OULUN AMMATTIKORKEAKOULU

TOIMINNAN OHJAUSJÄRJESTELMÄN UUSINTA

Ja sen vaikutus palvelinvarmenteiden ylläpitoon

Niko Naumanen
Opinnäytetyö (AMK)
Syksy 2024
Tietotekniikan tutkinto-ohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietotekniikan tutkinto-ohjelma
Ohjelmistokehitys

Tekijä(t): Niko Naumanen
Opinnäytetyön otsikko: Toiminnanohjausjärjestelmän uusinta
Työn ohjaaja(t): Pekka Alaluukas
Työn valmistumislukukausi ja -vuosi: syksy 2024
Sivumäärä: 27

Tässä työssä käsitellään toiminnanohjausjärjestelmän vaikutusta palvelinvarmenteiden ylläpitoon ja hallintaan. Työssä ei ole mainittu yrityksen nimeä, jossa työn laatija työskentelee. Nimettömäksi on myös jätetty konsulttiyritys, joka vastasi järjestelmän muutostyöstä. Päätös jättää yritykset nimettömäksi johtuu siitä, että työ voi olla mahdollisimman puolueeton kokonaisuus.

Yritys, jossa tämä työ on tehty, siirtyi toiminnanohjausjärjestelmästä nimeltä Efecte uuteen ServiceNow-järjestelmään. Järjestelmän vaihdoksen yhteydessä ilmeni suuria puutteita datassa, joka oli siirretty järjestelmien välillä. Tämän datan puuttumisesta johtui monen palvelinvarmennekortin puuttuminen uudesta järjestelmästä. Siirtyneissä korteissa oli myös puutteita vastuuhenkilöiden osalta, mikä johti siihen, ettei varmenteita saatu uusittua ajoissa. Varmenteiden vanheneminen aiheutti suuria häiriöitä kriittisissä järjestelmissä.

Toinen työn pääkohta on konsulttiyrityksen järjestämä koulutus uuteen toiminnanohjausjärjestelmään. Tämä koulutus todettiin puutteelliseksi eikä vastannut yrityksen tarpeita. Koulutuksessa ei pureuduttu lainkaan esimerkiksi varmenteiden ylläpidon ongelmiin. Tämä johti siihen, että yrityksen asiantuntijat joutuivat käyttämään suuren määrän työaikaa opetellessaan hallintajärjestelmän käyttöä.

Tämän työn pohjalta on toimitettu järjestelmän muutoksesta vastaaville henkilöille kirjalliset dokumentit kehitys- ja muutosehdotuksista. Työn laatijan ehdotukset koostuivat konsulttiyrityksen palveluiden vähentämisestä ja yrityksen sisäisen ammattitaidon hyödyntämiseen panostamisesta. Koulutuksen osalta työn laatija on kehottanut yritystä ottamaan yhteyttä konsulttiyrityksen kouluttajiin koulutusten laadun parantamiseksi tai siirtämään koulutusvastuun kokonaan yrityksen sisäisille asiantuntijoille.

ABSTRACT

Oulu University of Applied Sciences
Degree Program in Information Technology
Option of Software development

Author(s): Niko Naumanen
Title of thesis: Renewal of the Enterprise Resource Planning System
Supervisor(s): Pekka Alaluukas
Term and year when the thesis was submitted: Fall 2024
Number of pages: 27

This work examines the impact of an enterprise resource planning (ERP) system on the management and maintenance of server certificates. The company where this work was conducted is not named, nor is the consultancy firm responsible for the system modification. The decision to keep these entities anonymous aims to maintain the impartiality of the study.

The company in question transitioned from an ERP system called Efecte to a new system, ServiceNow. During the transition, significant data issues arose between the two systems. These issues resulted in many server certificate records being absent in the new system. Additionally, the transferred records lacked information about responsible personnel, leading to delays in renewing certificates. The expiration of certificates caused major disruptions in critical systems.

Another key focus of this study is the training provided by the consultancy firm for the new ERP system. The training was deemed inadequate and did not meet the company's needs. For example, the training did not address issues related to certificate maintenance. As a result, the company's experts had to spend a considerable amount of time learning how to use the system on their own.

Based on this work, written documents containing development and improvement suggestions were submitted to those responsible for the system transition. The author's recommendations included reducing the reliance on the consultancy firm's services and investing in the company's internal expertise. Regarding training, the author suggested that the company either contact the consultancy firm to improve the quality of the training or transfer responsibility for training entirely to internal experts.

SISÄLLYS

1 JOHDANTO

Tämä opinnäytetyö käsittelee toiminnanohjausjärjestelmän vaihdoksen aiheuttamia vaikutuksia palvelinvarmenteiden ylläpitoon ja hallintaan. Työ on tehty yhteistyössä yrityksen kanssa, jossa työn kirjoittaja työskentelee. Opinnäytetyössä vertaillaan varmenteiden hallintaa entisessä palvelunhallintajärjestelmässä Efectessä ja uudessa, tammikuussa 2024 käyttöön otetussa järjestelmässä, ServiceNow'ssa.

ServiceNow on yritystämme varten räätälöity palvelunhallintakokonaisuus, jonka toimintaa tarkastellaan opinnäytetyön aikana. Työssä käsitellään myös järjestelmän vaihdoksesta syntyneitä haasteita, sillä ne vaikuttavat suoraan varmenteiden hallintaan ja ylläpitoon. Opinnäytetyön tavoitteena on osoittaa, millaisia vaikutuksia järjestelmän muutoksella oli hallintaan ja ylläpitoon sekä esittää kehitysehdotuksia havaittujen puutteiden korjaamiseksi ja jatkokehityksen edistämiseksi.

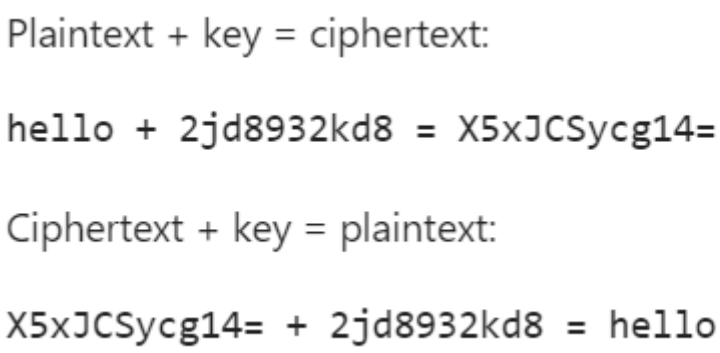
2 PALVELINVARMENTEET

Palvelinvarmenteita käytetään yleisesti internetin yli tapahtuvan liikenteen suojaamiseen. Varmenteet salaavat selaimen ja verkkosivun käyttämän palvelimen välisen liikenteen. Ne takaavat, että tieto siirtyy yksityisesti ja muuttumattomana selaimen ja palvelimen välillä. (DigiCert 2024.) Tarkemmin sanottuna varmenteet suojaavat TLS- ja SSL-liikennettä selaimen ja palvelimen välillä. Varmenteet varmistavat myös, että verkkosivusto tai palvelu on todella se, mitä se väittää olevansa.

2.1 SSL

SSL eli Secure Socket Layer on vuonna 1995 kehitetty internetin salausprotokolla. Protokollan kehittäjänä toimi yritys nimeltä Netscape. SSL-protokollan pääperiaate on luoda kahden laitteen välille turvallinen yhteys niin kutsutun kättelyn kautta. Tämä kättely salaa liikenteen selaimen ja palvelimen välillä tekemällä esimerkiksi lähetetystä tekstistä täysin lukukelvotonta ilman salauksen purkuun tarvittavaa avainta.

Protokollan toiminta perustuu siihen, että palvelin jakaa julkisen avaimen (public key), jonka varmenteen luonut taho on määrittänyt varmenteelle. Julkinen avain salaa esimerkiksi lähetetyn tekstin täysin lukukelvottomaksi, ja salaus voidaan purkaa ainoastaan yksityisellä avaimella (private key), joka on vain varmenteen käytössä eikä ole käyttäjien saatavilla. (Cloudflare 2024.) Alla on esimerkkikuva, joka havainnollistaa, miten salaus voidaan suorittaa.



Kuva 1. Esimerkki miten SSL-salaus voidaan suorittaa käyttäen julkista ja yksityistä avainta.

SSL-protokollaa ei kuitenkaan ole päivitetty vuoden 1996 version 3.0 jälkeen. Monet tietoturva-ammattilaiset eivät enää suosittele SSL-protokollan käyttöä lainkaan, sillä protokollassa on monia haavoittuvuuksia, eikä sitä ole päivitetty vuosiin. (geeksforgeeks, 19.6.2024) Lisäksi modernit selaimet eivät enää hyväksy SSL-sertifikaatteja. SSL-sertifikaattien käytöstä onkin siirrytty modernimpaan ja huomattavasti turvallisempaan TLS-sertifikaattiin.

2.2 TLS

TLS eli Transport Layer Security on vuonna 1999 Internet Engineering Task Forcen (IETF) kehittämä protokolla, joka on suurimmaksi osaksi korvannut SSL-protokollan käytön. TLS-protokollan kehitys alkoi SSL 3.1 -versiona, ennen kuin siitä tehtiin kokonaan oma protokolla. Tämän vuoksi SSL- ja TLS-nimityksiä käytetään usein vaihdellen, kun tarkoitetaan samaa asiaa. Suurin ero SSL- ja TLS-protokollien välillä on se, että SSL-protokollassa selain pyytää salausta, kun taas TLS-protokollassa liikenne on salattu automaattisesti.

Tämän opinnäytetyön kannalta on kuitenkin tärkeää huomioida, että TLS-protokolla ja TLS-sertifikaatit tarkoittavat eri asioita. TLS/SSL-sertifikaatit ovat digitaalisia tiedostoja, jotka mahdollistavat TLS/SSL-protokollan käytön, ja näin ollen mahdollistavat HTTPS (Hypertext Transfer Protocol Secure) käytön (Savvy Security, 30.1.2023).

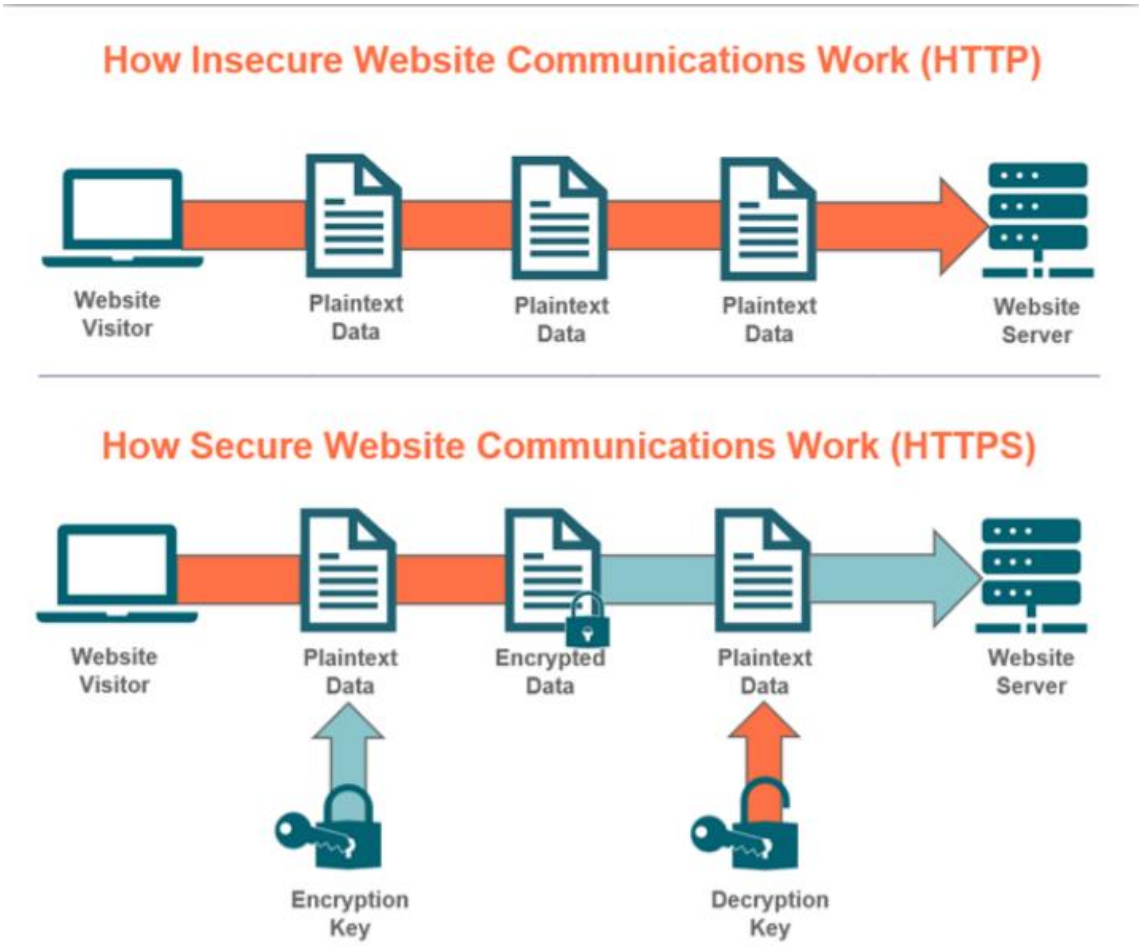
2.3 HTTP ja HTTPS

HTTP eli Hypertext Transfer Protocol on protokolla, jonka kehitti Tim Berners-Lee vuonna 1989 työskennellessään CERNissä (MDN Web Docs, 2024). Tämä

protokolla on niin kutsuttu sovelluskerroksen protokolla, joka mahdollistaa selaimen ja palvelimen välisen liikennöinnin. Samaan sovelluskerrokseen kuuluvat myös SSL- ja TLS-protokollat. HTTP-liikenne on kuitenkin täysin salaamatonta, joten kuka tahansa voi kaapata lähetetyn tai vastaanotetun liikenteen ja lukea sen sisällön ilman salauksen purkua, sillä data toimitetaan luettavassa tekstimuodossa.

HTTP-liikenteen salaamattomuus alkoi muodostua ongelmaksi erityisesti silloin, kun internetissä tapahtuva maksuliikenne yleistyi esimerkiksi Amazonin myötä. (DigiCert, 2024) Koska protokollaa käytettäessä selaimen ja palvelimen välisessä yhteydessä ei ole minkäänlaista salausta, pystyy esimerkiksi hakkeri varastamaan tai manipuloimaan käyttäjän tietoja. Tästä syystä palveluntarjoajat ovat pääasiassa siirtyneet käyttämään HTTPS-protokollaa vähintäänkin maksuliikennettä käsittelevillä sivustoillaan suurien tietomurtojen estämiseksi. Nykyaikainen HTTPS-protokolla koostuu tavallisesta HTTP-liikenteestä, joka on salattu TLS/SSL-protokollalla. HTTPS-protokolla on kehitetty vuonna 2000 The Internet Society’n toimesta.

Alla oleva kuva havainnollistaa paremmin HTTP- ja HTTPS-liikenteen eroavaisuudet.



Kuva 2. HTTP ja HTTPS liikenteen eroavaisuudet.

Kuten myös luvussa 2.2 mainittiin, jotta HTTPS-protokollan käyttämä TLS/SSL salaus toimii, vaatii se toimiakseen voimassa olevan TLS/SSL varmenteen.

2.4 TLS/SSL varmenne

TLS/SSL-varmenne on olennainen osa internetin tietoturvaa. Se toimii digitaalisen sertifikaatin tavoin ja takaa turvallisen yhteyden verkkoselaimen ja verkkosivuston käyttämän palvelimen välillä. Varmenteen päätehtävät ovat liikenteen salaus, palvelun tai verkkosivuston identiteetin varmistaminen ja tietojen eheyden takaaminen.

Ensisijaisesti TLS/SSL-varmenne suojaa verkkoliikennettä salaamalla sen. Tämä tarkoittaa, että käyttäjän selaimen ja palvelimen välinen tieto muutetaan salatussa muodossa sellaiseksi, etteivät ulkopuoliset tahot voi tarkastella tai siepata sitä. Esimerkiksi pankkitietojen, henkilötietojen tai kirjautumistietojen siirtäminen tapahtuu näin turvallisesti. Salaus perustuu julkisen avaimen infrastruktuuriin (PKI), jossa palvelin jakaa julkisen avaimen käyttäjälle. Tällä avaimella käyttäjän lähettämä tieto salataan, ja palvelimen yksityinen avain purkaa salauksen. Tämä mekanismi takaa, että vain oikea osapuoli voi lukea tiedot. (Mozzilla Developer Network, 2024.)

Toinen tärkeä tehtävä TLS/SSL-varmenteella on autentikointi. Varmenne vahvistaa verkkosivuston tai palvelun identiteetin, jolloin käyttäjä voi olla varma, että yhteys on luotu oikeaan sivustoon eikä esimerkiksi haitalliselle palvelimelle. Tämä suojaa käyttäjiä niin kutsutuilta "man-in-the-middle"-hyökkäyksiltä, joissa hyökkääjä yrittää huijata käyttäjän lähettämään tietojaan väärälle vastaanottajalle. Autentikointi perustuu siihen, että varmenteen myöntää luotettava kolmas osapuoli, kuten DigiCert, Let’s Encrypt tai GlobalSign.

Kolmas TLS/SSL-varmenteen tehtävä on taata tietojen eheys. Tämä tarkoittaa sitä, että tiedot, jotka siirtyvät selaimen ja palvelimen välillä, eivät muutu matkan aikana. Tietojen eheys varmistaa, että viestinnässä ei tapahdu luvattomia muutoksia tai manipulointia.

TLS/SSL-varmenteita käytetään monilla eri aloilla. Yksi yleisimmistä käyttötarkoituksista on verkkosivustojen suojaaminen HTTPS-protokollan avulla. HTTPS, joka näkyy käyttäjän selaimessa lukkosymbolina, takaa, että yhteys verkkosivustoon on suojattu ja autentikoitu. Lisäksi varmenteita käytetään suojaamaan sähköpostipalveluita, verkkopalveluita (API:t) ja jopa IoT-laitteita, joissa ne takaavat turvallisen tiedonsiirron palvelinten ja laitteiden välillä.

On tärkeää huomata ero vanhemman SSL-protokollan ja modernin TLS-protokollan välillä. SSL oli ensimmäinen protokolla, joka otti käyttöön tämän turvallisen yhteyden. Sen kehitys kuitenkin pysähtyi version 3.0 jälkeen vuonna 1996, ja protokollassa havaittiin ajan myötä useita haavoittuvuuksia. Tämän vuoksi SSL on

nykyään vanhentunut ja sen tilalle on tullut TLS (Transport Layer Security), joka tarjoaa paremman tietoturvan. Modernit selaimet eivät enää hyväksy SSL-varmenteita, ja kaikki uudet sertifikaatit käyttävät TLS:ää.

TLS/SSL-varmenteiden käyttö on välttämätöntä nykyisessä digitaalimaailmassa. Niiden avulla voidaan varmistaa yksityisyys, turvallisuus ja luottamus verkkoviestinnässä. Ilman TLS/SSL-varmenteita internet olisi altis tietovuodoille ja väärinkäytöksille. Onkin selvää, että varmenteet ovat olennainen työkalu, joka tukee turvallista ja luotettavaa verkkoviestintää.

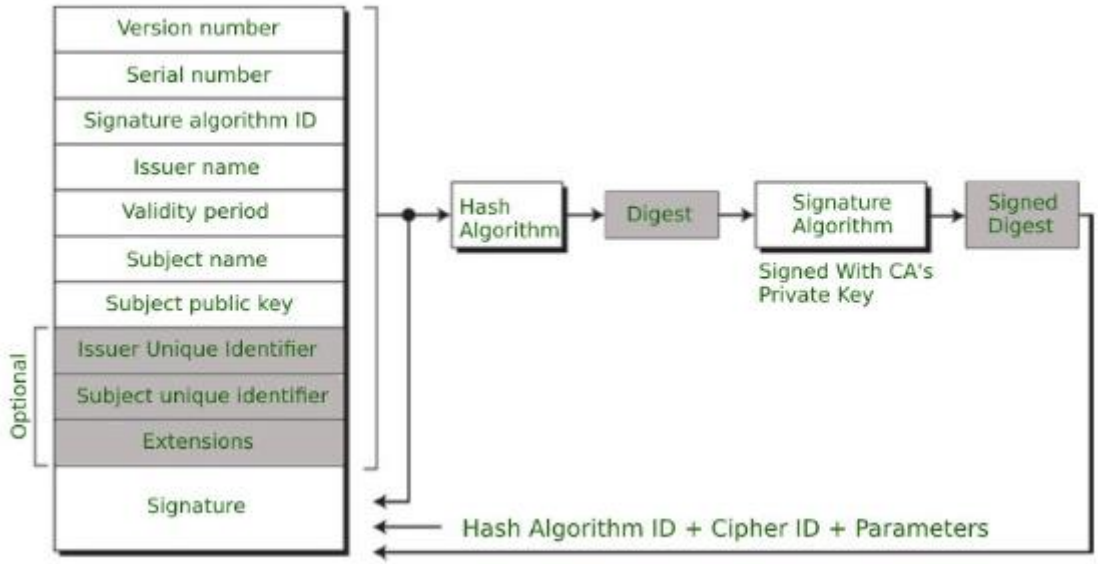
TLS/SSL-varmenteet ovat keskeisiä verkkoturvallisuuden takeita, mutta niiden hallintaan ja asennukseen liittyy omat haasteensa. Yksi tärkeimmistä vaiheista varmenteiden käytössä on niiden voimassaolon seuranta ja uusiminen. Varmenteiden voimassaolo väli onkahdesta viikosta 397 päivään asti ennen kuin ne tulee uusia, ja niiden vanheneminen voi aiheuttaa yhteysvirheitä käyttäjille. Vanhenemisen estämiseksi monet palveluntarjoajat ovat ottaneet käyttöön automaattisia uusimisjärjestelmiä, kuten Let’s Encrypt, joka tarjoaa ilmaisen varmenteen, jota voi helposti päivittää säännöllisesti (Let’s Encrypt, 2024).

TLS/SSL-varmenteiden asennus vaatii myös erityistä huolellisuutta palvelimen konfiguroinnissa. Väärin asennettu varmenne voi estää käyttäjiä pääsemästä sivustolle tai aiheuttaa varoitusviestejä selaimissa. Palvelimen konfiguroinnissa on tärkeää varmistaa, että ainoastaan turvalliset TLS-versiot ovat käytössä, ja heikommat, vanhemmat versiot, kuten SSL 3.0 ja TLS 1.0, on poistettu käytöstä. Tällä tavalla voidaan estää haavoittuvuuksia, jotka voisivat altistaa palvelimen hyökkäyksille (Mozilla, 2023).

Modernit selaimet myös suorittavat varmenteiden tarkistuksen OCSP-protokollan (Online Certificate Status Protocol) avulla varmistaakseen, ettei varmenteita ole peruutettu. Tämä tarkistus tehdään palvelun luotettavuuden takaamiseksi ja erityisesti haitallisten tai vanhentuneiden varmenteiden havaitsemiseksi. Tämä lisäturvallisuus on osa varmenteiden luomaa kokonaisvaltaista suojausta, joka toimii perustana luotettaville ja turvallisille HTTPS-yhteyksille (DigiCert, 2024).

2.5 Varmenteen rakenne

Palvelinvarmenne koostuu useasta eri osasta, jotka varmistavat varmenteen toiminnan sekä tarvittavan salaus asteen liikenteelle Alla oleva kuva havainnollistaa varmenteen rakennetta. Käymme tässä kappaleessa tarkemmin varmenteen osat läpi.



KUVA 3. Varmenteen rakenne.

2.5.1 Varmenteen versionumero

Varmenteen versionumero viittaa International Telecommunications Unionin (ITU) kehittämän X.509-standardin versioon, jota kyseinen varmenne käyttää. X.509 on vuonna 1998 kehitetty standardi, joka on laajalti hyväksytty standardi, joka varmistaa, että varmenteen julkinen avain kuuluu oikeasti taholle jolle, varmenne on myönnetty. Varmenne ei kuitenkaan pidä sisällään varmenteen luonnin yhteydessä luotua yksityistä avainta, vaan se säilötään omana tiedostonaan

erillään varmenteesta. (Chelsea, J 21.9.2020.) Yksityistä avainta käytetään varmenteen luoman salauksen purkuun, joten sen säilyttäminen varmenteen kanssa samassa tiedostossa tekisi varmenteesta hyödyttömän.

2.5.2 Varmenteen sarjanumero

Jokaiselle varmenteelle annetaan oma yksilöivä sarjanumero. Sarjanumeron perusteella voidaan tarvittaessa jäljittää varmenteen myöntäjä ja varmistua siitä, että varmenne on oikea. Sarjanumero on jokaiselle varmenteelle annettu uniikki merkkisarja, joka erottaa varmenteen muista varmenteista eikä esimerkiksi selaimen ja palvelimen välisessä liikenteessä käytetä virheellisesti väärää varmennetta.

2.5.3 Allekirjoitus algoritmi ja varmenteen myöntäjä

Allekirjoitusalgoritmi on varmenteen myöntäjän käyttämä allekirjoitus. Tämä osoittaa varmenteen luojan tiedot sekä heidän käymänsä salausmenetelmän. Allekirjoitusalgoritmi ei kuitenkaan itsessään toimi varmenteen salaus ominaisuutena vaan se on nimensä mukaisesti vain allekirjoitus ja varmennus, että varmenteen myöntäjä on oikea.

Varmenteen myöntäjän tiedoissa käy ilmi yrityksen nimi, maa, jossa yritys toimii, mahdollinen osavaltio ja kaupunki sekä onko kysymyksessä esimerkiksi yrityksen pääkonttori. Varmenteen myöntäjä sekä allekirjoitusalgoritmi ilmoitetaan selkokielisesti varmenteen sisällä.

2.5.4 Varmenteen voimassaoloaika

Varmenteen tiedoissa myös esitetään varmenteen voimassaoloaika, joka on kerrottu varmenteen myöntämispäivänä sekä varmenteen voimassaolon päättymispäivänä. Varmenteen voimassaoloaika voi vaihdella yleisesti kahdesta viikosta yhteen vuoteen. Elokuusta 2020 lähtien SSL/TLS-varmenteiden maksimi voimassa olo aika on ollut tarkalleen 397 päivää. Tämä johtuu suureksi osaksi

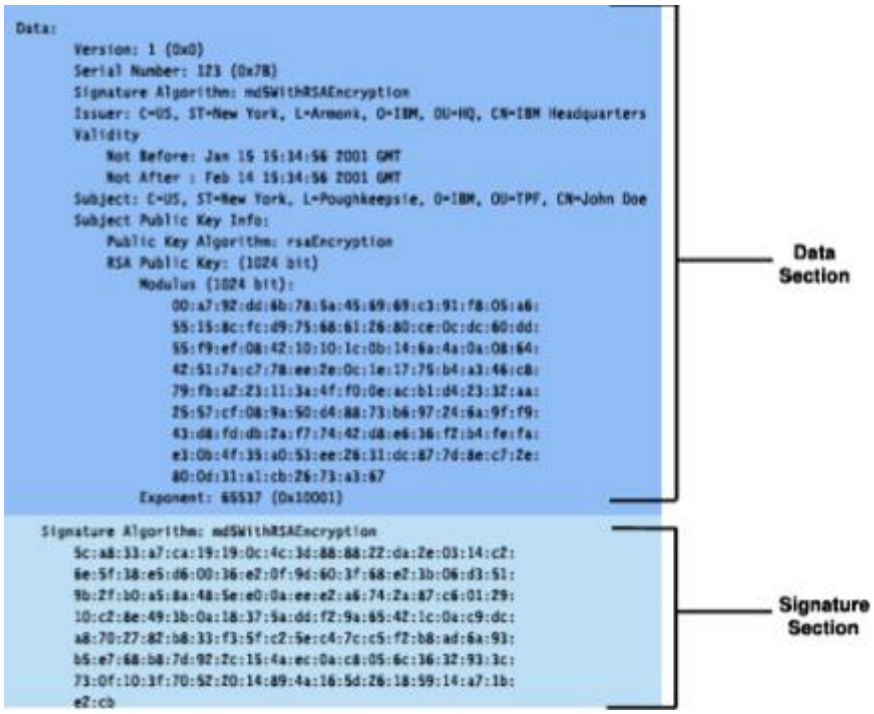
Applen päätöksestä olla luottamatta varmenteisiin Safari-selaimella, jotka ovat voimassa yli 398 päivää (SSL.com 8.5.2024.) Lyhyemmästä voimassa olo ajasta on kuitenkin ainakin kahdenlaisia hyötyjä. Se vähentää riskiä esimerkiksi varmenteen yksityisen avaimen vuotamiselle vääriin käsiin, sillä yksityinen avain vaihtuu aina kun varmenne uusitaan. Varmenteen ollessa lyhyemmän aikaa voimassa on siis ihmisestä johtuvan virheen tai väärinkäytön mahdollisuus pienempi. Toinen suuri hyöty lyhyemmästä voimassaolo ajasta on halu automatisoida prosessi. Jos esimerkiksi varmenne vanhenee kolmen kuukauden välein, on tilaajalla suurempi motivaatio kehittää automatisoitu prosessi varmenteen uusinnalle. Prosessin automatisointi varmistaa, ettei kyseinen varmenne pääse vanhenemaan eikä ylimääräisillä henkilöillä ole pääsyä varmenteen tietoihin.

2.5.5 Varmenteen haltijan tiedot

Varmenteen tiedoista myös löytyy varmenteen haltijan tiedot. Nämä tiedot on ilmoitettu samalla tavoin kuin varmenteen myöntäjän tiedot. Näillä tarkoilla tiedoilla varmistutaan jälleen, että kukin osapuoli on kuka väittää olevansa ja tiedot ovat selkokielisesti luettavissa varmenteen tiedoista tarkastusta varten.

2.5.6 Julkinen avain

Varmenne sisältää julkisen avaimen, jota käytetään liikenteen salauksen suorittamiseen. Julkinen avain on esitetty hash-koodi muodossa ja se sisältää kaiken tiedon, jotka on mainittu luvuissa 2.5.1–2.5.5 metadata-muodossa. Julkinen avain ei ole selkokielisessä muodossa vaan se on tarkoitettu koneiden väliseen viestintään. Alla oleva kuva esittää vielä myönnetyn varmenteen tiedot, siten kun ne on esitetty myönnetyssä varmenteessa.



Kuva 4. Myönnetyn varmenteen sisältö tekstitiedostona.

2.6 Varmenteiden myöntäjät

Varmenteen myöntäjä eli CA (Certificate Authority) on yleisesti luotettu ja puolueeton taho, joka myöntää yrityksille tarvittavat varmenteet turvalliseen liikennöintiin verkossa. Varmenteiden myöntäjät eivät keskity pelkästään myöntämään SSL/TLS-varmenteita vaan he myöntävät kaikkia verkossa tarvittavat varmenteet, joita käytetään esimerkiksi digitaaliseen allekirjoitukseen tai salatun sähköpostin lähettämiseen. Suurimpia ja luotetuimpia varmenteiden myöntäjiä ovat DigiCert, Let’s Encrypt, GlobalSign ja Entrust.

3 UUSI JA VANHA TOIMINNANOHJAUSJÄRJESTELMÄ

3.1 Efecte toiminnanohjaus järjestelmänä

Efecte on Suomalainen yritys, joka tarjoaa toiminnanohjaus palveluaan SaaS (Software as a Service) -periaatteella. Software as a Service -periaate tarkoittaa sitä, että asiakas maksaa palveluntuottajalle kuukausimaksua heidän kehittämästään palvelusta. Kuukausimaksu kattaa ohjelman ylläpidon sekä mahdollisten häiriöiden korjauksen. Saas palveluiden vahvuuksia ovat asiakkaalle syntyvien kustannuksia minimointi, sillä kuukausimaksu kattaa yleensä kaiken eikä asiakkaalla itsellään kulu aikaa esimerkiksi vikojen etsintään ja korjaukseen (Thomas. A. 10.7.2024).

3.1.1 Efecten käyttö tarkoitus

Efecte siis toimii Saas-periaatteella, joka tarjoaa asiakkaalle mahdollisuuden automatisoida toiminnanohjaus järjestelmäänsä sekä selkeyttää esimerkiksi raportointia ja antaa mahdollisuuden muokata käyttäjä kokemusta asiakkaan tarpeen mukaan. Yrityksemme käytti Efecteä pääsääntöisesti asiakas tikettien käsittelyyn, raportointiin, varmenteiden seuraamiseen sekä käytössä olevien laitteiden dokumentoimiseen.

3.1.2 Varmenteiden dokumentointi Efectessä

Palvelinvarmenteet, joita yrityksemme hallinnoi dokumentoitiin Efecteen datakortin muodossa. Korttiin on myös liitetty uuden varmenteen tilauksesta muodostunut tilaus lomake. Lomakkeesta käy ilmi varmenteen nimi, tilaajan tiedot, minkälainen varmenne oli kyseessä, asennus kohde, varmenteen luojan tiedot sekä asennuksesta huolehtivan tahon yhteystiedot. Varsinainen varmenteen datakortti piti sisällään palvelun eli varmenteen nimen sekä sen tarvitsemat lisänimet eli SAN-kentät. Subject Alternative Name eli SAN osoittaa mitkä nimet ja IP-osoitteet on sidottu kyseiseen SSL/TLS-varmenteeseen. (Gruhn, D. 5.3.2019)

3.1.3 Varmenteiden ylläpito Efectessä

Yrityksemme palveluissa käytettävät varmenteet ovat voimassa kerrallaan yhden vuoden ja niiden uusimisesta vastasi palvelusta tai sovelluksesta vastaava tiimi. Vastuutiimin sisällä oli määrätty vastuuhenkilö ja hänelle varahenkilö, jonka tehtävänä oli tehdä tarvittaessa varmenteen uusintapyyntö. Järjestelmä lähetti muistutusviestin sähköpostitse vastuuhenkilölle 90, 60 ja 30 päivää ennen varmenteen vanhenemista. Jos varmenne tuli uusia, oli yrityksen henkilökunnalle oma palvelukanavan lomake, josta pystyi varmenteen uusintapyynnön tekemään. Kun varmenne oli luotu varmenteen myöntäjän puolesta, toimitettiin sen tiedot yrityksen kyberturvapalveluille. Efecte uusi automaattisesti varmennekortin tiedot Efecteen ja kyberturvan asiantuntija toimitti varmenteen yksityisen avaimen vastuuhenkilölle. Vastuuhenkilö suoritti itse tai delegoi varmenteen asennustyön tarvittaville tahoille tämän jälkeen.

3.2 ServiceNow

ServiceNow on Efecten tapaan myös Saas-palveluun pohjautuva toiminnanohjaus järjestelmä. ServiceNow toimii kuitenkin pilvipalveluna ja mainostaakin itseään palveluna, jossa ei ole huollon aiheuttamia käyttökatkoja. ServiceNow on perustettu vuonna 2003 Kaliforniassa Fred Luddyn toimesta. (Crossfuze, 2024.)

3.2.1 ServiceNow’n käyttö tarkoitus

Kun ServiceNow otettiin ensimmäisen kerran käyttöön maailmalla, oli se tarkoitettu pelkästään IT-puolen toiminnanohjaukseen. ServiceNow’n suosio kuitenkin kasvoi nopeasti ja nykyisellään alustaa voidaan käyttää lähestulkoon missä tahansa toimialasta riippumatta. Yrityksessämme ServiceNow korvasi Efecten ja käyttötarkoitus palvelunhallintajärjestelmällä pysyi samana. Vaikka käyttötarkoitus pysyi samana, oli järjestelmän muutoksen tahtotilana suoraviivaistaa raportointia ja dokumentointia, joka onnistuu helpommin ServiceNow’n työkaluilla. ServiceNow’n suuri valtti on myös monien toistuvien tapahtumien automatisointi, joka vähentää ihmistyön määrää.

3.2.2 Varmenteet ServiceNowssa

Varmenteiden dokumentointi ja ylläpito toimii lähes samalla tavalla kuin Efectessäkin. ServiceNow tarjoaa kuitenkin paremman mahdollisuuden linkittää varmenteeseen liittyvät sovellukset, jotka käyttävät kyseistä varmennetta. Sovelluksista, jotka käyttävät varmennetta, muodostuu automaattisesti järjestelmän sisällä vuokaavio. Tämän avulla on helppo tarkastaa, miten esimerkiksi yksittäinen varmenne on linkittynyt sovellusten välillä.

Myös varmenteen vastuutiimin ja vastuuhenkilön linkittäminen toimii ServiceNow'ssa helpommin. Edellä mainitusta vuokaaviosta voidaan valita haluttu sovelluskortti, jonka kautta voidaan tarkastaa sovelluksen vastuuryhmä ja vastuuhenkilö, jotka vastaavat varmenteen ylläpidosta. Näin ollen uusintaprosessi ainakin teoriassa helpottui ja suoraviivaistui huomattavasti verrattuna Efecteen.

4 JÄRJESTELMÄN MUUTOKSEN VAIKUTUKSET VARMENTEIDEN YLLÄPITOON

Yrityksemme otti ServiceNow-järjestelmän käyttöön tammikuussa 2024, mutta tietoja vanhasta Efecte-järjestelmästä oli siirretty uuteen järjestelmään testattavaksi jo syyskuusta 2023 alkaen. Tämä testaus ei kuitenkaan kattanut varmenteita, laitteita tai sovelluksia, vaan sisälsi ainoastaan asiakastikettijärjestelmän ja asiakkaille tarkoitetun palveluportaalin. Varmenteiden osalta puutteellisen datan ja sovellusten siirto uuteen järjestelmään aloitettiin varsinaisen käyttöönoton yhteydessä.

Järjestelmän käyttöönotto oli hyvin sekava, ja puuttuvat tiedot aiheuttivat merkittävää ajanhukkaa vastuutiimeissä, kun korttien tietoja ja siirtoja vanhasta Efecte-järjestelmästä jouduttiin suorittamaan käsityönä. Varmenteiden hallinnassa suurimmaksi ongelmaksi osoittautui se, että automatiikka, joka oli varmenteille määritelty, ei toiminut oikein. Automatiikka ei lähettänyt varmenteiden vastuuhenkilöille muistutusviestejä uusimistarpeesta, minkä seurauksena suuri määrä varmenteita pääsi vanhenemaan. Myöskään automatiikan hajoamista ei oltu ennakoitu mitenkään kun järjestelmää valmisteltiin. Lisäksi Efecte-järjestelmästä siirrettyjen varmennekorttien tiedot olivat virheellisiä.

Sekaannusta lisäsi myös heikko perehdytys ServiceNow’n toimintoihin sekä epäselvyys siitä, miten järjestelmää oli suunniteltu käytettävän yrityksessämme. Perehdytyksestä ja järjestelmän konfiguraatiosta vastasi ulkopuolinen konsulttiyritys. Konsulttiyritys työskenteli yhteistyössä yrityksemme projektipäälliköiden ja muutamien valittujen henkilöiden kanssa, mutta esimerkiksi sovellusten vastuutiimien tarpeiden huomioiminen jäi hyvin vähäiseksi.

4.1 Tiedon siirto Efecten ja ServiceNow’n välillä

Selkeyden vuoksi tässä yhteydessä keskitytään tiedonsiirron osalta ainoastaan palvelinvarmenteiden datan siirtämiseen toiminnanohjausjärjestelmien välillä. Palvelinvarmenteille luotiin ServiceNow-ympäristöön testiksi varmennekortti, jotta voitiin tarkistaa, miten järjestelmä käsittelee tietoja sekä miten varmennekortti saadaan liitettyä sitä käyttäviin järjestelmiin ja ohjelmiin. Testaus aloitettiin kuitenkin liian myöhään järjestelmän kehitysaikataulussa, ja kun varmenteiden data siirrettiin Efectestä ServiceNow’hun, korttien data oli virheellistä ja osa korteista ei siirtynyt lainkaan.

Esimerkiksi siirron yhteydessä kaikilta varmenteilta katosi kokonaan tiedot vastuuryhmästä ja vastuuhenkilöstä. Tämä johti siihen, että automaattiset varoitukset varmenteen uusimistarpeesta eivät tavoittaneet oikeaa henkilöä, minkä seurauksena useita kriittisiä varmenteita jäi uusimatta. Tämä aiheutti käyttökatkoja monissa kriittisissä järjestelmissä, ja katkokset kestivät joissain tapauksissa useita tunteja, koska asiantuntijoilla ei ollut tietoa häiriön syystä.

Tämän työn kirjoittamishetkellä kyseistä vikaa ei ole vielä saatu korjattua järjestelmässä, ja varmenteiden valvonta suoritetaan pääosin manuaalisesti, mikä on työn laatijan vastuulla. Tämä käsin tehtävä valvonta työllistää työn laatijaa keskimäärin 12 tuntia viikossa.

Valvontatyöhön kuuluu vanhenevien varmenteiden seuranta sekä vastuuhenkilöiden etsintä. Kuten aiemmin mainittiin, kaikki varmennekortit eivät ole siirtyneet järjestelmien välillä oikein. Tämän puutteen paikkaamiseksi on jouduttu luomaan erikoistyökalu. Tämä työkalu on skripti, joka voidaan asettaa hakemaan vanhenevia varmenteita halutun päivämäärärajan sisällä.

Tiedonsiirron epäonnistuminen on siis johtanut tilanteeseen, jossa varmenteiden ylläpito aiheuttaa kohtuuttoman paljon lisätyötä ja haittaa. Kuten edellä on myös todettu, tämä on aiheuttanut käyttökatkoja kriittisissä järjestelmissä, mikä pahimmassa tapauksessa on voinut vaarantaa ihmishenkiä.

Tätä työtä kirjoittaessa ServiceNow-järjestelmä on ollut yrityksemme käytössä 11 kuukautta. Järjestelmän käyttöönotto on kuitenkin edelleen keskeneräinen, ja siitä löytyy jatkuvasti puutteita tai toimimattomia osioita. ServiceNow on alun perin englanninkielinen sovellus, joka on konsulttiyrityksen toimesta käännetty suomeksi. Suomennoksessa on edelleen puutteita, jotka aiheuttavat suurta sekaannusta sekä järjestelmän käytössä että koulutuksissa.

4.2 ServiceNow-koulutus

ServiceNow'n käyttöönotosta vastasi sama ulkopuolinen konsulttiyritys, joka vastasi järjestelmän konfiguroinnista yrityksemme tarpeisiin. Selkeyden vuoksi tässä työssä käsitellään koulutusta vain varmenteiden näkökulmasta. Ensimmäiset koulutukset varmenteiden hallinnasta pidettiin vasta, kun järjestelmä oli ollut käytössä jo 3 kuukautta.

Konsulttiyrityksen järjestämä koulutus on ollut hyvin yleisluontoista ja sekavaa, eikä siinä ole keskitytty lainkaan niihin konkreettisiin ongelmakohtiin, joita järjestelmän käytössä on havaittu. Esimerkiksi kouluttajat eivät käyneet läpi, miten uusi varmennekortti luodaan tai miten sitä tulee ylläpitää. Koulutus järjestetään yleensä Teams-puhelun kautta, jossa kouluttaja esittelee kalvosarjan, esimerkiksi kuinka uusi palvelupyyntö tulisi luoda järjestelmään. Käytännön esimerkit puuttuvat koulutuksista täysin.

Kuten edellä mainittu, varmennekortin ylläpitoon liittyen kouluttajilla ei ollut tietoa siitä, miten kortti voidaan luoda tai miten siihen voidaan lisätä tietoja. Lisäksi koulutuksille on varattu täysin riittämätön 30 minuutin aikaikkuna. Koulutus on lähes kokonaan kouluttajan nopea monologi, jossa ei ole aikaa kysymyksille, tai kouluttaja ei osaa vastata esitettyihin kysymyksiin.

Koulutuksen riittämättömyyden vuoksi sekä työn laatijalla että muilla asiantuntijoilla on kulunut huomattavasti työtunteja järjestelmän itsenäiseen opiskeluun. Konsulttiyrityksen kouluttajat mainitsevat koulutusten lopuksi, että tarvittaessa voidaan järjestää lisäkoulutuksia. Näitä lisäkoulutuksia on järjestetty esimerkiksi

varmenteiden hallinnasta, mutta koulutuksen sisältö on ollut lähes identtinen edeltävien koulutusten kanssa.

Varmenteiden ylläpitoon liittyvässä koulutuksessa konsulttiyrityksen kouluttaja ei osannut vastata moniin kriittisiin kysymyksiin. Esimerkiksi kouluttaja ei tiennyt, miten varmennekortti lisätään valvontalistalle tai miten uusi varmenne linkitetään sovellukseen tarvittaessa, jos automaatio ei pysty suorittamaan tehtävää. Tämä johti siihen, että työn laatija joutui käyttämään noin 80 työtuntia järjestelmän itsenäiseen opiskeluun ja luomaan oman hallintanäkymän ServiceNow-järjestelmän sisälle.

Tämän perusteella voidaan todeta, että konsulttiyrityksen tarjoama koulutus on ollut riittämätöntä eikä ole vastannut yrityksemme tarpeita.

5 POHDINTA

Tämän työn aiheena oli kerätä tietoa siitä, millainen vaikutus toiminnanohjausjärjestelmän vaihdolla oli palvelinvarmenteiden ylläpitoon. Kuten työssä on aiemmin esitetty, datan siirrossa järjestelmien välillä oli suuria haasteita. Varmennekorteista puuttui tärkeää tietoa, tietoja ei siirretty ajoissa tai kortti puuttui kokonaan uudesta järjestelmästä. Näistä puutteista aiheutuneet haitat veivät huomattavan määrän työaikaa ja aiheuttivat merkittäviä häiriöitä hallinnoitavissa järjestelmissä. Datan katoaminen olisi voitu estää tai ainakin minimoida tekemällä datan siirto yrityksen sisäisten ammattilaisten avulla sen sijaan, että työ ulkoistettiin konsulttiyritykselle. Konsulttiyrityksellä ei ollut täyttä ymmärrystä varmennedatan rakenteesta eikä siitä, kuinka kriittisestä asiasta oli kyse.

Datan siirrosta ja sen kehittämisestä on työn laatija tehnyt kirjallisen ehdotuksen yrityksen järjestelmämuutoksista vastaavalle henkilölle. Ehdotuksessa käsitellään tässä työssä havaitut epäkohdat ja suositellaan konsulttiyrityksen käytön vähentämistä. Lisäksi ehdotetaan yrityksen omien asiantuntijoiden hyödyntämistä varmennedatan käsittelyn kehittämisessä ja korjaamisessa.

Puutteellisen datan lisäksi uuden järjestelmän koulutus oli konsulttiyrityksen toimesta järjestetty huonosti. Koulutuskertoihin oli varattu liian vähän aikaa, eikä kouluttaja ollut selvästi perehtynyt aiheeseen riittävällä tarkkuudella. Lisäksi koulutusten 30 minuutin kesto oli täysin riittämätön käsiteltävän asiasisällön määrään nähden. Koulutuksista aiheutuu yritykselle huomattavia kustannuksia, mutta niistä ei ole saatu konkreettista hyötyä. Myös koulutusten laadusta on tehty kehitysehdotus yrityksen vastuuhenkilölle. Kehitysehdotuksessa on käsitelty koulutusten heikkoa laatua ja suositeltu konsulttiyritykselle annettavan palautetta koulutuksen parantamiseksi. Vaihtoehtoisesti on ehdotettu, että koulutukset toteutettaisiin yrityksen sisällä omien asiantuntijoiden toimesta. Näin koulutuksen sisältö ja laatu voitaisiin paremmin mitata ja mukauttaa vastaamaan yrityksen tarpeita.

Ehdotuksessa on lisäksi todettu, että tämä ratkaisu vaatisi yritykseltä investointeja, kuten uusien asiantuntijoiden palkkaamista, jotta koulutus ja järjestelmän ylläpito onnistuisivat sisäisesti. Näistä aiheutuvat kustannukset olisivat alkuvaiheessa merkittäviä, mutta pitkällä aikavälillä omien asiantuntijoiden käyttö tulisi edullisemmaksi kuin konsulttiyrityksen palveluiden hyödyntäminen.

Lopullisena yhteenvetona voidaan todeta, että konsulttiyrityksen palveluita on käytetty liiallisesti järjestelmän vaihdon yhteydessä, eikä konsulttiyrityksellä ole ollut täsmällistä kuvaa siitä, mitä yrityksen tarpeet ServiceNow-järjestelmältä edellyttävät. Yritystä, jossa työn laatija työskentelee, on informoitu puutteellisesta koulutuksesta sekä datansiirrossa tapahtuneiden virheiden vaikutuksista. Yritys ei kuitenkaan ole työn kirjoitushetkellä vastannut kehitysehdotuksiin.

LÄHTEET

Thomas, A 10.7.2024. What is SaaS. Luettavissa: https://builtin.com/articles/saas . Luettu 20.10.2024

Gruhn, D 5.3.2019. What is SAN (subject alternative name) and how to use it. Luettavissa: https://www.entrust.com/blog/2019/03/what-is-a-san-and-how-is-it-used . Luettu 29.10.2024

Digicert 2024. What are TLS/SSL certificates? Luettavissa: https://www.digicert.com/tls-ssl/tls-ssl-certificates . Luettu 30.10.2024

Cloudflare 2024. What is SSL? Luettavissa: https://www.cloudflare.com/learning/ssl/what-is-ssl/ . Luettu 1.11.2024

Cloudflare 2024. What is TLS handshake? Luettavissa: https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/ . Luettu 3.11.2024

Savvy Security 30.1.2023. TLS Version: What they are and which ones are still supported? Luettavissa: https://cheapsslsecurity.com/blog/tls-versions-what-they-are-and-which-ones-are-still-supported/ . Luettu 7.11.2024

Mdn web docs 2024. Evolution HTTP. Luettavissa: https://developer.mozilla.org/en-US/docs/Web/HTTP/Evolution_of_HTTP . Luettu 4.11.2024

Let's Encrypt 2024. How it Works. Luettavissa: https://letsencrypt.org/how-it-works/ . Luettu 9.11.2024

Mozilla 2023. Security/Server Side TLS. Luettavissa: https://wiki.mozilla.org/Security/Server_Side_TLS. Luettu 9.11.2024

DigiCert, 2024. OCSP & CRL and Revoked SSL Certificates. Luettavissa: https://www.digicert.com/kb/util/utility-test-ocsp-and-crl-access-from-a-server.htm. Luettu 9.11.2024

Chelsea, J 22.9.2020. An Overview of X.509 Certificates. Luettavissa: https://www.ibm.com/support/pages/system/files/inline-files/An_Overview_of_x.509_certificates.pdf . Luettu 10.11.2024

SSL.com, 8.5.2024. SSL Certificate Expiration Guide. Luettavissa: https://www.ssl.com/guide/ssl-certificate-expiration-guide/ . Luettu 11.11.2024

Crossfuze, 2024. What is ServiceNow. Luettavissa: https://crossfuze.com/servicenow/what-is-servicenow/ . Luettu 17.11.2024

Geeksforgeeks, 19.6.2024. Secure Socket Layer (SSL). Luettavissa: https://www.geeksforgeeks.org/secure-socket-layer-ssl/ . Luettu 18.11.2024

Mozilla Developer Network (MDN) 2024. Certificate Transparency Luettavissa: https://developer.mozilla.org/en-US/docs/Web/Security/Certificate_Transparency . Luettu 19.11.2024