Juuso Lähdekorpi

Yrityskohtaisen sertifikaattijärjestelmän harjoituksen toteuttaminen

Opinnäytetyö
Informaatiotekniikka

2020

Kaakkois-Suomen
ammattikorkeakoulu

Tekijä/Tekijät	Tutkinto	Aika
Juuso Lähdekorpi	Insinööri (AMK)	Toukokuu 2020

Opinnäytetyön nimi

Yrityskohtaisen sertifikaattijärjestelmän harjoituksen toteuttaminen

25 sivua
31 liitesivua

Toimeksiantaja

Kaakkois-Suomen ammattikorkeakoulu

Ohjaaja

Vesa Kankare

Tiivistelmä

Tämän opinnäytetyön tarkoituksena oli toteuttaa Xamkin ICTLABin virtuaaliympäristössä julkisten avainten infrastruktuuri ja tutkia sertifikaattiauktoriteettien toimintaa. Siltä pohjalta luotiin asennus- ja käyttöopas mahdollista kurssimateriaalia tai tuotantoympäristön sertifikaattipalvelua varten. Tutkimusongelmana oli selvittää, miten yrityskohtainen sertifikaattipalvelu toimii.

Sertifikaattipalvelut ovat internetin tukipilari, jota ilman salattu liikenne laitteiden tai palveluiden välillä ei toimi. Työn teoriaosuudessa käytiin läpi julkisten avainten kryptografiaa sekä miten sertifikaattihierarkia ja toiminnallisuus toteutetaan. Työn vaiheista laadittiin ohjeistus, jota voi hyödyntää jatkotutkimuksissa.

Tutkimusongelmaan etsittiin ratkaisua tutkimalla Microsoftin ohjeita sekä IETF-standardeja tarkoituksena löytää malleja toteutuksen mukaisista menetelmistä. Lisäksi etsittiin sertifikaattipalvelun kaksitasoisen hierarkian toteutuksen menetelmiä sekä x.509-standardiin perustuvia julkisten avainten menetelmiä. Löydetyillä menetelmillä luotiin kaksitasoinen sertifikaattienjakeluhierarkia.

Työ painottuu käytäntöön enemmän kuin varsinaiseen teoriaan. Opinnäytetyön aloitusvaiheessa tarkasteltiin sertifikaattihierarkiaympäristöjä ja julkisten avainten infrastruktuurin perusperiaatteita sekä niihin liittyviä salausprotokollia.

Työn lopputuloksena oli onnistunut testitoteutus ICTLABin virtuaaliympäristössä kaksitasoisella sertifikaattipalvelinhierarkialla sekä ohjeistus sertifikaattipalvelinympäristön käyttöönotosta. Tuloksista pystyi päättelemään, että sertifikaattipalveluympäristö on mahdollista toteuttaa ICTLABin virtuaaliympäristössä tarkalla suunnittelutyöllä.

Asiasanat

sertifikaatti, PKI, kryptografia, X.509

South-Eastern Finland University of Applied Sciences

Author (authors)	Degree	Time
Juuso Lähdekorpi	Bachelor of Engineering	May 2020

Thesis title

Enterprise certificate authority: a case study of designing and implementation

25 pages
31 pages of appendices

Commissioned by

South-Eastern Finland University of Applied Sciences

Supervisor

Vesa Kankare

Abstract

The objective of the thesis was to study the operations of certificate authorities and public key infrastructure so that possible learning material could be composed based on the written test results.

Certificate authority services are the backbone of the Internet without which encrypted traffic cannot be sustained. The theory part of the thesis investigates public key cryptography protocols and the certificate authority hierarchy. The different phases of the study were documented, so they can be used as a reference in the future. The phases consisted of designing and implementing certificate authority services using Microsoft's network and infrastructure baseline guides into XAMK ICTLAB virtual laboratory.

The thesis is mainly focused on the practical study of certificate authority functions. In order to create a conceptual basis, the certificate hierarchy environments and the basic principles of public key infrastructure as well as the use of cryptography protocols were studied at the start of the thesis.

The conclusion of the thesis was a successful test in the virtual lab environment with a nested stack certificate authority hierarchy, and instructions were made on how to build and operate a certificate authority in a test environment.

Keywords

certificate, PKI, cryptography, X.509

SISÄLLYS

KUVALUETTELO

1 JOHDANTO

Sertifikaatteja käytetään maailmassa hyvin suuressa määrin kaikessa turvatussa tietoliikenteessä ja varmistuksissa. Sertifikaatit ovat pieniä datatiedostoja, jotka ovat digitaalisesti allekirjoitettu avattavaksi vastapuolen avaimella (GlobalSign 2020). Sertifikaattien käyttö luo pohjan tietoturvalliselle tietojen välitykselle. Sertifikaatteja niin kuin käyttötarkoituksiakin on useita, käyttäjät voivat käyttää sertifikaatteja salattua sähköpostia käyttäen (S/MIME) tai pankkitietoja tarkasteltaessa. Sertifikaattien tarkoitus on mahdollistaa laitteiden tai palveluiden välisen tietoliikenteen salaus. Periaatteena on, että salauksessa käytetään etukäteen sovittua salausavainta, jolla vastaanottava laite tai palvelu voi avata salatun tiedon.

Käyttäjät voivat käyttää sertifikaatteja esimerkiksi asioidessaan verkkopankissa ja verkkokaupoissa, käyttäessään sähköpostia Internet-selaimella tai asiakasohjelmalla, sähköisiä allekirjoituspalveluita, julkisia palveluita kuten Vero.fi tai Suomi.fi-tunnistautumisessa. Käyttäjän ei yleensä tarvitse tehdä omia toimia sertifikaatteja käyttäessään, koska laitteet ja palvelut hoitavat sertifikaattien käytön automaattisesti. Käytettäessä sertifikaattia voidaan käyttäjän todennus toteuttaa vahvemmin kuin pelkällä käyttäjätunnus–salasana-parilla.

VPN-palveluiden ja langattomien verkkojen yhteyden muodostuksessa käyttäjän tunnistautumiseen voidaan hyödyntää sertifikaatteja. Niiden salaus tunnetaan yleisimmin SSL/TLS-kättelynä, jolloin sertifikaatin varmennus tapahtuu käyttäjän omistamalla salaisella avaimella ja varmistava palvelin varmentaa salaisen avaimen luotettavuuden eroten näin tavallisesta SSL-kanssakäymisestä (Comodo 2018). Palvelimet käyttävät sertifikaatteja luodessaan turvallisia salattuja yhteyksiä toisiin palvelimiin. Kaikkien näiden sertifikaattien tarkistusten ja identiteettien varmennuksen takana toimii sertifikaattiauktoriteetti.

1.1 Opinnäytetyön tavoite

Työssä on tavoitteena suunnitella ja toteuttaa Xamkin ICTLABin virtual lab -ympäristöön sertifikaattipalvelu palvelinympäristöön sekä käyttää siitä kerättyjä tietoja ja toimia kurssimateriaalina. Suunnittelu tapahtuu topologiakaavion laatimisella.

Työhön kuuluu käytännön toteutuksen lisäksi teoriaa, jossa pureudutaan sertifikaattipalvelimien perustaan, topologiaan sekä yleisessä käytössä oleviin toimintatapoihin. Käytännön osuudessa luodaan virtuaalilaboratorioympäristöön jaoteltu sertifikaattipalvelintopologia, mitä pystytään hyödyntämään kurssitoteutuksessa ja sertifikaattipalvelun testaamisessa.

Työn tutkimusongelmana on selvittää, miten sertifikaattipalvelujärjestelmien parhaita käytäntöjä harjoitellaan virtuaalilaboratorioympäristössä sekä miten niiden käyttöönotto järjestetään. Tämän opinnäytetyön tutkimuskysymykset ovat:

- Mitkä ovat yrityskohtaisten sertifikaattijärjestelmien parhaita käytäntöjä?
- Miten sertifikaatit saadaan toimimaan erilaisissa käyttötarkoituksissa?
- Miten näitä käytäntöjä voidaan harjoitella laboratorio ympäristössä?

1.2 Tutkimusmenetelmän valinta

Opinnäytetyön tutkimusmenetelmäksi valikoitui tapaustutkimus. Tapaustutkimus siitä kuinka rakennetaan yrityskohtainen sertifikaattijärjestelmä ja miten tältä pohjalta luodaan sovellettua kurssimateriaalia. Tavoitteena oli tuottaa uusia teoreettisia ideoita, ehdotuksia tai olettamuksia, jotka tuottavat tiettyjä käytäntöjä (Eriksson & Koistinen 2005, 13), tässä tapauksessa PKI-ympäristöstä.

Tutkimus keskittyy syventävästi, siihen miten suunnitellaan ja rakennetaan sertifikaattipalvelinympäristö parhaiden käytäntöjen mukaisesti. Sertifikaattien jakelun järjestämisessä erityisen merkittävää on hierarkkisuus, jonka määrittelee IETF:n standardi. (RFC 5280 2008.)

2 PKI – PUBLIC KEY INFRASTRUCTURE

PKI-malli perustuu rooleihin, toimintamalleihin sekä käytäntöihin, joita tarvitaan digitaalisten sertifikaattien luomisessa, hallinnassa, säilyttämisessä sekä kumoamisessa (Trcek 2006, 69). Mota käsittelee opinnäytetyössään ”Secure

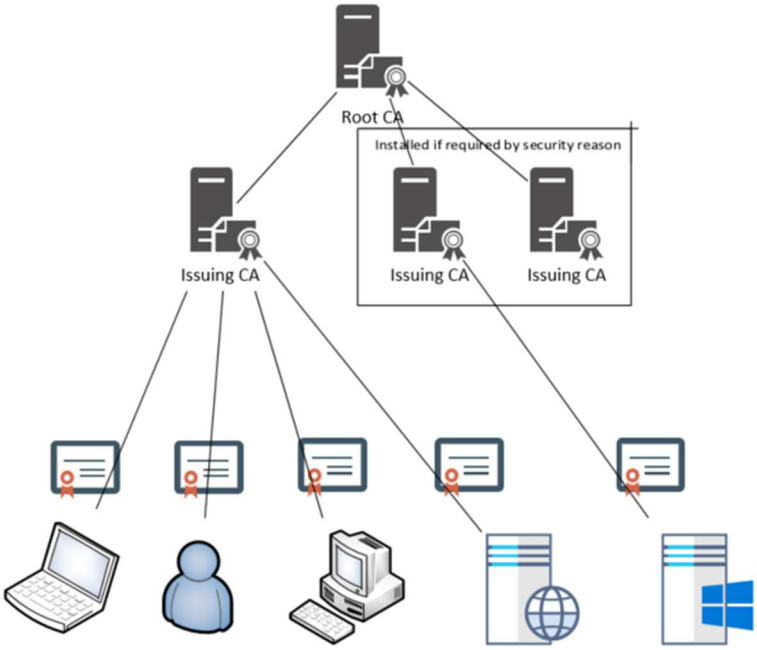
Certificate Management and Device Enrollment at IoT Scale” PKI:n tarkoitusta. PKI:n tarkoitus on turvallisen tiedonkulun varmistaminen kahden osapuolen välillä tietoliikenneyhteyksiä käyttäen.

Julkisten avainten infrastruktuurilla on kriittinen rooli, kun salasanapohjainen varmennus ei ole riittävä ja perusteellisempi varmennus tarvitaan. PKI on järjestely, joka sitoo julkisten avaimen tietyn verkkoresurssin identiteettiin, olkoon se käyttäjä, tietokone tai palvelin. Tämä sidos tapahtuu sertifikaattiauktoriteetin avulla, joka on vastuussa digitaalisten sertifikaattien rekisteröinnistä ja jakelusta, niitä tarvitseville asiakkaille tai verkko-osapuolille.

2.1 Root Certificate authority

Root- ja Subordinate-sertifikaattiauktoriteetteja käytetään sertifikaattien jakeluun käyttäjille, tietokoneille ja palveluille sekä hallinnoimaan sertifikaattien voimassaoloa. Standardin määrittelemänä sertifikaattienhierarkiajärjestys on IPRA, PCA (tarkemmin luvussa 3.) ja tämän jälkeen CA (RFC 5280 2008). Microsoft on soveltanut standardia omiin järjestelmiinsä niin, että aktiivihakemistossa on rooli, jolla on tehtävänä hoitaa sertifikaattienjakelu (Microsoft 2009). Root Certificate authority (CA) on julkisen avaimen sertifikaattipalvelin, joka määritellään toimimaan sertifikaattihierarkiassa ylimmällä tasolla.

Sertifikaattiauktoriteetit allekirjoittavat jaetut sertifikaatit käyttäen omaa salaista avaintaan. Sertifikaatit allekirjoitetaan lisäämällä varmentavan auktoriteetin varmentamismerkintä sertifikaattitiedostoon. Näin toinen osapuoli voi varmentaa sertifikaatin sisältävän tiedon, varmentaessaan sertifikaattiauktoriteetin, omalla julkisella avaimella. Toinen osapuoli saa sertifikaattiauktoriteetin julkisen avaimen julkaistusta sertifikaatista. Toinen osapuoli suorittaa allekirjoituksen tarkistamisen, joka sisältää julkisen avaimen toisesta sertifikaatista. (RFC 5280 2008.)



Kuva 1. PKI-infrastruktuurin hahmotus (oma piirros)

Kuva 1 edustaa sertifikaattihierarkiaa, joka sisältää neljä osapuolta, jossa loppukäyttäjän sertifikaatin jakaa jakelusertifikaattipalvelin (Issuing CA). Sertifikaatti on jaettu juurisertifikaattiauktoriteetilta (Root CA). Juurisertifikaattipalvelimen sertifikaatti on itsejulkaistu tarkoittaen, että sertifikaatti on allekirjoitettu omalla salaisella avaimella.

Allekirjoituksen varmennusketju alkaa loppukäyttäjän sertifikaatista. Jakelusertifikaattipalvelimen julkista avainta käytetään varmistamaan loppukäyttäjän sertifikaatin allekirjoitus. Sertifikaatin voimassaollessa juurisertifikaattipalvelimen julkista avainta käytetään varmentamaan jakelusertifikaattipalvelimen allekirjoitus. Juurisertifikaatin allekirjoitus varmennetaan sen omalla julkisella avaimella. (The SSL Store s.a.)

Allekirjoituksen varmennus juurisertifikaatin itseallekirjoittamalle sertifikaatille varmistaa juurisertifikaatin olevan muuttumaton. Se ei takaa, että tieto sertifikaatissa tai sertifikaattiauktoriteetissa itsessään ei ole luotettua, koska kuka vain voi luoda itseallekirjoitetun sertifikaatin ja määrittää itsensä sertifikaattiauktoriteetiksi. Ennen kuin julkisten avainten protokollia voidaan käyttää, tarvitsee luoda luottamussuhde omien sertifikaattiauktoriteettien sekä yksittäisten sertifikaattien välille. (RFC 5280 2008.)

2.2 Intermediate certificate authority

Intermediate certificate authority tai subordinate certificate authority on sertifikaatinjakelupalvelin, joka välittää sertifikaatteja alimmalle tasolle eli käyttäjätasolle. Juurisertifikaattiauktoriteetit eivät yleensä jakele sertifikaatteja suoraan loppukäyttäjälle. Sertifikaattihierarkiassa yleensä jakelusertifikaattipalvelimelle (Intermediate Certificate authority) allekirjoitetaan sertifikaattienjakeluoikeus juurisertifikaattipalvelimen salaisella avaimella, jolloin jakelusertifikaattipalvelimesta tulee luotettu sertifikaattienjakelija. Tämän jälkeen jakelusertifikaattipalvelimen salaista avainta käytetään loppukäyttäjien SSL-sertifikaattien myöntämiseen. (The SSL Store 2019.)

Lisäämällä jakelusertifikaattipalvelin välittäjäksi kasvatetaan sertifikaattienjakeluprosessin tietoturvaa. Tilanteessa, jossa sertifikaattienjakeluprosessiin tulee ongelmia tietoturvan tai sertifikaattien väärin jakamisen takia. Vain jakelusertifikaattipalvelimen sertifikaatti tarvitsee hylätä ja hakea uudelleen, jonka jälkeen kyseisen sertifikaattipalvelimen jakelemat sertifikaatit, tarvitsee jakaa uudelleen eikä koko ympäristön uudelleenjakelua tarvitse toteuttaa. (Mt.)

Jakelusertifikaattipalvelin suorittaa juurisertifikaatilla kirjoitetun sertifikaatin jakelun siitä hierarkiassa seuraaville osapuolille. Tällä mallilla juurisertifikaattipalvelin voidaan sammuttaa ja juuren salainen avain on turvattu ja hierarkia on joustavampi sekä skaalattavissa suuremmaksi. Jakelusertifikaattipalvelimen avulla palvelimien fyysisen sijainnin pystyy myös eriyttämään. (Microsoft 2009.)

2.3 Certificate revocation list

Client Revocation List (tästä eteenpäin CRL) on lista vanhentuneista sertifikaateista. Sertifikaatin voimassaoloajan päätyttyä sertifikaattiauktoriteetti lisää sertifikaatin sarjanumeron perusteella merkinnän CRL-listaan. Jokaisen sertifikaattiauktoriteetin CRL-viittaus löytyy CRL Distribution Point -merkinnästä (tästä eteenpäin CDP). (Comodo s.a.)

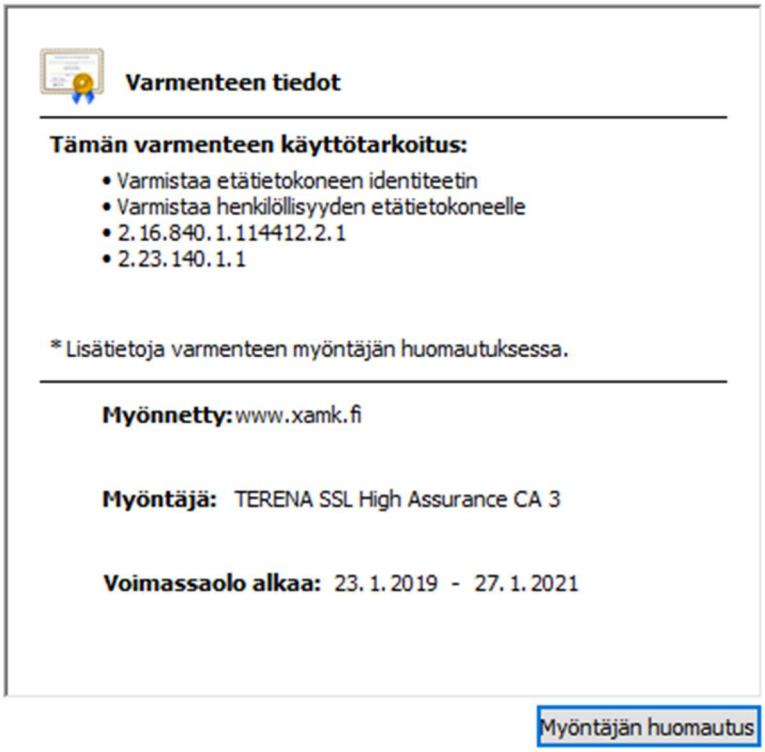
Sertifikaattipalvelimet julkaisevat CRL-listoja ajoittain, jotta hakevat osapuolet saavat tiedon onko sertifikaatti vanhentunut vai käytettävissä. CDP-listauksesta hakijat ja sovellukset tarkistavat sertifikaatin ja lataavat CRL-listalta vanhenemismerkinnän. CRL-listoissa löytyy sertifikaatin sarjanumero, joka on umpeutunut ja aikaleima, jossa on merkittynä sertifikaatin voimassaoloaika sekä mahdollinen vanhenemisen syy. CRL-listoilla kuten sertifikaateillakin on alkamisaika sekä vanhenemisaika, jolla määritetään aikaväli koska se on käytettävissä. Listoja luotaessa tulee huomioida CRL-listojen elinikä. Juurisertifikaattipalvelimelle voi määrittää pitkäikäisen CRL-listan, jos se jakaa sertifikaatteja harvoin toisille palvelimille. Johtuen useammin jaettavista sertifikaateista alemman tason sertifikaattipalvelimilta listojen elinikä voi olla lyhyempi aika. Lyhyemmän eliniän CRL-listoja tarvitaan esimerkiksi tunnistautumiseen käytettävissä käyttäjäsertifikaateissa. Uusia CRL-listoja luotaessa on huomioitava myös aikaväli, jolloin molemmat CRL-listat ovat voimassa. Sen tarkoitus on antaa CRL-listalle aikaa kopioitua hakijan säilöön ennen kuin edellinen vanhenee. (Microsoft 2009.)

Suurten CRL-listojen julkaisemisen sijaan voimassaolotiedon voi päivittää pienemmillä Delta CRL -listoilla. Delta CRL -listat kuten CRL-listat sisältävät voimassaolotiedon sertifikaateista, jotka ovat umpeutuneet viimeksi tavallisen CRL-listan julkaisun jälkeen. Delta CRL -listojen käyttö johtuu tavallisten CRL-listojen rajoituksista. Tavalliset CRL-listat voivat kasvaa suuriksi ajan myötä, koska ne sisältävät sarjanumeron sekä vanhenemisen syyn jokaisesta sertifikaatista, joka on kumottu sertifikaattiauktoriteetilla. Voimassaolevan CRL-listan haltijoiden tarvitsee ladata vain Delta CRL -lista päivittääkseen muuttuneet tiedot. CRL-listoissa määritetään, kuinka usein Delta CRL -lista julkaistaan. (Mt.)

2.4 Sertifikaatti käyttäjälle

Käyttäjälle sertifikaatin tiedot näkyvät sivustolla tai palvelussa yleensä luettavassa muodossa. Kuvasta 2 voi lukea tarkemmin kuinka paljon tietoa näkyy esimerkiksi Kaakkois-Suomen ammattikorkeakoulun sivujen sertifikaatista.

Yleisimpiä käyttäjäsertifikaatteja ovat PEM-salauksella, DER-salauksella ja PKCS-muodossa olevat sertifikaatit (Citrix s.a.).



Kuva 2. Sertifikaatin perustiedot

Kaksi yleisimpiin kuuluvaa salauskaaviota X.509-sertifikaateille ovat PEM- sekä DER-salausmenetelmä. PEM-salaus (Privacy Enhanced Mail) on yleisin käytössä oleva salausmenetelmä sertifikaattitiedostojen salaukseen, jossa toteutus tapahtuu salaamalla sisältö käyttäen Base64-koodausta. Base64-koodaus on menetelmä, jolla tietoliikenne salataan radix-64 -esityksellä (jokainen Base64 koodattu merkki edustaa kuutta tavua dataa) (Mozilla 2020). PEM-salattuja sertifikaatteja tuetaan suuressa määrin kaikissa sovelluksissa. PEM-salauksella sertifikaattitiedoston pääte on ”.pem”.

DER (Distinguished Encoding Rules) on toinen yleinen salausmalli sertifikaattitiedostoille. DER-säännöt pohjautuvat BER-salauksen rajoituksiin. DER-säännöissä jätetään jäljelle vain yhden lähettäjän asetukset. (RFC 1421

1993.) DER-salauksella toteutetut sertifikaatit ovat binääritiedostoja, jotka eivät ole tekstieditorilla luettavassa muodossa. DER-salauksella toteutettujen sertifikaattien pääte on .cer, .der ja .crt. (Google 2008.)

3 X.509-STANDARDI

X.509-standardin käyttäminen perustuu tasojärjestelmälliseen infrastruktuuriin ja se jaottuu tasoille 1, 2 ja 3. Infrastruktuurin tasolla yksi on Internet Policy Registration Authority (tästä eteenpäin IPRA), joka toimii pääsääntöisesti PEM-hierarkian juuressa. Se jakaa sertifikaatteja ensisijaisesti PCA-auktoriteeteille. IPRA:n julkinen osuus perustuu jokaisen sertifikaatin validointiin sen hierarkiassa. Tämän tarkoitus on varmentaa kaikki PCA-auktoriteetit tarkistaen niiden toimivan IPRA:n laatiman toimintapolitiikan mukaan. IPRA varmistaa pelkästään PCA:t eikä CA-auktoriteetteja tai käyttäjiä. Jokaisen PCA:n täytyy hakea kuvaus IPRA:n ehdotetusta toimintapolitiikasta. Kuvauksen kopio varmennetaan IPRA:ssa PEM-muotoon, sekä se jaetaan sähköisenä jakeluna IPRA:n toimesta. Tämä käytäntö on toiminnassa, jotta jokaisella käyttäjällä olisi lähtökohta sertifikaattien jakelussa käytössä oleviin käytäntöihin, joita käyttäjä saattaa kohdata. Digitaalisesti allekirjoitetun kopion olemassaolo varmistaa tietojen muuttumattomuuden. IPRA:n jakamalla sertifikaatilla sekä julkaisemalla toimintamenetelmädokumentti PCA ratifioidaan toimimaan hierarkiassa. (RFC 5280 2008.)

Tasolla kaksi on Policy Certification Authority (PCA). Julkisten avainten käytössä vaaditaan luottamussuhde salatun avaimen omistamalta taholta varmistamaan, että tämä taho on oikea. Tämä onnistuu käyttäen julkisen avaimen sertifikaatteja, jotka kiinnittävät julkisten avainten arvot kohteisiin. Liitos luodaan luotetulla sertifikaattipalvelimella, joka allekirjoittaa jokaisen sertifikaatin digitaalisesti. Sertifikaattipalvelin voi tehdä avain parituksen joko tarkistaessa vastaanottavaa osapuolta tai salaisen avaimen osoituksen myötä. Sertifikaatit ovat määräaikaisia, joka näkyy yleensä sertifikaatin tiedoissa (kuva 2). (Mt.)

3.1 Sertifikaattiavaimen luonti

Sertifikaattipohjainen laitetodennus tapahtuu useimmin salainen avain / julkinen avain -menetelmällä. Salainen avain luodaan palvelimella tai laitteella,

kun varmennusta pyytävä laite lähettää sertifikaatin allekirjoituskyselyn jakavalle palvelimelle. Sertifikaatin allekirjoituskysely (CSR) lähetetään julkisen avaimen luonnissa sertifikaattiauktoriteetille, joka luo sen perusteella julkisen avaimen pariksi salaiselle avaimelle vaarantamatta salaista avainta. (Digicert 2018.)

Sertifikaattiauktoriteetilla ei koskaan ole pääsyä salaiseen avaimeen. Salattu avain pysyy palvelimella tai laitteella eikä sitä jaeta missään tapauksessa. Julkinen avain sisällytetään SSL-sertifikaattiin ja se jaetaan eteenpäin muille tahoille esim. selaimelle, mobiililaitteelle tai palvelimelle. SSL-sertifikaatti koostuu julkisesta sekä salaisesta avaimesta. (Mt.)

3.2 Symmetriset avainparit

Symmetristen salausmenetelmien periaatteena toimii yksi avain, joka on jaettu kahden tai useamman tahon kanssa. Samaa avainta käytetään sekä salattaessa että salausta purettaessa ns. plain text -muotoon, joka on viesti salaamattomassa muodossaan (Binance academy s.a.). Salausprosessi koostuu alkuperäisen viestin kirjoittamisesta algoritmin läpi useita kertoja. Näitä algoritmeja ovat esimerkiksi Vigeneren salaus ja Advanced Encryption Standard (AES). AES on lohkosalausmenetelmä, joka hyödyntää symmetristä avainparia.

Symmetrisessä parissa avain luodaan selaimella, joka yhdistää palvelimelle. Yhteysavaimen koko on yleensä 128 tai 256 bittiä. Avaimen koko vaikuttaa siihen kuinka vahva salaus on. Symmetrisellä avaimella tapahtuu tiedon purkaminen sekä salaaminen SSL-yhteyden aikana. (Digicert 2018.)

Symmetrisiä avainpareja käytettäessä kestävän avaimen luonti on tehokasta. Avaimien koko on yleensä pienempi suhteessa saatuun tietoturvan tasoon. Symmetrisen kryptografian implementointi varsinkin laitetasolla voi olla erittäin tehokasta, koska salauksen purkaminen sekä salaaminen eivät kuormita järjestelmää suuresti. Koska salaus ei ole purettavissa kuin yhdellä symmetrisellä avaimella, symmetrinen kryptografia tuo myös lievää varmistusta datalle, jos avain pysyy kahden osapuolen välillä turvassa. (IBM 2017.)

Symmetristen salausmenetelmien turvallisuus perustuu siihen, kuinka hankalaa avaimen koodin purkaminen hyökkääjälle on. esimerkkinä 128-bittisen avaimen murtamiseen menisi teoriassa useita miljardeja vuosia. Mitä suurempi avaimen koko on, sitä vaikeampaa sen murtaminen on. Avaimia, joiden pituus on 256 bittiä, pidetään erittäin turvallisina. Todennäköisesti ne kestävät nykyään jopa kvanttitietokoneen ”brute force” -hyökkäyksen. (Binance academy s.a.)

Symmetrisiä salausalgoritmeja käytetään useissa nykyaikaisissa tietojärjestelmissä edistämään datan sekä käyttäjien turvallisuutta ja yksityisyyttä. AES:ia hyödynnetään laajasti sekä viestintä sovelluksissa, että pilvipalveluissa. AES on implementoitu suoraan tietokonejärjestelmiin. Laitepohjainen symmetrinen salausmenetelmä hyödyntää AES 256 -salausprosessia, jota on muokattu versio tavallisesta 256-bittisestä AES-salauksesta. (Mt.)

Kaksi nykypäivänä yleisimmin käytössä olevaa symmetrisen salauksen menetelmää ovat Block- ja Stream-menetelmä. Block-salauksessa datatietue salataan ennalta määritettyyn kokoon (datablock) ja jokainen pala salataan käyttäen avainta sekä salausalgoritmia. (Mt.)

3.3 Asymmetriset avainparit

Asymmetrinen salausmenetelmä, joka tunnetaan myös julkisen avaimen kryptologiana, on suhteellisen uusi menetelmä verrattuna symmetrisiin salausmenetelmiin. Asymmetrisissä salausmenetelmissä käytetään kahta avainta salaamiseen. Salaisia avaimia vaihdetaan internetin tai suuren verkon yli. (SSL2BUY s.a.)

Avaimien turvallisuudesta tulee huolehtia koska jokainen, joka omistaa salaisen avaimen pystyy purkamaan salatun liikenteen. Tästä syystä asymmetrisessä salausmenetelmässä käytetään kahta avainta. Julkinen avain on saatavilla kaikille, jotka haluavat salatun viestin purkaa. Viesti, jonka salaus halutaan purkaa, on purettavissa vain käyttämällä parin toista avainta. Salaisella avaimella puretaan julkisella avaimella salattu viesti ja julkisella avaimella pu-

retaan salatun avaimen salaama viesti. Julkisen avaimen tietoturva ei ole pakollista, koska se on julkisesti saatavilla ja siirrettävissä verkon välityksellä. Asymmetrisellä avainparilla on parempi kestävyys varmistamaan salatun tiedon siirtyminen. Asymmetristä salausmenetelmää käytetään päivittäisessä tietoliikenteessä erityisesti internetissä. Yleisimpiä asymmetristen salausmenetelmien algoritmeja ovat ElGamal, RSA, DSA ja PKCS. (Mt.)

Asymmetriseen avainpariin kuuluu 2048-bittinen SSL-sertifikaatti. Tiedon salaamiseen käytetään salausavainta palvelimelta ja SSL-sertifikaattia tai vaihtoehtoisesti julkista avainta. Tiedon purkamiseen käytetään salaista avainta, joka on palvelimella. (IBM 2017.)

4 SERTIFIKAATTIAUKTORITEETTIEN PARHAITA KÄYTÄNTÖJÄ

Sertifikaattien käytössä kannattaa arvioida käyttötarve, joka määrittelee sen, käytetäänkö julkista sertifikaattia vai auktorisoidaanko se itse. Yleisesti ottaen parhaisiin käytäntöihin vaikuttaa tietoturvallisuus, tiedon yksityisyys ja datan eheys. Tärkeinä osina PKI-ympäristön käyttöönotossa tulee huomioida ympäristön huolellinen suunnitteleminen, testaaminen ja toimenpiteiden tarkka dokumentointi. PKI-ratkaisusta on hyötyä, jos käytetään toimialueen sisäistä kaksivaiheista tunnistautumista (MFA) tai WWW-palvelimen sertifikaattia. (Keyfactor 2019.)

ADCS-asennuksen jälkeen sertifikaattipalvelimien nimiä ei kannata muuttaa, jotta julkaistut sertifikaatit pysyvät voimassaolevina. Sertifikaattipalvelimille kannattaa järjestää oma dedikoitu palvelin eli sitä ei kannata asentaa osaksi domain controller -palvelinta. (Serre 2014.)

Juurisertifikaattipalvelin on PKI-ympäristön tietoturvallisuuden kannalta mahdollisuus ja samalla riski. Ellei PKI-ympäristön tietoturvallisuudesta pidetä huolta, se tulee pitää pois päältä tai pois toimialueesta tai pois verkoista. Jos Juurisertifikaattipalvelimen salainen avain joutuu hyökkääjille, koko ympäristön luotettavuus on menetetty heti. Tämän takia PKI-ympäristön suunnittelu on erityisen tärkeää. Parhaisiin käytäntöihin kuuluu, että juurisertifikaatin salainen avain tulee pitää, niin ettei se ole saatavissa sähköisessä jakelussa. (Mt.)

Jakelusertifikaattipalvelin tulee juurisertifikaattipalvelimen tapaan toteuttaa komentokehoteasennuksella. Parhaiden käytäntöjen mukaan salaisen avaimen olisi syytä olla erikseen tallennettuna eri palotilassa tai sijainnissa. Sama vaatimus, joka koskee juurisertifikaatin salaista avainta ei koske jakelusertifikaatin salaista avainta koska sitä voidaan tarvittaessa käyttää palveluiden varmentamisessa. Jakelusertifikaattipalvelin voidaan määritellä jakamaan sertifikaatteja jakelupalvelimille tai käyttäjille. (Mt.)

Valmiiden sertifikaattimallipohjien käyttöä tulisi välttää ja luoda aina pohjista omat kopioidut sekä tarpeeseen sopivasti konfiguroidut versiot. Esimerkkinä web-palvelin, jolle valmiista mallipohjasta tehdään räätälöity kopio käyttötarpeen sekä tietoturvallisuuden mukaan. Sertifikaattijakelulistojen AIA-auktoriteettien sekä OCSP määritellään muuttamaan oletusarvoiset polut toisiin. (Mt.)

Sertifikaattien voimassaoloajasta on ollut keskustelua syyskuussa 2019, jolloin CA/Browser-foorumissa päädyttiin kompromissiin. Kaksi vuotta riittää tällä hetkellä (The SSL Store 2019). Verkkopalvelimille jaettuihin sertifikaatteihin sekä vastaaviin kriittisiin infrastruktuuripalveluihin on silti suositeltavaa käyttää vuoden tai vähemmän mittaista voimassaoloaikaa.

4.1 On-Premise CA

On-Premise CA on yrityksen paikallinen sertifikaattipalveluympäristö. Perinteisessä Windows-palvelinympäristössä juurisertifikaattipalvelu rakennetaan yhteen palvelimeen. Sieltä sertifikaatti jaetaan alempaan sertifikaattipalvelimeen, josta käyttäjä saa oman henkilökohtaisen sertifikaatin, jolla varmentaminen palveluiden sisäänkirjautumiseen todennetaan. (Microsoft 2009.)

On-Premise CA -ratkaisuissa on yleensä vähintään yksi juurisertifikaattipalvelin ja yksi sertifikaatteja jakava palvelin. Parhaisiin käytäntöihin kuuluu jättää juurisertifikaattipalvelin Active Directorystä ja virroista pois. Jos sertifikaattiympäristön juuren luottamus menetetään, pitää se rakentaa alusta lähtien uudestaan. Juurisertifikaattipalvelin nostetaan ylös vain silloin, kun jakelupalvelimille tarvitsee jakaa uusi sertifikaatti. (Mt.)

Juurisertifikaattipalvelinta pystytään käyttämään virtuaalikoneena virtualisointialustan kautta omasta verkostaan, jolloin sertifikaattien hierarkiassa alaspäin toteutetaan jakamalla sertifikaatti USB-tikulla tai virtualisointialustan salliessa sisäisellä tiedostojen siirrolla.

4.2 CA as a service

Kun hankitaan sertifikaatit palveluna, pyritään varmistamaan juurisertifikaattipalvelimen luotettavuus. Palveluna hankittaessa ei tarvitse itse käyttää laiteresursseja pki-ympäristön luomiseen. Palveluna hankitulla sertifikaatilla (CA as a service) on mahdollisuus rakentaa teknisesti samanlainen sertifikaattipalveluratkaisu kuin On-Premise-mallilla. Palveluna hankittu sertifikaattipalvelu toimii ilman ylimääräisiä hallittavuuden tai teknologisen osaamisen tarpeita, joita On-Premise-ympäristössä tarvitaan. (Globalsign. s.a.)

AWS Certificate Manager Private Certificate Authority (ACM PCA) on pilvipohjainen sertifikaattipalvelualusta, jota voi hyödyntää yrityskohtaisen sertifikaattipalvelun luomisessa käytettäessä Amazon Web Services -pilvipalveluita. ACM PCA hyödyntää AWS Certificate Managerissa käytettäviä julkisten avainten menetelmiä ja mahdollistaa niiden käytön myös sisäiseen sertifikaatinjakeluun. ACM PCA:n kautta luotuja sertifikaatteja käytetään käyttäjien, verkkopalvelinten, VPN-käyttäjien ja IOT-laitteiden tietoliikenneyhteyksien salaamisessa sekä identiteettien varmennuksessa organisaation sisällä. ACM PCA mahdollistaa myös kokonaisten sertifikaattihierarkioiden luomisen ilman oman sertifikaattiauktoriteetin kustannuksia. (Amazon, 2020, 6)

Palveluntuottaja tekee liiketoimintaa usein niin, että hyväksi havaitut toimintatavat tuotteistetaan ja myydään. Sertifikaattiauktoriteetti voi siis tuotteistaa sertifikaattinsa ja toimittaa ne palveluna kuten esimerkiksi toimivat Amazon, Globalsign ja Verisign. Microsoftilta tämänlaista palvelua ei ole saatavilla, koska Microsoft hyödyntää X.509-pohjaista sertifikaattia Microsoft-palveluiden sisäisesti On-Premise-ympäristössä.

5 TESTIYMPÄRISTÖN TOTEUTUS

Tarkoituksena oli selvittää, miten toteutetaan käytännössä yrityskohtainen sertifikaattijärjestelmä. Pyrkimys oli ottaa käyttöön tekninen ympäristö, jossa sertifikaattipalvelu toteutetaan paikallisena On-Premise-asennuksena.

Testiympäristöä lähdettiin toteuttamaan niin, että tavoitteena oli ottaa käyttöön yksi domain controller -palvelin, kaksi sertifikaattipalvelinta, kytkin ja yksi testityöasema. Testin tarkoitus oli päästä testaamaan sertifikaattien jakelua. Kahden sertifikaattipalvelimen tehtävät oli jaettu niin, että toinen on juurisertifikaattipalvelin ja toinen jakelusertifikaattipalvelin. Kun domain controller -palvelin ja sertifikaattipalvelimet olivat asennettu, testattiin sertifikaatin jakelu sertifikaattipalvelimien välillä. Tämän jälkeen havaittiin, että tarvitaan lisäksi vielä testityöasema, jolla voidaan testata sertifikaatin jako loppukäyttäjälle. Lisäsin testityöaseman toimialueelle, testityöasemalla haettiin jakelusertifikaattipalvelimen sertifikaatti käyttäen Windowsin Microsoft management konsolin (MMC) certmgr -työkalua.

Toteutuksen aikana ensimmäinen testiympäristö nollaantui ilmeisesti ICTLABin virtual lab -ympäristön päivityksen tai laboratorion aikavarauksen täyttymisen johdosta. Toisessa testiympäristössä sertifikaattijärjestelmän perustoimintojen käyttöönoton jälkeen domain controller -palvelin nollaantui selittämättömästä syystä. ICTLABin virtual lab -ympäristössä on kannattavaa ottaa varmuuskopioita toteutuksista. Ohjaavan opettajan pyynnöstä toteutettiin ICTLABin virtual lab -ympäristöön WWW-palvelimen, joka hyödyntää SSL-sertifikaatteja.

5.1 Testiympäristön suunnittelu

Ympäristön suunnittelu tapahtui hyödyntämällä Microsoftin server certificate deployment planning- sekä core network components -ohjeita. Microsoftin ohjeita ja työpaikalla käytännössä opittuja tietoja käyttämällä päädyttiin luomaan suunnitelma ratkaisusta, jolla voidaan luoda sertifikaatteja ja jaella niitä sekä testata sertifikaattien toiminta.

Suunnitelman mukaan tarkoitus oli määritellä ratkaisu ja toteuttaa ratkaisun mukainen Xamkin ICTLABin virtual lab -ympäristö, jossa toteutus ja testaus

voidaan suorittaa. Määrittely tapahtui jaetun hierarkian pohjalta, ettei topologiasta tule käyttötarkoitukseen liian monimutkaista tai jäykkää.

Testaus aloitettiin käyttöönotetussa ympäristössä jakamalla sertifikaatti seuraavalle osapuolelle, jossa testattiin sertifikaattipalvelimien välinen hierarkia ja sertifikaatin oikeellisuus. Tällä oli tarkoitus testata juurisertifikaattipalvelimen ja jakelusertifikaattipalvelimen välistä yhteyttä. Jakelupalvelimella luotiin jakelupiste, joka testattiin loppukäyttäjän sertifikaatin hakeminen sekä sertifikaatin oikeellisuus. Testaus toteutettiin luomalla sertifikaatin jakelupiste ja testaamalla sen toimivuus muiden kokoonpanon osien kanssa.

5.2 Teknisen ympäristön implementointi

Toteutuksen implementointi aloitettiin luomalla ympäristöön kolme Windows-palvelinta sekä yksi työasema, näille palvelimille lisättiin roolit Active Directory Domain Services, Certificate Authority, DHCP ja DNS. Palvelimet alustettiin ensin SYSPREP-komennolla, etteivät niiden Security ID:t ole identtisiä estäen toteutuksen. ICTLABin virtual lab -ympäristössä palvelimien templatet ovat identtisiä ja siitä seuraa, että Security ID:t pitää muuttaa ennen toimialueeseen liittämistä. WWW-palvelimen ja loppukäyttäjän välisen salatun yhteyden muodostamiseksi luotiin webpalvelin, jolle jaettiin vlab web server -sertifikaattimallista sertifikaatti salattua yhteyttä varten. Työasemaa käytettiin toteutuksen sertifikaattijakelun ja toimivuuden testaamiseen.

Palvelinympäristössä tarvittavat roolit Active Directory Domain Services, Certificate Authority, DHCP ja DNS ovat keskeisiä sertifikaattitoteutuksen luomisessa. Active Directory Domain Services tarvitaan, jotta Windows-koneet yhdistyvät saman toimialueen alle mahdollistaen yrityskohtaisen toimialue toteutuksen. Sertifikaattiratkaisua ei voi toteuttaa ilman ADDS-palvelua. CA-roolin merkitys on keskeinen sertifikaattijakelussa, sertifikaattipalvelimien sekä loppukäyttäjän kannalta. DHCP-roolin tehtävänä on jaella ennalta määritettyjen asetusten mukaisesti tietoja (helper-address) ja IP-osoitteita päätelaitteille. DNS-rooli on Active Directoryn kannalta keskeinen koska se pitää kirjaa konenimistä ja osoitteista sekä sitä hyödynnetään pääsynhallinnassa.

Testauksen yhteydessä tapahtuneiden ongelmien jälkeen saatiin lopulta toimiva testiympäristö valmiiksi. Onnistuneen testauksen jälkeen testivaiheessa kirjatuista työvaiheista laadittiin ohje sertifikaattiympäristön luomiseen.

6 YHTEENVETO

Lähtökohdat tämän työn tekemiseen olivat osaltani hyvät, koska aiempaa kokemusta sertifikaattiympäristöjen toiminnasta oli saatavilla työpaikkani tuotantoympäristössä. Sen käytössä olevia toimintamenetelmiä ja ratkaisuja pystyin analysoimaan sekä käyttämään testiympäristön suunnitelman luonnissa ja toteutuksessa.

Aluksi loin suunnitelman teknisen ympäristön toteutuksesta, jolla erilaisia sertifikaattiratkaisuita pystyi testaamaan. Käytännön toteutuksen edetessä ja testausten yhteydessä huomasin, että alkuperäistä suunnitelmaa oli muutettava. Ongelmakohdaksi osoittautui suunnittelun keveys, joka hidasti testiympäristön määrittelyä. Testiympäristöön liittyen työn tavoitteisiin päästiin vain osittain. Useiden yritysten jälkeen sertifikaattipalvelun perustoiminnallisuuden testaus onnistui. Virheellisten ja onnistuneiden yritysten jälkeen oli mahdollista luoda määritysohje sertifikaattipalveluiden käyttöönotolle. Sertifikaattiympäristön SSL-sertifikaatin jakelu toimintoa ei kuitenkaan saatu toimimaan kunnolla. Sertifikaattien jakelu ei onnistunut WWW-palvelimelle oikeassa muodossa (esim. www.domain.fi) niin, että sertifikaatti on myönnetty verkko-osoitteelle eikä palvelimen DNS-osoitteelle. Tuotantoympäristössä sertifikaatin asennus ja käyttöönotto oli onnistunut useita kertoja vastaavalla tavalla mitä testiympäristössä yritin.

Tarkoitus oli testata ja tuottaa materiaalia, jota voisi hyödyntää kurssimateriaalina. Tavoitteeseen päästiin vaikkakin opinnäytetyön kirjoittamisen loppupuoliskolla huomasin, että olisi kannattanut kysyä enemmän apua työn tekemisessä opinnäytetyönohjaajalta. Opinnäytetyön suunnan epäselvyydestä aiheutui hankaluuksia teknisen työn alustuksen luomisessa sekä aikataulussa pysymisessä. Teknisten ratkaisujen selvittämisessä en kokenut mitään vaikeuksia.

Työn tutkimusongelmana oli selvittää, miten sertifikaattipalvelujärjestelmien parhaita käytäntöjä harjoitellaan ICTLABin virtual lab -ympäristössä. Opinnäytetyön tutkimuskysymykset olivat:

- Mitkä ovat yrityskohtaisten sertifikaattijärjestelmien parhaita käytäntöjä?
- Miten sertifikaatit saadaan toimimaan erilaisissa käyttötarkoituksissa?
- Miten näitä käytäntöjä voidaan harjoitella laboratorio ympäristössä?

Työn toteutuksessa sain vastauksia tutkimuskysymyksiin seuraavasti:

- Testiympäristössä totesin että, seuraavat toiminnot toimivat hyvin ja vastaavat parhaita käytäntöjä: Auktoriteetin turvallisuudesta huolehtiminen salaisen avaimen tietoturvan valvominen, joka on ylläpitäjän vastuulla. Toimialueen laitteiden koventaminen.
- Sertifikaattien jakelukäytännöt onnistuin toteuttamaan ohjeiden mukaisesti.
- Laatimani yksityiskohtaisen ohjeen mukaan on mahdollista toteuttaa harjoitusympäristö ICTLABin virtual lab -ympäristöön.

Työtä tehdessäni perehdyin paremmin sertifikaattien toimintaperiaatteisiin sekä miten niitä pystytään hyödyntämään tuotantoympäristössä. Opin myös paljon laajemmin, miten sertifikaatit vaikuttavat verkkoympäristöissä. Implementoitaessa suunniteltua topologiaa haasteiksi osoittautui palvelininfrastruktuurin käyttöönotto, jossa määriteltiin muita palvelinominaisuuksia. Aloitustopologian sekä määrittelyiden luomisen jälkeen, voitiin aloittaa itse sertifikaattien jakeluprosessi.

Jatkokehitystä ajatellen toteutusta voisi jatkaa luomalla toimivat certificate enrollment policy web service sekä certificate enrollment web service -palvelut, jotka jäivät toteutuksessa vajaiksi. Lisäksi miten tapahtuisi esimerkiksi käyttäjien kirjautuminen käyttämällä työasemalle jaettua sertifikaattipohjaista tunnistamista Ja MFA-palvelun luominen Xamkin virtual lab -ympäristöön kirjautumista varten.

LÄHTEET

Amazon. 2020. AWS Certificate Manager Private Certificate Authority User Guide. PDF-dokumentti. Saatavissa: https://docs.aws.amazon.com/acm-pca/latest/userguide/pca-ug.pdf#PcaWelcome [viitattu 18.5.2020].

Binance Academy. s.a. What is Symmetric Key Cryptography. WWW-dokumentti. Saatavissa: https://www.binance.vision/security/what-is-symmetric-key-cryptography [viitattu 24.11.2019].

Citrix. s.a. What are the different formats of SSL certificates and how we can upload a certificate to NetScaler. WWW-dokumentti. Saatavissa: https://support.citrix.com/article/CTX213224 [viitattu 18.5.2020].

Comodo. 2018. What is SSL/TLS Client Authentication? How does it work. WWW-dokumentti. Saatavissa: https://comodosslstore.com/blog/what-is-ssl-tls-client-authentication-how-does-it-work.html [viitattu 21.04.2020].

Comodo. s.a. SSL Certificate Security Glossary. WWW-dokumentti. Saatavissa: https://comodosslstore.com/support/glossary.aspx [viitattu18.5.2020].

Digicert. 2018. What is a private key/public key pair. WWW-dokumentti. Saatavissa: https://knowledge.digicert.com/generalinformation/INFO2150.html [viitattu 29.03.2019].

Eriksson, P. & Koistinen, K. 2005. Monenlainen tapaustutkimus. Kuluttajatutkimuskeskuksen julkaisuja 4/2005. Kuluttajatutkimuskeskus. PDF-dokumentti. Saatavissa: https://helda.helsinki.fi/bitstream/handle/10138/152279/Monenlainen_tapaustutkimus.pdf [viitattu 27.03.2020].

Globalsign. s.a. Cost and Security Benefits of SaaS-based Certificate Authorities. PDF-dokumentti. Saatavissa: https://www.globalsign.com/en/resources/saas-based-ca-report.pdf [viitattu 18.5.2020].

Google. 2008. Basics of Digital Certificates and Certificate Authority. WWW-dokumentti. Saatavissa: https://sites.google.com/site/ddmwsst/digital-certificates [viitattu 30.03.2020].

IBM. 2017. Symmetric cryptography. WWW-dokumentti. Saatavissa: https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.14/gtps7/s7symm.html [viitattu 24.11.2019].

Keyfactor. 2019. PKI: The New Best Practices. PDF-dokumentti. Saatavissa: https://cdn2.hubspot.net/hubfs/408597/Keyfactor%20White%20Papers/PKI%20-%20The%20New%20Best%20Practices%20Keyfactor.pdf [viitattu 27.04.2020].

Microsoft. 2009. Designing and Implementing a PKI: Part I Design and Planning. WWW-dokumentti. Saatavissa: https://techcommunity.microsoft.com/t5/ask-the-directory-services-team/designing-and-implementing-a-pki-part-i-design-and-planning/ba-p/396953 [viitattu 14.04.2020].

Mota, S. 2016. Secure Certificate Management and Device Enrollment at IoT Scale. Aalto-yliopisto. Perustieteiden korkeakoulu. Opinnäytetyö. PDF-dokumentti. Saatavissa: http://urn.fi/URN:NBN:fi:aalto-201611025260 [viitattu 28.03.2019].

Mozilla. 2020. Base64. WWW-dokumentti Saatavissa: https://developer.mozilla.org/en-US/docs/Glossary/Base64 [viitattu 18.5.2020].

RFC 1421. 1993. Privacy Enhancement for Internet Electronic Mail: Part 1: Message Encryption and Authentication Procedures. WWW-dokumentti. Saatavissa: https://tools.ietf.org/html/rfc1421 [viitattu 30.3.2020].

RFC 5280. 2008. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. WWW-dokumentti. Saatavissa: https://tools.ietf.org/html/rfc5280 [viitattu 28.11.2019].

Serre, R. 2014. Public Key Infrastructure Part 10 – Best Practices about PKI. WWW-dokumentti. Saatavissa: https://www.tech-coffee.net/public-key-infrastructure-part-10-best-practices-pki/ [viitattu 27.04.2020].

SSL2BUY. s.a. Symmetric vs. Asymmetric Encryption – What are differences? WWW-dokumentti. Saatavissa: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences [viitattu 18.5.2020].

The SSL Store. s.a. Explaining the Chain of Trust WWW-dokumentti Saatavissa: https://www.thesslstore.com/knowledgebase/ssl-support/explaining-the-chain-of-trust/ [viitattu 27.04.2020].

The SSL Store. 2019. SSL Certificates: One Year Max Validity Ballot fails at the CA/B Forum. WWW-dokumentti. Saatavissa: https://www.thesslstore.com/blog/ssl-certificates-one-year-max-validity-ballot-fails-at-the-ca-b-forum/ [viitattu 27.04.2020].

The SSL Store. 2019. The Difference Between Root Certificates and Intermediate Certificates. WWW-dokumentti. Saatavissa: https://www.thesslstore.com/blog/root-certificates-intermediate/ [viitattu 18.5.2020].

Trcek, D. 2006. Managing Information Systems Security and Privacy. Berlin: Springer.

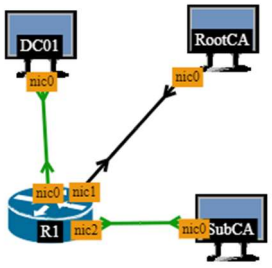
Liite 1/1

ENTERPRISE CERTIFICATE AUTHORITY MÄÄRITYSOHJE

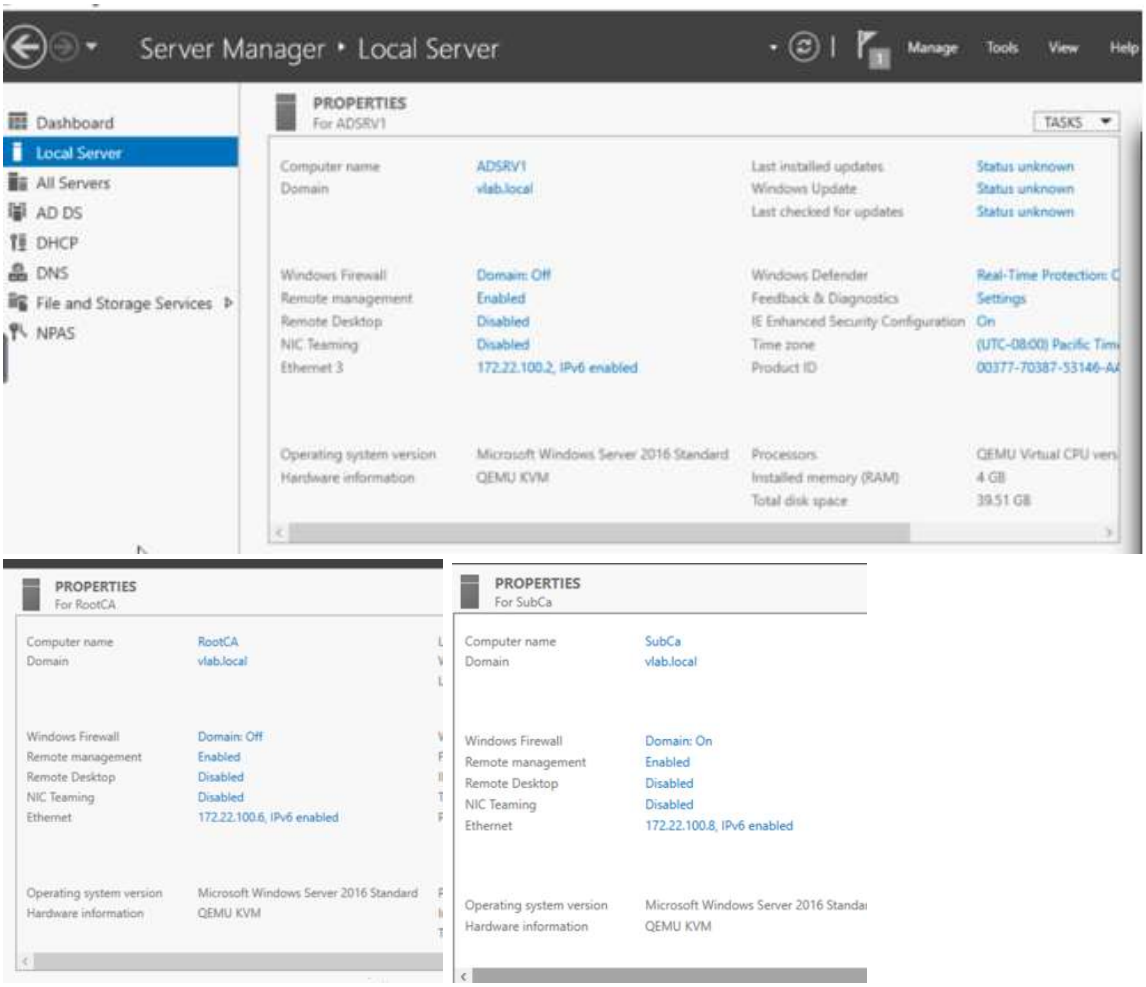
Sisällysluettelo

1. Valmistelu

Kolme palvelinta samassa domainissa yksi Domain Controller (DC01), yksi Root certificate authority (RootCA)sekä yksi Subordinate certificate authority (SubCA). Testaukseen lisätään yksi työasema jolla haetaan SubCA palvelimelta sertifikaatti.

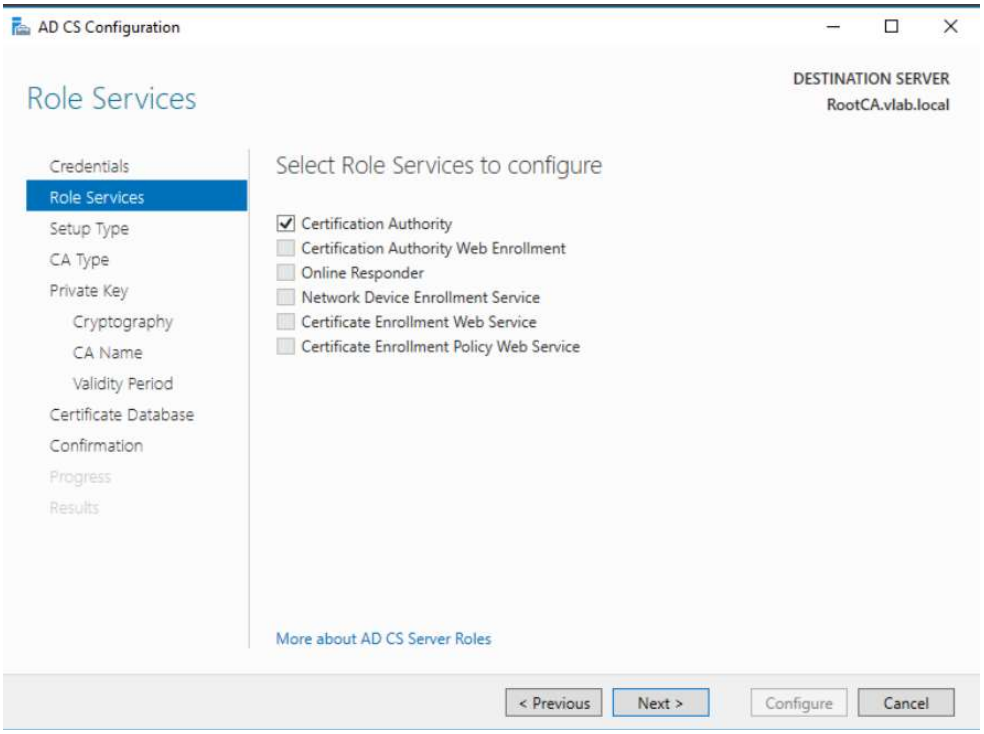


Seuraavat kuvat ovat lähtötila Domain Controllerista(ADSRV1), Root certificate authority sekä Subordinate certificate authority.

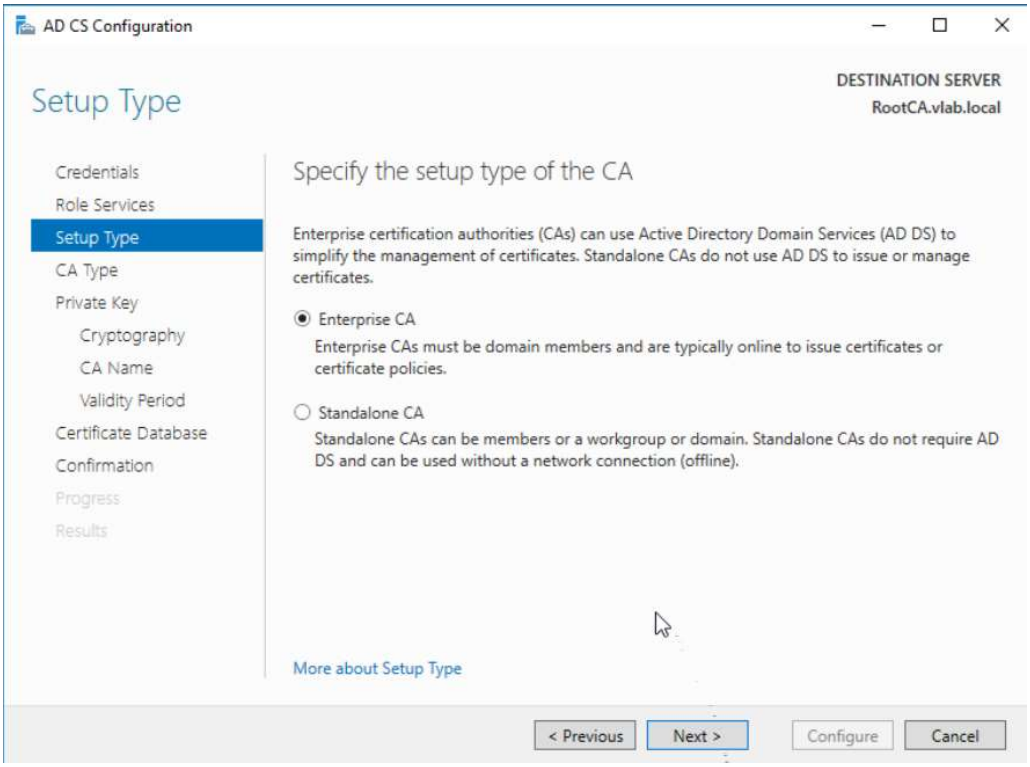


2. Root CA asennus ja alkukonfigurointi

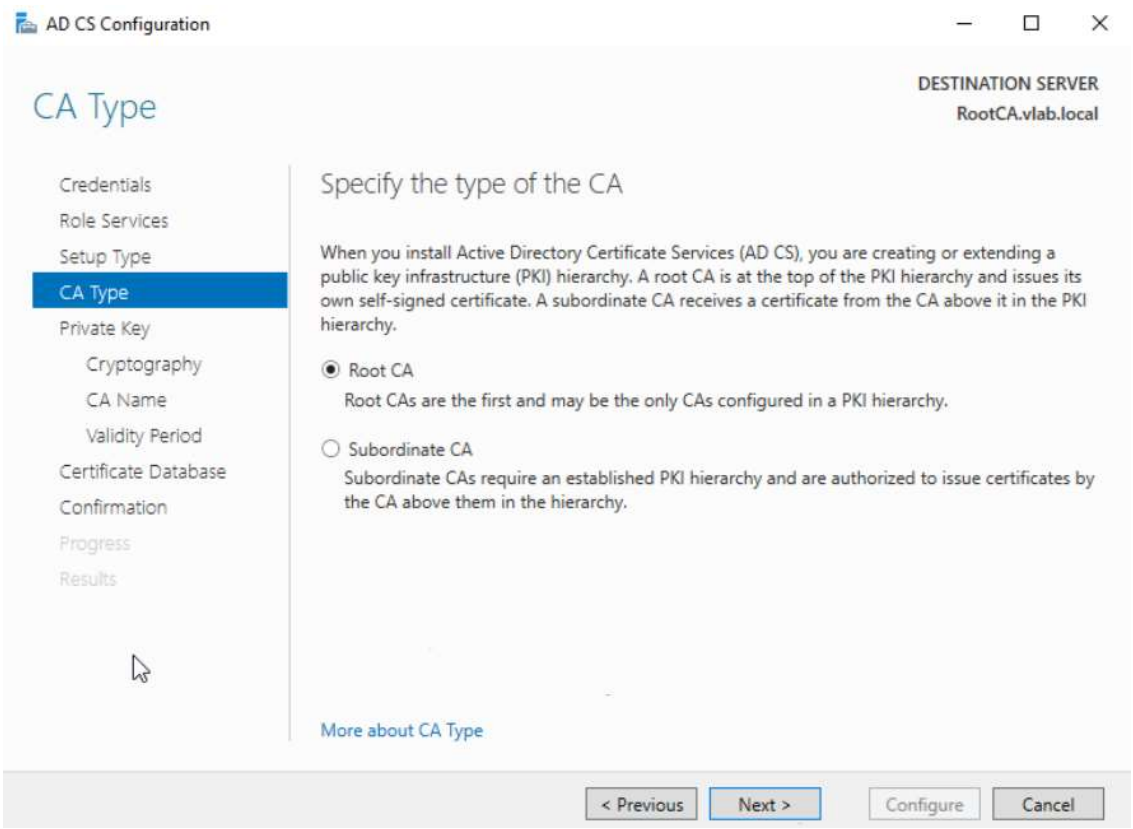
   Windows server roolia asentaessa Server Managerista valitaan Manage “add roles and features” josta aukeaa erillinen konfigurointi ikkuna. AD CS roolin asennuksen jälkeen Server Managerista klikataan lipun kohdalta lisätietoja, jossa palvelin sanoo Configure Certification Services tästä päästään AD CS konfigurointi ikkunaan.



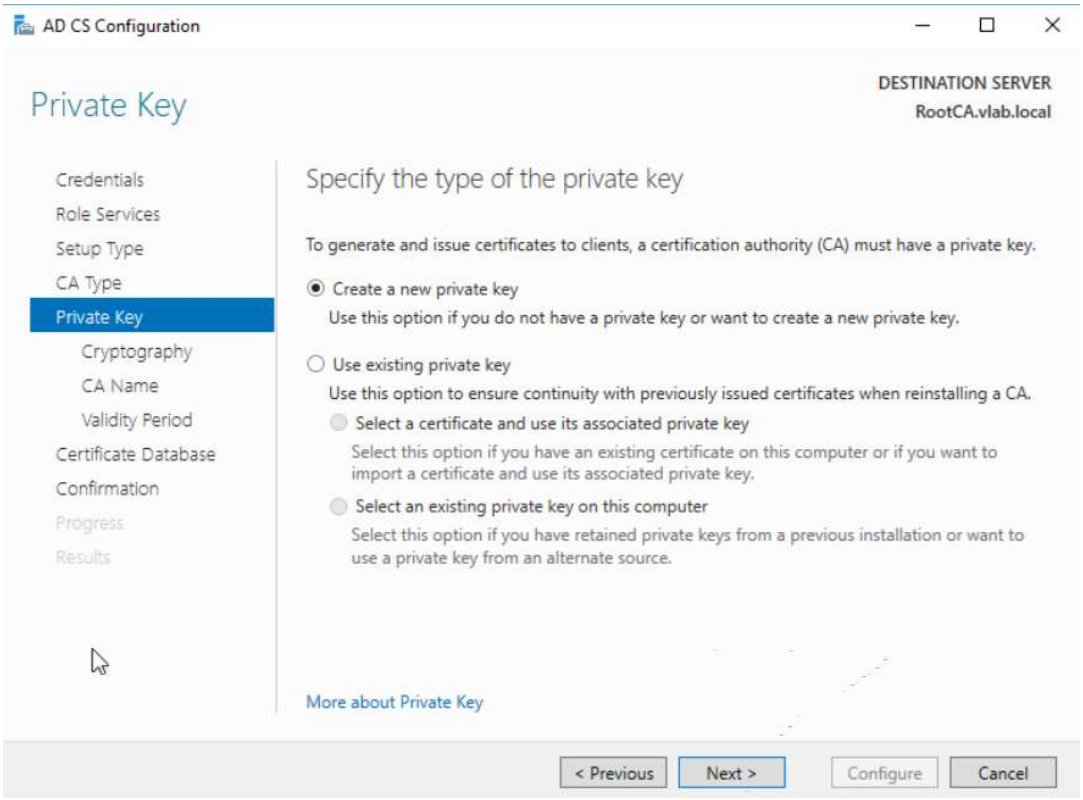
Juurisertifikaattipalvelinta asennettaessa palveluksi valitaan ”Certification Authority”, tässä voisi ottaa myös palvelut ”Certification Authority Web Enrollment” sekä Certificate Enrollment Web Service jos sertifikaatteja haluttaisiin jakaa verkon yli.



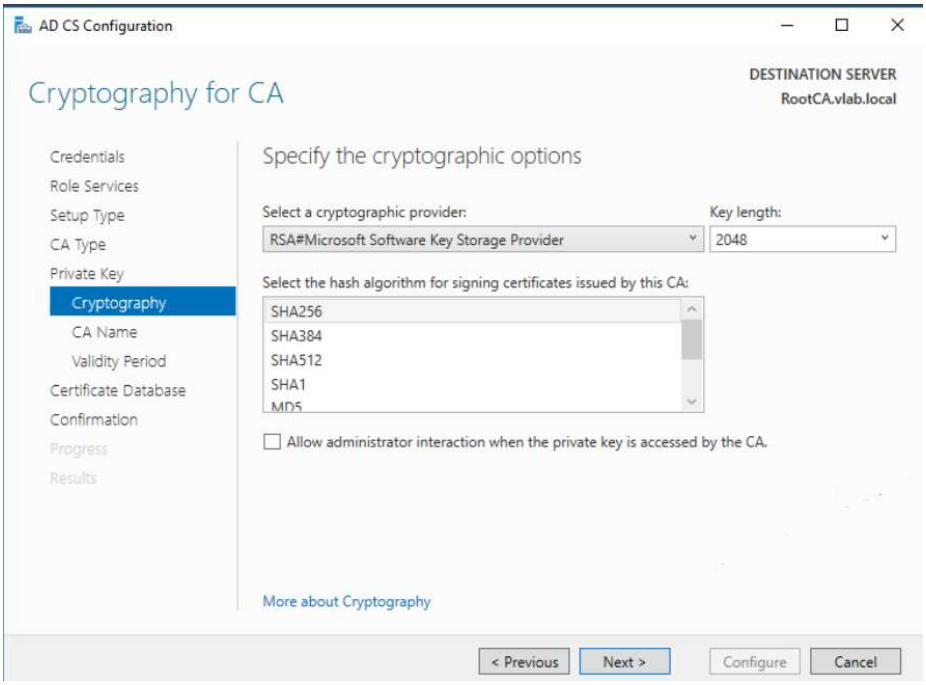
Tässä vaiheessa määritellään tehdäänkö yhden vai useamman auktoriteetin hierarkia, valitaan vaihtoehto ”Enterprise CA”, koska tarkoituksena on testata useamman auktoriteetin topologiaa.



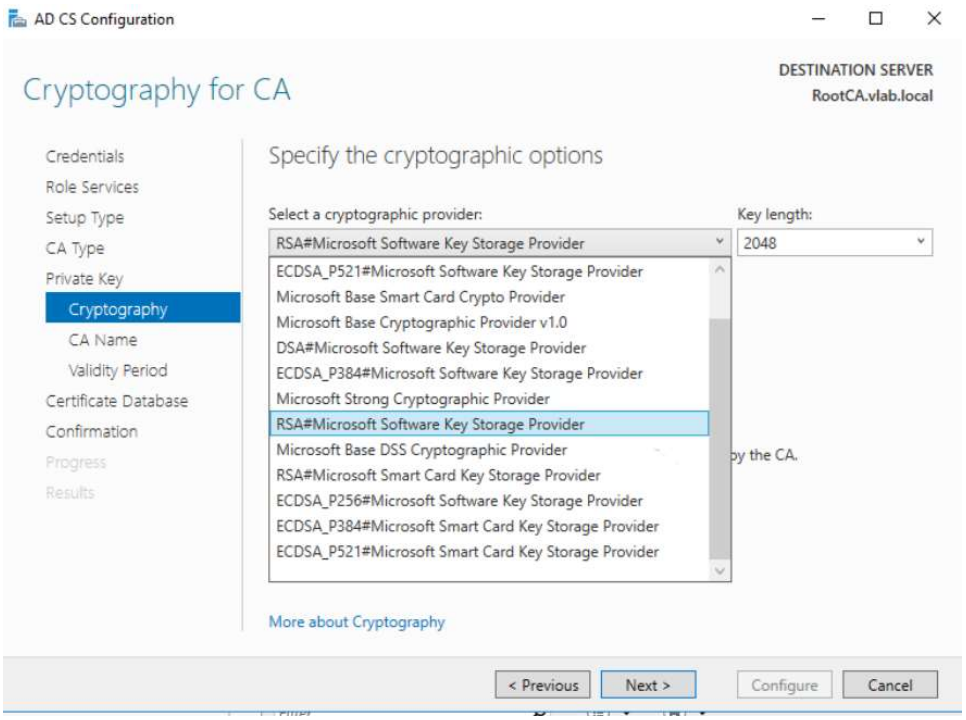
CA tyyppiä valittaessa valitse Root CA, myöhemmässä vaiheessa lisätään Subordinate CA.

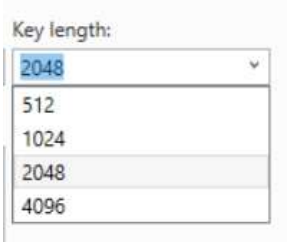


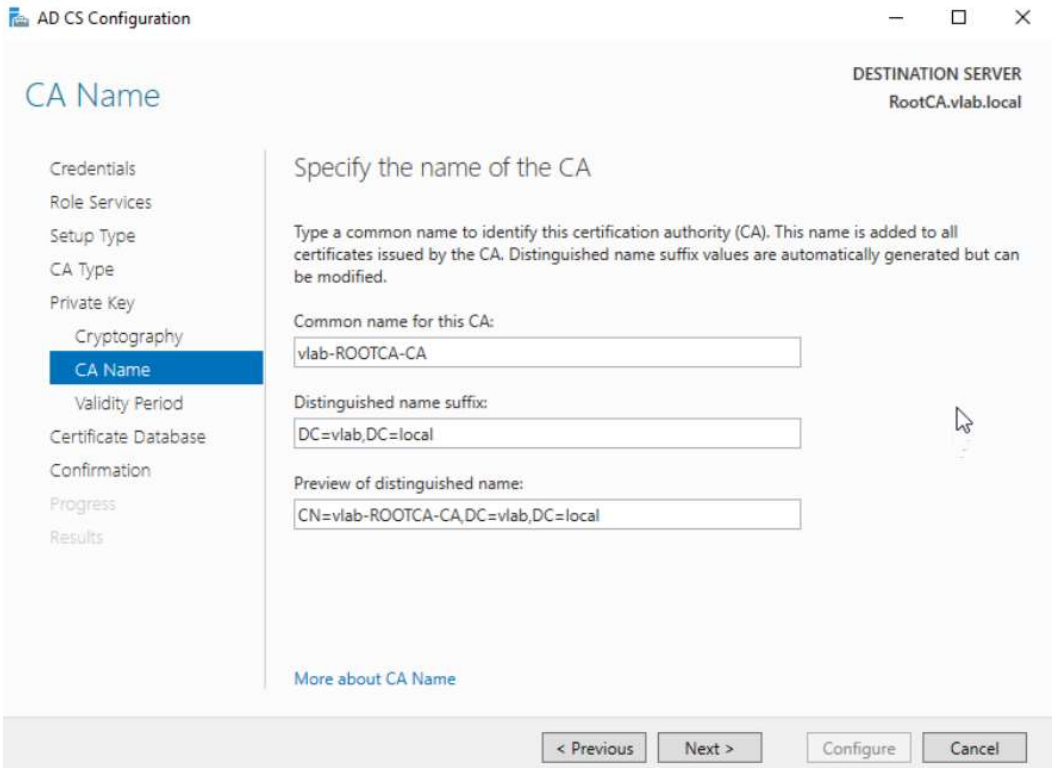
Tyhjässä asennuksessa valitsemme “Create a new private key” ellei aiempaa avainta ole käytettävissä.



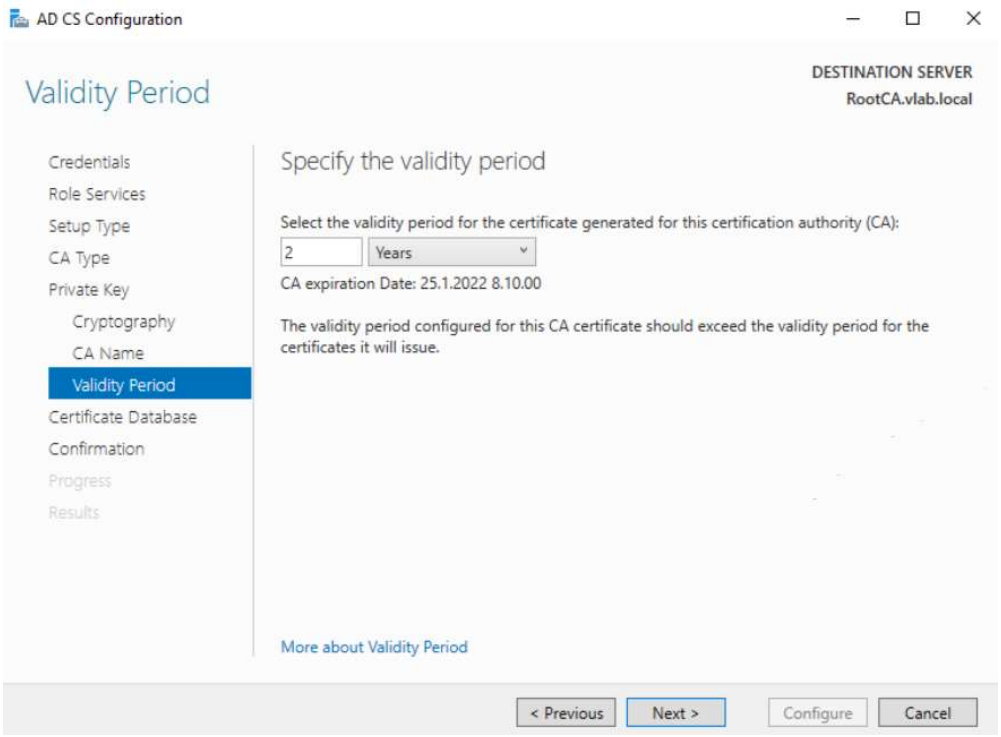
Avaimen kryptografia asetuksissa oletuksena on SHA256 hash sekä 2048-bittinen RSA tässä on valittavina myös muita vaihtoehtoja mutta menemme toteutuksessa oletusarvoilla.



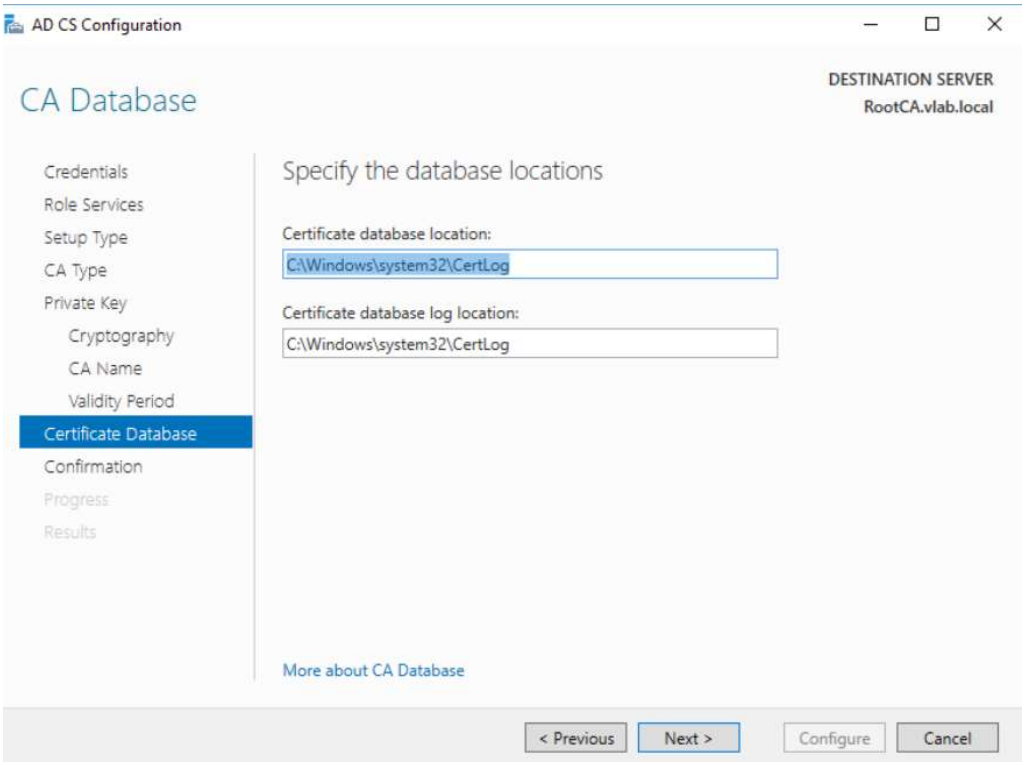




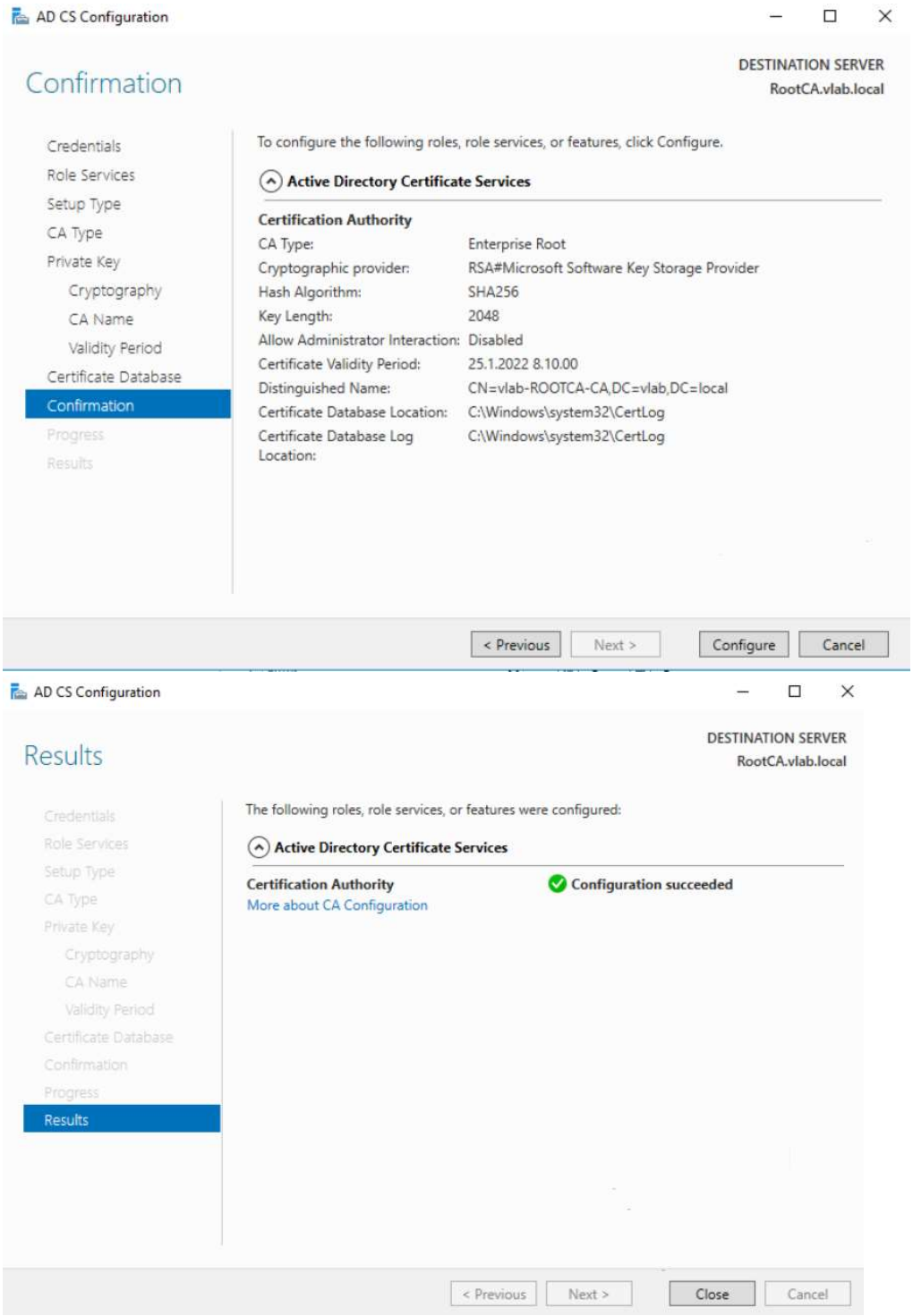
CA:n nimeäminen toimialueen nimeämispolitiikan mukaan.



Määritellään sertifikaattipalvelimen sertifikaattien voimassaoloaika tämä on oletuksena kaksi vuotta.

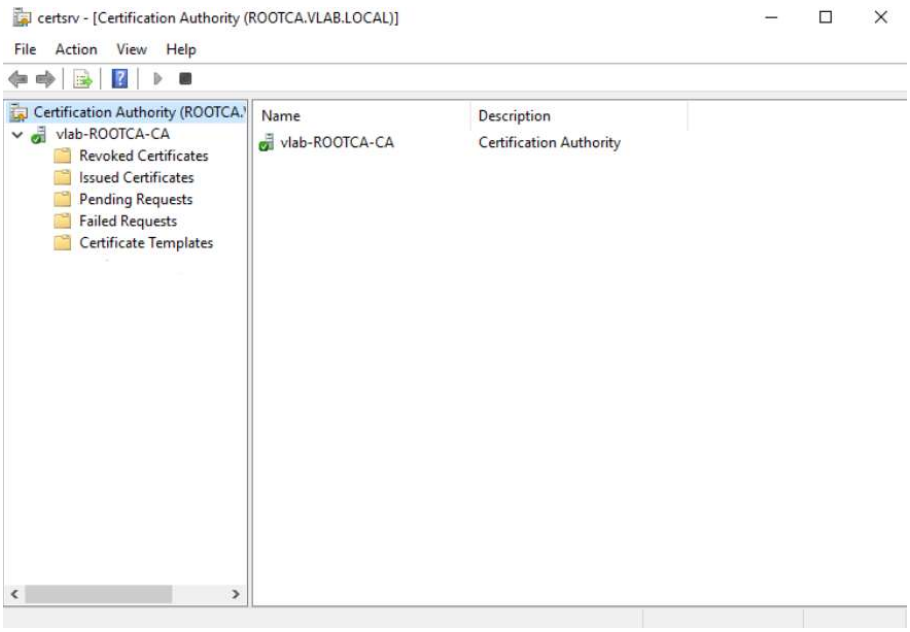


Sertifikaattien tietokannan määrittäminen oletuksilla, tämä on eri paikka kuin mistä sertifikaatit jaetaan.

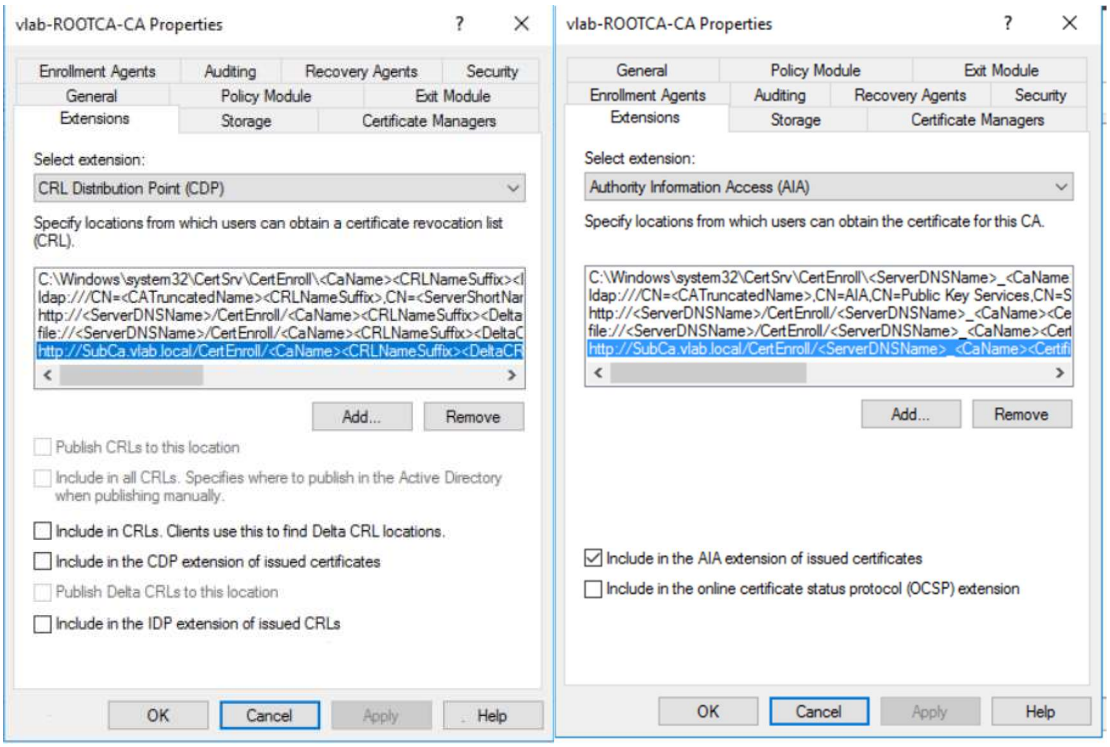


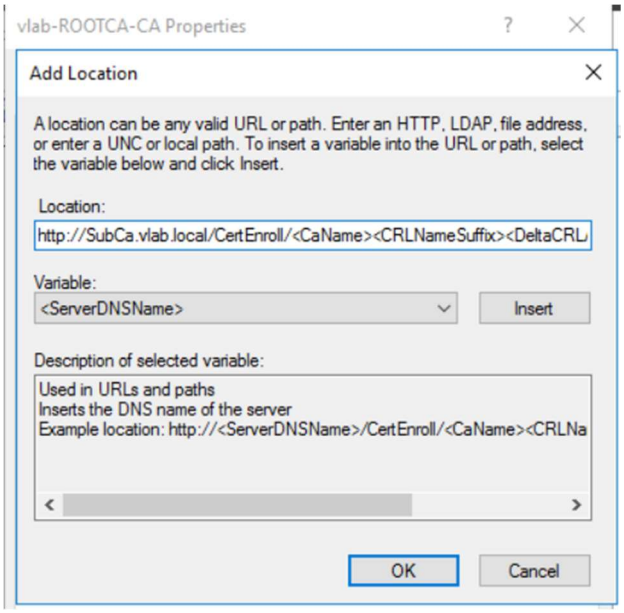
RootCA-palvelin asennuksen jälkeen

3. Juurisertifikaattipalvelimen jakelupisteen luonti

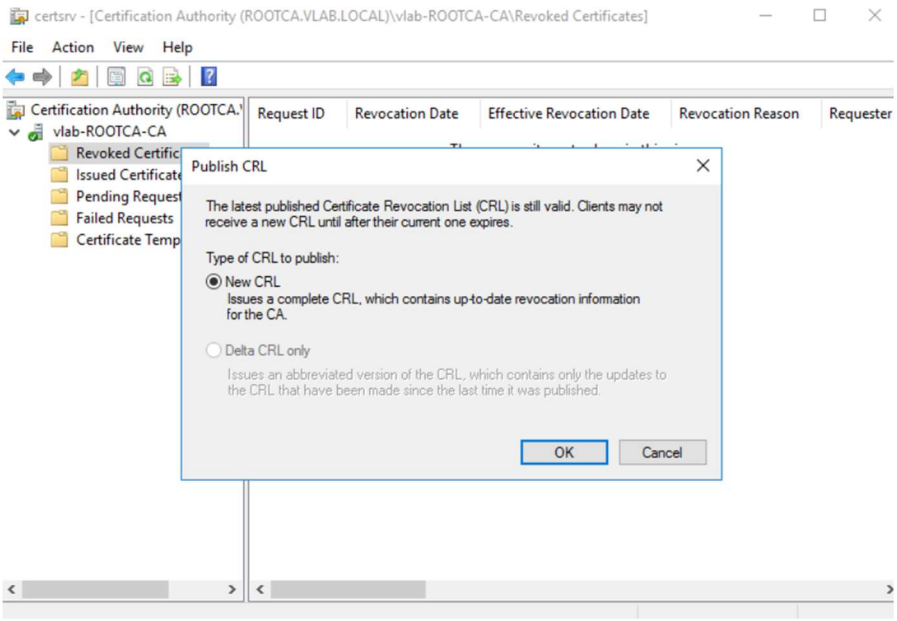


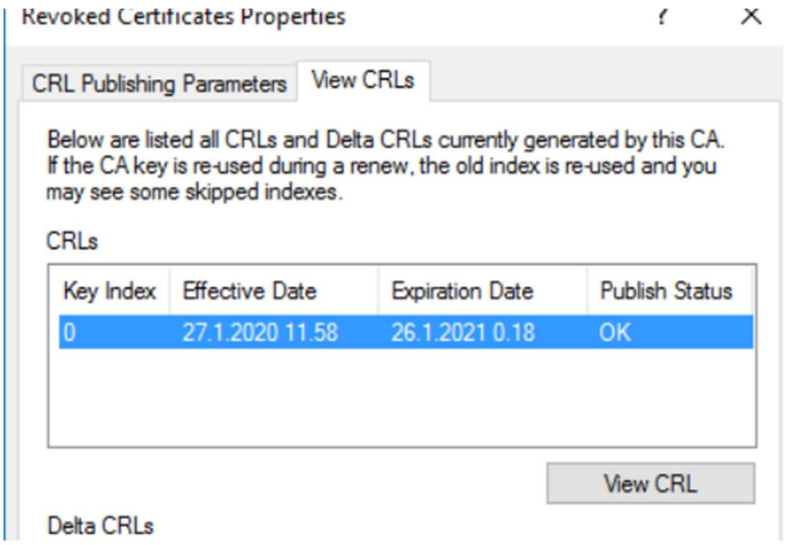
Avataan sertifikaattipalvelimen ominaisuudet nimen kohdalta hiiren oikealla painikkeella.





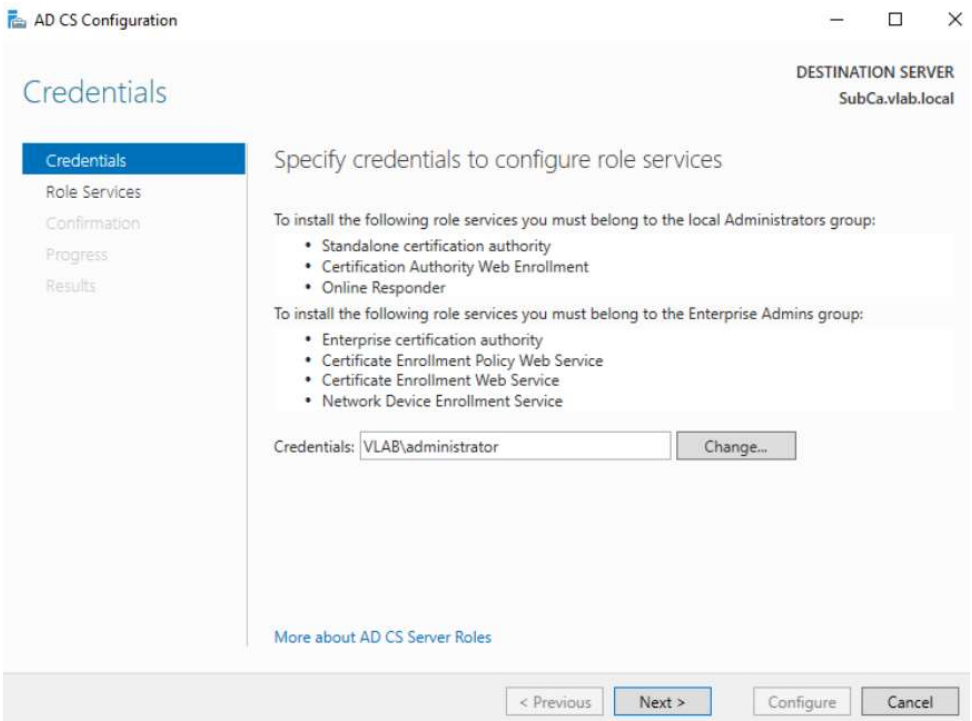
Määritellään palvelimen ominaisuuksista CDP sekä AIA sisältämään jakelu-palvelimen sertifikaattien verkkojako sekä asetukset niin että juurisertifikaatti-palvelimen sertifikaatin löytää jakelusertifikaattipalvelimelta.



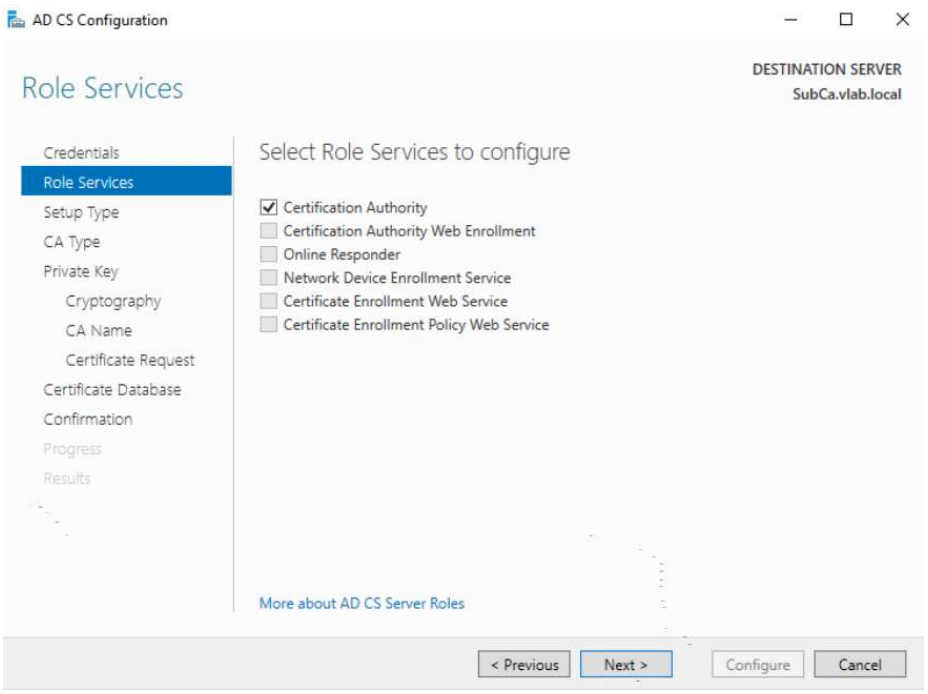


CRL julkaistaan juurisertifikaatti palvelimelta painamalla hiiren oikealla painikkeella kohdasta ”Revoked Certificates” ja ”All Tasks” ”Publish”. Kuvasta havaitaan että CRL on onnistuneesti julkaistu ja voimassa oleva vuoden.

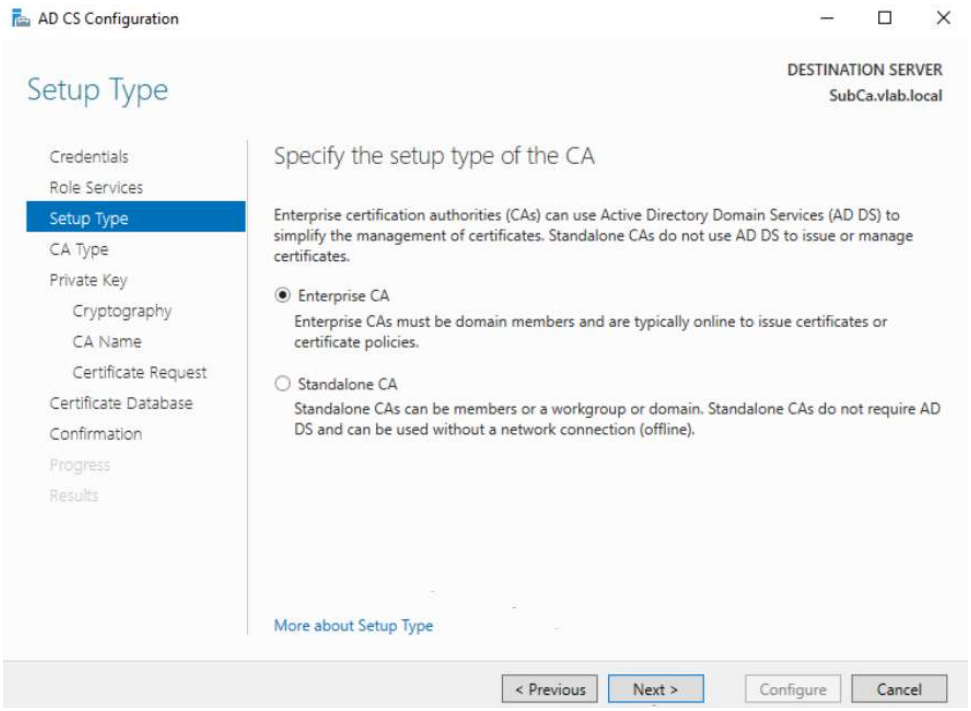
4. Subordinate certification authority alkukonffi

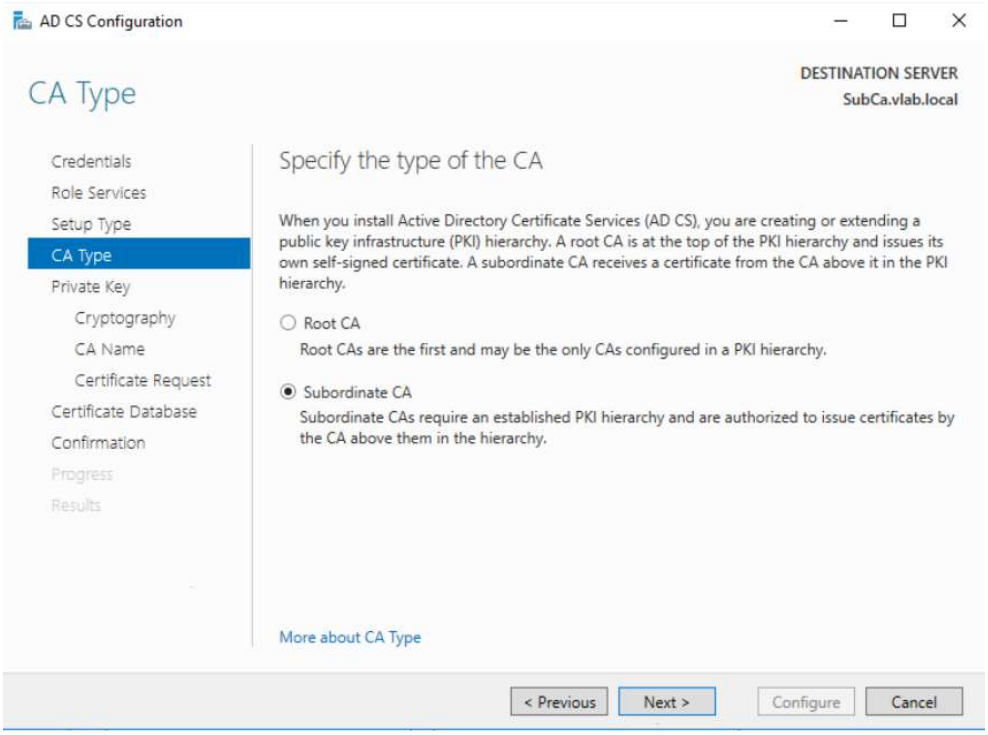


Jakelusertifikaattipalvelin määritteleminen tapahtuu samalla lailla kuin juurisertifikaattipalvelimen paitsi, että konfiguraatioon tehdään muutama muutos.

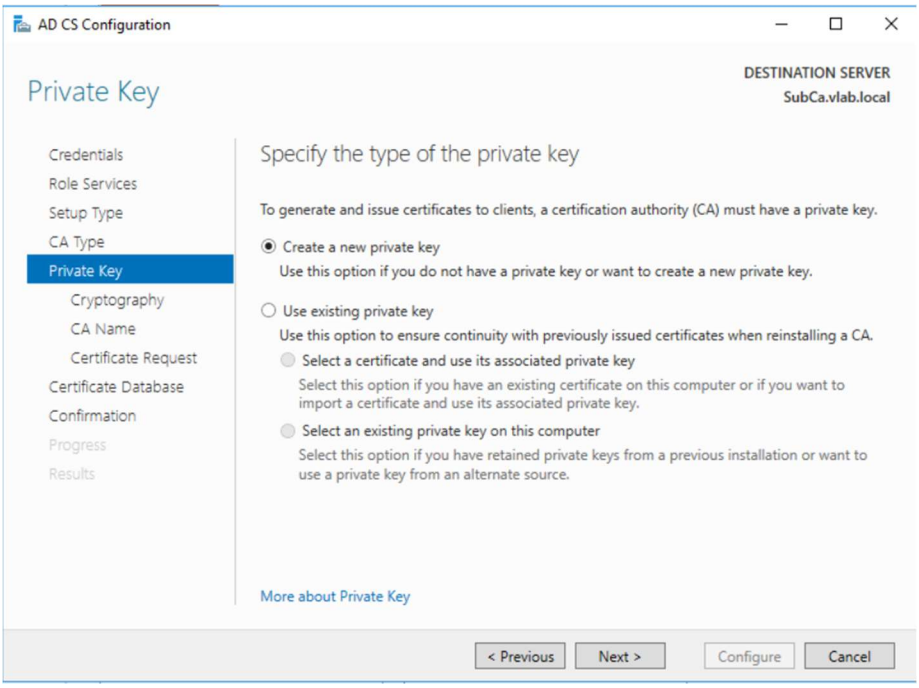


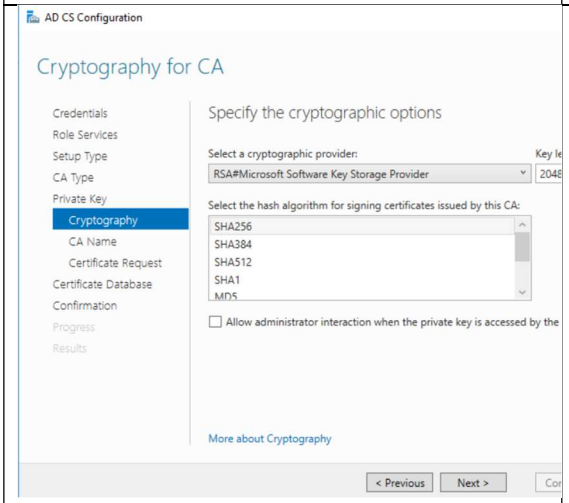
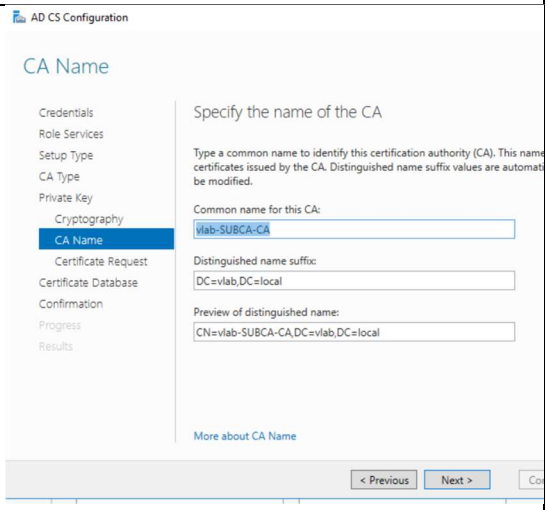
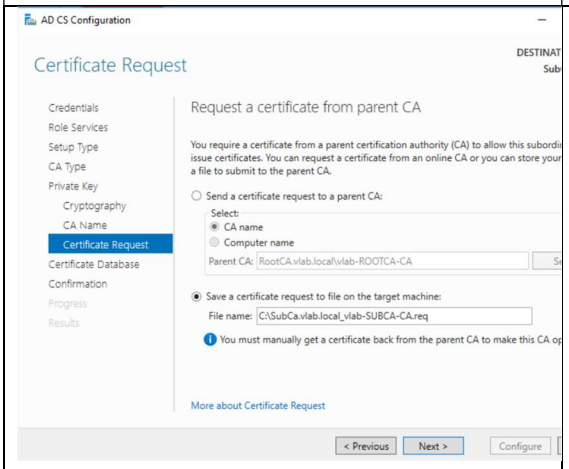
Tämän lisäksi vielä Certification Authority Web Enrollment rooli päälle.



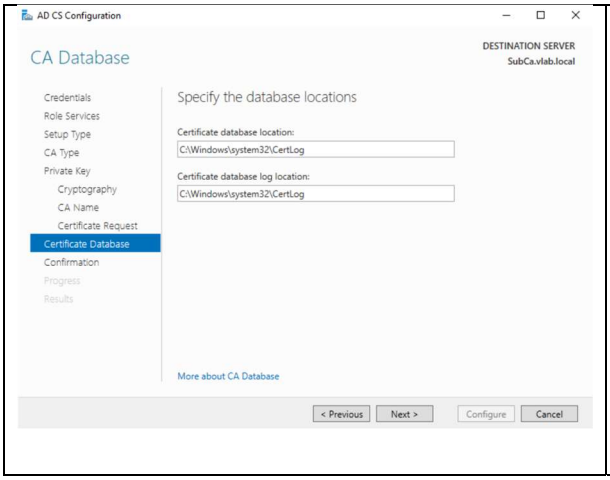


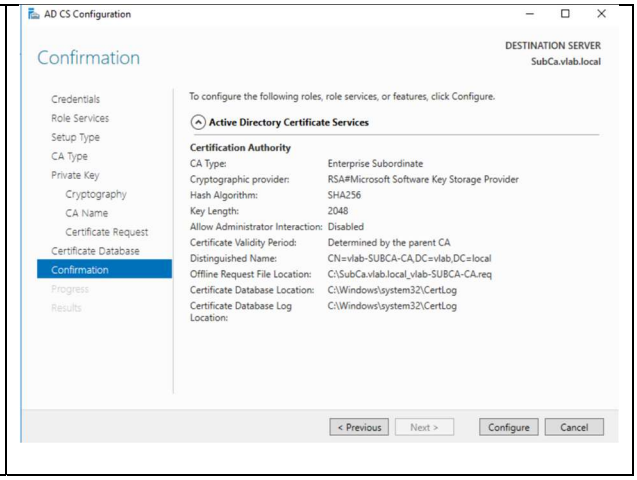
Root CA valinnan sijaan valitsemme Subordinate CA:n koska tämä palvelin tulee toimimaan sertifikaattien jakajana loppukäyttäjille sekä koneille.

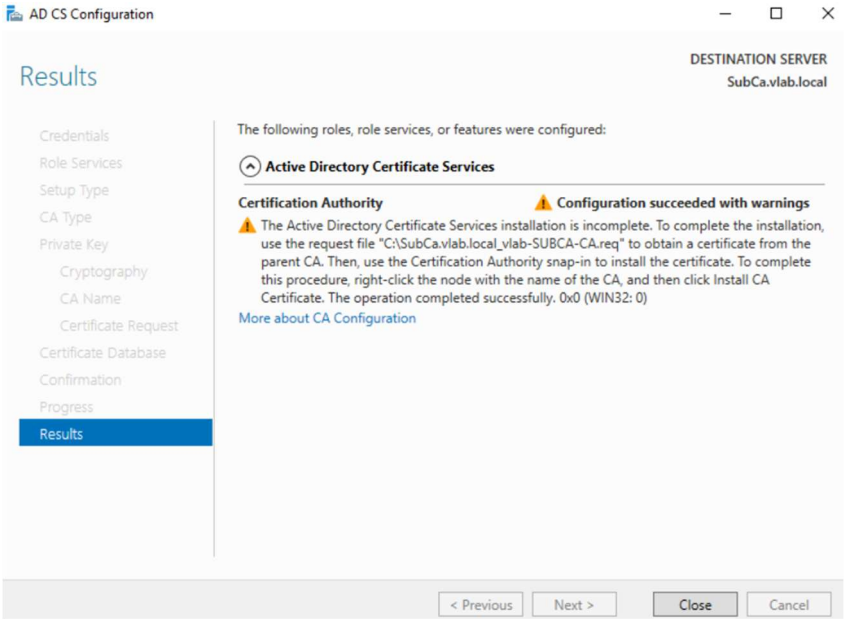


	Määritellään salainen avain, salaus-algoritmi sekä sertifikaattiauktoriteetin nimi niille haluttuun muotoon.
	
	

Koska tämä on jakelupalvelin ja PKI-infrastruktuuri konfiguroidaan käyttämään juurisertifikaattipalvelinta offline-tilassa, sertifikaattipyyntö tallennetaan manuaalisesti palvelimelle, täten saadaan haettua uusi sertifikaatti juuresta tarvittaessa. Tämän sertifikaatti pyynnön luomisessa voidaan käyttää myös ylempää ”Send a certificate request to a parent CA” vaihtoehtoa jos topologia on kolmitasoinen ja sisältää useamman jakelupalvelimen.



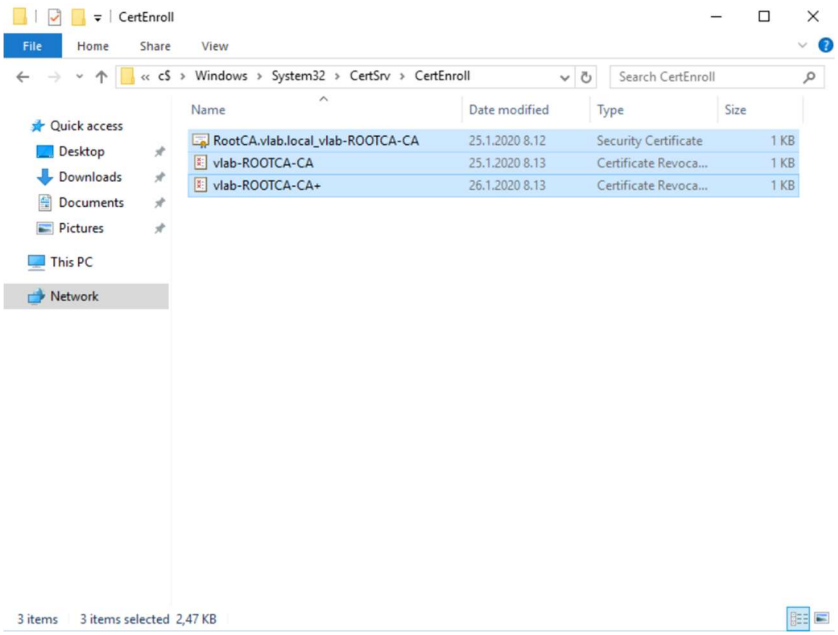




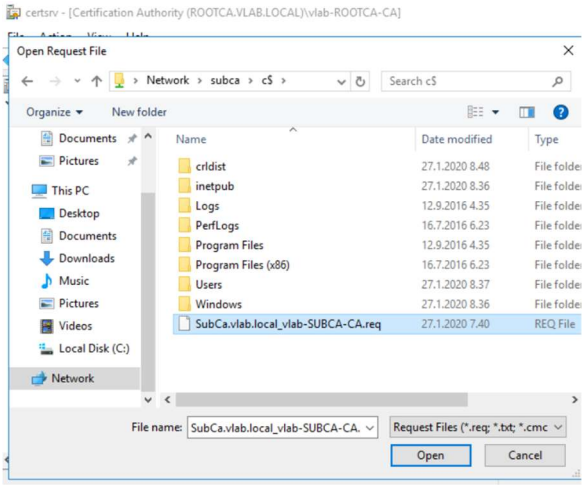
Määritystyökalu ilmoittaa ettei määritys ole vielä valmis, koska puuttuu sertifikaatin pyytäminen certificate request-tiedostolla.

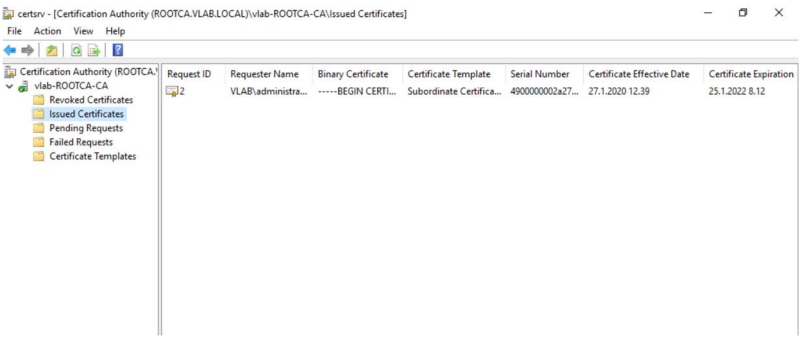
Tämä määrityksen jälkeen pitää muistaa lisätä certification authority web enrollment, certificate enrollment web policy service ja certificate enrollment web service ilman näitä web-palvelimelle jakaminen ei onnistu.

Kopioi juurisertifikaattipalvelimelta CertEnroll-hakemiston tiedostot jakelupalvelimelle samaan hakemistoon.

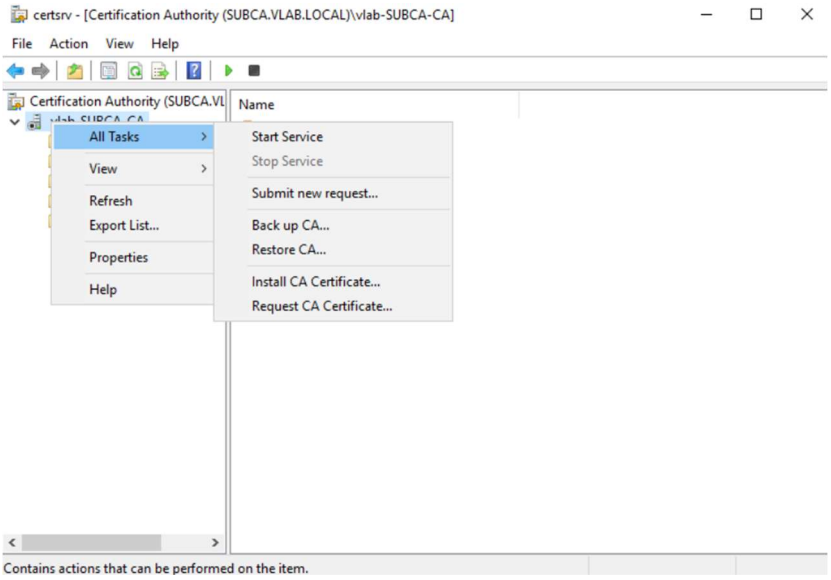


Sertifikaatin pyytäminen juuresta avaamalla juurisertifikaattipalvelimella certificate request-tiedosto

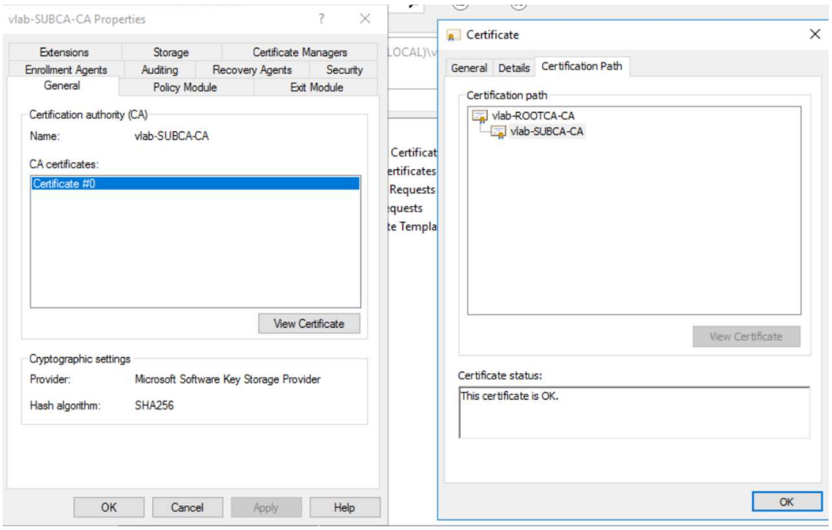




Tarkistetaan juurisertifikaattipalvelimen “Issued Certificates” kansiosta että jakelusertifikaattipalvelimen sertifikaattipyyntö näkyy listalla.

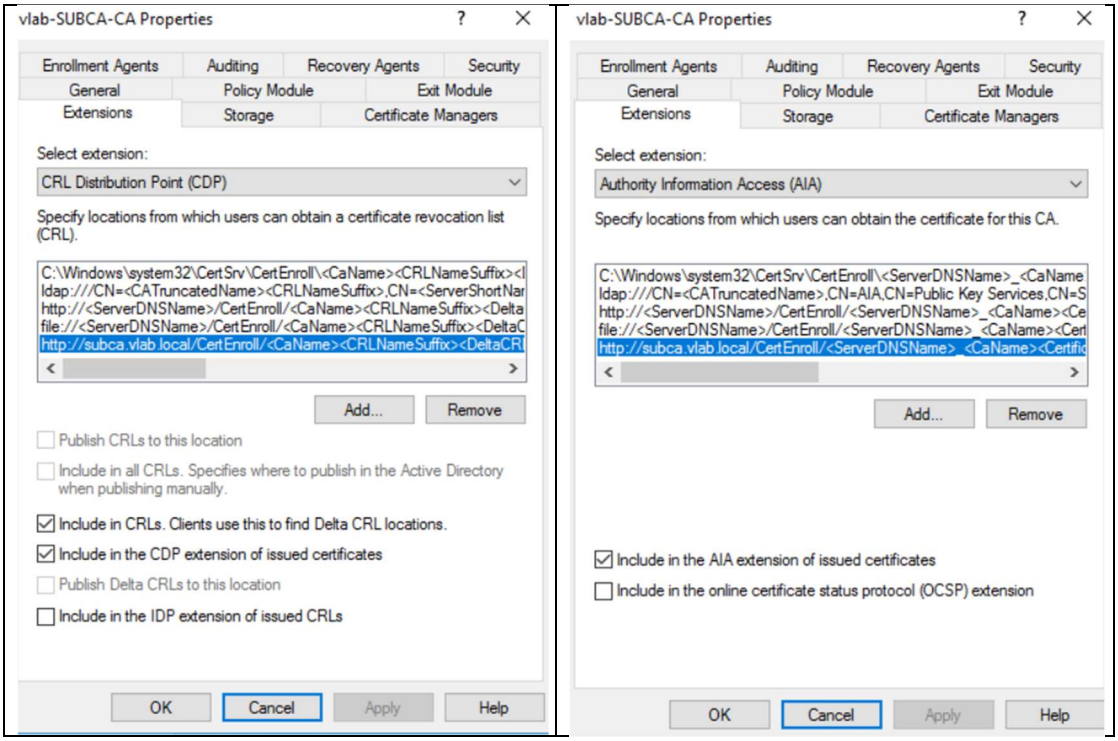


Sertifikaatin hakemisen jälkeen käynnistetään jakelusertifikaattipalvelimen certificate services palvelu.

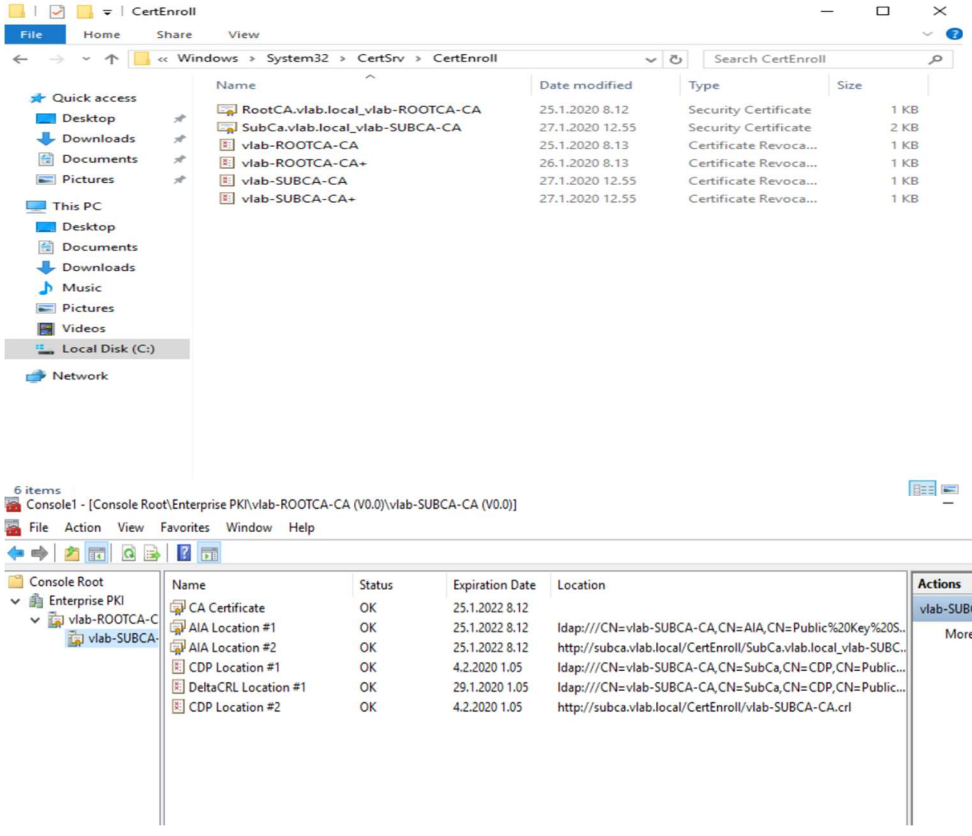


Jakelu palvelimen jakelupistemääritys

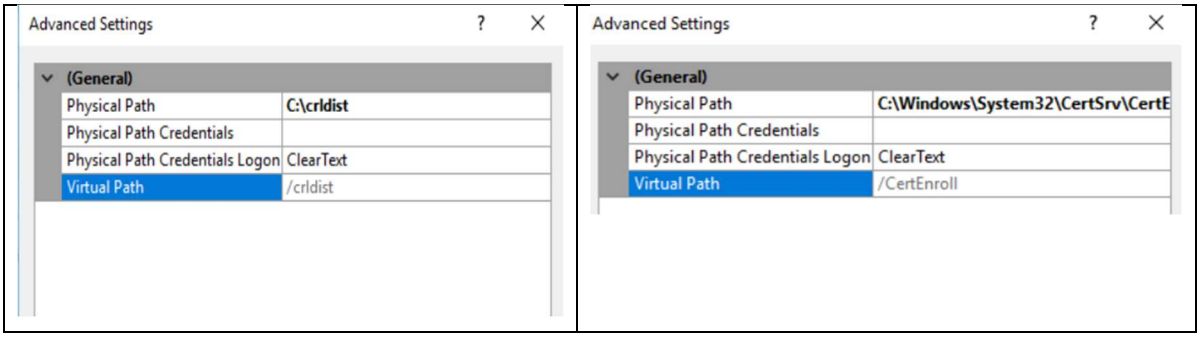
5. SUB CA CRL jakelu



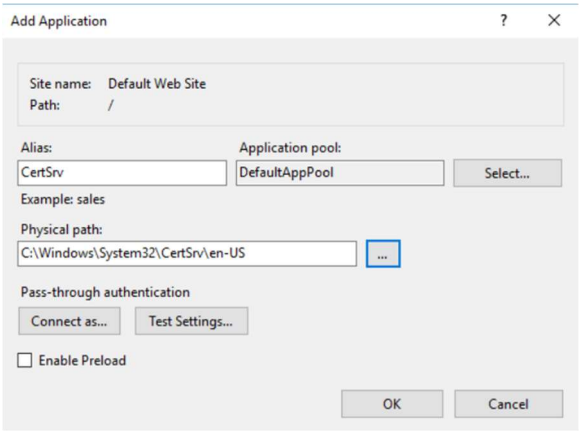
Jakelusertifikaattipalvelimen CDP eroaa juuresta sillä, että määrityksessä se vain sisällytetään CRL-listaan sekä sertifikaattien CDP lisämerkintään.



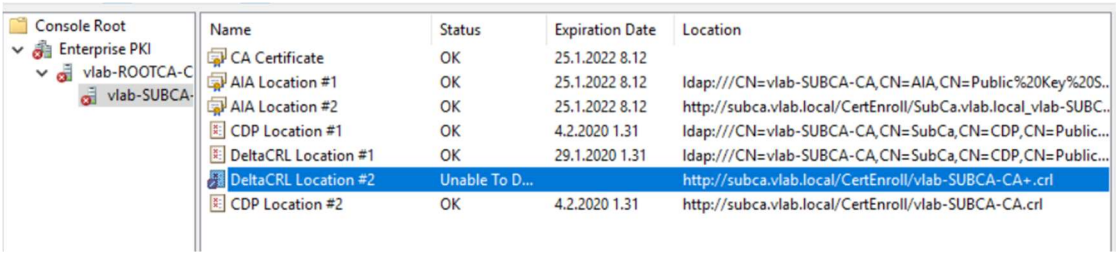
Tarkistetaan että CRL listat näkyvät jakelupalvelimen hakemistossa sekä Enterprise PKI näkymässä sertifikaattihierarkia on kunnossa. Enterprise PKI näkymään pääsee mmc:n kautta lisäämällä snap-in Enterprise PKI.



Tämän jälkeen määritellään jakelusertifikaattipalvelimelle IIS-palvelu, johon luodaan virtuaalihakemistot kansioista crldist, CertEnroll sekä sovellus CertSrv. IIS-palvelu suorittaa sertifikaattien jaon verkon yli työasemille.

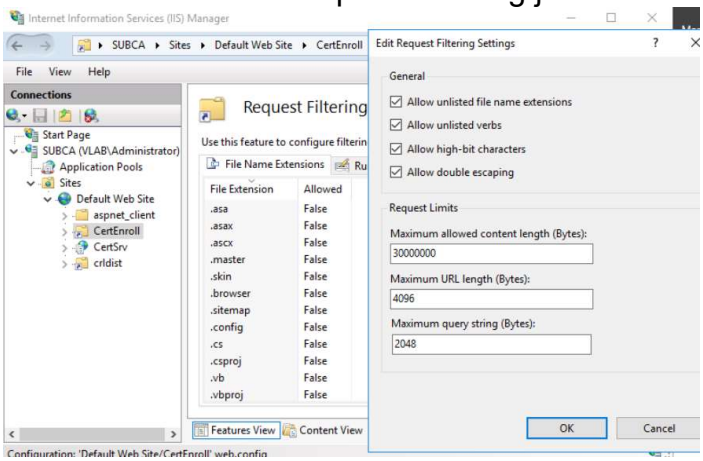


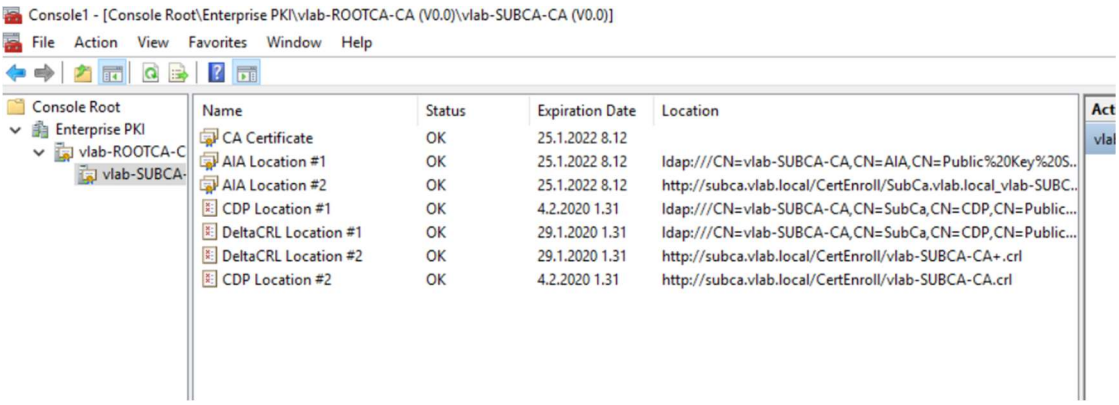
IIS-Palvelun asennuksen jälkeen PKI lopetti toimintansa, koska oletuksena double escaping on kielletty virtuaalihakemistoista



Double-escaping salliminen IIS palvelimesta CertEnroll virtuaalihakemistoon. Asetus löytyy IIS-palvelusta valitsemalla ensin CertEnroll virtuaalihakemisto

sen ominaisuuksita Request Filtering ja valitsemalla ”Edit Feature Settings”



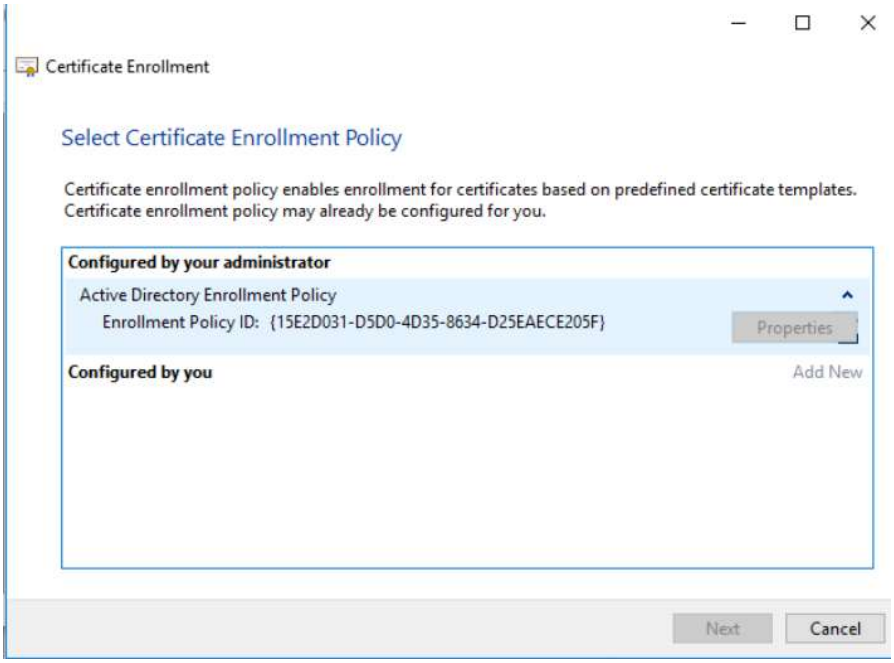


Tarkistetaan että PKI toimii jälleen. Tämän jälkeen juurisertifikaattipalvelin voidaan sammuttaa, koska jakelupalvelin toimii sertifikaattien jakajana.

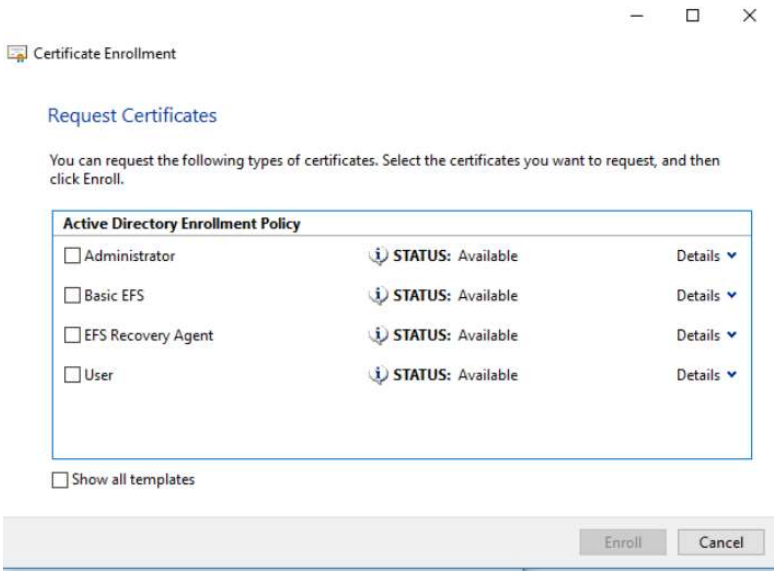
6. Toteutuksen testaus ja käyttäjän sertifikaattijako

Sertifikaatin hakeminen testi1-tietokoneella tapahtuu avaamalla certmgr hallintatyökalu mmc:llä hiiren oikealla painikkeella ”Personal” ”All Tasks”-valinta ja painamalla ”Request New Certificate” joka avaa sertifikaatin asennus aputyökalun. Tämän voi tehdä joko tämän hetkiselle käyttäjälle tai tietokoneelle halli-

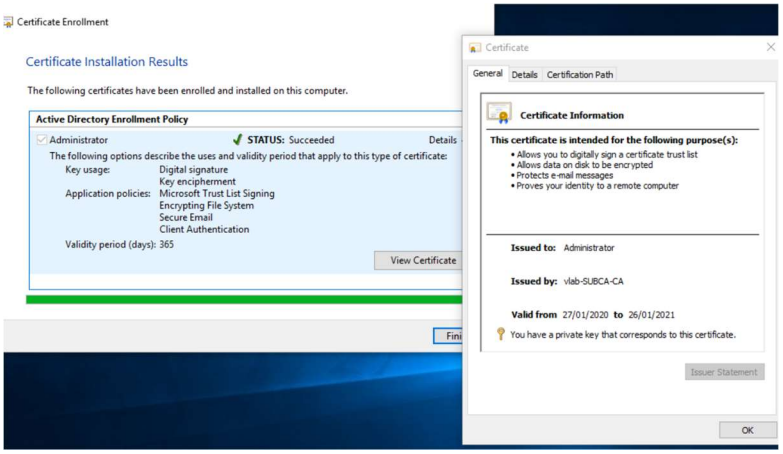
nalla riippuen mille sertifikaatti halutaan asentaa. Testaus on suoritettu hakemalla käyttäjäsertifikaatti.

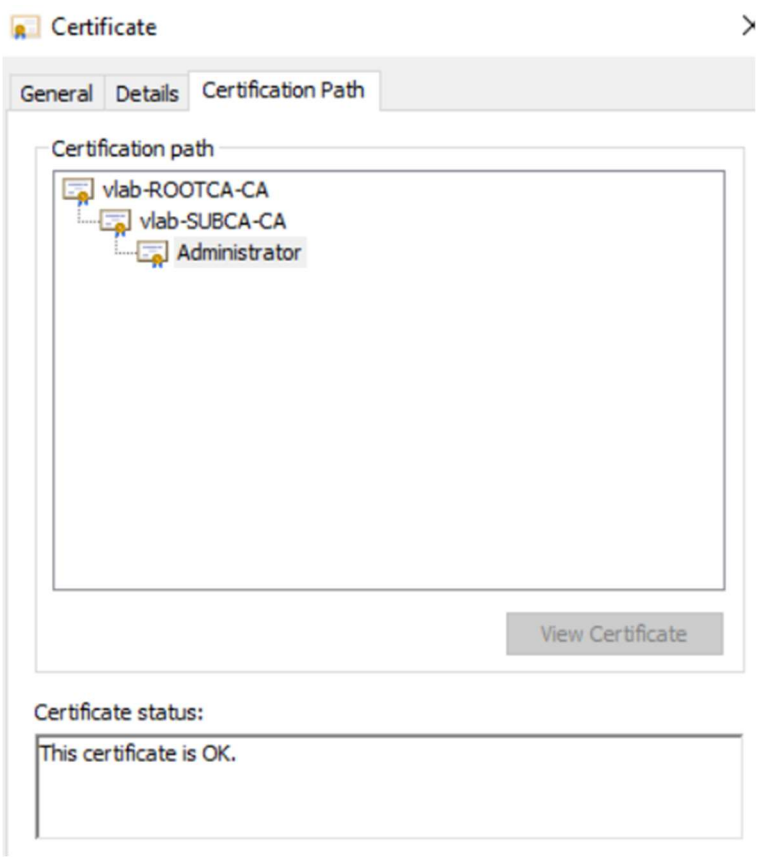


Valitaan sertifikaatin asennuskäytäntö, joka tulee jakelusertifikaattipalvelimelta.



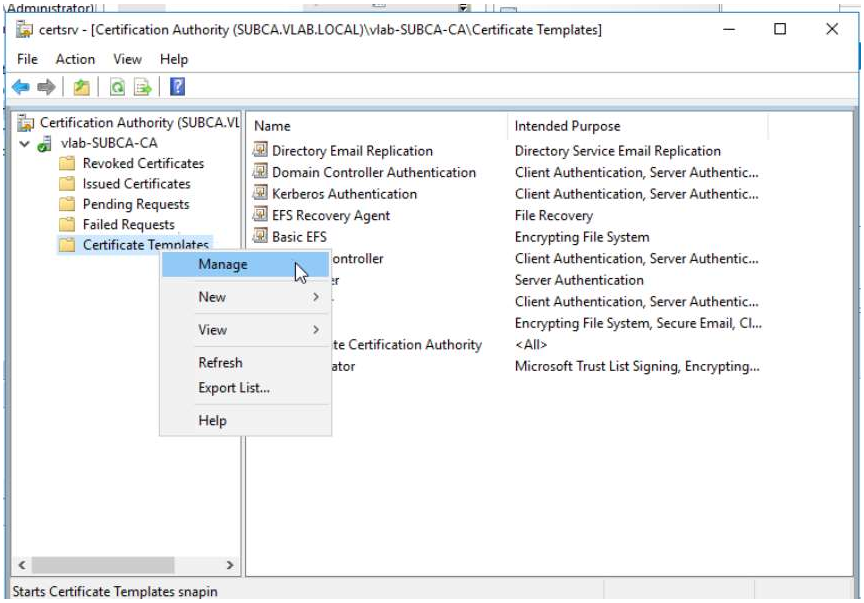
Tarkistetaan minkä tasoinen sertifikaatti tarvitaan, valitaan se ja painetaan enroll.



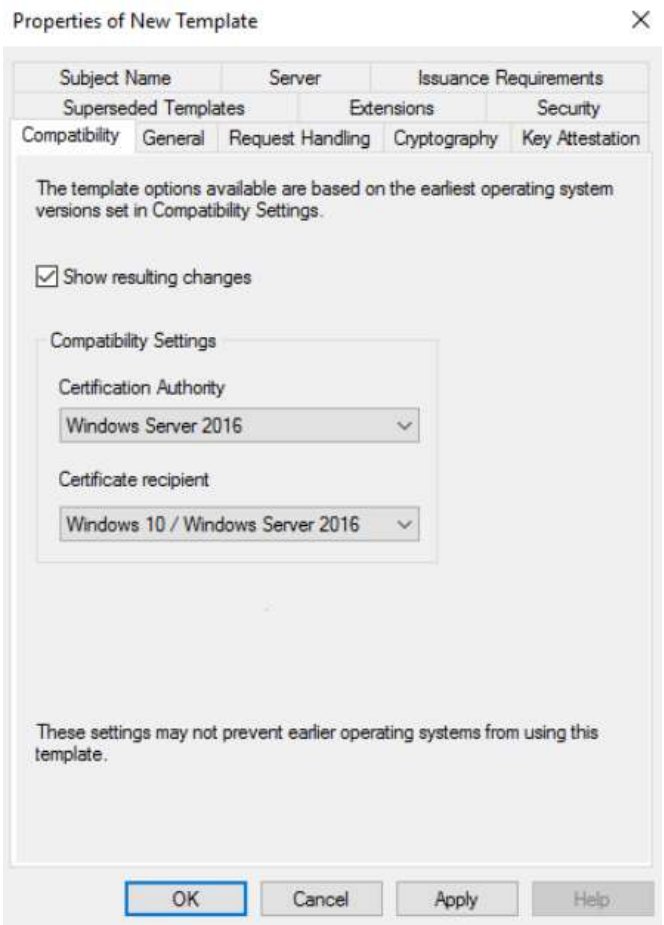


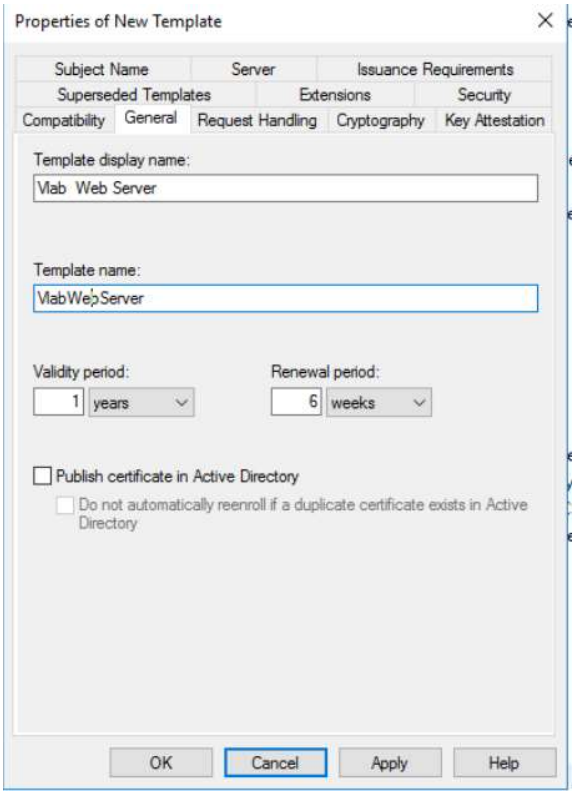
Tarkistetaan sertifikaatista, että siinä on oikeat tiedot ja että se on voimassa.

Certificate web enrollment sekä web-palvelimen sertifikaatinjako

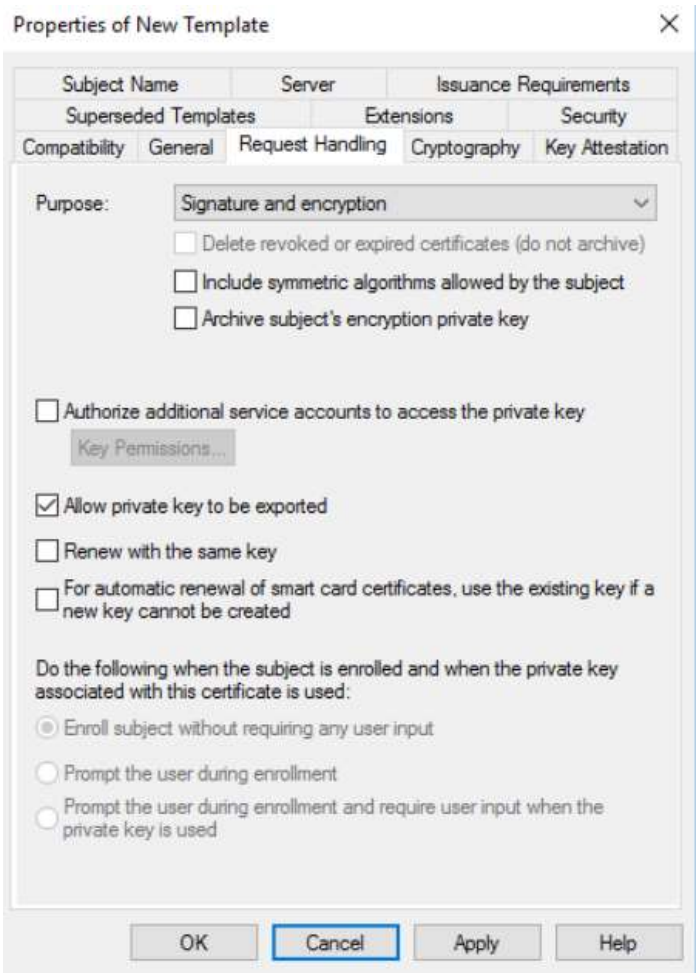


Jakelupalvelimen sertifikaatti malleista kopioidaan kahdennus toiminnolla Web Server malli

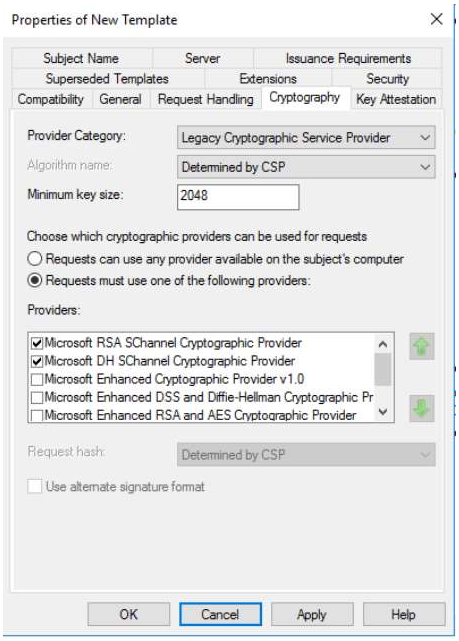




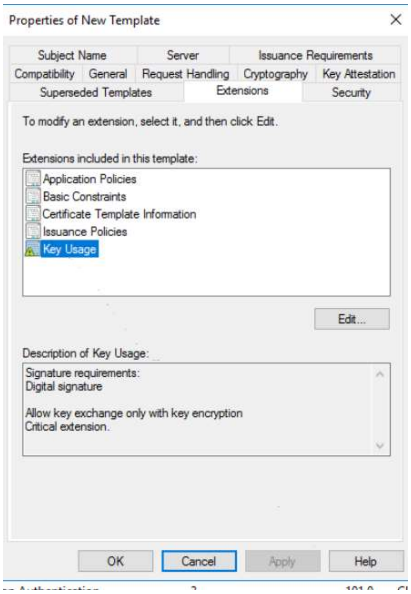
Vuoden voimassaoloaika tietoturvallisempien toimintatapojen takia



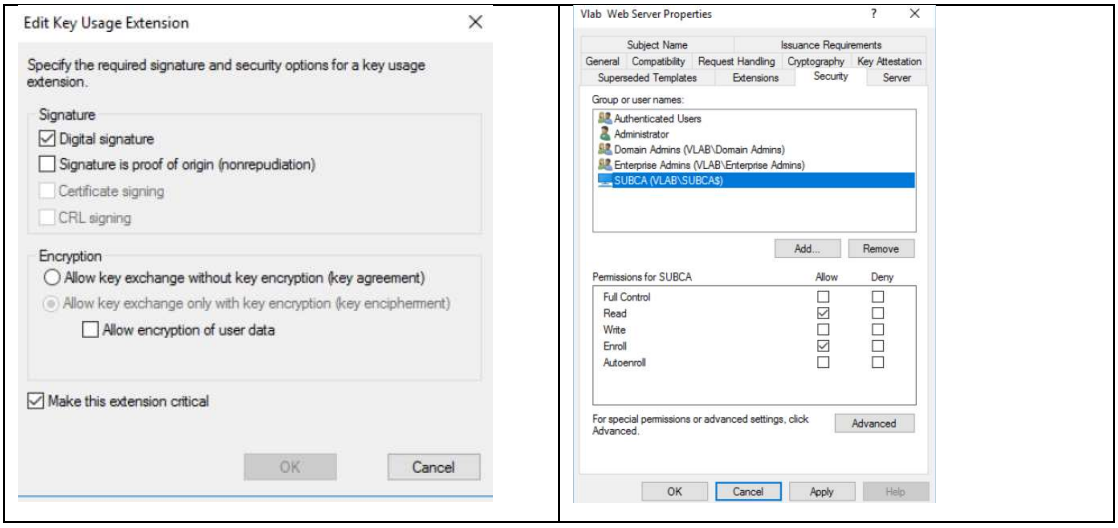
Request Handling välilehdellä määritellään mihin käyttöön mallilla tehtyjä sertifikaatteja käytetään valintoja ovat allekirjoitus, salaus, allekirjoitus ja salaus sekä allekirjoitus ja smart card autentikointi.



Windows Server 2016 versiossa oletuksena kryptografian määrityksessä käytössä on mikä tahansa salaus mikä on CSP:llä määriteltynä.

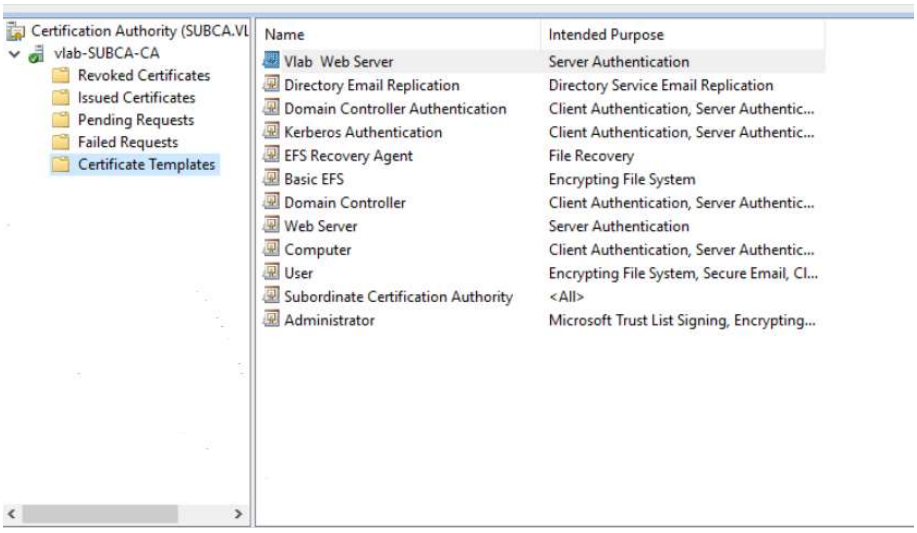


Mallin lisäosat välilehdessä voitaisiin määritellä tarkoitus mihin sertifikaattia käytetään esim. käyttäjien autentikointiin, palvelimien autentikointiin. Myös avaimen käyttö määritellään täältä.

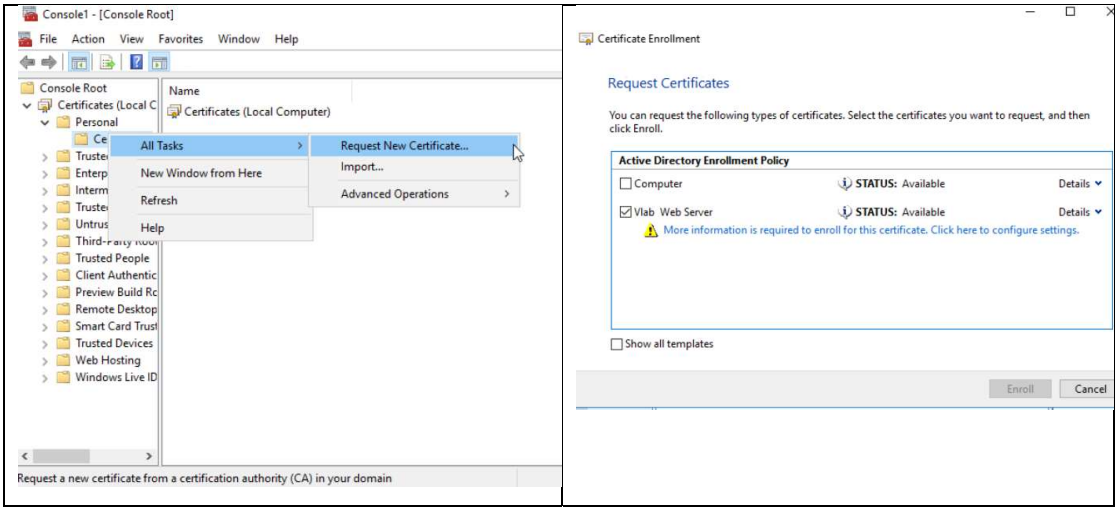


Lisätään Mallin ”Security” välilehdestä sertifikaatin hakemisoikeus jakelupalvelimelle, täten saamme lisättyä IIS-palveluun sertifikaatin.

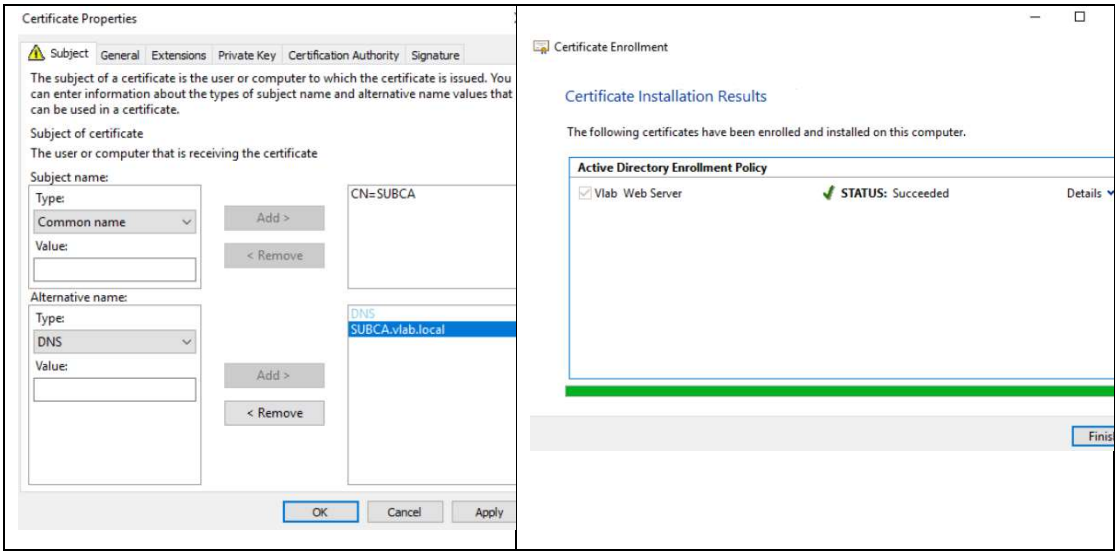
Näiden tarkistuksen jälkeen Apply ja OK sen jälkeen certsrv näkymässä hiiren oikealla napilla ”Certificate Templates” New ja ”Certificate Template to issue josta valitaan äsken tehty Sertifikaattimalli.



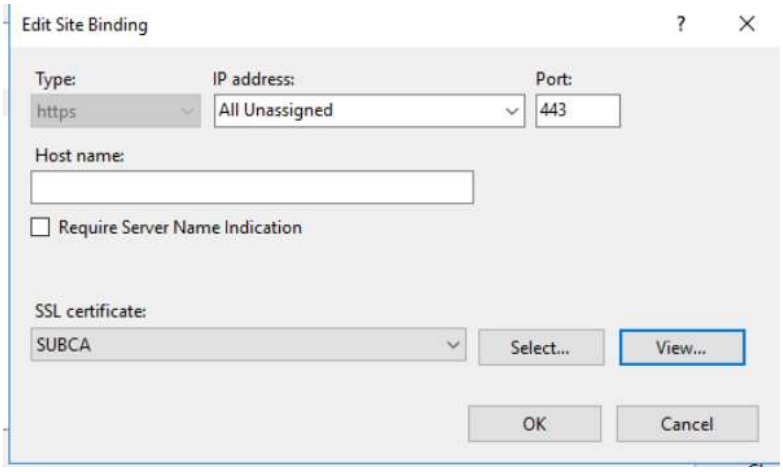
Näemme että uusi Sertifikaattimalli on listattuna.
HTTPS -ominaisuus otetaan käyttöön jakelupalvelimella, koska ilman tätä WEB-palvelimelle ei pysty hakemaan SSL-sertifikaattia.



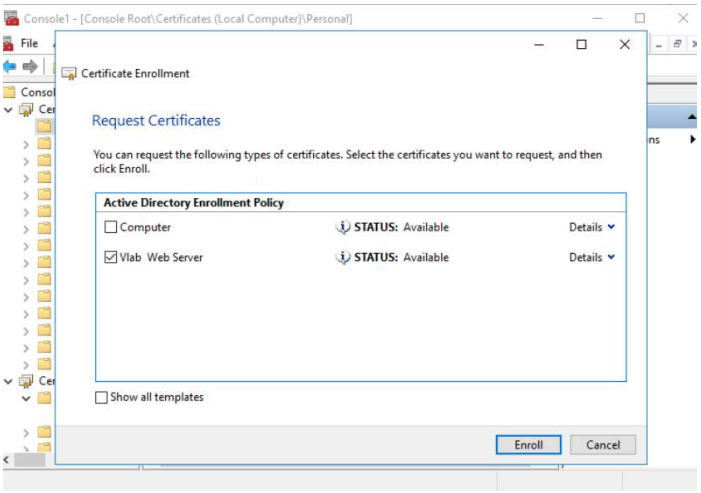
Uuden sertifikaatin haku uudesta mallista jakelupalvelimelle.



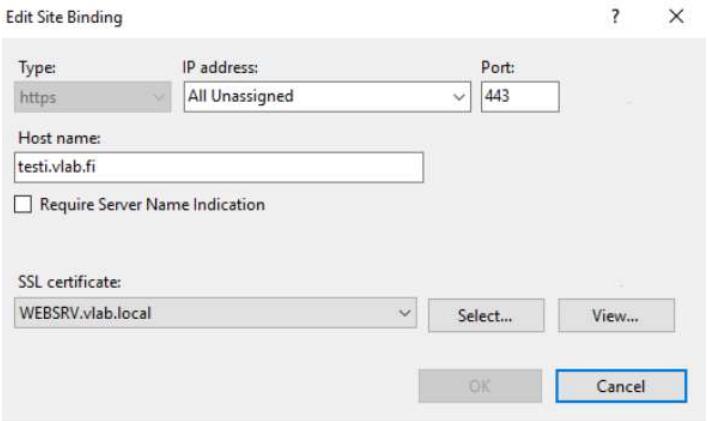
Konfiguroidaan ”Subject name” kohtaan alasveto-valikosta ”Common Name” FULL DN sijaan. Lisätään jakelusertifikaattipalvelin sertifikaattia hakevaksi osapuoleksi. Tämän jälkeen Apply, OK ja Enroll.



Jakelusertifikaattipalvelimen IIS palvelusta lisätään https ominaisuus ”Default Web Site” alle ”Edit Site” Bindings. Site Bindings osiossa
Tarkistetaan että SSL-sertifikaatti mitä halutaan käyttää on oikea, tässä tapauksessa palvelimen oma.

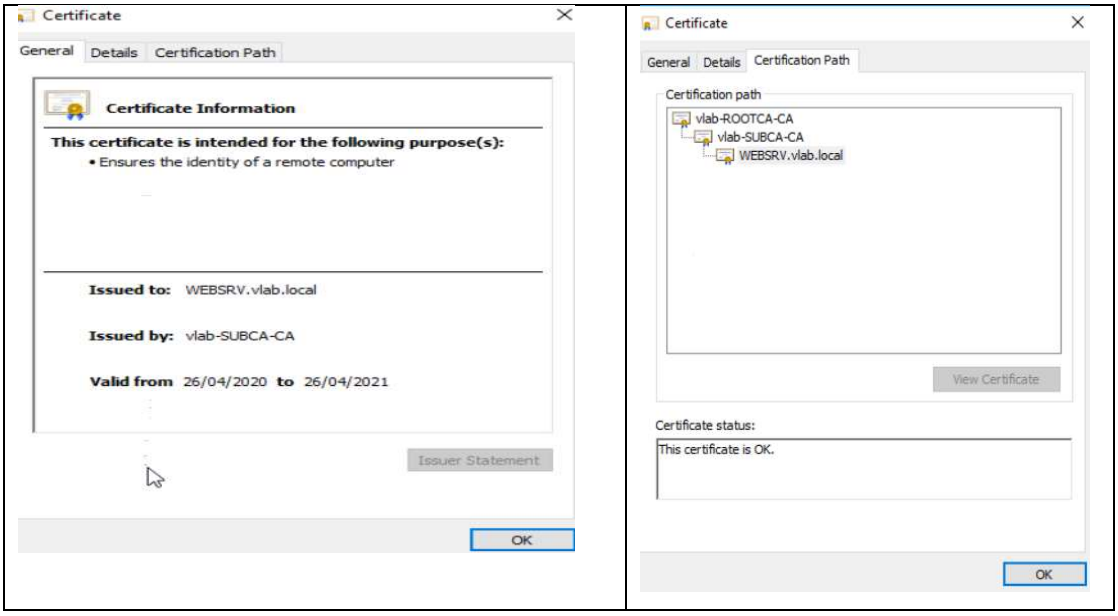


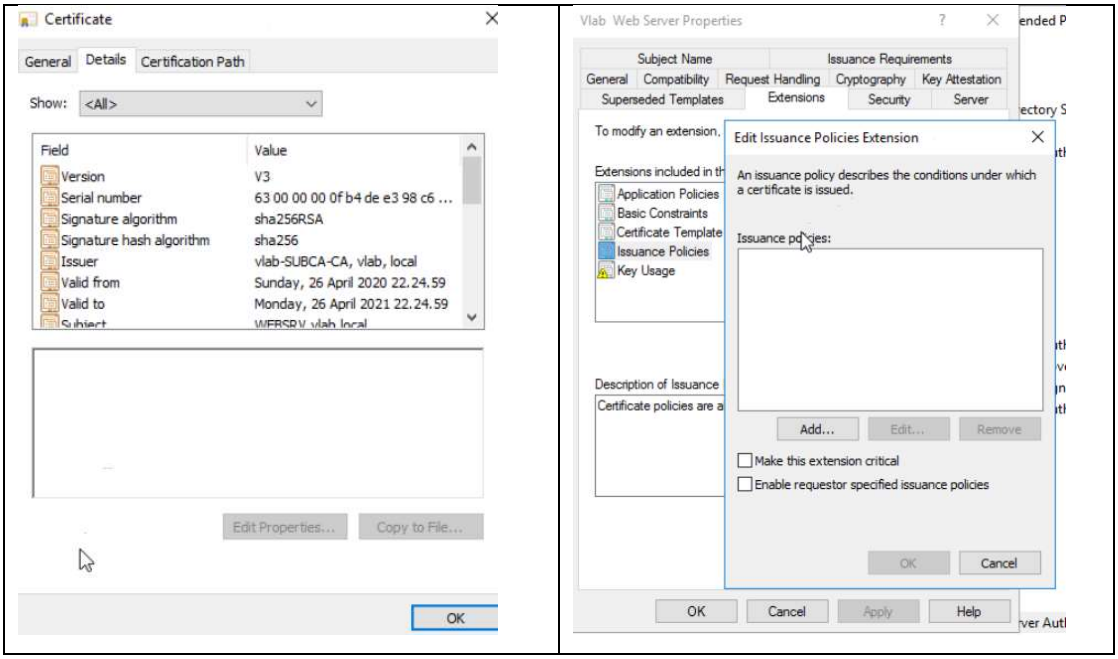
web-palvelimelle sertifikaatin manuaalinen hakeminen onnistui.



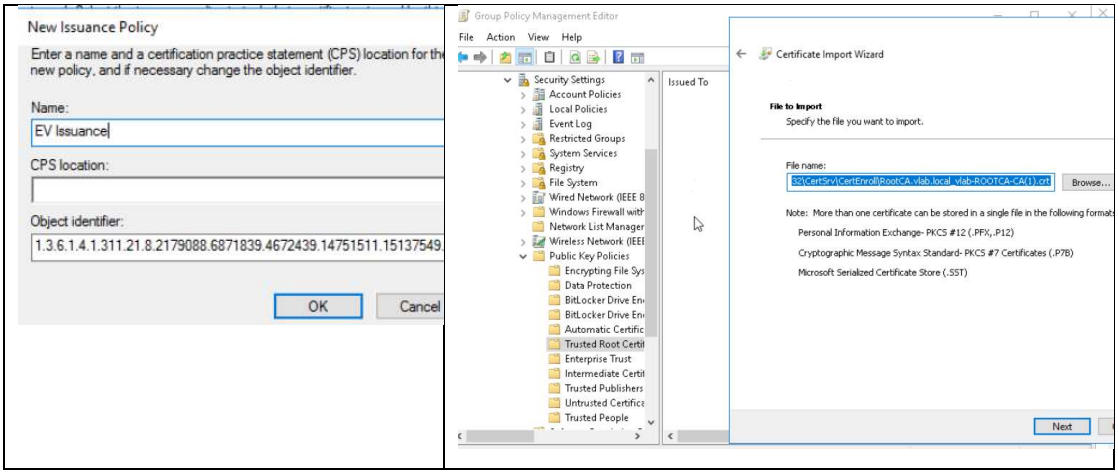
IIS-palvelimen https määritys.

DNS-määrityksen jälkeen onnistunut yhteys.

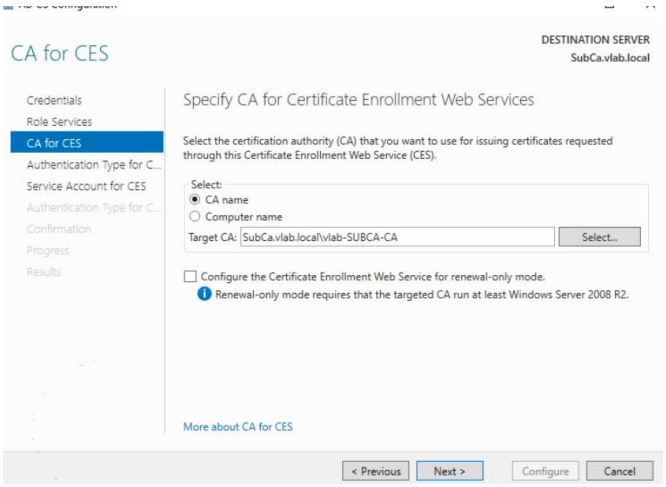




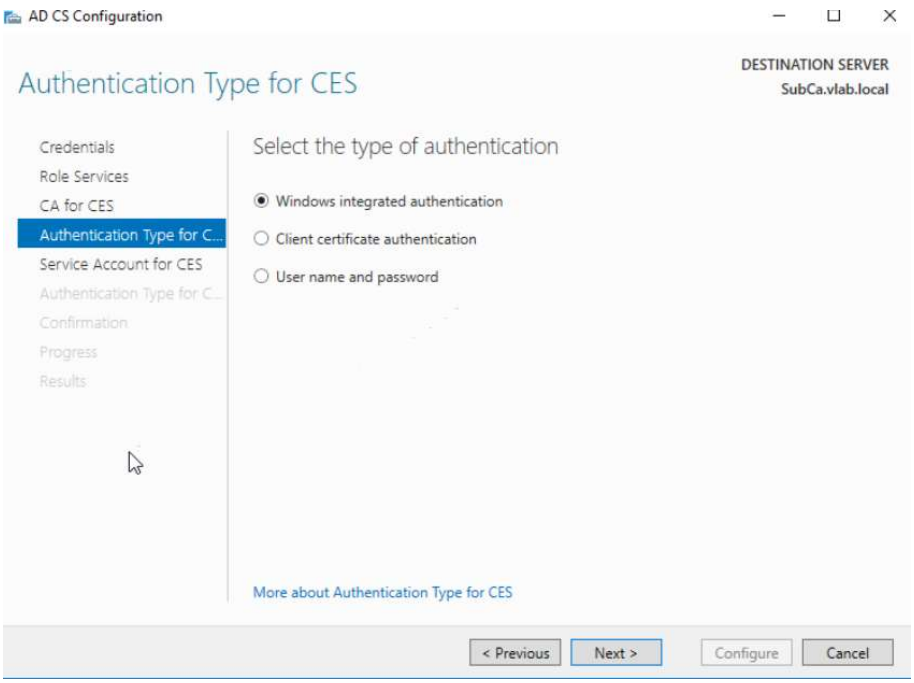
Jotta saataisin certificate error punaisesta vihreäksi tulee muokata aiemmin web-palvelimelle tehdyn sertifikaatti mallin ”Extensions” välilehdeltä löytyvää ”Issuance Policies” kohtaa lisäämällä sinne uusi Extended Validation Issuance Policy.

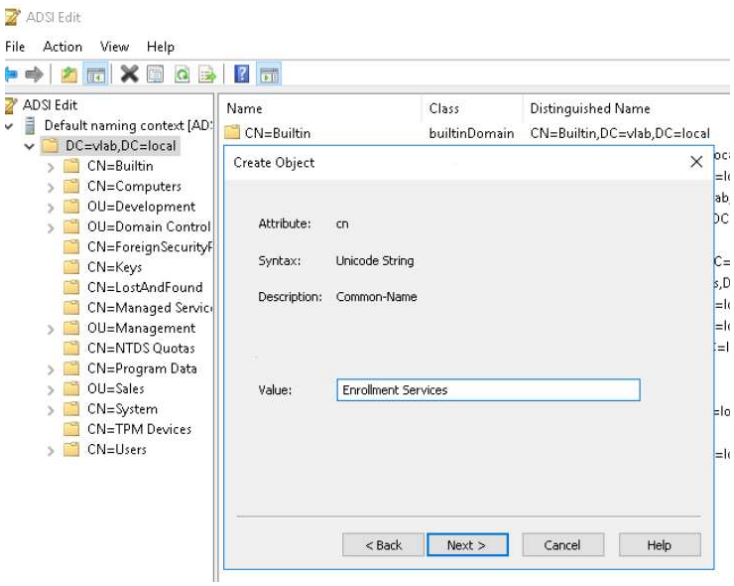


lisätään domain controllerilla rootCA trusted roottien joukkoon

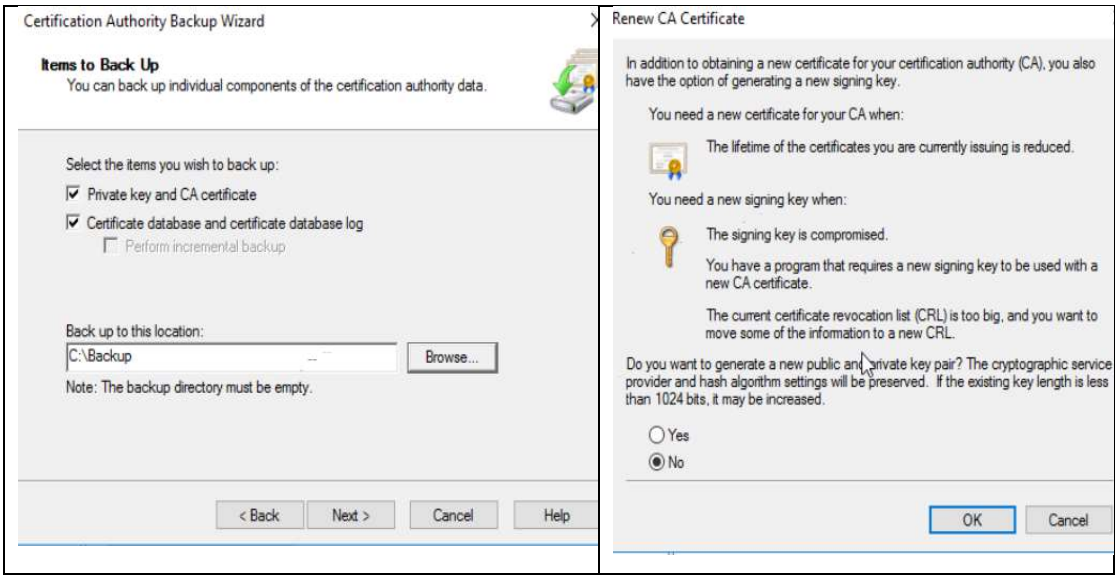


Certificate enrollment web servicen ja certificate enrollment policy web servicen määritys.





Toteutuksessa tarvitsi luoda ADSI edit -työkalulla uusi objekti nimeltä PKIEnrollmentservice uudestaan ilmeisesti domain controllerin nollaantumisen takia, jotta web-enrollaus saatiin toimivaksi web-palvelimelta. Samalla tuli testattua myös sertifikaattiauktoriteetin varmistustoiminto.



Tämän jälkeen haetaan uusi sertifikaatti. ”No” valinnalla käytetään aiempaa avainta.