Käyttäjähallintaominaisuuden implementointi WordPress-sivustolle

Sisällönhallinta sivustolla

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

Hämeenlinna, Kevät 2018

Samo Lintusalo

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutusohjelma
Visamäki

Tekijä Samo Lintusalo **Vuosi** 2018

Työn nimi Käyttäjähallintaominaisuuden implementointi WordPress-sivustolle

Työn ohjaaja Tommi Saksa

TIIVISTELMÄ

Työn tavoitteena oli toteuttaa DigiTrail-hankkeen WordPress-sivustoon käyttäjähallintaominaisuus, jonka kautta tuotetaan sivustolle sisältöä. Tavoitteena oli, että ominaisuuden kautta todennettu käyttäjä pystyy lisäämään DigiTrail-hankkeessa tehtävään erilliseen mobiilisovellukseen sisältöjä kuten uutisia, reittejä ja markkereita digitaaliselle kartalle. Työn toimeksiantaja oli Hämeen ammattikorkeakoulun Älykkäät palvelut -tutkimusyksikkö.

Työn teoriaosuudessa kerrotaan www-sisällönhallinnasta, esitellään Microsoft Azure -palvelua sekä kuvataan sivustolle rakennetun kirjautumisjärjestelmän taustatekniikoita, eli käydään lyhyesti läpi SAML-tekniikan toimintaperiaatteet sekä otetaan myös tietoturva huomioon.

Työn käytännön osuudessa toteutettiin kirjautumisjärjestelmä ja määriteltiin eri rooleja sivustoon kirjautuneille käyttäjille sisällöntuottamista varten. Käytännön tasolla selvitettiin erityisesti myös sitä, minkälaisin keinoin Microsoft Azure -palvelun ja WordPress-järjestelmän saa keskustelemaan keskenään. Tämä edellytti Azure-ominaisuuksien läpikäymistä työn teoriaosuutta syvällisemmin.

Työn seurauksena sivuston ylläpitotyökalujen avulla voidaan toteuttaa yksityiskohtaisesti digitaalista sisältöä työn toimeksiantajan kannalta sopivien käyttäjäroolien kautta. Reittien ja reittipisteiden tuomista sivustolle tullaan edelleen kehittämään sivuston ylläpitäjän toimesta.

Avainsanat Sisällönhallinta, WordPress, Microsoft Azure

Sivut 26 sivua, joista liitteitä 7 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Business Information Technology
Visamäki

Author Samo Lintusalo **Year** 2018

Subject Implementing the User Management Feature for WordPress

Supervisor Tommi Saksa

ABSTRACT

The aim of this thesis was to develop a user management feature on the DigiTrail project on WordPress, through which content is generated on the site. An authenticated user can add content, such as news, routes, and markers to a digital map in a separate mobile application in the DigiTrail project. The commissioner of this thesis was Häme University of Applied Sciences Smart Services Research Unit.

The theoretical part of the thesis describes Content Management, introduces Microsoft Azure and describes background techniques for Signing In to project's site, a brief overview of SAML technology and security principles.

In the practical part of the work, a login system was implemented and different roles were defined for the site-registered users for content creation. At the practical level, the way in which the Microsoft Azure and WordPress systems can be centrally deployed were also explored. This required the Azure features to go beyond the theoretical part of the work.

The author of the thesis has created a login system that utilizes the active directory created for the new domain. When a user is logged in, the service provider scans the identity of the customer's identity from the identity provider and displays them in the correct format.

The project resulted in a situation where digital content can be implemented in detail on the site through user roles suitable for the client. Showing routes and markers will be further developed by the site administrator.

Keywords Content Management, WordPress, Azure

Pages 26 pages including appendices 7 pages

SANASTO

API	Ohjelmointirajapinta (*Application Programming Interface*) on tapa, jolla eri ohjelmat voivat vaihtaa tietoja keskenään.
Azure	Microsoftin julkinen kokoelma pilvipalveluja.
GPX	XML-pohjainen muunnosformaatti, joka on suunniteltu yhteiseksi GPS-tietomuodoksi ohjelmistosovelluksille.
JSON	Ohjelmointikielistä riippumaton, standardoitu tiedonsiirtomuoto.
Marker	Digitaalisella kartalla näytettävä reittipiste.
Shortcode	Shortcode eli lyhytkoodi on WordPressissä käytettävä erityisominaisuus, jonka avulla voi suorittaa erilaisia asioita pienellä vaivalla.
SQL	Relaatiotietokantojen hallintaan käytettävä kyselykieli. Kielen avulla tietokannasta voi hakea tietoa, lisätä tietoa tai muokata tietoa.
WordPress	Avoimen lähdekoodin www-sisällönhallintajärjestelmä.
XML	Erilaisten merkintäkielien yhteinen tapa merkata tekstidokumentteja. Merkkaus tarkoittaa sitä, että itse tiedon sekaan kirjoitetaan tiedon rakennetta ja merkitystä kuvailevaa informaatiota.

SISÄLLYS

Liitteet

1 JOHDANTO

Työn toimeksiantaja on Hämeen ammattikorkeakoulussa toimiva Älykkäät palvelut -tutkimusyksikkö. Tutkimusyksikkö vastaa elinkeinoelämän ja yhteiskunnan digitalisoinnin ja palvelujen kehittämisen tarpeisiin (HAMK n.d.b).

Työn tavoitteena on toteuttaa DigiTrail-hankkeen WordPress-sivustoon käyttäjähallintaominaisuus eli käytännössä rakentaa kirjautumisjärjestelmä. Käyttäjähallinnan tarkoituksena on, että todennettu käyttäjä pystyy ominaisuuden kautta lisäämään DigiTrail-hankkeessa tehtävään erilliseen mobiilisovellukseen sisältöjä kuten uutisia, reittejä ja markkereita digitaaliselle kartalle.

Työn loppukäyttäjiä ovat Hämeen ammattikorkeakoulun DigiTrail-hankkeen parissa toimiva henkilöstö, hankkeen yhteistyökumppanit ja tahot, jotka haluavat saada luontoreittinsä näkyviin mobiilisovelluksessa. Hanke on aloitettu elokuussa 2016. Hankkeessa lisätään retkeilyreittien näkyvyyttä ottaen huomioon kansainväliset laatuvaatimukset. DigiTrail-hankkeen keskeisenä teemana on myös innostaa paikallisia yrittäjiä liittämään matkailupalvelujaan osaksi projektin tarjoamia reitistöitä. Hanke kestää vuoden 2018 loppuun asti. (HAMK n.d.a).

Aihe valittiin siksi, että opinnäytetyön tekijä halusi lisää kokemusta webkehittämisestä. Tämä aihe vaikutti myös sellaiselta, että tehdystä työstä saisi helposti palautetta ja työn tulokset olisivat selkeät. DigiTrail-hanke oli työn tekijälle jo entuudestaan tuttu, joten siihen oli helppo lähteä mukaan. Ehkäpä myös työelämässä tarvitsee tämän työn kaltaista osaamista.

Aihe rajattiin käsittelemään käyttäjähallintaominaisuuden luomista niin, että käyttäjä pystyy kirjautumaan hankkeen sivustolle sekä hallintapaneelin avulla lisäämään asiakkaan toivomaa sisältöä. Hanketta varten oli luotu WordPress-alusta valmiiksi. Opinnäytetyössä sivustoon kehitettiin käyttäjähallintaominaisuus eli käytännössä kirjautumisjärjestelmä.

Opinnäytetyön teoriaosuudessa käydään läpi muun muassa Microsoft Azure-palvelun tietokantarakennetta ja sen lisäosia. Työssä käsitellään myös kirjautumisjärjestelmän tietoturvaseikkoja. Opinnäytetyön käytännön osuudessa käydään läpi vaiheet, kuinka kirjautumisjärjestelmä sekä tietokantayhteyksien rakentaminen toteutetaan.

Opinnäytetyön tutkimuskysymykset ovat:

- Miten sivustoa päivitetään, kun sivuston sisältöihin tulee muutoksia?
- Miten kirjautumisjärjestelmä toteutetaan?
- Miten WordPress saadaan keskustelemaan Azure-tietokannan kanssa?

- Miten rakennetaan ylläpitoa niin, että sivu pysyy pystyssä vielä senkin jälkeen, kun taustapalvelut loppuvat?

2 WWW-SISÄLLÖNHALLINTA JA KOOSTAMISTEKNIIKAT

Tässä kappaleessa käydään läpi opinnäytetyön tietoperustaa. Tietoperustaan kuuluu ymmärrys muun muassa keskeisimmistä koostamistekniikoista ja www-sisällönhallinnasta.

2.1 Www-sisällönhallinta

Www-sisällönhallinnalla tarkoitetaan sellaista toimintaa, jossa verkkopalvelussa hallitaan digitaalista sisältöä yhtenäisesti ja keskitetysti. Tämä tarkoittaa verkkopalvelun kokonaisuuden hahmottamista, eli julkaistava sisältö yritetään pitää erillään sivuston rakenteesta ja ulkoasusta (Tolvanen 2007). Yleensä sivuston rakenteella tarkoitetaan esimerkiksi sivupohjia, joissa määritellään asetukset esimerkiksi sivuston navigaatiolle ja otsikoinnille. Sisällönhallintaan tarkoitetusta järjestelmästä voidaan käyttää muitakin käsitteitä kuten julkaisujärjestelmä tai lyhennettä CMS (*Content Management System*) (Ite Wiki OY (n.d.)).

Yleisesti moderneissa järjestelmissä sisältöä pyritään julkaisemaan erilaisten sivupohjien avulla niin, että kävijöiden toiminnasta sekä itse verkkopalvelun toiminnasta saadaan tietoa. Tällaista tietoa voi saada esimerkiksi niin, että integroidaan julkaisujärjestelmä jonkin kolmannen osapuolen kehittämän lisäosan kanssa. Lisäosa saa sopivat oikeudet esimerkiksi versionhallintaan tai hakujen hallintaan. Myös aivan keskeiset julkaisujärjestelmien toiminnallisuudet kuten käyttäjien hallinta ja sisällön muokkaaminen voidaan siis toteuttaa lisäosien avulla, vaikka nämä ominaisuudet toki löytyvät vakiona julkaisujärjestelmistä.

2.2 WordPress

WordPress on avoimen lähdekoodin www-sisällönhallintajärjestelmä. Avoin lähdekoodi tarkoittaa sitä, että käyttäjä voi tarkastella lähdekoodia ja käyttää sitä haluamallaan tavalla mutta kuitenkin ohjelmassa määritellyn lisenssin ehtojen mukaan (Open Source Initiative 2007). Koodin alkuperäinen kirjoittaja voi vaatia, että hänen kehittämäänsä ohjelmaa julkaistaisiin jatkossa samalla lisenssillä hyötyäkseen kehittämisyhteisön kirjoittamista korjauksista. Saman projektin parissa työskentelee miljoonia ihmisiä samaan aikaan, joten julkisesta kehittäjäyhteisöstä ongelmiin löytyy ratkaisuja nopeasti mutta toisaalta on paljon erimielisyyksiä siitä, mihin suuntaan ohjelmaa pitäisi kehittää.

Vuonna 2003 WordPressiä alettiin kehittää tarkoituksena luoda julkaisujärjestelmä, jolla pystyisi luomaan ja ylläpitämään henkilökohtaisia blo-

geja. Myöhemmin järjestelmä on kehittynyt täysimittaiseksi ja vakaaksi sisällönhallintajärjestelmäksi, jossa lisäosien asentaminen ja ohjelmiston päivittäminen tapahtuvat automatisoidusti. (WordPress.org n.d.a.)

WordPress on kirjoitettu PHP-ohjelmointikielellä. PHP on vuonna 1995 julkaistu ohjelmointikieli, jota käytetään etenkin palvelinpuolella webkehitykseen (The PHP Group n.d.). PHP-kieltä voi käyttää upottamalla koodia HTML-sivujen sisään tai omana erillisenä tiedostonaan, johon viitataan HTML-sivulla. WordPressissä tiedot tallennetaan MySQL-tietokantaohjelmistoon. WordPress-asennusta varten tarvitaankin siis sellainen palvelin, joka tukee PHP- ja MySQL -tekniikoita. Suurin osa palvelintilaa tarjoavista yrityksistä täyttää nämä ehdot. Tärkeitä kriteereitä palveluntarjoajaa valittaessa ovat palvelun nopeus ja luotettavuus. Luotettavuutta voidaan mitata esimerkiksi julkaistun asiakaspalautteen ja asiakasmäärän pohjalta. (WordPress.org n.d.e.)

2.3 Koostamistekniikat

2.3.1 HTML

HTML on internetin merkintäkieli, jolla internetsivut on kirjoitettu. HTML-kielellä kuvataan sivun rakenne niin, että eri elementit koodissa vastaavat sivun otsikkoa, leipätekstiä ja esimerkiksi alatunnistetta. HTML-dokumentteja kirjoitetaan siihen tarkoitetuilla tekstieditoreilla. HTML-kieli on pitkälti standardoitua. HTML-dokumentin tulisi täyttää kullekin dokumenttityypille asetetut vaatimukset esimerkiksi siitä, minkälaisia elementtejä voidaan käyttää. (W3C 2017.)

2.3.2 CSS

CSS (*Cascading Style Sheets*) on webtekniikka, jonka avulla esimerkiksi HTML-dokumentteihin voidaan yhdistää tyyliohjeita. CSS-ohjeet ehdottavat, kuinka dokumentin ulkoasu voidaan esittää. Kun jo tekniikan nimi viittaa tyylien porrastamiseen (*cascading*), se näkyy niin, että yhdelle dokumentille voi tyyliohjeita antaa samaan aikaan monta tyylitiedostoa. Esimerkiksi dokumentin käyttäjän ohjeet voivat korvata dokumentin tekijän antamat ohjeet. (W3C 2017.)

CSS-tyylejä voidaan yhdistää HTML-dokumenttiin esimerkiksi niin, että tuodaan tyylit erillisestä CSS-tiedostosta tai sitten niin, että upotetaan tyylit dokumenttiin. Yleisesti hyvänä pidetty tapa on pitää tyylit ja rakenne mahdollisimman erillään toisistaan.

3 MICROSOFT AZURE

Microsoft Azure on Microsoftin kokoelma julkisia pilvipalveluja (Microsoft n.d.). Pilvipalvelulla tarkoitetaan sellaista loppukäyttäjästä ulkoistettua ympäristöä, jonka resurssit voivat kasvaa käyttäjän tarpeen mukaan ja maksuja peritään käytön mukaan. Tunnusomaisesti pilvipalvelun resurssit ovat heti saatavilla päätelaitteesta riippumatta ja resurssien käyttöä pyritään optimoimaan tehokkailla mittauksilla. Mittauksien tarkoitus on lisätä läpinäkyvyyttä palveluntarjoajan ja kuluttajan välillä. Pilvipalvelun loppukäyttäjä ei juurikaan voi vaikuttaa siihen, missä dataa varastoidaan tai minkä maan lainsäädäntöä dataan sovelletaan. (Keso n.d.)

Azure on käytössä etenkin webkehittäjien tekemien sovellusten alustana ja virtuaalipalvelinten ajoympäristönä. Azure-palvelua mainostetaan Microsoftin sivustolla ensisijaisesti suuryrityksille, koska palvelussa on mahdollista tehdä laajalle skaalautuvia IT-ratkaisuja. (Microsoft n.d.c.)

3.1 Azure SQL -tietokanta

Azure SQL -tietokanta on yleiskäyttöinen relaatiotietokantapalvelu, joka tukee esimerkiksi JSON- ja XML-rakenteita. Se tuottaa käyttäjälleen dynaamisesti skaalautuvaa suorituskykyä ja tarjoaa myös analyysityökaluja. Tietokantaa voi käyttää muun muassa Azure Portal -palvelun, SQL Server Management Studion tai Visual Studion kautta. (Microsoft 2018c.)

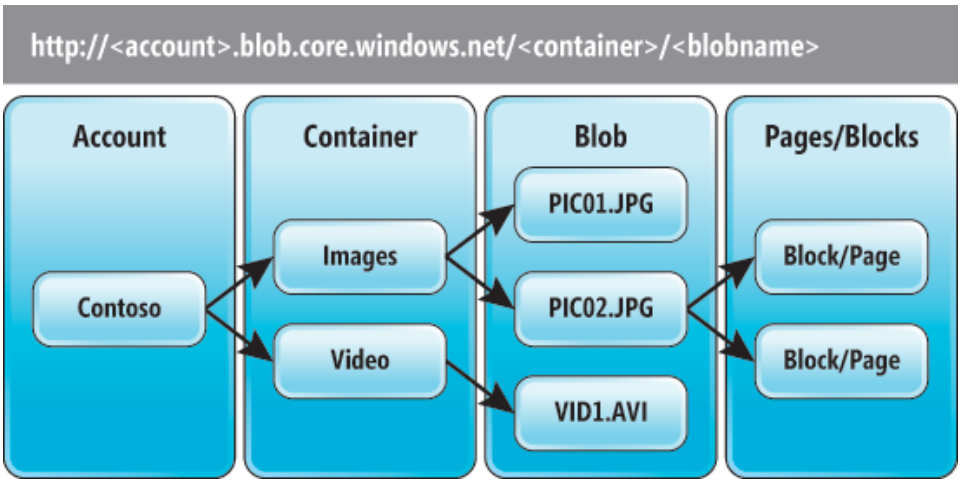
Azure-palvelussa voi ostaa tallennustilaa joko yksittäiselle tietokannalle, jos suorituskykyvaatimukset ovat ennalta suurin piirtein tiedossa, tai sitten voi ostaa joustavan palvelun (*elastic pool*) monelle tietokannalle. Taulukossa 1 on esimerkki yksittäisen tietokannan käyttöönoton hinnoittelusta eri palvelutasoille. Azure-palvelussa tietokantojen suorituskykyä verrataan transaktioyksiköiden (*DTU - Database Transaction Unit*) avulla. Tällainen transaktioyksikkö on suoritintehon, muistin määrän ja siirrännän (*I/O - input/output*) perusteella luotu arvo. (Microsoft 2017b.)

Taulukko 1. Hinnoittelu palvelulle, jossa yksittäinen tietokanta käytössä (Microsoft n.d.a)

Service Level	DTUs	Storage	Max Storage	Price for DTU
Basic	5	2 GB	2 GB	£0,005/hour
Standard S0	10	250 GB	250 GB	£0.0151/hour
Standard S1	20	250 GB	250 GB	£0.0301/hour
Standard S2	50	250 GB	250 GB	£0.0752/hour
Standard S3	100	250GB	1 TB	£0.1503/hour
Standard S4	200	250GB	1 TB	£0.1503/hour
Standard S6	400	250GB	1 TB	£0.3006/hour
Standard S7	800	250GB	1 TB	£0.6011/hour
Standard S9	1 600	250GB	1 TB	£1.2022/hour
Standard S12	3 000	250GB	1 TB	£2.2541/hour

3.2 Azure Blob Service

Azure Blob -tallennustila on palvelu, jolla yleensä tallennetaan suuria määriä jäsentymätöntä tietoa. Blob-tallennustilaan voi varastoida esimerkiksi monen tyyppisiä tekstejä tai binääritiedostoja. Jokaisella ”blobilla” on oma nimensä ja oma verkko-osoite (kuva 1). Blobeja on kolmen tyyppisiä. Lohkoblobit (*block blobs*) ovat ideaaleja tallennuskohteita, kun halutaan varastoida tekstiä tai binääritiedostoja. Yksi lohkoblob voi sisältää 50 000 lohkoa niin, että jokaisessa lohkossa voi olla 100 megatavua sisältöä. Liitäntäblobit (*append blobs*) taas ovat optimoitu lisätoimintoihin kuten kirjautumisratkaisuihin (Microsoft 2018b). Jokainen liitäntäblobin 50 000 lohkosta voi sisältää neljä megatavua dataa. Sivublobit (*page blobs*) voivat sisältää yhden teratavun verran dataa ja ne ovat optimikäytössä esimerkiksi silloin, kun luetaan tai kirjoitetaan virtuaalikoneiden dataa. (Microsoft 2017c.)



Kuva 1. Blob-tallennustilan osat (Microsoft 2013).

Tiedostoja tallennetaan itse luotuihin säiliöihin (*containers*), joita voi jokaista tiliä kohden luoda rajoittamattoman määrän. Blob-tallennustilaa voi Azure-palvelussa hallita joko yleiskäyttöön tarkoitetulla käyttäjätilillä tai Blob-tallennustilaan luodulla käyttäjätilillä. Käyttöoikeudet tiedostoihin ja metadataan määritellään säiliötasolla. (Microsoft 2017c.)

3.3 Azure-aktiivihakemisto

Aktiivihakemisto on alun alkaen Microsoftin aivan ensimmäisten käyttöjärjestelmien mukana julkaistu palvelu. Se on tarkoitettu Windows-palvelinten, verkon käyttäjien ja resurssien hallintaan. Organisaatiot voivat käyttää moderneja suojaustoimintoja suojatakseen tiedonsiirtoa. Suojattavaa tietoa voi olla esimerkiksi levyaseman tai sovelluksen jakaminen verkon eri käyttäjille. Käyttäjien tietoja käsitellään monella eri tasolla, ja eri tason objekteilla on erilaisia attribuutteja. (Talvivaara n.d.)

Azure-aktiivihakemisto on Microsoftin pilvilaskentapohjainen hakemisto ja identiteetinhallintapalvelu. Se yhdistää keskeiset hakemistopalvelut, sovellusten käytönhallinnan ja identiteettien hallinnan. Alusta noudattaa yleisimpiä netin standardeja, joiden avulla kehittäjät voivat tarjota pääsyn sovelluksiinsa keskitettyjen sääntöjen perusteella. (Microsoft 2017e.)

IT-järjestelmänvalvojille Azure-aktiivihakemisto mahdollistaa tiedonvaihdon muiden pilvilaskentaohjelmistojen kuten Office 365 ja DropBoxin kanssa. Azure-aktiivihakemisto sisältää suuren joukon identiteetinhallintaominaisuuksia, kuten itsepalveluna tapahtuva salasananhallinta, roolipohjainen pääsynhallinta ja sovellusten käytön monitorointi. (Microsoft 2017e.)

4 KEHITTÄMISTYÖN TAVOITE JA TARKOITUS

Opinnäytetyön ideana oli tehdä käyttäjähallintaominaisuus DigiTrail-hankkeen WordPress-sivustoon. Tämä tapahtui käyttämällä sopivaa lisäosaa, joka saa WordPressin vaihtamaan tietoja Azure-palvelun kanssa. Käyttäjien tunnistusta varten ei itse tehty koodia vaan tätä varten oli tarkoitus hyödyntää Azure-palvelun aktiivihakemistoa, johon hankkeen tulevilla julkaisijoilla oli jo työn tekemisen aikana tunnukset olemassa. Kun käyttäjä on tunnistautunut WordPressiin, hänet ohjataan hallintasivulle, jonka kautta hän voi lisätä mobiilisovellukseen teemoja, reittejä ja reittipisteitä (*markers*).

Asiakkaan toimesta tehtiin hanketta varten Azure-palveluun uusi aktiivihakemisto, jota käytetään mahdollisimman tietoturvallisesti. Aktiivihakemistossa annetaan hankkeen käyttäjille sopivat oikeudet: ylläpitäjä voi luoda ja poistaa reittejä ja teemoja, peruskäyttäjä voi vain luoda sisältöä. Sovellus hakee kaiken tarvitsemansa datan tietokannasta puhelimeen, tässä työssä ei keskitytä tietokantayhteyksien päivittämiseen tai muuhun optimointiin syvällisesti. Tapahtumakartan sovellus saa avoimen datan puolelta.

Opinnäytetyön aihe rajattiin käyttäjähallintaominaisuuden toteuttamiseen niin, että käyttäjä pystyy lisäämään sisältöjä mobiilisovellukseen. Työssä ei siis keskitytty verkkosivun ulkoasuun tai asiakaspuolen luomiseen vaan enemmänkin pelkkään ylläpitoon. Työn läpikäynti rajoittuu pitkälti lähtötilanteeseen, käytännön osuuden ja teorian yhdistämisen raportointiin sekä tuloksien kuvaamiseen.

5 UUDEN KIRJAUTUMISJÄRJESTELMÄN PERUSTEET

5.1 Kertakirjautuminen

Kertakirjautuminen (*SSO – Single Sign On*) tarkoittaa menettelytapaa, jossa yhdellä käyttäjätunnuksella kirjauduttuaan sisään käyttäjä voi työskennellä usean eri palvelun välillä. Menetelmän etuna pidetään yritysten työntekijöiden työskentelyn nopeutumista ja IT-osastojen ajan säästämistä. Kun käyttäjän tarvitsee monen palvelun sijasta muistaa salasana vain yhteen paikkaan, järjestelmäasiantuntijoiden voivat hallita salasanoja keskitetysti ja näin vapautuu aikaa muuhun työhön. Sovelluskehittäjien aikaa säästyy, kun he voivat hyödyntää valmiita kehystä käyttäjien tunnistuksessa. Kertakirjautumista käytetään varsinkin suurten yritysten tietopalveluratkaisuissa. (Korhonen 2014.)

Kertakirjautumisjärjestelmistä pyritään tekemään mahdollisimman älykkäitä. Voidaan määritellä organisaation sisällä, mitkä sovellukset ovat kaikkien käytettävissä ja mitkä taas ovat käyttöoikeuksiltaan rajatumpia. Peruskäyttäjä voisi esimerkiksi saada pääsyn yrityksen tiedotuskanavalle, mutta kun hän yrittää kirjautua palkanlaskentajärjestelmään, häneltä kysytään vahvempaa todennusmallia kuten biometriikkaa. Tätä kutsutaan kaksivaiheiseksi tunnistukseksi. (Korhonen 2014.)

Kertakirjautumismenetelmä tuo yritykselle myös teknisiä ja tietoturvallisia riskejä. Tekninen riski voisi olla esimerkiksi sellainen tilanne, että jos kertakirjautumisjärjestelmä ei jostain syystä toimi, silloin yhteenkään sovellukseen ei ole pääsyä, ellei sovelluksissa ole omaa tunnistautumispalvelua tai suunnitelmaa katastrofin varalle. Tietoturvariski taas muodostuu sellaisesta tilanteesta, jossa käyttäjä jakaa tunnistustietojaan verkon yli epätoivotuille henkilöille. Käyttäjä ei välttämättä aina edes itse tiedä, mihin palveluihin hän on yhteydessä ensimmäisen kirjautumisen jälkeen. Siksi onkin tärkeää, että käyttäjä muistaa kirjautua sessiosta ulos ja sulkea selaimensa. (AuthenticationWorld n.d.)

5.2 SAML 2.0 -tekniikka

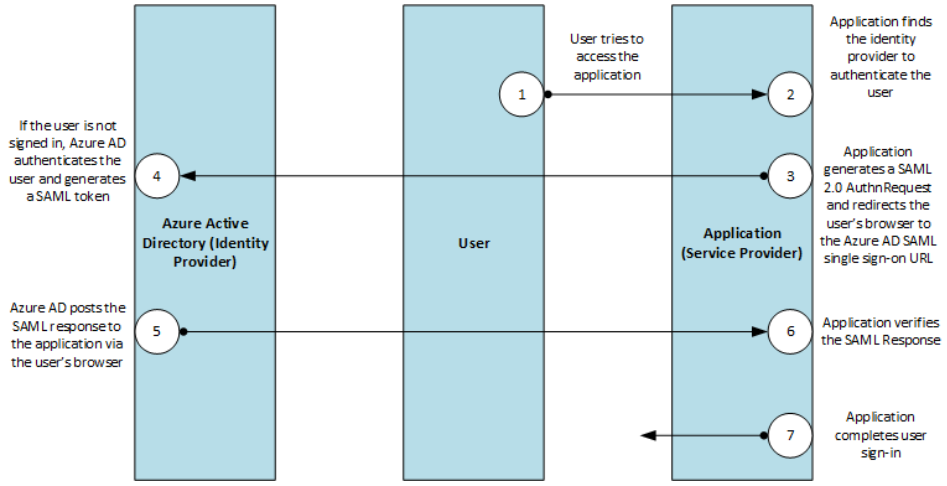
SAML on OASIS Security Services Technical Committeen ylläpitämä standardi, joka määrittelee XML-pohjaisen kehyksen (*framework*) tietojen jakamiseen. Standardin avulla verkkoyritysten välillä jaetaan käyttäjien todennus- ja valtuutustietoja. Moni palveluntarjoaja on antanut tuen SAML:in käytölle sovelluksissa ja se onkin laajasti käytössä eritasoisten organisaatioiden www-hallintajärjestelmissä. Standardin ensisijainen käyttötarkoitus on toteuttaa www-selaimella tapahtuva kertakirjautuminen internetpalveluun. Esimerkiksi sisäverkon tietoliikenteen yhdistäminen ulko-

verkkoon voi tietoturvasyiden ja yhteensopivuusongelmien takia osoittautua haasteelliseksi, joten SAML-tekniikalle on suuri tarve. (Korhonen 2014.)

5.2.1 Tekniikan toimintaperiaatteet lyhyesti

SAML koostuu rakennuspalikoista, jotka yhteen koottuna sallivat useiden käyttötapauksien tukemisen. SAML-tekniikan keskeisimpänä rakennuspalikkana toimii XML-muotoinen vakuutus (*assertion*), joka käsittelee yhtä tai useampaa toteamusta (*statement*). Yhteen tietopakettiin siis sisällytetään monta eri toteamusta, kuten esimerkiksi henkilötiedot ja lupatiedot. (OASIS 2005.)

SAML-vuorovaikutuksessa on yleensä mukana vähintään kolme toimijaa: palveluntarjoaja (*Service Provider* tai *relying party*), henkilöllisyydentarjoaja (*Identity Provider* tai *asserting party*) ja toimeksiantaja (*Principal*). Henkilöllisyydentarjoaja välittää luomansa tunnistetiedot käyttäjästä pyyntöjen perusteella eteenpäin (kuva 2). Palveluntarjoaja on yksi tai useampi taho, joka voi käyttää toteamusta ja valvoa pääsyä toteamuksen käyttöön paikallisella tasolla. (OASIS 2005.)



Kuva 2. Kertakirjautuminen, esimerkkikaavio (Microsoft 2017c).

Vakuutuksia pyydetään tai vain ”työnnetään” henkilöllisyydentarjoajalta palveluntarjoajalle. Miten ja mitkä vakuutukset pyydetään lähetettäväksi, määritellään SAML-protokollassa. Tätä alemmalla tasolla on vielä viestintäprotokolla, kuten http POST-kutsu tai SOAP-viesti, jonka toiminta määritellään XML-pohjaisessa sidonnassa (*binding*). (OASIS 2005.)

5.2.2 Tekniikan tietoturvallisuus

Tietojärjestelmään mahdollisesti liittyvän uuden riskin luonne riippuu useista tekijöistä, kuten viestintäympäristöstä, viestintävälineistä ja viestinnän luonteesta. Yksi keskeisimmistä tavoitteista SAML-tekniikan käytössä on varmistaa, että kahden osapuolen välillä kulkeva vakuutus pysyy muuttumattomana ja että paketin vastaanottava palveluntarjoaja voi luottaa siihen, että vakuutuksen vastaanottaminen on turvallista. Vakuutuksen kaapannut taho voisi toteuttaa aktiivisen salakuuntelun avulla (*Man-in-the-Middle-Attack*) hyökkäyksen (OASIS 2004). Monessa tapauksessa hyökkääjä muuttaa sisältöä haluamakseen ja esimerkiksi ”toistaa” viestiä myöhempänä päivämääränä vahingoittaakseen järjestelmää. (OASIS 2005.)

Ensisijainen mekanismi havaita vakuutuksiin kohdistettuja hyökkäyksiä on rakentaa kahden osapuolen välinen julkisilla avaimilla (*Public Key*) hallittava luottamussuhde. Julkisten avainten käyttö ei ole pakollista, mutta suotavaa. Jotta SAML-osat ovat turvallisia, täytyy julkisten avainten hallinta toteuttaa oikein. Jokaiselle SAML-profiilille määritetään tietoturvasuunnitelma. Yleisen, kaikkia profiileja koskevan ohjeistuksen mukaan viestien luottamuksellisuutta lisää muun muassa HTTPS-tekniikan käyttö. Tekniikalla voidaan TLS-protokollan avulla salata tiedot ennen niiden luovuttamista. (OASIS 2005.)

Julkisen avaimen salaus -tekniikka käyttää avainparia salaamaan ja purkamaan sisältöä. Avainpari koostuu yhdestä yksityisestä ja yhdestä julkisesta avaimesta, jotka ovat matemaattisesti yhteydessä toisiinsa. Kun esimerkiksi kaksi tietojärjestelmää aikoo kommunikoida toistensa kanssa, ne voivat jakaa julkiset avaimensa toisilleen, mutta pitää yksityiset avaimet salassa. Esimerkiksi Järjestelmä A voi lähettää viestin palvelulle B käyttämällä palvelun B julkista avainta, ja järjestelmä B voi käyttää yksityistä avaintaan purkamaan viesti. Järjestelmä A ei voi varmuudella tietää, että avain, jota se käyttää salaukseen, todella kuuluu järjestelmä B:lle. Tämän ongelman takia valtuutetaan luotettavia kolmansia osapuolia, sertifikointiviranomaisia (*CA – Certificate Authority*) myöntämään sertifikaatteja, jotka vahvistavat osapuolten identiteetit ja sitovat identiteetit sertifikaatin julkisiin avaimiin. Varmentaja allekirjoittaa todistuksen käyttämällä yksityistä avaintaan ja antaa vastaavan julkisen avaimen CA-sertifikaatilla. (Microsoft n.d.b.)

SAML-vakuutuksen tasolla vakuutuksen liikkeellelaskijalla ei ole enää työkaluja hallita vakuutusta. Liikkeellelaskija ei esimerkiksi voi määrittää, kuinka kauan vakuutus tai sen sisältämät väitteet säilyvät kuluttajan järjestelmissä eikä hän voi määrittää, keiden kanssa kuluttaja jakaa hänen lähettämiään tietoja. Vakuutuksen lähettäjän pitäisikin harkita suunnitelmaa sen varalle, että lähetetyt tiedot päätyvät vääriin käsiin. (OASIS 2004.)

SAML-protokolla on erityisesti alttiina palvelunestohyökkäyksille (*DoS - Denial of Service*). SAML-pyynnön käsitteleminen on kuluttavaa, koska se tyypillisesti vaatii viestin hakemista tietokannasta, viestin uudelleen jäsentämistä ja vastaussanoman rakentamista. Näin ollen pyyntöjen lähettäminen vaatii paljon vähemmän aikaa ja vaivaa kuin niiden käsitteleminen. (OASIS 2004.)

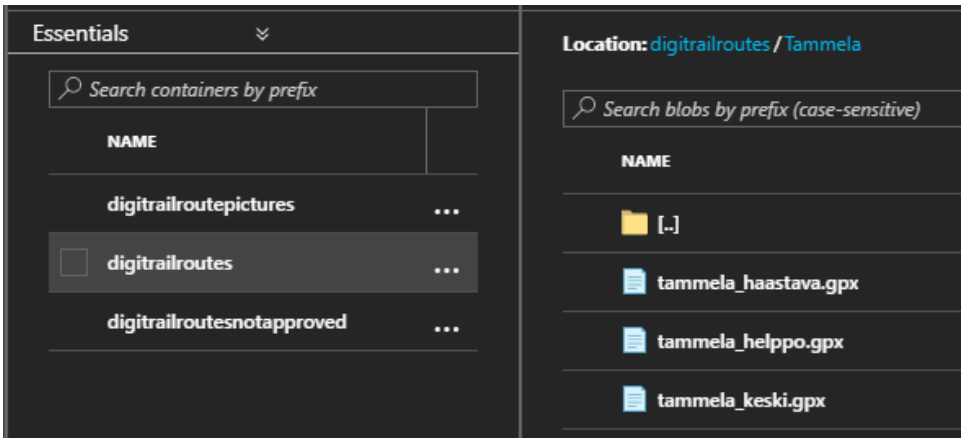
6 KÄYTÄNNÖN TOTEUTUS

Tämän luvun alussa kuvataan hieman hankkeen kansiorakennetta. Luvussa käydään läpi myös kirjautumisjärjestelmän toteuttamista ja sitä, minkälaisia erilaisia vaihtoehtoja on tietokantayhteyden luomiseen. Lopuksi käydään läpi WordPress-sisällöntuotantoa. Hankkeen Azure-ympäristön ominaisuudet tulevat tarkemmin ilmi kuin työn teoriaosuudessa.

6.1 Hankkeen kehittämisympäristö

Hanketta kehitetään ensisijaisesti DigiTrail-sivuston hallintapaneelissa. Hankkeen mobiilisovelluksen sisältöjä ja kansiorakenteita hallitaan Azure-palvelussa (kuva 3). Kansiot on nimetty paikkojen nimien mukaan. Jos perustason käyttäjä lisää reitin, ylläpitäjän tulee hyväksyä sen sisältämät tiedot ennen kuin reitti siirtyy hyväksymättömien reittien kansiosta hyväksyttyihin tiedostoihin.

Reittipisteet voidaan kategorisoida tietyn teeman alle. Teemoja voivat olla esimerkiksi liikunta tai luonto. Yleistason reittipisteet näkyvät kaikille tunnistautuneille käyttäjille, mutta teemoihin liittyvät eivät. Reittitiedot ovat Azure Blob Storage -tilassa GPX-tiedostoina. Tiedostoissa on määritelty muun muassa leveys- ja pituusasteet JSON-muodossa.



Kuva 3. Kuvakaappaus Blob-tallennustilan kansiorakenteesta.

6.2 Kirjautumisjärjestelmä

WordPress-ohjelmistossa on vakiona olemassa kirjautumisjärjestelmä, johon kirjoittamishetkellä sivuston ylläpitäjät kirjautuvat. Sivuston vakiokirjautuminen korvataan miniOrangen rakentamalla, ilmaisella kertakirjautumislisäosalla. Lisäosa sallii käyttäjän kirjautua todennetun identiteetin tarjoajan kautta. Tuettuja tarjoajia ovat muun muassa Google Apps, Shibboleth ja Azure AD. Hankkeen parissa työskentelevällä henkilöstöllä on jo

ennestään olemassa HAMKin aktiivihakemistossa tilit, joilla tunnistaudutaan Azure-alustaan. (WordPress.org n.d.g.)

Lisäosan asentamisen jälkeen täytyy tehdä määritys (Naktode 2018, liite 2), jonka mukaan Azure-aktiivihakemisto toimii lisäosan henkilöllisyydentarjoajana. Azure-hallintapaneelissa aktiivihakemiston App Registrations -välilehdellä luodaan uusi sovellus. Uusi sovellus luodaan DigiTrail-hanketta varten luodulle aktiivihakemistolle. Hankkeen henkilöstön luomalla Microsoft-käyttäjällä määritetään kirjautumisosoitteeksi DigiTrail-sivuston etusivu.

Sovelluksen rekisteröinnin jälkeen uusi aktiivihakemisto luo automaattisesti App ID URI -arvon, johon Azure-aktiivihakemisto voi ottaa yhteyttä. URI tarkoittaa yksilöllistä merkkijonoa, jota käytetään kertomaan www-sivun paikka (IETF 2005). Lisäosan asetuksissa arvoksi vaihdetaan SAML-lisäosan osoite siinä muodossa missä se on WordPressin kansiorakenteessa.

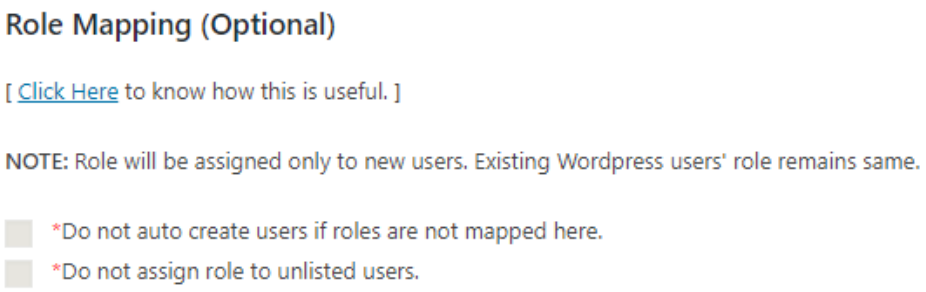
Aktiivihakemiston Endpoints-välilehdellä on asennukseen tarvittavat metatiedot, jotka syötetään lisäosan Service Provider -välilehdelle vastaamaan aktiivihakemiston arvoja. Arvoja ovat muun muassa SAML-lisäosan sisään- ja uloskirjautumisosoitteet, X.509 sertifikaatti ja EntityID. X.509 sertifikaatti on XML-muotoon pakattu binäärinen tunniste (OASIS 2005). Nämä arvot löytyvät websovellukselle luodusta Federation Metadata -dokumentista. (Naktode 2018, liite 2.)

Lisäosan Attribute Mapping -välilehdellä voidaan testikonfiguraation arvojen perusteella määrittää attribuutit hakemaan oikeat arvot. Attribuutit ovat henkilöllisyydentarjoajan hallussa olevia yksityiskohtaisia tiedonpalasia kirjautuneesta käyttäjästä. Attribuuttien kartoituksen tarkoituksena on löytää oikeat attribuutit henkilöllisyydentarjoajalta ja yhdistää ne WordPressin vastaaviin arvoihin kuten etunimi tai sukunimi. (Naktode 2018, liite 2.)

WordPress-järjestelmässä sivuston ylläpitäjä voi hallita niitä toimintoja, mitä käyttäjät voivat tehdä ja mitä ei. Rooleja on ennalta määritelty kuusi erilaista: Super Admin, Admin, Editor, Author, Contributor ja Subscriber. Esimerkiksi editoija voi julkaista ja hallita omia ja muiden kirjoituksia, mutta Author-tason käyttäjä voi hallita vaan omia kirjoituksiaan. Contributon-tason käyttäjä tehdä omia kirjoituksiaan, mutta ei julkaista niitä. Subscriber-tason käyttäjä voi ainoastaan hallita oman profiilin tietojaan ja tarkastella sivuston sisältöä. (WordPress.org n.d.f)

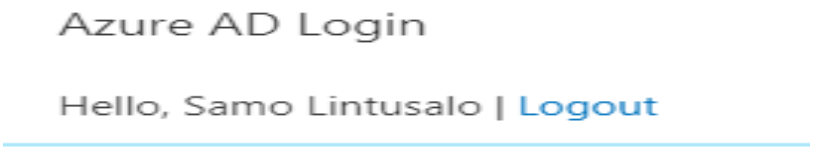
Lisäosan Role Mapping -välilehdellä voidaan määrittää tiettyyn ryhmään kuuluvien käyttäjien rooleja henkilöllisyydentarjoajalta. Määrityksen tallentamisen jälkeen roolit määritellään pelkästään uusille käyttäjille, eli olemassa olevien käyttäjien tietoja ei muuteta. Lisäosan kautta annetaan rooleja vain käyttäjille, joilla ei ole admin-tason oikeuksia. Admin-käyttäjien

oikeudet täytyy muuttaa manuaalisesti. Lisäosa kartoittaa automaattisesti sopivat roolit myös ei-listatuille käyttäjille ja automaattisesti pystyy luomaan uusia käyttäjiä, vaikka välilehdellä ei rooleja olisi kartoitettu, koska käyttäjien luonnin estäminen kuuluu Premium ja Enterprise -tason lisäosien ominaisuuksiin (kuva 4). (WordPress.org (n.d.g.)



Kuva 4. Kuvakaappaus lisäosan Roolien kartoitus -välilehdeltä.

Kun käyttäjä kirjautuu hankkeen aktiivihakemistoon siihen liitetyllä tunnuksella, Azure-hallintanäkymä näkyy oikein ja DigiTrail-hankkeen sivuston sivunavigaatiossa pitäisi lukea tervehdys kirjautuneelle käyttäjälle muodossa etunimi ja sukunimi (kuva 5). Käyttäjä voi myös sivuston kautta kirjautua uudelleen, edellyttää toista tunnusta kuin se, millä sillä hetkellä on kirjautuneena.



Kuva 5. Lisäosan luoma kuvake ilmoittaa hankkeen etusivulla käyttäjän olevan kirjautuneena.

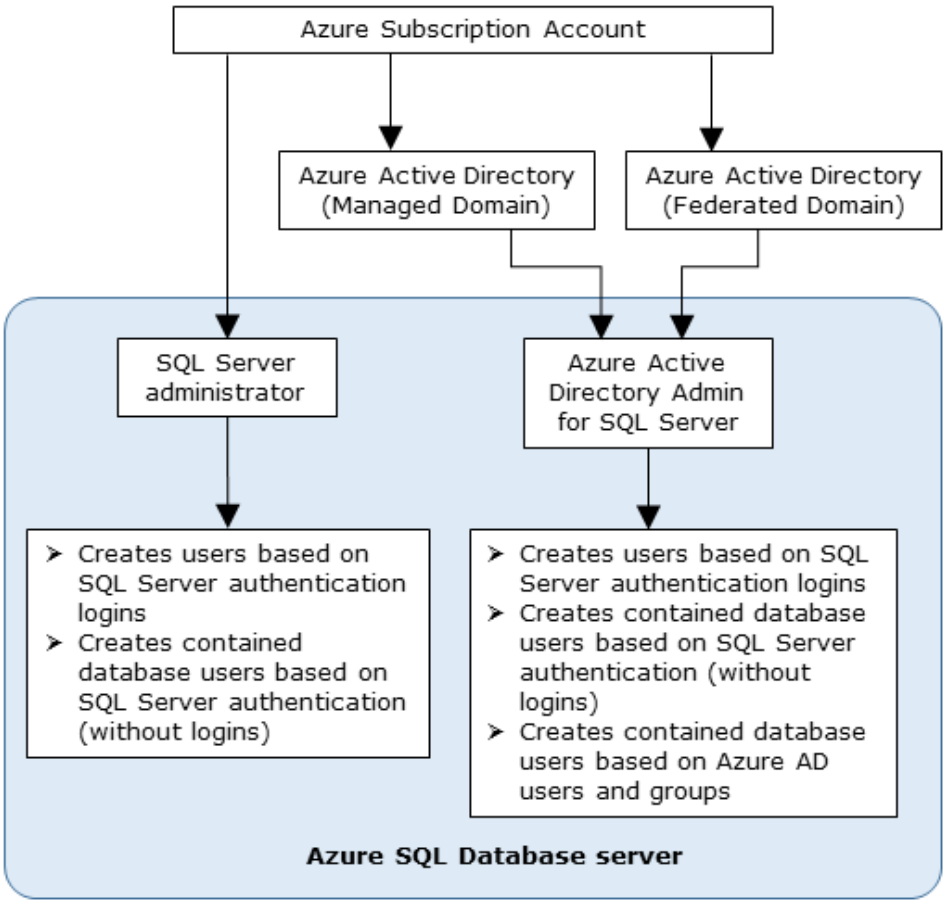
6.3 Tietokantayhteys

DigiTrail-hankkeen sivuja hallitaan WordPress-palvelussa. Tämä tarkoittaa sitä, että oletuksena sivuston HTML- ja PHP -tiedostoja ei pysty muokkaamaan. Uusille sivuston sisään luoduille sivuille kuitenkin pystyy upottamaan HTML- tai PHP -koodia erilaisten tekstinmuokkauseditoreiden kuten esimerkiksi Elementor-sovelluksen avulla.

Projektin tavoitteena on luoda monta erillistä kustomoitua sivua vastaamaan erilaisia sisällöntuotantomenetelmiä. Sivuja voivat olla esimerkiksi uutisen lisääminen, reitin lisääminen tai reittipisteen lisääminen digitaaliselle kartalle. Ideaalissa tapauksessa kaikki kustomoidut sivut suorittavat tietokantayhteyden luomiseen tarkoitetun erillisen template-tiedoston, joka on sivuston kansiorakenteen juuressa. Jokaisella kustomoidulla sivulla on sekä PHP- että HTML-koodia. Ongelma on, että WordPress-palveluun ei

voi tuoda omia sivuja, vaan sivuja pitää muokata erikseen asennetuilla editoreilla tai lisäosilla. WordPressiin löytyy lisäosa, jonka avulla voi tuoda omia tiedostoja osaksi WordPress-sivua. Kustomoituihin tiedostoihin voidaan kirjoittaa sekä HTML- että PHP-koodia. Yhteys otetaan sovelluksen tietokantaan.

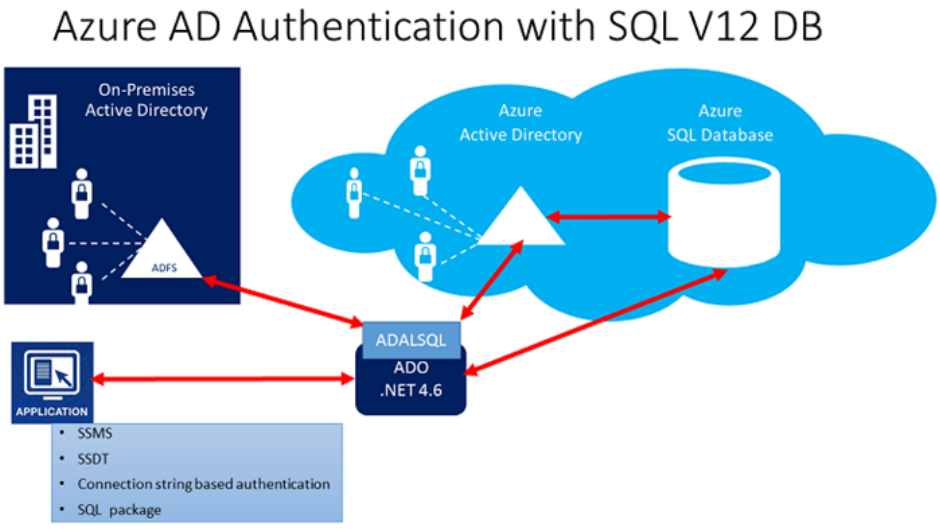
Azure-palvelun hallinnoinnin rakenteessa on kaksi ylläpitotason käyttäjää yhtä SQL-palvelinta kohden (kuva 5). Toinen käyttäjä on SQL-palvelimen ylläpitäjä ja toinen on Azure-aktiivihakemiston ylläpitäjä. Aktiivihakemiston ylläpitäjällä on muuten samat oikeudet kuin palvelimen ylläpitäjällä, mutta lisäksi hän voi tehdä käyttäjiä aktiivihakemiston tilien tai ryhmien perusteella. Aktiivihakemiston ylläpitäjä voi olla aktiivihakemiston käyttäjä tai aktiivihakemiston ryhmä. Jos kyseessä on ryhmätason käyttäjä, sitä voi käyttää kuka vaan ryhmään kuuluva henkilö. (Microsoft 2018c.)



Kuva 5. Azure-palvelun ylläpidon arkkitehtuuri (Microsoft 2018c).

Tietokantaan päästään käsiksi aktivoimalla autentikointi kuvan 6 mallin mukaisesti käyttäen Azure-aktiivihakemistoa. SQL-tietokannan käyttäminen edellyttää tässä tapauksessa, että käyttäjä on määritelty Azure-aktiivihakemistoon tietokannan käyttäjänä. Tarkoitus on käyttää uutta aktiivihakemistoa. Uusi aktiivihakemisto on eri toimialueella kuin Hämeen ammattikorkeakoulu, ja sinne voi kirjautua Microsoft Online -palvelussa. Luodaan

siis SQL-palvelimen tietokannan käyttäjät. Tietokannan käyttäjiä ei voi ylläpitäjää lukuun ottamatta luoda Azure-portaalissa. Azure SQL -palvelimeen määritetyt roolit eivät automaattisesti anna oikeutta ottaa yhteyttä SQL-tietokantaan. Lupa yhteydenottoon täytyy määritellä suoraan tietokannassa käyttäen Transact SQL -ilmaisua. (Microsoft 2018a.)



Kuva 6. Yhteydenotto SQL-tietokantaan Azure-aktiivihakemistoa hyödyntävällä tunnistautumisella (Microsoft 2018c).

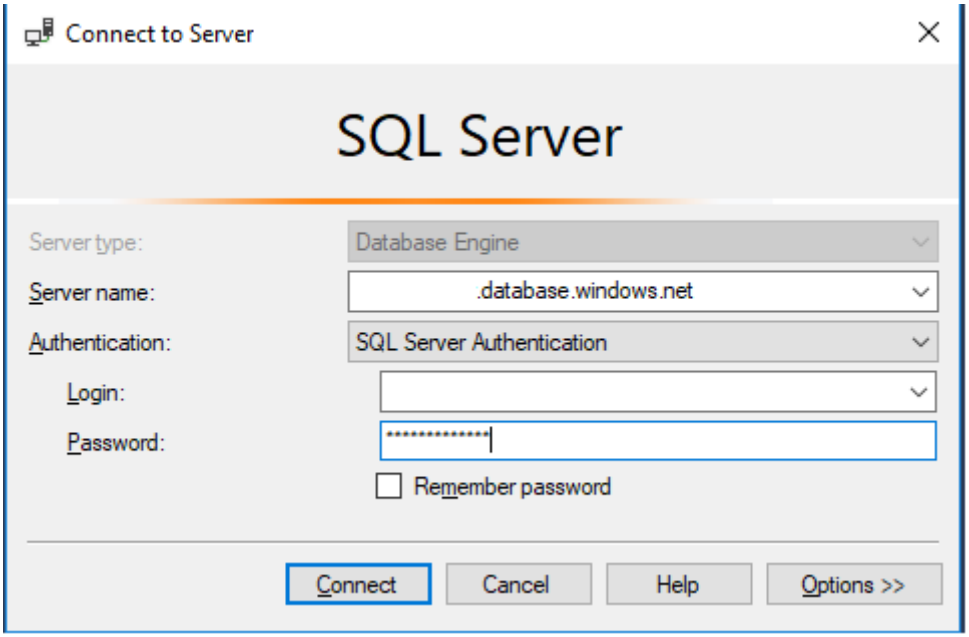
Kun käytetään Azure-aktiivihakemiston identiteettejä tietokantaan tunnistautumisessa, on kolme vaihtoehtoa siihen, miten se voidaan toteuttaa. Yksi on käyttää integroitua Windows-autentikointia, toinen on käyttää Azure-aktiivihakemiston pääasiallista nimeä ja salasanaa, ja kolmas vaihtoehto on käyttää sovelluksiin jaettavia tunnisteita (*tokens*) (Microsoft 2018). Pääasiallinen todennus tarkoittaa esimerkiksi Windows-tiliä tai Azure-aktiivihakemiston tiliä. (Microsoft 2018c.)

Uusia tunnuksia, joilla käytetään tietokantaa, luodaan siis pääasiallisten tunnusten perusteella. Uusi tunnus on käyttäjätunnus, jonka tiedot kartoitetaan yhteenkuuluviksi pääasiallisen tunnistautumisen kanssa. Jotta voidaan tehdä uusia käyttäjiä, tietokantaa muokkaavalla käyttäjällä täytyy olla päällä ALTER ANY USER -määritys. Sellaisen määrityksen voi tehdä kenelle tahansa tietokannan käyttäjistä. (Microsoft 2018a.)

Uusia käyttäjiä voi luoda monella eri tapaa. Voidaan luoda tietokannan käyttäjä, joka edustaa Azure-aktiivihakemiston tai tilauksen alla hallinnoitua verkkotunnuksen käyttäjää. Tämän pitäisi tarkoittaa sitä, että saman tilauksen alla olevan toimialueen käyttäjän pystyy liittämään tietokannan käyttäjäksi. Voidaan myös luoda saman toimialueen alla olevasta pääkäyttäjästä (*Principal*) samanniminen tunnus. (Microsoft 2018a.)

Määritetään työn tekijä aktiivihakemiston ylläpitäjäksi (*admin*), jotta voidaan muokata SQL-palvelinta. Seuraavaksi täytyy tarkistaa, että tietokantaa käyttävillä tietokoneilla on asennettuna .NET-kehyksen versio 4.6 tai myöhempi. Kehyksen saa ladattua Microsoftin verkkosivuilta. Myös Azure-aktiivihakemiston autentikointikirjasto ADALSQL.DLL täytyy ladata Microsoftin latauskeskuksesta. (Microsoft 2018a.)

Yksi tapa luoda tietokantayhteys on käyttää SQL Server Management Studio -ohjelmistoa. Kuvassa 7 luodaan tietokantayhteys tietokantaan. Kirjautumistunnus on SQL-palvelimen ylläpitotason käyttäjä.



Kuva 7. Kuvakaappaus yhteyden luomisesta SQL-tietokantaan.

Kun yhteys tietokantaan on luotu, voidaan klikata tietokantaa ja tehdä uusi kysely. Kysely tehdään muodossa: CREATE USER [käyttäjätunnus.toimialue.onmicrosoft.com]. (Microsoft 2018a.)

Sovellustasolla käyttäjä voi ottaa yhteyttä tietokantaan eri tavoin. Tietokantayhteyttä varten luotuja työpöydän asiakasohjelmia ovat esimerkiksi SQL Server Management Studio ja SQL Server Data Tools. Voidaan myös luoda yhteyksiä käyttämällä tietokantaan liitettyjä merkkijonoja (*connection strings*). (Microsoft 2018a.)

SQL-palvelimella on käytössä palomuuri, joka estää kirjautumisen aina, kun ei ennalta tiedetä uuden kirjautujan tietokonetta. Palomuuri antaa oikeuksia käyttää tietokantaa jokaisen uuden pyynnön perusteella kartoitettavasta IP-osoitteesta. SQL-tietokanta on käytettävissä vain TCP-portin 1433 kautta. Tietokantaan yhteyttä ottavan asiakaskoneen palomuurin

tarvitsee siis hyväksyä lähtevä liikenne kyseisestä portista. Azure-portaalissa täytyy olla yksi tai useampi palomuurin sääntö, joka sallii pääsyn SQL-palvelimelle. Jokaiseen määritykseen voi antaa yksittäisen IP-osoitteen tai IP-osoitealueen. (Microsoft 2017a.)

Yhteydenottoyrityksen tapahtuessa tietokantaan Internetin ja Azure-palvelun kautta katsotaan, läpäistäänkö tietokantatasoiset palomuurisäännöt. Jos ne läpäistään ja osoite löytyy tunnistetusta osoitealueesta, yhteys voidaan luoda suoraan tietokantaan. Jos osoitetta ei entuudestaan tunneta, tutkitaan, päästäänkö läpi palvelintason säännöistä. Jos palvelintason säännöt läpäistään, päästään käsiksi kaikkiin palvelimen kantoihin. (Microsoft 2017a.)

Azure SQL -palvelimeen päin vaikuttaa olevan paljon yhteyksiä blokattu, joten jos siihen haluaa ottaa yhteyttä asiakasohjelmalla, voidaan käyttää VPN-ohjelmistoa. Palvelimella olevaa tietokantaa voi kuitenkin lukea käyttämällä esimerkiksi Microsoft Azure Storage Explorer -ohjelmistoa.

6.4 Sisällöntuottaminen

Käytännön toteutusta sisällöntuottamiseen lähdettiin tekemään niin, että WordPress ja Azure-palvelu ikään kuin erotettiin toisistaan. Tämä tarkoittaa käytännössä sitä, että WordPressissä ei suoraan oteta yhteyttä DigiTrail-hakemiston tietokantaan. WordPressissä esimerkiksi Contributor-tason käyttäjä voi luoda siihen tarkoitetulle hallintasivulle julkaisuja, joissa annetaan uusi reitti. Uuteen reittiin kuuluu sen nimi, kuvaus ja varsinainen GPX-tiedosto. Kun kirjoitus on luotu, admin-tason käyttäjä käy tarkistamassa kirjoituksen, lataa kirjoituksen tiedot itselleen ja käsin syöttää tiedot Azure-portaalissa tietokantaan.

WordPress-oletusasetusten mukaan WordPress-tietokantaan ei voi ladata GPX-tiedostoja (WordPress.org n.d.c). Tälle tiedostomuodolle etsitään siis jokin toinen tapa. Maps Marker Pro -lisäosan Add new marker -näkymässä voidaan lisätä näkymään oma GPX-tiedosto. Tiedostoja voidaan käyttää hyväksi niin, että voidaan luoda uusi reittipiste valittuun paikkaan reitillä.

6.4.1 MapBox

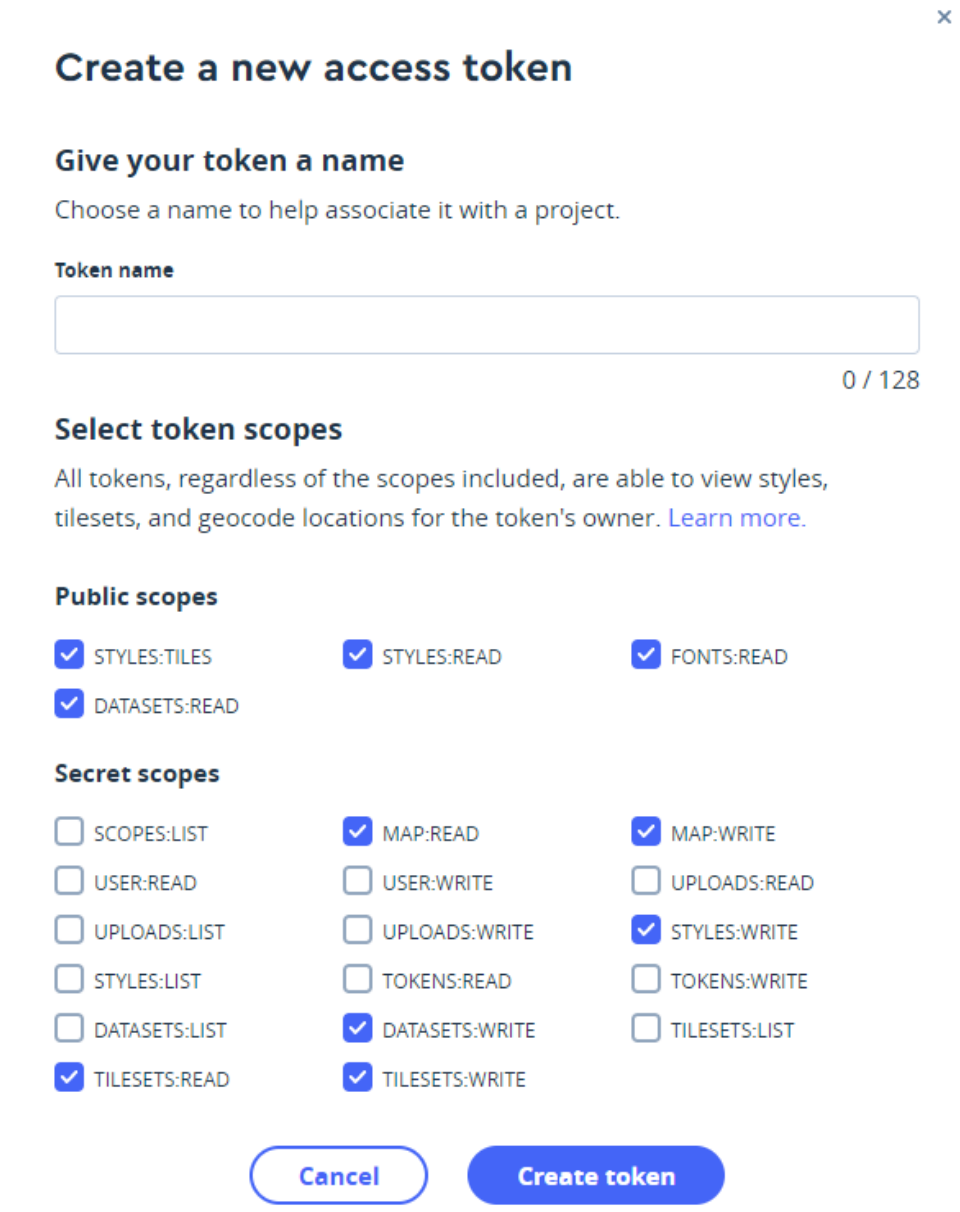
MapBox on suuri verkkokarttojen tarjoaja sivustoille ja verkkosovelluksille. Palvelun avointen rajapintojen (*API*) avulla voi lisätä omiin sovelluksiin sijaintitietoa, kuten haku- ja navigaatiopalveluja. (MapBox n.d.a.)

Palvelussa voi muokata karttoja MapBox Studiossa. Muokattavia karttoja kutsutaan tyyleiksi (*styles*). Tyyleihin valitaan jokin peruspohjista, riippuen siitä mitä käyttäjä haluaa painottaa. Vaihtoehtoja ovat esimerkiksi satelliittikartat, ulkoilmaa ja luontoa korostavat kartat tai katunäkymiä korostavat

kartat. DigiTrail-hankkeessa halutaan käyttää sellaisia karttoja, jossa luontopolut erottuvat hyvin kartassa, joten käytetään MapBoxin Outdoors-tyylejä. (MapBox n.d.b.)

6.4.2 Karttojen tuominen sivustolle

Tyyliä voi käyttää WordPressissä tekemällä tyyliin yhdistämistä varten tunnisteen (*token*), johon määritellään oikeudet muokata kartan sisältämää dataa. Oikeuksia muokata kartan sisältöä voidaan määritellä erikseen esimerkiksi tyylien, datasettien tai tilesettien mukaan (kuva 8).



Kuva 8. Salaisen tunnisteen luominen MapBox-palvelussa.

Tyyli halutaan jakaa muokattavaksi ”ShortCode”-ominaisuuksien eli koodinpätkien (*snippets*) avulla. Tätä varten asennetaan ShortCodes-lisäosa,

jonka avulla voidaan samaan koodinpätkään varastoida HTML- ja JavaScript -koodia. Koodinpätkässä varastoitu koodi suoritetaan siinä sivussa tai julkaisussa missä sitä käytetään. Ohjelmakoodissa halutaan ladata MapBox GL JS -kirjastot sivuston käyttöön ja tehdä sivulle ladattavasta kartasta uusi muuttuja. (Chakravarthy 2017.)

```
<script src='https://api.mapbox.com/mapbox-gl-js/v0.44.1/mapbox-gl.js'></script>
<link href='https://api.mapbox.com/mapbox-gl-js/v0.44.1/mapbox-gl.css' rel='stylesheet' />


<div id='map' style='width: 100%; height: 600px;'></div>
<script>
  mapboxgl.accessToken =
                                                                                    ';
  var map = new mapboxgl.Map({
    container: 'map',
    style: 'mapbox://styles/anttijun/cj9towgzh367k2so1epjp8sbj'
  });
</script>
```

Kuva 9. Kuvakaappaus koodinpätkästä, jolla tuodaan kaikki DigiTrail-hankkeen reitit sisältävä kartta sivustolle.

Kun ohjelmakoodi on tallennettu, siihen voidaan viitata sivuston missä tahansa paikassa. Viittaus tapahtuu valitsemalla ShortCode-widget ja täyttämällä Content-kohta. WordPressissä widget on sivuston itsenäinen osa, joka suorittaa tietyn toiminnon tai koodin, joka luo tällaisen alueen. Esimerkiksi WordPressissä on sisäänrakennettu widget, joka näyttää luettelon viimeaikaisista kommenteista sivuston Dashboardissa (WordPress.org n.d.b). Tässä tapauksessa Content-kohta täytetään näin: [sc name="addDigiTrailMap"]. (Chakravarthy 2017.)

Kun kartta on tuotu valitulle sivulle, siinä näkyy kaikki DigiTrail-hankkeen reitit (kuva 10). Seuraavaksi ratkaistavaksi asiaksi muodostuu se, miten voidaan saada näkymiä pelkästään niistä reiteistä, mitä halutaan nähdä kullakin sivulla.

Kuva 10. DigiTrail-hankkeen reitit kartalla.

6.4.3 Reittien ja reittipisteiden lisääminen

Leaflet Maps Markerilla (WordPress-lisäosa) voi näyttää WordPress-sivustolla karttoja. Karttoihin voi myös luoda reittipisteitä. (WordPress.org n.d.d.)

Määritettiin, että Maps Marker -lisäosassa voidaan Base Mapiksi valita MapBox. MapBoxiin voi lisätä kolme erilaista yksilöityä karttaa, joten projektissa voidaan käyttää kolmea eri hankkeen teemaa. Jotta voi luoda uusia reittipisteitä tai kerroksia (*layers*), niitä varten tulee olla valittuna tietty Base Map. Base Mapissa näkyy kaikki hanketta varten luodut reitit. Kerrokset taas mahdollistavat sen, että kartassa voi näyttää useampia luomiansa reittipisteitä samanaikaisesti.

MapBox vaatii mukautetun API-käyttöoikeusominaisuuden käyttämistä. Mukautetut MapBoxin pohja-arvot eivät enää toimi, jos on rekisteröinyt MapBox-tilin tammikuun 2015 jälkeen. Ongelman voi kuitenkin ratkaista lataamalla Maps Marker -lisäosasta Pro-tason version. Versio otetaan 30 päivän testikäyttöön Trial-lisenssiavaimen avulla. Pro-versiolla pystyy myös kunnolla lisäämään MapBox-kartalle karttapisteitä haluttuihin koordinaatteihin. (Maps Marker n.d.)

Hankittiin kartan tekijältä API-käyttöoikeusominaisuus ja lisättiin se Maps Marker -lisäosaan, ensimmäisen luodun kartan asetuksiin. Varmistettiin, että peruskartan valikossa näkyy juuri konfiguroitu MapBox-kartta.

Luotiin uusi salainen (*secret*) tunniste, johon annettiin laajennetut oikeudet käyttää APIa. Uusi tunniste määrittää haltijalleen esimerkiksi luku- ja kirjoitusoikeudet MapBox-sivustoon luotuihin tyyleihin ja datasetteihin.

Käytössä oleva Antti Juntusen tekemä MapBox-kartta on luotu niin, että MapBox-sivustolla GPX-tiedostot on määritelty tietyiksi joukkioiksi (*data-sets*) ja näistä joukkioista on luotu kerroksia kartalle. Esimerkiksi helpot reitit voidaan tuoda GPX-tiedostoina palveluun ja koota ne yhdeksi kerrokseksi.

Kun luodaan uutta reittipistettä, voidaan karttaan tuoda GPX-tiedosto omalta koneelta. Samasta valikosta löytyy myös ohjeet siitä, kuinka voidaan yhdistää monia GPX-tiedostoja yhdeksi tiedostoksi.

7 YHTEENVETO

Opinnäytetyön tekijä on oppinut paljon uutta Azure-palvelun ominaisuuksista, SAML-tekniikasta ja www-sisällönhallinnasta. Tekijä on myös oppinut luomaan tietokantayhteyksiä käyttäen siihen tarkoitettuja asiakasohjelmia kuten SQL Server Management Studiota.

Opinnäytetyön tekijä on luonut kirjautumisjärjestelmän, joka hyödyntää hankkeeseen luotua, uuteen toimialueeseen luotua aktiivihakemistoa. Kun käyttäjä on kirjautunut, palveluntarjoaja kartoittaa asiakkaan identiteetin tiedot henkilöllisyydentarjoajalta ja näyttää ne oikeassa muodossa.

Tutkimuskysymyksiin vastaaminen onnistui työssä tyydyttävästi. Työssä saatiin esimerkiksi selville, kuinka WordPress voidaan saada keskustelemaan Azure-tietokannan kanssa. Kirjautumisjärjestelmän toteutus kävi työssä ilmi. Kysymykset, jotka koskivat sivuston päivittämistä ja ylläpitämistä taustapalveluiden loppumisen jälkeen, jäivät ilman kattavaa, käytännönläheistä vastausta. Nämä kysymykset paljastuivat tämän työn kannalta epäolennaisiksi verrattuna keskeisten palveluiden rakentamiseen.

Työn teoriaosuudessa kerrotaan www-sisällönhallinnasta, esitellään Microsoft Azure -palvelua sekä kuvataan sivustolle rakennetun kirjautumisjärjestelmän taustatekniikoita, eli käydään lyhyesti läpi SAML-tekniikan toimintaperiaatteet sekä otetaan myös tietoturva huomioon.

Työn käytännön osuudessa toteutettiin kirjautumisjärjestelmä ja määriteltiin eri rooleja sivustoon kirjautuneille käyttäjille sisällöntuottamista varten. Käytännön tasolla selvitettiin erityisesti myös sitä, minkälaisin keinoin Microsoft Azure -palvelun ja WordPress-järjestelmän saa keskustelemaan keskenään. Tämä edellytti Azure-ominaisuuksien läpikäymistä työn teoriaosuutta syvällisemmin.

Keskeisimpiin haasteisiin projektin kannalta kuuluu se, että sivusto on hallinnoitu erillisellä palvelimella, eikä sivuja esimerkiksi luoda suoraan Azure-palveluun. Erilliselle palvelimelle ei ole hankkeessa pääsyä. Projektissa heräsi idea, että pitäisikö HAMKin tietohallinnolta pyytää käyttöön SSH-tunnukset, joilla kirjautua HAMKin palvelimelle, esimerkiksi niin, että on pääsy hankkeen WordPress-tiedostoihin.

Ideaalissa tapauksessa uutta sisältöä luotaisiin uuden aktiivihakemiston käyttäjien tunnuksilla, mutta ratkaisu edellyttäisi koko Azure-toimialueen tietojen siirtämistä toiseen. Toistaiseksi käytetään siis vanhaa toimialuetta. Uudessa käytännön toteutuksessa ei voida hyödyntää hankkeeseen luotua DigiTrail-hakemiston aktiivihakemistoa, koska kävi ilmi, että se on vain vä-

liaikainen ja että se poistuu palvelusta pian opinnäytetyön tekemisen jälkeen. Projektissa kävi ilmi, että edes projektin SQL-palvelimen ylläpitäjällä ei ole oikeutta luoda käyttäjiä HAMK-toimialueen aktiivihakemistoon.

Vaikka SQL-palvelimella pystyttäisiin tunnistamaan aktiivihakemiston käyttäjiä, siitä ei ole WordPressissä hyötyä, koska tiedostoon kirjoitettavia yhteydenottoja ei voi käyttää Azure-aktiivihakemiston tunnusten avulla. Kun navigoi yhteyden luomista varten tarkoitettujen merkkijonojen asetuksiin, nähdään että PHP-lomakkeella voi saada yhteyden vain SQL-palvelimeen luotujen tunnusten avulla.

Työn seuraava vaihe on luoda WordPress-järjestelmään yksinkertaisia yhteydenottolomakkeita, joiden avulla pystytään hakemaan tietokannassa olevaa sisältöä, muokkaamaan vanhaa sisältöä ja luomaan uutta. Tämä edellyttää kuitenkin sitä, että rakennetaan WordPressin ja Azure SQL -tietokannan välinen yhteys, jonka kautta tietokannan sisältöjä voidaan dynaamisesti muokata.

Työssä myös olisi oleellista selvittää, minkälaisia mahdollisuuksia ShortCodes-lisäosan tai jonkun muun työkalun avulla on muokata MapBox-karttojen sisältöjä. Voisi selvittää, voidaanko sivustolla suodattaa valitusta kartasta sen eri kerroksia. Esimerkiksi sivulla, jossa kerrotaan Aulangon reiteistä, voisi näyttää vain Aulangon reitit yhtenä kerrokseen liitettynä GPX-tiedostona. Tämän opinnäytetyön valmistumisen jälkeen hankkeen seuraava WordPress-ylläpitäjä jatkaa tätä työtä.

Niin kuin kuvasta 6 käy ilmi, SQL-palvelin ja tunnistautumiseen käytettävä aktiivihakemisto pitäisi olla samalla toimialueella, jotta SQL-serverille voi määrittää AAD-ylläpitäjän. SQL-palvelimella nimenomaan AAD-ylläpitäjän täytyy luoda uudet tietokannan käyttäjät pääkäyttäjien tunnusten perusteella (kuva 5). HAMKin tietohallinnolle pitäisi ehkä tehdä ehdotus, että DigiTrail-toimialueen aktiivihakemisto siirrettäisiin HAMKin toimialueeseen.

Valmiit, sovellukseen lisättävät reitit ja reittipisteet on tarkoitus tuoda Azure-palvelun Blob-tallennustilaan manuaalisesti hankkeen ylläpitäjän toimesta. Reittipisteitä voi Maps Marker -lisäosan kautta viedä WordPressistä muihin sijainteihin.

LÄHTEET

Aakash Chakravarthy (2017). ShortCoder. Haettu 5.3.2018 osoitteesta https://www.aakashweb.com/wordpress-plugins/shortcoder/

AuthenticationWorld (n.d.). Single Sign On. Haettu 4.2.2018 osoitteesta https://archive.is/20140315095827/http://www.authentication-world.com/Single-Sign-On-Authentication/

HAMK (n.d.a). DigiTrail – Kanta-Hämeen reitistöjen saavutettavuus ja näkyvyys. Haettu 14.1.2018 osoitteesta *http://www.hamk.fi/tyoelamalle/hankkeet/digitrail/Sivut/default.aspx*

HAMK (n.d.b). Älykkäät palvelut -tutkimusyksikkö. Haettu 10.1.2018 osoitteesta *http://www.hamk.fi/tyoelamalle/tutkimusyksikot/alykkaat-palvelut/Sivut/default.aspx*

IETF (2005). RFC 3986 – Uniform Resource Identifier (URI): Generic Syntax. Haettu 10.2.2018 osoitteesta https://tools.ietf.org/html/rfc3986

Ite Wiki OY (n.d.). Julkaisujärjestelmät (CMS). Haettu 14.1.2018 osoitteesta https://www.itewiki.fi/opas/julkaisujarjestelma-cms/

Juntunen, A. (2018). Teema DigiTrail. Sähköpostiviesti tekijälle 22.2.2018.

Keso, T. (n.d.). Verkon ylläpito ja virtualisointipalvelut-moduulin verkkoaineisto, Moodle. Hämeen ammattikorkeakoulu. Haettu 21.1.2018 osoitteesta https://moodle.hamk.fi/

Korhonen, K. SAML 2.0 -tuen lisäys IMS-ohjelmistoon. Haettu 3.2.2018 osoitteesta https://www.theseus.fi/bitstream/handle/10024/76867/KarriKorhonenTheseus.pdf?sequence=1

MapBox (n.d.a). About MapBox. Haettu 22.2.2018 osoitteesta https://www.mapbox.com/about/

MapBox (n.d.b). Maps. Haettu 22.2.2018 osoitteesta https://www.mapbox.com/maps/

Maps Marker (n.d.) How to Register for a free MapBox API Access token and Setup Custom MapBox Basemaps. Haettu 5.3.2018 osoitteesta: https://www.mapsmarker.com/docs/apis/how-to-register-for-a-free-mapbox-api-access-token-and-setup-custom-mapbox-basemaps/

Microsoft (2013). Windows Azure Insider. Haettu 3.2.2018 osoitteesta https://msdn.microsoft.com/en-us/magazine/dn198240.aspx

Microsoft (2017a). Azure SQL Database server-level and database-level firewall. Haettu 19.2.2018 osoitteesta https://docs.microsoft.com/en-us/azure/sql-database/sql-database-firewall-configure

Microsoft (2017b). Database Transaction Units (DTUs) and elastic Database Transaction Units (eDTUs). Haettu 4.2.2018 osoitteesta https://docs.microsoft.com/en-us/azure/sql-database/sql-database-what-is-a-dtu

Microsoft (2017c). Introduction to Blob Storage. Haettu 1.2.2018 osoitteesta https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction

Microsoft (2017d). Single Sign-On SAML protocol. Haettu 3.2.2018 osoitteesta https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-single-sign-on-protocol-reference

Microsoft (2017e). What is Azure Active Directory. Haettu 10.02.2018 osoitteesta https://docs.microsoft.com/en-us/azure/active-directory/active-directory-whatis

Microsoft (2018a). Configure Azure AD auth. Haettu 18.2.2018 osoitteesta https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

Microsoft (2018b). Introduction to Microsoft Azure Storage. Haettu 1.2.2018 osoitteesta https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction

Microsoft (2018c). Use Azure Active Directory Authentication for authentication with SQL Database, Managed Instance, or SQL Data Warehouse. Haettu 18.2.2018 osoitteesta https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure

Microsoft (2018d). What is the Azure SQL Database service. Haettu 10.1.2018 osoitteesta https://docs.microsoft.com/en-us/azure/sql-database/sql-database-technical-overview/

Microsoft (n.d.a). Azure SQL Database pricing. Haettu 4.2.2018 osoitteesta https://azure.microsoft.com/en-gb/pricing/details/sql-database/single/

Microsoft (n.d.b) Public Key Infrastructure. Haettu 10.2.2018 osoitteesta https://msdn.microsoft.com/en-us/library/windows/desktop/bb427432(v=vs.85).aspx

Microsoft (n.d.c). What is Azure. Haettu 14.1.2018 osoitteesta https://azure.microsoft.com/en-gb/overview/what-is-azure/

Naktode, L. (2018) Query for WordPress SAML Single Sign on. Sähköpostiviesti tekijälle 5.2.2018.

OASIS (2004). SAML 2.0 -tietoturvaa. Haettu 31.1.2018 osoitteesta https://www.oasis-open.org/committees/download.php/8733/sstc-saml-sec-consider-2.0-draft-05-diff.pdf

OASIS (2005). Security Assertion Markup Language (SAML) V2.0 Technical Overview. Haettu 31.1.2018 osoitteesta https://www.oasis-open.org/committees/download.php/14361/sstc-saml-tech-overview-2.0-draft-08.pdf

Open Source Initiative (2007). The Open Source Definition. Haettu 31.1.2018 osoitteesta https://opensource.org/osd

Talvivaara, J. (n.d.). Verkon nimi- ja hakemistopalvelut. Haettu 9.2.2018 osoitteesta http://www2.amk.fi/mater/tietotekniikka/nimipalvelut/8_activedirectory.html

The PHP Group (n.d.). PHP: Hypertext Preprocessor. Haettu 21.1.2018 osoitteesta https://secure.php.net/

Tolvanen, P. (2007). *Web-sisällönhallintajärjestelmä - ominaisuudet ja käyttöönotto*. Pro gradu -tutkielma. Tietojenkäsittelytieteiden laitos. Jyväskylän yliopisto. Haettu 21.1.2018 osoitteesta http://www.projekti55.fi/tutkielmat/2007-gradu-web-sisallonhallintajarjestelma.pdf

W3C (2017). HTML 5.2: 1. Introduction. Haettu 21.1.2018 osoitteesta https://www.w3.org/TR/html/introduction.html#introduction/

WordPress.org (n.d.a) About WordPress. Haettu 31.1.2018 osoitteesta https://wordpress.org/about/

WordPress.org (n.d.b) Codex. Definitions of various terms. Haettu 14.1.2018 osoitteesta https://codex.wordpress.org/Glossary#MySQL/

WordPress.org (n.d.c) Codex. Uploading files. Haettu 22.2.2018 osoitteesta https://codex.wordpress.org/Uploading_Files#About_Uploading_Files_on_Dashboard

WordPress.org (n.d.d). Leaflet Maps Marker. Haettu 23.2.2018 osoitteesta https://wordpress.org/plugins/leaflet-maps-marker/

WordPress.org (n.d.e) Requirements. Haettu 31.1.2018 osoitteesta https://wordpress.org/about/requirements/

WordPress.org (n.d.f) Roles and Capabilities. Haettu 10.2.2018 osoitteesta https://codex.wordpress.org/Roles_and_Capabilities

WordPress.org (n.d.g) SAML Single Sign On – SSO – WordPress Plugins. Haettu 27.1.2018 osoitteesta https://wordpress.org/plugins/miniorange-saml-20-single-sign-on/

Liite 1

DigiTrail-teemat, teemojen luontiopas

Teemat

Teemat ovat reittien varrelle luotuja karttapisteitä, jotka pongahtavat ilmoituksena Android-laitteen näytölle, kun käyttäjä saapuu karttapisteen vaikutusalueelle. Reitin teemana voi esimerkiksi olla jooga ja jokaisen karttapisteen sisältönä yksi joogaliike, jonka käyttäjä suorittaa reitin varrella. Reitillä voi olla useita eri teemoja joista käyttäjä voi valita, mutta reitillä voi olla vain yksi teema päällä kerrallaan. Teemakarttapiste voi pitää sisällään tekstiä, kuvia ja linkin videoihin tai muuhun verkkosisältöön (tarkemmat tiedot osiossa Teemakarttapisteen tekninen toteutus).

Kuva 1. Teemapisteet reitillä Aulanko helppo.

Teemakarttapisteen tekninen toteutus
Käyttäjälle näkyvän ilmoituksen rakenne on kuvattu seuraavassa kuvassa (kuva 2).

Kuva 2. Käyttäjälle näkyvä ilmoitus teemakarttapisteestä.

Ilmoitus koostuu
- kuvasta
- tekstistä
  - otsikko
  - sisältöteksti
- mahdollisesta linkistä

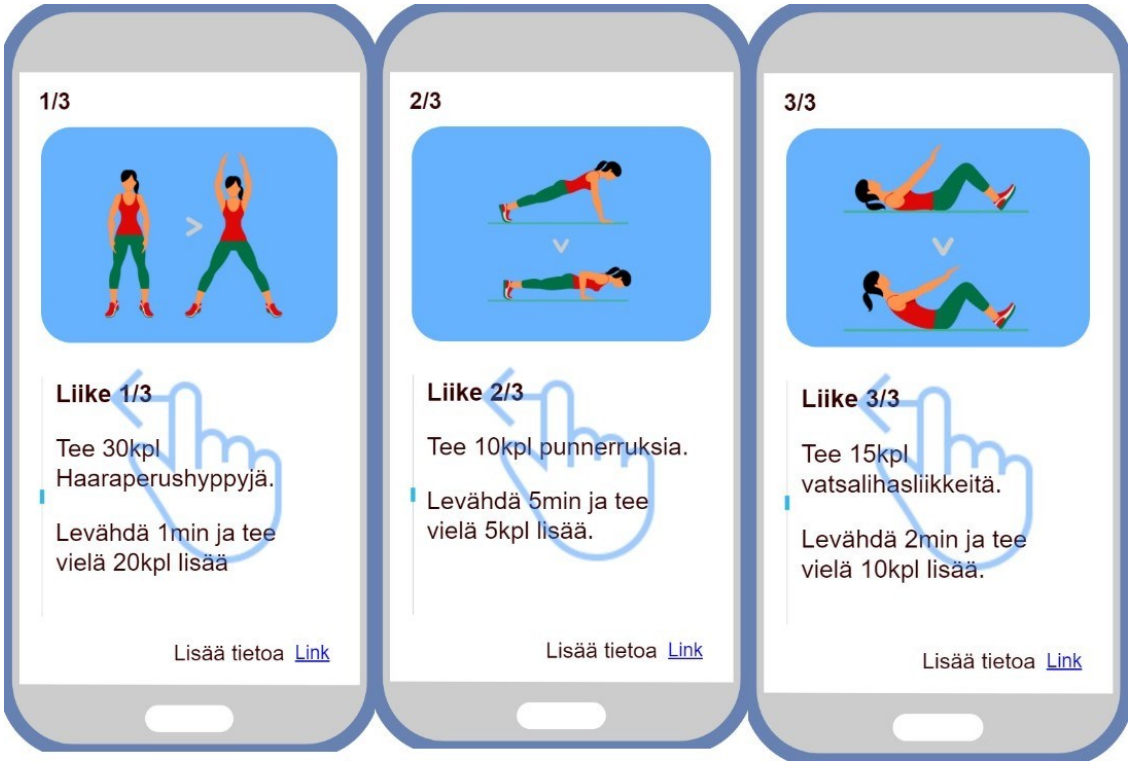
Sivuja voi olla useita ja sormella pyyhkäisemällä voi vaihtaa sivua. Osioita voi jättää pois, ilmoitus voi esimerkiksi pitää sisällään vain tekstiä. Linkki aukeaa Android-laitteen selaimeen, joka tarvitsee verkkoyhteyden. Ota siis huomioon, että verkkoyhteys ei välttämättä toimi reitillä tai käyttäjän puhelimessa ei ole verkkoyhteyttä.

Tekniset rajoitukset:

- Kuvan suurin sallittu tiedostokoko: 1.0MB (1000KB)
- Kuvan tiedostomuoto: PNG tai JPG
- Teemakarttapisteen sijainti muodossa: leveys pituus koordinaatit (esim. 60.976375, 24.477953)
- Teemakarttapisteen etäisyys seuraavaan teemapisteeseen vähintään: 100m
- Teemakarttapisteen vaikutusalue: 10-50m
- Sisältötekstin pituus korkeintaan: 1000 merkkiä
- Verkkosivun linkki voi olla minne vain, esim. Youtube-videoon tai kotisivuille. Varmista että linkki on toimiva myös tulevaisuudessa. Linkki ei toimi offline-tilassa.
- Yhdellä teemapisteellä voi olla enintään 3 sivua/näkymää. Teemapisteitä voi olla useita.

Ota huomioon:

- Kuvan maksimikoko on pieni, koska haluamme että sovellus on mahdollisimman sulavasti toimiva. Suuret kuvat latautuvat pitkään ja verkkoyhteys voi olla paikoittain hidas. Voit pienentää ja pakata kuvia eri tietokoneohjelmilla (esim. Paint, ohje: https://www.wikihow.com/Resize-an-Image-in-Microsoft-Paint)
- Teemakarttapistettä ei voi sijoittaa metrin tarkkuudella, joten et voi kohdistaa teeman pistettä fyysisesti olemassa olevaan kohteeseen, esimerkiksi tiettyyn puuhun. Tämä johtuu siitä, ettei Android-laitteen GPS-paikannus ole tarpeeksi tarkka. Voit toki laittaa teeman tehtäväksi esimerkiksi ”etsi läheiseltä alueelta vanha koivu” ja seuraavalle teeman sivulle koivun mielenkiintoista historiaa tms.
- Teemareittipisteen koordinaatit voit poimia vaikka sivustoa https://www.geoplaner.com/ käyttäen (huom. vaihda kartta OSM-karttaan, jotta näet polut ja maaston paremmin). Huomaa, että arvojen on oltava muotoa 60.976375, 24.477953.
- Karttapisteen vaikutusalue tarkoittaa aluetta, jossa käyttäjä saa ilmoituksen saapumisestaan teemapisteelle. Arvoksi syötetään siis säde, ei halkaisija.
- Pidä teksti lyhyenä ja ytimekkäänä, jotta käyttäjällä pysyy mielenkiinto yllä. 1000 merkkiä ehdoton maksimi.
- Linkit eivät toimi offline-tilassa, teeman tulisi toimia myös pelkästään kuvan ja tekstin pohjalta. Jos linkki on tärkeässä osassa teemaa, laita verkkosivuille ruksi ”Teema ei toimi ilman verkkoyhteyttä”.



Kuva 3. Esimerkki teemakarttapisteestä, jossa teemana kuntoilu.

Liite 2

Setup guide for Azure AD as IdP

STEP 1: Navigate to Azure Management Console. Proceed to the Azure Active Directory tab and navigate to the App Registrations Tab. Click on New Application Registration.

STEP 2: You need to enter the Name of the application. Select the application type as Web app/ API. And then enter the Sign-on URL. That relates to the ACS URL as shown in the Identity Provider tab of the plugin. Click on the Create button below to create the application.

Step 3: To configure the App ID URI, Select your application from the displayed apps. Select Properties in the Settings Tab. Enter the App ID URI in the respective field which relates to the SP Entity ID / Issuer in Identity Provider tab of the plugin and save the properties.

STEP 4: Navigate to the Endpoints button. There will be a metadata URL Information in this metadata document is required to configure your miniOrange WordPress SAML SSO plugin. Enter the following values in the Service Provider tab in the plugin configuration.

- IDP Entity ID: EntityID in the Federation Metadata document.
- SAML Login URL: The SAML-P Sign On Endpoint URL (See Image)
- SAML Logout URL: The SAML-P Sign Out Endpoint URL (See Image)
- X.509 Certificate: x.509 Certificate in the Federation Metadata document.

STEP 5:
In miniOrange SAML plugin, go to Attribute Mapping Section of Attribute/Role mapping Tab. Enter the following values: Note: You will get this values from the Test Configuration Result in Service Provider Tab.

- Username: Name of the username attribute from IDP (Keep NameID by default)
- Email: Name of the email attribute from IDP (Keep NameID by default)
- Full Name Attribute: Name of the firstname attribute from IDP and Name of the lastname attribute from IDP

OR

- Username: Name of the username attribute from IDP (Keep NameID by default)
- Email: Name of the email attribute from IDP (Keep NameID by default)
- FirstName: Name of the firstname attribute from IDP
- LastName: Name of the lastname attribute from IDP
- Group/Role Attrinute name of the groups/role received in SAML Response
- Display Select display name from drop-down list

STEP 6:
Go to Role Mapping Section of Attribute/Role mapping Tab tab. Enter the following values:
You can check the Test Configuration Results to get a better idea as to which values to map here.
Under the Role Mapping Section configure which GROUP value coming in the SAML response needs to be mapped to which role. The Group value coming in the SAML response will be mapped to the Role assigned here and the user will be assigned that role.

STEP 7:
Go to Sign In Settings tab. Enable Auto Redirect to IdP and Enable backdoor login option. Copy the URLs for backup.