitattu 23.8.2016]. Saatavana: http://www.asp.net

Microsoft. 2016c. TN Rules Extensions. [Verkkosivu]. Microsoft Corporation. [Viitattu 5.10.2016]. Saatavana: https://technet.microsoft.com/en-us/library/jj590309%28v=ws.10%29.aspx

Mäkelä, V-M. 2016. Atk-suunnittelija. Seinäjoen Ammattikorkeakoulun Tietohallinto. Haastattelu 25.5.2016.

Mäki, A. & Raatikainen, O. 2016. OILI - Opiskelijaksi-ilmoittautuminen ja lukukausi-ilmoittautuminen - CSC Wiki. [Verkkosivusto]. Espoo: CSC - TIETEEN TIETOTEKNIIKAN KESKUS OY. 5.7.2016. [Viitattu 23.8.2016]. Saatavana: https://confluence.csc.fi/display/OILI/OILI

Nordström, K. 2012. Microsoft Forefront Identity Manager 2010 R2 Handbook. [Verkkokirja]. Birmingham: Packt Publishing Ltd. [Viitattu 23.8.2016]. Saatavana Ebrary-tietokannasta. Vaatii käyttöoikeuden.

Ohjelmointiputka. 2009. Keskustelu: Tupas testaus. 30.6.2009. [Verkkosivu]. [Viitattu: 14.4.2016]. Saatavana: http://www.ohjelmointiputka.net/keskustelu/19329-tupas-testaus/sivu-1

Opetushallitus. Ei päiväystä. Opintopolku. [Verkkosivusto]. [Viitattu 23.8.2016]. Saatavana: https://opintopolku.fi/wp/fi/

Paytrail. 2016a. Paytrail - Integration guide, v3.6. [Verkkojulkaisu]. Jyväskylä: Paytrail Oyj. 19.1.2016. [Viitattu 12.4.2016]. Saatavana: http://docs.paytrail.com/en/index-all.html

Paytrail. 2016b. Paytrail - Kehittäjille - FORM- ja REST-rajapinnat. [Verkkosivu]. Jyväskylä: Paytrail Oyj. [Viitattu 5.10.2016]. Saatavana: https://www.paytrail.com/kehittajille-form-ja-rest-rajapinnat

Paytrail. 2016c. Paytrail - Tarinamme. [Verkkosivu]. Jyväskylä: Paytrail Oyj. [Viitattu 6.10.2016]. Saatavana: https://www.paytrail.com/tarinamme

SeAMK. 2009. Luovari - Käyttäjätunnusten luovutus. [Verkkosivu]. Seinäjoki: Seinäjoen Ammattikorkeakoulu. [Viitattu: 23.8.2016]. Saatavana: https://directory.seamk.fi/Luovari/Default.aspx Vaatii käyttöoikeuden.

Shafranovich, Y. 2005. RFC 4180 - Common Format and MIME Type for Comma-Separated Values (CSV) Files. [Verkkojulkaisu]. SolidMatrix Technologies, Inc. [Viitattu: 23.8.2016]. Saatavana: https://tools.ietf.org/html/rfc4180

TeliaSonera Finland Oyj. 2016. Sonera Mobiilivarmenne - Apu & Tuki - Sonera. [Verkkosivu]. Telia Company AB. [Viitattu 24.8.2016]. Saatavana: https://www.sonera.fi/asiakastuki/ohjeet/Sonera-Mobiilivarmenne?id=1241

Valtiokonttori. 6.6.2015. Tunnistautuminen pankkitunnuksilla - Suomi.fi. [Verkkosivu]. [Viitattu 14.4.2016]. Saatavana: https://www.suomi.fi/suomifi/suomi/asioi_verkossa/sahkoinen_tunnistus_ja_allekirjoitus/tunnistautuminen_pankkitunnuksilla/index.html

Valtori. 2015a. Suomalaisen julkishallinnon Vetuma-palvelu - Kutsurajapinnan määrittely - versio 3.5. [Verkkojulkaisu]. Jyväskylä: Valtion tieto- ja viestintätekniikka-keskus Valtori. 3.11.2015. [Viitattu: 13.10.2016]. Saatavana: http://www.valtori.fi/download/noname/%7BC038BD35-9E05-48E2-A517-CC8C522F535E%7D/12946

Valtori. 2015b. Suomalaisen julkishallinnon Vetuma-palvelu - Sovelluksille tarjotun toiminnallisuuden kuvaus - versio 3.5.1. [Verkkojulkaisu]. Jyväskylä: Valtion tieto- ja viestintätekniikka-keskus Valtori. 16.12.2015. [Viitattu: 13.10.2016]. Saatavana: http://www.valtori.fi/download/noname/%7BB6D4B783-146C-4712-826B-409B168805B1%7D/12944

Valtori. 2016. Kansalaisen tunnistus- ja maksamispalvelu Vetuma. [Verkkosivusto]. Jyväskylä: Valtion tieto- ja viestintätekniikka-keskus Valtori. 23.9.2016. [Viitattu 5.10.2016]. Saatavana: http://www.valtori.fi/palvelut/vetuma