SSL/TLS-sertifikaattien elinkaari, hallinnointi ja automatisointi

Helene Öller

Haaga-Helia ammattikorkeakoulu

Tietojenkäsittely

Opinnäytetyö

2023

Tiivistelmä

Tekijä(t)
Helene Öller

Tutkinto
IT-Tradenomi

Raportin/Opinnäytetyön nimi
SSL/TLS-sertifikaattien elinkaari, hallinnointi ja automatisointi

Sivu- ja liitesivumäärä
45 + 0

Tänä päivänä tieto on meidän tärkein hyödykkeemme, ja käytämme sitä yhä enemmän verkossa. Silloin haluamme voida luottaa siihen, että muut osapuolet ovat varmasti he, joita esittävät olevansa. Sertifikaatti on tietorakenne, joka sisältää tietoa muun muassa sen omistajasta, myöntäjästä, voimassaoloajasta ja käyttötarkoituksesta. Sertifikaatti on luotettavan tahon antama kiistämätön todiste siitä, että kyseinen toimija on se, jota hän esittää olevansa.

Tämän työn tavoitteena on selvittää sertifikaatteihin sekä niiden elinkaareen ja hallintaan liittyvät asiat. Tarkoituksena on lisäksi selvittää erilaisia menetelmiä ja työvälineitä, joita voi hyödyntää sertifikaattien hallinnassa ja pohdiskella tapoja, joilla hallintaa voisi automatisoida. Työ on rajattu käsittelemään sertifikaatteja SSL/TLS-yhteyksissä.

Työn taustatietona selvitetään sertifikaatteihin ja avainten hallintaan liittyvää tietoa, kuten salauksesta sekä sertifikaattien elinkaaresta ja käytöstä SSL/TLS-yhteyksissä. Taustatiedoissa esitellään myös julkisen avaimen infrastruktuurin (PKI) pääpiirteet.

Opinnäytetyö on tutkimustyyppinen ja työn tutkimusosassa hyödynnetään olemassa olevaa tutkimustietoa. Sen pohjalta keskustellaan erilaisista sertifikaattien hallintaan liittyvistä haasteista sekä esitetään erilaisia työkaluja, joita voi hyödyntää sertifikaattien hallinnassa. Pohdiskellaan lisäksi tapoja, joilla sertifikaattien hallintaa voisi automatisoida.

Tutkimuksen keskeisimmät tulokset ovat tarve lisätä käyttäjien ja järjestelmien ylläpitäjien tietoisuutta ja osaamista, tarve automatisointiin sekä sertifikaattien voimassaoloajan rajoittaminen. Tuloksiin pohjaten on olennaista, että palvelun tai sovelluksen vastuuhenkilö ymmärtää sertifikaattien olevan yhtä lailla osa kyseistä palvelua tai sovellusta, kuin esimerkiksi palvelimet ja ohjelmistot. Tuloksissa todetaan myös manuaalisten prosessien olevan työläitä ja kalliita, joten automatisoinnille on tarvetta, mutta vain tietyssä määrin. Sertifikaattien tarve vaatii edelleen ihmisen arviointia ja validointia. Sertifikaattien voimassaoloajan lyhentämistä perustellaan sillä, että lyhyet voimassaoloajat vähentäisivät tai poistaisivat kokonaan sertifikaattien peruuttamisen tarpeen. Tämä vähentäisi vahinkoa, jota sertifikaattien tai avainten vaarantuminen aiheuttaisi. Avainten ja sertifikaattien uusimiseen liittyy kuitenkin riskejä, ja prosessi on altis inhimillisille virheille.

Tämän opinnäytetyön pohjalta voi todeta, että tietoisuutta aiheesta kaivataan ja parempia ratkaisuja automatisointiin ja integrointiin nykyisiin ympäristöihin tarvitaan.

Asiasanat
Sertifikaatti, PKI, SSL/TLS, salaus, varmenneviranomainen, digitaalinen allekirjoitus

Sisällys

1 Johdanto

Tänä päivänä tieto on meidän tärkein hyödykkeemme. Haluamme luonnollisesti pyrkiä suojaamaan tätä hyödykettä mahdollisimman hyvin. Tiedon suojaamisen tarve on tunnettu jo muinaisaikoina ja jo silloin on käytetty salausmenetelmiä. Modernit salausmenetelmät ovat kuitenkin varsin erilaisia muinaisiin menetelmiin verrattuna, ja niitä käytetään eri tavalla ja erilaisissa ympäristöissä. Suurin osa nykymaailman kommunikaatiosta tapahtuu sähköisesti internetissä. Tämän sähköisen kommunikaation suojaamiseksi tarvitsemme keinoja, jotka ovat paitsi turvallisia, myös yritysmaailmassa tehokkaita, kustannustehokkaita ja lisäarvoa tuottavia.

Kun toimimme verkossa, olipa kyse verkko-ostoksesta, mielipiteen ilmaisusta blogissa tai pelkästä selaamisesta, yksi tärkeä osa on muille näkyvä ja internetin maailmaan jäävä tieto meistä ja identiteetistämme. Tietoa on valtavia määriä ja haluamme luonnollisesti hallita tai ainakin vaikuttaa siihen, mitä tietoa meistä esiintyy. Internetissä meillä on vapaus toimia toisella kuin meidän luonnollisella identiteetillämme, voimme olla anonyymejä tai piiloutua maskin taakse. Peter Steiner kuvasi tätä ideaa hyvin The New Yorkerissa vuonna 1993 julkaistussa sarjakuvassaan. Sarjakuvan pohjalta on syntynyt suosittu ja internetissä meemiksi noussut sanonta ”Internetissä kukaan ei tiedä, että olet koira” (englanniksi ”On the Internet, nobody knows you’re a dog”). (Adams & LLoyd 2002).

Verkossa hoidetaan nykypäivänä ostoksia, veroasioita ja muuta sellaista asiointia, jossa käytämme ja välitämme arkaluontoisia tietoja itsestämme ja muista. Siksi haluamme voida luottaa siihen, että muut osapuolet ovat varmasti he, joita esittävät olevansa. Tähän tarkoitukseen on sertifikaatteja. Sertifikaatti on tietorakenne, joka sisältää tietoa muun muassa sen omistajasta, myöntäjästä, voimassaoloajasta ja käyttötarkoituksesta. Sertifikaatti on luotettavan tahon antama kiistämätön todiste siitä, että kyseinen toimija on se, joka hän esittää olevansa. (Davies 2011).

1.1 Työn tarkoitus ja rajaus

Sanalla sertifikaatti on monta eri merkitystä ja käsitteenä se on myös monelle tietotekniikka-alan ammattilaisille täysin tai ainakin osittain vieras. Tämän opinnäytetyön tutkimuksen aiheena on koota yhteen tietoa sertifikaateista käsitteenä sekä tutkia niiden elinkaareen ja hallintaan liittyviä asioita.

Opinnäytetyössä on tarkoitus tarkastella SSL/TLS-sertifikaattien elinkaarta sekä tutkia millä tavoin sertifikaatteja voi hallinnoida tehokkaasti, ylläpitäen samalla hyvää tietoturvaa niiden koko elinkaaren ajan. Tarkoituksena on lisäksi vertailla ja keskustella erilaisista menetelmistä ja työvälineistä,

joita voi hyödyntää sertifikaattien hallinnassa. Sertifikaattien hallinnoimisen tehostamiseksi pohditaan myös tapoja, joilla hallinnointia voisi automatisoida.

Opinnäytetyö on tutkimustyyppinen, sertifikaattien hallintaa ja automatisointia tutkitaan tässä työssä esittelemällä aiheeseen liittyviä tutkimuksia sekä vertailemalla ja pohdiskelemalla erilaisia työvälineitä ja ohjelmistoratkaisuja. Tutkimus toteutetaan integroivana kirjallisuuskatsauksena, eli tarkoituksena on tutkia olemassa olevaa tutkimustietoa monipuolisesti eri näkökulmista (Salminen 2011).

Digitaalisia sertifikaatteja käytetään monessa eri yhteydessä, kuten laitteilla, käyttäjillä, ohjelmistoilla ja verkkosivustoilla. Tämä opinnäytetyö on rajattu keskittymään sertifikaatteihin, joita käytetään internetissä, eli SSL/TLS-yhteyksissä. Opinnäytetyö on rajattu käsittelemään sertifikaattien hallintaa ja elinkaarta, työ ei käsittele sertifikaattien asentamista ja päivittämistä kohdeympäristöön.

1.2 Lista keskeisistä käsitteistä

Certificate authority (CA) eli varmenneviranomainen on taho, jolla on oikeus myöntää sertifikaatteja muille tahoille ja sen toimia määrää tarkat ohjeet ja toimintatavat. Varmenneviranomaisen ylin taso on juuri, ja sen sertifikaatti on **root certificate,** eli juurisertifikaatti. Varmenneviranomaisen alla voi toimia yksi tai useampi **intermediate CA,** eli välittäjävarmenneviranomainen. Tämä on käytännössä se taho, joka allekirjoittaa käyttäjien sertifikaatit. Juuritason varmenneviranomainen sekä välittäjävarmenneviranomaiset luovat yhdessä **chain of trust**in, eli varmenneketjun.

Certificate revocation list (CRL) on varmenneviranomaisen ylläpitämä lista peruutetuista sertifikaateista.

Certificate Signing Request (CSR) on sertifikaatin myöntäjälle lähetettävä sertifikaatin allekirjoituspyyntö. CSR on standardisoitu koodattu tiedosto, joka sisältää tilaajan tunnistetietoja ja avainparin julkisen avaimen. Pyyntöön tarvitaan tyypillisesti nimi (esimerkiksi www.example.com), organisaatio, maa, avaintyyppi (tyypillisesti RSA) ja avaimen pituus (vähintään 2048 bittiä).

Data Encryption Standard (DES) ja sen korvaaja **Advanced Encryption Standard (AES)** ovat salaukseen käytettäviä algoritmeja, tai englanniksi ”block cipher”.

Internet Engineering Taskforce (IETF) on vuonna 1986 perustettu järjestö, joka kehittää ja ylläpitää useita internetissä käytettäviä standardeja.

Lightweight Directory Access Protocol (LDAP) on standardoitu sovellusprotokolla, jota käytetään hakemistotietopalveluihin internetissä.

National Institute of Standards and Technology (NIST) julkaisee Federal Information Processing standardeja (FIPS) and NIST-suosituksia (julkaistaan erikoisjulkaisuina, englanniksi “special publications”), jotka määrittävät arkaluontoisten ja luokittelemattomien tietojen salaustekniikat.

PKIX on IETF:n työryhmä, jonka tehtäviin kuuluu sertifikaattien ja niiden peruutuslistojen standardityöt.

Pretty Good Privacy (PGP) tai **OpenPGP** on vaihtoehtoinen muoto sertifikaateille. PGP:n luottamusmalli on erilainen kuin X.509 sertifikaateissa, se perustuu käytännössä tunnettujen ja siten luotettujen tahojen verkostoon (”Web of trust”).

Public Key Cryptography Standards (PKCS) on joukko RSA Security LLC:n kehittämiä kryptografian standardeja. Osaa näistä on käsitelty myös IETF:n toimesta ehdotuksina virallisiksi standardeiksi. PKCS #1 määrittää RSA:n julkisen ja yksityisen avaimen matemaattiset ominaisuudet ja muodon sekä algoritmit RSA:n salaukseen, purkamiseen sekä allekirjoituksien tuottamiseen ja todentamiseen.

Public key infrastructure (PKI) eli julkisen avaimen infrastruktuuri on prosesseista, teknologioista ja käytännöistä koostuva järjestelmä, jonka avulla tietoa voi salata ja allekirjoittaa digitaalisten sertifikaattien avulla.

RSA on luultavammin maailman käytetyin julkisen avaimen algoritmi. Ronald Rivest, Adi Shamir ja Leonard Adleman keksivät RSA:n ja julkaisi sen vuonna 1978. RSA:ta voi käyttää sekä digitaalisiin allekirjoituksiin että viestien salaamiseen julkisella avaimella.

Secure Hash Algoritm (SHA) on NSA:n kehittämä tiiviste algoritmi. Kryptograafinen tiivistefunktio on menetelmä, joka muuttaa pitkän jonon bittejä tietyn pituiseksi. Tulosta kutsutaan usein sormenjäljeksi (”fingerprint”), ja sitä käytetään yleisesti myös sertifikaateissa.

Secure Socket Layer (SSL) on turvallisuusprotokolla, joka salaa käyttäjän ja sivuston välisen kommunikaation.

Transport Layer Security (TLS) on SSL:n seuraaja, eli käytännössä SSL:n versio 4.0. SSL on käsitteenä tunnetumpi, siksi siitä puhutaan edelleen. Nykyään kuitenkin TLS on käytössä oleva protokolla.

Trust store tai **root store** on selaimissa ja sovelluksissa valmiiksi asennettu lista luotettujen varmenteiden tai varmenneviranomaisten (CA) juurisertifikaateista (”root certificates”).

X.509 on standardi (RFC 5280) joka määrittää julkisen avaimen sertifikaatin muodon, sertifikaattien peruutuslistoja sekä sertifikaatin validointialgoritmin, joka sallii välittäjävarmenneviranomaisen allekirjoituksen. SSL-sertifikaattien yleisin muoto on x.509.

2 Taustatiedot

Tämän työn taustatietona selvitetään salausmenetelmiin liittyvät käsitteet. Kappaleessa selvitetään lisäksi sertifikaatin ja digitaalisen allekirjoituksen eroa sekä esitetään sertifikaatin elinkaareen ja hallinnointiin liittyvät asiat ja käsitteet. Taustatiedoissa esitetään julkisen avaimen infrastruktuurin (PKI) pääpiirteet.

2.1 Symmetrinen ja asymmetrinen salaus

Tiedon salaamisen perusteluna on halu piilottaa kommunikaation sisältöä ulkopuolisilta. Viesti muutetaan, eli salataan tietyn avaimen ja salausmenetelmän (esim. DES tai AES) avulla ja salaus puretaan takaisin selkokieleksi saman tai toisen avaimen avulla. Salaukseen voi hyödyntää joko symmetristä tai asymmetristä menetelmää. (Adams & LLoyd 2002).

Symmetrinen salaus on perinteinen salausmenetelmä, joka hyödyntää ainoastaan yhden avaimen käyttöä. Molemmat osapuolet käyttävät samaa avainta sekä tiedon salaamiseen, että sen purkamiseen. Tätä menetelmää kutsutaan myös yksityisen avaimen salaukseksi. Symmetrinen salaus on varsin yksinkertainen, mutta haasteita liittyy salaisen avaimen jakamiseen tai siitä sopimiseen, suojatun yhteyden luomiseen tai järjestelmän laajentamiseen. Koska symmetrisessä salauksessa hyödynnetään vain yhtä avainta, voi vain yksi kommunikaatiopari jakaa avaimen. Jos kommunikointiin osallistuu useampi osapuoli, täytyy jokaiselle parille luoda oma uniikki salainen avain. Mitä useampi osapuoli, sen monimutkaisempi järjestelmästä kehittyy, kun kasvava määrä avaimia pitää säilyttää ja hallinnoida turvallisesti. (Adams & LLoyd 2002; Ferguson, Schneider & Kohno 2010).

Asymmetrinen salaus kehitettiin alun perin 1970-luvulla Whitfield Diffien ja Martin Hellmanin toimesta. Asymmetrisessä salauksessa käytetään yhden avaimen sijaan julkisen ja yksityisen avaimen paria. Menetelmää kutsutaan myös julkisen avaimen salaukseksi. Julkinen avain on julkisesti saatavilla esimerkiksi julkisessa repositoriossa tai kirjastossa ja käytetään tiedon salaamiseen. Tiedon purkamiseen tarvitaan lisäksi yksityinen avain, joka on ainoastaan avainparin haltijan tiedossa. Kun kaksi osapuolta kommunikoivat, heillä on molemmilla omat avainparit. Avaimet ovat näin ollen sidottuina haltijaan, toisin kuin symmetriset avaimet, jotka ovat sidottuna kommunikaatioon. (Ferguson, Schneider & Kohno 2010; Arampatzis 18.11.2022; Adams & LLoyd 2002).

2.1.1 Salauksen algoritmit

Avaimen lisäksi salaukseen sekä sen purkamiseen tarvitaan myös algoritmi. Algoritmeja on useita, ja tässä kannattaa aina seurata Kerchkoffin periaatetta, eli salausjärjestelmän salaus on riippuvainen vain avaimen salassapidosta, ei algoritmin salassapidosta. Julkinen algoritmi on parempi kuin

salainen, sillä julkisen algoritmin heikkoudet tulevat nopeammin ja helpommin esille ja korjattavaksi. (Ferguson, Schneider, & Kohno 2010).

Tunnetut ja julkiset algoritmit ovat usein standardoituja. Internet Engineering Task Force on vuonna 1986 perustettu järjestö, joka kehittää ja ylläpitää useita internetissä käytettäviä standardeja (IETF s.a.).

RSA

RSA on aikaisimpia ja tunnetuimpia julkisen avaimen algoritmeja. Sitä voi käyttää sekä salaukseen että digitaliseen allekirjoitukseen. PKCS #1 määrittää RSA:n julkisen ja yksityisen avaimen matemaattiset ominaisuudet ja muodon sekä algoritmit RSA:n salaukseen, purkamiseen sekä allekirjoituksien tuottamiseen ja todentamiseen. Tutkimuksien mukaan RSA-avaimien tulee toistaiseksi olla vähintään 1024 bittiä pitkiä, jotta ne olisivat tarpeeksi turvallisia. (Adams & LLoyd 2002).

DH

Diffien ja Hellmanin esittämä algoritmi tunnetaan lyhenteenä DH ja on aikaisimpia julkisen avaimen algoritmeja. Algoritmi on varsin yksinkertainen, sillä sitä käytetään vain avaimen luomiseen. Idea on, että molemmilla osapuolilla on oma yksityinen avain ja he käyttävät toisen osapuolen julkista avainta määrittääkseen yhteisen symmetrisen avaimen. Tässäkin tapauksessa DH-avaimet tulee toistaiseksi olla vähintään 1024 bittiä pitkiä. (Adams & LLoyd 2002).

SHA

Tiivistemenetelmät eivät ole itsessään julkisen avaimen algoritmeja, mutta tiivistemenetelmiä käytetään aina digitaalisissa allekirjoituksissa. Kryptografinen tiivistefunktio on menetelmä, joka muuttaa pitkän jonon bittejä tietyn pituiseksi. Tulosta kutsutaan usein sormenjäljeksi (”fingerprint”), joka on yleisesti käytössä myös sertifikaateissa. Secure Hash Algorithm (SHA) on National Security Agencyn (NSA) kehittämä ja National Institute of Standards and Technologyn (NIST) standardisoima tiivistemenetelmä. Alun perin tämä kehitettiin käytettäväksi Digital Signature Algorithmin (DSA) yhteydessä mutta sitä voi käyttää myös esim. RSA:n kanssa. SHA-perheeseen kuuluu useita eri tiivistefunktioita, joita käytetään eri pituisten avainten yhteydessä. (Ferguson, Schneider & Kohno 2010; Adams & LLoyd 2002).

2.2 Digitaalinen allekirjoitus

Digitaalinen allekirjoitus vastaa idealtaan käsin kirjoitettua allekirjoitusta ja perustuu asymmetriseen avainpariin. Julkinen avain on julkisesti saatavilla. Digitaalisen allekirjoituksen avulla eri tahot voivat tarvittaessa varmistaa avaimen omistajan identiteetin sekä todentaa, että allekirjoitus on kyseisen haltijan luoma. Avainparin omistajalla on hallussaan yksityinen avain, jonka avulla hän luo digitaalisen allekirjoituksen. (Adams & LLoyd 2002).

Digitaalisen allekirjoituksen prosessi tapahtuu kahdessa vaiheessa. Ensin viesti tai tieto tiivistetään tiivistealgoritmin, esimerkiksi SHA:n avulla tietyn pituiseksi, sen jälkeen tiivistearvo allekirjoitetaan ja salataan yksityisellä avaimella. Vastaanottaja verifioi allekirjoituksen laskemalla tiivisteen samoista tavuista, purkamalla salauksen lähettäjän julkisella avaimella ja vertaamalla tuloksia. Tulosten täsmätessä vastaanottajalle varmistuu, että lähettäjä on se, jota hän esittää olevansa. (Davies 2011). Digitaalisella allekirjoituksella todetaan tiedon alkuperä sekä varmistetaan että tieto on eheä, eli sitä ei ole luomisen jälkeen muutettu. (Adams & LLoyd 2002; Davies 2011).

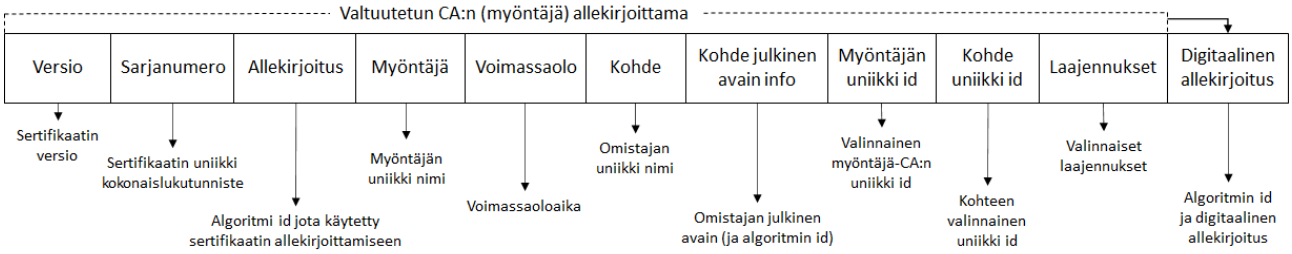
2.3 Sertifikaatti

Loren Kohnfelder esitti ensimmäisenä allekirjoitetun tietorakenteen tai sertifikaatin konseptin julkisen avaimen välittämisessä vuonna 1978. Tämä osoittautui turvalliseksi ja skaalautuvaksi tavaksi välittää julkisia avaimia. Julkisen avaimen sertifikaatin avulla sidotaan tietyn tahon nimi ja mahdollisesti myös muita ominaisuuksia yhteen tietyn julkisen avaimen kanssa. (Adams & LLoyd 2002).

Sana sertifikaatti voi olla käsitteenä monimutkainen ymmärtää. X.509-muotoisesta julkisen avaimen sertifikaatista puhuttaessa, käytetään usein sekä sanaa sertifikaatti että sanaa digitaalinen sertifikaatti. Digitaalista sertifikaattia käytetään sähköisessä muodossa olevasta sertifikaatista, mikä on hämmentävää koska suuri osa sertifikaateista ovat sähköisiä. Myös digitaalista sertifikaattia ja digitaalista allekirjoitusta sekoitetaan usein, pelkästään digitaalinen sertifikaatti ilman siihen kuuluvaa digitaalista allekirjoitusta ei käy tunnistautumiseen. Julkisen avaimen infrastruktuurin (PKI) yhteydessä käytetään usein pelkästään sanaa sertifikaatti, kun tarkoitetaan X.509-muotoista versio 3 julkisen avaimen sertifikaattia. (Adams & LLoyd 2002).

Sertifikaatteja on useita erityyppisiä ja tietyn tyypin variaatioitakin on paljon. Mahdollisesti yleisin muoto on X.509 v3, joka on standardoitu vaikkakin joidenkin mielestä turhan monimutkainen (Ferguson, Schneider & Kohno 2010). X.509 v3-sertifikaatin muoto ja ominaisuudet sekä siihen liittyvät sertifikaattien peruutuslistat ovat määritelty standardeissa RFC3280 (2002) ja RFC5280 (2008). Kuvassa 1 on kuvailtu X.509 v3-sertifikaatin rakenne. Sertifikaatin laajennusosaan voi

muun muassa lisätä kenttiä, jotka määrittävät tai rajoittavat avaimen käyttöä. (Adams & LLoyd 2002).



Kuva 1. X.509 v3 sertifikaatin rakenne (mukaillen Adams & Lloyd 2002)

Muita sertifikaattityyppejä ovat esimerkiksi Simple Public Key Infrastructure (SPKI) sertifikaatti, Pretty Good Privacy (PGP) sertifikaatti ja attribuuttisertifikaatti. (Adams & LLoyd 2002).

Yksi sertifikaattien tärkeimmistä ominaisuuksista on voimassaoloaika. Koska mitään kryptografista avainta ei tule käyttää ikuisesti, ovat myös sertifikaatit voimassa vain tietyn ajan, yleensä muutamasta kuukaudesta muutamaan vuoteen. (Ferguson, Schneider & Kohno 2010).

Toinen tärkeä ominaisuus on sertifikaattien peruuttaminen ennen voimassaoloajan päättymistä. Tämä voi olla tarpeen, jos esimerkiksi yksityinen avain on vaarantunut. Sertifikaatin käyttäjällä pitää olla jokin tapa, jolla tarkastaa sertifikaatin pätevyys, eli validoida se. Tätä varten voi hyödyntää säännöllisiä julkaisumekanismeja kuten peruutettujen sertifikaattien listoja (certificate revocation list CRL). Listat päivitetään ja julkaistaan säännöllisin väliajoin ja ovat saatavilla julkisesti esimerkiksi Lightweight Directory Access Protocol (LDAP), FTP tai http-palvelimilla. Peruutettujen sertifikaattien tietoja voidaan hakea myös reaaliaikaisten protokollien avulla kuten Online Certificate Status Protocol (OCSP) tai Lightweight Directory Access Protocol (LDAP), jolloin tiedot päivitetään ja ovat saatavilla jatkuvasti ilman viivettä. (Ferguson, Schneider & Kohno 2010; Adams & LLoyd 2002).

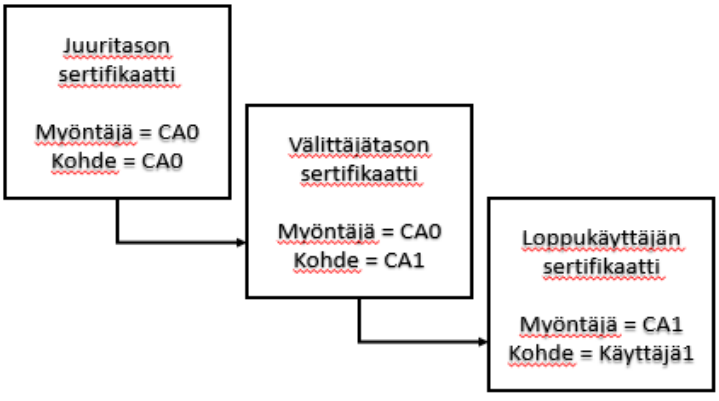
Sertifikaatit pitää säilyttää paikassa, josta osapuolet voivat turvallisesti hakea tai noutaa tarvitsemansa tiedot. Diffie ja Hellman esittivät alun perin idean vastaavien tietojen julkaisemisesta samaan tapaan kuin vaikkapa puhelinluettelo aikoinaan. Tämän päivän vastaava media on niin sanottu repositorio, eli jonkinlainen keskustietokanta. Tällaisia on olemassa erilaisia ratkaisuja, kuten esim. X.500, LDAP, web-palvelimia, FTP-palvelimia, DNS, tietokantoja yms. Näistä suosittu vaihtoehto on tietokanta, johon kommunikoidaan Lightweigt Directory Access Protocolin (LDAP) avulla. Sertifikaattitietoja ei kuitenkaan usein haluta säilyttää täysin julkisina, sillä vaikka sertifikaatin eheys on turvattu varmenneviranomaisen allekirjoituksella, muut turvallisuusseikat on otettava huomioon. Tästä syystä ratkaisuun vaaditaan myös pääsyn- tai valtuutustenhallintaa. (Adams & LLoyd 2002).

2.3.1 Varmenneviranomainen

Varmenneviranomainen on yleisesti ja todistetusti luotettava taho, jolla on valtuuksia sitoa avainpari ja sen omistaja yhteen. Varmenneviranomaisen valtuuksia ohjaa tarkat säännöt ja toimintatavat. Nämä määritetään muun muassa standardien sekä alan järjestöjen ja organisaatioiden toimesta. Varmenneviranomainen todentaa tietyn avaimen omistajan identiteetin julkisen avaimen sertifikaatin avulla. Varmenneviranomainen allekirjoittaa digitaalisesti omalla yksityisellä avaimellaan tietorakenteen, joka sisältää tietoa julkisesta avaimesta ja sen omistajan identiteetistä. (Adams & LLoyd 2002).

Sertifikaatteja on helppo saada tai teettä itse, joten käyttäjä ei välttämättä tiedä onko sertifikaatin myöntänyt taho on luotettava. Kaikki riippuu varmenneviranomaisen luotettavuudesta. Mikään varmenneviranomainen ei voi ikinä olla luotettavin ja yksi ylitse muiden. (Ferguson, Schneider & Kohno 2010).

Varmenneviranomaisia on eri tasoisia, ja eri tasojen varmenneviranomaiset muodostavat hierarkian tai ketjun. Ketju yhdistää sertifikaatin varmenneviranomaisen juureen. Sertifikaatin hierarkia voi teoriassa sisältää kuinka monta tasoa tahansa, mutta yleisesti käytetään yhtä välitasoa tai välittäjää. Hierarkia toimii käytännössä siten, että juuressa oleva taso luottaa välittäjään, joka myöntää sertifikaatin loppukäyttäjälle. Hierarkia mahdollistaa joustavamman toiminnan ja minimoi riskejä, siltä varalta, että yhden välittäjävarmenneviranomaisen luotettavuus vaarantuisi. Välittäjävarmenneviranomaisen sertifikaatissa on yleensä rajoitettu minkälaisia sertifikaatteja taho voi myöntää. (Ferguson, Schneider & Kohno 2010).



Kuva 2. Luottamusketju (mukaillen Arampatzis 31.10.2022)

Sertifikaatin hierarkiaa tai ketjua kutsutaan myös luottamusketjuksi, joka kertoo eri tasoisten sertifikaattien luotettavuudesta. Ylin taso on varmenneviranomaisen juuri, eli itse allekirjoitettu sertifikaatti, jonka luotettavuus on tästä syystä erittäin tärkeä. Luottamusketjussa ylimpänä tasolla

juuritason varmenneviranomainen allekirjoittaa välittäjävarmenneviranomaisen sertifikaatin. Tämän jälkeen välittäjävarmenneviranomainen allekirjoittaa seuraavan tason välittäjävarmenneviranomaisen sertifikaatin tai loppukäyttäjän sertifikaatin. (Arampatzis 31.10.2022).

PKI:n tärkein avain on juuritason avain, joka on niin sanottu ”masterkey” ja sitä säilytetään turvallisesti ja offline-tilassa. Juuriavainta käyttää ainoastaan juuritason varmenneviranomainen, allekirjoittaakseen oman juurisertifikaattinsa tai välittäjävarmenneviranomaisen sertifikaatin. Mikäli juuriavain vaarantuu, koko PKI vaarantuu. Myös juuriavainta ja juurisertifikaattia pitää päivittää säännöllisesti, joskaan ei yhtä usein kuin loppukäyttäjän avainta ja sertifikaattia. Juurisertifikaatti päivitetään allekirjoittamalla uusi sertifikaatti vanhalla juuriavaimella. Tämän jälkeen kaikki juurisertifikaatin alla olevat sertifikaatit pitää myös päivittää. (Ferguson, Schneider & Kohno 2010).

Varmenneviranomaisen alaisuudessa toimii rekisteröintiviranomainen, varmenneviranomaisen valtuuttama taho, joka vastaanottaa, kerää ja validoi käyttäjien tunnistetietoja varmenneviranomaisen puolesta. Näitä toimintoja pidetään turvallisuussyistä erillään toisistaan ja on tärkeätä erotella, että rekisteröintiviranomainen huolehtii tunnistautumisesta ja varmenneviranomainen sertifikaattien myöntämisestä. (Viegas & Kuyucu 2022; Adams & LLoyd 2002).

2.3.2 Avaimen ja sertifikaatin elinkaari

Avaimen elinkaaressa on useita vaiheita, mutta kaikki avaimet eivät käy läpi kaikkia vaiheita. Ensimmäisessä vaiheessa luodaan julkisen ja yksityisen avaimen avainpari. Tähän käytetään avaingeneraattoria, tai tilataan avainpari varmenneviranomaiselta. (Ferguson, Schneider & Kohno 2010). Avainparin generointi on tärkeää ja sen sijainnissa (paikallisesti, varmenneviranomaisella tai kolmannella osapuolella) on monta huomioonotettavaa seikkaa, kuten suorituskyky, oikeudelliset seikat sekä avaimen käyttötarkoitus (Adams & LLoyd 2002).

Seuraavaksi julkinen avain viedään turvallisesti varmenneviranomaiselle, joka myöntää sille sertifikaatin, eli todentaa avaimen haltijan luotettavuuden digitaalisen allekirjoituksen avulla. Varmenneviranomainen määrittää samalla mitkä oikeudet avaimella on, eli minkä tyyppinen sertifikaatti on kyseessä. Yksityiselle avaimelle tulee löytää turvallinen säilytyspaikka ja -tapa, kuitenkin siten, että avain on tarvittaessa helposti saatavilla, jos ja kun avainta pitää päivittää tai peruuttaa. Sertifioitu julkinen avain jaetaan tarvittaville osapuolille ja avainta käytetään aktiivisesti kommunikointiin. Myös julkinen avain tarvitsee turvallisen säilytyspaikan, tämän pitää kuitenkin olla julkisesti saatavilla tarvittaville osapuolille. Aktiivisen vaiheen aikana sertifikaattia käytetään, kun julkista avainta tarvitaan tiedon salaamiseen tai kun digitaalinen allekirjoitus pitää verifioida (Adams & LLoyd 2002).

Aktiivisen vaiheen jälkeen tulee passiivinen vaihe, jolloin avain on vielä voimassa, mutta se ei ole enää aktiivisesti käytössä, vaan lähestyy loppuaan. Lopulta avain vanhenee eikä ole enää pätevä. Tämä voi johtua joko sertifikaatin vanhenemisesta tai sen peruuttamisesta. Kun avain peruutetaan asianmukaisesti, se päätyy sertifikaattien peruutuslistalle. (Ferguson, Schneider & Kohno 2010; Arampatzis 18.11.2022)

Avaimen elinkaareen kuuluu myös varmuuskopiointi ja palautus. On mahdollista, että avainta käytetään sellaisen tiedon salaamiseen, joka on avaimen kadotessa saavuttamattomissa. Avainten varmuuskopiointi joko paikallisesti, varmenneviranomaisella tai kolmannella osapuolella voi silloin olla ajankohtaista. Avaimen palautusmahdollisuus pitää myös huomioida. (Adams & LLoyd 2002).

Sertifikaateille on asetettu tietty voimassaoloaika ja kun ne lähenevät vanhenemista, voi uusiminen tai päivittäminen olla tarpeen. Sertifikaatin uusiminen on saman julkisen avaimen liittäminen uuteen sertifikaattiin, päivittäminen taas on uuden avainparin luominen ja liittäminen uuteen sertifikaattiin. Jos sertifikaattia päivitetään, tämä on syytä tehdä hyvissä ajoin ennen edellisen sertifikaatin vanhenemista, jotta kaikki osapuolet ehtivät saada ja päivittää uudet tiedot. Sertifikaatin uusiminen voi olla hyödyllistä silloin kun alkuperäisen sertifikaatin tiedot ovat edelleen voimassa ja alkuperäistä avainparia pidetään edelleen kryptografisesti vahvana. (Adams & LLoyd 2002).

Sekä avaimen että sertifikaatin elinkaari loppuu joko sertifikaatin vanhenemisen myötä tai sertifikaatin peruuttamisella. Vanhentuneet avainmateriaalit voidaan säilyttää avainhistoriana ja tarpeen mukaan ne voidaan myös arkistoida. Avainhistoria säilytetään tyypillisesti paikallisesti ja helposti saavutettavissa siltä varalta, että on tarvetta päästä käsiksi tietoon, joka on salattu vanhentuneella avaimella. Arkisto on tyypillisesti joko varmenneviranomaisen tai kolmannen osapuolen ylläpitämä. (Adams & LLoyd 2002).

2.3.3 Sertifikaatin allekirjoituspyyntö

Sertifikaatin voi tilata varmenneviranomaiselta luomalla allekirjoituspyyntöä. Pyyntö luodaan paikallisesti palvelimella tai laitteella, johon sertifikaattia tarvitaan. Käytännössä luodaan julkinen ja yksityinen avainpari. Käyttäjä tallentaa ja huolehtii itse yksityisestä avaimestaan ja lähettää varmenneviranomaiselle ainoastaan julkisen avaimen. CSR on standardisoitu koodattu tiedosto, joka sisältää tilaajan tunnistetietoja sekä tyypillisesti nimen (esimerkiksi www.example.com), organisaation, maan, avaintyypin (tyypillisesti RSA) ja avaimen pituuden (vähintään 2048 bittiä). Nimen voi myös merkitä asteriskillä (esimerkiksi *.example.com), jolloin kyseessä on ”wildcard” sertifikaatti, eli sitä voi käyttää eri palveluihin, jotka kuuluvat saman verkkotunnuksen alle. (DigiCert, Inc. 2022a).

Sertifikaatin pyynnön luomiseen voi hyödyntää myös sertifikaattien hallintaohjelmistoa tai palvelua, kuten Venafi TLS Protect, AWS Certificate Manager, AppviewX CERT+, Keyfactor Command tai DigiCertin CertCentral (Gartner, Inc. 2023).

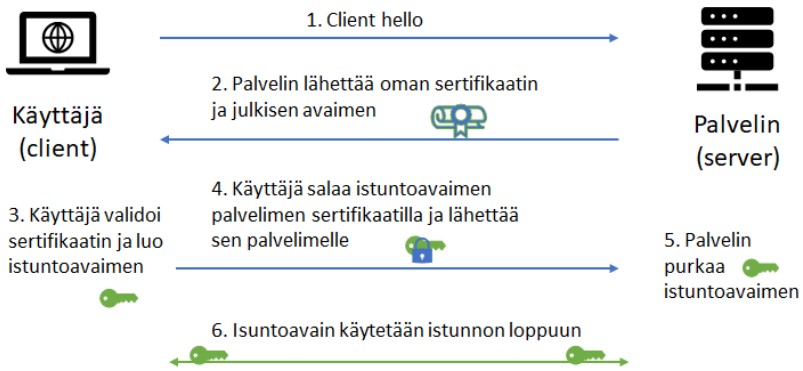
2.4 Sertifikaatteja SSL/TLS yhteyksissä

Riippumatta mitä salausmenetelmä kommunikoinnissa käyttää, esiintyy näissä yksi yhteinen ongelmakohta, eli miten tunnistaa, että kommunikoinnin toinen osapuoli on oikeasti se, jota hän esittää olevansa (Adams & LLoyd 2002). Suojatussa kommunikaatiossa on oleellista sekä salata viestit että todentaa niiden lähettäjän identiteetti. Sertifikaatin avulla voidaan suojata sekä viestin luottamuksellisuus että eheys ja lisäksi todentaa lähettäjä. (Ferguson, Schneider & Kohno 2010). Useimmat selaimet hyväksyvät ainoastaan sertifikaatteja, jotka ovat luotettavan tahon myöntämiä ja allekirjoitettuja. Verkkoselaimilla on valmiiksi asennettu lista luotettujen varmenneviranomaisten sertifikaateista. (DigiCert, Inc. 2022a).

Useimmat verkkosivustot käyttävät nykyään SSL tai TLS-turvallisuusprotokollaa. SSL eli Secure Socket Layer on Netscapen kehittämä protokolla, joka salaa käyttäjän ja sivuston välisen kommunikaation. Protokolla vaatii, että sivustolla on sertifikaatti, joka huolehtii sekä yhteyden salauksesta että todennuksesta ja luo näin suojatun yhteyden. Salaus suojaa tiedot ulkopuolisilta ja todennus varmistaa, että tieto on oikean tahon lähettämä ja eheä. TLS eli Transport Layer Security on SSL:n seuraaja, jonka Internet Engineering Taskforce IETF on standardisoinut. Vaikka TLS on oikeastaan nykyään käytössä oleva protokolla, puhutaan kuitenkin edelleen SSL:stä, sillä se on käsitteenä tunnetumpi. (DigiCert, Inc. 2022a; Ferguson, Schneider & Kohno 2010).

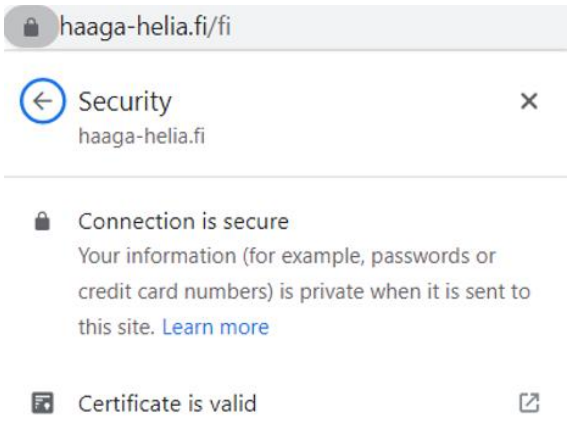
Kaksi osapuolta luo suojatun SSL/TLS yhteyden suorittamalla niin sanotun ”SSL/TLS-Handshaken”, jossa yksi osapuoli tunnistautuu lähettämällä sertifikaatin ja vastaanottaja validoi sen (Winnard, Bussche, Choi & Rossi 2016). Handshake-tapahtumassa käytetään julkista avainta, yksityistä avainta sekä istuntoavaimia. Julkista ja yksityistä avainta käytetään ainoastaan yhteyden luomisessa, jonka jälkeen symmetristä istuntoavainta käytetään kommunikaation salaamiseen. Tämä johtuu siitä, että asymmetrisen tai julkisen avaimen salausmenetelmän käyttö koko kommunikoinnin suojaamiseksi vaatii liikaa laskentatehoa ja on hidasta (Adams & LLoyd 2002). Kuva 3 näyttää käyttäjän (client) ja palvelimen (server) välisen kommunikaation. Käyttäjä lähettää ensin viestin palvelimelle aloittaakseen keskustelun. Palvelin vastaa ja tunnistautuu lähettämällä oman sertifikaatin ja julkisen avaimen. Käyttäjä validoi sertifikaatin ja jos se on luotettava, eli jos myöntäjä (CA) löytyy selaimen luotettujen varmenteiden listasta, käyttäjä hyväksyy sertifikaatin ja luo istuntoavaimen. Käyttäjä salaa istuntoavaimen palvelimen julkisella avaimella ja lähettää sen

palvelimelle. Palvelin purkaa istuntoavaimen yksityisellä avaimellaan ja aloittaa suojatun keskustelun istuntoavainta käyttäen. (Bisson 2022).



Kuva 3. SSL/TLS Handshake (mukaillen Bisson 2022)

Sivuston suojattu yhteys osoitetaan usein jonkinlaisella kuvakkeella tai värillä, kuten lukon kuvalla tai merkityllä osoiterivillä. Klikkaamalla kuvaketta selain kertoo, mikäli yhteys kyseiseen sivustoon on suojattu ja mikäli sertifikaatti on pätevä. (DigiCert, Inc. 2022a). Tästä esimerkki kuvassa 4.

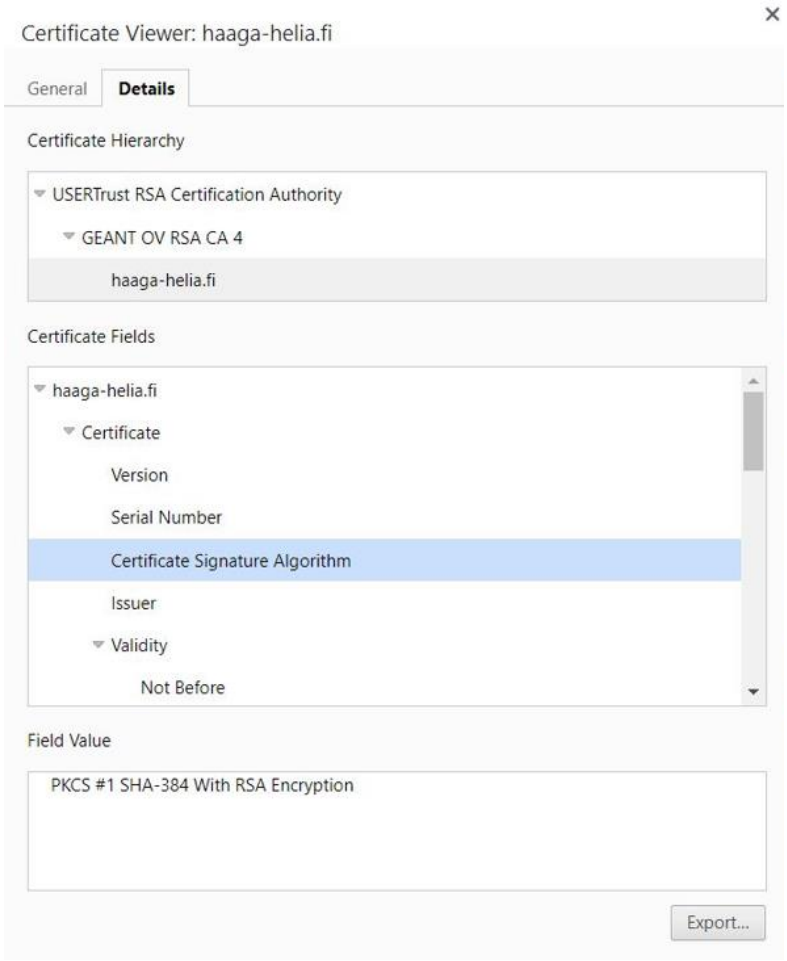


Kuva 4. Kuvakaappaus sivuston suojatusta yhteydestä (Haaga-Helia ammattikorkeakoulu Oy, s.a. 19.12.2022).

Kuvat 5 ja 6 esittävät minkälaisia tarkempia tietoja selaimen sertifikaattien katseluohjelman avulla on saatavilla Haaga-Helian ammattikorkeakoulun pääsivuston sertifikaatista.

Kuva 5. Kuvakaappaus sivuston sertifikaatin tiedoista (Haaga-Helia ammattikorkeakoulu Oy, s.a. 19.12.2022).

Kuten kuvassa 5 näkyy, sertifikaateissa on muun muassa tietoa sertifikaatin ja/tai sivuston omistajasta sekä sertifikaatin myöntäneestä tahosta ja sen voimassaoloajasta. Kuvassa 6 näkyy lisäksi tarkemmat tiedot kuten tietoa sertifikaatin salausmenetelmästä, haltijan julkinen avain, sertifikaatin mahdolliset rajoitukset ja käyttörajoitukset sekä sertifikaatin sarjanumero, jota käytetään yleisesti sertifikaatin tunnistetietona. Kuvassa 6 näkyy myös sertifikaatin myöntäjän hierarkia, tai ketju. Tässä tapauksessa juuritason varmenneviranomainen on Sertigon USERTrust RSA Certfification Authority ja välittäjänä toimii GEANT Vereniging (GEANT OV RSA CA 4).

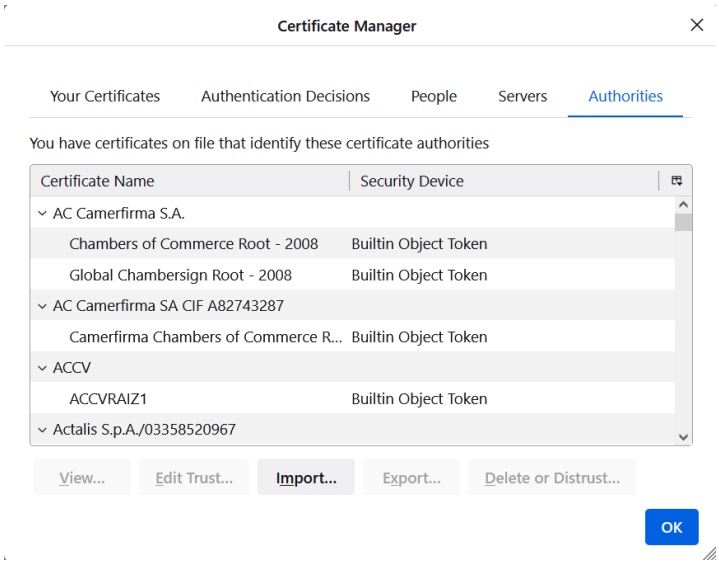


Kuva 6. Kuvakaappaus sivuston sertifikaatin lisätiedoista ja hierarkiasta (Haaga-Helia ammattikorkeakoulu Oy, s.a. 19.12.2022).

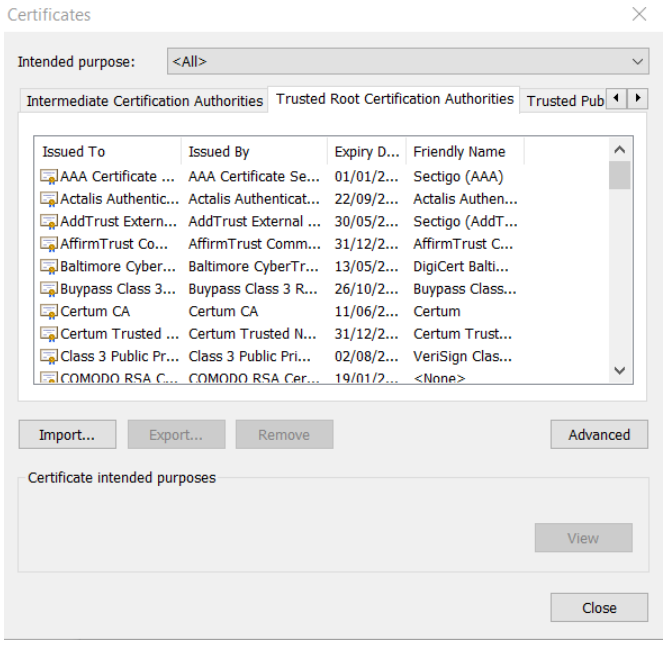
2.4.1 Luotettujen sertifikaattien lista

Verkkoselaimilla ja käyttöjärjestelmillä on valmiiksi asennettu lista luotettujen varmenneviranomaisten (CA) juurisertifikaateista, jota kutsutaan nimellä ”trust store” tai ”root store” (Arampatzis 31.10.2022).

Kuvat 7a ja 7b ovat tammikuussa 2023 otettuja kuvakaappauksia Mozilla Firefoxin ja Google Chrome-selainten tallennettujen sertifikaattien listasta ja hallintaohjelmasta. Tarkasteluhetkellä Firefoxilla oli listassaan 159 tallennettua varmenneviranomaista.



Kuva 7a. Kuvakaappaus sertifikaattien hallintaohjelmasta Mozilla Firefox selaimessa (17.1.2023, versio 110.0).



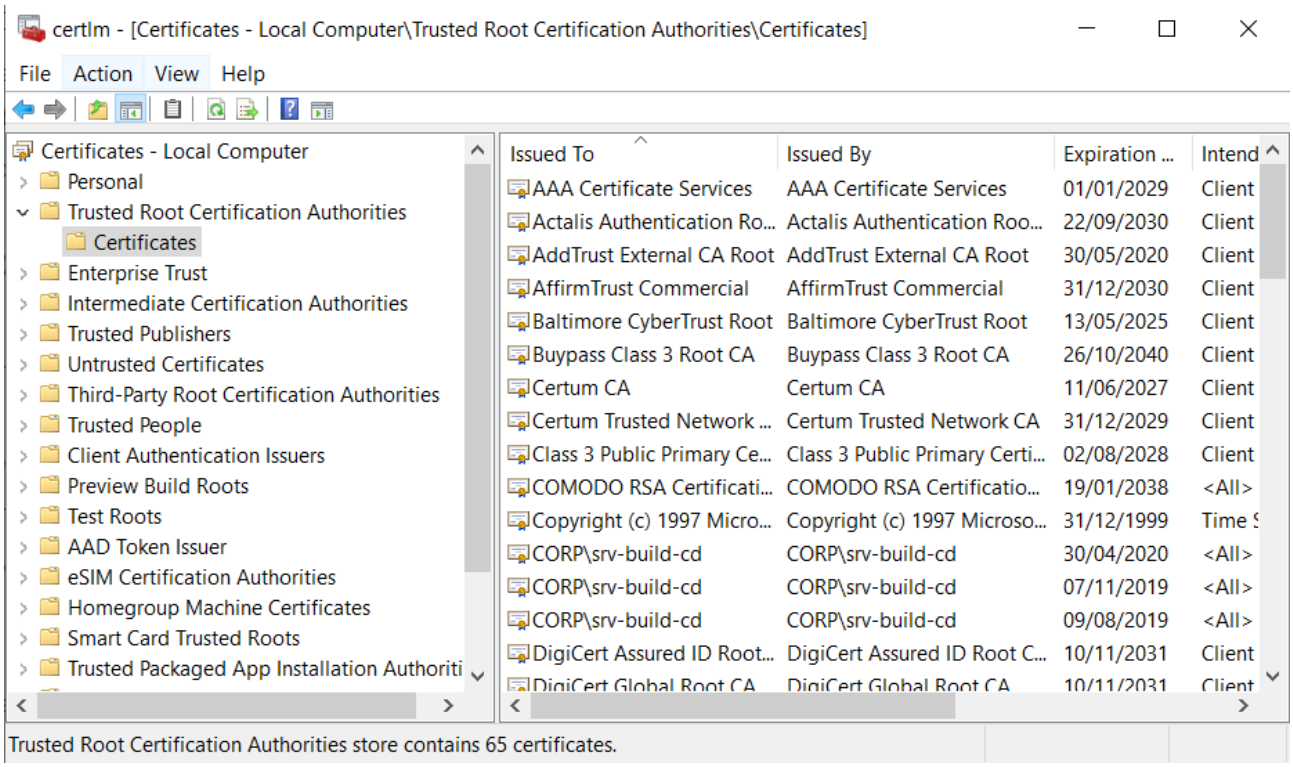
Kuva 7b. Kuvakaappaus sertifikaattien hallintaohjelmasta Google Chrome selaimessa (17.1.2023 versio 110.0.5481.178).

Luotettujen sertifikaattien listalle voi tuoda omia sertifikaatteja. Selaimeen oletusarvoisesti tallennetut sertifikaatit päivittyvät selaimen päivittämisen myötä. Tarvittaessa selaimeen voi tuoda ja tallentaa omia sertifikaatteja. Tämä voi olla tarpeen esimerkiksi organisaation sisäisessä verkossa, kun työntekijät tarvitsevat pääsyä tiettyihin verkkopalveluihin.

Jos käyttäjä hakee verkkosivua, jonka sertifikaatti ei löydy luotettujen sertifikaattien listasta, selain esittää käyttäjälle virheviestin. Virheviestien ulkonäkö vaihtelee selaimesta riippuen. Tilanne voi johtua siitä, että sertifikaatti on tuntematon tai että sertifikaatti on itse allekirjoitettu. Käyttäjä voi halutessaan jatkaa sivustolle selaimen suosituksen vastaisesti ja/tai lisätä sivuston sertifikaatin omalle luotettujen sertifikaattien listalle, jolloin virheviestiä ei jatkossa näytetä. Tämä tarkoittaa käytännössä, että käyttäjällä on loppupeleissä valtaa päättää, mikäli hän haluaa ohittaa sertifikaatin tuoman turvatoimen.

Selain saattaa myös ilmoittaa, että sivuston sertifikaatti on vanhentunut. Tämä on sivuston ylläpitäjän ongelma, ja virheilmoitus poistuu, kun ylläpitäjä päivittää sertifikaatin.

Luotettujen sertifikaattien listoja löytyy myös käyttöjärjestelmillä. Kuva 8 näyttää esimerkin Windows-käyttöjärjestelmän listan tallennetuista sertifikaateista. Listassa näkyy 65 luotettua juuritason sertifikaattia.



Kuva 8. Kuvakaappaus Windows 10-käyttöjärjestelmän tallennetuista sertifikaateista (10.2.2023).

2.4.2 Sertifikaatteja eri tarkoituksiin

On olemassa erilaisia sertifikaattityyppejä, jotka ovat luotettavuudeltaan eritasoisia sekä sopivat eri tarkoituksiin. Sertifikaatteja voi olla esimerkiksi laitteille, ohjelmistoille, käyttäjille tai verkkosivustoille. Eri varmenneviranomaiset tai eritasoiset varmenneviranomaiset myöntävät eri tarkoituksiin

käytettävät sertifikaatit. Itse allekirjoitettu sertifikaatti sopii sisäiseen kommunikaatioon, mutta se ei ole ulkopuolisille tahoille luotettava.

Verkkosivustoihin on myös olemassa eritasoisia sertifikaatteja. Domain Validated (DV) on matalan tason sertifikaatti, joka on helppo saada. Se varmistaa ainoastaan, että sertifikaatin hakija on myös kyseisen verkkotunnuksen haltija. DV-sertifikaatti sopii mille tahansa sivustolle, joka ei kerää yksityistietoa. DV-sertifikaattien haku- ja myöntämisprosessi sopii hyvin automatisointiin. Organization Validated (OV) on keskitason sertifikaatti, joka sisältää tarkemmat yritystietojen tarkistukset ja sopii yrityssivustoille tai kirjautumissivuille. Ylimmän todentamisen tason antaa Extended Validation (EV) sertifikaatti, jonka myöntämisen käsittelyssä varmistetaan yrityksen tiedot erityisen tarkasti. Sekä OV- että EV-sertifikaateissa tarkistetaan verkkotunnuksen omistaja sekä yritystiedot kuten nimi, tyyppi, status ja fyysinen osoite. EV-sertifikaateissa tarkistetaan vielä enemmän yritystietoja ja varmistetaan myös hakijan rooli yrityksessä puhelinsoiton avulla. Julkisilla verkkosivuilla suositellaan EV-sertifikaattien käyttöä. (Viegas & Kuyucu 2022; DigiCert, Inc. 2022b).

2.5 Julkisen avaimen infrastruktuuri

Public key infrastructure (PKI) eli julkisen avaimen infrastruktuuri on prosesseista, teknologioista ja käytännöistä koostuva järjestelmä. Järjestelmän avulla voi hallinnoida digitaalisia sertifikaatteja ja salauksia, jotka hyödyntävät asymmetrista salausta suojatakseen palvelimen ja käyttäjän välisen yhteyden. (Viegas & Kuyucu 2022). PKI-järjestelmän avulla on mahdollista ratkaista kryptografian vaikein ongelma, eli avainten hallinta (Ferguson, Schneider, & Kohno, 2010). PKI on yhtenäinen turvallisuusjärjestelmä, jonka avulla voi hallinnoida useiden sovellusten, laitteiden ja palvelimien julkisia avaimia. Hallinnointiin kuuluu muun muassa avainten säilyttäminen, jakaminen ja hakeminen. PKI:n päämäärä on, että avaimia käytetään, käsitellään ja ymmärretään yhtenäisellä tavalla. PKI lisää avainten hallintaan liittyvää tehokkuutta ja läpinäkyvyyttä sekä vähentää kustannuksia. (Adams & LLoyd 2002).

PKI-järjestelmän keskeiset komponentit ovat digitaaliset sertifikaatit, varmenneviranomainen sekä rekisteröintiviranomainen. Digitaalinen sertifikaatti on käyttäjien, laitteiden, verkkosivujen ja organisaatioiden sähköinen tunniste. Varmenneviranomainen on keskeisessä roolissa julkisen avaimen infrastruktuurissa, joskaan sellaista tahoa ei pienimuotoisissa PKI:ssa välttämättä tarvitakaan (Adams & LLoyd 2002). Varmenneviranomainen on taho, joka todentaa ja myöntää digitaalisia tunnisteita. Rekisteröintiviranomainen on varmenneviranomaisen valtuuttama taho, joka vastaanottaa, kerää ja validoi käyttäjien tunnistetietoja varmenneviranomaisen puolesta. (Viegas & Kuyucu 2022).

PKI:n päätehtäviin kuuluu huolehtia tiedon turvallisuudesta, eli sen todennuksesta, eheydestä ja luottamuksellisuudesta. Todentamisella varmistetaan tahon identiteetti ja PKI-järjestelmä voi identiteetin perusteella myöntää tietylle taholle tietyn roolin. Tällä roolilla saa pääsyn palveluihin ja tietoon esimerkiksi symmetrisen avaimen muodossa. Todentamisella tarkoitetaan myös tiedon alkuperän todistaminen, kun halutaan esimerkiksi selvittää mikä taho on luonut tietyn tiedon. Identiteetin todentaminen tapahtuu tyypillisesti jonkun tunnistettavan tiedon, kuten salasana tai pin, laitteiston, biometrisen tunnisteen tai toiminnan perusteella. Tiedon eheys tarkoittaa, että tieto pysyy muuttumattomana. Tietoa voi suojata sopivilla kryptografisilla algoritmeilla ja avaimilla. Luottamuksellisuus tarkoittaa, että tieto on saatavilla ainoastaan sellaiselle taholle, jolla on siihen tarvittavat valtuudet. (Adams & LLoyd 2002).

PKI-järjestelmä on erityisen hyödyllinen ja suosittu huolehtimaan niin sanotusta ”single-sign-on” (SSO) toiminnallisuudesta. SSO sallii käyttäjän tunnistautumaan useampaan sovellukseen ja verkkosivuun samoilla tunnistautumistiedoilla. Esimerkiksi sisäisissä järjestelmissä tunnistautumista tarvitsee suorittaa vain kerran. Järjestelmää voi hyödyntää myös muihin tehtäviin, kuten suojaamaan sähköposti-, verkko- (HTTPS) ja muita yhteyksiä, sähköisesti allekirjoittamaan ohjelmistokoodia ja sovelluksia, salaamaan ja purkamaan tiedostoja, kansioita ja levyjä, todentamaan älykortteja sekä laitteita verkkoon (Viegas & Kuyucu 2022).

PKI on infrastruktuuri, joka tarjoaa tavan yhdistää nimen (tahon) tiettyyn avainmateriaaliin (avainpari). PKI huolehtii ainoastaan todentamisesta, ei valtuutuksesta, siksi se on hyvä yhdistää toiseen järjestelmään tai ohjelmistoon, joka huolehtii pääsyn- ja valtuutushallinnasta. (Adams & LLoyd 2002).

PKI-järjestelmä on oleellinen osa organisaation turvallisuusinfrastruktuuria. Organisaatiot voivat implementoida oman sisäisen PKI:n hallinnoimaan laitteiden, palvelimien sekä sisäisten verkkopalveluiden sertifikaatteja. (Viegas & Kuyucu 2022).

3 Tutkimukset ja ohjelmistoratkaisut

Tässä kappaleessa esitetään työn tutkimusosuus. Tutkimus toteutetaan integroivana kirjallisuuskatsauksena, eli tarkoituksena on tutkia olemassa olevaa tutkimustietoa monipuolisesti eri näkökulmista (Salminen 2011). Tämä toteutetaan esittelemällä sertifikaattien hallintaan liittyviä tutkimuksia eri näkökulmista sekä vertailemalla ja pohdiskelemalla erilaisia työvälineitä ja ohjelmistoratkaisuja.

Ensimmäisenä esitetään NIST:in (National Institute of Standards and Technology) suosituksia avainten asianmukaisesta hallinnasta, sekä muutama avainten ja sertifikaattien hallintaan liittyvä tutkimus. Seuraavaksi esitetään muutama työkalu ja ohjelmistoratkaisu, jota voi hyödyntää sertifikaattien hallinnassa.

3.1 Parhaita käytäntöjä avainten hallinnassa

Kryptografisilla avaimilla on tärkeä rooli sertifikaattien hallinnassa. Tämän takia myös avaimia tulee hallinnoida asianmukaisella tavalla. (Barker, Barker, Burr, Polk & Smid 2012). Kryptografialla turvataan luottamuksellisuutta, eheyttä sekä todennusta algoritmista tai sovelluksesta riippumatta. Tästä syystä käyttäjillä ja järjestelmillä on oltava varmuus siitä, että avain on aito, sen omistaa se taho kenelle tai jolle sen väitetään kuuluvan eikä luvaton taho ole päässyt siihen käsiksi. (Barker & Barker 2019). Kaikkien avainten eheys on turvattava, ja salaisten sekä yksityisten avainten osalta on suojattava myös luottamuksellisuus. Avainten hallinta sisältää koko avaimen elinkaaren, eli avainten suojatun luomisen, säilyttämisen, jakamisen, käyttämisen ja tuhoamisen. Avainten hallinnan suunnittelu tulee NIST:n suositusten mukaan tehdä jo alusta alkaen kryptografisen kehitystoiminnan yhteydessä. Puutteellinen avainten hallinta voi vaarantaa vahvoja algoritmeja ja kryptografisten mekanismien virheellinen käyttö saattaa aiheuttaa suojauksen illuusion. (Barker ym. 2012).

Yksi tärkeä osa avainten hallinnassa on NIST:in suositusten mukaan avainten voimassaoloaika. Aivan kuten sertifikaateille on asetettu voimassaoloaika, myös kryptografisille avaimille tulee asettaa voimassaoloaika. Julkisen ja yksityisen avaimen voimassaoloajat voivat olla yksilöllisiä, kuten myös julkiseen avaimeen liitetty sertifikaatin voimassaoloaika voi olla yksilöllinen. NIST tarjoaa suosituksia avainten voimassaoloaikaan eri avaintyypeille ja käyttötarkoituksiin. NIST:in suosituksissa mainitaan myös avainten asianmukaisesta peruuttamisesta ja niiden käytön lopettamisesta, silloin kun avain on vaarantunut tai on syytä epäillä, että avain voi olla vaarantunut. Avainten voimassaoloajan rajoittamisella voidaan minimoida mahdollista vahinkoa, jota avainten vaarantumisesta voi aiheutua. (Barker ym. 2012).

NIST:in suosituksissa käsitellään myös avainten suojaamistapoja eri tilanteissa ja niiden vaarantumisella aiheutuvaa haittaa sekä esitellään tapoja, joilla avainten vaarantumisen haittoja voi minimoida:

- Rajoittamalla symmetristen tai yksityisten avainten selväkielisen muodon säilytyksen fyysisesti suojattuihin säilytyksiin. Estämällä ihmisten pääsyä avainten selväkieliseen muotoon sekä rajoittamalla aikaa, jonka symmetrinen tai yksityinen avain on selväkielisessä muodossa.
- Luomalla vastuullisuusjärjestelmä, joka seuraa jokaista pääsyä symmetristen ja yksityisten avainten selväkieliseen muotoon.
- Käyttämällä eheystarkastuksia varmistaakseen, että avaimen eheys tai sen yhteys muihin tietoihin ei ole vaarantunut. Avaimia voi esimerkiksi salata siten, että luvattomat muutokset havaitaan.
- Avaimen vahvistuksen käyttäminen varmistaakseen, että avain on oikeasti luotu.
- Käyttämällä luotettuja aikaleimoja allekirjoitetulle tiedolle.
- Avainten tuhoaminen heti, kun niitä ei enää tarvita.
- Luomalla palautussuunnitelma avainten vaarantumisen varalta, erityisesti jos on kyse varmenneviranomaisen vaarantumisesta. (Barker ym. 2012).

Pahimmassa tapauksessa avaimen vaarantumista ei huomata. Tätä tapahtuman haittaa voi minimoida luomalla tai hyödyntämällä hallintajärjestelmiä, jotka ovat suunniteltu minimoimaan avaimen vaarantumisesta aiheutuvaa haittaa. Yhtä avainta tulee esimerkiksi käyttää rajatusti, eli salaamaan pienen määrän kohteita mieluummin kuin suuren määrän. (Barker ym. 2012).

NIST esittää suosituksissaan kolme hyödyllistä ohjausperiaatetta ja perustelee, miten niitä voi soveltaa avainten suojaamiseksi:

Vastuullisuus – Tunnistetaan tahot, joilla on pääsy tai jotka käsittelevät kryptografisia avaimia niiden elinkaaren ajan. Vastuullisuus auttaa selvittämään milloin vaarantuminen on voinut tapahtua, ja kenellä on ollut avaimeen pääsy. Se helpottaa myös vaarantumisen jälkeistä palautumista, kun tiedetään missä ja miten avaimet ovat käytetty. Tyypillisesti käyttäytyminen on myös varovaisempia, kun tietää olevansa vastuussa asioista.

Tarkastus – Turvallisuussuunnitelma ja sitä tukevat prosessit tulee tarkastaa säännöllisesti, jotta voidaan varmistaa, että ne edelleen tukevat avainhallintapolitiikkaa. Käytettyjen suojausmekanismien kannalta tulee säännöllisesti uudelleenarvioida, että ne edelleen tarjoavat odotettua suojaa. Uudet teknologiakehitykset ja hyökkäykset tulee ottaa huomioon. Tulee lisäksi varmistaa jatkuvasti, että henkilöt, jotka käyttävät ja ylläpitävät järjestelmää edelleen noudattavat vakiintuneita turvallisuustoimia.

Selviytyminen – Kryptografisten avainten pääsyn ja jatkuvuuden turvaaminen. Tätä tukee esimerkiksi varmuuskopiot, avainten palautusmekanismit ja varautumissuunnitelman luominen ja ylläpitäminen. (Barker ym. 2012).

3.2 Sertifikaattien hallintaan liittyviä haasteita

Yksi PKI:n haasteista on sertifikaattien asianmukainen peruuttaminen. Sertifikaatteja voi peruuttaa eri syistä, esimerkiksi koska avain tai varmenneviranomainen on vaarantunut, tiedot ovat muuttuneet tai sertifikaatin tarve on lakannut. Sertifikaattien tilanteen tarkistaminen voi olla haasteellista silloin kun tieto ei ole saavutettavissa, esimerkiksi peruutettujen sertifikaattien listoista (CRL), jotka eivät ole reaaliaikaisia tai Online Certificate Status Protocolin (OCSP) osalta, jos yhteys palvelimeen puuttuu. Haasteita voi liittyä myös yksityisyyteen ja luotettavuuteen, jos peruutettujen sertifikaattien tietoja hallinnoi kolmas osapuoli. Berkowskyn ja Hayajnehin (2017) mukaan ongelman voi ratkaista lyhentämällä sertifikaattien voimassaoloaikaa, ja sertifikaattien peruuttamisesta voisi luopua jopa kokonaan, jos voimassaoloaika olisi vain muutaman päivän.

3.2.1 Sertifikaattien uusiminen Heartbleed-haavoittuvuuden yhteydessä

Vuonna 2014 suoritettiin tutkimus, jossa tutkittiin miten ja missä määrin sertifikaatteja peruutettiin ja uusittiin huhtikuussa 2014 julkaistun Heartbleed-haavoittuvuuden jälkeen. Heartbleed OpenSSL-haavoittuvuus mahdollisti yksityisten avainten havaitsemattoman vaarantumisen OpenSSL:ssä jo vuodesta 2012. Tämä ilmeni kuitenkin julkiseen tietoon vasta 7 huhtikuuta 2014. Tutkimuksessa hyödynnettiin Heartbleed-haavoittuvuuden ajankohtana tarkoituksena selvittää miten ja missä määrin palvelinten ylläpitäjät ovat ryhtyneet toimiin sertifikaattien osalta haavoittuvuuden julkaisemisen yhteydessä. Tuloksista nähtiin, että suurinta osaa haavoittuneista sertifikaateista ei ollut uusittu. Niistä verkkotunnuksista, jotka uusivat sertifikaattejaan, 60 % eivät peruuttaneet haavoittuneita sertifikaatteja ja näistä 20 % jäivät voimaan vielä kaksi vuotta tai pidempään, ellei niitä peruutettu jälkikäteen. Käytännössä tämä tarkoitti, että selaimet olivat alttiina haitallisille kolmansille osapuolille, jotka käyttivät varastettuja avaimia naamioituakseen vaarantuneeksi sivustoksi vielä pitkän aikaa haavoittuvuuden julkaisemisen jälkeen. Tutkimuksessa tehtiin myös analyysi koskien EV-sertifikaatteja, jotka oletettavasti ovat luotettavampia koska niiden myöntämisprosessi on perusteellisempi. Analyysissa todettiin, että vaikka EV-sertifikaattien osalta on parempia turvallisuuskäytäntöjä, 67 % sertifikaateista jäi uusimatta ja 88 % peruuttamatta jopa viikkoja haavoittuvuuden julkaisemisen jälkeen. (Zhang, Choffnes, Levin, Dumitras, Mislove, Schulman ja Wilson 2014).

Tutkimustuloksissa todettiin, että palvelinten ylläpitäjät reagoivat linjassa korjaustoimenpiteiden kanssa. Sertifikaattien peruutusmäärät olivat pian haavoittuvuuden julkaisemisen jälkeen jyrkästi

nousussa, jonka jälkeen ne vähenivät suhteellisen pian. Havaittavissa oli myös selvää laskua sertifikaattien peruutusmäärissä viikonloppuna. Tämä oletettavasti johtui siitä, että peruuttamisprosessiin liittyy ihmisten tekemät toimenpiteet. On kuitenkin epäselvää, johtuiko tämä palvelinten vai CRL:ien ylläpitäjistä vai molemmista, jotka eivät työskennelleet viikonloppuisin. (Zhang ym. 2014).

Tutkimuksessa havaittiin myös, että toisin kuin aikaisemmin oli oletettu sertifikaattien uusintaa ja peruuttamista ei tehty yhtäaikaisesti. Peruuttaminen tapahtui melkein aina vasta uusimisen jälkeen tai ei ollenkaan. Viivästynyttä peruuttamista selitetään tutkimuksessa sillä, että siihen liittyi manuaalisia toimenpiteitä. Tutkimus ei kuitenkaan pystynyt selittämään miksi sivusto uusisi vaarantuneen sertifikaatin ilman vanhan sertifikaatin peruuttamista. (Zhang ym. 2014).

Tutkimuksessa todetaan, että kaikilla sivustoilla esiintyi sertifikaattien hallinnan ja niiden myötä turvallisuuden parhaissa käytännöissä vakavia puutteita. Mahdollisten syiden selvittämiseen teetettiin tutkimuksessa myös pienimuotoinen kyselyn palvelinten ylläpitäjien keskuudessa. Kyselystä selvisi, että moni luotti hallittuihin palvelimiin tai automaattisiin päivityksiin ja eivätkä he näin ollen ryhtyneet erikseen toimenpiteisiin Heartbleed-haavoittuvuuden yhteydessä. Sertifikaattien uusimisen ja peruuttamisen osalta oli havaittavissa suurta eroa. Harvat sekä peruuttivat että uusivat sertifikaatit mutta he, jotka sen tekivät, tekivät sen 48 tunnin sisällä. Monet eivät peruuttaneet eivätkä uusineet sertifikaatteja ja yleinen perustelu sille oli, että haavoittuvat palvelut eivät sisältäneet arkaluontoista tietoa. Osa ei pitänyt sertifikaattien toimenpiteitä tärkeinä, koska he olivat korjanneet virheen nopeasti, vaikka haavoittuvuus oli ollut olemassa kaksi vuotta ennen sen julkistamista. Jotkut ilmoittivat, että sertifikaatti oli uusittu mutta ei peruutettu sillä se oli vain sisäiseen käyttöön. Kyselyn tulosten perusteella pääteltiin, että moni palvelinten ylläpitäjä ei ymmärrä tai arvosta sertifikaattien uusimista ja peruuttamista, ja he jotka ymmärsivät sen tärkeyden pitivät prosessia liian monimutkaisena. (Zhang ym. 2014),

Tutkimuksensa tulosten perusteella pidettiin tarpeellisena lisätä sertifikaattien hallintaan liittyvää koulutusta ja mahdollisesti enemmän avustamista varmenneviranomaisilta. PKI:n parhaiden käytänteiden osalta pidettiin hyödyllisenä automatisoida sertifikaattien peruutusprosessia. Sertifikaattien lyhyemmät voimassaoloajat lyhentäisivät ajan, jonka vaarantuneet sertifikaatit voivat olla voimassa. Menetelmät, jotka mahdollistaisivat sertifikaattien yhtäaikaisen uusimisen ja peruuttamisen vähentäisivät lisäksi vaarantuneiden sertifikaattien käyttöä. Viimeiseksi ylläpitäjien voisi olla hyödyllistä käyttää työkaluja, jotka validoivat käytössä olevat sertifikaatit, jotta vaarantuneet sertifikaatit eivät jäisi voimaan uusittujen rinnalle. (Zhang ym. 2014).

3.2.2 Varmenneviranomaisiin liittyvät haasteet

Varmenneviranomaiset ovat sertifikaateissa heikko lenkki. Varmenneviranomaisen vaarantumista pohtiessa, ei ole kyse siitä tapahtuuko tämä ollenkaan, vaan ennemminkin siitä, koska tämä tulee tapahtumaan. Varmenneviranomaiset ovat suosittuja hyökkäyksen kohteita ja niiden tulisi paitsi estää tietosuojaloukkauksia myös hillitä, toipua ja raportoida niistä. Luotettava varmenneviranomainen ottaa vastuun virheistään ja raportoi mahdollisista tietosuojaloukkauksista. Varmenneviranomaiset kuitenkin harvoin raportoivat asianmukaisesti tietosuojaloukkauksista, eikä laki usein myöskään velvoita heitä tekemään näin. Tyypillisesti varmenneviranomaiset irtisanovat itsensä vastuusta ja väittävät, että loppukäyttäjän tulisi manuaalisesti verifioida sertifikaatin tiedot. (Berkowsky & Hayajneh 2017).

Yksi merkittävimmistä varmenneviranomaisiin kohdistuvista tietosuojaloukkauksista on hollantilaisen varmenneviranomaisen Diginotarin tapaus vuodelta 2011. Diginotar joutui iranilaisten hakkereiden tekemän tietosuojaloukkauksen uhriksi, jota se kuitenkin yritti peittää kahden kuukauden ajan. Tapaus tuli julkisuuteen, kun iranilainen internetkäyttäjä julkaisi sertifikaatin virheviestiin liittyvän kysymyksen julkisella keskustelupalstalla. Tämä aloitti tutkimuksen, joka paljasti satoja virheellisesti myönnettyjä sertifikaatteja ja lisäksi useita turvallisuuspuutteita Diginotarin toimissa. Ohjelmistot ja järjestelmät olivat usein paikkaamattomia, niistä ei pidetty riittävästi lokeja, eikä käytetty antivirusohjelmistoa. Myös kaikki sertifikaatteja myöntävät palvelimet olivat saman verkkotunnuksen alla. Tästä huolimatta Diginotar oli läpäissyt pakolliset tarkastukset. Koska Diginotarin lokitus oli puutteellista, tutkijoilla oli vaikeuksia selvittää tietosuojaloukkauksen laajuutta, mutta teoriassa oli mahdollista, että mikä tahansa Diginotarin myöntämä sertifikaatti saattoi olla virheellinen. Tapaus johti siihen, että selaintoimittajat poistivat Diginotarin luotettujen sertifikaattien listoilta ja lopulta Diginotar meni konkurssiin. (Berkowsky & Hayajneh 2017; Arnbak & Eijk 2012).

Diginotarin tapaus oli aikoinaan ainutlaatuinen, mutta sen jälkeen on todettu, että varmenneviranomaiset vaarantuvat systemaattisesti. Varmenneviranomaisen poistaminen luotettujen sertifikaattien listalta on kuitenkin haasteellista. Monesta varmenneviranomaisesta ajatellaan, että ne ovat ”liian isoja kaatuakseen” koska niiden poistaminen vaikuttaisi internetviestintään maailmanlaajuisesti. Yksi esimerkki siitä on Comodon (nykyään Sectigo) tietosuojaloukkaus samoihin aikoihin Diginotarin tapauksen kanssa, jossa yhteen Comodon välittäjävarmenneviranomaiseen kohdistui myös iranilaisten hakkereiden tekemä tietosuojaloukkaus. Comodo peruutti välittömästi virheelliset sertifikaatit ja raportoi tapauksesta. Vaikka tapauksessa ei vaarantunut juuritason sertifikaatteja, tapaus vaikutti arviolta 85 000–200 000 sertifikaattiin. (Berkowsky & Hayajneh 2017; Arnbak & Eijk 2012).

Varmenneviranomaiset voivat myös itse väärinkäyttää asemaansa. Näin teki kiinalainen WoSign vuosina 2015 ja 2016. Mozilla dokumentoi 13 pientä virhettä, ei-suositeltua toimea sekä törkeää rikkomusta. Tammikuussa 2016 yhteisö ja selaintoimittajat päättivät luopua SHA-1 algoritmista, koska se ei enää täyttänyt turvallisuusvaatimuksia. WoSign päätti kuitenkin jättää suosituksen huomioimatta ja myönsi pitkäaikaisia SHA-1 sertifikaatteja sekä asetti voimassaoloaikoja takautuvasti ennen määräaikaa. Ongelmia todettiin myös WoSignin sertifikaattipyyntöjen validointiin liittyen. Tämä johti siihen, että palvelimelle, jota ei itse omistanut oli mahdollista saada sertifikaatti. Myös aliverkkotunnuksen haltija pystyi saamaan sertifikaatin perusverkkotunnukselle. Lopulta WoSign kiellettiin vuodeksi Mozillan ja Applen palveluista. (Berkowsky & Hayajneh 2017).

Varmenneviranomaisten määrä on myös ongelmallinen. On tavallista, että luotettujen sertifikaattien lista voi koostua sadoista juuritason varmenneviranomaisista ja jopa tuhansista välittäjätason varmenneviranomaisista. Koska yksikin vaarantunut tai huonosti käyttäytyvä varmenneviranomainen voi vaarantaa koko pakan, tätä haastetta kutsutaan yhdeksi epäonnistumispisteeksi (englanniksi ”single point of failure”). Yksi tapa lieventää ongelmaa on hyödyntää HTTP Public Key Pinningiä, jolloin selain säilyttää tietyn yhteyden takaaman välittäjävarmenneviranomaisen juuren välimuistissaan. Jos varmenneviranomainen muuttuu, selain hylkää sen tai ilmoittaa siitä käyttäjälle. Tätä kautta Diginotarin tapaus tuli aikoinaan julkisuuteen. (Berkowsky & Hayajneh 2017).

Tämänhetkisessä varmenneviranomaisten mallissa myös läpinäkyvyyden puute on iso ongelma. Käytännössä mikä tahansa varmenneviranomainen voi myöntää verkkosivustolle sertifikaatin ilman, että verkkotunnuksen omistaja on tästä tietoinen. (Berkowsky & Hayajneh 2017).

Lopuksi löytyy vielä ongelma luotettujen sertifikaattien listaan liittyen. Listalle on mahdollista lisätä juurisertifikaatteja, joilla on haitallisia tarkoituksia. Nämä voivat olla peräisin haittaohjelmasta tai sosiaalisesta manipuloimisesta mutta myös esimerkiksi tietokoneen valmistajilta. Tästä on esimerkkejä vuodelta 2015 kun Lenovo käytti tietokoneissaan itseallekirjoitettua sertifikaattia, jota käytettiin mainosohjelmaan. Vastaavasti samana vuonna tuli ilmi, että Dell oli asentanut kaksi sertifikaattia luotettujen sertifikaattien listaan, joita Dellin asiakaspalvelu käytti asiakkaiden avustamiseksi. Molemmissa tapauksissa nämä valmistajien asentamat sertifikaatit aiheuttivat turvallisuusriskin, sillä niiden avulla oli mahdollista suorittaa niin sanottu ”man-in-the-middle” hyökkäys. (Berkowsky & Hayajneh 2017).

Tutkijoiden mukaan suurimmat varmenneviranomaisiin liittyvät haasteet ovat valvonnan ja vastuun kantamisen puute, epäluotettavat ja turvattomat varmenneviranomaiset sekä sertifikaattien läpinäkyvyyden puute. Näiden ongelmien korjaamiseksi tehdään parhaillaan ja jatkuvasti töitä. Myös lisääntynyt koulutus aiheesta on tarpeellista. (Berkowsky & Hayajneh 2017).

3.3 Menetelmiä ja työvälineitä

Sertifikaattien ja avainten elinkaaren hallinnassa voidaan hyödyntää useita erilaisia työkaluja. Osa työkaluista on valmiiksi asennettu tietyn käyttöjärjestelmän tai ohjelmiston yhteydessä ja osa on kaupallisia ja/tai itsenäisiä ohjelmistoja. Valmiiksi paketiksi räätälöityjä ratkaisuja ja ohjelmistoja hyödynnetään usein (Kortelainen 2018).

3.3.1 Microsoftin sertifikaattipalvelut

Windows Server-käyttöjärjestelmiin kuuluu sertifikaattipalvelu, joka hakee ja vastaanottaa uusia digitaalisia sertifikaatteja. Palvelun avulla ylläpitäjä voi lisätä elementtejä sertifikaattien peruutuslistalle sekä julkaista allekirjoitettuja peruutuslistoja. Sertifikaattipalvelun avulla yritys voi hallinnoida sisäistä sertifikaattien myöntämistä, uusintaa ja peruuttamista. Palvelu tukee muun muassa aktiivihakemiston (Active Directory Certificate Service ADCS) käyttöä ja varmenneviranomaisen hierarkiaa. (Microsoft 1.7.2021).

Monet yritykset toimivat Windows ympäristössä, joten Windowsiin perustuva PKI järjestelmä on usein kätevä ja integroituu helposti olemassa olevaan infrastruktuuriin. Windows palvelimet toimivat PKI järjestelmän varmenneviranomaisina ja Internet Information Services (IIS) verkkopalvelimia voi hyödyntää rekisteröintiviranomaisina, joiden avulla sertifikaattien jakelua eri laitteisiin ja palveluihin voi automatisoida. IIS palvelin voi myös kerätä käyttäjien identtiteettitietoja joita verifioidaan aktiivihakemiston kautta. (Fernbach & Kastner 2012).

Microsoftin sertifikaattien hallintatyökalu Certmgr.exe on komentorivin apuohjelma ja Certmgr.msc on Microsoft Management Consolen (MMC) laajennus. Hallintatyökalun avulla voi hallinnoida käyttäjien ja koneiden sertifikaatteja, luotettujen sertifikaattien listoja sekä sertifikaattien peruutuslistoja. Sertifikaattien hallintatyökalu asennetaan automaattisesti Visual Studion kanssa. (Microsoft 15.9.2021).

3.3.2 OpenSSL

OpenSSL on avoimen lähdekoodin kryptografinen kirjasto. Se on kirjoitettu C-kielellä ja toimii UNIX ja Windows käyttöjärjestelmien kanssa. Tämän lisäksi OpenSSL tarjoaa useita komentorivityökaluja, joita voidaan käyttää yleisiin PKI toimintoihin sekä TLS testauksiin. Komentorivityökalut vaativat, että työkalupakki on asennettu ympäristön kaikkiin laitteisiin. (Fernbach & Kastner 2012). Komentorivityökaluja voi myös hyödyntää avainten ja sertifikaattien hallintaan. OpenSSL:n toimintoja voi hyödyntää esimerkiksi omana yksityisenä varmenneviranomaisena. (Ristić 2022).

Monet käyttäjät hyödyntävät OpenSSL:ä määrittämään ja pyörittämään verkkopalvelinta, joka tukee SSL:ä. Prosessi koostuu kolmesta vaiheesta:

1. Yksityisen avaimen luonti
2. Sertifikaatin allekirjoituspyynnön luonti ja sen lähettäminen varmenneviranomaiselle
3. Varmenneviranomaisen myöntämän sertifikaatin asentaminen verkkopalvelimelle (Ristić, 2022).

OpenSSL:n PKI-toiminnallisuudet ovat lähinnä manuaalisia ja näin ollen sopivia pienissä ympäristöissä. Isompiin projekteihin toiminnallisuudet voidaan skriptata, jolloin on mahdollista saavuttaa automaatiomaista hallinnointia. (Fernbach & Kastner 2012).

3.3.3 KeyStore Explorer

KeyStore Explorer on avoimen lähdekoodin graafinen käyttöliittymä, joka korvaa Javan komentorivin ohjelmia ”keytool” ja ”jarsinger” (Kramer 2013-2022). Jarsinger-työkalu käyttää avainsäilöstä (keystore) saatuja avain- ja sertifikaattitietoja Java Archive (JAR) -tiedostojen digitaalisten allekirjoitusten luomiseen. Keystore on yksityisistä avaimista ja niiden x.509 sertifikaattiketjuista koostuva tietokanta. Keytool-komentoa käytetään avainsäilöjen luomiseen ja hallintaan. (Oracle 2020). Keytoolin avulla voi muun muassa luoda avainpareja ja itseallekirjoitettuja sertifikaatteja, luoda CSR:iä sekä tarkastaa, tuoda ja viedä sertifikaattitiedostoja. (Fernbach & Kastner 2012).

KeyStore Explorerin avulla voi muun muassa luoda, importoida ja/tai exportoida avainpareja, muuttaa salasanoja, luoda CSR sekä tuoda, viedä, tarkastaa ja validoida sertifikaatteja. KeyStore Explorerin avulla voi lisäksi luoda digitaalisia allekirjoituksia Java sovelluksiin, JSON Web Tokeneihin, sertifikaatteihin ja CRL:iin sekä hallinnoida eri avainsäilöjen, avainparien ja sertifikaattien muotoja. (Kramer 2013-2022).

3.3.4 Kaupallisia työkaluja

Tähän alalukuun on poimittu tietoja viiden kaupallisen ohjelmiston keskeisimmistä ominaisuuksista. Valinta perustuu käyttäjäarviointien avulla tehtyyn luokitteluun viiden suosituimman PKI:n ja sertifikaattien hallintaohjelmistoon. (Gartner, Inc. 2023).

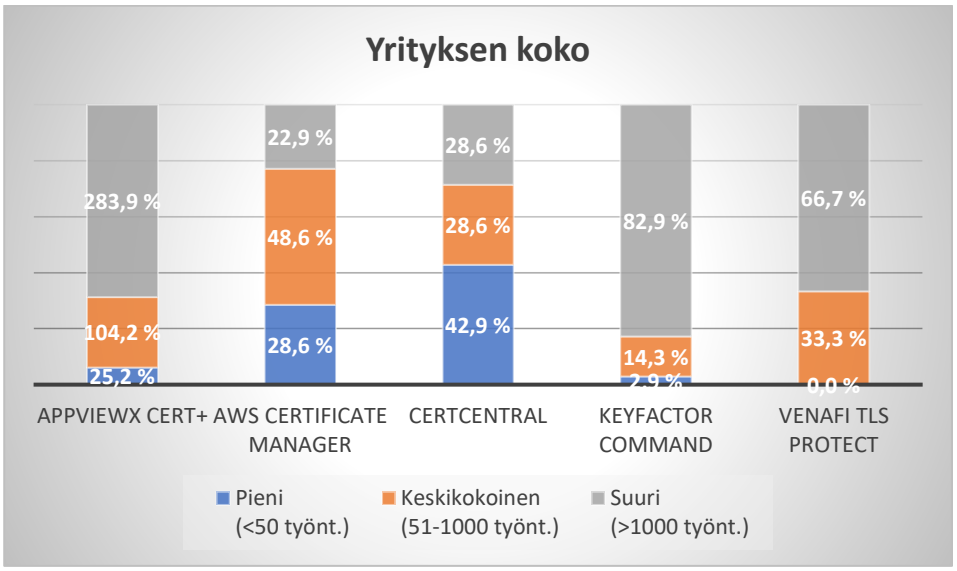
	AppviewX CERT+	AWS Certificate Manager	CertCentral	Keyfactor Command	Venafi TLS Protect
Kokonaisluokitus	**4.6** **94% suosittelee**	**4.3** **84% suosittelee**	**4.2** **83% suosittelee**	**4.6** **96% suosittelee**	**5** **100% suosittelee**
Arvosteluiden määrä	36 kpl	52 kpl	23 kpl	28 kpl	100 kpl
Kokonaiskykypisteet	**4.8**	**4.5**	**4.4**	**4.7**	**4.9**
Arviointi ja sopimus	**4.8**	**4.3**	**4.4**	**4.7**	**4.9**
Hintajoustavuus	4.8	4.0	4.8	4.6	4.8
Tarpeiden ymmärrettävyys	4.7	4.5	5	4.9	4.9
Integrointi ja käyttöönotto	**4.7**	**4.4**	**4.3**	**4.9**	**4.9**
Käyttöönoton helppous	4.4	4.3	5	4.7	4.8
Käyttäjäkoulutus	4.5	4.2	4.8	4.8	4.9
Integroinnin helppous	4.5	4.2	4.8	4.6	4.8
Yhteensopivuus	4.9	3.8	4.5	4.6	4.8
Palvelu ja tuki	**4.8**	**4.5**	**4.4**	**4.9**	**4.9**
Tuen vastausaika	4.8	4.5	3.8	5	4.9
Teknisen tuen laatu	4.8	4.4	4.3	4.9	4.8
Vertaiskäyttäjäyhteisön laatu	4.6	4.3	4.5	4.8	4.8
	+ hyvä kustomointi	+ integrointi muiden AWS palveluiden kanssa	+ sisäistä ja ulkoista kurssimateriaalia	+ useita autentikointi-vaihtoehtoja	+ tuen vastausaika
	- ei riittävä dokumentaatio	- ei tue automaattista domain validointia	- ei riittävä dokumentaatio	- ei riittävä kustomointi	- ei riittävä kustomointi
	+ helppokäyttöinen	+ julkiset sertifikaatit maksuttomia	+ hyvät ohjeet käyttöönotolle	+ hallitut palvelut, ei tarvitse itse käyttää alustaa	+ integrointi muiden ohjelmistojen/tuotteiden kanssa
	- työnkulkujen rakentaminen tai muokkaaminen työläistä	- ei mahdollista käyttää muissa pilvipalveluissa tai paikallisesti	- hieman hämmentävä validointikäytäntö	- parannettavaa tukitoiminnoissa	- raskas käyttöönotto
		- ei sovi useamman alueen käyttöön	- tuen vastausaika	- epäselviä virheviestejä	

Kuva 9. Gartnerin vertailun perusteella tehty kooste keskeisimmistä elementeistä (Gartner, Inc. 2023).

Kuten käyttäjäarvioinneissa ilmenee, useimmat ohjelmistot ovat helppokäyttöisiä ja tukevat sertifikaattien hakua sekä tuontia eri ympäristöissä. Yhteinen tärkeä ominaisuus on lisäksi roolipohjainen pääsynhallinta, jolla voi määrittää kenellä on oikeus hallita minkälaisia sertifikaatteja tai mitä osia sertifikaattien elinkaaresta, esimerkiksi uusimista ja peruuttamista. (Gartner, Inc. 2023).

Kuvassa 9 esitetyt ohjelmistot tukevat sertifikaatin elinkaaren kokonaista tai osittaista automatisointia. Ohjelmistot tarjoavat lisäksi näkyvyyttä sertifikaatteihin sekä yhden klikkauksen toimintoja, esimerkiksi uusimista ja peruuttamista. Ohjelmistojen erot ovat lähinnä yksityiskohtia ja riippuvat paljon eri yritysten sekä ylläpitäjien tarpeista. Käyttäjäarviointien perusteella käyttäjät arvostavat eniten helppokäyttöisyyttä, kustomointimahdollisuuksia, integraatiota muiden järjestelmien ja ohjelmistojen kanssa sekä sujuvaa tukitoimintaa. (Gartner, Inc. 2023).

Alla oleva pylväsdiagrammi kuvaa esiteltyjen ohjelmistojen käyttöä eri kokoisissa yrityksissä. Arvot perustuvat G2:n tekemiin käyttäjäarviointeihin. (G2.com, Inc 2023).



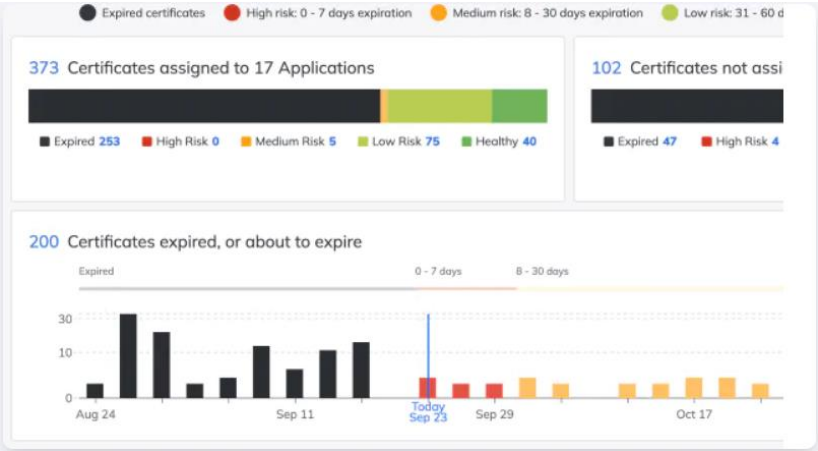
Kuva 10. Käyttäjien yritysten koko G2 käyttäjäarviointien perusteella (G2.com, Inc, 2023)

Venafi TLS Protect

Venafin TLS Protect ohjelmistoa voidaan käyttää pilvipalveluissa tai paikallisesti palvelinkeskuksessa. Ohjelmistoa voidaan käyttää joko graafisen käyttöliittymän avulla tai ohjelmistorajapintojen (API) kautta tai näiden yhdistelmänä. Kuva 12 on esimerkki TLS Protect-ohjelmiston käyttöliittymästä. (Venafi Inc., 2023).

Venafin TLS Protect on Gartnerin luokituksen mukaan suosituin ohjelmisto, ja käyttäjäarvosteluissa käyttäjät kertovat arvostavansa ohjelmiston integrointia muiden tuotteiden ja ohjelmistojen sekä varmenneviranomaisten kanssa. (Gartner, Inc. 2023).

G2:n tekemien käyttäjäarviointien mukaan vastaajien yritykset toimivat tietotekniikka ja -palvelut-alalla, rahoituspalvelualalla sekä tietokone- ja verkkoturvallisuusalalla. (G2.com, Inc 2023).



Kuva 11. Venafi TLS Protect käyttöliittymä (Venafi, Inc. 2023)

AWS Certificate Manager

Erityistä AWS Certificate Managerissa on integrointi AWS palveluiden kanssa. Integrointi on käyttäjäarvosteluiden perusteella helppoa ja sujuvaa (Gartner, Inc. 2023). AWS tarjoaa lisäksi maksuttomia julkisia sertifikaatteja, joita se hallinnoi. Sertifikaatteja voi hallinnoida hallintakonsolin, komentorivin tai ohjelmointirajapintojen (ACM API) kautta. Sertifikaattien tietoja voi tarkastaa AWS CloudTrail lokien avulla. AWS tukee kolmannen osapuolen sertifikaattien tuontia ja seurantaa, mutta sitä kautta ei ole mahdollista ladata sertifikaatteja tai hyödyntää sertifikaattipalvelua muissa pilvipalveluissa tai paikallisesti. (Amazon Web Services, Inc. 2023).

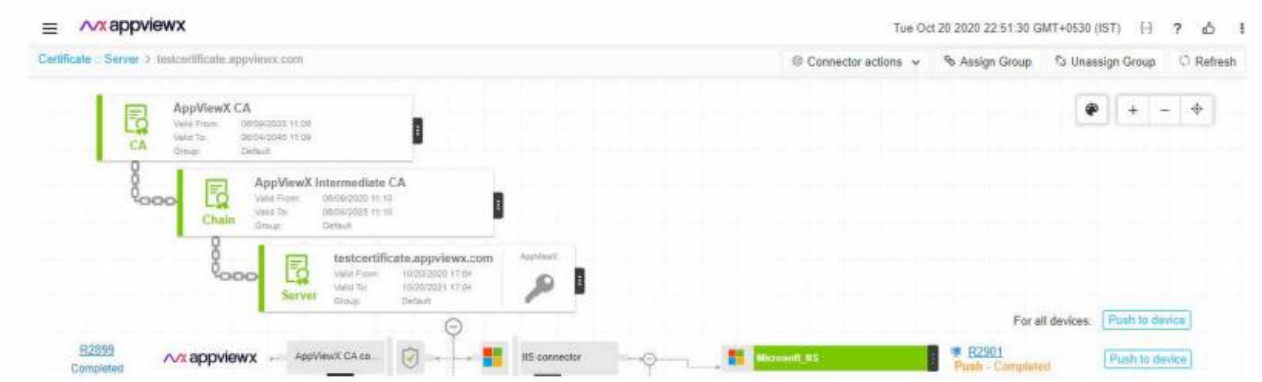
Gartnerin käyttäjäarvostelut kertovat, että käyttäjät ovat tyytyväisiä palvelun helppokäyttöisyyteen ja sujuvaan integrointiin muiden AWS palveluiden kanssa. Huonoina asioina arvosteluissa on mainittu, että palvelu ei tue automaattista verkkotunnuksen vahvistusta eikä toimintaa useimmalla alueella. (Gartner, Inc. 2023).

G2:n tekemien käyttäjäarviointien mukaan 20 % vastaajien yrityksistä toimivat tietokoneohjelmistoalalla ja 17,7 % tietotekniikka ja -palvelut-alalla (G2.com, Inc. 2023).

AppViewX CERT+

AppViewX CERT+ ohjelmistossa sertifikaattien hallinnoinnin voi automatisoida muokattavien työnkulkujen avulla. Niiden avulla voi hoitaa sertifikaatteihin liittyvät toiminnat, kuten uusinnan tai viennin laitteelle tai tallennuspaikalle joko täysin tai osittain automatisoituna. Ohjelmisto tukee API-pohjaista integraatiota muun muassa useiden varmenneviranomaisten ja pilvipalveluiden kanssa. Ohjelmistoa voi käyttää paikallisesti, pilvipalvelussa tai täysin hallinnoituna Saas-palveluna. Erityinen esille nostettu ominaisuus on sertifikaattien luottamusketjun läpinäkyvyys. (AppViewX, Inc. 2023).

Alla on esimerkki AppViewX CERT+:n luottamusketjun näkyvyydestä.



Kuva 12. AppViewX CERT+ ohjelmiston näkymä sertifikaatin varmenneketjusta (AppViewX, Inc. 2023)

G2:n tekemien käyttäjäarviointien mukaan 15,6 % vastaajien yrityksistä toimivat tietotekniikka ja -palvelut-alalla, 15,6 % toimivat pankkialalla, 9,4 % toimivat jälleenmyynnissä ja 9,4 % toimivat tietokoneohjelmistoalalla. (G2.com, Inc. 2023).

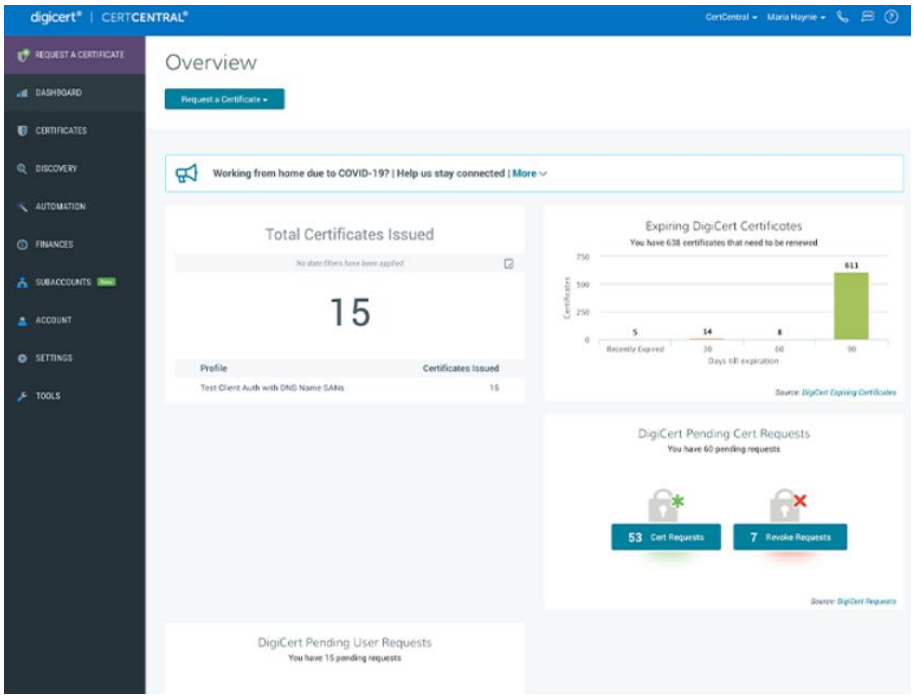
Keyfactor Command

Keyfactor Command ohjelmistoa voi käyttää itsehallinnoimana paikallisesti tai pilvipalvelussa, täysin hallinnoituna Saas-palveluna tai hybridimallina, jossa sertifikaattien elinkaaren automaatio on hallinnoituna palveluna ja PKI itsehallinnoituna. Keyfactorin erityinen ominaisuus on sertifikaattien merkintä ja looginen ryhmittely metadatan avulla. (keyfactor 2023).

G2:n tekemien käyttäjäarviointien mukaan 28,6 % vastaajien yrityksistä toimivat rahoituspalvelualalla, 14,3 % toimivat tietotekniikka ja -palvelut-alalla ja 11,4 % toimivat vakuutusalalla. (G2.com, Inc. 2023).

CertCentral

DigiCertin sertifikaattien hallintaohjelmisto CertCentral tarjoaa automatisointia sekä sertifikaattien uusimisessa että asentamisessa. Ohjelmisto tarjoaa lisäksi analyysejä muun muassa verkon kunnosta sekä haavoittuvuuksista ja heikoista konfiguraatioista. Alla on esimerkki CertCentralin käyttöliittymän näkymästä. (DigiCert, Inc. 2023).



Kuva 13. DigiCertin CertCentralin käyttöliittymä (DigiCert, Inc. 2023)

G2:n tekemien käyttäjäarviointien mukaan 28,6 % vastaajien yrityksistä toimivat tietotekniikka ja -palvelut-alalla, 10,7 % toimivat tietokoneohjelmistoalalla ja 10,7 % toimivat tietokone- ja verkkoturvallisuusalalla. (G2.com, Inc. 2023).

3.4 Automatisointi

Yrityksillä on tänä päivänä kasvava määrä laitteita, käyttäjiä ja palveluita hallittavana. Useimmat näistä vaativat sertifikaattia, mikä tarkoittaa, että myös sertifikaattien määrä kasvaa. (Callan 2021).

Avainten ja sertifikaattien hallinta on tyypillisesti manuaalista, mikä saattaa toimia hyvin pienimuotoisessa ympäristössä. Se kuitenkin skaalautuu huonosti, on altis inhimillisille virheille sekä on kallista. Keskitetyn ja skaalautuvan järjestelmän ylläpitämälle automaattinen avainten hallinnalle on tänä päivänä kysyntää. (Björkqvist, Cachin, Haas, Hu, Kurmus, Pawlitzek & Vukolic 2010).

Sertifikaattien hallinnan kannalta automatisointi on hyödyllistä paitsi manuaalisen työn vähentämiseksi, myös kustannussäästönä ja tehokkuuden lisäämiseksi. Automatisoimalla avainten ja sertifikaattien elinkaareen liittyviä toimenpiteitä ja prosesseja lisätään koko infrastruktuurin turvallisuutta. Sertifikaattien hallinta manuaalisena prosessina on työlästä ja vie paljon aikaa ja resursseja. Muun muassa Björkqvist ja kumppanit (2010) ovat todenneet, että manuaalinen prosessi on altis ihmisen tekemiin virheisiin ja tästä syystä mahdollisimman suuri osa prosessista olisi

automatisoitava. (Björkqvist ym. 2010). Myös NIST mainitsee suosituksissaan, että tarvitaan parempia työkaluja automatisoimaan avainten hallintapalveluja, jotta voidaan parantaa kryptografisten avainhallintajärjestelmien turvallisuutta, suorituskykyä ja käytettävyyttä. (Barker & Barker 2019).

Edellisessä kappaleessa esitetyt ohjelmistot sisältävät erimuotoisia ratkaisuja tai työnkulkuja sertifikaattien hallinnan automatisoimiseksi joko kokonaan tai osittain. Kokonaisvaltainen automatisointi tarkoittaa, että käytännössä sertifikaatin hallinta koko sen elinkaaren ajan on täysin automatisoitu, eikä vaadi ollenkaan manuaalisia toimenpiteitä. Tähän sisältyy myös sertifikaatin jatkuva uusiminen. Yritykset voivat vähentää hyökkäysten riskiä ja palvelukatkoksia hyödyntämällä täysin automatisoitua ratkaisua sertifikaattien hallinnoimiseen. Lisäksi yritykset pystyvät reagoimaan muuttuviin tilanteisiin nopeasti ja ketterästi, kun sertifikaattien elinkaaren hallinta on automatisoitu. (Callan 2021). Sertifikaatin koko elinkaaren hallinta on mahdollista automatisoida täysin, paitsi mahdollisen peruuttamisen osalta. Sertifikaatin peruuttaminen vaatii aina manuaalista toimenpidettä, mutta monessa ohjelmistossa peruuttaminen on pyritty tekemään todella helpoksi.

Sertifikaattien automatisoinnissa on neljä pilaria: etsiminen, käyttöönotto, elinkaaren hallinta ja uusiminen. Irrallisia sertifikaatteja ovat turvallisuusriski, joten sertifikaattien etsiminen ja kerääminen yhteen on olennainen osa yrityksen turvallisuusinfrastruktuuria. Kaupallisissa ohjelmistoissa on usein automaattinen etsintäominaisuus, joiden avulla sertifikaatteja tuodaan yhteen inventaarioon. Sertifikaatin luominen ja käyttöönotto sekä tietojen dokumentoiminen voi olla manuaalisena prosessina työläs ja aikaa vievää. Automatisoimalla tätä prosessia säästetään aikaa, vähennetään inhimilliset virheet sekä lisätään luotettavuutta ja johdonmukaisuutta. Sertifikaattien peruuttaminen ja uusiminen on sekä päivittäminen ovat elinkaaren tärkeimmät tapahtumat. Näiden toimenpiteiden sujuvoittaminen automatisoidulla ratkaisulla on olennaista ja esimerkiksi edellisessä kappaleessa esitetyissä ohjelmistoissa sertifikaatin peruuttaminen, uusiminen ja päivittäminen on mahdollista suorittaa yhdellä klikkauksella. Sertifikaatin uusiminen tai päivittäminen oikeaan aikaan on olennaista turvallisen ympäristön ylläpitämiseksi ilman katkoja. Tämän saavuttamiseksi hyödynnetään useimmiten hälytysviestejä. Hälytysviestit voivat olla sähköpostin tai ilmoitusviestin muotoisia ja niissä on tärkeää, että ne saapuvat oikeaan aikaan sekä oikeille ihmisille tai tahoille. Tämäkin tietenkin vaatii jonkinlaista hallintaa, sillä hälytysviestin vastaanottaja pitää määrittää oikein ja myös päivittää tarpeen mukaan. Monet yritykset ajattelevat, että sertifikaatin uusimisprosessi on automatisoitu, kun sen vanhenemisesta on määritelty automaattinen sähköposti ilmoitus. Sähköposti ei kuitenkaan suinkaan tarkoita, että prosessi olisi automatisoitu, sillä sähköposti vaatii reagoimista. Eniten hyötyä automatisoinnista saadaan, kun koko prosessi suoritetaan mahdollisimman vähällä manuaalisilla toimenpiteillä. Automatisointi on parhaiten onnistunut, kun kaikki neljä pilaria integroidaan yhteen hallinnointialustaan. (Callan 2021).

Automatisointia voi tällä hetkellä helpoiten toteuttaa skriptien avulla. Skriptejä voidaan hyödyntää esimerkiksi avaimen ja/tai sertifikaatin uusimis- ja CSR:n lähetysprosessissa. Kaupallisiin sertifikaattien hallintaohjelmistoihin sisältyy usein mahdollisuus hyödyntää omia tai valmiita skriptejä osana sertifikaattien hakuprosessia. Kaupallisten ohjelmistojen automatisointimekanismeista saa eniten hyötyä, kun ohjelmisto integroidaan mahdollisimman laajasti yrityksen turvallisuusinfrastruktuuriin. (Gartner, Inc. 2023).

Oleellinen osa automatisointia on avaimen tai sertifikaatin elinkaareen liittyvien prosessien tunnistaminen. Kun tunnistetaan prosessin kaavan, voidaan ryhmittää avaimet ja sertifikaatit ja toteuttaa toimenpiteitä koko ryhmittymälle kerralla. Tämä on eräänlainen automaatio, joka säästää aikaa ja manuaalista työtä. (Björkqvist ym. 2010).

4 Tulokset

Opinnäytetyön keskeisempinä tuloksina nähdään kootut taustatiedot sertifikaateista ja niiden elinkaaresta ja hallinnasta. Tutkimusosuuden pohjalta on havaittavissa tapoja, joilla sertifikaattien hallintaa voidaan tehostaa ja parantaa. Automatisointi on yksi näistä tavoista.

4.1 Tietoisuus ja koulutus

Yksi tärkeimpiä asioita, joita tämän tutkimuksen perusteella voi päätellä on, että käyttäjien ja erityisesti järjestelmien ja palveluiden ylläpitäjien tietoisuutta ja osaamista on lisättävä, näin arvioi muun muassa Berkowsky & Hayajneh (2017). Sertifikaattien hallinnassa kuten monissa muissa tietoturvallisuuteen liittyvissä aiheissa ihminen on usein heikoin lenkki. Tästä syystä olisi tärkeää minimoida ihmisen osuus toimenpiteissä. Paras tapa tähän on automatisoimalla mahdollisimman suuri osuus sertifikaatteihin liittyvistä prosesseista. Näin arvioivat Björkqvist ja kumppanit (2010) sekä Callan (2021). Sen lisäksi, että tämä vähentäisi virheiden määrä, se myös lisäisi tehokkuutta sekä vähentäisi kustannuksia. (Björkqvist ym. 2010). Toki automatisoinnin implementointi tai valmiin ohjelmiston käyttöönotto vaatii jonkin verran sekä resurssien että varojen investointia. Tämä on havaittavissa Gartnerin ja G2:n käyttäjäarviointien perusteella. Monessa arvioinnissa on mainittu raskaasta ja monimutkaisesta käytönotosta, josta on selvitty ainoastaan tukihenkilöstön avulla. (Gartner, Inc. 2023; G2.com, Inc. 2023).

Olli Kortelainen (2018) on opinnäytetyössään todennut, että paljon turhaa aikaa ja resursseja kuluu siihen, että sertifikaattien hallinnasta vastuussa olevat henkilöt joutuvat toistuvasti selittämään sertifikaatteja sekä niiden toimenpiteisiin liittyviä asioita ja prosesseja palvelujen ja sovellusten ylläpitäjille. Tämä on kuitenkin tehtävä, sillä on olennaista, että palvelun tai sovelluksen vastuuhenkilö ymmärtää, sertifikaattien olevan yhtä lailla osa sovellusta kuin esimerkiksi palvelimet ja ohjelmistot. (Kortelainen 2018). Lisäämällä työntekijöiden tietoisuutta ja ymmärrystä voidaan vähentää aikaa, jota sertifikaattien liittyien toimenpiteiden selittäminen vie.

Esitetyissä tutkimuksissa jää avoimeksi pari ongelmallista ilmiötä. Yksi näistä on sertifikaattien päällekkäisyydet. Yllättävän usein uusitaan sertifikaatti ilman, että vanha sertifikaatti peruutetaan. Tämä johtaa siihen, että palveluilla saattaa olla useita voimassaolevaa sertifikaattia, joka aiheuttaa turvallisuusriskin. Ongelmallista tässä on syy miksi näin tehdään, mikä jää tutkimuksessa epäselväksi. Ratkaisuksi kuulutetaan menetelmiä, jotka mahdollistaisivat sertifikaattien yhtäaikaisen uusimisen ja peruuttamisen sekä työkaluja, jotka validoivat käytössä olevat sertifikaatit. (Zhang ym. 2014). Toinen ratkaisematta jäävä ongelma on millä tavoin

varmenneviranomaisten toimet saataisin läpinäkyvämmäksi sekä millä tavoin saataisiin heitä kantamaan paremmin vastuuta. (Berkowsky & Hayajneh 2017).

4.2 Jatkuva uusiminen

Monet ohjelmistot ja automatisoinnin ratkaisut esittävät sertifikaattien automatisointia koko elinkaaren ajan, sisältäen myös jatkuvan uusimisen. Jatkuva uusiminen toteutetaan automaattisella ratkaisulla. Monen lähteen mielestä, esimerkiksi Callan (2021), sertifikaatin automaattisella uusimisella tai päivittämisellä voidaan minimoida manuaalisen työn määrää, mikä vähentää kustannuksia, säästää aikaa ja minimoi inhimillisten virheiden aiheuttamat haitat. Automaattisesti tapahtuvaa jatkuvaa uusimista tai päivittämistä pidetään näin ollen olennaisena sertifikaattien hallinnassa. (Callan 2021; Björkqvist ym. 2010). Kortelaisen (2018) opinnäytetyön yhteydessä tehdyssä haastattelussa esitetään kuitenkin väite, että täysin automatisoitu sertifikaattien uusimisjärjestelmä on typerä, sillä jonkun pitää arvioida, onko sertifikaatille edelleen tarvetta. Jossain vaiheessa sertifikaattien uusintaprosessia vaaditaan ihmisen tekemä validointi. Muuten on mahdollista, että jatkuva uusiminen rullaa päällä ja luo turhia jatkuvia kustannuksia, vaikka sertifikaatin tarve on jo lakannut. NIST:in (2012) suosituksissa muistutetaan myös mahdollisesta tarpeesta arvioida, onko yksityinen avain vielä riittävän turvassa, vai olisiko avaimen uusiminen ajankohtaista.

Kortelaisen (2018) opinnäytetyössä esiintyy viitteitä siitä, että sertifikaattien erääntymistä on olennaista seurata ja siihen tarvitaan parempia keinoja. Erääntymisen seurantaan hyödynnetään lähinnä hälytysviestejä, mikä tarkoittaa, että niitäkin pitää hallinnoida. Paras mahdollinen lopputulos saadan kuitenkin kun koko uusimis- tai päivittymisprosessi on automatisoitu, ja vaatii mahdollisimman vähän ihmisten tekemiä toimenpiteitä. (Callan 2021).

4.3 Sertifikaatin voimassaoloaika

Muun muassa Berkowsky & Hayajneh (2017) sekä Zhang ja kumppanit (2014) ehdottavat sertifikaattien hallinnan sujuvoittamiseksi niiden voimassaoloajan lyhentämistä vaikkapa vain muutamaan päivään. Tämä ratkaisisi monta ongelmaa esimerkiksi poistamalla sertifikaattien peruuttamisen tarpeen kokonaan ja vähentämällä tietovuotojen riskiä Heartbleed-haavoittuvuuden kaltaisissa tapauksissa. NIST:in (2012) suosituksissa perusteellaan kryptografisten avainten voimassaoloajan rajoittamista sillä, että tämä vähentäisi avaimen vaarantumisesta aiheutuvaa vahinkoa. Toisaalta avainten vaihtaminen useammin saattaisi lisätä vaarantumisen riskiä, sillä avaimen uusimisen, päivittämisen ja luomisen prosessit ovat alttiita inhmillisiin virheisiin ja

heikkouksiin. Avainten lyhyet voimassaoloajat voivat olla haitaksi varsinkin palvelunestohyökkäyksien kohdalla. Yleisesti ottaen NIST kuitenkin esittää, että kun tiedon arkaluontaisuus tai kryptografialla suojattujen kohteiden kriittisyys kasvaa, avainten voimassaoloaika tulisi pienentyä, jotta avainten vaarantumisesta aiheutuva vahinko vähentyisi. (Barker, ym. 2012).

5 Pohdinta

Tässä kappaleessa esitetään johtopäätöksiä tutkimuksiin ja tuloksiin peilaten. Johtopäätöksissä keskitytään lähinnä sertifikaattien hallinnan, uusimisen ja voimassaolon tärkeyteen sekä työkaluihin, joilla näitä prosesseja voi toteuttaa ja automatisointia tehostaa. Kappaleessa pohditaan myös opinnäytetyön oppimisprosessia ja jatkokehittämisen kohteita.

5.1 Johtopäätökset

Tutkimuksen tulosten perusteella voidaan päätellä, että yksi tärkeimmistä, jollei jopa tärkein seikka, joka vaikuttaa sertifikaattien hallinnan sujuvuuteen ja ennen kaikkea tietoturvallisuuden ylläpitämiseen on tietoisuus. Kaikkien, joilla on jotain tekemistä sertifikaattien kanssa, kuten järjestelmien ylläpitäjien, sovelluskehittäjien ja palveluiden vastuuhenkilöiden sekä tietyssä määrin myös käyttäjien tulisi ymmärtää mikä sertifikaatti on ja miten se toimii. Sertifikaattien hallintaa tulisi käsitellä osana yrityksen tietoturvallisuusinfrastruktuuria ja siten sisältyä aiheena myös tietoturvallisuuden koulutuksiin. Yksi tapa tuoda kipeästi tarvittavaa tietoisuutta sertifikaateista ja niiden tarpeista on palvelimen tai järjestelmän vastuuhenkilön osallistuminen sertifikaattien tarpeen validointiprosessiin ja uusimiseen. Jos sertifikaattien uusiminen on jatkuvaa ja sekä uusiminen että uuden sertifikaatin asennus tai käyttöönotto ovat automaattisia prosesseja, nämä jäävät helposti pyörimään itsenäisesti takahuoneessa ja unohtuvat. Kun vastaan tulee tilanne, jossa jokin avain on vaarantunut, on hyvin mahdollista ja jopa todennäköistä, että ylläpitäjät kokevat sertifikaatin peruuttamisen ja uusimisen tarpeettomana. He eivät kerta kaikkiaan ymmärrä mistä on kyse. Tässä yhteydessä on tarkoituksella käytetty sanaa ”kun” eikä ”jos”, sillä avainten vaarantuminen on väistämätöntä.

Mielestäni on hälyttävää, että tietotekniikka-alan ammattilaiset pitävät hyvänä ratkaisuna uusia sertifikaatin ilman vaarantuneen sertifikaatin peruuttamista. Tällaisen tilanteen ehkäisemiseksi tarvitaan ehdottomasti menetelmiä ja työkaluja. Toki on myös mahdollista, että tällaisia tilanteita voitaisiin välttää lisäämällä tietoisuutta ja koulutusta aiheesta.

Sertifikaattien uusimiseen sisältyy niiden erääntymisen seuranta, johon taas liittyy hälytykset erääntymisestä. Hälytykset toteutetaan useimmiten sähköposti ilmoituksen avulla. Tämä voi olla ongelmallista, sillä monelle saapuvien sähköpostien määrä on valtava ja suuri osa niistä on tarpeettomia. Tämä koskee erityisesti ohjelmistoista tai palveluista tulevia automaattisia viestejä, joita jätetään usein systemaattisesti huomiotta. Tästä syntyy ongelmatilanne, josta on mainittu Olli Kortelaisen (2018) opinnäytetyössä. Kenelle olisi järkevää osoittaa hälytys sertifikaatin erääntymisestä? Hälytys osoitetaan monesti joko taholle, joka hoitaa sertifikaattien hallinnan

prosessit tai taholle, joka ylläpitää tai on vastuussa palvelusta tai sovelluksesta, johon sertifikaattia tarvitaan. On myös mahdollista, että ilmoitukset ohjataan geneeriseen sähköpostikansioon, jota ei lueta säännöllisesti tai jolla on taipumus tulvia viesteistä, jolloin tärkeät viestit usein hukkuvat. Berkowskyn & Hayajnehin tulosten (2017) pohjalta voisi arvioida, että hälytykset tulisi osoitettava sellaiselle henkilölle jolla on riittävää ymmärrystä ja osaamista hälytyksiin reagoimiseen. Jos tämä henkilö ei ole palvelun tai sovelluksen vastuuhenkilö, hänen tulisi kuitenkin osallistua prosessiin, jotta ymmärtäisi sen tärkeyden.

Muutaman päivän voimassaolevat sertifikaatit lisäisivät huomattavasti sertifikaattien uusimisen tarvetta, joka johtaisi siihen, että manuaalinen uusinta ei olisi enää järkevää missään tilanteessa. Todennäköisesti sertifikaattien hallintaan liittyvät kustannukset myös nousisivat, sillä jokaisen sertifikaattia käyttävän tahon olisi hankittava jonkinlainen automaatio, vaikka toiminta olisi pienimuotoista. Muutaman päivän sertifikaatit lisäisivät myös tietoliikenteen määrän moninkertaiseksi, mikä on tänä päivänä erityisen huomioonotettava seikka, kun tietoliikenteen määrä joka tapauksessa nousee koko ajan. Tietoa lähetetään yhä enemmän paikasta toiseen ja tiedon odotetaan olevan koko ajan saatavilla.

Tutkimuksessa esitetyt työkalut helpottavat sertifikaattien hallintaa ja saattavat myös ratkaista monta siihen liittyvää ongelmaa. Projektille tai yritykselle ei kuitenkaan todennäköisesti löydy mitään valmista pakettiratkaisua, vaan olemassaolevia ohjelmistoja ja työkaluja pitää räätälöidä omaan tarpeeseen. Sopivan kokonaisuuden kokoamiseen ja valintaan vaikuttaa moni tekijä. Vaikuttavia tekijöitä ovat muun muassa kustannukset, vapaat resurssit sekä mahdolliset integraatiot ja yhteensopivuus olemassa olevaan infrastruktuurin ja käytettäviin sovelluksiin. Näiden tekijöiden lisäksi tulisi huomioida myös hyvää tietoturvallisuuden ylläpitämistä jatkuvasti. Tutkimusosassa kuitenkin on selkeästi havaittavissa, että sertifikaattien hallinnan tehostamiseksi olisi tärkeätä hoitaa kaikki siihen liittyvät toimenpiteet samalla alustalla. Tämän vuoksi sopivan ohjelmiston tai ratkaisun löytäminen tai itse räätälöiminen on olennaista, ja siihen kannattaa panostaa sekä resursseja että aikaa.

Voidaan todeta, että automatisoinnin lisäämistä suositellaan ja siihen kannustetaan, mutta kuitenkin vain tietyssä määrin. Vielä ei taida ainakaan olla hyödyllistä tai edes haluttua automatisoida sertifikaattien hallintaa täysin. Mielestäni tärkein asia automatisoinnin käyttöönottamisessa on sertifikaattien elinkaareen liittyvien prosessien tunnistaminen ja määrittäminen. Kun esimerkiksi uusimisen, päivittämisen tai peruuttamisen prosessit ovat selkeitä ja johdonmukaisia, myös niiden automatisoiminen onnistuu vaivatta.

Sertifikaattien määrä on kasvava, tämä on tosiasia. Tämän myötä myös sertifikaattien liittyvät toimenpiteet lisääntyvät ja yritykset tulevat tarvitsemaan yhä enemmän tehokkaita ja

kokonaisvaltaisia ratkaisuja sertifikaattien hallinnoimiseen. Kasvava määrä sertifikaatteja tarkoittaa myös, että varmenneviranomaisten määrä tai ainakin niiden rooli kasvaa. Tämän vuoksi olisi hyödyllistä lisätä varmenneviranomaisten luotettavuutta ja läpinäkyvyyttä. Tämä on kuitenkin hankalaa toteuttaa, sillä varmenneviranomaiset kuten myös monet heidän palveluitaan käyttävät yritykset ovat maailmanlaajuisia. Samat lait eivät näin ollen velvoita kaikkia osapuolia.

Covid-19 pandemian myötä verkossa tapahtuva etäasiointi on lisääntynyt merkittävästi. Samalla myös työnteko on muuttunut enemmän etäpainoitteiseksi. Tapaamisia, koulutuksia ja konferenssеja järjestetään yhä enemmän verkossa. Kun työnteko tapahtuu muualla kuin yrityksen tiloissa, myös laitteiden käyttö muuttuu. Työntekoon käytetään yhä enemmän erilaisia laitteita, kuten puhelimia ja tabletteja ja lisäksi ”bring-your-own-device”-ilmiö lisääntyy. Tämä tarkoittaa, että yksittäinen työntekijä on entistä enemmän vastuussa käyttämiensä laitteiden turvallisesta käytöstä, jolloin sertifikaattien rooli on merkittävä.

5.2 Jatkokehittäminen

Sertifikaattien hallinta ja automatisointi on laaja aihe ja tutkittavaa riittää. Se on myös aihe, joka kehittyy koko ajan sitä mukaan, kun uusia teknologioita kuten salausmenetelmiä, hyökkäystekniikoita ja ohjelmistoja kehitetään.

Tärkeä asia, joka työssä on tullut esille, on erityisesti tietoisuuden ja ymmärryksen lisääminen sekä koulutuksen tarve. Tähän peilaten näkisin kiinnostavana tutkia haastattelutyyppisesti enemmän miten nykyiset järjestelmien ylläpitäjät suhtautuvat sertifikaatteihin ja niiden elinkaaren aikana tehtäviin toimenpiteisiin. Koska sertifikaatteihin liittyvät asiat ovat oletettavasti monelle sekä tietotekniikka-alan että tavallisille käyttäjille melko epäselviä, olisi myös mielenkiintoista ja jopa hyödyllistä tutkia eritaustaisten henkilöiden suhtautumista niihin. Yksi lähtökohta voisi olla tietotekniikka-alan opiskelijat, voisi nimittäin olettaa, että heidän tulevaan työarkeen liittyy enemmin tai myöhemmin sertifikaatteihin liittyviä työtehtäviä.

Olisi lisäksi kiinnostavaa kokeilla erilaisia ohjelmistoratkaisuja käytännössä, esimerkiksi virtuaaliympäristössä. Tämä on tietenkin hyödyllistä myös siinä tilanteessa, kun on ajankohtaista valita yritykselle sopiva ratkaisu, ja täten uskoisin sen olevan erityisesti yleishyödyllistä.

5.3 Oppimisprosessi

Koen, että olen saavuttanut työni tavoitteet ja olen prosessin aikana oppinut valtavia määriä. Olen tietenkin oppinut paljon uutta ja syventänyt tietämystäni sertifikaateista, niiden elinkaaresta sekä niiden hallinnasta ja automatisoinnista. Olen lisäksi oppinut tieteellisestä kirjoittamisesta ja tiedonhausta sekä tiedon esittelemisestä.

Erityinen haaste, jonka opinnäytetyössä kohtasin, oli käsitteiden kääntäminen suomeksi. Tämä osoittautui haasteeksi osittain siitä syystä, että suomi on minulle vieras kieli ja osittain siitä syystä, että useat tietotekniikka-alan käsitteistä ei ole yleisesti suomennettu ja alalla käytetään usein työkielenä pääosin englantia. Käsitteiden suomenkielisiä termejä ei siis tunneta. Vaikka jotkut käsitteet saattavat tuntua suomeksi vierailta, koen kuitenkin, että olen onnistunut suomennoksessa varsin hyvin ja olen pyrkinyt esittämään hankalimmat käsitteet myös englanniksi, jolloin ne saattavat tuntua tutummilta.

Toinen varsin odottamaton haaste oli aiheen laajuus ja koin ajoittain hankalaksi rajoittaa kiinnostavan aiheen opinnäytetyön raameihin. Mielestäni olen siinä onnistunut, vaikka jälkikäteen pohdittuna näkisin hyödyllisenä määrittää rajaukset tarkemmin jo opinnäytetyöprosessin alussa.

Pienempi haaste oli itse tieteellinen kirjoittaminen. Varsinkin työn strukturointi kuten kappalejako ja otsikointi tuntui ajoittain haasteelliselta, ja vei huomattavasti enemmän aikaa kuin olin odottanut.

Lähteet

Adams, C.;& LLoyd, S. 2002. *Understanding PKI: Concepts, Standards, and Deployment Considerations, Second Edition.* Addison-Wesley Professional. Boston, Massachusetts, USA. E-kirja. Luettu 6.1.2023.

Amazon Web Services, Inc. 2023. *AWS Certificate Manager features*. Luettavissa: https://aws.amazon.com/certificate-manager/features/?nc=sn&loc=2. Luettu 16.2.2023.

AppViewX, Inc. 2023. *Simplify Certificate Lifecycle Management with AppViewX CERT+.* Luettavissa: https://www.appviewx.com/Collaterals/Datasheet/CERT+.pdf. Luettu 16.2.2023.

Arampatzis, A. 31.10.2022. *How Does a Browser Trust a Certificate?* Venafi blogi. Luettavissa: https://www.venafi.com/blog/how-does-browser-trust-certificate. Luettu 3.1.2023.

Arampatzis, A. 18.11.2022. *What is Encyption Key Management?* Venafi blogi. Luettavissa: https://www.venafi.com/blog/what-encryption-key-management. Luettu 3.1.2023.

Arnbak, A. M.;& Eijk, N. A. 2012. *Certificate Authority Collapse: Regulating Systemic Vulnerabilities in the HTTPS Value Chain.* 2012 TRPC. Universiteit van Amsterdam, Faculty of Law, Institute for Information Law. Luettavissa: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2031409. Luettu 6.1.2023.

Barker, E.;& Barker, W. C. 2019. *NIST Special Publication 800-57 Part 2 (Revision 1): Recommendation for Key Management: Part 2 - Best Practices for Key Management Organizations.* Information Technology Laboratory, Computer Security Division. National Insitute of Standards and Technology. Gaithersburg. Luettavissa: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt2r1.pdf. Luettu 22.2.2023.

Barker, E.;Barker, W.;Burr, W.;Polk, W.;& Smid, M. 2012. *NIST special publication 800-57: Recommendation for Key Management - Part 1: General (Revision 3).* Information Technology Laboratory, Computer Security Division. National Institute of Standards and Technology. Gaithersburg. Luettavissa: https://adgrafics.net/docs/other/sp800-57_part1_rev3_general.pdf. Luettu 19.12.2022.

Berkowsky, J. A.;& Hayajneh, T. 2017. *Security Issues with Certificate Authorities.* 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON). IEEE. New York, NY, USA. Luettavissa: https://ieeexplore.ieee.org/document/8249081/citations#citations. Luettu 19.12.2022.

Bisson, D. 15.9.2022. *What is an x.509 Digital Certificate?* Venafi blogi. Luettavissa: https://www.venafi.com/blog/what-ssltls-x509-certificate. Luettu 3.1.2023.

Björkqvist, M.;Cachin, C.;Haas, R.;Hu, X.-Y.;Kurmus, A.;Pawlitzek, R.;& Vukolic, M. 2010. *Design and Implementation of a Key-Lifecycle Management System.* In: Sion, R. (eds) Financial Cryptography and Data Security. Lecture Notes in Computer Science, vol 6052, ss. 160–174. Springer, Berlin, Heidelberg. Luettavissa: https://ifca.ai/pub/fc10/30_88.pdf. Luettu 19.12.2022.

Callan, T. 14.4.2021. *When Certificate Management Becomes Daunting, Automate It.* CPO Magazine. Luettavissa: https://www.cpomagazine.com/cyber-security/when-certificate-management-becomes-daunting-automate-it/. Luettu: 20.3.2023.

Davies, J. 2011. *Implementing SSL/TLS Using Cryptography and PKI.* Wiley. Indianapolis, Indiana, USA. E-kirja. Luettu 6.1.2023.

DigiCert, Inc. 2022a. *What is an SSL certificate?* Luettavissa: https://www.digicert.com/what-is-an-ssl-certificate. Luettu 19.12.2022.

DigiCert, Inc. 2022b. *What's the difference between DV, OV & EV SSL certificates*. Luettavissa: https://www.digicert.com/difference-between-dv-ov-and-ev-ssl-certificates. Luettu 3.1.2023.

DigiCert, Inc. 2023. *CertCentral TLS/SSL Certificate Management*. Luettavissa: https://www.digicert.com/tls-ssl/certcentral-tls-ssl-manager#features. Luettu 16.2.2023.

Ferguson, N.;Schneider, B.;& Kohno, T. 2010. *Cryptography Engineering: Design Principles and Practical Applications.* Wiley Publishing, Inc. Indianapolis, Indiana, USA.

Fernbach, A.;& Kastner, W. 2012. *Certificate management in OPC UA applications: An evaluation of different trust models.* Proceedings of 2012 IEEE 17th International Conference on Emerging Technologies & Factory Automation (ETFA 2012), pp. 1-6. Luettavissa: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6489675. Luettu 19.12.2022.

G2.com, Inc. 2023. *Best Certificate Lifecycle Management (CLM) Software* . Luettavissa: https://www.g2.com/categories/certificate-lifecycle-management-clm. Luettu 20.2.2023.

Gartner, Inc. 2023. *Public Key Infrastructure (PKI) and Certificate Lifecycle Management*. Luettavissa: https://www.gartner.com/reviews/market/public-key-infrastructure-pki-and-certificate-lifecycle-management. Luettu 3.1.2023.

Haaga-Helia ammattikorkeakoulu Oy. s.a. *Etusivu | Haaga-Helia*. Luettavissa: https://www.haaga-helia.fi/fi. Luettu 19.12.2022.

IETF | Introduction. s.a. Luettavissa: https://www.ietf.org/about/introduction/. Luettu 3.1.2023.

keyfactor. 2023. *Keyfactor Command | PKI & Machine Identity Automation*. Luettavissa: https://www.keyfactor.com/platform/keyfactor-command/. Luettu 16.2.2023.

Kortelainen, O. 2018. *Automating Certificate Enrollment For Helsinki and Uusimaa Hospital District.* AMK-opinnäytetyö. Metropolia ammattikorkeakoulu, Tietojenkäsittely. Luettavissa: https://www.theseus.fi/bitstream/handle/10024/152123/Kortelainen_Olli.pdf?sequence=4&isAllowed=y. Luettu 19.12.2022.

Kramer, K. 2013-2022. *KeyStore Explorer*. Luettavissa: https://keystore-explorer.org/features.html. Luettu 9.2.2023.

Microsoft. 1.7.2021. *Certificate Services - Win32 apps*. Luettavissa: https://learn.microsoft.com/en-us/windows/win32/seccrypto/certificate-services. Luettu 9.2.2023.

Microsoft. 15.9.2021. *Certmgr.exe (Certificate Manager Tool)*. Luettavissa: https://learn.microsoft.com/en-us/dotnet/framework/tools/certmgr-exe-certificate-manager-tool. Luettu 9.2.2023.

Oracle. 2020. *jarsinger*. Java SE Documentation. Luettavissa: https://docs.oracle.com/javase/7/docs/technotes/tools/windows/jarsigner.html. Luettu 9.2.2023.

Ristić, I. 2022. *OpenSSL Cookbook*. 3rd Edition. Feisty Duck. London. E-kirja. Luettavissa: https://www.feistyduck.com/library/openssl-cookbook/online/. Luettu 9.2.2023.

Salminen, A. 2011. *Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallinto-tieteellisiin sovelluksiin.* Vaasan yliopisto. Vaasa. Luettavissa: https://www.uwasa.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf. Luettu 20.3.2023.

Venafi, Inc. 2023. *Manage and Protect Your TLS Certificates with TLS Protect*. Luettavissa: https://venafi.com/tls-protect/. Luettu 16.2.2023.

Viegas, V.;& Kuyucu, O. 2022. *IT Security Controls: A Guide to Corporate Standards and Frameworks.* Apress. New York, NY, USA. E-kirja. Luettu 6.1.2023.

Winnard, K.;Bussche, M. v.;Choi, W.;& Rossi, D. 2016. *Managing Digital Certificates across the Enterprise.* IBM Redbooks. Armonk, NY, USA. E-kirja. Luettu 6.1.2023.

Zhang, L.;Choffnes, D.;Levin, D.;Dumitras, T.;Mislove, A.;Schulman, A.;& Wilson, C. 2014. *Analysis of SSL certificate reissues and revocations in the wake of heartbleed.* IMC '14:

Proceedings of the 2014 Conference on Internet Measurement Conference, 489–502. Luettavissa: https://dl-acm-org.ezproxy.haaga-helia.fi/doi/pdf/10.1145/2663716.2663758. Luettu 19.12.2022.