Tampereen yliopisto

Pekko Vilpola

Kertakirjautumisen implementointi WordPress-sivulle Google Apps Login -palvelun avulla

Informaatioteknologian ja viestinnän tiedekunta
Kandidaatintyö
Kesäkuu 2019

TIIVISTELMÄ

Pekko Vilpola
Kertakirjautumisen implementointi WordPress-sivulle Google Apps Login -palvelun avulla
Tampereen yliopisto
Ohjelmistotekniikka
Kandidaatintyö
Kesäkuu 2019

Organisaatioiden ja palvelujen rajojen hämärtyessä on tarvetta keskitetylle autentikoinnille ja auktorisoinnille. Kertakirjautuminen tarjoaa ratkaisun tähän ongelmaan. Kertakirjautumisen avulla käyttäjä saa pääsyn useisiin palveluihin ja resursseihin yksillä tunnuksilla ja tunnistautumistiedoilla. Ratkaisulla vältytään toteuttamasta tunnistautumista toisteisesti, samalla tunnistautumistietojen ylläpito voidaan hoitaa keskitetysti.

Tutkielmassa perehdytään kertakirjautumiseen, sen haasteisiin ja kirjautumiseen liittyviin tekniikoihin. Käytännön työnä toteutetaan kertakirjautuminen WordPress-sivulle Google Apps Login -palvelun avulla. Tutkimusta varten luodaan oma verkkotunnus ja sinne WordPress-sivu. Luodun sivun tietoturvaa parannetaan asetusten konfiguroinnilla.

Tutkimus osoittaa, että kertakirjautuminen laajasti käytössä olevan palvelun tunnuksilla parantaa sivun käytettävyyttä ja lisää tietoturvaa. Tietoturvaa vaarantavia tekijöitä ovat päivittämättömät WordPress-versiot ja -liitännäiset, sekä puutteelliset asetukset. Kertakirjautumisen implementointi WordPress-sivulle osoittautui yksinkertaiseksi toimenpiteeksi. Asetusten muokkauksella pystyttiin parantamaan luodun sivuston tietoturvaa. Kertakirjautumisen haasteista todettiin olevan keskeisimpiä sitä hyödyntävien sivujen puutteellinen toteutus ja uloskirjautumisen standardoinnin puute.

Avainsanat: WordPress, kertakirjautuminen, verkkopalvelu, tietoturva

LYHENTEET JA MERKINNÄT

API	ohjelmointirajapinta, lyhenne sanoista Application Programming Interface, rajapinnan avulla sovellukset voivat keskustella ja vaihtaa tietoja
FTP	tiedostojensiirtoprotokolla, lyhenne sanoista File Transfer Protocol
HTML	hypertekstin merkintäkieli, lyhenne sanoista Hypertext Markup Language
HTTP	hypertekstin siirtoprotokolla, lyhenne sanoista Hypertext Transfer Protocol
HTTPS	HTTP-protokollan ja TLS/SSL-protokollan yhdistelmä, lyhenne sanoista Hypertext Transfer Protocol Secure
TSL/SSL	salausprotokolla, lyhenteet sanoista Transport Layer Security (TLS) ja Secure Sockets Layer (SSL)

SISÄLLYSLUETTELO

1. JOHDANTO 1
2. AUTENTIKOINTI JA AUKTORISOINTI 2
2.1 Autentikointi 2
2.2 Auktorisointi 2
3. KERTAKIRJAUTUMINEN 3
3.1 Protokollat ja tekniikat 3
3.1.1 SSL 4
3.1.2 OAuth 5
3.2 Kertakirjautumispalvelut 6
3.2.1 AD 6
3.2.2 Facebook Connect 7
3.2.3 Google Sign-in 7
4. KERTAKIRJAUTUMISEN TIETOTURVA 8
4.1 Suunnitteluratkaisut tietoturvan uhkana 9
4.2 Uloskirjautumisen haasteet 9
5. TUTKIMUKSEEN VALITUT PALVELUT 10
5.1 WordPress 10
5.2 Google Apps Login 11
6. WORDPRESSIN ASENNUS JA ASETUSTEN KONFIGUROINTI 12
6.1 WordPress-sivun luominen 12
6.2 Google Apps Login – liitännäisen lisääminen WordPress-sivulle 12
6.3 Asetusten konfigurointi 14
6.4 Tietoturvaliitännäiset 15
7. TULOKSET 16
8. YHTEENVETO 17
LÄHTEET 18

1. JOHDANTO

Kertakirjautuminen on keskeisessä asemassa nykyaikaista tietotekniikkaa, ja sen avulla voidaan toteuttaa tehokkaasti käyttäjätietojen- ja tunnustenhallinta (Joshi et al. 2018). Yksinkertaistetusti kertakirjautuminen voi käytännössä tarkoittaa kirjautumista sivustolle Gmail- tai Facebook-tunnuksilla. Kertakirjautumismekaniikat mahdollistavat tunnistautumisen ja autentikoinnin ulkoistamisen kolmannelle osapuolelle tai keskitetyille palvelimille. WordPress on laajalle levinnyt ilmaispalvelu, jonka avulla pystytään luomaan verkkosivuja ja -palveluita. Vuonna 2015 suosituimpien kymmenen miljoonan verkkosivun joukosta 24 prosenttia oli toteutettu WordPress-palvelun avulla (Trunde & Weippl 2015). Yleisin palvelun sovelluskohde ovat blogit, mutta sen avulla pystytään luomaan myös suurempia kaupallisia sovelluksia. Uusien sivustojen ja palveluiden luominen on tehty yksinkertaiseksi, mutta asetusten ja liitännäisten tarkempi konfigurointi vaatii enemmän asiantuntemusta.

Kertakirjautumisen implementointiin WordPress-sivustolle on tarjolla useita palveluja asennettavien liitännäisten muodossa. Ongelmana on palvelun asentaminen ja konfigurointi, mikä voi osoittautua haasteelliseksi. Tässä työssä esitetään ratkaisu ongelmaan toteuttamalla WordPress-sivulle kertakirjautuminen Google Apps Login -kirjautumispalvelun avulla. Työn tavoitteena on tutustua WordPress-palvelun toimintaan ja asetusten räätälöintiin paremman tietoturvan saavuttamiseksi. Tämän työn sekundaarisena tarkoituksena on tutustua kertakirjautumiseen ja Google Apps Login -palveluun.

Tämän työn toisessa luvussa käsitellään autentikointi ja auktorisointi. Kolmannessa luvussa esitellään kertakirjautuminen sekä siihen liittyvät protokollat ja tekniikat. Neljännessä luvussa perehdytään kertakirjautumisen tietoturvaongelmiin. Viidennessä luvussa käsitellään työssä tutkittavat palvelut WordPress ja Google Apps Login. Kuudennessa luvussa kerrotaan, mitä käytännön tasolla tutkimuksessa tehtiin. Seitsemännessä luvussa esitellään tutkimuksen tulokset ja kahdeksannessa luvussa on yhteenveto tutkimuksesta.

2. AUTENTIKOINTI JA AUKTORISOINTI

Tässä luvussa määritellään termit autentikointi ja auktorisointi. Tiedon luotettavaan siirtoon verkossa tai järjestelmissä tarvitaan protokollia, siis sovittuja toimintamalleja. Käyttäjiin ja oikeuksiin perustuvat tietojärjestelmät tarvitsevat keinon todentaa käyttäjän tai palvelun henkilöllisyys tietoturvan takaamiseksi.

2.1 Autentikointi

Autentikoinnilla, jota kutsutaan myös todennukseksi, tarkoitetaan käyttäjän identiteetin varmistamista. Autentikointi on yleensä kaksiosainen tapahtuma, joka koostuu käyttäjän tunnistuksesta (identification) ja varmistuksesta (authentication). Käyttäjän salasanan tai tunnistetiedon tulee olla tallennettuna autentikoivalle taholle ennen autentikointia. Autentikointi voidaan tehdä lokaalisti tai kolmannen osapuolen avulla. Käyttäjän tai palvelun antamia tietoja verrataan autentikoivan tahon tallentamiin tietoihin, jotka voivat olla esimerkiksi salasanoja tai biometrisiä tunnisteita. (Jäppinen 2007)

Autentikoinnin uhkana on tunnistuksen ja varmistuksen luotettavuus. Tunnistetiedot tulee säilyttää salattuina ja autentikoinnissa tulee noudattaa turvallisia protokollia. Käyttäjällä on vastuu omasta toiminnastaan tietoturvan takaamiseksi. Salasanojen tulee olla riittävän vahvoja, avuksi voidaan käyttää salasanojen hallintaohjelmia. Käyttäjän tulee myös huolehtia ohjelmiensa versioiden ajantasaisuudesta, koska vanhentuneet ohjelmat voivat tarjota reitin hyökkääjälle päästä käsiksi tunnistetietoihin.

2.2 Auktorisointi

Auktorisointi eli valtuutus vastaa kysymykseen, onko käyttäjällä oikeus tiettyyn toimintoon. HTTP-protokollan otsikkokenttä *authorization* aiheuttaa sekaannusta termien käytössä, koska yleensä kyseessä on autentikointi (Autentikointi 2015). Lähteestä riippuen termejä käytetään tarkoittamaan hieman eri asioita. Usein puhutaan pääsynhallinnasta, käyttäjille tarjotaan pääsy tiettyihin tietoihin ja rajoitetaan pääsyä toisiin. Auktorisointi mahdollistaa käyttäjäroolit, joiden avulla voidaan helpottaa käyttäjien ja käyttäjäryhmien hallintaa.

Käyttäjien hallinnan automatisointi on tärkeää hajautetuissa verkoissa. Työsuhteet voivat olla lyhyitä tai projektikohtaisia, joten tarve pääsynhallinnalle on suuri. Käyttäjäoikeuksien elinkaaren hallinnalla voidaan välttää väärinkäytökset ja estää pääsy asiaankuulumattomilta tahoilta, kuten yrityksen entisiltä työntekijöiltä.

3. KERTAKIRJAUTUMINEN

Modernissa tietotekniikassa järjestelmät ovat hajautettuja useiden palveluntarjoajien ja yritysten verkkoihin, jolloin perinteistä yrityksen sisäisen verkon rajaa ei enää ole. Alansa standardiksi yleistyneiden pilvipalveluiden avulla voidaan rakentaa entistä moninaisempia kokonaisuuksia ja arkkitehtuureja. Tämän kaltaisessa toimintaympäristössä tavanomainen autentikointi voi osoittautua riittämättömäksi. Kertakirjautuminen tarjoaa ratkaisun ongelmaan keskittämällä tunnusten hallinnan ja autentikoinnin. Käyttäjä pääsee kirjautumaan kaikkiin kirjautumispalvelun alaisiin sovelluksiin yhdellä tunnistautumisella. Bertino et al. (2010, s.55) mukaan tämä ei tarkoita sitä, että käyttäjällä olisi vain yksi tunnus-salasana-pari, vaan useat kirjautumistiedot pikemminkin piilotetaan yksien kertakirjautumispalvelun tunnusten alle. Keskitetyllä autentikoinnilla ja tunnusten hallinnalla voidaan välttää useat tietoturvaongelmat kuten unohtuneet tai hävinneet salasanat, liian sallivat oikeudet ja puutteelliset salausalgoritmit. Tunnusten hallinnan automatisointi vähentää työkuormaa ja lisää palvelujen toimintavarmuutta. Lisäksi automatisoinnilla voidaan poistaa manuaalisen tunnusten hallinnan mukanaan tuomat inhimilliset virheet. (Joshi et al. 2018)

Kolmannessa luvussa käydään läpi kertakirjautumisen mahdollistavia protokollia ja tekniikoita, sekä erilaisia kertakirjautumispalveluja. Listaus ei ole kattava, vaan tarkoituksena on antaa yleiskuva kertakirjautumiseen liittyvistä tekniikoista.

3.1 Protokollat ja tekniikat

Tässä luvussa käydään läpi keskeisiä kertakirjautumisen mahdollistavia protokollia. Valinta protokollista tehtiin niiden oleellisuuden kannalta kertakirjautumista ajatellen. Tarkempaan tarkasteluun on valittu Secure Socket Layer (SSL) ja Open Authentication (OAuth).

OpenID on avoin standardi ja hajautettu autentikointiprotokolla. OpenID-identiteettipalveluntarjoaja takaa käyttäjille pääsyn sitä tukeviin palveluihin yksillä kirjautumistunnuksilla. Standardi määrää autentikointiprosessin kulun. OpenID kirjautumisen hyväksyviä tunnettuja palveluja ovat monien muiden lisäksi Amazon.com, WordPress ja Steam. Puhuttaessa OpenID:stä tarkoitetaan yleensä OpenID Connect:ia, joka on Oauth 2.0 -standardin päälle rakennettu autentikointikerros (Ubisecure 2019)(OpenID 2019).

Security Assertion Markup Language (SAML) on avoin XML-pohjainen kommunikaatiostandardi, joka mahdollistaa tietojen vaihtamisen palvelun- ja identiteetintarjoajan kesken. Standardi mahdollistaa viestinnän salauksen ja erilaiset käyttäjäroolit sekä takaa turvallisen käyttäjän autentikoinnin. Käyttäjän tehdessä pyynnön palvelulle palvelu tekee pyynnön identiteettipalvelulle, joka autentikoi käyttäjän. SAML:in avulla saavutetaan parempi yhteensopivuus eri järjestelmien välillä standardin sisältämien kertakirjautumisselainprofiilien ansiosta. (SAML 2005)

Shibboleth on avoimen lähdekoodin SAML:iin pohjautuva identiteettiratkaisu, jonka avulla eri organisaatiot voivat käyttää yhteistä identiteettitietoa tietoturvalliseen keskinäiseen kommunikaatioon. Shibboleth mahdollistaa identiteetin hallinnan yhdistetyissä järjestelmissä (federated networks). (Shibboleth 2019)

Kerberos on yleensä symmetriseen salaukseen perustuva todennusprotokolla. Asiakas tekee pyynnön autentikoimisserverille, jolta saa tiketin todisteeksi onnistuneesta autentikoinnista. Tätä tikettiä voidaan käyttää kirjautumiseen haluttuun palveluun. Protokollan käytöllä voidaan estää salakuuntelu ja toistohyökkäykset. (Microsoft 2009)

Seuraavaksi esitellään tekniikat **SSL** ja **OAuth**.

3.1.1 SSL

SSL on turvallisuusprotokolla, joka takaa turvallisen kommunikoinnin kahden koneen välillä. SSL-sertifikaatti on itsessään pienikokoinen tiedosto, jonka avulla autentikoidaan sivusto. Kun SSL on asennettu palvelimelle, palvelimen ja selaimen välille voidaan muodostaa HTTPS-protokollaa hyödyntävä yhteys, jossa tieto liikkuu salatussa muodossa. SSL:n kehittyneempi muoto on Transport Layer Securiy (TSL), josta usein kuitenkin käytetään SSL-nimikettä (Sectigo 2019).

SSL ja TSL ovat molemmat kryptograaffisia protokollia, joiden tarkoituksena on taata yhteyden luotettavuus. Julkiseen ja yksityiseen avaimeen perustuva autentikointiprosessi koostuu kuudesta askeleesta:

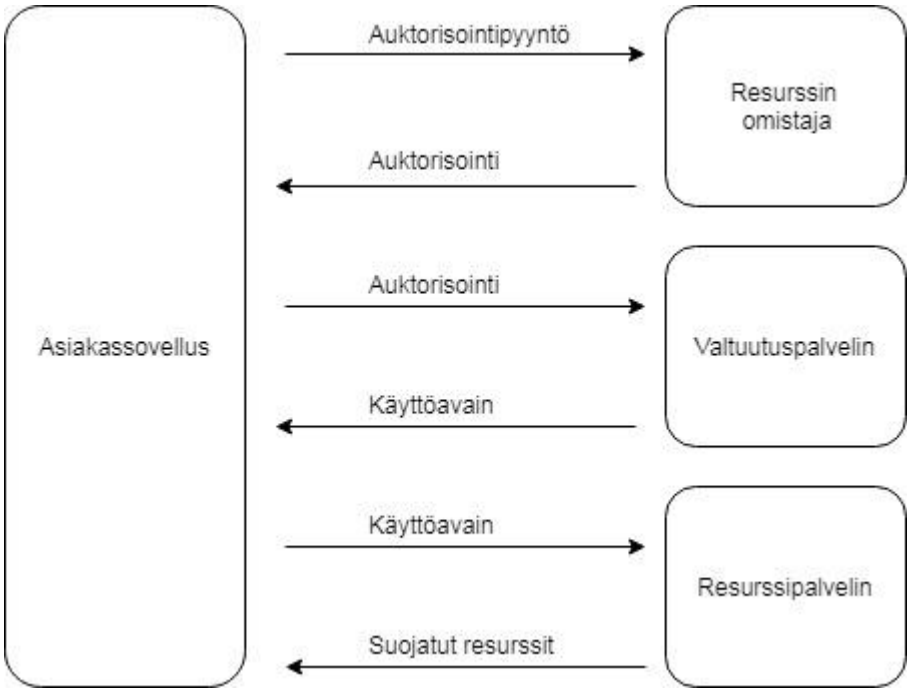
- Käyttäjä vierailee SSL-sertifikoidulla sivulla selaimellaan.
- Selain lähettää tunnistautumispyynnön palvelimelle.
- Palvelin vastaa pyyntöön lähettämällä kopion SSL-sertifikaatistaan.
- Selain tarkistaa saamansa SSL-sertifikaatin luotettavuuden ja lähettää hyväksynnän palvelimelle.

- Palvelin vastaa digitaalisesti allekirjoitetun hyväksynnän aloittaa SSL-salattu sessio.
- Selaimen ja palvelimen välinen viestintä on nyt salattu. (Sectigo 2019)

SSL-sertifikaatin tulee olla luotettavan tahon (Certficate Authority, CA) allekirjoittama. Näiden tahojen tulee noudattaa tarkkoja tietoturvamääräyksiä ja järjestää säännöllisiä auditointeja todentaakseen tietoturvansa ja autentikointiprosessinsa laatu. Salatun kommunikoinnin lisäksi SSL tarjoaa palvelulle luotettavuutta asiakkaan näkökulmasta, suojan kalasteluhyökkäyksiltä ja paremman hakukonesijoituksen verrattuna palveluihin ilman SSL-sertifikaattia. (Sectigo 2019)

3.1.2 OAuth

OAuth on standardiksi muodostunut tunnistusmekanismi. Se ei suoranaisesti ole protokolla, vaan pikemminkin kehys tai standardi tietojen turvalliselle vaihtamiselle kahden osapuolen kesken. Käyttäjä voi kirjautua verkkopalveluun paljastamatta tunnuksiaan kolmannen osapuolen välityksellä. Nykyään on laajemmin käytössä kehittyneempi versio OAuth 2.0, joka ei ole yhteensopiva vanhemman version kanssa. Tämä avoin protokolla tarjoaa turvallisen tunnistuksen verkko-, mobiili ja työpöytäsovelluksiin. OAuth 2.0 -standardia käyttävät muiden joukossa tekniikkajätit Amazon, Microsoft, Google, Twitter ja Facebook. (OAuth 2019)



Kuva 1. *OAuth 2.0 -protokollan auktorisointiprosessi (Anicas 2014).*

Kuva 1 antaa esimerkin OAuth-standardin käyttämisestä auktorisointiin. Toimijana kuvassa ovat asiakassovellus (client) ja resurssin omistaja (resource owner). Resurssin omistaja voi antaa muille tahoille oikeudet käyttää resurssia. Resurssin omistaja yrittää aluksi käyttää asiakassovellusta, joka ohjaa resurssien omistajan valtuutuspalvelimelle (authorization server). Valtuutuksen hyväksymisen jälkeen resurssin omistaja ohjataan takaisin asiakassovellukseen, joka saa valtuutuspalvelimelta valtuutuskoodin (authorization grant). Saatuaan valtuutuskoodin asiakassovellus todentaa itsensä valtuutuspalvelimella ja saa rajallisen ajan voimassa olevan käyttöavaimen (access token) ja uudistamisavaimen (refresh token). Saatuaan nämä asiakassovellus lähettää resurssipalvelimelle (resource server) pyynnön haluttuun resurssiin. Resurssipalvelin vastaa pyyntöön antamalla pääsyn haluttuun resurssiin. (Savolainen 2013)

3.2 Kertakirjautumispalvelut

Tässä luvussa käydään läpi kertakirjautumispalveluita. Kertakirjautumispalveluiden määrä on kasvanut räjähdysmäisesti eri toimijoiden toteuttaessa omia versioitaan palvelusta. Karkeasti palvelut voidaan jakaa kaupallisiin ja avoimen lähdekoodin palveluihin. Tunnetuimmasta päästä kaupallisia sovelluksia ovat Microsoftin Active Directory (AD) ja Facebookin luoma Facebook Connect. Avoimen lähdekoodin esimerkkinä voisi mainita Accounts-SSO, jonka Nokia kehitti matkapuhelimiaan varten, mutta joka myöhemmin on levinnyt laajempaan käyttöön.

3.2.1 AD

AD ei niinkään ole yksittäinen protokolla, vaan joukko erilaisia identiteettiin ja hakemistoihin liittyviä palveluja. Domain controller on palvelin, jolla ajetaan Active Directory Domain Service (AD DS) -palvelua. AD DS huolehtii järjestelmän käyttöoikeuksista, rooleista, autentikoinnista ja auktorisoinnista (Active Directory 2003).

Tyypillisesti AD DS käytetään kolmeen tarkoitukseen: sisäisen hakemiston, ulkoisen hakemiston tai sovellushakemiston autentikointiin ja auktorisointiin. Sisäinen hakemistopalvelu mahdollistaa organisaation sisäisen verkon hallinnan ja suojatun etäyhteyden (Virtual Private Network, VPN) verkon ulkopuolelta. Ulkoisten hakemistojen käyttötarkoitus on hallinnoida organisaation tarjoamien sovellusten ja palveluiden käyttöoikeuksia. Sovellushakemiston toimii sellaisen tiedon säilönä, mistä sovelluksen ulkopuoliset tahot eivät ole kiinnostuneet. Ratkaisulla pyritään vähentämään ylimääräistä verkkoliikennettä. (Active Directory 2003).

3.2.2 Facebook Connect

Facebook Connect on joukko ohjelmointirajapintoja (API), jotka mahdollistavat käyttäjän kirjautumisen kolmannen osapuolen sivustolle Facebook-tunnuksilla. Tällä voidaan myös välttää rekisteröitymisprosessi, mutta toisaalta käyttäjä antaa kirjautumissivustolle pääsyyn omiin Facebook-tietoihinsa, kuten Facebook-seinälleen, kaverilistaansa ja toimintoihinsa. Yleisimmillään Facebook Connect ilmenee palvelussa sisällön kommentointimahdollisuutena. (Facebook Connect 2019)

Facebook Connect tarjoaa autentikoinnin ja identiteetin varmentamisen lisäksi käyttäjälle samat yksityisyysasetukset kuin Facebook itsessään. Palvelun tarjoajalle käyttäjän kommentointi omalla varmistetulla identiteetillä on hyvä asia, sillä se vähentää asiattomien kommenttien määrää. (Facebook Connect 2019)

3.2.3 Google Sign-in

Google Sign-in tarjoaa käyttäjille tunnistautumisen kolmannen osapuolen palveluihin Google Account -tunnuksien avulla. Palvelu saa tietoonsa käyttäjän nimen, sähköpostiosoitteen ja profiilikuvan. Näiden tietojen avulla voidaan tarkastella, onko käyttäjällä jo olemassa oleva tili palveluun. Kolmannen osapuolen palvelu voi käyttää hyväkseen Googlen epäilyttävien tapahtumien havaitsemispalvelua. ()

Google Sign-in käyttää hyväkseen OAuth 2.0 -protokollaa autentikoinnissa ja auktorisoinnissa. Asiakassovellus pyytää Google Authorization Server:iltä tunnistetta (token) ja käyttää saamaansa tunnistetta kirjautuakseen haluttuun Google API:in. (Google Identity Platform)

4. KERTAKIRJAUTUMISEN TIETOTURVA

Tässä luvussa käsitellään kertakirjautumisen tietoturvaa. Kertakirjautuminen tarjoaa monia etuja yksityisen käyttäjän ja organisaatioiden kannalta ajateltuna. Muistettavien salasanojen määrä pienenee, jokaisen palvelun ei tarvitse implementoida omaa toteutustaan kirjautumisesta ja potentiaalisesti tietoturva paranee laadukkaiden autentikointisovellusten ansiosta. Käyttäjä voi samoilla tunnuksilla kirjautua useisiin eri palveluihin ja käyttäjien hallinta voidaan automatisoida keskitetyn käyttäjätietokantojen avulla. Mahdolliset inhimilliset riskitekijät voidaan minimoida käyttäjien hallinnan automatisoinnin avulla ja käyttäjien oikeudet voidaan rajata koskemaan vain haluttuja henkilöjä halutun aikavälin sisällä. Näistä monista saavutetuista eduista huolimatta kertakirjautumisessa piilevät omat riskinsä ja sen toteuttamisessa oikein voidaan kohdata haasteita. (Joshi et al. 2018)

Yksi yleinen kritiikin kohde on uhka siitä, että potentiaaliselle hyökkääjälle tarjotaan pääsy moniin sovelluksiin yhdellä tietomurrolla. Jos hyökkääjä pääsee murtautumaan kirjautumispalvelun tarjoajan järjestelmään, hän voi saada pääsyn useisiin kohteisiin yhdellä tietomurrolla. Toisaalta käyttäjän tunnusten tai kirjautumisen kaappaaminen voi taata hyökkääjälle useisiin eri kohteisiin. Tätä voitaisiin yksinkertaistetusti verrata tilanteeseen, jossa käyttäjällä on useisiin palveluihin sama salasana.

Toinen keskeinen riski on kirjautumispalvelun saatavuus. Luotettaessa kolmanteen osapuoleen autentikoinnissa ja auktorisoinnissa, muodostuu palvelun toimintavarmuus tärkeään asemaan. Pahimmassa tapauksessa tekninen ongelma palveluntarjoajan päässä voi lamauttaa koko organisaation toiminnan, kun työntekijät eivät pääse käyttämään palveluita kirjautumisen toimiessa ulkopuolisen todennuksen välityksellä.

EU:n tietosuoja-asetus General Data Protection Regulation (GDPR) (GDPR 2018) asettaa käyttäjien oikeuksille ja tietojen tallennukselle tiettyjä rajoituksia, jotka osaltaan vaikuttava myös tunnistuksessa kerättäviin ja tallennettaviin käyttäjätietoihin:

- Käyttäjältä tulee erikseen pyytää lupa tietojen käsittelyyn.
- Käyttäjällä on oikeus saada kopio hänestä kerätyistä tiedoista.
- Käyttäjällä on oikeus pyytää tuhota tai muuttaa tallennetut tiedot.
- Kerätyt tiedot tulee suojata.
- Kerättyjen tietojen eheys tulee varmistaa.

Kertakirjautumispalvelun tulee noudattaa näitä asetuksia toimiakseen lainvoimaisesti EU:n alueella. Myös EU:n ulkopuolisten organisaatioiden tulee noudattaa edellä mainittuja asetuksia, jos niiden käsittelemiin tietoihin sisältyy EU:n alueella vaikuttavien organisaatioiden tai yksilöiden tietoja. (Dayman 2018)

Huolimatta edellä mainituista kertakirjautumisen riskeistä ja rajoituksista voidaan kertakirjautumista pitää pääsääntöisesti oikein toteutettuna tietoturvaa edistävänä ratkaisuna. Palvelun tarjoajilla on verraten enemmän resursseja ja asiantuntemusta toteuttaa autentikointi luotettavasti ja tietoturvallisesti keskimääräiseen organisaatioon nähden.

4.1 Suunnitteluratkaisut tietoturvan uhkana

Miljoonat käyttäjät luottavat Facebook Connect-kirjautumiseen. Kirjautumisen käyttämä OAuth 2.0 - protokolla on todistettu turvalliseksi, mutta kirjautumista käyttävien sivustojen tietoturva ja kirjautumisen toteutus saattavat olla puutteellisia. Usein syynä ovat yksinkertaisuuden nimissä tehdyt suunnitteluratkaisut. (Sun et al. 2012)

Useat verkkopalvelut Sun et al. (2012) tekemässä tutkimuksessa eivät käyttäneet SSL-salausta, vaikka sitä vaadittaisiin kyselyiden (requests) ja vastausten (responses) allekirjoitukseen. Tämä puute voi johtaa vaikeasti tunnistettavaan hyökkäykseen, jossa käytetään kaapattuja kertakirjautumistunnuksia tai -sessioita. Ongelmaksi voi muodostua myös session tallennuksen implementointi, jos palvelu ei tarkista session vanhenemista.

4.2 Uloskirjautumisen haasteet

Usein puhutaan kertakirjautumisen yhteydessä sisäänkirjautumisesta, mutta uloskirjautuminen on jäänyt vähemmälle huomiolle. Perinteisessä verkkopalvelussa uloskirjautuminen on yksinkertaista, käyttäjän sessio lopetetaan ja käyttäjä on kirjautunut ulos järjestelmästä yhdellä painikkeella. Laajemmissa kertakirjautumista hyödyntävissä palveluissa asia ei kuitenkaan ole näin yksinkertainen. (Suoranta et al. 2013)

Identiteetintarjoaja tarjoaa mahdollisuuden uloskirjautumiseen, mutta ei määrittele kuinka palveluntarjoaja toteuttaa sen. Käyttäjän sessio voi jäädä auki joihinkin palveluihin, jolloin julkisessa tilassa sijaitsevan koneen seuraava käyttäjä voi päästä kirjautumaan palveluihin edellisen käyttäjän tiedoilla. Käyttäjän kannalta selkeintä olisi, että sessio lopetettaisiin ja uloskirjaus tapahtuisi kaikista palveluista yhdellä painalluksella, mutta tässä ratkaisussa kertakirjautumisesta saatava hyöty kumoutuu käyttäjän joutuessa kirjautumaan uudestaan jokaiseen haluamaansa palveluun. Käyttäjälle tulisikin tarjota mahdollisuus kirjautua ulos lokaalisti tai kokonaan ja uloskirjautuminen kertakirjautumisjärjestelmistä vaatisi standardointia. (Suoranta et al. 2013)

5. TUTKIMUKSEEN VALITUT PALVELUT

Tässä luvussa käsitellään tutkimukseen valitut palvelut. Tutkimuksen kohteiksi valikoitui WordPress ja sen lisäosa Google Apps Login. Valinnan kriteereinä olivat palveluiden tunnettavuus, tuttuus ja kyseisten palveluiden teknisen toteutuksen kiinnostavuus tutkimuskohteena. Googlen sähköpostiosoitteiden yleisyys edesauttoi tehdä valinta ottaa mielekkäältä vaikuttava tutkimuskohde tarkempaa tarkastelua varten. Oleellista tietoa kuitenkin on, että Google Apps Login ei tuo lisäarvoa yksinkertaisen palvelun kuten blogin yhteydessä käytettynä, vaan hyötyä saavutetaan käyttämällä sitä maksullisten lisäsisältöjen ja muiden kirjautumista edellyttävien ominaisuuksien kanssa.

5.1 WordPress

WordPress on ilmainen avoimeen lähdekoodiin perustuva sisällönhallintapalvelu, jonka avulla pystytään helposti luomaan ja hallitsemaan verkkosivustoja ja laajempiakin kokonaisuuksia. Käyttäjälle tarjotaan kehys (framework) sivujen hallinnointiin sekä maksuton hostaus- ja verkkotunnuspalvelu (domain service). Oman domainin käyttö on mahdollista, jolloin asetusten muokkaaminen onnistuu monipuolisesti. Pohjana WordPress-palvelussa toimii PHP- ja MySQL-ohjelmointikielet, mutta käyttäjä voi muokata kokonaisuutta vapaasti haluamillaan kielillä ja liitännäisillä.

Laajan suosion saavuttanut palvelu on toisaalta altis hyökkäyksille avoimen lähdekoodinsa ja tunnetun toteutustapansa ansiosta. Toinen mahdollinen uhka piilee haitallisissa liitännäisissä. WordPress-palveluun on julkaistu lukuisia tietoturvaoppaita ja hyökkäyksiltä suojaavia sovelluksia, joiden lisäksi palvelua päivitetään aktiivisesti tietoturva-aukkojen ilmetessä. Runsas määrä liitännäisiä voi tuoda mukanaan suorituskykyongelmat sovelluksen paisuessa (Härkönen 2017).

WordPress itsessään oikein käytettynä pystyy luomaan hyvän tietoturvan toteuttavia palveluita, jos vain sovelluskehittäjät ovat tietoisia potentiaalisista riskeistä. Kuten muidenkin verkkopalveluiden kanssa toimiessa, voidaan tietoturva nähdä useammasta palasesta koostuvana kokonaisuutena. Tärkeä lähtökohta on luotettavan palveluntarjoajan palvelin, jonka asetukset ja ohjelmat ovat oikein konfiguroituja. Tiedostojen oikeudet tulevat olla kunnossa, palomuurin sekä muun valvonnan asetukset tulevat olla kunnossa. Sovellustasolla tietoturva muodostuu kriittisesti valikoitujen liitännäisten ja teemojen käytöstä. Liitännäisten koodit tulee tarkastaa potentiaalisten haittaohjelmien varalta. Lisäksi

tulee pitää huolta ohjelmien ja liitännäisten säännöllisestä päivittämisestä. Varmuuskopiointi on hyvä tapa valmistautua hyökkäysten varalle. Käyttäjätason tietoturvalla tarkoitetaan sivuston ylläpitäjien ja sisällönpäivittäjien vastuuta tietoturvasta. Oikeudet tulevat olla käyttäjän tarpeiden mukaan rajattuja ja salasanojen suhteen tulee olla riittävän monimutkaisia. (Virenius 2014)

5.2 Google Apps Login

WordPress-palvelun, avoimeen lähdekoodiin perustuva, liitännäinen Google Apps Login mahdollistaa kertakirjautumisen Googlen sähköpostiosoitteen avulla WordPress-sivulle. Autentikoimisprotokollana käytetään OAuth2-protokollaa. Liitännäinen konfiguroidaan G Suite - tilin avulla sallimaan halutut verkko-osoitteet ja antamalla sille G Suite - sovelluksen turvakoodit. Liitännäisen Enterprise- ja Premium-versioissa on enemmän toimintoja ja ominaisuuksia, kuten automaattinen WordPress-tilin luominen kirjautumisen yhteydessä. Google Apps Login asettaa seuraat vaatimukset sivustolle:

- PHP 5.2.x tai uudempi versio JSON-lisäkkeellä
- WordPress 4.0 tai uudempi versio.

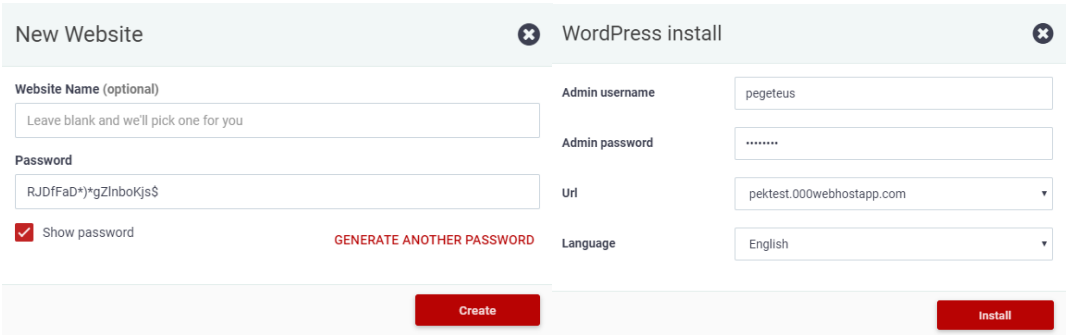
Näiden lisäksi vaaditaan Google-tili asennuksen suorittamiseksi. Liitännäistä päivitetään satunnaisesti, kirjoittamishetkellä uusin versio 3.2 on julkaistu 29.3.2019. (Google Apps Login 2019) Tutkimuksen alkuvaiheessa maaliskuun 2019 alussa viimeisimmästä päivityksestä oli kulunut kahdeksan kuukautta.

6. WORDPRESSIN ASENNUS JA ASETUSTEN KONFIGUROINTI

Tässä luvussa käydään läpi WordPress-sivun luominen ja Google Apps Login-liitännäisen asentaminen luodulle sivulle. Asennuksen suorittamiseen vaaditaan oma verkkotunnus, koska WordPress.com ei salli liitännäisten asennusta. Tutkimusta varten luotiin myös Googlen sähköpostiosoite.

6.1 WordPress-sivun luominen

WordPress-sivun luominen aloitettiin ilmaisen hostauspalvelun (hosting) etsinnällä. Prosessin helpottamiseksi palvelun tulisi oman domainin lisäksi sisältää automaattinen WordPress-sivun luonti. Palveluksi valikoitui Biz.nf-palvelu, jonka avulla sivusto saatiin luotua ja saavutettavaksi verkon välityksellä 15 minuutin työn tuloksena. Ongelmaksi muodostui kuitenkin SSL-tuen puuttuminen ilmaisversiosta. Salatun yhteyden puute johti siihen, ettei kirjautumislisäosa saanut yhteyttä Googlen palveluun.



Kuva 2. *Vasemmalla verkkosivun luonti ja oikealla WordPress:in asennus.*

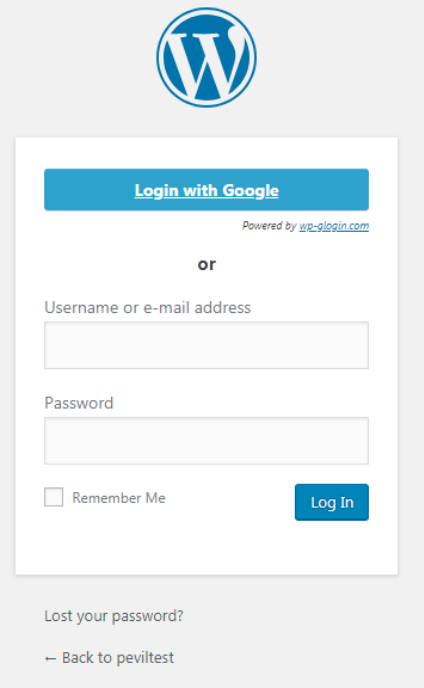
Seuraavana optiona käytettiin 000webhost-palvelua, joka tarjoaa ajantasaiset PHP 7.1 - ja WordPress 5.1.1. - versiot sovelluksista. Palvelun valttikortteina ovat maksuttomuus, nopea käyttöönotto ja selkeä käyttöliittymä. Palvelu tarjoaa automaattisesti SSL-tuen, joka mahdollistaa lisäosien asennuksen luodulle WordPress-sivulle. Asennuksessa luodaan uusi verkkosivu ja määritetään haluttu URL-osoite sekä salasanat sivulle (Kuva 2).

6.2 Google Apps Login – liitännäisen lisääminen WordPress-sivulle

Liitännäisen lisääminen tapahtuu WordPress-sivun hallintapaneelin avulla. Plugins-valikosta haetaan haluttu liitännäinen asennettavaksi. Asennuksessa ilmeni aluksi ongelmia

tiedostojensiirrossa, asennusohjelma ei saanut yhteyttä palvelimeen. Ongelmat ratkesivat valitsemalla 000webhost-palvelun hallintapaneelista asetuksista toiminto Repair my Website, joka on tarkoitettu korjaamaan tiedostojensiirron ongelmat. Toiminnon suorittamisen jälkeen liitännäisen asentui onnistuneesti. Asennuksen jälkeen liitännäinen konfiguroitiin liitännäisen antamien ohjeiden avulla seuravasti:

- Googlen ohjelmointirajapinnan (https://console.developers.google.com/) avulla luotiin uusi projekti.
- Credentials valikon kautta valittiin OAuth consent screen - välilehti ja syötettiin sähköpostiosoite ja haluttu sovellusnimi.
- Luotiin uusi OAuth Client ID - objekti tyyppinään Web-sovellus.
- Client ID - objektiin asetuksiin määrättiin auktoroiduiksi osoitteiksi Javascript-osoitteeksi WordPress-sivun osoite https://peviltest.000webhostapp.com ja uudelleenohjaus URI:ksi WordPress-sivun sisäänkirjausosoite https://peviltest.000webhostapp.com/wp-login.php.
- Saadut Client ID ja Client Secret - arvot syötettiin liitännäisen asetuksiin.



Kuva 3. *Kirjautumisvalikko.*

Lopputuloksena WordPress-sivun sisäänkirjautumissivulle saatiin optio kirjautumiseen Gmail-sähköpostiosoitteella (Kuva 3). Vaihtoehtona näkymässä on kirjautua WordPress-tunnuksella.

6.3 Asetusten konfigurointi

WordPress-palvelun tietoturvaa voidaan parantaa liitännäisillä ja asetuksilla. Tässä luvussa esitellään palvelun tietoturvaa parantavia toimenpiteitä. Lähteenä toimenpiteiden etsimiseen käytettiin wpbeginner.com-sivuston listausta (WPBeginner 2019) tietoturvauhista ja haavoittuvuusskannereiden tuloksia. Konfigurointi aloitettiin vaihtamalla ylläpitokäyttäjänimi pois oletusarvosta, toimenpiteellä oletusarvoa käyttävät hyökkäykset saadaan torjuttua. Seuraavaksi tiedostoon /public_html/.htaccess tehtiin taulukon 1 mukaiset muokkaukset.

Taulukko1. Tiedostoon */public_html/.htaccess* tehdyt muutokset.

Vaikutus	Lisätyt rivit
Uudelleenohjaus HTTP-protokollasta HTTPS-protokollaan	*RewriteEngine On* *RewriteCond %{HTTPS} off* *RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]*
HSTS-header kertoo selaimelle, että sivustolle tulisi päästä vain HTTPS-protokollaa käyttäen	*# Use HTTP Strict Transport Security to force client to use secure connections only Header always set Strict-Transport-Security "max-age=300; includeSubDomains; preload"*
Tiedostolistauksen esto, potentiaaliset hyökkääjät eivät näe hakemistojen sisältöä	*Options –Indexes*
Estää XML-RPC, joka mahdollistaa brute force - hyökkäykset	# Block WordPress xmlrpc.php requests <Files xmlrpc.php> order deny,allow deny from all allow from 123.123.123.123 </Files>

Tämän jälkeen poistettiin oikeus muokata sivuston koodia suoraan admin-alueen käyttöliittymästä lisäämällä rivi wp-config.php-tiedostoon:

- define('DISALLOW_FILE_EDIT', true);

Toimenpiteellä estetään ylläpitoalueelle murtautuneen käyttäjän haitallinen toiminta.

6.4 Tietoturvaliitännäiset

WordPress-palveluun on tehty lukuisia tietoturvaa parantavia liitännäisiä. Tutkimuksen puitteissa ei kuitenkaan ollut mahdollisuutta tutustua niihin syvemmin. Liitännäisiä käyttäessä on hyvä muistaa niiden päivityksen tarpeellisuus. Päivittämättömät liitännäiset tarjoavat potentiaalisesti hyökkääjälle reitin sovellukseen. Taulukko 2 esittelee neljä tietoturvaliitännäistä ja niiden käyttötarkoitukset.

Taulukko 2. Tietoturvaliitännäisiä WordPress:in ja niiden käyttötarkoituksia.

Liitännäinen	Käyttötarkoitus
Inactive Logout	Käyttäjän automaattinen uloskirjaus määrätyn ajan puitteissa
VaultPress	Palvelun varmuuskopiointi
Sucuri	Palomuuri ja tietoturva yleisemmin, monet tutkimuksessa esitetyistä muutoksista voidaan automaattisesti tehdä Sucurilla
WP Security Questions	Turvakysymyksen lisääminen sisäänkirjautumiseen

Liitännäisten asennus on tehty WordPressiin vaivattomaksi. Asennus tapahtuu WordPressin oman hallintapaneelin avulla, jonka kautta liitännäiset voidaan myös päivittää. Hallintapaneeli ilmoittaa myös päivittämistä vaativista sovelluksista.

7. TULOKSET

WordPress-sivun luominen ja hostauspalvelu löydettiin vaivattomasti. Erilaisten maksuttomien hostauspalveluiden kirjo on laaja, mikä mahdollisti tarkoitukseen sopivan palvelun valikoinnin tarvittavien ominaisuuksien perusteella. Palveluna 000webhost tarjoaa sujuvan käyttöliittymän ja riittävästi konfiguraatiomahdollisuuksia, toisin kuin Bix.nf-palvelu, jonka ominaisuudet eivät vastanneet tämän tutkimuksen tarpeita. SSL-tuki parantaa tietoturvaa ja on oleellinen osa nykyaikaista verkkopalvelua. Tässä luvussa käydään läpi tutkimuksen tulokset.

Kertakirjautumisen lisääminen palveluun Google Apps Login - lisäkkeen avulla mahdollistaa kirjautumisen ilman WordPress-tunnuksia. Kirjautuminen toimi nopeasti ja teki WordPress-palvelun käyttökokemuksesta sujuvamman vähentämällä tarvetta erilliselle tunnukselle. Lisäkkeen asentaminen aiheutti odotettua enemmän vaikeuksia. Vaikeudet saattoivat johtua päivittämättömästä liitännäisversiosta, joka ei ollut yhteensopiva uusimman WordPress-version kanssa. Toinen ongelmakohta saattoi piillä 000webhost-palvelun tarjoamassa WordPress-asennuksessa, jonka FPS-tuki ei toiminut sellaisenaan, vaan vaati 000webhost-palvelun tarjoaman korjausoperaation suorittamisen.

Yksinkertaiseen blogisivustoon kertakirjautumisen lisääminen ei tuo juurikaan lisäarvoa, mutta maksullisten kirjautumista vaativien sisältöjen yhteydessä sen implementointi palveluun on tarkoituksen mukaista. Käyttäjät arvostavat sujuvaa käyttökokemusta ja kirjautumistunnusten sekä salasanojen määrä kuormittaa nykyisellään käyttäjiä kohtuuttomasti. Tarjoamalla kirjautuminen jo olemassa olevilla tunnuksilla saavutetaan laajempi käyttäjäryhmä palvelulle. Aktiivinen Google-tili löytyy 1500 miljoonalta käyttäjältä (Gmail Statics 2018), joten sen käyttämistä autentikointiin ja auktorisointiin voidaan pitää optimaalisena valintana.

8. YHTEENVETO

Kertakirjautuminen on nykyajan verkkosovelluksien kannalta tärkeä tekniikka, johon törmäämiseltä ei voi välttyä verkossa liikkuessa. Kertakirjautuminen helpottaa verkkopalvelujen rakentamista vähentämällä palvelun toteuttamiseen vaadittavaa työmäärää. Autentikointi ja auktorisointi voidaan ulkoistaa kolmannelle osapuolelle, eikä sovelluksen toteuttajien tarvitse tehdä omaa versiota sisäänkirjautumisesta. Tällä voidaan myös parantaa tietoturvaa, sillä kirjautumisiin erikoistuneet tahot pystyvät toteuttamaan autentikoinnin ja auktorisoinnin laadukkaasti ja tietoturvallisesti. Kertakirjautumisen haittapuolina voidaan pitää luottaminen ulkopuoliseen tahoon, kirjautumispalvelun vakaus ja palvelun kiinnostavuus hyökkäyksen kohteena. Standardoinnin puute vaivaa kertakirjautumisen toteutuksia ja voi aiheuttaa ikäviä yllätyksiä verkkosovellusten käyttäjille ja kehittäjille.

Tutkimuksen kohteena ollut WordPress tarjoaa helpon tavan luoda verkkopalveluja ja hallita niiden sisältöä. Suosiota saavuttanut palvelu mahdollistaa palvelujen luomisen ilman koodaamistaitoja. Tutkimuksen tuloksena todettiin, että tunnettu toteutustapa ja standardoidut tiedostorakenteet voivat kuitenkin tarjota hyökkääjälle otollisen alustan. WordPress-palvelun liitännäiset voivat tarjota suojaa hyökkäyksiä vastaan, kuten myös oikein suoritettu asetusten konfigurointi. Liitännäisiä käyttäessä tulee kuitenkin olla kriittinen ja muistaa ajantasaiset päivitykset. Tutkimuksen tulosten perusteella voidaan parantaa WordPress-sivun tietoturvaa suorittamalla esitetyt konfiguraatiot.

Tulevaisuudessa verkkopalveluiden luominen tulee mitä todennäköisimmin helpottumaan entisestään. Tämä voi olla riski, jos palveluiden tietoturvaan ei kiinnitetä riittävää huomiota. Käyttäjät ovat tottuneet sujuvaan käyttökokemukseen, jota kertakirjautuminen voi edesauttaa. Helppokäyttöisyyttä tavoitellessa saatetaan valitettavasti tehdä kompromisseja tietoturvan suhteen. Oikeanlaisilla standardoiduilla ratkaisuilla ja paremmalla suunnittelulla voidaan saavuttaa sekä parempi käytettävyys, että parempi tietoturva.

LÄHTEET

Active Directory. (2003). Active Directory on a Windows Server 2003 Network, Active directory collection. Microsoft. Saatavissa (viitattu 5.4.2019): https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780036(v=ws.10)#w2k3tr_ad_over_qbjd

Anicas, M. (2014). An Introduction to OAuth 2, DigitalOcean. Saatavissa (viitattu 21.5.2019): https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2

Autentikointi. (2015). Autentikointi, TIE-23500 Web-ohjelmointi, Tampereen yliopisto. Saatavissa (viitattu 16.4.2019): http://www.cs.tut.fi/~seitti/2015/kalvot/auth/all.html

Bertino, E., Takahashi, K. (2010). Indentity Management: Concepts, Technologies, and Systems, Artech House, s. 197.

Dayman, D. (2018). GDPR impact for non-EU companies, blogikirjoitus. Saatavissa (viitattu 9.4.2019): https://blog.returnpath.com/gdpr-impact-for-non-eu-companies/

Facebook Connect. (2019). Facebook Connect, Definition, Technopedia. Saatavissa (viitattu 24.4.2019): https://www.techopedia.com/definition/4827/facebook-connect

GDPR. (2018). General Data Protection Regulation. Saatavissa (viitattu 18.4.2019): https://gdpr-info.eu/

Gmail Statics. (2018). Gmail: active users worldwide 2012-2018, The Statistic Portal, Statista. Saatavissa (viitattu 25.4.2019): https://www.statista.com/statistics/432390/active-gmail-users/

Google Account Help. (2019). Use your Google Account to sign in to other sites or apps. Saatavissa (viitattu 29.6.2019): https://support.google.com/accounts/answer/112802?hl=en&ref_topic=7188760

Google Apps Login 2019. (2019). Google Apps Login, description. Saatavissa (viitattu 18.4.2019): https://wordpress.org/plugins/google-apps-login/#description

Google Identity Platform. (2019). Using OAuth 2.0 to Access Google APIs. Saatavissa (viitattu 29.6.2019): https://developers.google.com/identity/protocols/OAuth2

Härkönen, J. 2017. (2019). WordPressin soveltuvuus sivujen luontiin, opinnäytetyö, Lahden Ammattikorkeakoulu. Saatavissa (viitattu 12.5.2019): http://urn.fi/URN:NBN:fi:amk-2017060913124

Joshi, U., Cha, S., Sardari, S. E. (2018). Towards Adoption of Authentication and Authorization in Identity Management and Single Sign On. Advances in Science, Technology and Engineering Systems Journal, 2018, Vuosikerta / Sarjan

osa 3, Numero 5. Saatavissa (viitattu 17.3.2019): https://www.astesj.com/publications/ASTESJ_030556.pdf

Jäppinen, P. (2007). Tietoturvan Perusteet Autentikointi, Digitaalimaailman Keinot. Saatavissa (viitattu 16.4.2019): https://docplayer.fi/17848089-010627000-tietoturvan-perusteet-autentikointi.html

Lintusalo, S. (2018). Käyttäjähallintaominaisuuden implementointi WordPress-sivustolle. Ammattikorkeakoulututkinnon opinnäytetyö. Hämeenlinna: Hämeen ammattikorkeakoulu. Saatavissa (viitattu 17.3.2019): http://urn.fi/URN:NBN:fi:amk-2018090314816

Ma, X. (2015). Managing Identities in Cloud Computing Environments, 2015 2nd International Conference on Information Science and Control Engineering, Shanghai, s.290–292. Saatavissa (viitattu 17.3.2019): https://ieeexplore-ieee-org.libproxy.tut.fi/document/7120611/

Microsoft. (2009). What Is Kerberos Authentication, Comparison of Windows Server 2003 Editions: General, Microsoft Docs. Saatavilla (viitattu 18.4.2019): https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780469(v=ws.10)

OAuth 2.0. (2019). Oauth. Saatavissa (viitattu 24.4.2019): https://oauth.net/2/

OpenID Connect. (2019). OpenID Connect FAQ and Q&As, OpenID. Saatavissa (viitattu 18.4.2019): https://openid.net/connect/faq/

SAML. (2005). Security Assertion Markup Language (SAML) v2.0, OASIS Standards. Saatavissa (Viitattu 24.4.2019): https://www.oasis-open.org/standards#samlv2.0

Savolainen, L. (2013). OAuth 2.0-valtuutusprotokolla, Seminaariraportti, Tietojenkäsittelytieteen laitos, Helsingin Yliopisto. Saavissa (viitattu 16.5.2019): https://docplayer.fi/7318290-Oauth-2-0-valtuutusprotokolla.html

Sectigo. (2019). About TLS/SSL Certificate. Saatavissa (viitattu 16.4.2019): https://www.instantssl.com/about-tls-ssl-certificates

Sermersheim, J. (2006). Lightweight Directory Access Protocol (LDAP): The Protocol. Novell, Inc. Saatavissa (viitattu 4.4.2019): https://tools.ietf.org/rfc/rfc4511.txt

Shibboleth. (2019). What’s Shibboleth?, Shibboleth. Saatavissa (viitattu 18.4.2019): https://www.shibboleth.net/index/

Sun, S.-T., Beznosov, K. (2019). The Devil is in the (Implementation) Details: An Empirical Analysis of OAuth SSO Systems, Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, Canada. Saatavissa (viitattu 24.4.2019): https://dl-acm-org.libproxy.tuni.fi/citation.cfm?id=2382238

Suoranta, S., Tontti, A., Ruuskanen, J., Aura, T. (2013). Logout in Single Sign-on Systems. In: Fischer-Hübner S., de Leeuw E., Mitchell C. (eds) Policies and Research in Identity Management. IDMAN 2013. IFIP Advances in Information

and Communication Technology, vol 396. Springer, Berlin, Heidelberg. Saatavissa (viitattu 25.4.2019): https://link.springer.com/content/pdf/10.1007/978-3-642-37282-7_14.pdf

Tolvanen, P. (2011). Käsitteet ojennukseen: Active Directory (AD), LDAP, SSO ja identiteetinhallinta. Intranet-ostajan opas. Saatavissa (viitattu 4.4.2019): https://intranet-ostajanopas.fi/2011/04/29/kasitteet-ojennukseen-active-directory-ad-ldap-sso-ja-identiteetinhallinta/

Trunde, H., Weippl, E. (2015). WordPress security: an analysis based on publicly available exploits. In Proceedings of the 17th International Conference on Information Integration and Web-based Applications & Services (iiWAS '15). ACM, New York, NY, USA, , Article 81 , 7 pages. Saatavissa (viitattu 25.4.2019): http://dx.doi.org.libproxy.tuni.fi/10.1145/2837185.2837195,

Ubisecure. (2019). SAML vs OAuth 2.0 vs OpenID Connect, Ubisecure. Saatavissa (viitattu 18.4.2019): https://www.ubisecure.com/about/resources/saml-oauth-openid-connect/

Virenius, M. (2014). Vieraskynä: Katsaus WordPress-sivustojen tietoturvaan, Vierityspalkki.fi. Saatavissa (viitattu 21.5.2019): https://vierityspalkki.fi/2014/08/18/vieraskyna-katsaus-wordpress-sivustojen-tietoturvaan/

WPBeginner. (2019). The Ultimate WordPress Security Guide – Step by Step (2019), Beginner’s guide for WordPress, WPBeginner. Saatavissa (viitattu 25.4.2019): https://www.wpbeginner.com/wordpress-security/