jamk

Kyberturvallisten sähköpostipalveluiden laboratorioympäristö

Tero Lång

Opinnäytetyö, AMK
Marraskuu 2022
Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Lång Tero

Kyberturvallisten sähköpostipalveluiden laboratorioympäristö

Jyväskylä: Jyväskylän ammattikorkeakoulu. Marraskuu 2022, 36 Sivua

Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Sähköposti on vanha ja paljon käytetty kommunikaatiojärjestelmä. Ajan kanssa sähköpostin tieturvallisuudessa on löytynyt aukkoja, jotka juontuvat jo yli 50 vuoden takaa. Sähköpostin turvallisuutta on pyritty parantamaan useilla muutoksilla vuosien varrella, mutta vielä tänä päivänäkään, sähköpostien lähettäjän autenttisuutta ei tarkisteta tai varmenneta ilman siihen tarkoitettujen todennuslisäosien asentamista ja konfigurointia.

Opinnäytetyön tarkoituksena oli kehittää Jyväskylän ammattikorkeakoululle, Virtual Learning Environment -laboratorioympäristöön nykyaikainen sähköpostijärjestelmä, käyttäen jo olemassa olevia sovelluksia, joissa oli mahdollista hyödyntää yleisimpiä sähköpostin lähettäjän todentamiseen tarkoitettuja tekniikoita. Järjestelmää oli tarkoitus hyödyntää opetuskäytössä, erillisten laboratorioharjoitteiden osana.

Opinnäytetyö oli palvelun, tuotteen tai produktion kehittämiseen keskittyvä. Opinnäyteyön ympäristön toteutuksessa käytettiin Postfix-sovellusta, sähköpostien välittämiseen sähköpostipalvelimien välillä, Dovecot-sovellusta sähköpostien paikalliseen välittämiseen sähköpostilaatikoihin ja sähköpostitilien hallintaan. Sähköpostien pääkäyttäjäsovelluksena käytettiin Roundcube-ohjelmaa, joka mahdollisti sähköpostien käyttäjäkohtaisen hallinnan.

Opinnäytetyön ympäristön koventamisessa käytettiin Sender Policy Frameworkia, DomainKeys Identified Mail ja Domain-based Message Authentication lisäosia, joilla voidaan todentaa sähköpostin lähettäjän identiteetti.

Työn tavoitteena on selventää mitä sähköpostin turvallisuus on ja perehdyttää lukijaa kyseisten metodien käyttöönotossa ja niiden toiminnan todentamisessa.

Avainsanat (asiasanat)

Sähköposti, Tietoturva, Viestintä, Palvelun kehittäminen

Muut tiedot (salassa pidettävät liitteet)

-

jamk

Description

Lång Tero

Laboratory environment for cybersecure e-mail services

Jyväskylä: JAMK University of Applied Sciences, November 2022, 36 Pages

Degree Programme in Information and Communication Technology. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

E-mail is an older but still very much the most used communication method. As e-mail got older and gained more and more usage, the security flaws, that can be traced back to e-mails first versions, which are over 50 years old, have started to became more known. There has been attempts in making email more secure way to communicate, but even nowadays the authenticity of the sender is not checked without the use of external programs.

The objective of the thesis was to develop a modern email-system that utilizes already existing software which in turn use the most common of sender authentication methods. The end use for this system was to be used in teaching as part of separate laboratory exercises.

The research method used on the thesis was developing of a service, product, or production. The end product utilises Postfix-software as mail transfer agent, to transfer e-mails between e-mail servers. It utilises Dovecot as local delivery agent and as e-mail address manager. Dovecot handles e-mails in local environment, and delivers them from the MTA to users e-mail folder. For end-users there was Roundcube-webmail which made it possible to read, write and manage e-mails.

For hardening of the e-mail environment, the thesis utilises Sender Policy Framework, DomainKeys Identified Mail and Domain-based Message Authentication add-ons, which can be used to verify the identity of the e-mail sender.

The goal of the thesis was to clear up, what is e-mail security and to orient the Reader in the use and deployment of those methods.

Keywords/tags (subjects)

email, data security, communication

Miscellaneous (Confidential information)

-

Sisältö

Kuviot

1 Johdanto

Sähköposti on läsnä monien elämässä päivittäin, niin työn kuin vapaa-ajankin merkeissä. Melkein puolet maailman väestöstä lähettää sähköposteja päivittäin. Keskiarvollisesti vuonna 2021 lähetettiin päivässä 319.6 miljardia sähköpostiviestiä (Number of sent and received e-mails per day worldwide from 2017 to 2025.) Sähköposti on useille tärkein kommunikaatioväline, toisille pakollinen riesa. Etenkin edellisvuosina sähköpostin haavoittuvuuksia ollaan käytetty suurenevissa määrin hyödyksi, erilaisten haittaviestien ja roskapostin lähettämiseksi.

Isona ongelmana sähköpostin kanssa on se, ettei sähköpostiin itseensä kuulu melkein mitään turvallisuustarkastuksia, vaan kaikki nykyaikaiset turvausmekanismit täytyy erikseen asentaa ja ottaa käyttöön. Turvaamatonta sähköpostipalvelinta on todella yksinkertaista käyttää väärissä tarkoituksissa, sillä kuka vain voi lähettää sen nimissä sähköposteja, esiintyen sähköpostin oikeana käyttäjänä. Tästä syystä tarve opetukseen sähköpostipalveluiden turvaamisesta on noussut.

Tässä opinnäytetyössä tehtävänä oli pystyttää IT-instituutin Virtual Learning Environment- ympäristöön todellisuutta mallintava sähköposti-infrastruktuuri, joka käyttää nykyaikaisia laajennuksia, SPF:ia, DKIM:ia ja DMARC:ia, sähköpostiliikenteen koventamiseksi.

2 Teoriapohjaa

Sähköposti on kommunikointiteknologia, jolla viestejä välitetään verkkojen ylitse. Sähköposti viittaa sekä viestien lähetysjärjestelmään, että yksittäisiin viesteihin. Sähköposti on ollut nykyisen tyylisessä mallissa olemassa jo vuodesta 1971 lähtien, kun Ray Tomlinson kehitti sen internetin edeltäjään, Arpanettiin. Ensimmäinen kerran sähköpostille ehdotettiin standardia vuonna 1973. Ensimmäisen kerran sähköposti standardisoitiin Arpanetissä vuonna 1977. Nykyaikana sähköposti on yksi yleisimmin käytetyistä digitaalisista viestinnänmuodoista. (Gibbs Samuel 2016).

2.1 VLE

Virtual Learning Environment, eli VLE, on Jyväskylän ammattikorkeakoulun sisäisen opetusverkon, LabraNetin osa, jota käytetään niin ammattikorkeakoulun, kuin ylemmänkin ammattikorkeakoulun tutkinto-ohjelmissa (Virtual Learning Environment.)

“VLE mahdollistaa opiskelijoille kurssikohtaiset laboratorio- ja harjoitusympäristöt eri aihepiirien opiskeluun.” (Virtual Learning Environment)

VLE mahdollistaa raskaidenkin kurssiympäristöjen hyödyntämisen, riippumatta opiskelijan tietokoneen tehoista, ajasta tai paikasta. Näin ollen poistaen myös kurssiympäristöjen asentamisessa mahdollisesti ilmenevät muuttujat kurssitoteutuksesta (Virtual Learning Environment.)

VLE on toteutettu Jyväskylän ammattikorkeakoulun omana pilvipalveluna ja se ajetaan täysin JAMK:in tiloissa omilla palvelimillaan. Ympäristöön yhdistämiseksi täytyy opiskelijan ottaa VPN-yhteys LabraNet:iin ja kuulua vähintään yhdelle kurssille, jolla VLE:tä hyödynnetään (Virtual Learning Environment.)

2.2 Simple mail transfer protocol

Simple mail transfer protocol, lyhennettynä SMTP on sähköpostin välittämiseen käytettävä TCP protokolla. SMTP käyttää porttia 25 jossa kulkevat viestit eivät ole salattuja, vaan viestit lähetetään paljaana tekstinä, HTML muotoisena, tai molempia yhteisesti käyttäen. SMTP:n tarkoitus on kuljettaa sähköposteja efektiivisesti ja luotettavasti verkon ylitse. (Klensin 2008)

SMTP standardi on ensimmäiseksi määritelty dokumentissa RFC 821, vuonna 1982, ja on vuosien kuluessa saanut useita päivityksiä. Nykyinen standardin versio on määritelty vuonna 2008, dokumentissa RFC5321. (Klensin 2008).

SMTP on tekstipohjainen, yhteyssuuntautunut protokolla, jossa käyttäjä kommunikoi palvelimen kanssa käyttäen yksinkertaisia komentosarjoja TCP kanavan ylitse. Eri komentoja ovat: “HELO”, “MAIL FROM:”, “RCPT TO:” ja “DATA” (Klensin 2008).

HELO komennolla identifioidaan lähettävä taho, useimmiten SMTP serveri. Mikäli palvelinta ei ole suojattu, tähän voi laittaa mitä tahansa, eikä palvelin tarkista sitä (Klensin 2008).

Alla on esimerkkikomennot, joilla sähköpostiviestin voisi lähettää suojaamattomasta SMTP palvelimesta käyttäen telnet yhteyttä.

HELO lokero.vle.fi

MAIL FROM: lähettäjä@lokero.vle.fi

RCPT TO: vastaanottaja@osoite.esimerkki

DATA

Hei maailma!

.

MAIL FROM: kertoo keneltä sähköposti on tullut ja samalla osoittaa mihin sähköpostiosoitteeseen vastaukset tulisi ohjata (Klensin 2008).

RCPT TO: Kertoo kenelle viesti halutaan lähettää, tämän komennon voi toistaa useita kertoja, jolloin sähköposti lähetetään kaikille vastaanottajille kerralla (Klensin 2008).

DATA osioon kirjoitetaan itse viesti, mukaan lukien sähköpostin aihe. Datan loppu osoitetaan yksittäisellä, omalla rivillään olevalla pisteellä "." (Klensin 2008).

Sähköpostiin perustuvat kyberhyökkäykset ovat niin yleisiä, että SMTP:n käyttämä portti 25, on kyberturvallisuuskeskuksen suosituksesta suurimmalta osin estetty Suomessa. Portti 25 on auki vain teleyritysten, eli yritysten, jotka tarjoavat verkko- tai viestintäpalvelua ennalta rajaamattomalle käyttäjäpiirille, lähtevien sähköpostien SMTP palvelimille (Tiettyihin tietoliikenneportteihin suuntautuvan liikenteen tietoturvaperusteinen suodattaminen teleyritysten verkoissa 2020.)

"Lain määritelmän mukaan teleyrityksellä tarkoitetaan sitä, joka tarjoaa verkkopalvelua tai viestintäpalvelua ennalta rajaamattomalle käyttäjäpiirille eli harjoittaa yleistä teletoimintaa." (Mikä on teletoimintaa? 2021.)

2.3 Postfix

Postfix on hyvin suosittu avoimen lähdekoodin sähköpostin välityssovellus, eli MTA. Postfix vastaa sähköpostin välittämisestä vastaanottajan sähköpostipalvelimelle internetin ylitse. (The Postfix Home Page)

Postfix vastaa noin 32.5% kaikesta julkisesta sähköpostiliikenteestä. Toinen hyvin suosittu välitys-sovellus on Exim internet mailer, joka vastaa noin 60.9% kaikesta julkisesta sähköpostiliikenteestä. Näiden lisäksi on vielä monia vähemmän suosittuja välityssovelluksia, kuten Sendmail, noin 3.51% ja MailEnable, noin 1.91% ja useita muita, joiden prosenttiosuus on alle yhden. (Mail (MX) Server Survey 2022)

Ensimmäinen versio Postfixistä julkaistiin joulukuussa vuonna 1998 (Markoff 1998).

Postfix toimii useimmilla UNIX-pohjaisilla käyttöjärjestelmillä, kuten linux ja MacOS X. (Postfix feature overview)

2.4 Dovecot

Dovecot on avoimen lähdekoodin sähköpostin jakeluagentti, joka hoitaa sähköpostien jakamisen sähköpostilaatikoihin paikallisessa verkossa. Ja mahdollistaa sähköpostien hakemisen käyttäen IMAP ja POP3 protokollia (Dovecot manual.)

Ensimmäinen versio Dovecotista julkaistiin heinäkuussa 2002. Dovecot keskittyy turvallisuuteen, keveyteen, nopeuteen ja käytön helppouteen ja se toimii yleisimmillä Linux ja UNIX pohjaisilla käyttöjärjestelmillä (Dovecot manual.)

2.5 Roundcube

Roundcube on avoimen lähdekoodin selainpohjainen verkkosähköpostiohjelmisto, jossa on sovellustyylinen käyttöliittymä ja kaikki normaalit sähköpostisovelluksen ominaisuudet, kuten osoitekirja, erilliset kansiot saapuville, lähteville, luonnoksille ja roskaposteille. (About the Roundcube webmail project)

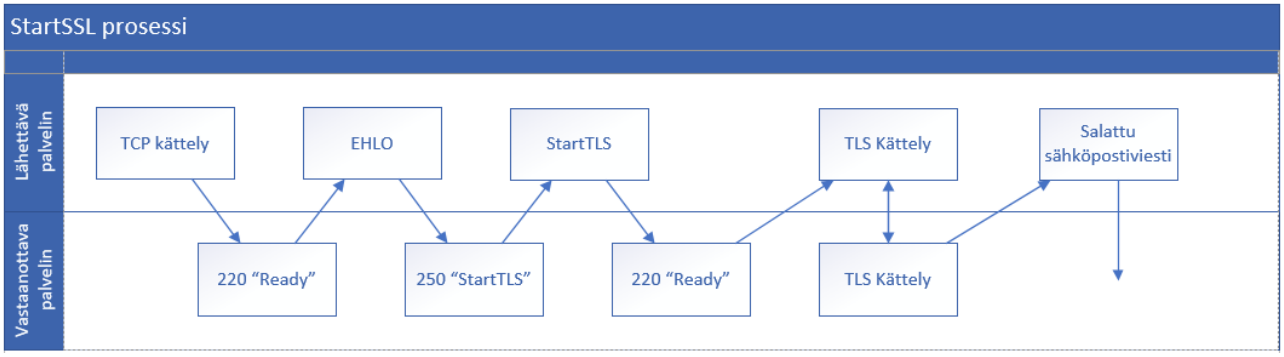
Roundcube on helposti asennettavissa yleisimpien verkkopalvelimien, kuten Apache ja Nginx, päälle. Ohjelmiston käyttöliittymä ja ominaisuudet ovat helposti muokattavissa tavoitteisiin sopivaksi. (About the Roundcube webmail project)

2.6 Sähköpostin turvaaminen

2.6.1 SMTPS & StartTLS

Normaali simple mail transfer protokolla ei käytä salausta, jolloin data jää haavoittuvaiseksi esimerkiksi väliintulo tai salakuuntelu hyökkäyksille. SMTPS, eli Simple Mail Transfer Protocol Secure, lisää salauksen sähköpostien kuljetukseen palvelimien välillä, lisätäkseen näin turvallisuutta. SMTPS on käyttänyt ennen portteja 465 ja 587, joista nykysin suositellaan, ettei porttia 465 tulisi enää käyttää lainkaan, vaan TLS suojattu sähköpostin välitys tulisi suorittaa käyttäen porttia 587 (SMTPS: Securing SMTP and the Differences Between SSL, TLS, and the Ports They Use 2022.)

StartTLS lisää TLS salauksen SMTP ja IMAP liikenteeseen, näin lisäten sähköpostin turvallisuutta, kun sitä ei enää siirretä puhtaana tekstinä palvelimien välillä. Vaikka StartTLS olisi konfiguroituna, alkaa sähköpostipalvelimien välinen yhteys silti aina ilman salausta, mutta kuten kuviosta 1 nähdään, StartTLS kysely lähetetään heti lähettävän palvelimen “EHLO” viestin jälkeen. Mikäli StartTLS on toiminnassa, salaus tulee toimintaan ennen sähköpostin lähetystä (Griffin 2020.)



Kuvio 1 SMTP servereiden välinen StartSSL prosessi

2.6.2 SPF

SPF, eli Sender Policy Framework, on TXT tyylinen, eli tekstiä sisältävä DNS, eli Domain Name System tallenne, joka listaa kaikki autentikoidut sähköpostipalvelimet, joilla on lupa lähettää sähköposteja kyseisen verkkotunnuksen nimissä. SPF kehitettiin alun perin siksi, että sähköpostien lähettämisessä käytetty simple mail transfer protokolla, ei tarkista lähettäjän “MAIL FROM:” osoitetta, mikä mahdollistaa sähköpostien lähettäjien esiintymisen kenenä vain. (What is a DNS SPF record?)

Sähköpostin verkkotunnuksen omistajan tulee lisätä SPF:n DNS-tallenne verkkotunnuksensa hallintajärjestelmässään, josta vastaanottajan sähköpostipalvelin voi tarkistaa, mitkä ovat lähettäjän sallimien MTA palvelimien osoitteet, kun vastaanottaja tarkistaa saapuneen sähköpostiviestin.

“EHLO” komennossa olevan identifioinnin tulee vastata SPF tallenteessa olevaa osoitetta. Näin pyritään estämään kolmansien osapuolien sähköpostiväärennöksiä, joissa lähettäjä yrittää käyttää valheellista lähetysosoitetta, esiintyäkseen jonain muuna henkilönä tai palveluna. (Carranza Pablo 2013.)

2.6.3 DKIM

DKIM, eli DomainKeys Identified Mail, on sähköpostin todennusmenetelmä, joka helpottaa sähköpostiverkkotunnuksen suojaamista haitallisten tekijöiden esiintymistä kyseisen verkkotunnuksen omistajana tai asiakkaana. DKIM on nykyaikainen oleellinen osa sähköpostijärjestelmien turvaamisessa ja toimii yhdessä SPF:n ja DMARC:n kanssa tehdäkseen sähköpostiosoitteiden väärentämisestä mahdollisimman hankalaa. (What is a DNS DKIM record?)

DKIM toimii lisäämällä sähköposteihin DKIM-otsikon, jonka aitouden vastaanottava palvelin voi tarkistaa lähettävän verkkotunnuksen DKIM DNS tallenteesta (What is a DNS DKIM record?)

DKIM:n DNS tallenne on TXT tyylin tallenne, joka sisältää DKIM:n versionumeron, salaustyylin ja julkisen DKIM avaimen, jota vastaanottaja tarvitsee avatakseen DKIM otsikossa olevan digitaalisen allekirjoituksen (What is a DNS DKIM record?)

2.6.4 DMARC

DMARC, eli Domain-based Message Authentication Reporting and Conformance, on sähköpostin todennusmenetelmä, joka tarvitsee sekä, SPF, että DKIM järjestelmät toimiakseen. Käytännössä DMARC, DKIM ja SPF yhdessä, muodostavat kattavat tarkistuksen ja varmistavat, että sähköpostin lähettäjä todella on se taho, kuka hän sanoo olevansa. (What is a DNS DMARC record?)

DMARC määrittelee, mitä tulee tehdä sähköpostiviestille, jotka epäonnistuvat joissakin tarkastuksissa. Usein näissä tilanteissa sähköposti merkataan roskapostiksi, tai estetään sen vienti perille

kokonaan, riippuen miten lähettävän verkkotunnuksen DMARC DNS tallenne ohjeistaa. Kuten DKIM ja SPF, ei DMARC ole alun perin asetettu tarkistamaan saapuvia sähköposteja, jolloin se ei myöskään tee niille mitään. (What is a DNS DMARC record?)

DMARC tarvitsee jälleen oman DNS TXT tallenteen, jolla kerrotaan DMARC:in versio, haluttu toimenpide, jos lähetetty sähköposti ei läpäise tarkistuksia ja sähköpostiosoite, jonne DMARC raportit halutaan vastaanottaa. (What is a DNS DMARC record?)

DMARC tunniste kertoo, mikä on haluttu toimenpide, mikäli sähköposti ei läpäise DMARC tarkastusta. Eri vaihtoehtoja tälle ovat “none”, “reject” ja “quarantine”, joista ensimmäinen ei estä sähköpostin toimittamista, mutta ottaa virheistä logit ja lähettää ne tallenteessa osoitettuun sähköpostiosoitteeseen. (What is a DNS DMARC record?)

Reject asetus estää sähköpostin toimittamisen ja ohjeistaa vastaanottavaa sähköpostipalvelinta poistamaan viestin. (What is a DNS DMARC record?)

Quarantine asetus estää sähköpostin toimittamisen, mutta jättää sen karanteeniin, josta järjestelmänvalvoja voi sen vielä hyväksyä toimitettavaksi. Tämä on myös joissain sähköpostisovelluksissa sama, kuin postin siirto roskapostikansioon, josta loppukäyttäjä voi halutessaan viestin hakea (What is a DNS DMARC record?)

2.7 Sähköpostin komponentit

Sähköposti on nykyisin yleisesti käytetty sähköinen viestintätapa, joka on ollut olemassa, ainakin jossain mallissa, jo vuodesta 1971 alkaen. Sähköpostiviestit kulkevat usean eri komponentin läpi matkallaan lähettäjältä vastaanottajalle, mutta yksinkertaistetusti, sähköposti kirjoitetaan ja lähetetään käyttäen jonkinlaista sähköpostisovellusta, josta se lähetetään SMTP serverille, joka lähettää DNS kyselyn vastaanottajan @osoitteen mukaisesta MX tallenteesta ja saatuaan vastauksen siihen, siirtää viestin vastaanottajan SMTP palvelimelle, josta vastaanottajan MDA siirtää sähköpostin vastaanottajan MUA:lle luettavaksi. (Trivedi Yatri 2016.)

2.7.1 Mail transfer agent (MTA)

MTA:n tehtävä on vastaanottaa sähköpostiviestejä, joko loppukäyttäjiltä MUA:n kautta, tai toiselta MTA:lta, josta se siirtää sähköpostiviestin eteenpäin, joko LDA:lle, mikäli vastaanottaja on paikallinen käyttäjä, tai eteenpäin seuraavalle MTA:lle, mikäli sähköpostiosoite ei ole paikallisen käyttäjän. (Miles Tracy, Wayne Jansen, Karen Scarfone, Jason Butterfield, 2007, 18)

2.7.2 Mail delivery agent (MDA)

MDA:n tehtävä on hoitaa sähköpostiviestin toimittamisesta oikean loppukäyttäjän sähköpostilaatikkoon, josta vastaanottaja voi sen lukea, käyttäen jotain sähköpostisovellusta tai palvelua. (Miles Tracy, Wayne Jansen, Karen Scarfone, Jason Butterfield, 2007, 18)

MDA voidaan tuntea myös nimellä LDA, eli Local Delivery Agent, sillä useimmiten se hallitsee sähköposteja vain sisäverkossa. Vaikka jotkin MTA:t pystyvät hoitamaan myös MDA:n tehtäviä, on se yleisesti erillinen sovellus. (Miles Tracy, Wayne Jansen, Karen Scarfone, Jason Butterfield, 2007, 18)

2.7.3 Mail sending/submission agent (MSA)

MSA on useimmiten valmiiksi sisäistetty komponentti sähköpostin välityssovelluksissa, tai MTA:issa. MSA:n tehtävänä on vastata lähetettävien sähköpostien vastaanottamisesta loppukäyttäjältä ja sen siirto eteenpäin, lähetettäväksi vastaanottajalle. (Miles Tracy, Wayne Jansen, Karen Scarfone, Jason Butterfield, 2007, 18)

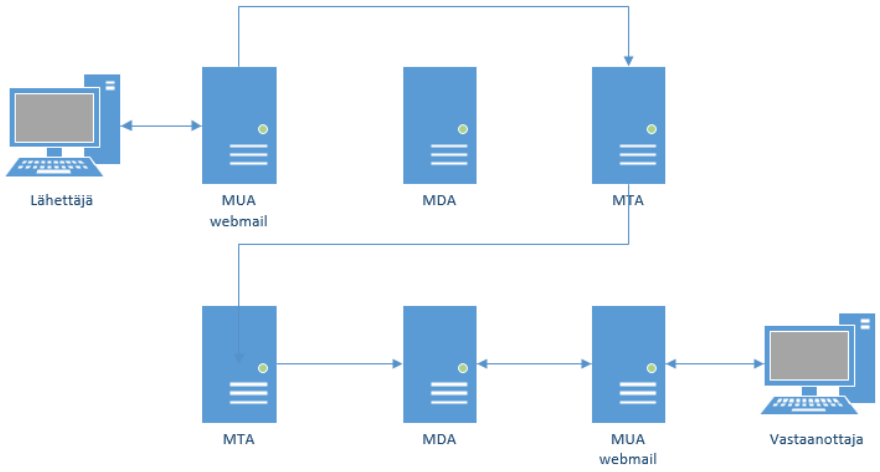
2.7.4 Mail user agent (MUA)

MUA:n tehtävä on antaa loppukäyttäjälle pääsy sähköpostipalvelimelle, mahdollistaen sähköpostiviestien lukemisen, kirjoittamisen ja lähettämisen. (Miles Tracy, Wayne Jansen, Karen Scarfone, Jason Butterfield, 2007, 18)

2.8 Sähköpostin kulku palvelimien välillä

Yksinkertaistettuna sähköpostin matka lähettäjältä vastaanottajalle on kuvattu Kuviossa 2, joka kuvastaa, miten sähköpostin lähetys toimii verkkopohjaisella sähköpostisovelluksella, jonne käyttäjä ottaa ensimmäisenä yhteyden.

MUA tässä tapauksessa on siis erillinen verkkopalvelin, jossa sähköpostisovellus on toiminnassa. Siellä lähettäjä kirjoittaa sähköpostin ja lähettää sen. Seuraavana MUA siirtää sähköpostiviestin paikalliselle MTA:lle, joka siirtää viestin eteenpäin, vastaanottajan MTA:lle, joka ohjaa sähköpostiviestin eteenpäin vastaanottajan MDA:lle, josta vastaanottaja voi MUA:n kautta käydä lukemassa sen.



Kuvio 2 Sähköpostin matka lähettäjältä vastaanottajalle

MUA voisi olla myös erillinen sovellus käyttäjän päätelaitteella, jolloin verkkopohjaista MUA:ta ei käytettäisi, vaan sähköpostisovellus ottaisi yhteyden päätelaitteelta suoraan MDA:lle vastaanotettaessa ja MTA:lle lähetettäessä sähköpostiviestejä.

3 Tarkoitus ja tavoitteet

Työn tarkoituksena on toteuttaa esimerkkitoteutus todellisuutta vastaavasta sähköposti-infrastruktuurista, joka sisältää erilliset palvelimet jokaiselle sähköpostin pääkomponentille MTA, MDA ja MUA. Tämän lisäksi työssä otetaan käyttöön ja hyödynnetään nykyaikaisia turvallisuuslaajennuksia, DKIM, DMARC ja SPF, sähköpostiliikenteen koventamiseksi ja turvallisuuden lisäämiseksi.

Toteutettua ympäristöä voidaan myöhemmässä vaiheessa käyttää myös opetustarkoitukseen Jyväskylän ammattikorkeakoulun opintokursseilla malliesimerkkinä ja sen ympärille voidaan kehittää laboratorioharjoitteita opiskelijoille.

4 Toteutus

4.1 Toteutusympäristö

Toteutukseen käytetään virtuaalisen opiskeluympäristön infrastruktuuria, VLE:tä, joka on osa Jyväskylän ammattikorkeakoulun sisäistä opetusverkkoa, LabraNet:iä. (Virtual Learning Environment (VLE))

VLE tarjoaa realistisen IT-infrastruktuurin laboratorioharjoitteille syventävien kurssien yhteydessä, helpottaen kurssiympäristöjen käyttöönottoa, sillä koko ympäristö saadaan loppukäyttäjälle yhdellä napinpainalluksella. (Virtual Learning Environment (VLE))

Käyttöjärjestelminä virtuaalipalvelimilla on Rocky Linux 8, joka on avoimen lähdekoodin yrityskäyttöjärjestelmä, joka on suunniteltu täysin bugikohtaisesti yhteensopivaksi Red Hat Enterprise Linuxin kanssa (Rocky Linux Wiki 2022.)

Sähköpostien välittäjäsovellukseksi, eli MTA:ksi otettiin käyttöön Postfix. Postfix valittiin, koska se on avoimen lähdekoodin ohjelmisto, tunettua ja paljon käytetty sähköpostin välityssovellus ja koska yrityksessä jo käytössä oleva sähköpostijärjestelmä käyttää Postfixiä, jolloin ongelmatilanteiden ratkaisu helpottuu.

Sähköpostin välittämisessä paikallisessa verkossa, eli MDA:na, käytetään Dovecot:ia

Loppukäyttäjän sähköpostisovelluksena, eli MUA:na käytetään Roundcube-sovellusta.

4.2 Tekemisvaihe

Tässä osiossa kerrotaan, miten palvelun asennus ja käyttöönotto toteutettiin.

Työn tekeminen alkoi luomalla yksi Rocky Linux virtuaalipalvelin, johon asennettiin testausta ja opettelua varten kaikki kolme sähköpostipalvelun komponenttia, Postfixin, Dovecotin ja Roundcube. Tämän tyylinen, yhden palvelimen järjestelmä on yleinen ja yksinkertainen tapa luoda sähköpostijärjestelmä. Mutta se ei täytä työn tarkoituksia, joten sitä käytettiin vain komponenttien ensimmäiseen, nopeaan testaukseen.

Postfix, Dovecot ja Roundcube ovat kaikki alkuperin konfiguroituna käyttämään lokaaleja yhteyksiä yhden palvelimen toteutuksessa. Tämä helpotti ohjelmien testausta ja mahdollisti sähköpostien kulun tarkistamisen. Tämä ei kuitenkaan ole tämän työn tarkoitus, vaan ohjelmien kuuluisi olla ajettuna omilla virtuaalipalvelimillaan.

Työtä jatkettiin luomalla jokaiselle ohjelmalle oma virtuaalipalvelin. Ensimmäiseen palvelimeen asetettiin isäntänimeksi (eng. hostname) "*mail.lokero.vle.fi*" ja sille asennettiin Postfix ohjelmisto.

Toiselle palvelimelle asetettiin isäntänimeksi "*mda.lokero.vle.fi*" ja asennettiin Dovecot ohjelmisto vastaamaan sähköpostiosoitteista ja sähköpostin perille viemisestä.

Viimeiselle palvelimelle asetettiin isäntänimeksi "*www.lokero.vle.fi*" ja asennettiin Apache HTTP verkkopalvelinohjelmisto, jonne Roundcube asennettiin toimimaan, jotta käyttäjät voivat päästä käsiksi sähköpostiviesteihinsä,

4.3 DNS tallenteet

Sähköpostit tarvitsevat oikeanlaiset DNS tallenteet, jotta sähköpostit löytävät oikeaan loppupisteeseen. Tätä varten tulee palvelimien DNS tallenteet lisätä VLE:n verkkotunnus järjestelmään.

Ensimmäisenä luotiin uusi isäntävyöhyke (eng. Master zone) verkkotunnukselle "lokero.vle.fi", jonne muut DNS tallenteet lisätään kuvion 1 mukaisesti.

Kuvio 3 DNS-tallenteet

MX tallenteet kertovat SMTP palvelimille, mikä on "*lokero.vle.fi*":n SMTP palvelimen osoite, tässä tapauksessa se ohjaa "*mail.lokero.vle.fi*" A-tyypin tallenteeseen, josta löytyy palvelimen IP-osoite, jotta sähköpostit, joiden osoitteessa on "*@lokero.vle.fi*" voidaan toimittaa sille. MX tallenteilla olisi myös mahdollista jakaa sähköpostia useammalle SMTP palvelimelle, mikäli esimerkiksi sähköpostien määrä on niin suuri, että tarvitaan kuormituksen tasaamista.

4.4 Postfixin käyttöönotto

Kun palvelimien alkuvalmistelut oli tehty, täytyi aloittaa ohjelmistojen asetuksien muuttamista, jotta ne vastaavat työn tarpeisiin. Muutokset aloitettiin Postfixistä, jonka konfiguraatiotiedostoon *main.cf* tehtiin muutoksia riveille 95 (myhostname), 103 (mydomain), 119 (myorigin) ja 184 (mydestination).

Riville 95 lisättiin palvelimen hostname, "*mail.lokero.vle.fi*", jotta se osoittaa Postfixille, mikä on palvelimen "nimi", tämän asetuksen on tärkeää olla oikein, sillä sitä käytetään useassa muussa asetuksessa oletusasetuksena.

Riville 103 asetettiin "*mydomain = lokero*", sillä myöhemmin tullaan käyttämään virtuaalisia sähköpostidomaineja, eikä tämä asetus silloin voi sisältää koko järjestelmän domainia "lokero.vle.fi".

Rivilltä 119 poistettiin kommenttimerkki "#" rivin "*myorigin = $myhostname*" alusta, jolloin Postfix käyttää palvelimen hostnamea "mail.lokero.vle.fi" kertoessaan vastaanottavalle palvelimelle, mistä sähköposti on lähetetty. Tässä olisi mahdollista käyttää myös muuttujaa "$mydomain" mutta se ei ollut yhteensopiva virtuaalisten sähköpostidomainen kanssa.

Riviltä 184 poistettiin kommenttimerkki “#” rivin “*mydestination = localhost*” alusta, jolloin tämä postfix serveri on lopullinen sähköpostin vastaanottaja vain lokaalisti lähetetyille sähköposteille, sillä muiden sähköpostiosoitteiden kohdalla palvelimen halutaan tarkistavan, löytyvätkö ne virtuaalisista sähköpostidomaineista, missä tapauksessa sähköpostiviesti ohjataan eteenpäin Dovecotille.

Tiedoston loppuun lisätään rivi “*virtual_mailbox_domains = lokero.vle.fi*”, joka kertoo Postfixille, mitä virtuaalisia domaineja se käsittelee, tämä asetus luo pohjan virtuaalisille domaineille, vaikkakin tässä tapauksessa niitä oli vain yksi. Tarvittaessa *virtual_mailbox_domains* asetusriville voidaan antaa useita eri domaineja pilkulla eriteltynä. *“Adomain.example, Bdomain.example”*

Tässä vaiheessa Postfix on valmis käyttöönotettavaksi, ja se voidaan käynnistää komennolla “*systemctl start postfix”.*

4.5 Dovecotin käyttöönotto

Tässä kokonaisuudessa Dovecot toimittaa MDA:n virkaa, mahdollistaen sähköpostien lukemisen Roundcubesta. Dovecot vastaa myös sähköpostitilien hallinnasta.

Dovecotin asetukset on jaettu useaan eri tiedostoon conf.d kansiossa. Niiden nimeämiset ovat aluksi hieman erikoiset, mutta kuitenkin hyvin loogiset, ensimmäiseksi täytyy muuttaa tiedostoa 10-mail.conf, jonne riville 31, lisättiin “*mail_home = /var/virtmail/%d/%n*” joka kertoo Dovecotille, minne saapuvat sähköpostit tulisi tallettaa. Muuttujat %d ja %n ovat sähköpostiosoitteen domain ja käyttäjänimi, tuossa järjestyksessä. Näin ollen Dovecot luo jokaiselle käyttäjälle oman sähköpostikansion domain nimen alle, tässä tapauksessa siis m1889 käyttäjän sähköpostit olisivat */var/virtmail/lokero.vle.fi/m1889* kansion alla.

Alkuvaiheessa Dovecotin plaintext kirjautuminen otettiin käyttöön, sillä se helpotti järjestelmän käyttöönottoa ja testausta. Tätä muutosta varten täytyi muokata tiedostoja 10-auth.conf ja 10-sll.conf.

Tiedostossa 10-auth.conf täytyi riviltä 10 poistaa kommenttimerkki “#”, rivin “disable_plaintext_auth = no” edestä. Ja tiedostosta 10-ssl.conf täytyi muuttaa riviltä 8 olevaa asetusta “*ssl = required*” muotoon “*ssl = yes*”, jolloin TLS salauksen käyttö on mahdollista, muttei välttämätöntä.

Myöhemmin nämä asetukset oli helppo käydä muuttamassa takaisin vanhoihin asetuksiinsa, jolloin salaus on pakollinen kirjautumisessa. Tätä varten tarvittaan TLS certifikaatti, jonka pystyy VLE:ssä pyytämään Let’s Encrypt palvelusta.

Seuraavaksi asetetaan Dovecot hoitamaan sähköpostitilejä. Toteutustavaksi valittiin yksinkertainen passwd-file menetelmä, jossa käyttäjätunnukset, eli sähköpostiosoitteet ja salasanojen hashit tallennetaan “users” nimiseen tiedostoon, josta Dovecotin authentikaatioprosessi pystyy tarkistamaan ne sisäänkirjautumisissa ja saapuvissa sähköposteissa.

Tämä toteutustapa valittiin ajanpuutteen vuoksi. Tämä ei ole paras mahdollinen järjestelmä, sillä tässä menetelmässä ylläpitäjän täytyy manuaalisesti ylläpitää käyttäjälistauksia users tiedostossa, kun sähköpostiosoitteita ja salasanoja vaihdetaan, tai lisätään. Jatkokehityksessä tämä voidaan vaihtaa esimerkiksi LDAP järjestelmään, jolloin se voidaan yhdistää jo olemassa oleviin käyttäjätileihin VLE:ssä.

Jotta Dovecot huomioisi Users tiedoston, täytyy asetuksia muuttaa tiedostoissa auth-passwdfile.conf.ext ja 10-auth.conf.

Auth-passwdfile.conf.ext tiedostossa muokataan passdb osiota, varmistaen että “args” rivillä on “*args = scheme = SHA512-CRYPT username_format=%u /etc/dovecot/users*”, jossa “*shceme=SHA512-CRYPT*” kertoo Dovecotille, millä järjestelmällä salasanat on sotkettu. Tässä tapauksessa SHA512-CRYPTillä.

Seuraavana oleva, “username_format=%u” kertoo, missä muodossa käyttäjätunnus on. Tässä tapauksessa “%u” tarkoittaa, että käytetään koko käyttäjätunnusta, joka sisältää myös sähköpostiosoitteen loppuosan, esimerkiksi “m1889@lokero.vle.fi”. Viimeisenä asetuksena on vielä users tiedoston sijainti.

Uusien salasanojen hashin luomiseksi voidaan käyttää Dovecotin omaa “doveadm” työkalua. Komennolla “*doveadm pw -s sha512-crypt*” saadaan tehtyä salasanasta hash, joka voidaan kopioida Users tiedostoon.

Viimeisenä vaiheena pitää tämä juuri konfiguroitu asetustiedosto laittaa ladattavaksi dovecotille. Sitä varten on muokattava tiedostoa “10-auth.conf” ja poistettava kommenttimerkki “#” rivin 125 alusta.

Tässä vaiheessa Postfix ja Dovecot ovat toimintakuntoisia, vaikkeivat vielä lopullisessa konfiguraatiossa, mutta nyt Roundcuben käyttöönotto on mahdollista.

4.6 Roundcuben käyttöönotto

Ensimmäisenä tuli Roundcuben ohjelmisto ladata Roudncuben verkkosivuilta, jonka jälkeen ladattu tiedosto purettiin kansioon *“/var/www/roundcube*”. Nyt Roundcuben tiedostot ovat verkkopalvelimen saatavilla, mutta sille täytyy vielä kertoa, mistä tiedostot löytyvät. Eli täytyy luoda Roundcuben oma virtualhost tiedosto “*/etc/httpd/conf.d/roundcube.conf*”. Jonka sisältö on tarkasteltavissa kuviossa 4, siinä määritellään serverin nimi, tiedostojen sijainti ja minne logitiedostot tulisi tallentaa.

```
<VirtualHost *:80>
  ServerName www.lokero.vle.fi
  DocumentRoot /var/www/roundcube/

  ErrorLog /var/log/httpd/roundcube_error.log
  CustomLog /var/log/httpd/roundcube_access.log combined

  <Directory />
    AllowOverride All
  </Directory>

  <Directory /var/www/roundcube/>
    AllowOverride All
    Order allow,deny
    Allow from all
  </Directory>

</VirtualHost>
```

Kuvio 4 Roundcuben Virtualhost

Tämän jälkeen asennettiin Roundcuben tarvitsemat ohjelmistot, PHP 7.4 ja MySQL tietokantajärjestelmä. Edellä mainittujen ohjelmistojen lisäksi Roundcube tarvitsee myös useita PHP:n lisäosia: *php-curl, php-json, php-xml, php-mbstring, php-imap, php-mysqlnd, php-cli* ja *php-gd*.

Roundcuben asennusprosessi osaa havaita ja huomauttaa, mikäli jokin tarpeellisista lisäosista puuttuu. Asennusprosessin aikana on myös nähtävillä lista muista lisäosista, jotka eivät ole pakollisia, mutta mahdollisesti parantaisivat loppukäyttäjän käyttäjäkokemusta.

Asennusvaiheessa, Roundcubessa on verkkopohjainen asennusprosessi, jossa annetaan tiedot palvelun nimestä, tietokannan tunnukset ja yhteystiedot, sähköpostin domain, IMAP ja SMTP palvelimien osoitteet, ja muut, mitkä ovat nähtävillä myös Roundcuben asetustiedostossa config.inc.php, joka on nähtävissä kuviossa 5.

Verkkopohjainen asennus ei kuitenkaan jostain syystä kyennyt asettamaan kaikkia annettuja tietoja, kuten IMAP ja SMTP servereiden osoitteita tähän tiedostoon, vaan ne tuli lisätä manuaalisesti.

```
<?php

$config['product_name'] = 'Lokero Webmail';
$config['db_dsnw'] = 'mysql:                                                    ';
$config['mail_domain'] = 'lokero.vle.fi';
$config['imap_host'] = 'mda.lokero.vle.fi';
$config['smtp_host'] = 'mail.lokero.vle.fi:25';
$config['support_url'] = 'mailto:haltija@lokero.vle.fi';
$config['des_key'] = '                          `;
$config['plugins'] = ['emoticons'];
```

Kuvio 5 Roundcuben asetustiedosto

Seuraavassa vaiheessa pystyi Roundcuben asetuksia, kuten IMAP yhteyttä ja sähköpostin lähettämistä, testaamaan. Kun asennus valmistui, tuli kansio "*installer*" poistaa Roundcuben tiedostoista, koska muuten se aiheuttaisi mahdollisuuden kenelle tahansa muuttaa palvelun asetuksia.

4.7 SASL authentikaatio

Hyödynnetään Dovecotin IMAP authentikaatiota ja käytetään sitä authentikoidaksemme käyttäjän Postfixille. Näin voidaan rajoittaa ei authentikoituijen käyttäjien sähköpostin lähetystä.

Ensimmäiseksi Dovecotille täytyy lisätä “kuuntelija” joka odottaa authentikointi pyyntöjä Postfixiltä. Tämä on mahdollista lisäämällä “*inet_listener { port = 12345 }*” Dovecotin 10-master.conf tiedostossa olevan *service auth* asetuksen sisään. Portin ei tarvitse olla *12345* vaan käytännössä siihen voi valita minkä vain vapaan portin, kunhan saman portin laittaa myös Postfixille.

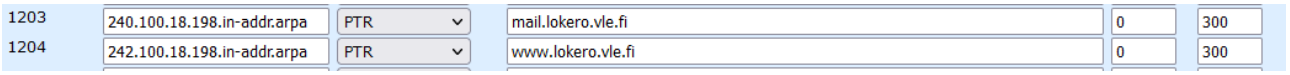
Seuraavaksi Postfixin asetuksiin tulee lisätä kolme riviä: “*smtpd_sasl_auth_enable = yes*”, “*smtpd_sasl_type = dovecot*” ja “*smtpd_sasl_path = inet:[mda.lokero.vle.fi]:12345*”.

Ensimmäinen rivi kertoo Postfixille, että SASL authentikaatio on käytössä, toinen rivi tarkentaa, että authentikaatiokyselyihin on vastaamassa Dovecot ja viimeinen rivi antaa authentikaatiopalvelun osoitteen ja portin.

4.8 Todennuksien käyttöönotto

Kun järjestelmä on saatu asennettua, on aika ottaa kovennuksia käyttöön. Tavoitteina oli saada vähintään SPF, DKIM ja DMARC todennukset toimimaan.

Aluksi täytyy varmistaa, että palvelimilla on PTR tallenteet, sillä muuten SPF tarkistukset voivat antaa “*fail*” statuksen, koska se ei kykene tarkistamaan serverin verkkotunnusta IP-osoitteen avulla. PTR tallenteet asetettiin kuvion 6 mukaisesti. mda.lokero.vle.fi, ei tarvitse PTR tallennetta, mutta sille olisi mahdollista sellainen asettaa, jos tarvetta myöhemmässä vaiheessa esiintysi.



Kuvio 6 Palvelimien PTR tallenteet

Seuraavana asetetaan SPF toimintaan, jota varten luodaan DNS tallenne, jonka tyyli on TXT ja sisältö "*v=spf1 mx ~all*". Jossa v=spf1 kertoo, että kyseessä on SPF tallenne ja että käytössä oleva versio on spf1. "mx ~all" osoittaa, että kaikki sähköpostit tulisi olla lähetettynä vain verkkotunnuksen MX tallenteissa osoitetuista palvelimista. Muiden palvelimien lähettämät sähköpostit merkataan epäluotettaviksi.

Tässä olisi myös mahdollista käyttää tiukempia sääntöjä, kuten -all jolloin kaikki sähköpostit jotka on lähetetty ei tunnistetusta lähteestä tulisi hylätä kokonaan.

Vaikka SPF on nyt toiminnassa lähteville sähköposteille, ei saapuville sähköposteille vielä tehdä SPF-tallenteen todennusta.

Tätä ominaisuutta varten tulee asentaa uusi ohjelma, pypolicyd-spf. Tämä onnistuu komennolla "*yum install pypolicyd-spf*".

Tälle ohjelmalle tulee lisätä oma käyttäjä, joka onnistuu komennolla "*adduser policyd-spf --user-group --no-create-home -s /bin/false*".

Viimeiseksi täytyy vielä Postfixille kertoa, että sen tulisi tarkistaa saapuvien sähköpostien SPF tallenteet käyttäen juuri asennettua policyd-spf ohjelmaa. Tätä varten pitää Postfixin *master.cf* tiedostoon lisätä kaksi riviä kuvion 7 mukaisesti ja *main.cf* tiedostoon kuusi riviä kuvion 8 mukaisesti.

```
policyd-spf  unix  -       n       n       -       0       spawn
    user=policyd-spf argv=/usr/libexec/postfix/policyd-spf
```

Kuvio 7 SPF tarkistuksien käyttöönotto master.cf tiedostossa

```
#SPF Things
policyd-spf_time_limit = 3600
smtpd_recipient_restrictions =
   permit_mynetworks,
   permit_sasl_authenticated,
   reject_unauth_destination,
   check_policy_service unix:private/policyd-spf
```

Kuvio 8 SPF asetuksia

Nyt saapuvista sähköposteista tarkistetaan SPF tietueet. Näin ollen riippuen lähettäjän SPF asetuksista, pystyy Postfix tekemään johtopäätöksiä siihen, onko sähköposti lähetetty sieltä, mistä se sanoo olevansa.

Toisena osana kovennusta asetetaan lähteviin sähköposteihin DKIM allekirjoitus ja asetetaan saapuviin sähköposteihin DKIM allekirjoituksen tarkistus käyttäen OpenDKIM ohjelmistoa.

OpenDKIM voidaan asentaa komennolla "*yum install opendkim opendkim-tools*".

Tehdasasetuksillaan OpenDKIM on asetettu pelkästään tarkistamaan saapuvien sähköpostien DKIM allekirjoituksen, mutta muuttamalla asetustiedostosta opendkim.conf riviä 39 "*node v*" asetusta muotoon "*node sv*", asetetaan OpenDKIM myös lisäämään DKIM allekirjoitus lähteviin sähköposteihin.

Allekirjoitusta varten täytyy edellä mainitun asetuksen lisäksi OpenDKIMille vielä tehdä ja asettaa allekirjoitusavain, sekä kertoa, minkä verkkotunnuksen sähköposteja sen tulisi allekirjoittaa. Tätä varten tulee *opendkim.conf* tiedostosta poistaa kommenttimerkki "#" kuvion 9 mukaisesti riveiltä 103, 108 ja 115.

```
##  Gives the location of a file mapping key names to signing keys. In simple terms,
##  this tells OpenDKIM where to find your keys. If present, overrides any KeyFile
##  directive in the configuration file. Requires SigningTable be enabled.
 KeyTable       /etc/opendkim/KeyTable

##  Defines a table used to select one or more signatures to apply to a message based
##  on the address found in the From: header field. In simple terms, this tells
##  OpenDKIM how to use your keys. Requires KeyTable be enabled.
 SigningTable   refile:/etc/opendkim/SigningTable

##  Identifies a set of "external" hosts that may send mail through the server as one
##  of the signing domains without credentials as such.
# ExternalIgnoreList    refile:/etc/opendkim/TrustedHosts

##  Identifies a set "internal" hosts whose mail should be signed rather than verified.
 InternalHosts  refile:/etc/opendkim/TrustedHosts
```

Kuvio 9 OpenDKIM asetukset allekirjoitukselle

Seuraavaksi tulee muokata *SigningTable* tiedostoa, jolla OpenDKIMille kerrotaan, minkä domainin lähetettävät sähköpostit sen tulee allekirjoittaa milläkin domainavaimella. Tässä tapauksessa tiedoston loppuun lisättiin "**@lokero.vle.fi 09112022._domainkey.lokero.vle.fi*", joka osoittaa että, kaikki sähköpostit, joiden verkkotunnuksena on "lokero.vle.fi", tulee allekirjoittaa verkkotunnusavaimella "*09112022._domainkey.lokero.vle.fi*".

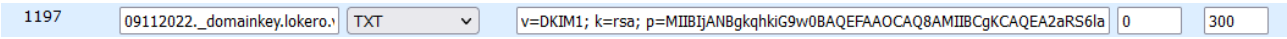
DKIM-allekirjoitusta varten tarvitaan privaatti ja julkinen avain. Nämä avaimet voidaan luoda opendkim-genkey työkalulla, joka sisältyy OpenDKIM ohjelmistoon.

Avaimet luodaan komennolla "*opendkim-genkey -b 2048 -d lokero.vle.fi -D /etc/opendkim/keys/lokero.vle.fi -s 09112022 -v*" jossa "*-d*" osoittaa verkkotunnuksen, jolle avaimet luodaan ja "*-D*" osoittaa, minne luodut avaimet tulee tallentaa.

Nämä tiedostot tulee asettaa OpenDKIM käyttäjän omistukseen. Se onnistuu komennolla "*chown opendkim:opendkim -R /etc/opendkim/keys/*"

Aiemin osoitettuun*"KeyTable*" tulee lisätä DKIMi:ä varten luodun privaattiavaimen sijainti. Tämä tapahtuu lisäämällä *KeyTable* tiedoston loppuun rivi: "09112022._domainkey.lokero.vle.fi lokero.vle.fi:09112022:/etc/opendkim/keys/lokero.vle.fi/09112022.private".

Seuraavana askeleena DKIM:in käyttöönotossa tulee julkinen avain laittaa DNS tallenteella näkyviin kuvion 10 mukaisesti. Tämä on tarpeellista, jotta vastaanottava sähköpostipalvelin kykenee purkamaan DKIM-allekirjoituksen ja todentamaan sen aitouden.



Kuvio 10 DKIM avain TXT tietue

Viimeiseksi OpenDKIM yhdistetään vielä Postfixiin, jotta lähtevät sähköpostit allekirjoitetaan ja saapuvien sähköpostien allekirjoitukset tarkastetaan. Tätä varten lisätään muutoksia Postfixin *main.cf* tiedostoon kuvion 11 mukaisesti. Nyt lähteviin sähköposteihin lisätään DKIM-allekirjoitus ja saapuvista sähköposteista DKIM-allekirjoitukset tarkistetaan.

```
#OpenDKIM,
# Milter configuration
milter_default_action = accept
milter_protocol = 6
smtpd_milters = inet:127.0.0.1:8891,
non_smtpd_milters = $smtpd_milters
```

Kuvio 11 DKIM asetukset Postfixille

Viimeisenä kovennuksena tulee aktivoida vielä DMARC, jolla voidaan estää sähköpostiosoitteiden huijausta, tai “spoofausta”, hyödyntäen edellä asetettuja SPF ja DKIM kovennuksia. Tähän käytetään OpenDMARC ohjelmistoa.

OpenDMARC asennetaan komennolla “*yum install opendmarc*” jonka jälkeen täytyy OpenDMARC:in asetustiedostoon *opendmarc.conf* tehdä muutoksia.

Rivillä 28 tulee poistaa kommenttimerkki “#” ja lisätä rivin loppuun osio: “*OpenDMARC*”, jonka lisäksi riville 29 tulee lisätä “*TrustedAuthServerIDs*” rivin perään “*mail.lokero.vle.fi*”.

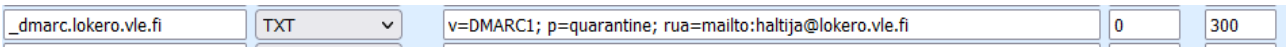
Rivillä 318 poistetaan kommenttimerkki “#” ja muutetaan “*RejectFailures false*” muotoon “*RejectFailures true*”. Tällöin sähköpostit, jotka epäonnistuvat DMARC tarkistuksessa hylätään.

Seuraavaksi yhdistetään OpenDMARC ohjelman tarkistus saapuville sähköposteille Postfixiin. Tämä onnistuu tekemällä Postfixin asetustiedostoon, *main.cf* pieni lisäys, jo lisättyyn DKIM konfiguraatioon, kuvion 12 mukaisesti. Riville "*smtpd_milters = inet:127.0.0.1:8891*" lisätään "*inet:127.0.0.1:8893*".

```
#OpenDKIM, OpenDMARC
# Milter configuration
milter_default_action = accept
milter_protocol = 6
smtpd_milters = inet:127.0.0.1:8891,inet:127.0.0.1:8893
non_smtpd_milters = $smtpd_milters
```

Kuvio 12 OpenDMARC lisäys main.cf tiedostoon

Viimeiseksi pitää DMARC:ia varten luoda vielä DNS tietue kuvion 13 mukaisesti.



Kuvio 13 DMARC DNS Tietue

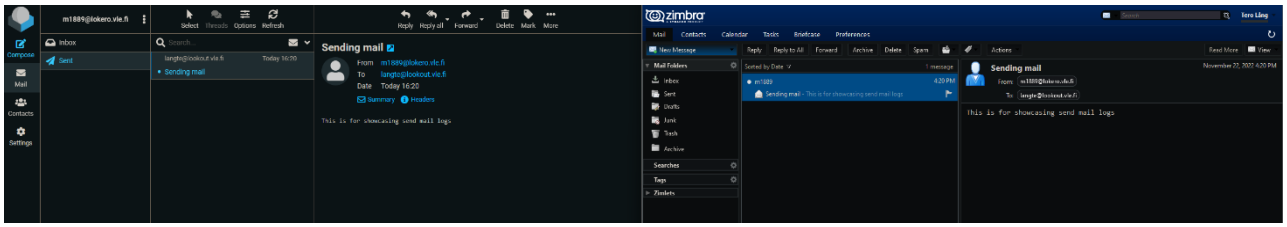
Tässä "*v=DMARC1*" kertoo kyseessä olevan DMARC tietue ja että käytössä on DMARC:in versio 1, "*p=quarantine*", osoittaa, että sähköpostit, jotka epäonnistuvat DMARC tarkistuksessa, tulee asettaa karanteeniin ja "rua=mailto:haltija@lokero.vle.fi" joka osoittaa, mihin sähköpostiosoitteeseen DMARC:in koostetut raportit tulisi lähettää.

Viimeisenä vaiheena tulee Postfix käynnistää uudelleen, se tapahtuu komennolla "*systemctl restart postfix*"

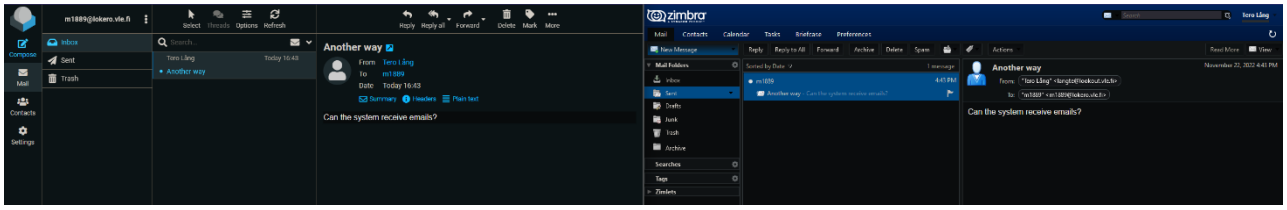
Nyt jälkeen kovennuksien pitäisi olla asennettuna, konfiguroituna ja aktiivisena.

4.9 Järjestelmän ja kovennuksien testaus

Kun yksittäiset osat ovat asennettu ja konfiguroitu, on aika testata ja todentaa, että järjestelmä pystyy vastaanottamaan ja lähettämään sähköposteja. Aloitetaan lähettämällä sähköposti osoitteesta “*m1889@lokero.vle.fi*” osoitteeseen “*langte@lookout.vle.fi*”. Kuten kuvioista 14 ja 15 näkyy, sähköposti kulkee palvelimien välillä.



Kuvio 14 Sähköpostin lähetystestaus



Kuvio 15 Sähköpostin vastaanottotestaus

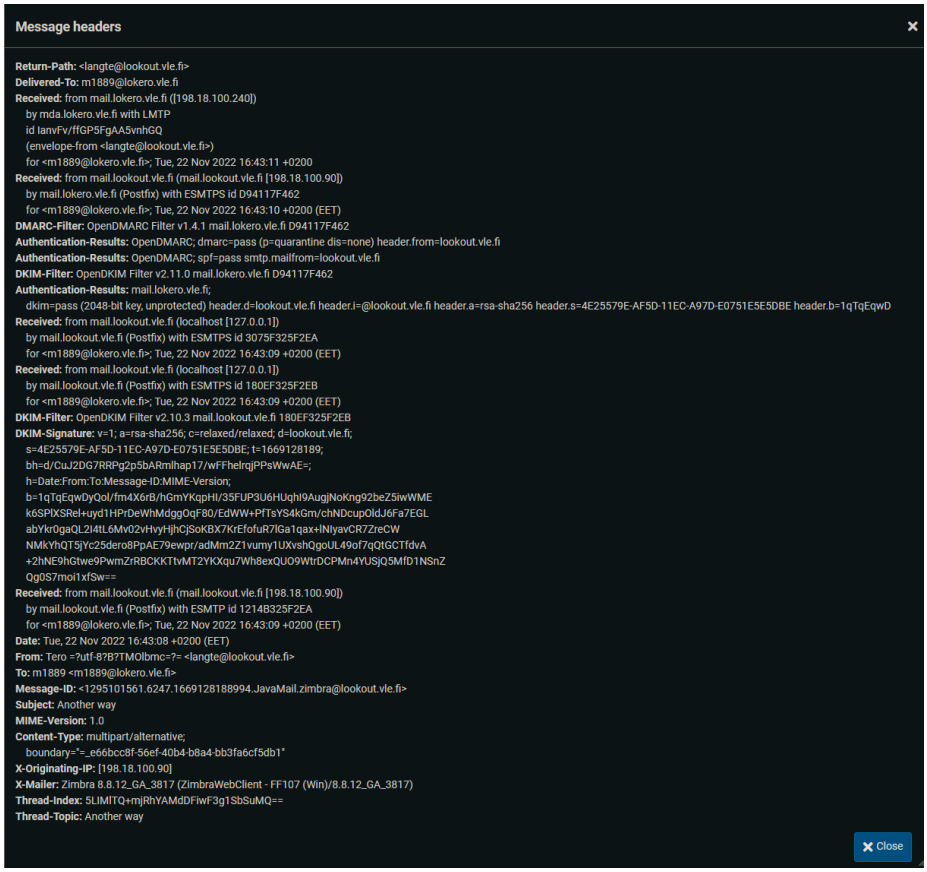
Seuraava tarkastelun kohde on, käyttääkö järjestelmä sinne asetettuja kovennuksia. Tämä voidaan tarkistaa tarkastelemalla sähköpostipalvelimen lokitiedostoista ja sähköpostin otsikoita.

Kuviosta 16 nähdään kuviossa 15 vastaanotetun sähköpostiviestin headerit, joista käy ilmi, että vastaanottava lokeron sähköpostipalvelin suoritti halutut tarkistukset.

DMARC tarkistaa riveillä 12 ja 13 vastaanotetun sähköpostiviestin autentikaation, ja palauttaa arvot “dmarc=pass (p=quarantine dis=none) header.from=lookout.vle.fi” ja “spf=pass smtp.mailfrom=lookout.vle.fi”.

Eli sähköpostin DMARC ja SPF tallenteet vastaavat *lookout.vle.fi* DNS tallenteista löytyviä tietoja, osoittaen, että sähköposti on aidosti lähetetty palvelimelta *lookout.vle.fi*.

Rivillä 16 voidaan huomata DKIM tarkistuksen tulos, joka on palauttanut arvon “dkim=pass” joka osoittaa, että sähköpostista on löytynyt DKIM otsikko, joka on kyetty avaamaan *lookout.vle.fi*:n DKIM tallenteessa olevalla julkisella avaimella.



Kuvio 16 Vastaanotetun sähköpostin headerit

Viimeisenä testataan vielä, mitä tapahtuu, jos saapuva sähköpostiviesti ei läpäise tarkistuksia.

Tätä varten pyritään lähettämään sähköpostiviesti Telnetillä käyttäen satunnaista virtuaalikonetta VLE:n sisällä.

Kovennuksista johtuen, ei telnetillä sähköpostin lähettäminen ole enää niin suoraviivaista, kuin se aluksi oli. Nyt sähköpostin DATA osiossa, täytyy olla FROM, TO ja DATE osiot. Ilman näitä, sähköposti hylätään välittömästi ilman muita tarkastuksia.

EHLO lookout.vle.fi

MAIL FROM: langte@lookout.vle.fi

RCPT TO: m1889@lokero.vle.fi

DATA

FROM: ”Tero Lång” <langte@lookout.vle.fi>

TO: ”Tero Lång” <m1889@lokero.vle.fi>

DATE: Fri 18. Nov 09:39:11

Hei Maailma!

.

Kuviossa 17 nähdään, että yhteys tulee “*from unknown[198.18.100.241]*”, joka väittää olevansa “*lookout.vle.fi*”, mutta OpenDMARCin SPF tarkistus palauttaa arvon “*fail*”, sillä palvelimen IP-osoite ei vastaa *lookout.vle.fi:*n SPF tallennetta, jolloin sähköpostiviesti on epäonnistunut DMARC tarkastuksessa ja jää karanteeniin, joka näkyy lokitiedostossa viestinä “*milter triggers HOLD action*”.

Kuvio 17 SPF result fail

Tarkistetaan vielä toiseen suuntaan kulkevista sähköposteista, että halutut tietueet näkyvät.

Kuviosta 18. nähdään, että *lokero.vle.fi*:stä lähetetyssä sähköpostissa löytyy DKIM allekirjoitus, ja se luetaan onnistuneesti.

Valitettavasti *lookout.vle.fi* palvelussa ei ole SPF ja DMARC tallenteiden todennusta otettuna käyttöön, joten niiden tarkistaminen ei ole mahdollista ja jää näinollen jatkokehityksen aiheeksi.

```
Return-Path: <m1889@lokero.vle.fi>
Received: from mail.lookout.vle.fi (LHLO mail.lookout.vle.fi)
 (198.18.100.90) by mail.lookout.vle.fi with LMTP; Tue, 22 Nov 2022 16:20:30
 +0200 (EET)
Received: from mail.lookout.vle.fi (localhost [127.0.0.1])
        by mail.lookout.vle.fi (Postfix) with ESMTPS id 03DC6325F2EA
        for <langte@lookout.vle.fi>; Tue, 22 Nov 2022 16:20:30 +0200 (EET)
Received: from mail.lookout.vle.fi (localhost [127.0.0.1])
        by mail.lookout.vle.fi (Postfix) with ESMTPS id E98B4325F2EB
        for <langte@lookout.vle.fi>; Tue, 22 Nov 2022 16:20:29 +0200 (EET)
Received: from mail.lokero.vle.fi (mail.lokero.vle.fi [198.18.100.240])
        by mail.lookout.vle.fi (Postfix) with ESMTPS id E4A4A325F2EA
        for <langte@lookout.vle.fi>; Tue, 22 Nov 2022 16:20:29 +0200 (EET)
Received: from www.lokero.vle.fi (www.lokero.vle.fi [198.18.100.242])
        by mail.lokero.vle.fi (Postfix) with ESMTPA id 5FBA67F462
        for <langte@lookout.vle.fi>; Tue, 22 Nov 2022 16:20:25 +0200 (EET)
DKIM-Filter: OpenDKIM Filter v2.11.0 mail.lokero.vle.fi 5FBA67F462
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=lokero.vle.fi;
        s=09112022; t=1669126825;
        bh=6GslBYx/4Um+X2vtITNDMm+y/P1pbfiAgQo2wMOpL5s=;
        h=Date:From:To:Subject:From;
        b=iisXLs4jdmbpwHCOv8xZuJDETCgXIvap12GZCpbv7hoc3Lb9NGvWI44ixjh9zdfIV
         bfThLN3AxSxGy0zsGe8rzYkL0l3fCs4JiIIarQF39/g8JZvgF8bV72I2coEfbk9+Ce
         LsbCY1sCHz6qfOmwD0MM7bqZc0/bT1mNK/Oe7ws7BbjoqSTcyNMGuXefwqU/uOySqj
         1nRiI4Isi5WbPKd1wtT9CsFwv4iJ3ObX1PHnh7GdQG5oC4GTohZrrsIK9ElX4pAiV4
         2LKrWz1hBlT+nZCONkF09/E9N98sPgnSYn39Qfl9UTij8v3kvNy9NWlXkpW8HYgpT1
         mvYva3f3LKDDQ==
MIME-Version: 1.0
Date: Tue, 22 Nov 2022 16:20:25 +0200
From: m1889@lokero.vle.fi
To: langte@lookout.vle.fi
Subject: Sending mail
Message-ID: <0af6521eea717abcce7fc708df75e706@lokero.vle.fi>
X-Sender: m1889@lokero.vle.fi
Content-Type: text/plain; charset=US-ASCII;
 format=flowed
Content-Transfer-Encoding: 7bit

This is for showcasing send mail logs
```

Kuvio 18 Lokero.vle.fistä vastaanotetun sähköpostin otsikot

Näistä testeistä voidaan päätellä, että järjestelmä kovennuksineen toimii. Ainakin vastaanotettaville sähköposteille suoritetaan halutut todennukset.

5 Tulos: Lokero.vle.fi

Työn tuloksena saatiin toimiva, todellisuutta mallintava, nykyaikaisesti suojattu sähköpostijärjestelmä. Tätä järjestelmää on yhä mahdollista jatkokehittää, mutta se on nyt työlle asetettujen tavoitteiden mukainen. Sähköpostijärjestelmä hyödyntää nykyaikaisia koventamislaajennuksia, SPF, DKIM ja DMARC.

Koventamislaajennukset todentavat, että sähköpostiviestit ovat tulleet sieltä, mistä niiden kuuluisikin ja mahdollistavat myös vastaanottajalle lähetettyjen viestien autenttisuuden tarkistuksen,

mikäli he ovat ottaneet sen käyttöön. Valitettavasti VLEssä jo käytössä oleva sähköpostijärjestelmä, *lookout.vle.fi*, ei ole ottanut kaikkia kovennusmenetelmiä käyttöön, jolloin tuotetun palvelun lähetettyjen sähköpostien turvausta ei voitu täydellisesti todentaa.

Laboratorio-ohjeistus järjestelmälle jäi myös aikataulusyistä jatkokehityksen tehtäväksi.

6 Tuloksen analyysi ja arviointi

6.1 Johtopäätökset

Työ oli hyvin mielenkiintoinen, mutta isoimman ongelman toi heti alkuun se, etten ollut ennen pystyttänyt sähköpostijärjestelmää. Tähän lisättynä vielä hyvin kiireinen aikataulu aiheutti, ettei järjestelmässä ole mitään käyttäjämukavuutta lisääviä ominaisuuksia.

Isoimpana ongelmana työn toteutuksessa oli se, kun järjestelmä pystyi lähettämään sähköpostiviestejä normaalisti, mutta ei kyennyt vastaanottamaan viestejä lainkaan. Tässä ongelmaksi ilmeni lopulta virheellinen muotoilu Dovecotin asetustiedostossa, jolloin sähköpostiosoitteiden kirjoitusmuoto ei vastannut sähköpostien lähetysosoitetta.

Dovecotin kohdalla kehittäjien dokumentaatio oli välillä hieman vajavainen, eikä näin ollen virheilmoituksista meinannut aina löytyä ohjeistusta, kuten edellä mainitussa tilanteessa. Mutta onneksi kaikki työssä käytetyt ohjelmat ovat yleisesti käytettyjä avoimen koodipohjan sovelluksia, joten tarkalla etsimisellä apua löytyi aina lopulta.

Tärkeimpänä oman sähköpostijärjestelmän pystytyksen esteenä on se, että Suomessa SMTP:n käyttämä portti 25 on suljettu käytännössä kaikissa yksityisten ihmisten verkkopalveluissa. Jolloin sähköpostit tulee joko ohjata eri portin kautta, jolloin todennusmekanismit voivat hälyttää virheellisesti, sillä osoite ei vastaa standardin mukaista porttijärjestelyä, tai käyttää verkonhaltijan mahdollisesti tarjoamaa sähköpostin välityspalvelinta. Näihin ohjeet löytyvät useimmiten palveluntarjoajan verkkosivuilta.

6.2 Hyödynnettävyys

Nyt rakennettu sähköpostijärjestelmä on siinä tilassa että, sitä voidaan hyödyntää malliesimerkkinä oppilaille. Sähköpostin todennukset ovat toiminnassa ja sähköposti kulkee molempiin suuntiin halutusti.

Palvelua jatkokehittämällä, se voidaan tarvittaessa ottaa käyttöön koko Virtual Learning Environmentin laajuisesti, jolloin opiskelijoille voidaan luoda sähköpostitilejä sinne, käyttäen jo olemassa olevaa Jyväskylän ammattikorkeakoulun LDAP järjestelmää automaattisesti, kurssi-ilmoittautumisten mukaan.

Järjestelmää voidaan hyödyntää esimerkiksi opiskelijoiden omien sähköpostijärjestelmien kovennuksien todentamiseen, kurssien laboratorioharjoitteiden myötä.

Lähteet

About the Roundcube webmail project. N.d. Viitattu 23.11.2022. https://roundcube.net/about/

Dovecot manual. N.d. Viitattu 10.09.2022. https://doc.dovecot.org

Carranza Pablo. How To use an SPF Record to Prevent Spoofing & Improve E-mail Reliability, 2013. Viitattu 26.09.2022. https://www.digitalocean.com/community/tutorials/how-to-use-an-spf-record-to-prevent-spoofing-improve-e-mail-reliability

Ceci L. 2022. Viitattu 20.09.2022. Number of sent and received e-mails per day worldwide from 2017 to 2025. https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/

Griffin Julie. What is StartTLS?, 2022. Viitattu 20.10.2022. https://sendgrid.com/blog/what-is-starttls/

Gibbs Samuel. 2016. Viitattu 18.09.2022. How did email grow from messages between academics to a global epidemic? https://www.theguardian.com/technology/2016/mar/07/email-ray-tomlinson-history

J. Klensin, 2008, Simple Mail Transfer Protocol, viitattu 25.09.2022, https://www.rfc-editor.org/rfc/rfc5321

Mail (MX) Server Survey. 2022. Viitattu 23.11.2022. http://www.securityspace.com/s_survey/data/man.202210/mxsurvey.html

Markoff John. Sharing Software, IBM to Release Mail Program Blueprint. 1998. Viitattu 19.10.2022. https://archive.nytimes.com/www.nytimes.com/library/tech/98/12/biztech/articles/14blue.html

Mikä on teletoimintaa. 2021. Viitattu 28.11.2022. https://www.traficom.fi/fi/viestinta/viestintaverkot/mika-teletoimintaa

Miles Tracy, Wayne Jansen, Karen Scarfone, Jason Butterfield. Guidelines on Electronic Mail Security. 2007. Viitattu 11.10.2022. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-45ver2.pdf

Postfix feature overview. N.d. Viitattu 10.09.2022. https://www.postfix.org/features.html

Rocky Linux Wiki. 2022. Viitattu 28.11.2022. https://wiki.rockylinux.org/

Scott Rose, J. Stephen Nightingale, Simson Garfinkel, Ramaswamy Chandramouli, 2019. Trustworthy Email. Viitattu 26.09.2022. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf

SMTPS: Securing SMTP and the Differences Between SSL, TLS, and the Ports They Use. 2022. Viitattu 30.09.2022. https://www.agari.com/blog/smtps-how-to-secure-smtp-with-ssl-tls-which-port-to-use

The Postfix Home Page. N.d. Viitattu 10.09.2022. https://www.postfix.org/start.html

Tiettyihin tietoliikenneportteihin suuntautuvan liikenteen tietoturvaperusteinen suodattaminen teleyritysten verkoissa. 2020. Viitattu 25.09.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Suositus3122020.pdf

Trivedi Yatri. 2016. How Does Email Work? Viitattu 22.11.2022. https://www.howtogeek.com/56002/htg-explains-how-does-email-work/

Virtual Learning Environment (VLE). 2021. Viitattu 23.11.2022. https://student.labranet.jamk.fi/virtual-learning-environment-vle/

Virtual Learning Environment. N.d. Viitattu 28.11.2022. https://www.jamk.fi/fi/virtual-learning-environment

What is a DNS SPF record? N.d. Viitattu 20.10.2022. https://www.cloudflare.com/learning/dns/dns-records/dns-spf-record/

What is a DNS DKIM record? N.d. Viitattu 20.10.2022. https://www.cloudflare.com/learning/dns/dns-records/dns-dkim-record/

What is a DNS DMARC record? N.d. Viitattu 20.10.2022. https://www.cloudflare.com/learning/dns/dns-records/dns-dmarc-record/

Liitteet