TEKNIIKKA JA LIIKENNE

Tietotekniikka

Tietoverkot

INSINÖÖRITYÖ

PKI-JÄRJESTELMÄN KÄYTTÖÖNOTTO JA HALLINTA

Työn tekijä: Arto Pentikäinen
Työn ohjaajat: Kari Järvi

Työ hyväksytty: ___. ___. 2011

Kari Järvi
Yliopettaja

ALKULAUSE

Tämä insinöörityö tehtiin Metropolia Ammattikorkeakoululle. Kiitän mahdollisuudesta insinöörityön tekemiseen. Kiitokset työnohjaajalle Kari Järvelle sekä kielten tarkastajille Jussi Alhonrinteelle ja Jonita Marteliukselle. Lisäksi kiitokset erityisesti vaimolleni ymmärtämisestä ja jaksamisesta.

Helsingissä 25.12.2010

Arto Pentikäinen

TIIVISTELMÄ

Työn tekijä: Arto Pentikäinen

Työn nimi: PKI-järjestelmän käyttöönotto ja hallinta

Päivämäärä: 25.12.2010 **Sivumäärä:** 124 s. + 3 liitettä

Koulutusohjelma: Tietotekniikka

Suuntautumisvaihtoehto: Tietoverkot

Työn ohjaaja: Yliopettaja Kari Järvi

Tietoverkot eivät ole nykyään enää suljettuja järjestelmiä. Organisaatioiden tietoverkot voivat koostua intraneteista, extraneteista ja julkisista Internet-palveluista. Asiaton henkilö voi mahdollisesti päästä käsiksi tai jopa luvatta muuttaa organisaation yksityistä tietoa. Esimerkiksi joku voi monitoroida ja muuttaa tietoa sen kulkiessa tietoverkossa. Hyvin suunnitellulla PKI-järjestelmällä voidaan ehkäistä erilaisia hyökkäyksiä tietoturvaa vastaan.

Julkisen avaimen järjestelmä (PKI) koostuu laitteistoista, ohjelmistoista, ihmisistä ja erilaisista käytännöistä. Järjestelmä tarvitaan sertifikaattien luomiseen, jakamiseen, käyttöön, tallentamiseen ja sulkemiseen. PKI on järjestelmä, joka sitoo julkisen avaimen käyttäjään; tämän sitomisen toteuttaa varmentaja eli CA. Kun käyttäjä on rekisteröitynyt järjestelmään, myönnetään hänelle sertifikaatti. Tämän sitomisen suorittaa käytännössä rekisteröijä eli RA.

Ennen sertifikaattipalveluiden käyttöönottoa organisaation on mietittävä ympäristön hierarkia. Rakennettavaan hierarkiaan vaikuttavat käytettävät sovellukset, tietoturvan taso, liiketaloudelliset ja teknologiset vaatimukset. Suunnittelussa kaksi pääkohtaa on hierarkiatasojen määrä ja kuinka monta palvelinta asennetaan kullekin tasolle. Muita suunniteltavia asioita ovat esimerkiksi kuka hallinnoi sovelluksia, käyttäjien lukumäärä, kuinka sertifikaatit jaetaan ja mitkä sovellukset tarvitsevat sertifikaatteja. Käyttöönotto aloitetaan juuri-CA:n asennuksesta ja tämän jälkeen asennetaan juuri-CA:n alle tarvittavat CA-palvelimet valituille tasoille. Lopuksi järjestelmä luonnollisesti testataan.

Tämä työ esittelee salauksen perusteet, jota käytetään PKI-sovelluksissa. Lisäksi esitellään PKI-järjestelmä Windows Server 2003/2008 -sertifikaattipalvelinympäristössä ja lopuksi ympäristön asentaminen. Ohjeen perusteella voidaan asentaa yksi-, kaksi- tai kolmetasoinen PKI-järjestelmä.

Avainsanat:
PKI, sertifikaatti eli varmenne, sertifikaatti-palvelin, CA

Metropolia

ABSTRACT

Name: Arto Pentikäinen

Title: PKI System Deployment and Management

Date: 25.12.2010 **Number of pages:** 124 p + 3 appendices

Department: Information technology **Study Programme:** Data networks

Instructor: Kari Järvi, Principal Lecturer

Supervisor:

Computer networks are no longer closed systems. An organization's network might consist of intranets, Internet sites, and extranets. An unauthorized person with malicious intentions could potentially access, view or alter the organization's digital information. A person can monitor or alter information as it crosses the network. A thief who steals a laptop computer can try to access confidential information stored on the computer hard disk. A well-planned PKI can reduce these common attacks.

The Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures. PKI is needed to create, manage, distribute, use, store, and revoke digital certificates. A PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The binding is established through the registration and issuance process. The process can be carried out by CA's software or under human supervision. The PKI role that assures this binding is called the Registration Authority (RA).

Before deploying Microsoft Windows Server 2003/2008 Certificate Services, an organization must spend time designing the certification authority hierarchy. Developing the correct structure involves investigating and processing related requirements for application, security, business and technology. Two basic considerations addressed in the design process are the number of tiers to include in the CA hierarchy and how many individual CAs will be required at each tier. Other considerations are for example who will manage the applications, the number of users, the certificate distribution, and how certificates are used by the applications. Implementation of a CA hierarchy always begins at the root CA and proceeds to the direct subordinates of the root CA. The installation process continues until all CAs in the hierarchy are installed and tested.

The present study introduces the fundamentals of cryptography and provides a basic understanding of the type of encryption and signing that takes place in PKI-enabled applications. It also introduces a PKI and how it is deployed in the Windows Server 2003/2008 Certificate Services infrastructure. Finally, the study provides detailed instructions for installing a CA hierarchy. The instructions can be used to build a hierarchy with a single CA or a hierarchy with two or more tiers.

Keywords:
PKI, certificate, certificate server, certification authority, CA hierarchy

SISÄLLYS

LYHENTEET JA KÄSITTEET

AAA	Authentication (todentaminen tai autentikointi), Authorization (valtuutus) ja Accounting (tilastointi). AAA-protokolla on menetelmä, jolla voidaan tunnistaa toinen osapuoli tietoverkossa.
AIA	Authority Information Access. Sertifikaatin laajennos, joka ilmaisee, missä CA:n sertifikaatti on julkaistu.
AKI	Authority Key Identifier. Sertifikaatin laajennos; ilmaiseen CA:n julkisen avaimen, jolla varmistetaan kyseisen CA:n allekirjoitus.
CA	Certification Authority. Varmentaja, joka toimii kolmantena osapuolena varmentaen, että julkinen avain kuuluu kyseiselle taholle.
CDP	Certficate Distribution Points. Sertifikaattien julkaisupiste; asiakkaat voivat ladata CA:n sertifikaatin sieltä.
CDP	CRL Distribution Point. Sulkulistan julkaisupaikka.
CP	Certificate Policy. Varmennepolitiikka, joka esittelee varmentajan keskeiset toimintaperiaatteet, joihin varmentaja toiminnassaan sitoutuu.
CPS	Certificate Practices Statement. Varmennekäytäntö(lausuma), joka on varmennepolitiikan (CP) yksityiskohtainen toteutussuunnitelma.
CRL	Certificate Revocation List. Sulkulista, johon tallennetaan käytöstä poistetut sertifikaatit.
CSP	Cryptographic Service Provider. Ohjelmakirjasto, joka toteuttaa salaus- ja purkutoiminnot.
CTL	Certificate trust list. Varmenneluottolista on tapa luoda luottosuhde eri organisaatioiden välille. Varmenneluottolista toimii vain Microsoftin omissa käyttöjärjestelmissä.

EAP	Extensible Authentication Protocol. Autentikointiprotokolla, jota käytetään lähinnä langattomissa verkoissa ja Point-to-Point-yhteyksissä.
EICA	Enterprise Issuing CA. Myöntäjä-CA, joka jakaa sertifikaatit loppukäyttäjille, koneille tai palveluille.
EKU	Extended Key Usage. Laajennettu avaimen käyttökohde. Ilmaisee mihin sertifikaatin julkista avainta voi käyttää (esim. EFS-salaukseen).
FIPS	Federal Information Processing Standard. Julkisia standardeja, jotka Yhdysvaltain liittohallitus on kehittänyt tietoteknisien järjestelmien käyttöön.
FTP	File Transfer Protocol. Tiedostojen siirtoon tarkoitettu protokolla.
HSM	Hardware Security Module. Moduuli, johon voidaan tallentaa CA:n yksityinen avain. Jos moduuliin murtaudutaan, yksityinen avain tuhotaan, joten se ei missään tapauksessa voi joutua vääriin käsiin.
HTTP	Hyper Text Transfer Protocol. Hypertekstin siirtoprotokolla, jota selaimet ja WWW-palvelimet käyttävät tiedonsiirtoon.
ICA	Intermediate CA. Alivarmentaja, jolle juurivarmentaja on myöntänyt sertifikaatin.
IDP	Issuer Distribution Point .Sulkulistan sisältämä laajennuskenttä, jossa ilmaistaan sulkulistan käyttötarkoitus; esim. sulkulista sisältää vain loppukäyttäjien sertifikaatteja, ei CA:n sertifikaatteja.
KRA	Key Recovery Agent. Avaimen palautusagentti, jolla on valtuudet palauttaa hukkunut avain käyttäjälle. Avain palautetaan tietokannasta, johon se on luonnin yhteydessä tallennettu. Avaimen palautusagentilla on oma sertifikaattinsa tätä tehtävää varten.

L2TP	Layer 2 Tunneling Protocol. Tunnelointiprotokolla VPN-yhteyksiä varten. Microsoftin ja Ciscon kehittämä protokolla toimii OSI-mallin 2. kerroksella. Näin ollen se tukee myös muita kuin IP-protokollia. L2F:n ja PPTP:n yhdistelmä.
LDAP	Lightway Directory Access Protocol. Hakemistopalvelujen käyttöön tarkoitettu verkkoprotokolla.
NDES	Network Device Enrollment Service. NDES-palvelun avulla voidaan jakaa sertifikaatit Ciscon laitteille SCEP-protokollaa käyttäen.
OCSP	Online Certificate Status Protocol. Protokolla, jolla tarkastetaan X.509-standardiin perustuvan sertifikaatin tila. OCSP-palvelin (responderi) palvelee verkossa reaaliaikaisesti ja vastaa asiakkaan kyselyyn sertifikaatin tilasta (onko sertifikaatti esim. poistettu käytöstä).
OID	Object Identifier. Objektin tai attribuutin yksilöivä tunnus.
PDS	PKI Disclosure Statement. Varmennekuvaus, joka sisältää varmennepolitiikan (CP) ja varmennuskäytännön (CPS) keskeiset ratkaisut.
PKCS #12	Public-Key Cryptography Standards (PKCS) -standardiin kuuluva standardi (Personal Information Exchange Syntax Standard), joka kuvaa henkilökohtaisen informaation siirtämiseen ja tallentamiseen käytettäviä menetelmiä. Standardin on kehittänyt RSA Laboratories.
PKCS #7	Public-Key Cryptography Standards (PKCS) -standardiin kuuluva standardi (Cryptographic Message Syntax Standard), joka kuvaa salatun tiedon syntaksia. Standardin on kehittänyt RSA Laboratories.
PKI	Public Key Infrastructure. Julkisen avaimen infrastruktuuri, jossa tietoturvapalveluita tuotetaan julkisen avaimen menetelmällä.

PPTP Point-to-Point Tunneling Protocol. VPN-tunnelointiprotokolla, joka pohjautuu PPP-protokollaan. Alun perin tarkoitettu Windows-työasemien kytkeytymiseen Windows-palvelimille julkisen verkon yli. PPP-protokollan laajennus, joka voi tunneloida muitakin protokollia kuin TCP/IP-protokollaa.

RA Registration Authority. Rekisteröijä, joka tunnistaa varmenteen hakijan varmennepolitiikan ja varmennuskäytännön mukaisesti juurivarmentajan (RCA) toimeksiannosta.

RADIUS Remote Authentication Dial In User Service. Suunniteltu sisäänsoittopalveluissa tapahtuvaan tunnistukseen. Jos lähiverkossa käytetään AAA-palveluita, on lähiverkossa oltava RADIUS-palvelin, johon ethernet-kytkimet ja WLAN-tukiasemat ottavat yhteyttä RADIUS-protokollalla tarkistaakseen luvan kirjautumiseen.

RAID Redundant Array of Independent Disks. Tekniikka, jolla tietokoneiden vikasietoisuutta ja nopeutta kasvatetaan käyttämällä useita erillisiä kiintolevyjä, jotka yhdistetään yhdeksi loogiseksi levyksi.

RCA Root Certification Authority. Juurivarmentaja on organisaatio, joka myöntää varmentajan sertifikaatit. Lisäksi juurivarmentaja laatii toimintaansa kuvaavan varmennepolitiikan (CP) sekä varmennuskäytännön (CPS).

SCEP Simple Certificate Enrollment Protocol. Ciscon verkkolaitteissa käytössä oleva protokolla, jolla ladataan laitteelle tarvittava sertifikaatti.

SFS Suomen Standardisoimisliitto. Suomalainen standardisoinnin keskusjärjestö. Jäsenenä kansainvälisessä standardisoimisjärjestössä ISOssa ja eurooppalaisessa standardisoimisjärjestössä CENissä.

SKI Subject Key Identifier. Varmennetun avaimen tunniste.

SMB Server Message Blocks. Tiedostojen jako.

SSL	Secure Sockets Layer. Alunperin Netscapen kehittämä protokolla tiedon salaamiseen Internetin yli.
TLS	Transport Layer Security. Tunnettiin aiemmin nimellä Secure Sockets Layer (SSL). Salausprotokolla, jolla voidaan suojata Internet-sovellusten tietoliikenne IP-verkkojen yli.
WEP	Työaseman ja tukiaseman välistä langatonta tietoliikennettä suojaamaan kehitetty salausmenetelmä, jonka tietoturvataso on matala. Perustuu IEEE:n 802.11-standardiin.
VPN	Virtual Private Network. Menetelmä, jolla kaksi tai useampia tietoverkkoja voidaan yhdistää julkisen verkon yli muodostaen näennäisesti yksityisen verkon.

1 JOHDANTO

Erilaiset palvelut verkon kautta lisääntyvät. Yhä enemmän asioita, jotka perinteisesti on hoidettu käymällä virastoissa tai lähettämällä postia, hoidetaan nykyisin verkon välityksellä. Palveluita julkaistaan sekä yrityksen omissa että julkisissa verkoissa. Näitä palveluita käyttävät käyttäjät tulee tunnistaa sekä siirrettävä tieto salata, koska verkoissa tieto on alttiina luvattomalle käytölle. Tietoa voidaan tiedonsiirron aikana salakuunnella ja jopa mahdollisesti muuttaa. Myös kannettava tietokone voidaan varastaa ja varastettua tietoa käyttää hyväksi. Reaaliaikainen käyttäjätunnistus ja tiedon salaaminen voidaan toteuttaa julkisen avaimen järjestelmällä (PKI).

Käyttäjien tunnistuksessa sekä tiedon salaamisessa PKI-järjestelmässä käytetään apuna sertifikaatteja. Nämä sertifikaatit tulee jakaa tunnistetuille käyttäjille turvallisesti ja koko sertifikaattien elinkaari tulee hallita mielellään kustannustehokkaasti. Sertifikaattien jakamiseen ja hallintaan tarvitaan sertifikaattipalvelimia, jotka asennetaan hierarkkisesti eri tasoille. Tasojen määrä riippuu lähinnä halutusta tietoturvatasosta, verkon laajuudesta sekä käyttäjien määrästä.

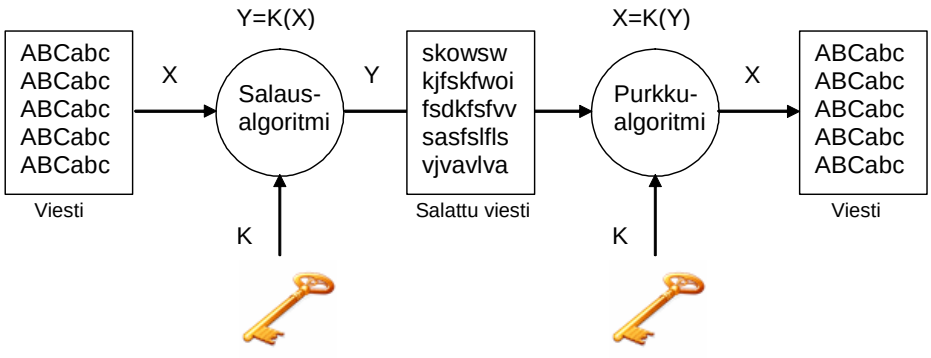
Tässä työssä käydään läpi PKI-järjestelmää teorian ja käytännön kautta Windows 2003/2008 -ympäristössä. Aluksi käydään läpi teoriatasolla salausta ja käyttäjien tunnistusta sekä PKI-järjestelmää. Tämän jälkeen suunnitellaan toimiva PKI-ympäristö yritykselle ja lopuksi asennetaan sertifikaattipalvelimet toimimaan aktiivihakemistoympäristössä. Ympäristö on asennettu ja testattu Windows Server 2003 Enterprise Edition- ja Windows Server 2008 Enterprise Edition -palvelimilla. Ympäristöön on asennettu kolmetasoinen hierarkia ja palvelimet on asennettu omiin virtuaalikoneisiin yhteen fyysiseen tietokoneeseen.

Tämän työn tavoitteena on tutkia PKI-ympäristön kustannuksia organisaatiolle sekä asennuksen monimutkaisuutta. Samalla kun tutkitaan, mitkä asiat vaikuttavat järjestelmän kustannuksiin, mietitään myös tietoturvaa sekä yleensä, mitä asioita tulee ottaa huomioon ympäristön suunnittelussa. Ympäristö tuleekin suunnitella erittäin huolellisesti, jotta suurilta uudelleen asennuksilta vältytään ympäristön mahdollisen laajentumisen tai tietoturvaloukkauksen yhteydessä.

2 KRYPTOKRAFIA JA TIEDON SALAAMINEN

2.1 Algoritmi ja avain

Tiedon salaamista tarvitaan nykyisin tiedon siirtämiseen verkossa turvallisesti. Teknisesti kryptografia on tiedon salaamista matemaattisella menetelmällä, niin ettei tieto ole siirron aikana luettavassa muodossa; lähettäjä laittaa viestin lukkoon avaimella ja vastaanottaja avaa sen avaimella. Salakirjoitus perustuu algoritmiin ja avaimeen. Algoritmi on matemaattinen funktio, jonka tehtävä on muuttaa alkuperäinen informaation avaimen avulla piilotetuksi informaatioksi. Avainta käytetään syötteenä algoritmille, jolloin algoritmi voi salata tiedon sekä purkaa salauksen (kuva 1). Algoritmin paljastuminen ei ole vaarallista, mutta itse avaimen paljastuminen on tietoturvariski. Salausavaimet tulisikin tallentaa varmaan paikkaan.



Kuva 1. Tiedon salaus

Salausta käyttävät sovellukset sopivat tietyistä asioista ennen varsinaisen tiedon siirtämistä. Näitä asioita ovat muun muassa:

- käytettävän algoritmin sopiminen. Sovelluksilla voi olla joukko algoritmeja, joista valitaan paras yhteiseen käyttöön.
- avaimen generoiminen. Parhaassa tapauksessa avain on kertakäyttöinen, jolloin sitä käytetään vain kerran salatessa ja purettaessa tietoa. Tällöin mahdollisen hyökkääjän on hankalampi paljastaa salattu tieto differentiaalisen kryptoanalyysin avulla. Kryptoanalyysissa hyökkääjä pyrkii paljastamaan avaimen syöttämällä algoritmin ja näytteet, jotka ovat salattu salausavaimella.

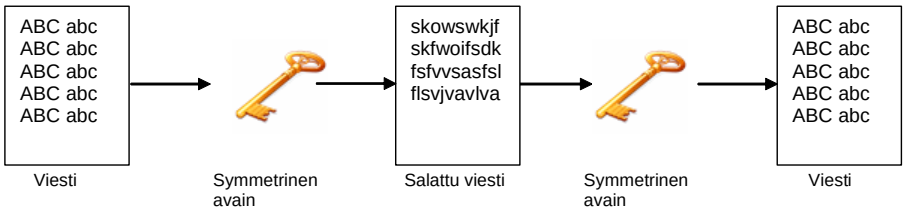
- sopiminen tavasta, jolla avain siirretään. Avain tulee salata vahvasti siirron aikana lähettäjän ja vastaanottajan välillä tai se lähetetään jollakin muulla tavalla kuin verkon kautta. [1, s. 4.]

2.2 Symmetrinen ja epäsymmetrinen tiedon salaus

Salauksessa käytetään yleisesti kahta menetelmää: symmetrisen avaimen ja julkisen avaimen (epäsymmetrisen avaimen) menetelmää.

2.2.1 Symmetrinen salaus

Symmetrisellä salauksella tarkoitetaan salausmenetelmää, jossa informaatio salataan ja salaus puretaan yhdellä ainoalla avaimella. Kuva 2 näyttää salauksen yksinkertaistettuna. Tässä ongelma on, että vähintään kahden henkilön on tiedettävä salausavain eikä salausavainta välitetä viestin mukana. Hyvänä puolena on, että tällä menetelmällä voidaan salata suuri määrä tietoa lyhyessä ajassa johtuen algoritmin yksinkertaisuudesta verrattuna epäsymmetriseen salaukseen verrattuna. Kun data salataan symmetrisellä salausmenetelmällä, lähettäjä generoi yleensä satunnaisen symmetrisen avaimen. Avaimen pituus, joka yleensä mitataan bittijonon pituutena, määräytyy algoritmin ja sovelluksen mukaan. Kun avain on generoitu, avainta käytetään salaamaan selväkielinen tieto salatuksi tiedoksi. Salattu tieto lähetetään tämän jälkeen vastaanottajalle. Vastaanottaja purkaa tiedon tällä samalla avaimella. Avaimen lähettäminen on suurin tietoturvariski symmetristä salausta käytettäessä. [2, s. 304-305; 1, s. 5.]



Kuva 2. Tiedon salaus

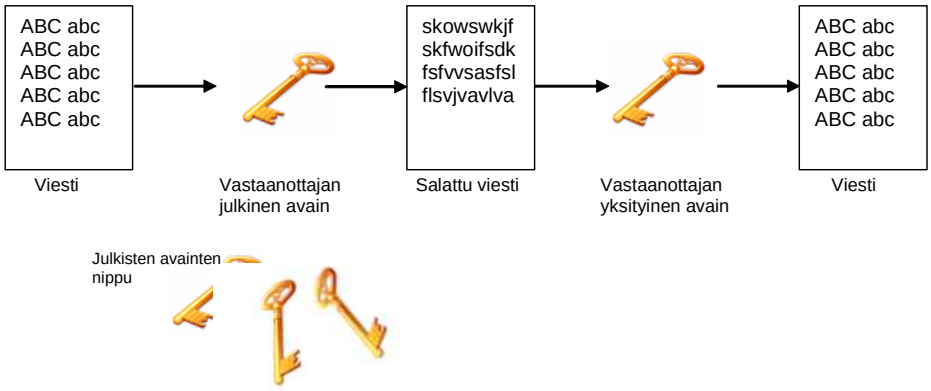
Symmetrisessä salauksessa käytetään mm. seuraavia algoritmejä:

- Data Encryption Standard (DES). Salaus on luonteeltaan symmetrinen lohkosalain. Tässä salauksessa lohkon pituus on 64 bittiä ja avaimen efektiivinen pituus on 56 bittiä. Algoritmia ei pidetä enää turvallisena. Salaus on murrettu Brute-force-menetelmällä alle 24 tunnissa.

- Data Encryption Standard XORed (DESX). Tämä on vahvempi variaatio DES-salauksesta. Selväkielinen data prosessoidaan XOR-funktiolla 64-bittisen avainmateriaalin kanssa ennen kuin tehdään varsinainen salaus DES-algoritmilla. Salattu tieto prosessoidaan vielä kertaalleen 64-bittisen avainmateriaalin kanssa. Näin saatu salaus on vahvempi kuin pelkkä 56-bittinen salaus.
- Rivest's Cipher version 2 (RC2). Lohkosalain, jossa on vaihtuvan kokoinen avain. Avaimen koko 8 - 128 bittiä 8 bitin välein. Lohkon koko 64 bittiä. Salaus on haavoittuva kryptoanalyysia vastaan.
- RC4. Suosittu jonosalain, jota käytetään mm. SSL- ja WEP-salauksissa.
- Triple DES (3DES). Muunnelma DES-salauksesta. DES-salaus suoritetaan kolme kertaa salattavalle tiedolle. Tieto salataan avaimella A, puretaan avaimella B ja salataan uudelleen avaimella C. Usein salauksessa käytetään vain kahta avainta, jolloin salaus menettää tehoaan.
- Advanced Encryption Standard (AES). Kehitetty DES-salauksen seuraajaksi. Salain voi käyttää avaimia, joiden pituus on 128-, 192- ja 256-bittiä. [1, s. 5.]

2.2.2 Epäsymmetrinen salaus

Epäsymmetrisessä salausmenetelmässä, jota on kuvattu kuvassa 3, informaatio salataan julkisella avaimella (public key) ja puretaan vastaanottajan yksityisellä avaimella (private key). Menetelmässä on kaksi toisistaan riippuvaa avainta; julkinen avain voidaan jakaa vapaasti, mutta yksityinen avain pidetään tarkasti vartioituna omana tietona. Tämä lisää salauksen tietoturvaa, kun avainta ei siirretä verkossa. Epäsymmetrinen salausmenetelmä on raskas menetelmä. Ohjelmistopohjaisessa salauksessa se on vähintään 100 kertaa hitaampi kuin symmetrinen salaus ja laitteistopohjaisessa jopa 10 000 kertaa hitaampi. Tästä syystä julkisen avaimen menetelmään yhdistetään symmetrinen salausmenetelmä, joka on kevyempi. Siis varsinainen tieto salataan symmetrisellä avaimella ja tämä symmetrinen avain salataan vastaanottajan julkisella avaimella. Tällöin vastaanottaja purkaa omalla yksityisellä avaimellaan salauksen, jolloin symmetrinen avain vapautuu käyttöön ja sillä voidaan poistaa salaus varsinaisesta datasta. [1, s. 7; 2, s. 305.]



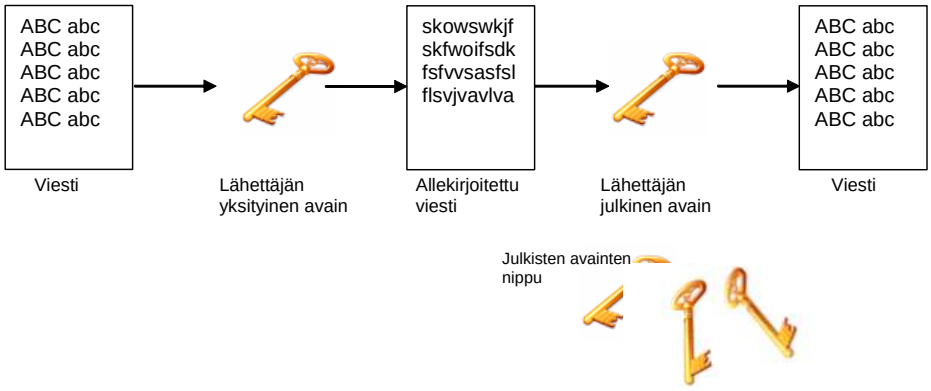
Kuva 3. Epäsymmetrinen salaus

Epäsymmetrisessä salauksessa käytetään mm. seuraavia algoritmeja:

- Diffie-Hellman-avaimenvaihtoprotokolla. Algoritmi perustuu matemaattiseen funktioon, jonka avulla osapuolet voivat generoida yhteisen salaisuuden. Tämän yhteisen salaisuuden avulla voidaan generoida salattu avain tiedon salausta varten. Huomattavaa on, ettei algoritmia käytettäessä todenneta vastapuolta. Diffie-Hellman oli ensimmäinen julkisen avaimen salausmenetelmä.
- Rivest Shamir Adleman (RSA). Algoritmia käytetään salaukseen sekä todentamiseen. Erittäin suurien alkulukujen (jaollinen vain itsellään) tulontekijöihinjako on vaikeaa. Siis tämä salausfunktio on helppo laskea, mutta hankala ja aikaa vievä laskea taaksepäin. Avaimen pituus 1024 bittiä tai pitempi.
- Digital Signature Algorithm (DSA). Algoritmia käytetään vain todentamiseen. Sillä ei voi salata tietoa. Avaimen pituus 1024 bittiä. [1, s. 9-10.]

2.2.3 Lähettäjän todentaminen

Epäsymmetrisessä salausmenetelmässä voidaan lähettäjä todentaa. Tällöin lähettäjä allekirjoittaa viestin omalla yksityisellä avaimellaan. Vastaanottaja todentaa lähettäjän käyttämällä lähettäjän julkista avainta. Tässä luonnollisesti korostuu kolmannen luotetun osapuolen rooli; se varmentaa lähettäjän julkisen avaimen, jotta se todella kuuluu lähettäjälle (kuva 4). Lisäksi yksityinen avain ei saa päätyä kenenkään ulkopuolisen käsiin, jolloin avainta voidaan väärinkäyttää.



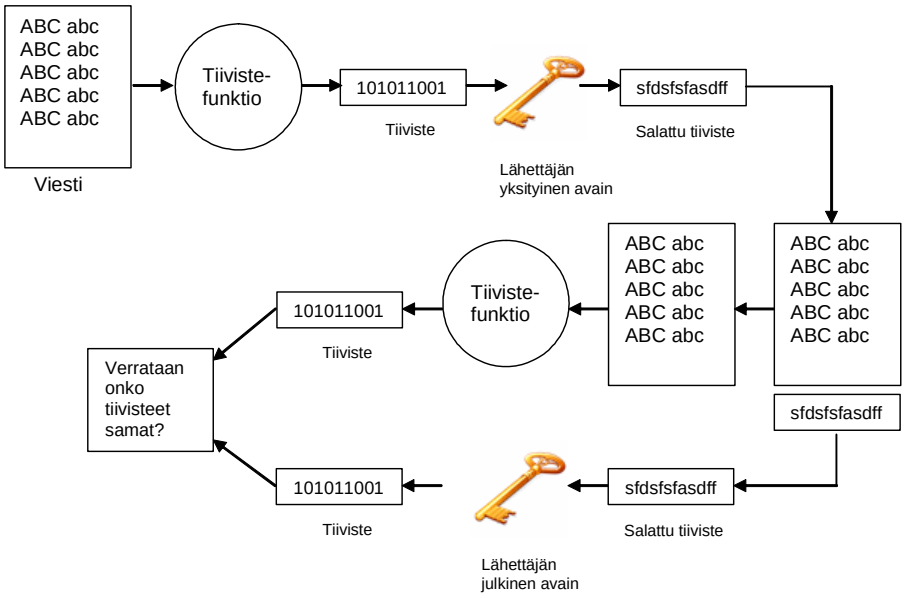
Kuva 4. Lähettäjän todentaminen digitaalisella allekirjoituksella

Digitaalinen allekirjoitus suojaa tietoa myös luvattomalta muuttamiselta todentamisen lisäksi. Tiedosta lasketaan tiiviste matemaattisella menetelmällä. Tämä tiiviste on ainutkertainen. Jos lähetettävä tieto muuttuu edes hiukan, myös tiiviste muuttuu.

Sovelluksissa laskettu tiiviste yleensä vielä allekirjoitetaan lähettäjän yksityisellä avaimella (kuva 5). Vastaanottaja purkaa tiivisteen lähettäjän julkisella avaimella. Tätä tiivistettä verrataan vastaanottajan itsensä laskemaan tiivisteeseen vastaanotetusta tiedosta. Jos tiivisteet eivät ole samanlaiset, joko tieto on muuttunut matkalla tai lähettäjä ei ole oikea. Tarvittaessa lähettäjä voi vielä salata tiedon. [1, s. 12; 2, s. 305.]

Tiivisteissä käytetään mm. seuraavia algoritmeja:

- Message Digest 5 (MD5). Viesti voi olla minkä mittainen tahansa. Lopputuloksena on 128-bittinen tiiviste.
- Secure Hash Algorithm 1 (SHA1). Viesti voi olla maksimissaan (2^{64} - 1) bittiä pitkä. Lopputuloksena syntyy 160-bittinen tiiviste. SHA1-algoritmia pidetään turvallisempana kuin MD5:ttä. [1, s. 12.]



Kuva 5. Tiivisteen allekirjoittaminen

2.3 CNG eli Cryptography Next Generation

Windows 2008 -ympäristön tietoturvauudistukset tunnetaan nimellä CNG eli Cryptography Next Generation. Parannukset pitävät sisällään uusien Suite B -algoritmien käyttöönoton. Suite B on NSA:n uusi määritys, jolla lisätään turvaa uusien salausalgoritmien, kuten elliptisten käyrien, avulla. Suite B sisältää AES-salausalgoritmit 128- ja 256-bittisillä avaimenpituuksilla symmetristä salausta varten, SHA-2-tiivistealgoritmit (SHA-256, SHA-384 ja SHA-512), Elliptic Curve Diffie-Hellman (ECDH) julkisen avaimen salausta varten ja Elliptic Curve Digital Signature Algorithm (ECDSA) allekirjoitusta varten. Suite B:n määritysten mukaan ympäristöt jaetaan salaisiin ja erittäin salaisiin ympäristöihin. Salaisissa ympäristöissä käytetään lähinnä 256-bittisiä avainten pituuksia ja erittäin salaisissa ympäristöissä lähinnä 384-bittisiä avainten pituuksia kuten taulukko 1 esittää. Suite B:n muikaisessa ympäristössä CA voi myöntää ECC-sertifikaatteja ja asiakkaat voivat hakea ECC- ja SHA-2-sertifikaatteja. Uusien algoritmien käyttö vaatii työasemapäässä vähintään Windows Vista -käyttöjärjestelmän ja palvelinpäässä Windows Server 2008- tai Windows Server 2008 R2 -käyttöjärjestelmän.

Taulukko 1. Suite B:n algoritmit

Algoritmi	**Salainen**	**Erittäin salainen**
Salaus: Advanced Standard (AES)	128 bittiä	256 bittiä
Digitaalinen allekirjoitus: Elliptic Curve Digital Signature Algorithm (ECDSA)	256 bittinen elliptinen käyrä.	384 bittinen elliptinen käyrä.
Avaimen vaihto: Elliptic Curve Diffie-Hellman (ECDH)	256 bittinen elliptinen käyrä.	384 bittinen elliptinen käyrä.
Tiiviste: Secure Hash Algorithm (SHA)	SHA-256	SHA-384

[8]

3 JULKISEN AVAIMEN JÄRJESTELMÄ ELI PKI

PKI on toimintamalli, jossa tieto salataan avoimissa tietoverkoissa epäsymmetristä salausta käyttäen. Järjestelmä luo salauksen tarvitsemat avainparit sekä ylläpitää avainhakemistoja ja sulkulistoja. PKI on yhdistelmä ohjelmistoja, salaustekniikoita ja palveluita, jotka mahdollistavat yrityksen tietoturvaratkaisujen rakentamisen; sertifikaattien, julkisten avainten ja yksityisten avainten hallinnan. Järjestelmä tarvitaan nimenomaan siksi, että viestin lähettäjä saa haltuunsa vastaanottajan julkisen avaimen ja voi olla varma siitä, että tätä julkista avainta vastaava yksityinen avain kuuluu viestin vastaanottajalle. PKI yhdistää sertifikaatit, julkisen avaimen salauksen ja sertifiointiauktoriteetit eli varmentajat (CA) yhdeksi tietoturva-arkkitehtuuriksi. Lisäksi se mahdollistaa tiedon luottamuksellisuuden takaamisen, tiedonvälityksen osapuolten autentikoinnin (tunnistamisen) ja tiedon muuttumattomuuden varmistamisen (digitaalinen allekirjoitus) sekä lakisääteisesti sitovan elektronisen allekirjoittamisen.

Luottamus on olennainen osa PKI-järjestelmää. Kolmas osapuoli tarvitaan varmistamaan kahden viestivän osapuolen henkilöllisyys. Kolmas osapuoli on varmentaja, johon molemmat viestivät osapuolet luottavat. Varmentaja myöntää sertifikaatin, jossa yhdistetään toisiinsa julkinen avain ja sen haltija. Luottamuksellinen viestintä ja digitaaliset allekirjoitukset toimivat vaikka osapuolet eivät tuntisikaan toisiaan. [2, s. 305-306.]

3.1 Sertifikaatit

Sertifikaatti eli varmenne on työkalu tunnistamista ja tiedon salaamista varten. Se on standardoitu tapa kytkeä julkinen avain tiettyyn identiteettiin, joka voi olla esimerkiksi henkilö, työasema tai palvelin. Sertifikaatin myöntää varmentaja (CA). CA allekirjoittaa sertifikaatin omalla salaisella avaimellaan, jolloin sertifikaatin sisältöä ei päästä huomaamatta muuttamaan. Perustana on, että CA on luotettu taho, joka tunnistaa käyttäjät ennen sertifikaattien myöntämistä ja se myös huolehtii omasta sertifikaatistaan sekä avaimistaan. Tämän luotetun osapuolen avulla voidaan luottaa siihen, että sertifikaatin omistaja on se, kuka hän väittää olevansa. Sertifikaatteja voidaan myötää eri tarkoituksiin; esim. verkkokäyttäjien tunnistukseen, palvelinten tunnistukseen, salattuun sähköpostiin, verkkoyhteyksien salaamiseen tai ohjelmakoodin allekirjoitukseen. Windows-ympäristössä sertifikaattia voidaan käyttää mm. toimialueeseen (domain) kirjautumiseen. CA käyttää sertifikaattia myös varmistaessaan itsensä muille käyttäjille. CA:n tehtäviin kuuluu luonnollisesti sertifikaattien myöntäminen eri identiteeteille sekä koko sertifikaatin elinkaaresta huolehtiminen. CA luo hierarkian, jolla sertifikaatit hallitaan. Sertifikaatti voidaan julkaista esim. jossain määrätyssä hakemistossa tai www-osoitteessa. Sertifikaatit määritellään ITU:n X.509 standardissa. Sertifikaatti sisältää mm. seuraavia asioita:

- käyttäjän nimi
- käyttäjän sähköpostiosoite
- koneen nimi
- ajan milloin sertifikaatti on voimassa
- sertifikaatin sarjanumero
- CA:n nimi, joka on myöntänyt sertifikaatin
- sertifikaattien käyttötavat (esim. sähköposti)
- sulkulistan sijaintipaikka.

PKI:ssa voidaan käyttää kolmenlaisia sertifikaatteja:

- X.509 versio 1
- X.509 versio 2
- X.509 versio 3.

Eri versioiden X.509-sertifikaattien sisältö selviää tarkemmin seuraavasta taulukosta (taulukko 2).

Taulukko 2. X.509-varmenteen sisältö.

X.509-sertifikaatti	ver.1	ver.2	ver.3
Versionumero	x	x	x
Sarjanumero	x	x	x
Allekirjoitusalgoritmi	x	x	x
Myöntäjän nimi	x	x	x
Voimassaoloaika	x	x	x
Kohteen nimi	x	x	x
Kohteen julkinen avain	x	x	x
Myöntäjän yksikäsitteinen tunniste		x	x
Kohteen yksikäsitteinen tunniste		x	x
Laajennokset			x
Myöntäjän digitaalinen allekirjoitus	x	x	x

CA allekirjoittaa

Versio 1 julkaistiin vuonna 1988. Tämä versio ei ole juurikaan enää käytössä. Myöntäjän nimi- ja kohteen nimi -kentät mahdollistavat luottoketjun muodostamisen. Luottoketjun avulla voidaan myönnetty sertifikaatti yhdistää sen myöntäjään.

Versio 2 julkaistiin vuonna 1993. Se lisäsi sertifikaattiin kaksi kenttää: Myöntäjän yksikäsitteisen tunnisteen ja kohteen yksikäsitteisen tunnisteen. Nämä kentät helpottivat sertifikaatin uusimista sekä luottoketjun muodostamista. Versio 2:sta ei kuitenkaan tullut yleisesti tuettua formaattia.

Versio 3 julkaistiin vuonna 1996. Merkittävin uudistus oli laajennokset, joilla korjattiin aikaisempien versioiden puutteita. Laajennokset ilmaisevat mm. avainten tunnisteet ja käyttötarkoituksen, sertifikaattikäytännöt, erilaiset rajoitukset sertifikaattien käyttöön, nimien laajemman käytön sekä sulkulistan ja myöntäjän sertifikaattien julkaisupaikan.

Versio 3 on nykyisin yleisesti käytössä. [1, s. 17-26; 2, s. 306-308; 6.]

3.2 Sertifikaatin elinkaari

Sertifikaattia ei voida käyttää ikuisesti, koska muutoin mahdollisella hyökkääjällä on paljon aikaa murtaa yksityinen avain. Sertifikaateilla on tietyn mittainen elinkaari ja ne vanhenevat elinkaaren lopussa. Elinkaarta voidaan pidentää myöntämällä sertifikaatti uudelleen, muussa tapauksessa sen käyttö lopetetaan. Elinkaaren pituuteen vaikuttavat sertifikaatin käyttötarkoitus ja tietoturva-asiat. Yleensä pitempi avain antaa sertifikaatille ja avaimelle pitemmän käyttöajan. Pitempi käyttöaika vähentää ylläpidon määrää ja vähen-

tää myös kustannuksia. Asioita, jotka vaikuttavat avaimen pituuteen, tulee miettiä sertifikaattia myönnettäessä:

- Avaimen pituus: Pitempi avain on vaikeampi murtaa.
- CA:n luotettavuus. Kuinka luotettava CA on ja kuinka hyvin se hoitaa tietoturvan.
- Salauksessa käytettävän teknologian vahvuus: Mikä on tällä hetkellä esim. pöytäkoneiden laskentateho; kuinka nopeasti se purkaa käytetyn salauksen. Käytetäänkö laitteistoon perustuvaa tunnistusta/salausta, esim. toimikortit ja lukijat.
- Kenelle sertifikaatti luodaan. Yleensä oman yrityksen työntekijään luotetaan enemmän kuin vieraaseen henkilöön. Näin oman henkilökunnan sertifikaattien elinkaari voisi olla pitempi.
- CA:n myöntämien sertifikaattien määrä. Mitä julkisempi CA on, sen houkuttelevampi kohde se on murtautumisyrityksille. [1, s. 7; 2, s. 310-311.]

3.3 CA:n sertifikaatin voimassaoloaika

CA:lla on myös oma sertifikaattinsa, johon sen toiminta perustuu. Yleensä CA myöntää itselleen oman sertifikaatin tai se on hankittu joltakin toiselta luotetulta taholta. Joka tapauksessa CA:n oman sertifikaatin voimassaoloaika (elinkaari) on erittäin tärkeä asia huomioida varsinkin, jos sertifikaattipalvelua ylläpidetään yrityksen sisällä itse.

CA ei voi myöntää sertifikaatteja, jos sen oman sertifikaatin voimassaoloaika umpeutuu eikä se voi myöntää sertifikaatteja pitemmäksi aikaa kuin sen oma sertifikaatti on voimassa. Siis jos CA:n sertifikaatti vanhenee, vanhenevat myös kaikki muut CA:n myöntämät sertifikaatit! Näin ollen täytyy tarkkaan miettiä käytäntö, kuinka sertifikaatti uusitaan. Esim. jos CA:n sertifikaatti on voimassa viisi vuotta, pitää se uusia neljän vuoden jälkeen, jotta CA voi myöntää sertifikaatteja, joiden voimassaoloaika on vuosi. Huomioitava on myös, että sertifikaattien voimassaoloajan tulee olla lyhyempi kuin sen ajan, joka kuluu mahdolliselta murtautujalta murtaa CA:n avain. [2, s. 312.]

3.4 Sertifikaattien sulkeminen

CA julkaisee sulkulistaa, jossa ilmoitetaan sertifikaatit, jotka eivät ole enää voimassa. Sulkulistalla näkyy myös syy miksi sertifikaatti on lakkautettu sekä aika, milloin sulkeminen on tapahtunut. Mahdollisia syitä ovat esim. avain on

paljastunut, henkilö lopettanut työsuhteen, sertifikaatti on korvattu toisella. Sovellus voi tarkastaa sulkulistalta, onko sertifikaatti vielä voimassa. Asiakassovellus normaalisti tallentaa sulkulistan välimuistiinsa, jotta sen ei joka kerta tarvitse ottaa yhteyttä CA:han. Sulkulista säilyy välimuistissa tietyn ajan, jonka jälkeen käydään tarkastamassa mahdolliset muutokset. Tämä aiheuttaa myös ongelman. On mahdollista, että sertifikaatti laitetaan sulkulistalle, mutta asiakas ei lue sulkulistaa vaan hakee tiedon välimuististaan. Ratkaisuna tähän on OCSP-palvelin (käytetään myös nimitystä OCSP-responderi), josta sulkulistatieto on saatavissa reaaliaikaisesti. Windows 2003/XP -ympäristössä tämä vaatii lisäohjelmien asentamista, mutta Windows 2009/Vista/Windows 7 -ympäristössä on valmis tuki OCSP-tekniikalle. OCSP-palvelimen haittapuoli verrattuna sulkulistoihin on se, että palvelimen tulee olla verkkoyhteydessä koko ajan reaaliaikaisesti. Käytännössä tämä vaatii vikasietoisen järjestelmän. Palvelimelle onkin asennettava klusteri, jolloin palvelun vikaantuessa palvelu siirtyy toiselle palvelimelle automaattisesti. Tämä tekee siitä luonnollisesti vaikeammin hallittavan kuin sulkulistat sekä myös huomattavasti kalliimman ratkaisun. [2, s. 312-313; 6, s. 35.]

4 SERTIFIKAATTIPALVELUT JA HIERARKIA

Windowsin palvelinkäyttöjärjestelmän sertifikaattipalvelulla voidaan rakentaa koko CA-hierarkia tai asentaa se pelkästään yhteen koneeseen. Normaalisti PKI-ympäristö sisältää monta CA-palvelinkonetta. Osa palvelimista on irrotettu verkosta tietoturvasyistä ja osa on verkossa jakamassa sertifikaatteja asiakkaille. Käyttöjärjestelmä sisältää lisäksi useita työkaluja CA:n, sertifikaattien ja sertifikaattipohjien hallintaan. Käyttöjärjestelmän mukana tullut palvelu on tiukasti sidottu aktiivihakemistoon (tai se on mahdollista asentaa aktiivihakemistoympärisistöön), mikä helpottaa hallinnointia ja sertifikaattien jakamista asiakkaille. Näin ollen ryhmäkäytännöllä voidaan hallita käyttäjien ja koneiden sertifikaatit, jolloin ne voidaan jakaa jopa automaattisesti ilman ylläpitäjän toimenpiteitä. [2, s. 313.]

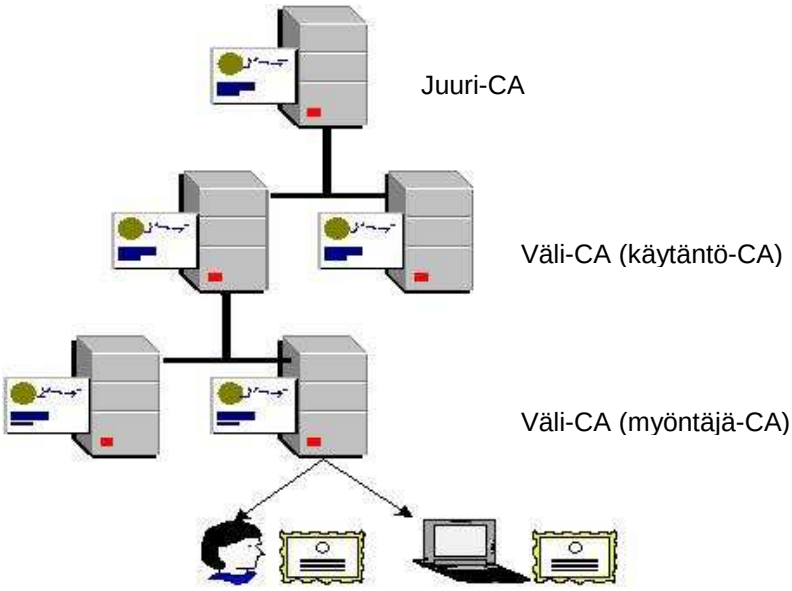
4.1 Juuri-CA

Ensimmäinen vaihe PKI-järjestelmän luonnissa on asentaa CA. Ensimmäinen CA, joka asennetaan, on juuri-CA. Juuri-CA voi olla kahta eri tyyppiä: enterprise tai standalone. Enterprise CA vaatii aktiivihakemiston asennuksen, joten se on harvoin käytetty tyyppi nimenomaan juuri-CA-palvelimessa;

normaalisti enterprise CA on käytössä alemmalla tasolla, kun asiakkaille jaetaan sertifikaatteja. Enterprise CA -ympäristö mahdollistaa sertifikaattien myöntämisen automaattisesti; esim. käyttäjä saa sertifikaatin automaattisesti salatessaan tiedostoja. Ominaisuus vähentää ylläpidon tarvetta, joten se saa aikaan kustannussäästöjä. Standalone CA:ta voidaan myös käyttää aktiivihakemistoympäristössä, mutta se ei kuitenkaan vaadi sitä. Automaattitoimintoja ei tueta, joten sertifikaatti anotaan web-selaimella. Normaalisti juuri-CA asennetaan standalone-tyyppiseksi ja lisäksi se kytketään pois verkosta tietoturvan takia kuten myöhemmin selostetaan. [1, s. 28-29; 2, s. 314.]

4.2 CA-hierarkiat

Hierarkisen CA-rakenteen muodostavat juuri-CA sekä yksi tai useampi väli-CA (kuva 6). Juuri-CA myöntää sertifikaatit väli-CA:ille, jotka edelleen myöntävät sertifikaatit joko toisille väli-CA:ille tai loppukäyttäjille. Väli-CA:t jaetaan vielä käytäntö-CA- ja myöntäjä-CA -palvelimiin. Normaalisti myöntäjä-CA jakaa sertifikaatit loppukäyttäjille ja käytäntö-CA toisille CA-palvelimille. Luottoketjun ansiosta väli-CA:t voivat myöntää loppukäyttäjille sertifikaatteja. Luottoketjua voidaan havainnollistaa kolmen ihmisen avulla. Jos Pekka luottaa Mattiin ja Matti luottaa Maijaan, tällöin myös Pekka luottaa Maijaan, koska Pekan uskottu kaveri Matti luottaa Maijaan. Tilanne on sama CA-palvelinten välillä ja tämä luottamus määritellään myöntämällä sertifikaatti luotetulle asiakkaalle. Käytännössä jos myönnetty sertifikaatti voidaan jäljittää juureen asti luottoketjun avulla, voidaan siis juuri-CA:han tällöin luottaa. Luottoketjun muodostamisessa käytetään apuna sertifikaatin kenttiä.



Kuva 6. Hierarkkinen CA-rakenne

Hierarkia voidaan rakentaa niin, että käytäntö-CA:t jakavat sertifikaatteja myöntäjä-CA:ille, jotka puolestaan jakavat sertifikaatit loppukäyttäjille (kuva 6). Väli-CA:t eivät ole pakollisia. Ne kuitenkin mahdollistavat laajemman hierarkian luomisen. Lisää tietoturvaa tuo, jos juuri-CA kytketään irti verkosta; hyökkäykset eivät ole tällöin mahdollisia juuri-CA:ta vastaan. Juuri-CA voidaan kytkeä irti verkosta, koska se myöntää sertifikaatteja ja julkaisee sulkulistoja hyvin harvoin. Eri CA:iden asentaminen on hyvin samantyyppistä. Jos juuri-CA on irrotettu verkosta, väli-CA:n asennuksessa sertifikaattihakemus tallennetaan tiedostoksi, joka toimitetaan manuaalisesti juuri-CA-koneeseen. Tällöin ei siis ole mahdollista automaattisesti saada verkon kautta tarvittavaa sertifikaattia juuri-CA:lta. Juuri-CA-koneessa tehty sertifikaatti palautetaan edelleen manuaalisesti väli-CA-koneeseen. Siis ylemmän tason CA varmentaa (osoittaa luottamuksensa) omalla sertifikaatillaan alemman tason CA:n. Näin toimitaan ketjun jokaisen CA:n kanssa. Näin käytännössä syntyy luottoketju, jonka asiakas voi tarkastaa. Juuri-CA-koneessa sertifikaattihakemus tehdään joko **web-selaimen** kautta tai erillisellä **certreq**-ohjelmalla. Web-selaimen käyttö vaatii web-palvelimen asentamista CA-koneeseen. Web-palvelimen asentaminen juuri-CA-koneeseen ei kuitenkaan ole välttämätöntä eikä myöskään suositeltavaa, koska se myöntää hyvin vähän sertifikaatteja, joten normaalisti käytetään certreq-ohjelmaa. Sertifikaattihakemus siis toimitetaan manuaalisesti ylemmän tason palvelimeen ja se on nähtävissä Certification Authority -konsolissa, joka löytyy Administrative Tools -ryhmästä.

Tässä konsolissa ylläpitäjä hyväksyy hakemuksen, jolloin syntyy sertifikaattitiedosto. Tämä tiedosto toimitetaan manuaalisesti väli-CA:lle, jossa se edelleen asennetaan.

Väli-CA:t (käytäntö-CA:t) voidaan määritellä niin, että ne jakavat vain tietyntyyppisiä sertifikaatteja. Esim. väli-CA jakaa sertifikaatteja tiettyyn nimiavaruuteen kuten rnko.fi tai jaettavat sertifikaatit ovat käytössä vain EFS-salauksessa tai älykorteissa. Lisäksi voidaan määritellä myös, että sertifikaatit myönnetään vain henkilökohtaisen tunnistautumisen jälkeen tai sertifikaatit myönnetään pelkästään käyttäjätunnuksen ja salasanan perusteella kirjauduttaessa järjestelmään.

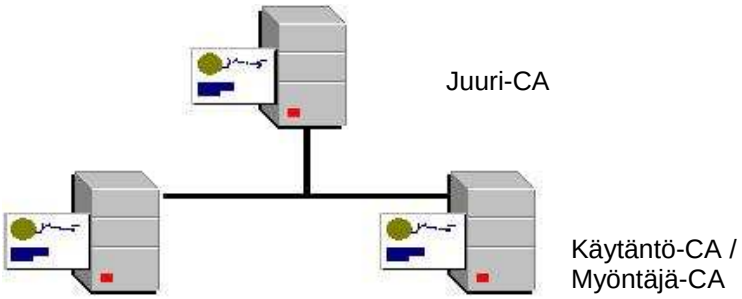
Seuraavaksi käydään lyhyesti läpi yleisimmät hierarkiatasot. Tasoja on normaalisti yhdestä kolmeen. Käytännössä useampaa kuin neljää tasoa ei kannata asentaa. Muuten rakenteesta tulee vaikeasti hallittava.

4.2.1 Yksitasoinen CA-hierarkia

Tässä hierarkiassa on vain yksi CA-kone. Se asennetaan enterprise juuri-CA -koneeksi, joka on toimialueen jäsen ja jakaa sertifikaatit asiakkaille. Yritykset, joissa on vähemmän kuin 300 käyttäjätiliä, voidaan asentaa yksitasoisiksi. Etuna on ympäristön yksinkertaisuus ja helppo hallinnointi sekä kustannussäästöt. Huonoja puolia ovat vähäinen tietoturva ja vikasietoisuuden puute. Jos CA-kone pettää, on koko sertifikaattipalvelu alhaalla. Tässä hierarkiassa avaimet tulisi suojata laitetasolla hsm-moduulilla tai vähintään älykortilla ja kortinlukijalla. [1, s. 67-68.]

4.2.2 Kaksitasoinen CA-hierarkia

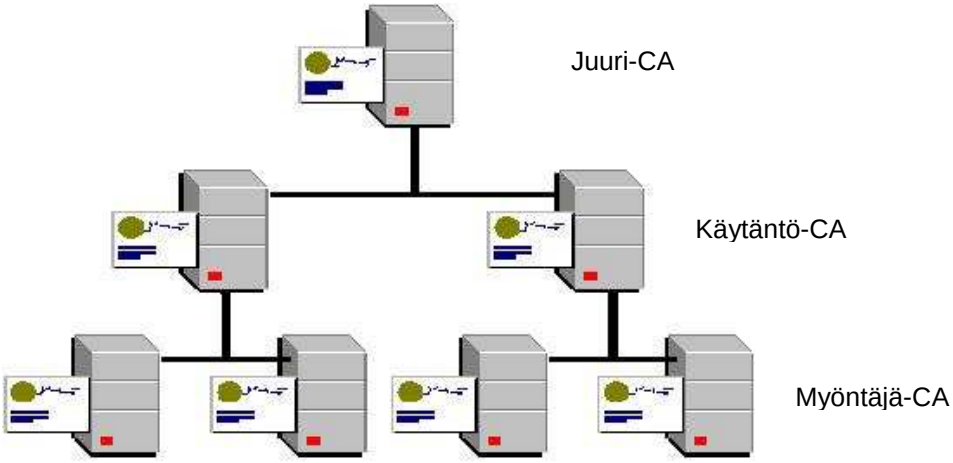
Tässä mallissa tietoturvatasoa voidaan nostaa. Juuri-CA voidaan kytkeä pois verkosta, jolloin se ei ole hyökkäysten kohteena. Juuri-CA asennetaan siis standalone CA -palvelimeksi, jolloin se ei ole domainin jäsen. Juuren alla on yksi tai useampi myöntäjä-CA (kuva 7). Myöntäjä-CA on käytännössä käytäntö-CA:n ja myöntäjä-CA:n yhdistelmä. Tämän toisen tason palvelimet jakavat sertifikaatit asiakkaille, joten palvelinten tulee olla jatkuvasti saatavilla verkossa. Tässä hierarkiassa myöntäjä-CA ja juuri-CA muodostavat ketjun. Vikasietoisuutta saadaan kasvatettua lisäämällä toiseen tasoon yksi tai useampi palvelin. Jos palvelin vikaantuu, samalla tasolla oleva toinen palvelin voi myöntää edelleen sertifikaatteja. [1, s. 68-69.]



Kuva 7. Kaksitasoinen hierarkia

4.2.3 Kolmitasoinen CA-hierarkia

Kolmitasoisella hierarkialla saavutetaan paras tietoturva (kuva 8). Myös sertifikaattien jako voidaan toteuttaa joustavammin. Tässä mallissa juuri-CA sijaitsee ylimmällä tasolla ja se voidaan poistaa verkosta kuten edellisessäkin mallissa. Juuri-CA:n alapuolella on yksi tai useampi käytäntö-CA -palvelin. Myös tämän toisen tason palvelimet on poistettu verkosta tuomaan lisäturvaa. Kolmannella tasolla sijaitsevat myöntäjä-CA -palvelimet, jotka jakavat sertifikaatit asiakkaille. [1, s. 69-70.]



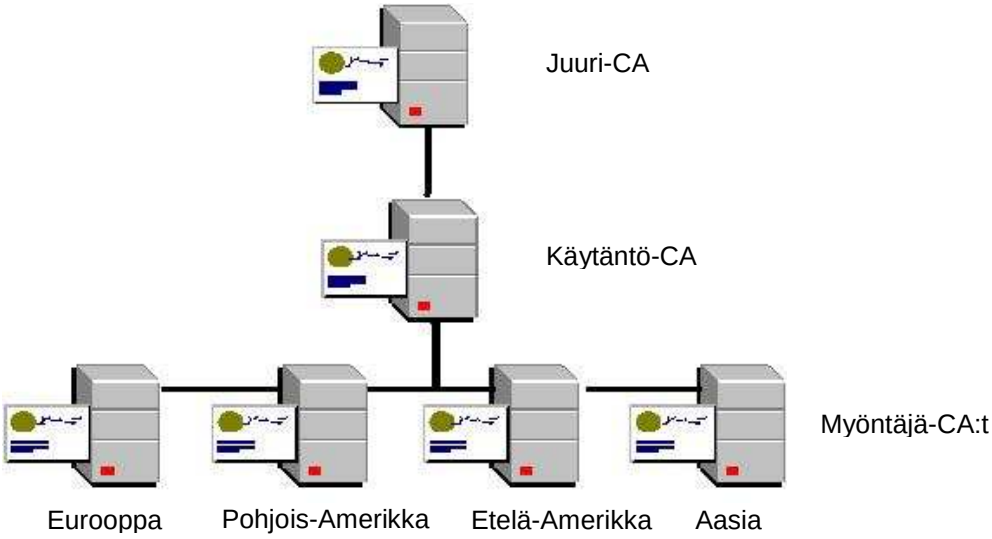
Kuva 8. Kolmetasoinen hierarkia

Tämä malli mahdollistaa sertifikaattien jakamisen laajalla maantieteellisellä alueella tai eri myöntäjä-CA:t voivat jakaa sertifikaatteja eri sertifikaattikäytäntöjen mukaan; käytäntö-CA:t rajoittavat, mitä sertifikaatteja myöntäjä-CA -palvelimet voivat myöntää. Esimerkiksi kahdesta myöntäjä-CA:sta toinen voi jakaa sertifikaatteja sähköpostin käyttöön ja toinen tiedostojen salausta varten. Eri käytäntö-CA-palvelimilla voidaan myös toteuttaa erilainen CPS. CPS on kuvaus menettelytavoista ja toimintaperiaatteista, joita sertifikaatteja myönnettäessä noudatetaan. CPS siis määritellään käytäntö-CA-

palvelimessa ja se on voimassa kaikissa palvelimissa, jotka ovat kyseisen käytäntö-CA:n alapuolella hierarkiassa. Myös hallinnoinnin hajauttaminen on mahdollista tässä arkkitehtuurissa. Maantieteellisesti etäällä sijaitsevat käytäntö-CA:t voivat olla paikallisten ylläpitäjien hallittavana.

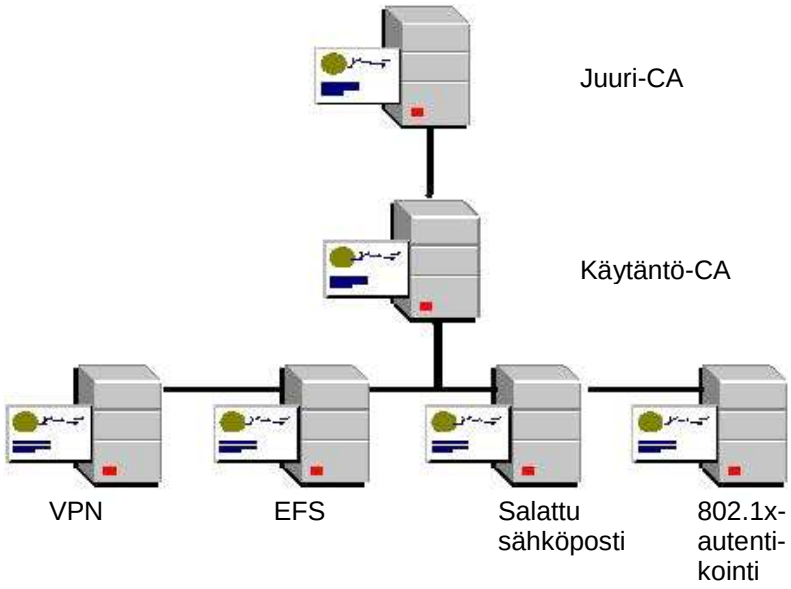
4.3 Myöntäjä-CA-tason suunnittelu

Myöntäjä-CA-sertifikaattipalvelinten määrä riippuu pitkälti siitä, kuinka paljon sertifikaatteja myönnetään asiakkaille sekä itse asiakkaiden määrästä. Asiakkaita voivat olla käyttäjät, koneet, palvelut tai verkon laitteet. Jos organisaation toiminta on levinnyt maantieteellisesti hyvin laajalle alueelle, tulee myös palvelimet sijoittaa tämän mukaan.



Kuva 9. Sertifikaattipalvelimet eri maanosissa

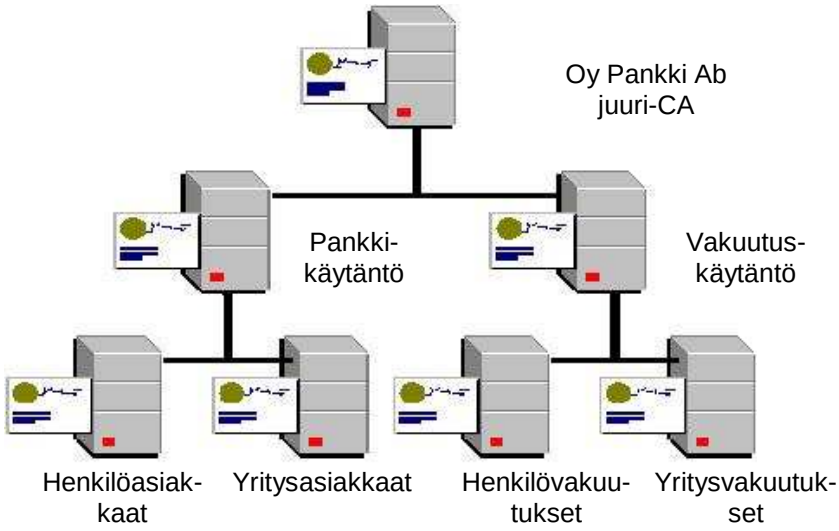
Kuva 9 esittää tilannetta, jossa eri maanosiin on sijoitettu omat sertifikaattipalvelimet sertifikaattien myöntämistä varten. Mahdollista on että, myös käytäntö-CA-palvelimia pitää asentaa enemmän, jos esimerkiksi eri maanosissa on erilaisia sertifikaattikäytäntöjä käytössä. Myös PKI-ympäristön hallinnointi ja ylläpito mahdollisesti vaikuttavat palvelinten määrään. Mahdollisesti jokaista PKI-sovellusta halutaan hallinnoida omassa palvelimessaan.



Kuva 10. Sertifikaattityypeillä omat palvelimet

Kuva 10 esittää tilannetta, jossa esimerkiksi sertifikaatit VPN:n käyttöä varten jaetaan omalta palvelimelta. Palvelinta ylläpitää ryhmä, jonka jokaisella jäsenellä on oma roolinsa sertifikaattien hallinnoinnissa vain omassa palvelimessaan. EFS-käyttöä varten sertifikaatit jaetaan omalta palvelimeltaan ja tätä palvelinta hallinnoi ja ylläpitää oma ryhmänsä organisaatiossa.

Jos organisaatio on suuri ja se on jakautunut eri liiketoiminta-aloihin, vaikuttaa tämä hierarkian rakenteeseen ja tätä kautta myöntäjä-CA-palvelinten määrään.



Kuva 11 Organisaatioperustainen rakenne

Kuva 11 esittää kuvitteellista pankki-organisaatiota, jossa perinteisen pankkitoiminnan lisäksi hoidetaan vakuutusasioita. Molemmilla puolilla on kaksi

osastoa, osasto henkilöasiakkaita varten ja osasto yritysasiakkaita varten. Sertifikaatit jaetaan työntekijöille osastoittain omista palvelimista. [1, s. 71-73.]

4.4 Arkkitehtuurin valinta

Myöntäjä-CA-tason suunnittelussa esille tulleet asiat, kuten organisaation koko ja toimiala sekä hallinnointimalli, vaikuttavat arkkitehtuurin valintaan. Arkkitehtuuria valittaessa tulee miettiä seuraavia asioita:

- käytettävät pki-sovellukset
- tietoturva
- tekniset vaatimukset
- liiketoiminnan vaatimukset
- ulkoiset vaatimukset. [1, s. 73-74]

4.4.1 Käytettävät PKI-sovellukset

Organisaation tarpeet määrittelevät käytettävät PKI-sovellukset. Seuraavassa on lueteltu lyhyesti yleisesti käytettyjä sovelluksia PKI-ympäristössä.

802.1x-autentikointi mahdollistaa käyttäjien ja koneiden autentikoinnin eli todentamisen 802.11-standardin mukaiseen langattomaan verkkoon tai Ethernet-verkkoon pääsyn yhteydessä. Tämä EAP/TLS-autentikoituminen tapahtuu RADIUS-palvelimen kautta.

Digitaalinen allekirjoitus mahdollistaa lähettäjän tunnistamisen sekä sen, ettei tietoa ole muutettu siirron aikana. Lisäksi tähän tarkoitukseen myönnetty sertifikaatti mahdollistaa lähettäjän kiistämättömyyden eli lähettäjä ei voi kieltää lähettäneensä tietoa.

EFS-salauksessa käytetään molempien symmetrisen ja epäsymmetrisen salauksen ominaisuuksia hyväksi. Tiedosto salataan symmetrisellä avaimella, joka edelleen salataan käyttäjän julkisella avaimella. Symmetrinen avain liitetään tiedoston mukaan salattuna. Tiedosto avautuu käyttäjän yksityisellä avaimella. EFS tarjoaa kaksi tapaa varautua mahdollisiin ongelmiin. Järjestelmään voidaan määritellä palautusagentti, joka voi myös purkaa salauksen tiedostoista. Lisäksi on mahdollista määritellä avaimen palautusagentti, joka voi tarvittaessa palauttaa käyttäjän avaimen. Itse EFS-salausta varten käyt-

täjä tarvitsee sertifikaatin, mutta myös palautukseen liittyvät agentit tarvitsevat molemmat omat sertifikaattinsa.

SSL-sertifikaatit www-palvelimissa mahdollistavat itse palvelimen tunnistamisen ja tiedon salaamisen asiakkaan ja palvelimen välillä. Siis palvelin on varmasti se, mikä se kertoo olevansa. Lisäksi asiakkaan on mahdollista hankkia sertifikaatti, jolla palvelin voi varmistua asiakkaan aitoudesta.

IPSec mahdollistaa kahden osapuolen autentikoitumisen sertifikaattien avulla. Autentikoitumisen jälkeen osapuolet voivat käyttää digitaalista allekirjoitusta ja tiedon salaamista kaikessa liikenteessä verkon yli.

Salattu sähköposti mahdollistaa tiedon salaamisen ja eheyden sekä kiistämättömyyden. Sertifikaatilla voidaan varmistaa lähettäjä ja tiedon siirto salattuna sekä tiedon muuttumattomuus matkalla.

Älykortit tuovat lisäturvaa kirjauduttaessa verkkoon tai eri palveluihin. Käyttäjällä tulee olla kyseinen kortti hallussaan sekä hänen pitää tietää kortin PIN-tunnus. Tämä tuo lisäturvaa verrattuna perinteiseen kirjautumiseen käyttäjätunnuksella ja salasanalla.

Ohjelmistojen allekirjoitus tuo lisäturvaa eri sovellusohjelmien ja käyttöjärjestelmien käytölle. Makrot, ajurit sekä muut ohjelmakomponentit voidaan allekirjoittaa, jolloin niiden käyttö tai asennus voidaan tarvittaessa estää.

VPN on käytössä lähinnä etäyhteyksissä. PPTP- tai L2TP-protokollalla muodostetaan tunneli organisaation verkkoon etäpisteestä julkisen verkon yli. Sertifikaattia voidaan käyttää käyttäjän autentikoinnissa.

Sertifikaatteja voidaan myöntää käyttäjille, koneille, palveluille sekä verkon laitteille lähinnä edellä kuvattuihin tarkoituksiin. Käyttäjän sertifikaatti identifioi käyttäjän. Siis sertifikaatti varmistaa, että käyttäjä on se, kuka hän väittää olevansa. Käyttäjäsertifikaatti voi mahdollistaa kaikkien sovellusten käytön tai se voidaan rajoittaa vaikkapa vain EFS-salausta varten. Käyttäjäsertifikaattiin voidaan siis liittää ne ominaisuudet, jotka organisaatio tarvitsee.

Konesertifikaatti identifioi tietokoneen. Asiakas voi olla käyttäjä tai toinen tietokone, joka ottaa yhteyttä palvelua tarjoavaan koneeseen. Fyysisesti sertifikaatti on tallennettu koneen Local Machine certificate -säiliöön. Säiliön sisältöä voi tutkia mm. mmc-konsolilla tehdyllä Certificates-työkalulla. Konesertifi-

kaatti voi olla myönnetty asiakkaalle tai palvelimelle. Tämä käyttötarkoitus määritellään sertifikaatin laajennoksissa. Jos sertifikaatti on myönnetty asiakkaan autentikoitumista varten palvelinkoneelle, on sertifikaatin Enhanced Key Usage- (EKU) tai Application Policies -laajennokseen merkitty Client Authentication OID. Jos taas sertifikaatti on palvelinkoneen identiteetin varmistamiseen, kun asiakas ottaa siihen yhteyttä, on laajennukseen merkitty Server Authentication OID. OID siis määrittelee sertifikaatin käyttötarkoituksen. OID on käsitelty tarkemmin kappaleessa 13 OID-tunnukset.

Palvelut tarvitsevat sertifikaatteja autentikoitumista tai tiedon salaamista varten. Itse asiassa palveluiden sertifikaatit ovat joko kone- tai käyttäjäsertifikaatteja. Myönnetty sertifikaatti asennetaan Local Machine store -säiliöön tai käyttäjätilin, joka on liitetty palveluun, profiiliin. Esimerkiksi www-palvelimen SSL-sertifikaatti on tallennettu Local Machine store -säiliöön ja EFS-palautusagentin sertifikaatti on tallennettu käyttäjätilin, joka on annettu palautusagentille, profiiliin.

Erilaiset VPN-, palomuuri- ja reititinlaitteet mahdollistavat sertifikaatin asentamisen asiakas/palvelin-autentikointia varten. Asennustapa on laitekohtainen, joten asennuksessa kannattaa turvautua laitteen manuaaliin. [1, s. 74-76.]

4.4.2 Tietoturva

Organisaatiolla tulisi olla määriteltynä tietoturvakäytäntö, jossa määritellään tietoturvavaatimukset PKI:n suunnittelua ja käyttöä varten. Fyysistä turvallisuutta varten jotkin CA-koneista voidaan kytkeä irti verkosta. Kaksitasoisessa mallissa juuri-CA voidaan poistaa ja kolmitasoisessa voidaan juuri-CA:n lisäksi poistaa käytäntö-CA. Verkosta poistetut palvelimet, lähinnä niiden kiintolevyt, tulee tallentaa fyysisesti turvalliseen paikkaan. Verkossa toimiva palvelin tulee sijoittaa fyysisesti turvalliseen huoneeseen, jonka käyttöä rajoitetaan esimerkiksi kulunvalvonnan keinoin. Palvelimesta tulee myös poistaa ylimääräiset palvelut. Käytännössä sertifikaattipalvelin ei tarvitse muita palveluita kuin itse sertifikaattipalvelun. Myös www-palvelimen, jossa julkaistaan sertifikaatit ja sulkulistat, voi asentaa johonkin toiseen palvelimeen; tai vaihtoehtoisesti kannattaa käyttää hyväksi jo olemassa olevaa www-palvelinta. Lisäksi palvelimeen tulee tehdä tietoturva-asetukset organisaatiossa testatun tietoturvapohjan perusteella. CA:n yksityisen avaimen tallentamista tulee myös miettiä. Riittääkö softapohjainen CSP suojaamaan avain-

ta vai tarvitaanko älykortti tai jopa HSM-laite? Sertifikaattien myöntämistapa tulee myös määrittää. Esimerkiksi myönnetäänkö sertifikaatit perustuen käyttäjätunnukseen ja salasanaan vai vaaditaanko fyysinen tunnistautuminen kuvallisen henkilökortin avulla. [1, s. 76-78.]

4.4.3 Tekniset vaatimukset

Teknisiin vaatimuksiin luetaan mm. PKI:n ylläpitäjien määrittäminen, riskien minimointi ongelmien tullessa sekä sertifikaattien voimassaoloaika ja julkaisupaikka.

Jos ylläpito pitää delegoida pois omasta hallinnasta, kannattaa asentaa ylimääräinen CA-palvelin ja määrittää tähän palvelimeen ylläpitäjille tarvittavat roolit. Ylläpitäjille on mahdollista antaa seuraavat roolit kussakin CA-palvelimessa:

- **CA administrator** on vastuussa tilien hallinnoinnista ja avainparien luomisesta sekä yleensäkin CA-koneen asennuksista ja konfiguroinneista. Lisäksi hän määrittää Certificate manger -roolin omaavat henkilöt.
- **Certificate manager** on vastuussa sertifikaattien hallinnoinnista kuten myöntämisestä, sulkemisesta ja poistamisesta. Lisäksi tehtäviin kuuluu avaimien toimittaminen arkistosta avaimen palautusagentille. Ylläpitäjä saa tämän roolin, kun CA-palvelimessa määritellään Issue and Manage Certificates -oikeudet ylläpitäjälle. Roolista käytetään myös nimeä **CA officer**.
- **Auditor** on vastuussa loki-tietojen ylläpidosta ja tarkastamisesta liittyen PKI:n hallintaan ja toimintoihin. Ylläpitäjä saa tämän roolin, kun hänelle määritellään Manage Auditing and Security Log -oikeus ryhmäkäytännössä tai CA-palvelimen local security policy -konsolissa.
- **Backup operator** on vastuussa PKI-järjestelmän tietojen varmuuskopioinnista ja CA:n tietokannan ja konfiguraatioiden palautuksesta. Ylläpitäjä saa tämän roolin, kun hänelle annetaan Back Up Files and Directories- ja Restore Files and Directories -oikeudet ryhmäkäytännössä tai CA-palvelimen local security policy -konsolissa. Oikeudet voidaan tarvittaessa myös erotella, jolloin ylläpitäjä voi vain varmuuskopioida tai vain palauttaa varmuuskopion.

Kannattaa huomioida, että Backup operator- ja Auditor-roolit ovat käyttäjien oikeuksia käyttöjärjestelmässä, joten kyseiset roolit mahdollistavat myös

muita kyseisiä ylläpitotehtäviä kuin pelkästään sertifikaattipalveluihin liittyviä. Kaikki nämä roolit voidaan erotella niin, ettei yhdelläkään henkilöllä ole enempää kuin yksi rooli.

Riskien minimoiminen käsittää lähinnä levyjärjestelmät. Levyjen toiminta on käsitelty kappaleessa 11 Levyjärjestelmät. [1, s. 78-79.]

Sertifikaattien voimassaoloajan miettiminen kannattaa aloittaa loppukäyttäjien, jotka voivat olla myös koneita tai palveluita, sertifikaateista. Nyrkkisääntönä voisi pitää sitä, että myöntäjän sertifikaatin voimassaoloaika on kaksi kertaa myönnetyn sertifikaatin voimassaoloaika. Näin ollen jos loppukäyttäjälle myönnetään sertifikaatti, joka on voimassa kaksi vuotta, sertifikaatin myöntävän CA:n oma sertifikaatti tulee olla voimassa tällöin neljä vuotta. CA ei voi myöntää sertifikaatille enempää voimassaoloaikaa kuin sen omalla sertifikaatilla on myöntämishetkellä. CA:n kannattaa tässä tapauksessa uusia oma sertifikaattinsa aina kahden vuoden välein. Tällöin sertifikaattien myöntäminen onnistuu katkeamatta. Sääntönä voisi siis pitää, että CA uusii oman sertifikaattinsa, kun puolet sertifikaatin voimassaoloajasta täytyy. Ensimmäisellä kerralla käytetään voimassa olevaa avainparia ja toisella uusimiskerralla luodaan uusi avainpari. Siis parittomina uusimiskertoina vanha avainpari säilytetään ja parillisina kertoina avainpari uusitaan. Tällöin sama avainpari ei ole pitempään käytössä kuin alun perin suunnitellun ajan. Tässä esimerkkitapauksessa neljä vuotta. Samaa periaatetta käytetään hierarkian jokaisessa CA:ssa. Aina yläpuolella olevalla CA:lla on sertifikaatin voimassaoloaika puolet pitempi kuin alapuolella olevalla CA:lla. Kannattaa myös huomioida, että mitä pitempi on sertifikaatin voimassaoloaika, sitä pitempi tulee olla myös avaimen pituus. [1, s. 82-83.]

Sulkulistat ja CA:n sertifikaatit tulee julkaista jossakin julkaisupisteessä. Tällöin asiakassovellus voi tarkastaa luottoketjun eheyden sekä onko sertifikaatti mahdollisesti sulkulistalla. Sertifikaattien laajennokset sisältävät tiedon julkaisupaikasta luottoketjun ja sulkulistan tarkastamiseksi. Siis CA:n asennuksen yhteydessä määritellään julkaisupaikka, josta CA:n myöntämien sertifikaattien tila voidaan tarkastaa. Tämä tieto tallentuu kaikkiin CA:n myöntämiin sertifikaatteihin (sertifikaattien laajennoskenttiin).

Julkaisu voidaan tehdä eri protokollilla. Yksi mahdollisuus on käyttää HTTP-protokollaa. Tällöin julkaisu saadaan nopeasti asiakkaiden käyttöön. Lisäksi

asiakkaat voivat olla sekä sisäisiä että ulkoisia asiakkaita. HTTP-protokolla on hyvä valinta silloin, kun asiakkaat eivät ole toimialueen jäseniä eivätkä näin käytä aktiivihakemiston palveluja hyväkseen tai julkaisupalvelin on palomuurin takana.

Aktiivihakemisto-ympäristössä yleensä käytetään LDAP-protokollaa. Sulkulistat ja sertifikaatit ovat tallennettuina aktiivihakemistoon, jolloin asiakkaat voivat ladata ne miltä tahansa toimialueen ohjauskoneelta. Haittapuolena on, että tietojen replikointi kaikkiin ohjauskoneisiin saattaa kestää joskus hyvinkin kauan lähinnä silloin, kun ympäristössä on ns. site-rakenne (verkkoalueet). Verkkoalueiden välinen replikointi voi olla ajoitettu esimerkiksi tapahtuvaksi yöaikaan, jos saitteja yhdistää hidas tietoliikenneyhteys.

Julkaisu on mahdollista tehdä myös FTP-protokollalla. Tällöin julkaisu esim. palomuurin takaa on helppoa. Neljäs mahdollisuus on tehdä julkaisu tiedostojakona lähiverkon tiedostopalvelimessa.

Sertifikaatin laajennoskentässä olevat protokollat, joilla julkaisupisteen tieto noudetaan, merkitään tiettyyn järjestykseen. Asiakkaat kokeilevat näitä polkuja järjestyksessä ensimmäisestä viimeiseen. Jos esimerkiksi ensimmäiseksi protokollaksi merkitään LDAP, eikä asiakas tue tätä protokollaa, kuluu noin 10 sekuntia ennen kuin asiakas kokeilee toista protokollaa. Siis protokollien merkitsemisjärjestyksellä on merkitystä, kun halutaan mahdollisimman pienet vasteajat. Ensimmäiseksi tulisikin merkitä asiakkaiden eniten käyttämä protokolla, seuraavaksi toiseksi yleisin jne. [1, s. 83-85.]

4.4.4 Liiketoiminnan vaatimukset

Yrityksen liiketoiminta vaikuttaa myös hierarkiaan ja palvelimien lukumäärään. Jos haetaan kustannussäästöjä, voidaan CA-palvelimien rooleja yhdistää samaan koneeseen. Esimerkiksi kolmetasoisesta rakenteesta voidaan jättää yksi taso pois, jolloin toiseen tasoon voidaan yhdistää käytäntö- ja myöntäjä-CA -koneet. Luonnollisesti tällöin joudutaan tinkimään tietoturvasta.

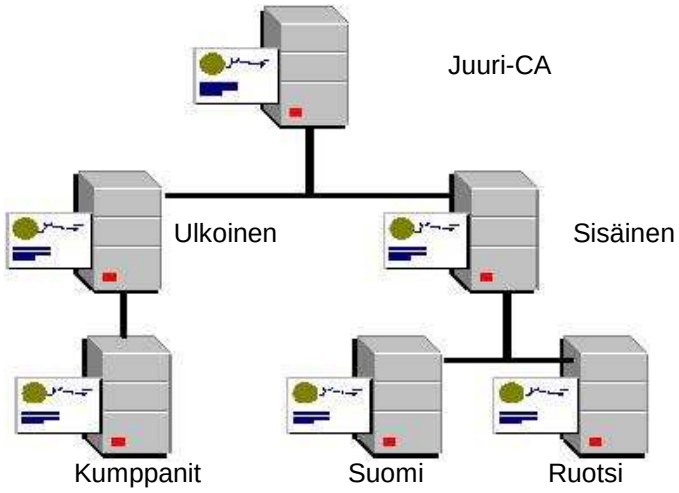
Vikasietoisuus pakottaa asentamaan useampia palvelimia ympäristöön. Tällöin samat sertifikaattipohjat pitää julkaista vähintään kahdelta palvelimelta. Jos verkko on kovin suuri, joudutaan CA-palvelin asentamaan jokaiseen maantieteellisesti kaukana sijaitsevaan verkkoon.

Jos yrityksellä on ulkoisia asiakkaita, joudutaan asentamaan käytäntö-CA-palvelimia, joissa on määritelty yrityksen CPS. Tässä CPS-dokumentissa yritys kertoo omat velvollisuutensa sertifikaattien myöntäjänä. Dokumentin sanamuoto on normaalisti suunniteltu lainoppineiden avulla. [1, s. 85.]

4.4.5 Ulkoiset vaatimukset

Jos PKI-sovellusten käyttö on niin laajaa, että yritys käyttää sertifikaatteja ulkopuolisen yrityksen tai yritysten kanssa, joudutaan miettimään ulkoisia vaatimuksia. Tilanteessa, jossa yrityksen sertifikaattien tulee olla tunnistettuja ja luotettuja toisen yrityksen taholta, joudutaan tekemään niin sanottu ristiinsertifiointi. Tällöin toisen yrityksen CA-palvelimet liitetään osaksi oman yrityksen CA-palvelimien luottoketjua. Toinen mahdollisuus on käyttää ulkopuolisen tahon tarjoamaa sertifikaattipalvelua.

Tilanteessa, jossa oman organisaation työntekijä joutuu käyttämään omia sertifikaatteja toisessa yrityksessä, voidaan PKI-ympäristöön asentaa kaksi käytäntö-CA-palvelinta, kuten kuva 12 esittää. Näin ympäristöön muodostuu kaksi haaraa, sisäinen ja ulkoinen. Sisäinen haara on yrityksen omien työntekijöiden sertifikaatteja varten ja ulkoinen haara on yhteistyöyritystä varten. Yrityksen ulkopuoliseen käyttöön sertifikaatit jaetaan ulkoisesta haarasta. Näin saadaan julkaistuksi oma CPS myös ulkoista käyttöä varten. Tätä rakennetta on hyvä käyttää myös tilanteissa, jossa pitää myöntää sertifikaatti oman yrityksen ulkopuoliselle henkilölle.



Kuva 12. Kaksi käytäntö-CA-palvelinta: sisäinen ja ulkoinen

Myös lainsäädäntö voi vaikuttaa PKI:n hierarkiaan ja rakenteeseen. Kuinka tietoa kerätään ja säilytetään yksityisessä yrityksessä, sanelee omat sään-

tönsä. Jos yrityksellä on toimintaa useassa maassa, tulee perehtyä jokaisen maan omaan lainsäädäntöön.

Lopuksi kannattaa muistaa, että sulkulistat ja CA:n sertifikaatit tulee julkaista esim. julkisessa www-palvelimessa, jotta sovellusten suorittamat sulkulistojen ja luottopolkujen tarkistukset onnistuvat. [1, s.85-87.]

5 SERTIFIKAATTIPOHJAT (CERTIFICATE TEMPLATES)

Suurissa yrityksissä voidaan myöntää jopa tuhansia sertifikaatteja käyttäjille ja koneille. Tällöin sertifikaattipohjat (certificate templates) helpottavat sertifikaattien myöntämistä. Ylläpitäjä voi muokata pohjat haluamikseen. Windows Server 2003 sekä Server 2008 tukevat versio 2 -pohjia, joita Windows 2000-ympäristö ei tue. Lisäksi Windows Server 2008 tukee version 3 pohjia. Pohjaan määritellään ominaisuudet, mitä tarkoitusta varten sertifikaatti on (esim. EFS-salausta varten), kenellä on oikeus anoa sertifikaattia (käyttäjäryhmä) sekä luodaanko sertifikaatti automaattisesti vai luoko ylläpitäjä sen. Windows 2000 -ympäristössä ovat käytössä versio 1 -pohjat. Näitä pohjia ei voi editoida eikä poistaa, niistä ei myöskään voida automaattisesti luoda sertifikaatteja. Näistä pohjista kuitenkin kopioidaan versio 2 -pohjat, jonka jälkeen näitä uusia pohjia voi editoida ja ne korvaavat vanhat pohjat. Kannattaa huomioida, että vain Windows Server 2003/2008 Enterprise Edition- ja Windows Server 2003/2008 Datacenter Edition -versiot voivat myöntää version 2 sertifikaatteja ja Windows Server 2008 Enterprise Edition- ja Datacenter Edition -versiot version 3 pohjia, joita käytetään uudessa CNG-salauksessa. Liite 1 sisältää versioiden 1 ja 2 sertifikaattipohjat. Oletuksena Windows Server 2008 -palvelimessa on vain yksi versio 3 -sertifikaattipohja valmiina: OCSP Response Signing -sertifikaattipohja [6; s. 263]. Tällä pohjalla määritellään OCSP-palvelimen sertifikaatti, jolla allekirjoitetaan vastaukset OCSP-asiakkaiden kyselyihin sertifikaattien tilasta. Muut pohjat kopioidaan versioiden 1 ja 2 pohjista. [2, s. 320-327; 6.]

6 SERTIFIKAATTIEN JAKAMINEN JA SULKULISTA

Jos sertifikaatteja halutaan jakaa automaattisesti, pitää tämä toiminto ottaa käyttöön. Automaattisesti jaetut sertifikaatit perustuvat versioiden 2 tai 3 pohjiin ja version 1 sertifikaatit pitää jakaa manuaalisesti. Kannattaa kuitenkin huomioida, ettei kaikkia versioiden 2 tai 3 sertifikaattejakaan voida jakaa

automaattisesti. Jokin sertifikaatti voi vaatia käyttäjän tunnistamisen henkilökohtaisesti, ennen kuin voidaan tarvittava sertifikaatti myöntää. Joskus tulee myös tilanne, että sertifikaatti täytyy ottaa pois käytöstä. Tällöin sertifikaatti laitetaan sulkulistalle. Syitä tähän voi esim. tietokone poistetaan käytöstä, työntekijä lähtee yrityksestä tai yksityinen avain on paljastunut. [2, s. 331; 6.]

6.1 Sertifikaatin käyttöönottoprosessi

Seuraavassa kuvataan pääkohdat sertifikaatin käyttöönottoprosessissa. Käyttöönottoprosessi sisältää sertifikaatin haun ja asennuksen käyttäjää, konetta tai palvelua varten:

- Kun käyttäjä hakee uutta sertifikaattia, käyttöjärjestelmä lähettää kyselyn Cryptogrphic Service Provider (CSP) -palvelulle (palvelu on asennettu käyttäjän koneeseen).
- CSP luo yksityisen ja julkisen avaimen (avainpari). CSP luo avainparin käyttäjän koneeseen (ohjelmistoperustainen, software based). Jos CSP on laiteperustainen (hardware based) kuten esim. toimikortti (smart card), CSP ohjeistaa laitteistoa luomaan avainparin.
- Julkinen avain lähetetään CA:lle muun informaation mukana. CSP salaa yksityisen avaimen käyttäjän koneessa (käyttäjän profiilissa). Laiteperustaisessa avain on kortilla salattuna.
- CA joko hyväksyy tai hylkää haun. Jos haku hyväksytään, CA luo ja allekirjoittaa sertifikaatin.
- CA lähettää sertifikaatin hakijalle, joka asentaa sen koneeseen tai laitteeseen. [2, s. 332-333; 6.]

6.2 Sertifikaatin myöntämistavat

CA:n tyyppi määrää, kuinka sertifikaatin haku tehdään; manuaalisesti vai automaattisesti. Esim. standalone CA ei voi myöntää sertifikaatteja automaattisesti, enterprise CA voi. Myöskään koneet, jotka eivät ole verkossa, eivät voi myöntää automaattisesti sertifikaattia, vaan se täytyy tehdä manuaalisesti. Tällainen tilanne tulee eteen käytännössä, kun CA-hierarkia rakennetaan.

Sertifikaatin haku standalone CA:lta tapahtuu jollakin seuraavista tavoista:

- Web-selain
- Certificates-työkalu, joka luodaan mmc:llä
- Certreq.exe-komentokehotetyökalu.

Web-selain on loppukäyttäjille helpoin tapa hakea sertifikaattia. Sertifikaatti myös asentuu koneeseen linkkiä painamalla. Certificates-työkalu pitää luoda mmc-konsolissa; käyttäjän kannalta tämä on hankala osuus. Ylläpitäjä voi luoda työkalun valmiiksi ja antaa sen loppukäyttäjälle. Certreq.exe-komento ajetaan suoraan komentokehotteesta ja sen varsinainen tarkoitus on ajaa skriptejä, joita ei voida toteuttaa ryhmäkäytännön (Group Policy) kautta. Tämä työkalu on tarkoitettu vain ylläpitäjän käyttöön.

Sertifikaatin haku enterprise CA:lta tapahtuu muuten samoin kuin standalone CA:ta, paitsi lisänä on mahdollisuus automatisoida käyttöönottoprosessi (autoenrollment of certificates) ryhmäkäytännön (Group Policy) kautta. Sertifikaattien automaattinen myöntäminen määritellään sertifikaattipohjien kautta. Sertifikaattipohjissa ylläpitäjä määrittelee, kuka saa hakea sertifikaattia, sertifikaatin käyttötarkoituksen ja tapahtuuko myöntäminen automaattisesti vai manuaalisesti. Jokainen sertifikaatti luodaan perustuen sertifikaattipohjaan.

Kannattaa huomioida, että Windows 2000 -asiakas ei voi saada automaattisesti käyttäjän sertifikaattia mutta voi saada konesertifikaatin. Uudemmat asiakkaat (Windows XP/Vista/7, Windows Server 2003/2008) voivat saada molemmat sertifikaatit automaattisesti. Luonnollisesti sertifikaattipohjien tulee olla versioiden 2 tai 3 pohjia. Windows 2000 -käyttöjärjestelmää aikaisemmat asiakkaat voivat saada sertifikaatin vain manuaalisesti, koska ne eivät tue ryhmäkäytäntöjä, joten käytännössä sertifikaatin haku tapahtuu samalla tavalla kuin standalone CA:lta haettaessa eli vaihtoehtoina on web-selain, certificates-työkalu tai certreq.exe-ohjelma.

Manuaalisessa haussa web-selaimella CA pitää olla asennettu palvelimeen, jossa on Certificate Services -palvelu sekä IIS-palvelinohjelmisto asennettuna. Haku tapahtuu oletuksena osoitteesta: http://ServerName/certsrv. Ylläpitäjä voi halutessaan muuttaa osoitteen. Kannattaa huomioida, ettei yhteys ole oletuksena salattu (https), joten salattu yhteys kannattaa rakentaa itse. Tällöin itse www-palvelimessa luodaan sertifikaattihaku, joka lähetetään CA:lle. CA hyväksyy haun ja myöntää sertifikaatin. Sertifikaatti toimitetaan asiakkaalle esimerkiksi sähköpostilla ja tämän jälkeen sertifikaatti asennetaan samaan www-palvelimeen, jossa hakemus tehtiin. Lisäksi www-palvelimessa tulee määritellä vielä SSL-liikenne oletuksena TCP-porttiin 443.

Certificates-työkalulla voidaan hakea sertifikaattia CA:lta, joka on konfiguroitu enterprise CA:ksi. Työkalu näyttää myös mm. voimassaolevat sertifikaatit, luotetut juuri-CA:t ja sertifikaattien luottosuhteet. Koneen pääkäyttäjä voi hallita sertifikaatteja, jotka on myönnetty käyttäjälle, koneelle ja palvelulle. Normaali käyttäjä (User) voi hallita vain omaa käyttäjäsertifikaattia. Certreq-komentokehotetyökalulla voi lähettää sertifikaattihaun CA:lle komennolla certreq -submit, noutaa sertifikaatin CA:lta komennolla certreq -retrieve sekä hyväksyä ja asentaa sertifikaatin komennolla certreq -accept.

Automaattinen käyttöönotto mahdollistaa sekä kone- että käyttäjäsertifikaattien hallinnan. Sertifikaatit voidaan hallita keskitetysti koko elinkaaren ajan; käyttöönotto, sertifikaattien uudistaminen sekä korvaus. Toiminto on loppukäyttäjälle automaattinen, eikä hänen tarvitse tehdä mitään toimenpiteitä. Tämä siis helpottaa eri sovellusten (toimikortit, EFS, SSL, S/MIME) käyttöä sekä tuo yritykselle kustannussäästöjä. Automaattiseen käyttöönottoon ryhmäkäytännössä on kaksi asetusta. Ensimmäinen on *Automatic Certificate Request Settings* -asetus, joka on ryhmäkäytäntö, jolla jaetaan versio 1:n konesertifikaatit Windows 2000- Windows XP/Vista/7- ja Windows Server 2003/2008 -käyttöjärjestelmille. Tätä sertifikaattia käytetään yleensä IPSec-yhteyksien rakentamisessa. Ryhmäkäytäntö löytyy polusta: Computer Configuration/Windows Settings/Security Settings/Public Key Policies/Automatic Certificate Request Settings. Ryhmäkäytäntö kannattaa ylläpitää Group Policy Management Tools -työkalulla, joka on ladattavissa Microsoftin www-sivulta; Windows 2008 sisältää työkalun, eikä sitä tarvitse erikseen hakea. Autoenrollment Settings -asetuksella hallitaan versioiden 2 ja 3 kone- ja käyttäjäsertifikaatteja (pohjia) Windows XP/Vista/7- ja Windows Server 2003/2008 -koneissa. Konesertifikaattien asetukset löytyvät polusta: Computer Configuration/Windows Settings/Security Settings/Public Key Policies ja käyttäjien sertifikaattien asetukset löytyvät polusta: User Configuration/Windows Settings/Security Settings/Public Key Policies. Oletuksena käyttäjien ja koneiden sertifikaattien automaattinen käyttöönotto on asetettu päälle. Jotkin sertifikaattihaut vaativat käyttäjän toimenpiteitä, kuten esim. toimikorttien sertifikaatit. Jossakin vaiheessa käyttäjän tulee siis laittaa kortti kortinlukijaan. Tällaisessa tapauksessa voidaan sertifikaattipohjaan määrittää, että käyttäjälle ilmoitetaan toimenpiteestä, joka hänen tulee tehdä sertifikaattihaun onnistumiseksi. [2, s. 333-338.]

6.3 Sertifikaattien sulkeminen

Sertifikaatti halutaan joskus ottaa pois käytöstä. Tällöin se laitetaan sulkulistalle. Syynä voi olla esim. se, että työntekijä on lähtenyt yrityksestä, kone on poistettu käytöstä tai yksityinen avain on paljastunut. Sertifikaatin sulkeminen tapahtuu joko Certification Authority -työkalulla tai Certutil.exe-komentokehotetyökalulla. Listalle on myös mahdollista laittaa syy, miksi sertifikaatti on poistettu käytöstä. Sitä kuitenkin kannattaa käyttää harkiten. Asiakkaat lataavat sulkulistan välimuistiin ja tarkistavat sieltä sertifikaatin voimassaolon. Sulkulista voi olla *full CRL* -tyyppinen tai *Delta CRL* -tyyppinen. *Full CRL* -lista pitää sisällään täydellisen listauksen sulkulistasta, joka julkaistaan oletuksena kerran viikossa. *Delta CRL* -lista pitää sisällään vain lisäykset, jotka julkaistaan oletuksena kerran päivässä. Ne ovat lisäyksiä, jotka ovat tulleet *full CRL* -listan julkaisun jälkeen. [1, s. 338-339.]

Windows 2008 Server -käyttöjärjestelmässä on mahdollista määritellä OCSP-palvelin, jolta asiakas tarkistaa sertifikaatin voimassaolon. Tarkistettavan sertifikaatin AIA-kentässä on merkitty OCSP-palvelimen osoite, josta tarkistus voidaan suorittaa. Tällöin ei käytetä erillisiä sulkulistoja, vaan kysely suoritetaan reaaliaikaisesti. Sulkulistan huono puoli on se, että se tallennetaan asiakkaan välimuistiin tietyksi ajaksi, jolloin ennen uuden sulkulistan lataamista on mahdollista, että sulkulistalle laitettu sertifikaatti on toiminnassa. OCSP-protokolla poistaa tämän ongelman. OCSP:n toinen etu on, että siirrossa siirretään vain vähän tietoa; sulkulista voi olla kooltaan erittäin suuri. Huonona puolena on, että OCSP-palvelimen tulee olla verkossa koko ajan. Tästä syystä palvelin tulee sijoittaa omaan klusteriinsa, jossa palvelu siirtyy toiselle palvelulle mahdollisessa vikatilanteessa. Klusteri ja sen ylläpito luonnollisesti aiheuttavat lisäkustannuksia. Tämä on syy, miksi sulkulista on edelleenkin yleisin tapa tarkistaa sertifikaattien voimassaolo. OCSP-asiakasohjelmisto on asennettavissa Windowsin Vista/7- ja Server 2008 -järjestelmissä ja OCSP responder eli OCSP-palvelin on asennettavissa Certificate Server -palvelimissa. Windows XP ja Windows 2003 Server tarvitsevat kolmannen osapuolen ohjelmiston OCSP:n käyttöä varten. [6, s.35-37.]

6.4 Sulkulistojen ja sertifikaattien julkaiseminen

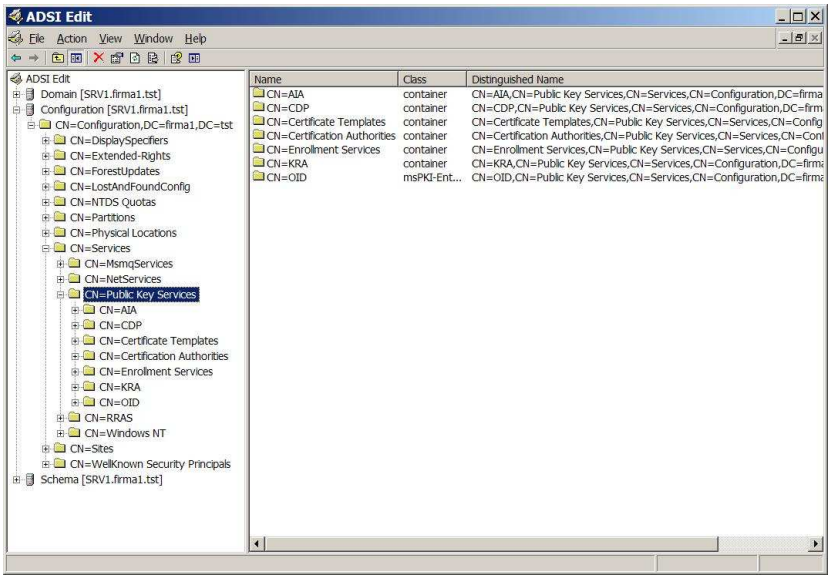
Asiakas voi ladata sulkulistan CA-palvelimelta tai joltakin muulta palvelimelta eri protokollilla: Shared folders (SMB), Hypertext Transfer Protocol (HTTP),

File Transfer Protocol (FTP) ja Lightweight Directory Access Protocol (LDAP). Oletuksena Windows Server 2003/2008 -sertifikaattipalvelimelta julkaistaan sulkulista jaetusta resurssista \\Server\CertEnroll\. LDAP-protokollalla lista löytyy nimellä: CN=CAName, CN=CAComputer-Name, CN=CDP,CN=PublicKeyServices,CN=Services,CN=Configuration, DC=Forest-RootNameDN. Web-selainta käytettäessä osoite on oletuksena http://Server/certenroll/. Jakoja joudutaan muuttamaan tai toisille palvelimille tekemään uusia jakoja, jos CA on offline-tilassa tai se ei jostakin muusta syystä ole verkossa näkyvissä. Tällainen tilanne voi olla esimerkiksi silloin, kun verkko on suojattu palomuurilla; myös tietoturvan vuoksi voidaan tietty CA-palvelin poistaa verkosta. Jos sulkulista julkaistaan joltakin muulta palvelimelta, se tulee luonnollisesti kopioida palvelimeen, josta julkaisu tapahtuu. [1, s. 84; 2, s. 340.]

Asiakkaita varten offline-sertifikaattipalvelinten sertifikaatit ja sulkulistat tulee julkaista aktiivihakemistossa. Tällöin toimialueen asiakkaat saavat palvelinten sertifikaatit ja sulkulistat automaattisesti ryhmäkäytännön avulla. Juuri-CA:n sertifikaatti tallentuu asiakkaan trusted root CA store -säiliöön ja muiden CA-koneiden sertifikaatit intermediate CA store -säiliöön. Asiakaskoneessa käyttäjä voi tutkia sertifikaatteja esimerkiksi mmc-konsolilla tehdyllä Certificates-työkalulla tai IE-selaimen Internet Options -asetuksista Content-välilehden Certificates-painikkeella ja valitsemalla edellä mainittu säiliö. Siis näin voidaan tarkastaa, että sertifikaatti on latautunut aktiivihakemistosta paikalliseen koneeseen. Palvelimen sertifikaatin pitää olla kyseisessä säiliössä, jotta luottoketju voidaan tarkastaa ja näin myönnettyyn sertifikaattiin voidaan luottaa. Sertifikaattia käytettäessä certificate chaining engine tarkastaa luottoketjun. Jos tarkastettavan sertifikaatin on myöntänyt jokin muu CA-palvelin kuin juuri-CA, tulee sen palvelimen sertifikaatti löytyä asiakkaan intermediate CA store -säiliöstä. Jos sertifikaatin on myöntänyt suoraan juuri-CA, tulee juuri-CA:n sertifikaatti löytyä trusted root CA store -säiliöstä. Siis PKI-arkitehtuurin tasojen määrä (palvelinten määrä) määrittää, mistä säiliöstä palvelimen, joka myöntää sertifikaatin, sertifikaatti tulee löytyä. Esimerkiksi jos tasoja on kolme, niin tällöin CA-palvelimet ovat ylhäältä alaspäin juuri-CA, käytäntö-CA ja myöntäjä-CA. Jotta luottoketju on ehyt, tulee asiakkaan intermediate CA store -säiliössä olla myöntäjä-CA:n (myöntää asiakkaalle sertifikaatin) sertifikaatti; myöntäjä-CA:n intermediate CA store -säiliössä tulee olla käytäntö-CA:n sertifikaatti ja käytäntö-CA:n trusted root CA store

-säiliössä tulee olla juuri-CA:n sertifikaatti. Myös sulkulistojen tulee olla samoissa paikoissa sertifikaattien kanssa.

Ylläpitäjä voi tarkastaa, että sertifikaatit on julkaistu aktiivihakemistossa. Tämän voi tehdä esimerkiksi ADSI Edit -työkalulla.



Kuva 13. ADSI Edit -työkalu

Kuva 13 näyttää aktiivihakemiston Configuration-osion sisällön ADSI Edit -työkaluikkunassa. Kaikkien CA-palvelimien sertifikaatit on julkaistu CN=AIA,CN=Public Key Services, CN=Services, CN=Configuration, ForestRootDomain -säiliössä. ForestRootDomain on domainin LDAP-nimi, esim. rnko.fi-domainin LDAP-nimi on DC=rnko, DC=fi. Juuri-CA:n sertifikaatti on julkaistu edellisen lisäksi CN=Certification Authorities,CN=Public Key Services, CN=Services, CN=Configuration,ForestRootDomain -säiliössä. Asiakkaiden sertifikaatit myöntänyt myöntäjä-CA-palvelimen, joka on tyyppiä enterprise CA, sertifikaatit on julkaistu CN=NTAuthCertificates,CN=Public Key Services,CN=Services, CN=Configuration,DC=ForestRootDomain -säiliössä. Certificate chaining engine käyttää AIA- ja Certification Authorities -säiliöitä hyväkseen muodostaessaan luottoketjun.

Sulkulistat julkaistaan CN=CDP,CN=Public Key Services,CN=Services, CN=Configuration,ForestRootDomain -säiliössä. Esimerkiksi jos palvelimen NetBIOS-nimi on JUURI1, julkaistaan sulkulista CN=JUURI1, CN=CDP,CN=Public Key Services, CN=Services, CN=Configuration, For-

estRootDomain -säiliössä. Sulkulista julkaistaan aktiivihakemistoon certutil-komennolla:

certutil -dspublish -f CAName.crl

Käskyssä CAName on juuri-CA:n looginen nimi, kun julkaistaan juuri-CA:n sulkulista. Julkaistaessa väli-CA:n sulkulista, CAName on kyseisen CA:n looginen nimi.

Sertifikaatit ja sulkulistat ladataan Windows XP- ja Windows Server 2003/2008 -ympäristön asikaskoneisiin komennolla:

gpupdate /target:computer /force

Tarvittaessa annetaan vielä komento:

certutil -pulse

Jos komentoja ei anneta, noin 90 minuutin päästä autoenrollment-prosessi päivittää sertifikaatit koneisiin. Myös koneen uudelleenkäynnistys tekee päivitykset. [1, s. 104-106; 6, s. 113.]

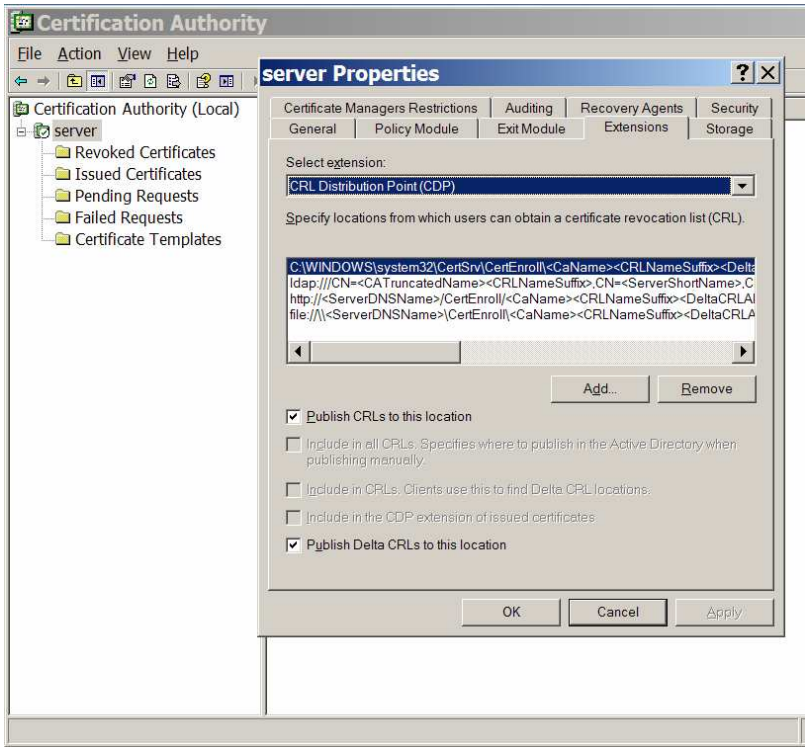
6.5 Sulkulistojen ja sertifikaattien julkaisu

Sulkulistat tulee julkaista tietyin väliajoin. Sulkulistoja ovat pääsulkulista ja lisäsulkulista (delta CRL). CA:n asennuksen yhteydessä julkaisuajat määritellään CAPolicy.inf-tiedostossa. Lisäksi nämä asetukset kannattaa määrittää toistamiseen certutil-ohjemalla koneen oman rekisteriin. Seuraavilla komennoilla voidaan määrätä pääsulkulista julkaistavaksi kaksi kertaa vuodessa ja lisäsulkulistaa ei julkaista ollenkaan.

certutil -setreg CA\CRLPeriodUnits 6
certutil -setreg CA\CRLPeriod “months"
certutil -setreg CA\CRLDeltaPeriodUnits 0
certutil -setreg CA\CRLDeltaPeriod “days”

Yleensä lisäsulkulista julkaistaan vain sertifikaatteja myöntävässä palvelimessa (myöntäjä-CA). Juuri-CA- ja väli-CA -palvelimissa ei julkaista lisäsulkulistaa, koska normaalisti koneet on irroitettu verkosta. Edellisissä käskyissä molemmille listoille tulee määritellä numeroarvon lisäksi myös yksikkö, joka voi olla days, weeks, months tai years.

Julkaisupisteet määritellään CA-koneen Certification Authority -konsolissa palvelimen ominaisuuksien Extensions-välilehdellä. Konsolin voi käynnistää Administrative Tools -valikosta. Kuva 14 näyttää avatun ikkunan julkaisupisteistä. Select Extensions -alasvetovalikosta voidaan valita CRL Distribution Point (CDP) tai Authority Information Access (AIA). Ensimmäisellä valinnalla määritellään sulkulistojen julkaisupisteet ja jälkimmäisellä sertifikaattien julkaisupisteet. Polku voidaan määritellä paikalliseksi, LDAP- ja HTTP-protokollilla sekä tiedostojaon kautta. Lisäksi polkujen määrityksissä voidaan käyttää apuna muuttujia, jolloin pitkien polkujen kirjoittaminen helpottuu. Polku lisätään Add-painikkeella.

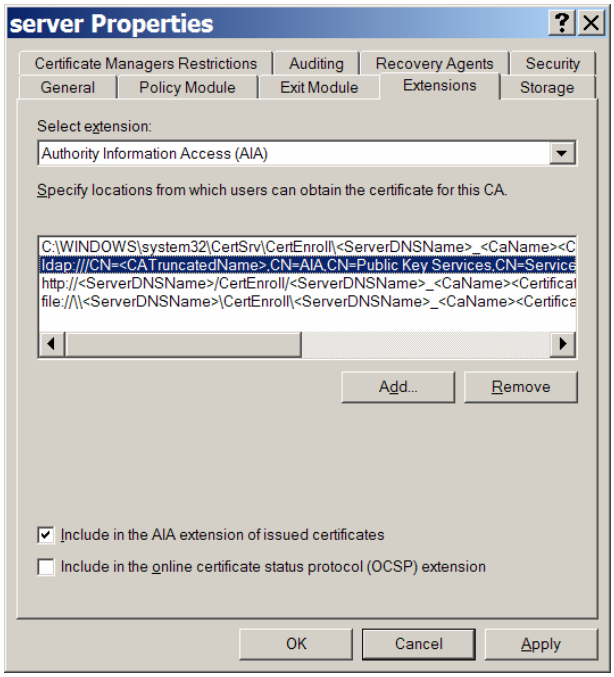


Kuva 14 Certification Aurhority -konsoli

Ikkunan alalaidassa on optiot, jotka voidaan määrittää kullekin polulle erikseen. Esimerkiksi edellisen kuvan paikalliselle polulle (paikallinen polku on kuvassa aktivoituna korostettu sinisellä) määritellään, että sulkulista (ensimmäinen optio: Publish CRLs to this location) sekä lisäsulkulista (viides optio: Publish delta CRLs to this location) julkaistaan kyseisessä hakemistossa. Toinen optio (Include in all CRLs. Specifies where to publish in Active Directory when publishing manually.) määrittelee LDAP-protokollan polun, kun julkaisu tapahtuu aktiivihakemistosta. Tämän option voi valita vain LDAP-poluille, ei muille. Kolmas optio (Include in CRLs. Clients use this to

find delta CRL locations.) määrittelee, mistä lisäsulkulista löytyy. Optio määritellään itse sulkulistaan, josta se on löydettävissä itse sulkulistan tarkastuksen yhteydessä. Neljäs optio (Include in the CDP extension of issued certificates.) määritellään sertifikaatin laajennoskenttään, josta luottoketjua tarkastettaessa löydetään tieto, missä sijaitsee viimeisin sulkulistan versio. Windows Server 2008 -palvelimessa on lisäksi optio Include in the IDP extension of issued CRLs. Tällä optiolla voidaan kertoa ei-Windows asiakkaille sulkulistan tyyppi; esim. sulkulista sisältää vain loppukäyttäjien sertifikaatteja. Edellisistä poluista voidaan määritellä jokaiselle polulle haluttu kombinaatio optioita. Kaikki optiot eivät ole valittavissa kaikkiin polkuihin, jolloin optiot näkyvät harmaina eikä niitä voi valita.

Myös CA:n sertifikaateille voidaan määrittää julkaisupisteet. Select extension -alasvetovalikosta valitaan Authority Information Access (AIA) -valinta kuten kuva 15 näyttää.



Kuva 15 Julkaisupisteiden valinta Certification Aurhority -konsolissa

Julkaisu voidaan tehdä samoilla protokollilla kun sulkulistatkin. Myös muuttujia voidaan käyttää apuna polkujen muodostamisessa. Optioita on kuitenkin vähemmän. Ensimmäinen optio (Include in the AIA extension of issued certificates) määrittää, että polku lisätään myönnetyn sertifikaatin laajennuskenttään. Toinen optio (Include in the online certificate status protocol (OCSP) extension.) mahdollistaa reaaliaikaisen tarkistuksen OCSP-palvelimelta.

Windows Server 2003 -palvelimessa tämä ominaisuus vaatii kolmannen osapuolen lisäohjelmien asentamista. Windows Server 2008 -palvelimessa tämä ominaisuus on kuitenkin käytössä ilman lisäosien asennuksia.

Julkaisupisteet ja sertifikaatit voidaan julkaista myös certutil-ohjelmalla. Taulukko 3 näyttää arvot (Value), joilla voidaan valita haluttu optio. Esimerkiksi sulkulistan ja lisäsulkulistan julkaiseminen (kuva 14) saadaan arvolla 65, joka koostuu arvoista 1 ja 64; nämä arvot lasketaan yhteen.

Taulukko 3. Sulkulistan optioiden arvot

DISPLAY NAME	**VALUE**
PUBLISH CRLS TO THIS LOCATION.	1
INCLUDE IN ALL CRLS. SPECIFIES WHERE TO PUBLISH IN ACTIVE DIRECTORY WHEN PUBLISHING MANUALLY.	2
INCLUDE IN CRLS. CLIENTS USE THIS TO FIND DELTA CRL LOCATIONS.	4
INCLUDE IN THE CDP EXTENSION OF ISSUED CERTIFICATES.	8
PUBLISH DELTA CRLS TO THIS LOCATION.	64
INCLUDE IN THE IDP EXTENSION OF ISSUED CRLS.	128

Jos sulkulistat haluttaisiin julkaista paikallisesti, http- ja ldap-protokollilla, voisi komento olla seuraava:

certutil -setreg CA\CRLPublicationURLs “1:%windir%\system32\CertSrv\ CertEnroll\%%3%%8%%9.crl\n8:http://www.rnko.fi/CertData/%% 3%%8%%9.crl\n10:ldap:///CN=%%7%%8,CN=%%2,CN=CDP,CN=Public Key Services,CN=Services,%%6%%10”

- 1:%windir%\system32\CertSrv\ CertEnroll\%%3%%8%%9.crl julkaisee sulkulistan paikallisesti. Optio on 1, mikä tarkoittaa pääsulkulistan julkaisua.

- 8:http://www.rnko.fi/CertData/%%3%%8%%9.crl julkaisee sulkulistan http-prokollalla. Optio 8 määrittää, että polku tallennetaan myönnettyjen sertifikaattien laajennoskenttään.
- 10:ldap:///CN=%%7%%8,CN=%%2,CN=CDP,CN=Public Key Services,CN=Services,%%6%%10” julkaisee sulkulistan aktiivihakemistossa (optio 2) ja lisää polun myönnettyihin sertifikaattien laajennoskenttiin (optio 8). Siis optiot 2 ja 8 lasketaan yhteen, jolloin saadaan optio 10.

Certutil-komennossa muuttujien eteen tulee lisätä vielä toinen %-merkki. Tämä on nimenomaan certutil-komennon ominaisuus. Jos muuttujia käytetään esimerkiksi CAPolicy.inf-tiedostossa, riittää yksi %-merkki. \n-merkki on erotinmerkki multi-value -rekisteriarvoissa. Edellisessä komennossa certutil-komennolla tehtiin muutos rekisterin arvoon, jonka tyyppi on multi-value. Muuttujilla voidaan yhtenäistää komentojen suoritusta. Esimerkiksi muuttuja %1 vastaa CA-palvelimen DNS-nimeä, %2 vastaa palvelimen NETBIOS-nimeä ja %3 vastaa CA:n nimeä. Lista muuttujista löytyy liitteestä 4.

Sertifikaattien julkaisu voisi tapahtua esimerkiksi komennolla:

certutil -setreg CA\CACertPublicationURLs “1:%windir%\system32\CertSrv\ CertEnroll\%%1_%%3%%4.crt\n2:http://www.rnko.fi/CertData/ %%1_%%3%%4.crt\n2:ldap:///CN=%%7,CN=AIA,CN=Public Key Services,CN=Services,%%6%%11”

- **1:%windir%\system32\CertSrv\ CertEnroll\%%1_%%3%%4.crt** julkaisee sertifikaatin paikallisesti.
- **2:http://www.rnko.fi/CertData/ %%1_%%3%%4.crt** lisää julkaistavan sertifikaatin polun myönnettävien sertifikaattien laajennoskenttiin.
- **2:ldap:///CN=%%7,CN=AIA,CN=Public Key Services,CN=Services, %%6%%11** lisää julkaistavan sertifikaatin polun myönnettävien sertifikaattien laajennoskenttiin kuten edellisessä kohdassa. [1, s. 107-110.]

6.6 Sertifikaattien voimassaoloaika

CA myöntää asiakkaille sertifikaatit vain tietyksi aikaa. Voimassaolo voidaan määritellä certutil-komennoilla:

certutil -setreg CA\ValidityPeriodUnits 5
certutil -setreg CA\ValidityPeriod “Years”

Nämä komennot määrittelevät sertifikaateille voimassaoloajan viideksi vuodeksi. Näiden komentojen vaikutus eroaa riippuen annetaanko ne standalone CA- vai enterprise CA -koneella. Standalone CA:n kohdalla asia on yksinkertainen: kaikille myönnettäville sertifikaateille määritellään tämä sama voimassaoloaika. Enterprise CA:n tapauksessa voimassaoloaikaan vaikuttaa myös itse CA:n sertifikaatin voimassaoloaika. Jos CA myöntää sertifikaatin pitemmäksi aikaa kuin tämän itsensä sertifikaatin voimassaoloaika, voimassaoloajaksi tulee CA:n sertifikaatin jäljellä oleva voimassaoloaika. Tämän lisäksi sertifikaattipohjissa on oma voimassaoloaikansa. Käytännössä myönnettävän sertifikaatin voimassaoloajaksi tulee näiden kolmen asetuksen pienin arvo. Sertifikaattipalvelua suunniteltaessa tuleekin miettiä tarkkaan, kuinka pitkään itse CA:n sertifikaatit ovat voimassa ja milloin ne uusitaan.

Jos sertifikaatteihin tai sulkulistoihin tehdään muutoksia esimerkiksi polkuihin, pitää muutokset julkaista. Tämä tapahtuu komennolla:

certutil -CRL

7 YLLÄPITÄJIEN ROOLIT JA NIIDEN EROTTELEMINEN (ROLE SEPARATION)

Ylläpitäjien roolien erottamisella määritellään jokaiselle ylläpitäjälle vain yksi tehtävä. Näin voidaan estää tilanne, jossa jollakin ylläpitäjällä on niin paljon oikeuksia, että hän voi väärinkäyttää järjestelmää. Tehtävien suorittamiseen tarvitaan useampi ylläpitäjä, mikä vähentää väärinkäytösten riskiä. Kannattaa kuitenkin huomioida, että usealla ylläpitäjällä voi olla kuitenkin sama rooli.

Certificate Issuing and Management Components Family of Protection Profiles (CIMC) on standardoitu dokumentti, jossa määritellään vaatimukset X.509-sertifikaattien hallintaan. Dokumentti määrittelee tasot yhdestä neljään. Tasolla neljä on korkeimmat turvamääritykset. Myös ylläpitäjien rooleja on neljä kappaletta:

- **CA administrator** on vastuussa tilien hallinnoinnista ja avainparien luomisesta.
- **Certificate manager** on vastuussa sertifikaattien hallinnoinnista.
- **Auditor** on vastuussa loki-tietojen ylläpidosta ja tarkastamisesta.
- **Backup operator** on vastuussa PKI-järjestelmän tietojen varmuuskopioinnista.

Tasolta kolme puuttuu backup operatorin rooli ja tasoilta yksi ja kaksi lisäksi puuttuu auditorin rooli. Tasolla yksi vaaditaan luonnollisesti käyttäjien auditointi sekä salausalgoritmit, jotka ovat FIPS 140-2 level 1 -tason mukaisia. Taso kaksi lisää tähän lisävaatimuksia auditoinnista, lokeista sekä varmuuskopioinnista. Lisäksi käytettävien turvamoduulien tulee olla FIPS 140-2 level 2 -tason mukaisia. Taso kolme lisää turvaa lähinnä fyysisellä tasolla jos henkilö, jolla ei ole oikeutta CA:n laitteistoon, pääsee fyysisesti siihen käsiksi. Edelleen taso neljä määrittelee lisäturvaa auditointilokien allekirjoitetuilla aikamerkinnöillä sekä FIPS 140-2 level 4 -tason turvalla.

Windows Server 2003/2008 mahdollistaa CIMC tason 4 mukaisen ylläpitäjien roolituksen. Rooleja käsiteltiin tarkemmin kappaleessa 4.4.3 Tekniset vaatimukset. [1, s. 207-215.]

8 SERTIFIKAATTIPALVELUN DOKUMENTOINTI, VARMUUSKOPIOINTI JA PALAUTUS

8.1 Dokumentointi

Kaikkien PKI:n ylläpitoon liittyvien asioiden pitää olla dokumentoitu ja varmistettu. Pahimmassa tapauksessa koko PKI-ympäristö aktiivihakemistoineen voidaan joutua asentamaan uudelleen, jolloin tärkeiden tietojen pitää olla saatavilla. Viimekädessä ne saadaan tehdystä dokumentaatiosta. Ainakin seuraavat asiat tulee dokumentoida ympäristöstä:

- Kaikki sertifikaattipohjat jotka ovat käytössä, mukaan lukien kaikkien välilehtien asetukset. Sertifikaattipohjien hallintaan voidaan käyttää skriptejä. Esimerkiksi pohjan lisääminen onnistuu komennolla certutil -SetCAtemplates +<SertifikaattiPohjanNimi> ja poistaminen komennolla certutil -SetCAtemplates -<SertifikaattiPohjanNimi>.
- Kaikki oikeudet (permissions). CA Administrator- ja certificate manager -oikeudet sekä käyttäjät ja ryhmät jotka voivat lukea CA:n konfiguraation tai hakea sertifikaatteja. Nämä oikeudet määritellään Certification Authority -konsolin ominaisuuksissa Security-välilehdellä. Lisäksi ryhmäkäytännöt (paikalliset sekä toimialueen), jotka määrittelevät, ketkä ylläpitäjät voivat varmuuskopioida ja palauttaa varmuuskopion (Backup Operators) sekä ketkä voivat auditoida järjestelmää (Auditors).

- Certification Authority -konsolin ominaisuuksien Certificate Manager Restrictions -välilehden asetukset, joilla rajoitetaan ylläpitäjien oikeuksia. Lisäksi Recovery Agents -välilehden sertifikaatit, joilla voidaan palauttaa avaimia.
- Kaikki CA-koneisiin liittyvät nimet, joita ovat CA:n looginen nimi (CA's logical name), CA-koneen NetBIOS-nimi sekä toimialueen tai työryhmän nimet.
- Komentojonot, joilla konfiguroidaan CA-koneet. Certutil-komennolla voidaan konfiguroida hyvin paljon rekisteriasetuksia, jolloin suora rekisterin konfigurointi ei ole tarpeen eikä ole suositeltavaakaan. Loppupuolen esimerkissä konfiguroidaan CA-palvelin käyttäen komentojonoa.
- CA:n tietokannan, lokien ja konfigurointien sijaintipaikat. Rekisterimääritykset kertovat näiden konfigurointitietojen sijaintipaikan, joten palautuksessa niiden tulee olla samassa paikassa.
- CA:n sertifikaattien ja sulkulistojen julkaisupaikat. Asiakkaat etsivät sertifikaatit ja sulkulistat kerrotusta paikasta, joten aikaisempi julkaisupaikka ei saa muuttua.
- CSP:n, joka suojelee CA:n yksityistä avainta tulee olla sama kuin aikaisemmassa asennuksessa. Esimerkiksi HSM-moduulille voi olla asennettu oma CSP, jolloin yksityinen avain on tallennettu erilliseen laitteeseen lisäämään tietoturvaa.
- CA:n sertifikaatin avaimen pituus.
- CA-koneen levyjärjestelmässä tulee asematunnusten ja hakemistorakenteen tietokannalle, lokitiedostoille, mahdolliselle konfigurointihakemistolle ja käyttöjärjestelmälle, pysyä samoina. Aseman koko tai RAID-taso voi tarvittaessa muuttua.
- CAPolicy.inf-tiedosto tulee palauttaa %windir%-hakemistoon, jos käyttöjärjestelmä asennetaan uudelleen. Tiedosto tarvitaan, kun CA:n sertifikaatti uusitaan. Tämä tiedosto tehdään, kun CA-kone asennetaan. Tiedoston luonti kerrotaan kappaleessa 17.2 CAPolicy.inf-tiedosto. [1, s. 234-235.]

8.2 Varmuuskopiointi

Sertifikaattipalvelu pitää varmuuskopioida, kuten mikä tahansa kriittinen palvelu. Varmuuskopiointi voidaan tehdä System State -varmuuskopiona tai manuaalisesti.

8.2.1 System State -varmuuskopiointi

System State -varmuuskopiointi on suositeltu tapa tehdä varmuuskopiointi. Yhdellä varmuuskopiolla saadaan varmistetuksi kaikki tärkeät tiedot, eikä tällöin palautuksessa tarvitse palauttaa useista eri varmuuskopioista. Varmuuskopiointi voidaan tehdä koneen omalla backup-ohjelmalla tai kolmannen osapuolen ohjelmalla, jolla voi tallentaa System State -asetukset. Varmuuskopiointiin sisältyvät seuraavat tiedot:

- CA:n tietokanta, jossa on kaikkien myönnettyjen ja suljettujen sertifikaattien tiedot.
- CA:n avainpari. CA:n sertifikaatti voi olla itse myönnetty, kuten yleensä juuri-CA:n tapauksessa tai sertifikaatti voi olla jonkin toisen CA:n myöntämä. Joka tapauksessa ympäristön palautus täytyy tehdä samalla avainparilla, joka oli käytössä ennen palautusta. Tällöin jo myönnetyt sertifikaatit asiakkaille pysyvät voimassa. Jos CA:n sertifikaatti uusitaan uudella avainparilla, pitää kaikki versiot avainpareista varmuuskopioida. Jos käytössä on HSM-moduuli, johon on tallennettu CA:n yksityinen avain, pitää avainparin varmuuskopioinnissa käyttää HSM:n omia ohjelmia ja varmuuskopiointiohjelmaa. On erityisen tärkeä huomata, että kun avain siirretään HSM-moduuliin asennuksen aikana, yksityinen avain poistetaan koneesta, joten se ei tule mukaan System State -varmuuskopioon.
- IIS-palvelimen metabase-tietokanta. Muutokset sertifikaattipalvelun www-sivulle tallentuvat IIS metabase -tietokantaan. Tämä tietokanta tallentuu System State -varmuuskopiossa.
- Rekisterin varmuuskopio. Asennuksessa tulee hyvin paljon erilaisia konfigurointeja koneen rekisteriin. [1, s. 235-236.]

System state -varmuuskopiointi suoritetaan seuraavasti:

- Ensin tarkastetaan, että Certificates-palvelu on käynnissä. Tämä tapahtuu käynnistämällä Certificates Authority -työkalu Administrative Tools -valikosta ja tutkimalla, että palvelimen kuvakkeen päällä on vihreä v-merkki. Toinen tapa katsoa on Administrative Toolsin Services-työkalu. Varmuuskopiointi ei onnistu, jos palvelu ei ole päällä.
- Käynnistetään Backup-ohjelma Start - All Programs - Accessories - System Tools -valikosta.
- Jos ohjelmaan käynnistyy ohjattu toiminto, valitaan linkki Advanced mode.

- Valitaan Backup-välilehti.
- My Computer -kuvakkeen alta rastitetaan kohta System State.
- Browse-painikkeella valitaan tallennuspaikka.
- Painetaan Start Backup -painiketta.
- Advanced-painikkeella avataan options-ikkuna, josta valitaan Verify data after backup ja varmuuskopion tyypiksi Normal. OK-painikkeella kuitataan ikkuna.
- Valitaan valinta Allow only the owner and the Administrator access to the backup data.
- Start Backup -painikkeella suoritetaan varmuuskopiointi. [1, s. 237-238.]

8.2.2 Manuaalinen varmuuskopio

Manuaalinen varmuuskopiointi voidaan tehdä Certification Authority -työkalulla, Backup-ohjelmalla tai kolmannen osapuolen ohjelmalla.

Kun manuaalinen varmuuskopio tehdään Certification Authority -työkalulla, ohjattu toiminto avustaa yksityisen avaimen ja CA:n sertifikaatin sekä tietokannan varmuuskopioinnissa. Halutessa voidaan varmuuskopioida pelkästään avain ja sertifikaatti tai pelkästään tietokanta. Ohjattu toiminto kysyy salasanan, jolla salataan varmuuskopio. Tämä salasana tarvitaan palautuksessa.

Manuaalinen varmuuskopio ei tallenna IIS metabase -tietokantaa eikä rekisteriasetuksia. Nämä täytyy varmuuskopioida erikseen, jotta täydellinen palauttaminen on mahdollista. [1, s. 236-237.]

Manuaalinen varmuuskopio suoritetaan seuraavasti:

- Avataan Administrative Tools -valikosta Certification Authority -työkalu.
- Varmistetaan, että palvelu on käynnissä.
- Klikataan hiiren kakkospainikkeella palvelimen kuvaketta ja valitaan All Tasks ja edelleen Backup CA.
- Welcome-ikkunan jälkeen tulee Items to Backup -sivu. Valitaan kohdat Privat key and CA certificate ja Certificate database and certificate database log. Ensimmäinen valinta valitsee CA:n sertifikaatin sekä yksityisen avaimen varmuuskopioon. Jos yksityinen avain on tallennettu laitteeseen (HSM-moduuli tai toimikortti), jätetään tämä valinta tyhjäksi. Toinen valinta valitsee itse tietokannan ja lokitiedostot.

- Browse-painikkeella valitaan, minne varmuuskopio halutaan tallentaa.
- Lopuksi kysytään salasana, jolla suojataan PKCS #12-muotoinen tiedosto, johon tallennetaan yksityinen avain ja sertifikaatti.

Kun varmuuskopiointi on suoritettu, avataan kansio, johon PKCS #12 -tiedosto tallennettiin. Tarkastetaan, että hakemistossa on p12-tarkentiminen tiedosto ja alihakemisto nimeltään Database, jossa ovat tietokanta ja lokitiedostot. [1, s. 237-238.]

8.3 Palautus

Palautus Certification Authority -työkalulla tehdään napsauttamalla hiirellä koneen kuvaketta, valitsemalla All Tasks ja edelleen valitsemalla Restore CA. Palautuksen ajaksi sertifikaattipalvelu pysäytetään Lisäksi kysytään salasana sekä lopuksi käynnistetään palvelu.

Käytettäessä Backup-ohjelmaa sertifikaattipalvelun tiedostot varmuuskopioidaan System State -valinnassa, joten ne palautuvat palautettaessa System State. Kolmannen osapuolen varmuuskopiointiohjelmissa luonnollisesti turvaudutaan ohjelman käyttöohjeisiin. [1, s. 242-245.]

9 AUDITOINTI

Sertifikaattipalvelun tapahtumia tulee seurata toiminnan sekä mahdollisten hyökkäysten varalta. Auditointi tallentaa halutut tapahtumat järjestelmän lokiin, josta niitä voidaan katsoa, tarkemmin sanottuna Event Viewer:in security-lokiin. Offline CA:n auditointi määritellään Local Security Policy -konsolissa, joka löytyy Administrative Tools -työkaluista. Offline-tilassa eli verkosta poistettuna toimivat juuri-CA-palvelin ja tämän alapuolella sijaitseva käytäntö-CA -palvelin, jos kyseessä on kolmitasoinen hierarkia. Online-tilassa verkossa sertifikaatteja myöntävän myöntäjä-CA-sertifikaattipalvelimen auditointi määritellään sen organisaatioyksikön ryhmäkäytännössä, jossa palvelin sijaitsee. Määrittely tapahtuu molemmissa tapauksissa aktivoimalla Audit Object Access -asetus ryhmäkäytännön Audit Policy -kohdassa. Molemmat, sekä onnistuneet että epäonnistuneet tapahtumat tulee määritellä merkittäväksi lokiin. Tämän jälkeen Certification Authority -työkalulla valitaan tarkkailtavat tapahtumat. Valittavat tapahtumat löytyvät CA:n ominaisuuksien Auditing-välilehdeltä. Välilehdeltä voidaan valita seuraavat tapahtumat tallennettavaksi lokiin:

- CA:n tietokannan varmuuskopiointi ja palauttaminen
- CA:n konfiguraation muuttaminen
- CA:n tietoturva-asetuksien muuttaminen
- sertifikaattikyselyjen hallita
- sertifikaattien käytöstä poistaminen ja sulkulistan julkaiseminen
- arkistoitujen avaimien tallentaminen ja palauttaminen
- sertifikaattipalvelun käynnistäminen ja pysäyttäminen.

Näiden asetusten muuttaminen vaatii, että muuttajalla on Manage Auditing and Security Log -oikeus CA-koneella. Asetukset on myös mahdollista antaa certutil-komennolla. Kaikkien tapahtumien lokiin tallentaminen voidaan määrittää komennolla:

certutil -setreg CA\AuditFilter 127 [1, s. 118; 2, s. 351.]

10 SERTIFIKAATTIEN ARKISTOINTI JA PALAUTUS

Windows Server 2003/2008 -sertifikaattipalvelin voi automaattisesti arkistoida käyttäjän yksityisen avaimen. Arkistointi on mahdollista, jos käytetään ohjelmistopohjaista CSP:tä. Laitteistopohjaista CSP:tä käytettäessä turvaudutaan laitteen omiin ohjelmistoihin. Avaimen arkistoimiseksi ylläpitäjä tekee sertifikaattipohjaan asetuksen, joka varmuuskopioi käyttäjän yksityisen avaimen samalla kun sertifikaatti myönnetään. Tällöin avaimen kadotessa saadaan tiedostot auki tällä vara-avaimella, joka siis palautetaan arkistosta. Tarvittaessa tiedostojen avaamisen jälkeen avain laitetaan sulkulistalle ja käyttäjälle luodaan uusi sertifikaatti ja avaimet. Käyttäjän avaimet voidaan arkistoida myös manuaalisesti käyttäjän koneelta tiedostoon mm. Certificates-työkalulla. Myös palautus voidaan tehdä samalla työkalulla. Käyttäjän yksityinen avain on tallennettu käyttäjän profiiliin salattuna. Fyysisesti avain sijaitsee \Documents and Settings \ UserName \ ApplicationData \ Microsoft \ Crypto \ RSA \ User SID- tai \Documents and Settings \ UserName \ Application Data \ Microsoft \ Crypto \ DSS \ User SID -hakemistossa. Windows 2008:n CNG-salausta käytettäessä tallennus tapahtuu \Documents and Settings \ UserName \ ApplicationData \ Microsoft \ Crypto -hakemistoon. Näin ollen käyttäjä voi hukata avaimensa mm. seuraavista syistä:

- Käyttäjän profiili tuhoutuu.
- Käyttöjärjestelmä asennetaan uudelleen.

- Levy korruptoituu.
- Kone varastetaan.

Käyttäjän yksityinen avain voidaan siis varmuuskopioida siltä varalta, että hän hukkaa yksityisen avaimensa tavalla tai toisella. Automaattisen arkistoinnin lisäksi avain voidaan tallentaa vaihtoehtoisesti manuaalisesti tiedostoksi Sertifikaatti-työkalun vienti-toiminnolla. Tämä tulee kysymykseen luonnollisesti vain pienissä ympäristöissä. [1, s. 311-312; 2, s. 15.]

10.1 Avaimien vienti (Exporting Keys)

Avaimien vienti Sertifikaatti-työkalulla (Certificates) on yksinkertaisempi tapa varmuuskopioida käyttäjän yksityinen avain ja myös tarvittaessa julkinen avain. Varmuuskopioinnin voi tehdä tarvittaessa myös Internet Explorer -selaimella, Outlook-sähköpostiohjelmalla, Certutil.exe-ohjelmalla tai Certificate Authority -konsolilla. Vientitoiminnossa voi valita kaksi tiedostomuotoa. PKCS #12 -tiedostomuoto tukee yksityisen avaimen vientiä ja PKCS #7 -tiedostomuoto tukee julkisen avaimen vientiä. Yksityistä avainta tallennettaessa pitää antaa salasana, jolla suojataan avaimen luvaton palauttaminen PKCS #12 -tiedostosta. Kannattaa huomioida myös, että Outlook-asiakasohjelmasta voidaan avaimet tallentaa EPF-tiedostomuotoon (Exchange Protection File). Lisäksi kannattaa huomioida, että sertifikaatit perustuvat sertifikaattipohjiin, joissa voidaan määrätä, voidaanko yksityistä avainta yleensä tallentaa. Tietoturvaan perustuen yksityisen avaimen tallentaminen voidaan halutessa kieltää. Sertifikaattipohja määrää, mitä tarkoitusta varten sertifikaatti myönnetään, joten kaikkia sertifikaatteja ei voi tallentaa kaikilla edellä mainituilla ohjelmilla.

Sertifikaatin tallennuksessa vientitoiminnolla pitää ottaa kantaa seuraaviin asetuksiin:

- **Include all certificates in the certification path if possible**: Asetus tallentaa koko sertifikaattipolun; siis palautuksessa palautetaan koneeseen oman sertifikaatin lisäksi myös kaikki muut CA:n sertifikaatit aina juuri-CA:ta myöten. Tätä asetusta käytetään, jos kone ei voi kommunikoida verkon kautta sertifikaatin myöntäneen CA:n tai ylempien CA:iden kanssa.
- **Enable strong protection**: Tallentaa PKCS #12 -tiedoston, joka sisältää yksityisen avaimen, salattuna 128-bittisellä salauksella. On suositeltavaa

käyttää tätä asetusta. Vanhoissa ympäristöissä kannattaa huomioida, että tämä asetus vaatii IE 5.0-selaimen ja Windows NT 4.0 Service Pack 4:n tai uudemman.

- **Delete the private key if the export is successful**: Tämä asetus tuhoaa yksityisen avaimen koneesta siirron lopuksi.

Viennin yhteydessä tiedosto kannattaa salata. Avaimen sisältävä tiedosto tulee tallentaa siirrettävälle medialle ja tallentaa tämä media varmaan paikkaan, esim. kassakaappiin. [2, s. 344-346.]

10.2 Avaimen arkistointi

Version 2 ja 3 sertifikaattipohjiin voidaan määritellä käyttäjän yksityisen avaimen automaattinen arkistointi sertifikaatin luonnin yhteydessä. Avaimen palautukseen liittyy läheisesti kaksi ylläpitäjän roolia. Certificate manager -roolin omaava ylläpitäjä vastaa käyttäjän salatun yksityisen avaimen noutamisesta tietokannasta sekä määrittää palautusagentin. Avaimen palautusagentin roolin omaava ylläpitäjä poistaa salauksen tästä käyttäjän avaimesta ja palauttaa sen käyttäjälle.

Avain tallennetaan CA:n tietokantaan salattuna. Normaalisti sertifikaatin luonnin yhteydessä asiakas ei lähetä yksityistä avaintaan CA:lle, vaan tallentaa sen suoraan käyttäjän profiiliin. Julkinen avain sen sijaan lähetetään CA:lle. Automaattisen arkistoinnin yhteydessä myös yksityinen avain lähetetään CA:lle. Siirron alussa se salataan CA:n julkisella avaimella. Saatuaan tiedoston CA purkaa salauksen omalla yksityisellä avaimellaan. Näin avain on saapunut turvallisesti CA:lle. Tämän jälkeen CA tarkastaa asiakkaan avaimen ja salaa sen symmetrisellä salauksella. Asiakkaan salattu avain arkistoidaan tietokantaan. Edelleen symmetrinen avain salataan **avaimen palautusagentin** (KRA - Key Recovery Agent) julkisella avaimella. Symmetrinen avain tallennetaan samaan tiedostoon asiakkaan yksityisen avaimen kanssa. Tallennettu tiedosto on BLOB-tiedostomuodossa (Binary Large Object). Edellä mainittujen toimenpiteiden ansiosta palautusagentti (KRA) pääsee palauttamaan asiakkaan yksityisen avaimen tarvittaessa. CA ei itsessään sisällä mitään tietoa asiakkaan yksityisen avaimen palauttamiseksi, sillä palautus voidaan tehdä avaimen palautusagentin eli KRA:n yksityisellä avaimella, joka on tallennettu hänen omaan profiiliinsa. Näin asiakkaiden yk-

sityiset avaimet eivät suoraan paljastu edes siinä tapauksessa, että joku ulkopuolinen pääsee murtautumaan CA:han.

Seuraavat asiat tulee toteuttaa, jotta avaimien arkistointi ja palautus toimii:

- Yhdellä tai useammalla ylläpitäjällä pitää olla haettuna avaimen palautusagentin sertifikaatti, jolla käyttäjien avaimia voidaan palauttaa. Avaimen palautusagentti pitää myös määritellä toimintaan CA-koneessa.
- Sertifikaatit, joiden avain arkistoidaan, perustuvat version 2 tai 3 sertifikaattipohjiin. Lisäksi sertifikaattipohjassa tulee olla valittuna valinta Archive Subject's Encryption Private Key. Tämä tehdään Certificate Template -työkalulla (Certtmpl.msc) Request Handling -välilehdellä.
- CSP:n tulee tukea yksityisen avaimen vientiä. Sertifikaattihaku epäonnistuu, jos sertifikaattipohjassa on määritelty avaimen arkistointi ja CSP ei salli tätä.
- Sertifikaatin myöntävän palvelimen tulee olla Windows Server 2003- tai 2008 -palvelin.
- Kaikkien asiakkaiden tulee olla Windows XP/Vista/7- tai Windows Server 2003/2008 -asiakkaita.
- Käytössä on **enterprise CA.**
- Windows Server 2003- tai 2008 -skeman laajennokset (schema extensions) on ajettu aktiivihakemiston metsässä (forest). Tämä tulee tehdä silloin, jos kaikki palvelimet eivät ole Windows Server 2003- tai 2008 -palvelimia vaan ainakin osa on Windows 2000 -palvelimia; siis metsä on Windows 2000 -metsä (Windows 2000 forest). Jos laajennoksia ei ajeta, version 2 ja 3 pohjat eivät ole käytössä. Laajennokset ajetaan adprep.exe /forestprep -komennolla.

Lyhyesti yhteenvetona voidaan todeta, että käyttäjä saa sertifikaatin, jonka CA allekirjoittaa. Samalla sertifikaatti ja yksityinen avain arkistoidaan CA:n tietokantaan salattuna. Salauksen ansiosta käyttäjän avaimen voi palauttaa vain tietty, ennalta määrätty avaimen palautusagentti.

10.3 Avaimen palautus

Asiakkaan avain voidaan palauttaa tietokannasta **certutil**-työkalulla. Palautukseen tarvitaan asiakkaan sertifikaatin sarjanumero, joka voidaan etsiä Certificates-konsolilla. Certificate manager -roolin omaava ylläpitäjä antaa komennon:

certutil -getkey 1234567890 BlobFile

Komennon tuloksena tietokannasta palautetaan sarjanumeroa 1234567890 vastaava salattu BLOB-tiedosto. BLOB-tiedosto on PKCS #7 -muodossa. BLOB-tiedosto toimitetaan avaimen palautusagentille (KRA), joka omassa koneessaan purkaa salauksen. PKCS #7 -tiedosto sisältää myös avaimen palautusagentin tiedot, joiden perusteella palautusagentti tunnistetaan. Avaimen palautusagentti (KRA) antaa komennon:

certutil -recoverkey BlobFile user.pfx -p password

Komento annetaan nimenomaan tätä toimenpidettä varten tarkoitetussa työasemassa, johon on asennettu palautusagentin yksityinen avain. Avaimen palautusagentti antaa palautuksen yhteydessä salasanan, joka asiakkaan tulee antaa avainta palauttaessaan. Avain tallennetaan user.pfx-tiedostoon, joka on PKCS #12 -tiedostomuodossa. Avaimen palautusagentti toimittaa tiedoston ja tarvittavan salasanan asiakkaalle, joka palauttaa yksityisen avaimen Certificates-konsolilla tai sertifikaatin tuonti -toiminnolla (kaksoisnapsautus tiedostoon) omalle työasemalleen.

Certificate manager on yleensä eri henkilö kuin avaimen palautusagentti (KRA). Nämä voivat olla myös sama henkilö; tällöin henkilöllä on mahdollisuus päästä käsiksi asiakkaiden henkilökohtaiseen tietoon! Tietoturvan kannalta nämä roolit kannattaa eriyttää. Windows Server 2003 Resource Kit -työkalut sisältävät Key Recovery -työkalun (krt.exe), jolla voidaan suorittaa edellä kuvatut toimenpiteet helpommin graafisessa ympäristössä. Resource Kit -työkalut voi ladata Microsoftin www-palvelimelta. Tämä työkalu mahdollistaa seuraavat toimet:

- Arkistoitujen avaimien etsinnän CA:n tietokannasta.
- Näyttää arkistoidun avaimen palautusagentin (KRA).
- Noutaa salatun PKCS #7 -tiedoston tietokannasta.
- Poistaa salauksen PKCS #7 -tiedostosta ja asettaa salasanan syntyneeseen pfx-tiedostoon.

Kuten jo aikaisemmin mainittiin, asiakkaan yksityisen avaimen palautus tulee tehdä sitä varta vasten luodussa turvallisessa työasemassa. Varmuuden vuoksi palautusagentin avaimet tulisi poistaa palautusagentin profiilista tässä työasemassa. Avaimet tulisi palauttaa työasemassa sijaitsevaan profiiliin

vain silloin, kun niitä tarvitaan. Avaimet säilytetään turvallisessa paikassa kuten kassakaapissa. Nämä varotoimenpiteet tulee suorittaa siitä syystä, että palautusagentin avaimilla käytännössä päästään lukemaan asiakkaiden henkilökohtaista tietoa ja vääriin käsiin joutuessaan avaimet tekevät salaisesta tiedosta julkista. PKCS #12 -tiedosto, joka toimitetaan asiakkaalle, tulee toimittaa turvallisesti, jotta tiedoston sisältämä yksityinen avain ei paljastu. Lopuksi tämä tiedosto tulee tuhota, jotta avaimia ei voida yrittää palauttaa asiattomasti uudelleen. Nämä toimenpiteet tulee kirjata yrityksen tietoturvakäytäntöön.

Avaimen palautusagentin rooli on erittäin kriittinen. Kannattaa harkita, kenelle tämä rooli yrityksessä annetaan, tarvitaanko mahdollisesti vahvaa kirjautumista työasemaan (esim. toimikortti) sekä jaetaanko rooli jopa usealle käyttäjälle. Jos halutaan, ettei yksi yksityinen henkilö pääse palauttamaan kenenkään toisen yksityistä avainta ja mahdollisesti väärinkäyttämään tätä oikeutta, annetaan palautusagentin rooli esim. kolmelle henkilölle. Tällöin kirjautumiseen palautusagentin tunnuksella vaadittava salasana jaetaan kolmeen osaan ja jokainen osa annetaan eri henkilöille. Tällöin yksityisen avaimen palautuksessa kirjauduttaessa työasemaan, jossa palautus voidaan suorittaa, pitää olla jokaisen kolmen henkilön kirjoittamassa oma osaansa salasanasta.

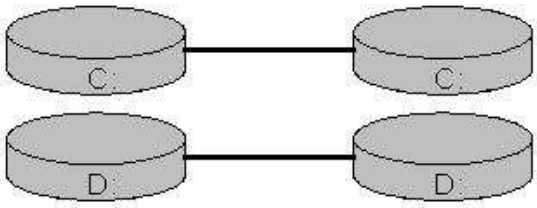
Kun asiakkaan yksityinen avain on palautettu ja asiakas on purkanut salatun tiedon, pitää asiakkaan sertifikaatti laittaa sulkulistalle. Asiakkaalle luodaan uusi sertifikaatti ja asiakas salaa tiedot uudestaan näillä uusilla avaimilla. Tällä varmistetaan se, ettei palautusprosessin jälkeen mahdollisesti paljastunutta vanhaa yksityistä avainta voida enää käyttää salaisen tiedon tarkasteluun. [1, s. 311-326; 2, s. 343-351.]

11 LEVYJÄRJESTELMÄT

Sertifikaattipalvelimen levyjärjestelmä tulisi miettiä ja valita käytön mukaan. Offline-tilassa toimiva palvelin ei tarvitse niin tehokasta levyjärjestelmää kuin online-tilassa toimiva. Molemmissa tiloissa käyttöjärjestelmä tulisi erottaa tietokannasta ja loki-tiedostoista. Myös levytilaa tulee varata riittävästi.

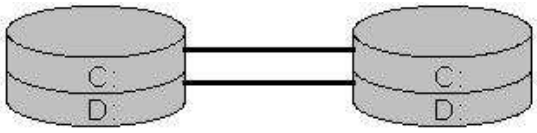
Offline-tilassa toimivaan palvelimeen voidaan asentaa käyttöjärjestelmä C:-asemalle omalle levylle ja tietokanta sekä loki-tiedostot omalle levylle D:-

asemalle (kuva 16). Molemmat levyt peilataan erikseen RAID 1 -järjestelmään.



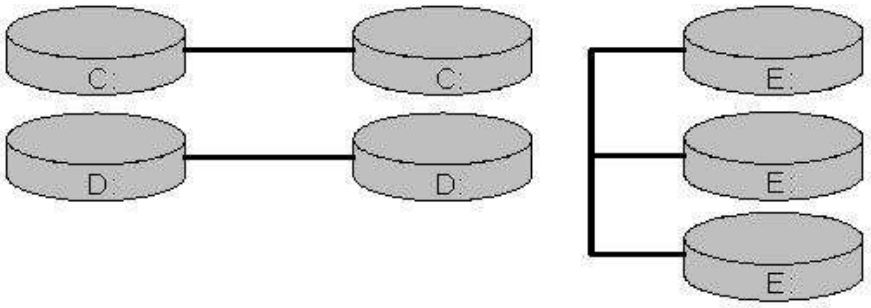
Kuva 16. Offline-palvelimen levyjärjestelmänä kahden levyn RAID 1 eli levyjen peilaus.

Vaihtoehtoisesti yksi levy voidaan jakaa kahteen osioon ja nämä osiot määritellä omiksi levyasemikseen C: ja D: (kuva 17). Levylle luodaan RAID 1 -peilaus. Konfigurointi säästää kustannuksissa mutta antaa tarvittavan vikasietoisuuden levylle.



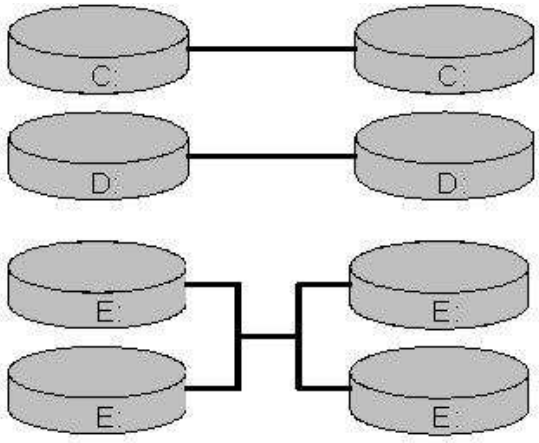
Kuva 17. Offline-palvelimen levyjärjestelmä edullisemmin rakennettuna

Online-tilassa toimiva sertifikaattipalvelin vaatii tehokkaamman levyjärjestelmän kuin offline-tilassa toimiva palvelin. Tästä syystä on suositeltavaa käyttää RAID 1 -peilauksen lisäksi RAID 5 - tai RAID 0+1 -levyjä. Kuva 18 esittää ensimmäisen vaihtoehdon. Siinä käyttöjärjestelmä on asennettu C-asemalle omalle levylle ja tästä levystä on tehty RAID 1 -peilaus. Lokitiedostot on asennettu D-asemalle omalle levylleen ja tästä on tehty samoin RAID 1 -peilaus. Tietokanta on tallennettu RAID 5 -levylle, joka antaa paremman suorituskyvyn levyltä luettaessa.



Kuva 18. Online-palvelimen levyjärjestelmä, RAID 1 ja RAID 5

Kuva 19 esittää toisen vaihtoehdon. Tässä vaihtoehdossa käyttöjärjestelmä ja loki-tiedostot on asennettu samalla tavalla kuin edellisessä vaihtoehdossa, mutta tietokanta on asennettu RAID 0+1 -levylle. Tällöin siis tiedot kirjoitetaan raidoittain, mikä lisää suorituskykyä ja tämä raitasarja sitten peilataan omalle levylleen. RAID 0+1 on suorituskyvyltään parempi kuin RAID 5, joten se kannattaa valita ympäristöissä, joissa sertifikaatteja myönnetään erittäin suuria määriä. [1, s. 80-81.]



Kuva 19. Online-palvelimen vaihtoehtoinen levyjärjestelmä, RAID 1 ja RAID 0+1

12 POLITIIKAT JA KÄYTÄNNÖT

Ennen PKI-ympäristön asentamista pitäisi tarkastaa **tietoturvakäytäntö** (security policy) ajan tasalle PKI:ta varten ja että sellainen yleensäkin on olemassa. Tietoturvakäytännön tehtävä on informoida sekä sopia pelisäännöt koko yrityksen henkilöstölle työtehtävissä, kuinka tietoturva otetaan huomioon ja sitä sovelletaan. Lisäksi tulisi luoda **varmennepolitiikka** (certificate policy, CP), jossa kuvataan varmentajan keskeiset toimintaperiaatteet hyvin yleisellä tasolla. Varmennepolitiikkaa yksityiskohtaisempi kuvaus löytyy **varmennekäytäntölausumasta** (certificate practice statement - CPS). Varmennekäytäntölausuma on julkinen dokumentti. Siinä kuvataan erittäin tarkasti toimet ja tehtävät, jotka CA tekee tietoturva- ja varmennekäytäntöjen ylläpitämiseksi. Sitä voidaan pitää sopimuksena CA:n ja asiakkaan, joka hakee sertifikaattia CA:lta, välillä. **Varmennekäytäntö** määrittää, mitkä tunnistustoimenpiteet vaaditaan sertifikaatteja myönnettäessä. Esimerkiksi voi riittää, että käyttäjä on kirjautunut käyttäjätunnuksellaan ja salasanallaan järjestelmään tai voidaan vaatia henkilökohtainen tunnistautuminen kuvallisen henkilökortin kanssa. Muut organisaatiot määrittelevät varmennekäytännön

ja varmennekäytäntölausuman perusteella, kuinka paljon ne luottavat CA:n toimintaan ja edelleen hankkivatko ne sertifikaattinsa tältä CA:lta. CA:n kannalta varmennekäytäntölausuma ja varmennepolitiikka ovat juridisia dokumentteja, jotka tulee tarkastaa erittäin huolellisesti ennen niiden julkaisua. Dokumenttien tekemiseen yleensä osallistuu lainoppineita henkilöitä. [1, s. 35-47.]

13 OID-TUNNUKSET

OID on ainutkertainen standardoitu (ISO/IEC 8824) numerosarja, jolla voidaan yksilöidä muun muassa organisaatioita, esineitä, laitteita, koodistoja, asiakirjoja ja ohjelmistoja maailmanlaajuisesti. Järjestelmä on hierarkkinen puurakenne, jolloin tunnuksen saanut organisaatio voi määrittää saamansa tunnuksen alapuolelle haluamansa järjestelmän. Esimerkiksi organisaatio on saanut tunnuksen 1.2.3. Tällöin organisaatio voi itse määrittää esim. tunnuksen 1.2.3.1 alle laitteet ja tunnuksen 1.2.3.2 alle ohjelmistot.

PKI-järjestelmässä OID-tunnuksella voidaan yksilöidä esim. sertifikaattipohjat ja CPS. Jos PKI-sovelluksia käytetään ulkopuolisen organisaation kanssa, tulee OID-tunnukset hakea julkiselta OID-hallinnoijalta, jolloin voidaan varmistua, että tunnukset ovat yksilöllisiä Internetissä. Julkisia OID-tunnuksia myöntävät mm. IANA, ANSI ja eri maiden omat organisaatiot. Esimerkiksi OID-yksilöintitunnus 1.2.246 on Suomen juuri. SFS myöntää tunnukset Suomen juuren alle. IANA:n tunnukset alkavat numerosarjalla 1.3.6.1.4.1, jonka merkitys on iso(1).org(3).dod(6).internet(1).private(4) .enterprise(1). ANSI:n tunnukset alkavat aina numerosarjalla 2.16.840.1, jonka merkitys on joint-iso-itu-t(2).country(16).US(840).US company arc(1). Pääjuuren numerolla yksi alkavaa puuta hallinnoi ISO ja numerolla kaksi alkavaa puuta ITU.

Microsoft on varannut oman tunnuksen ISO:n OID-avaruudesta. Jos käytetään näitä olemassa olevia tunnuksia, ne ovat muotoa 1.3.6.1.4.1.311.21.8.a.b.c.d.e.1.402. Sarja a.b.c.d.e on yksilöllinen numerosarja, joka perustuu asennetun metsän GUID-tunnukseen. Organisaatio voi käyttää tätä olemassa olevaa OID-avaruutta, jos PKI:n käyttö on organisaation sisäistä. Muussa tapauksessa tulee hankkia julkinen OID-tunnus. [1, s. 96-97.]

14 LUOTTOSUHTEET ORGANISAATIOIDEN VÄLILLÄ

Joskus organisaation sertifikaattien tulee olla luotettuja myös toisissa organisaatioissa. Tällaisia tilanteita voivat olla esimerkiksi salatun sähköpostin käyttö organisaatioiden välillä tai jos ohjelmistokoodi on allekirjoitettu toisen organisaation sertifikaatilla. Alla on lueteltu tapoja, joilla luottosuhde voidaan rakentaa:

- varmenneluottolista (CTL / certificate trust list)
- yhteinen juuri-CA
- ristiinsertifiointi (cross-certification)
- pätevä alaisuussuhde (qualified subordination)
- silta-CA (Bridge CA).

Seuraavassa on lyhyt kuvaus näistä tavoista luoda luottosuhde.

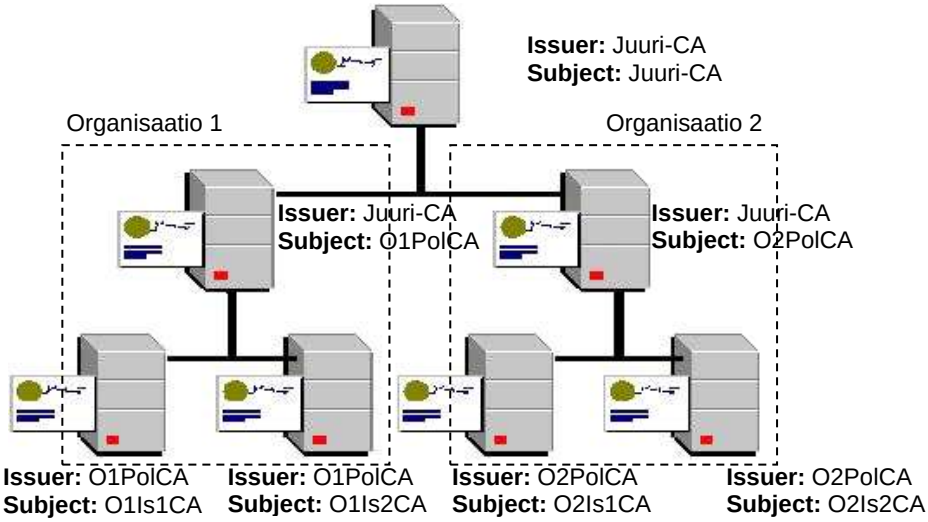
14.1 Varmenneluottolista

Varmenneluottolista on Microsoftin oma tapa luoda luottosuhde eri organisaatioiden välille. Tämä toimii vain Microsoftin omissa käyttöjärjestelmissä eikä ole toteutettavissa muissa käyttöjärjestelmissä. Varmenneluottolistan avulla voidaan määritellä toisen organisaation juuri-CA, johon oma organisaatio luottaa. Luottosuhdetta voidaan hienosäätää rajoituksilla. Rajoituksilla voidaan määritellä aika, kuinka kauan toisen organisaation sertifikaatteihin luotetaan sekä sertifikaattien tyyppi, johon luotetaan (esim. sähköpostin käyttöön myönnetty sertifikaatti).

Varmenneluottolista määritellään voimaan ryhmäkäytännöllä. Ryhmäkäytäntöasetus linkitetään siihen verkkoalueeseen, domainiin tai organisaatioyksikköön, johon luottosuhde halutaan luoda. Luottosuhde kohdistuu niihin koneisiin, joiden konetili sijaitsee kohteessa, johon ryhmäkäytännön linkitys kohdistuu. Määritys tapahtuu ryhmäkäytännön Computer Configuration\WindowsSettings\ Security Settings\Public Key Policies\ Enterprise Trust -säiliössä määrittelemällä uusi varmenneluottolista (New -> Certificate Trust List). Tämä käynnistää ohjatun toiminnon, jolla varmenneluottolista saadaan muodostettua. Asetus kannattaa määritellä ryhmäkäytännön koneasetuksiin eikä käyttäjäasetuksiin, koska tällöin asetukset tulevat voimaan kaikille koneeseen kirjautuville käyttäjille.

14.2 Yhteinen juuri-CA

Kaksi tai useampi organisaatio voi rakentaa ympäristön, jossa niillä on yhteinen juuri-CA. Tällöin kaikki myönnetyt sertifikaatit linkittyvät tämän yhteisen juuren kautta ja ovat näin ollen luotettuja kaikissa näissä organisaatioissa. Kuva 20 esittää tilannetta, jossa kahdella organisaatiolla (O1 ja O2) on yhteinen juuri-CA.

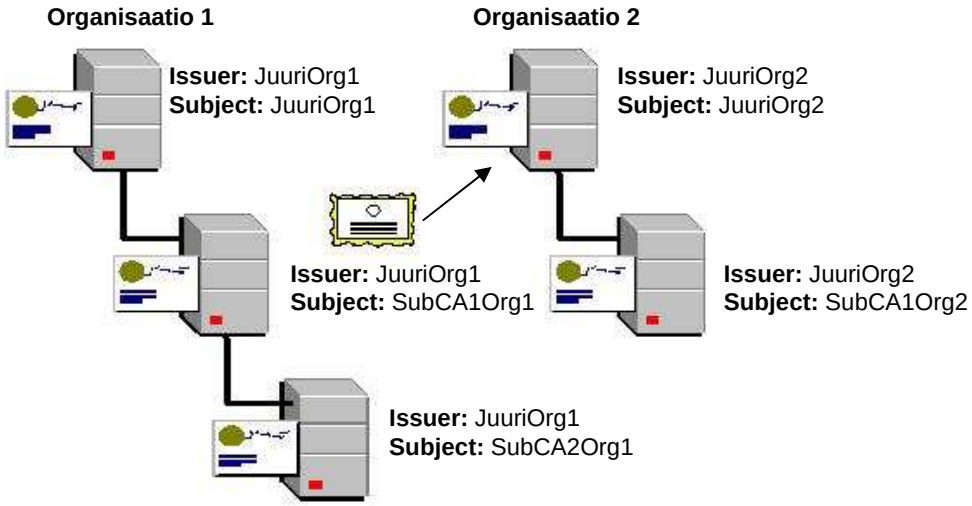


Kuva 20. Kahdella organisaatiolla yhteinen juuri-CA

Kuvassa Issuer ilmoittaa, mikä CA on myöntänyt sertifikaatin ja Subject ilmoittaa itse CA:n nimen. Juuri-CA on myöntänyt itselleen sertifikaatin, koska Issuer-kohdassa lukee juuri-CA. Edelleen juuri-CA on myöntänyt sertifikaatin Organisaatio1:n O1PolCA-palvelimelle ja O1PolCA-palvelin on myöntänyt sertifikaatin edelleen O1IS1CA-palvelimelle. Organisaatio 2:n puolella juuri-CA on myöntänyt sertifikaatin O2PolCA-palvelimelle, joka on edelleen myöntänyt sertifikaatin O2Is2CA-palvelimelle. O1Is1CA- ja O1Is2CA-palvelimet myöntävät sertifikaatteja Organisaatio1:n asiakkaille ja O2Is1CA- ja O2Is2CA-palvelimet myöntävät sertifikaatteja Organisaatio2:n asiakkaille. Koska asiakkaiden sertifikaattien luottoketjut on muodostettavissa samaan juuren, kaikki asiakkaat luottavat toisiinsa.

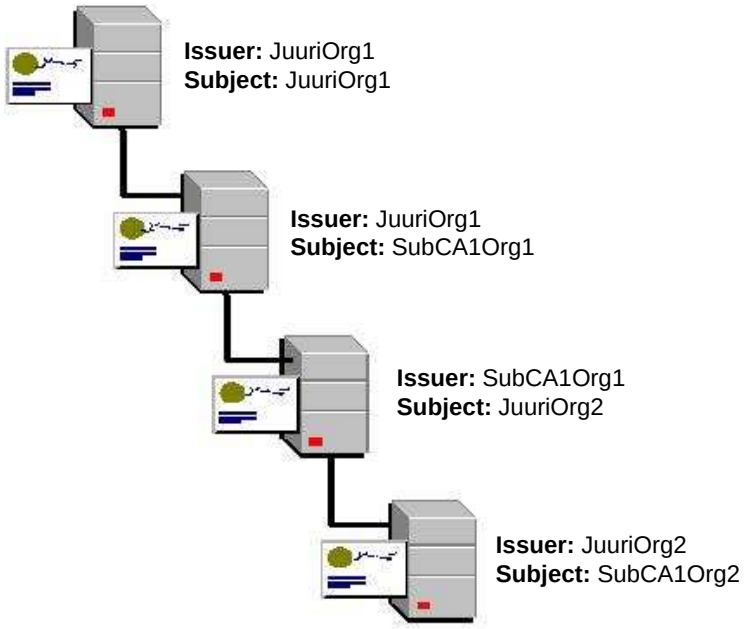
14.3 Ristiinsertifiointi

Ristiinsertifioinnissa oman organisaation CA myöntää ristiinsertifiointisertifikaatin toisen organisaation CA:lle. Normaalisti tämä myöntävä CA on jokin juuri-CA:n alla oleva CA.



Kuva 21. Ristiinsertifiointi kahden organisaation välillä

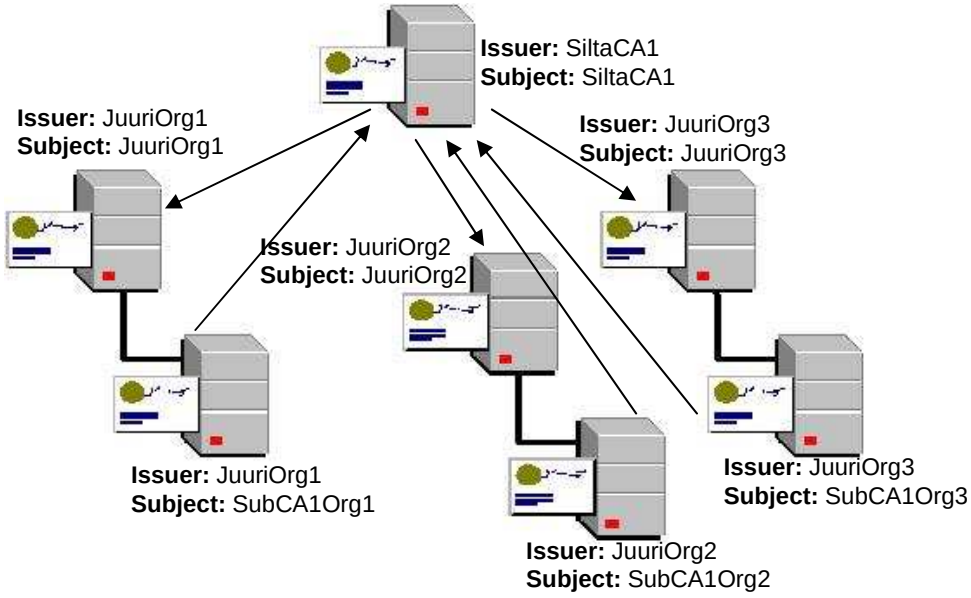
Kuva 21 esittää tilannetta, jossa organisaatio 1:n SubCA1Org1-palvelin on myöntänyt sertifikaatin organisaatio 2:n juuri-CA:lle. Kun tilannetta katsotaan Organisaatio 1:n näkökulmasta, tilanne näyttää siltä, että organisaatio 2:n juuri-CA on hierarkiassa SubCA1Org1-palvelimen alapuolella (kuva 22). Tällöin luottoketju on rakennettavissa organisaatio 2:n sertifikaateista organisaatio 1:n juureen asti. Tämän rakenteen etu on, ettei käyttäjille tarvitse myöntää uusia sertifikaatteja. SubCA1Org1-palvelimelta myönnettävään sertifikaattiin organisaatio 2:lle pitää käytännössä vielä määritellä ehdot, joiden puitteissa sertifikaatit toimivat. Ehtoihin kuuluu lähinnä määritys, kuinka pitkä luottoketju voidaan muodostaa organisaatio 2:n puolella, mihin nimiavaruuteen (domainin nimi) sertifikaatit myönnetään sekä sertifikaattien käyttötarkoitus (esimerkiksi salattu sähköposti) ja myötämiskäytäntö (myönnetäänkö sertifikaatti esimerkiksi vain kun käyttäjä on tunnistettu henkilökohtaisesti) [1, s. 288].



Kuva 22. Ristiinsertifiointi Organisaatio 1:n näkökulmasta

14.4 Silta-CA

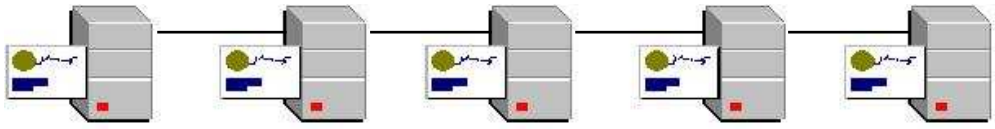
Silta-CA toimii hyvin pitkälle samalla tavalla kuin ristiinsertifiointi. Silta-CA:ta käytetään normaalisti, kun luottosuhteita rakennetaan hyvin usean organisaation välillä (kuva 23).



Kuva 23. Silta-CA kolmen organisaation välillä

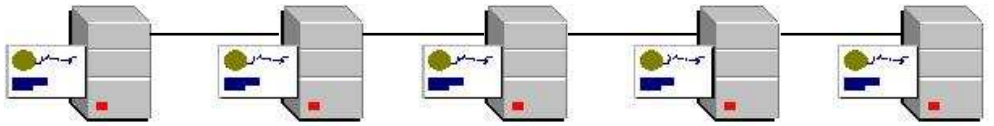
Tässä luottosuhde on rakennettu kolmen organisaation välille. Nuolet kuvassa osoittavat sertifikaattien myöntäjät sekä kenelle sertifikaatti myönnetään; nuolen alkupää ilmaiseen myöntäjän ja nuolen kärki ilmaisee kohteen, kenelle sertifikaatti myönnetään. Kuvasta voidaan todeta, että SiltaCA1 myöntää

sertifikaatit jokaisen organisaation juuri-CA:lle ja jokaisen organisaation SubCA myöntää sertifikaatin SiltaCA1:lle. Jos organisaatio 2:n sertifikaatteja tutkitaan organisaatio 1:n puolella, näyttää syntynyt luottoketju viiden palvelimen mittaiselta (kuva 24). Organisaatio 2:n sertifikaatit ketjuuntuvat silta-CA:n kautta organisaatio 1:n SubCA-palvelimeen ja sitä kautta juureen.



Kuva 24. Luottoketju katsottuna organisaatio 1:stä

Kuva 25 näyttää tilanteen organisaatio 2:sta katsottuna. Organisaatio 1:n sertifikaattien luottoketjut rakentuvat silta-CA:n kautta organisaatio 2:n Sub-CA-palvelimeen ja sitä kautta juureen. Silta-CA liittää kahden organisaation CA-palvelimet ketjuksi kuten ristiinsertifioinnissa, mutta silta helpottaa luottoketjujen hahmottamista varsinkin jos organisaatioita on enemmän kuin kaksi.



Kuva 25. Luottoketju katsottuna organisaatio 2:stä

Normaalisti organisaatio myöntää sertifikaatin silta-CA:lle myöntäjä-CA -palvelimelta eikä juuresta tai käytäntö-CA -palvelimelta. Jos yksi organisaatio poistuu ketjusta, saadaan kyseiset sertifikaatit sulkulistalle suhteellisen nopeasti, koska myöntäjä-CA -palvelin julkaisee sulkulistan useammin kuin käytäntö-CA- tai juuri-CA -palvelin. [1, s. 279-287.]

15 AKTIIVIHAKEMISTOYMPÄRISTÖN TARKASTAMINEN ENNEN ASENNUSTA

Alustavat toimenpiteet riippuvat toimialueiden ja metsien määrästä sekä toimialueen moodista (domain functional level). Toimenpiteitä ei juurikaan tarvita jos käytössä on yksi Windows Server2008 -toimialue. Joka tapauksessa

Windows-toimialueen ohjauskoneet voivat olla Windows 2000-, Windows Server 2003- tai Windows Server 2008 -ohjauskoneita. Toimialueen ei myöskään tarvitse toimia Windows Server 2008 -moodissa, vaan sertifikaattiympäristön Windows Server 2008 CA -palvelimineen voi asentaa toimimaan esimerkiksi Windows 2000 -toimialueella Windows 2000 -moodissa (domain or forest functional level). Windows 2000 -palvelimeen joudutaan asentamaan vähintään service pack 4, joka on minimitaso, kun tehdään Windows Server 2008 skeeman laajennus.

Skeeman laajennus on tehtävä, jos käytössä on Windows 2000- tai Windows Server 2003 -toimialue. Skeeman laajennuksella saadaan uudet ominaisuudet käyttöön. Uusia ominaisuuksia ovat mm. versio 3 -sertifikaattipohjat, OCSP-palvelin, NDES-palvelu (Network Device Enrollment Service) ja tuki elektronisiin allekirjoituksiin (rfc 3739). NDES-palvelun avulla voidaan jakaa sertifikaatit Ciscon laitteille SCEP-protokollaa (Simple Certificate Enrollment Protocol) käyttäen ilman, että aktiivihakemistoon tarvitsee luoda konetiliä.

Ennen skeeman laajennusta tulee etsiä ohjauskone, joka hoitaa schema operation master -roolia ja laajennus tulee suorittaa tältä koneelta. Laajennos suoritetaan **adprep /forestprep** -komennolla; adprep-ohjelma löytyy asennuslevyltä. Kun laajennokset ovat replikoituneet kaikille ohjauskoneille, suoritetaan jokaisessa toimialueessa asennuslevyltä **adprep /domainprep /gpprep** -komento jossakin toimialueen ohjauskoneessa.

Jos toimialueita on useita, CA-palvelin tulee liittää jokaisen toimialueen Cert Publishers -ryhmään. Jos toimialueita on vain yksi, ei tätä toimenpidettä tarvitse tehdä. Liittäminen täytyy tehdä, jotta CA pääsee tarvittaessa tallentamaan sertifikaatin käyttäjäobjektin userCertificate-attribuuttiin. Attribuuttiin tallennetulla sertifikaatilla käyttäjä saa haetuksi aktiivihakemistosta vastaanottajan julkisen avaimen. Liittäminen on yksinkertainen toimenpide, jos toimialue on alun perin luotu Windows Server 2003 - tai Windows Server 2008 -ympäristössä. Jos ympäristö on domainin luontivaiheessa Windows 2000, on liittäminen hankalampaa, koska Cert Publishers -ryhmä on global-ryhmä eikä domain local, kuten Windows Server 2003- ja Windows Server 2008 -ympäristöissä. Jotta liittäminen onnistuu, tulee Cert Publishers -ryhmä muuttaa global-ryhmäksi. Toinen vaihtoehto on muuttaa Cert Publishers -ryhmän oikeudet (luku ja kirjoitus) käyttäjäobjektin userCertificate-

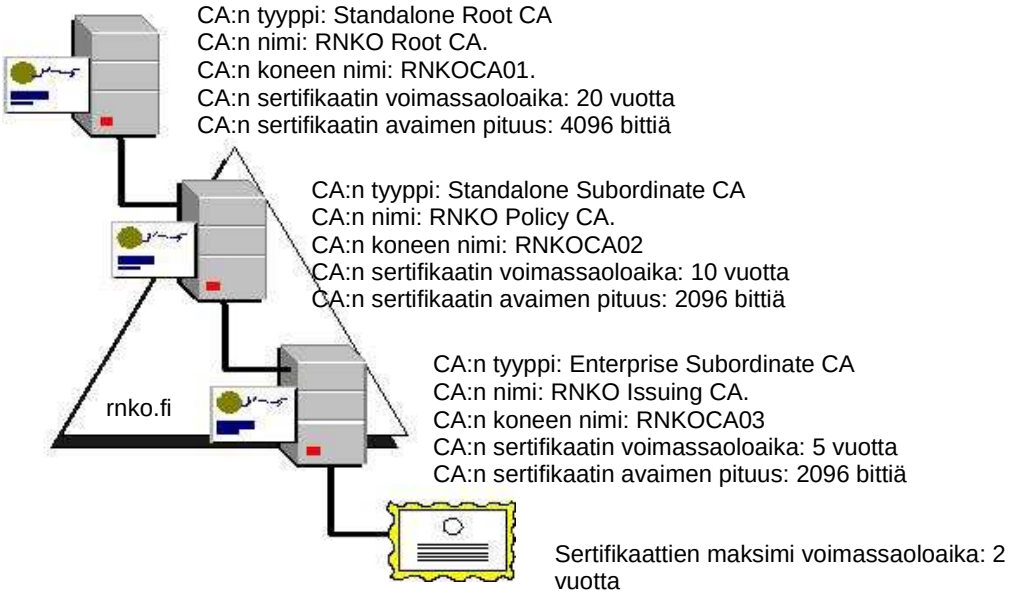
attribuuttiin jokaisessa toimialueessa. Molempiin toimenpiteisiin löytyvät ohjeet ja skriptit Microsoftin saitilta.

Jos CA:n yksityistä avainta ei tallenneta erilliseen laitteeseen kuten HSM-moduulin, tulee CA-koneen paikallisen Administrators-ryhmän jäsenyys rajoittaa. Paikallisen Administrators-ryhmän jäsen voi halutessaan tallentaa CA:n yksityisen avaimen vaikkapa USB-muistimoduuliin ja luoda uuden CA-palvelimen. Jos toimialueita on vain yksi ja se on Windows Server 2008 -toimialue, on tämä ainoa toimenpide, joka on pakko (tai ainakin erittäin suositeltavaa) suorittaa. [6, s.59-67.]

Jos Windows Server2003 -CA asennetaan Windows 2000 -toimialueelle, tulee lisäksi tarkastaa, onko Microsoft Exchange Server 2000 tai 2003 asennettu. Jos palvelin on asennettu, tulee tarkastaa onko inetOrgPerson kit-asennettu tai vastaavasti Windows Server 2003 -skeemalaajennus tehty ennen Exchange-palvelimen asennusta. Lisäksi tulee tarkistaa, että Windows 2000- palvelimiin on asennettu vähintään Service Pack 3. Jos Windows Server 2003 -skeemalaajennus tehdään, eikä inetOrgPerson kit-asennusta ole tehty ennen Exchange-palvelimen asennusta, käyttäjien LDAP-nimet eivät näy oikein. Microsoftin saitilta ja Support Tools -paketista löytyy tarvittavat ohjeet ja skriptit nimien korjaamiseen. [1, s.51-62.]

16 PKI-ASENNUSYMPÄRISTÖN KUVAUS JA ALUSTAVAT TOIMENPITEET

Seuraavaksi määritellään asennettava PKI-ympäristö. Kuva 26 selventää asennettavat palvelimet. Kahden ensimmäisen tason palvelimet juuri-CA- ja käytäntö-CA -palvelimet irrotetaan verkosta, joten niitä ei liitetä toimialueeseen. Kolmannella tasolla oleva myöntäjä-CA liitetään toimialueeseen, joten se toimii aktiivihakemistoympäristössä. Tässä työssä ei kuvata aktiivihakemiston asennusta eikä koneiden liittämistä toimialueeseen. Mainittavaa kuitenkin on, ettei CA-koneita kannata asentaa toimialueen ohjauskoneisiin, vaan koneissa on ainoastaan asennettuna sertifikaattipalvelu. Tällä järjestelyllä koneiden kuormitus pysyy normaalina, ja tietoturva on helpompi ottaa huomioon.



Kuva 26. PKI:n rakenne esimerkkiympäristössä

Sertifikaattipalvelimiin liittyvät yksityiskohtaiset asetukset käydään läpi ennen jokaisen tason asentamista, joten tässä vaiheessa vastataan karkeasti neljään kysymykseen:

- Millainen CA:n hierarkia rakennetaan?
- Kuinka CA:n avaimet suojataan?
- Mihin luodaan julkaisupisteet?
- Tehdäänkö ympäristöstä Suite B -yhteensopiva?

Hierarkian tasojen määrä määräytyy tietoturvan ja käytettävyyden asteista kuten jo aikaisemmin käytiin läpi. 3-tasoisella mallilla saadaan aikaan korkein tietoturva-aste. 2-tasoinen malli voidaan rakentaa jättämällä toinen vaihe tekemättä, siis toiselle tasolle juuren alle yhdistetään käytäntö-CA ja myöntäjä-CA. PKI:n rakentaminen aloitetaan aina juuri-CA -tasosta. Juuritaso yleensä myöntää itselleen sertifikaatin, kuten tässäkin työssä tehdään. Syntynyt yksityinen avain suojataan ja tallennetaan mahdollisimman hyvin. 2- tai 3-tasoinen malli on tietoturvallisempi kuin 1-tasoinen malli, jossa juuri-CA on suoraan kytketty verkkoon. Kuitenkaan käytännössä ei kannata tehdä enempää kuin kolme tasoa takaamaan tietoturvaa. Erityisen pienet ympäristöt, jotka eivät tarvitse korkeaa tietoturvaa, voivat tulla toimeen 1-tasoisella mallilla, jolloin juuri-CA jakaa sertifikaatit. Keskisuuret yritykset tarvitsevat 2-tasoisen mallin ja suuret yritykset 3-tasoisen mallin, jossa tasot 1 ja 2 toimivat offline-tilassa (poistettu verkosta). Jos pieni ympäristö tarvitsee erityisesti korkean tietoturvatason, silloin asennetaan 3-tasoinen malli nimenomaan tie-

toturvan takia. Tässä työssä asennetaan 3-tasoinen malli,minkä lisäksi myös selvitetään jokaisen tason asennukseen liittyvät vaiheet. Rinnakkaisia käytäntö-CA- tai myöntäjä-CA -koneita ei asenneta, koska asennus on käytännössä lähes kopio samalla tasolla olevasta CA-koneesta.

Juuri-CA:n avaimen pituuden olisi hyvä olla 4096 bittiä. Myöntäjä-CA:n avaimen pituus voi olla 2048 bittiä. Jos ympäristössä on käytössä kolmansien osapuolien ohjelmia tai laitteita, voi näillä olla ongelmia pitemmän kuin 2048 bitin avaimen pituuden kanssa. Siis avaimen pituus tulee miettiä ja testata tarkkaan ennen PKI:n rakentamista. Tässä työssä on käytetty suositeltuja avaimenpituuksia.

CA:n yksityinen avain täytyy suojata. Jos avain tallennetaan normaalisti järjestelmään, paikalliset ylläpitäjät pääsevät kopioimaan avaimen järjestelmästä ja voivat näin luoda uuden CA:n, joka jakaa valesertifikaatteja. Myös mahdolliset hyökkäykset CA:ta vastaan saattavat paljastaa avaimen. Avain voidaan tallentaa myös esim. toimikortille (Smart Card). Tällöin vaarana on, että kortti häviää tai varastetaan. Sama tilanne on myös, jos avain on tallennettu virtuaalikoneeseen; kiintolevy tai CD, jossa avain sijaitsee voidaan myös varastaa. Varmin turva saadaan HSM-moduulilla, mutta tämä on kallein ratkaisu. HSM-moduulista ei avaimia saa urkituksi; myöskin mahdolliset fyysiset murtautumisyritykset moduuliin aiheuttavat avaimien tuhoutumisen. Avaimen turvaamisen lisäksi turvaa lisää CA:n poistaminen verkosta (offline). Tämä tehdään muille CA-koneille, paitsi CA:lle, joka jakaa sertifikaatteja asiakkaille. Tässä työssä juuri-CA ja käytäntö-CA on poistettu verkosta, mutta HSM-laitetta ei ole käytetty, joten avaimet tallennetaan kiintolevylle.

Seuraavaksi mietitään julkaisupisteet sulkulistalle ja CA:n julkisille avaimille. Julkaisuun voidaan käyttää protokollia: HTTP, LDAP, FTP ja SMB (tiedostojen jako) kuten jo aikaisemmin käytiin läpi. LDAP- ja HTTP-protokollat ovat käytetyimmät. LDAP-protokollaa käytetään aktiivihakemistoympäristössä (sisäinen käyttö), kun tiedot julkaistaan aktiivihakemistosta. HTTP-protokollaa käytetään, jos yhteys halutaan selaimella (ulkoinen käyttö). Tällöin tiedot julkaistaan www-palvelimelta. Myös vikasietoisuus tulee ottaa huomioon. Aktiivihakemistoympäristössä on yleensä vähintään kaksi ohjauskonetta, jolloin tiedot on ”kahdennettu” automaattisesti. Myös www-palvelimia tulee asentaa vähintään kaksi. Tällöin yhteydenotot ohjataan dns-palvelimen round-robin-asetuksella molemmille palvelimille vuorotellen kuorman tasaamiseksi. Täs-

sä työssä julkaisu tapahtuu aktiivihakemistoon sekä www-palvelimelle. Itse www- ja dns-palvelimen asennusta ja konfiguroimista toimintakuntoon ei käydä läpi.

Windows Server 2008 -CA:n asennus tapahtuu hyvin pitkälti samalla tavalla kuin Windows Server 2003 -ympäristössäkin. Samat hierarkia- ja tietoturva-asiat tulee ottaa huomioon molemmissa ympäristöissä. Asennusrutiinit ovat pitkälti samat. CA:n asennuksen yhteydessä määritellään, tuleeko ympäristöstä yhteensopiva aiempien ympäristöjen kanssa vai asennetaanko puhtaasti uusi Suite B -yhteensopiva ympäristö. Jotta uudet ominaisuudet saadaan hyödynnetyksi, tulee ympäristöstä tehdä täysin Suite B -yhteensopiva. Käytännössä tämä tarkoittaa silloin, että vanha ja uusi järjestelmä eivät ole yhteensopivia keskenään. Jos molemmat järjestelmät halutaan pitää yllä, asennetaan uusi järjestelmä vanhan rinnalle ja tehdään järjestelmien välille ristiinsertifiointi.

Kun PKI-ympäristö on yksi Windows Server 2003 tai 2008 -toimialue, ei erityisiä valmisteluja toimialueeseen tarvita. Toimialueen sekä dns-domainin nimenä käytetään rnko.fi-nimeä.

Seuraavaksi kuvatun asennusvaiheen tarkoitus on selvittää asennuksen eri vaiheet organisaation oman järjestelmän jokaisella kolmella tasolla sekä vaiheiden monimutkaisuutta ja vaikeustasoa.

17 JUURI-CA:N ASENTAMINEN

PKI:n asentaminen aloitetaan juuri-CA:n asennuksesta. Seuraavat asiat on määritelty ennen asennusta:

- Palvelimen aika ja päivämäärä ovat oikein.
- Käyttöjärjestelmä on asennettu C-asemalle.
- Tietokanta ja log-tiedostot asennetaan D-asemalle.
- CA:n tyyppi: Standalone Root CA.
- CA:n nimi: RNKO Root CA.
- CA:n koneen nimi: RootCAsrv.
- CA:n sertifikaatti on myönnetty itse.
- CA:n sertifikaatin voimassaoloaika: 20 vuotta.
- CA:n sertifikaatin avaimen pituus: 4096 bittiä.
- Sulkulistat julkaistaan puolen vuoden välein.

- Lisäsulkulistoja ei julkaista.
- CA:n sertifikaatti ei sisällä CDP- ja AIA-laajennoksia, joten sertifikaatin voimassaoloa ei voida tarkastaa (itsemyönnettyjen sertifikaattien kohdalla toimitaan näin).

Kun CDP- ja AIA-laajennoksia (sulkulista ja CA:n sertifikaatti) ei julkaista sertifikaatissa, juuri-CA:n avainten paljastuessa joudutaan koko hierarkian sertifikaatit myöntämään uudelleen. Ei riitä, että pelkästään juuri-CA:n sertifikaatti uusitaan. Edellä mainittuja polkuja ei ole suositeltavaakaan julkaista juuri-CA:n sertifikaatissa, koska jos sertifikaatti paljastuu, laitettaisiin se tämän jälkeen sulkulistalle ja allekirjoitusta varten ei olisi olemassa käyttökelpoista sertifikaattia (paljastuneella avaimella ei voida suorittaa allekirjoitusta).

Seuraavaksi jatketaan varsinaisella asennuksella.

17.1 Asennus työryhmään

Organisaation juuri-CA asennetaan työryhmän jäseneksi, koska se on kytketty irti verkosta ja näin ollen sillä ei ole yhteyttä toimialueen ohjauskoneeseen. Koneen nimeksi tulee valita sopiva nimi, jota ei käytetä muissa koneissa. Tämä siitä syystä, että nimi julkaistaan myöhemmin aktiivihakemistossa. Määritetään siis tässä vaiheessa koneen nimi ja työryhmä, koska myöhemmin niitä ei voi enää muuttaa. Määritys tapahtuu ohjauspaneelin System-kuvakkeen takaa Computer Name -välilehdellä, jos muutos tehdään käyttöjärjestelmän asennuksen jälkeen. Asennuksen tai määrityksen jälkeen kannattaa tehdä tarkastus **net config workstation** -komennolla.

```
C:\>net config workstation
Computer name                \\ROOTCASRV
Full Computer name           RootCAsrv
User name                    Administrator

Workstation active on
        NetbiosSmb (000000000000)
        NetBT_Tcpip_{F940F1B4-6593-446F-BEDA-79CE45619F54}
(0003FFEC97F6)

Software version             Microsoft Windows Server 2003
```

Workstation domain WORKGROUP
Logon domain ROOTCASRV

COM Open Timeout (sec) 0
COM Send Count (byte) 16
COM Send Timeout (msec) 250
The command completed successfully.

Listauksesta tulee tarkastaa, että logon domain ja palvelimen nimi ovat samat. [3, s. 62.]

17.2 CAPolicy.inf-tiedosto

Yleensä juuri-CA myöntää sertifikaatin itselleen. Juuri-CA sijaitsee itse hierarkian ylimmällä tasolla ja näin ollen juuri-CA ei voi periä sertifikaatilleen ominaisuuksia ylemmältä tasolta, kuten sertifikaatit normaalisti tekevät. Juuri-CA:n sertifikaatin ominaisuudet määritellään CAPolicy.inf-tiedostossa, josta ne tulevat voimaan. Siis tämä tiedosto on konfiguroitava ennen kuin sertifikaatti luodaan. Tämä on ehdottomasti tehtävä, koska muussa tapauksessa myöhemmin asiakkaille myönnettävät sertifikaatit määritellään väärin, lähinnä CRL- ja AIA-polut, jotka kertovat sulkulistan ja CA:n tiedot, tulevat myönnettyihin sertifikaatteihin väärin. CAPolicy.inf-tiedosto tallennetaan Windows-käyttöjärjestelmän asennushakemistoon, joka tunnetaan %Systemroot%-hakemistona. Hakemisto voidaan määritellä myös vaihtoehtoisesti nimellä %Windir%. Huomioitavaa on, että tehtävässä tarvitaan Administrator-tason oikeudet. Asennuksen ehtojen mukaan CAPolicy.inf on seuraavanlainen: [1, s. 114; 3, s. 63.]

[Version]
Signature= "$Windows NT$"
[Certsrv_Server]
RenewalKeyLength=4096
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=20
[CRLDistributionPoint]
[AuthorityInformationAccess] [1, s. 114; 3, s. 140.]

Version-otsikon alla määritellään tiedostomuodoksi Windows NT -formaatti. Avain on 4096-bittinen, voimassa 20 vuotta. CRLDistributionPoint- ja Autho-

rityInformationAccess-otsakkeet jätetään tyhjiksi, koska sulkulista ja palvelimen tiedot julkaistaan aktiivihakemistossa myöhemmin. Kun nämä kohdat jätetään tyhjiksi, ei alemman tason CA tarkasta juuri-CA:n sertifikaatin luotettavuutta kuten aiemmin mainittiin. Alemman tason CA luottaa juuri-CA:han, kun tämän sertifikaatti ja sulkulista on julkaistu alemman tason CA:n trusted root CA store -säiliössä. CAPolicy.inf-tiedostoa ei poisteta asennuksen jälkeen, vaan se tulee jättää paikoilleen. Tämä siitä syystä, että myöhemmin sertifikaatin uusinnassa parametrien, kuten esimerkiksi avaimen pituus, tulee olla samat. CA:n asennuksen ja sertifikaatin luonnin jälkeen kannattaa asennus tarkastaa. Tämä tapahtuu katsomalla %systemroot%**Certocm.log**-tiedostoa. Asennuksessa ei välttämättä tule virheilmoitusta, jos CAPolicy.inf-tiedosto on määritelty väärin, joten asennuksen tarkastus on suotavaa. CAPolicy.inf-tiedosto voidaan tehdä esimerkiksi Muistiolla. Edellä mainitut asetukset kirjoitetaan tai kopioidaan Muistioon. Tiedosto tallennetaan %systemroot%-hakemistoon nimellä CAPolicy.inf. [1, s. 114; 3, s. 63-64.]

Jos lisäksi halutaan ottaa käyttöön Suite B:n mukaiset CNG-algoritmit tiivisteiden muodostukseen sekä sertifikaattien allekirjoitukseen, lisätään vielä DiscreteSignatureAlgorithm-käsky saman otsikon alle. Alla on näkyvissä käskyt täydellisessä muodossaan:

```
[Certsrv_Server]
DiscreteSignatureAlgorithm = 1
```

Suite B tuo mukanaan uusia algoritmeja tiivisteiden ja allekirjoitusten muodostamiseen. Nämä diskreetit allekirjoitusalgoritmit tulee esitellä, jotta osapuolet osaavat tulkita uusia algoritmeja. Tätä uutta algoritmia käytetään tässä tapauksessa, kun juuri-CA allekirjoittaa käytäntö-CA:n sertifikaatin. [6, s.122.]

17.3 Juuri-CA:n asennus ja sertifikaatin luonti

Juuri-CA-koneeseen kirjaudutaan Administrator-oikeudet omaavalla tunnuksella. Tästä tunnuksesta tulee **CA Administrator** asennuksen yhteydessä; oikeudet voidaan tarvittaessa myöhemmin delegoida toiselle käyttäjätunnukselle. Koneen aika ja päiväys kannattaa tarkastaa ennen asennusta. Seuraavaksi lisätään Certificate Services -komponentti. Tämä tapahtuu WindowsServer 2003 -palvelimessa ohjauspaneelissa:

- Valitaan Start > Settings > Control Panel.
- Valitaan edelleen Add or Remove Programs.
- Valitaan Add/Remove Windows Components.
- Rastitetaan kohta Certificate Services.

Jos koneeseen halutaan asentaa www-palvelin, jatketaan seuraavilla valinnoilla. Muussa tapauksessa painetaan Next-painiketta.

- Valitaan Application Server ja painetaan Details-painiketta.
- Valitaan Internet Information Services (IIS) ja painetaan Details-painiketta.
- Valitaan World Wide Web services ja painetaan Details-painiketta.
- Rastitetaan kohdat Active Server Pages ja World Wide Web services.
- OK-painikkeella palataan takaisin edelliseen ikkunaan, josta tarkastetaan että Common Files- ja Internet Information Services Manager -valinnat on valittu automaattisesti.
- Painetaan edelleen OK-painiketta ja tarkastetaan ikkunasta, että Enable network COM+ access -valinta on valittu automaattisesti.
- Lopuksi painetaan OK- ja Next-painiketta. [3, s. 65.]

Windows Server 2008 -palvelimessa Certificate Services -komponentti lisätään Administrative Tools -valikon Server Managerin kautta lisäämällä rooli. Roles Summary -kohdasta valitaan Add Roles. Select Server Roles -sivulla valitaan Active Directory Certificate Services -valintaruutu.

Huomattakoon, että normaalisti www-palvelinta ei asenneta juuri-CA-koneeseen; normaalisti yksitasoisessa mallissa asennus tehdään. Tietoturvan takia ei ole suotavaa asentaa koneeseen muita palveluita (Windows komponentteja). IIS-palvelin kannattaa myös jättää asentamatta, jos sitä ei tarvita; Windows Server 2003- ja Server 2008 -ympäristöissä offline-sertifikaatit voidaan anoa Certification Authority -työkalulla, mikä ei ollut mahdollista Windows 2000 -ympäristössä.

Kannattaa huomioida, että tämän jälkeen ei voida enää vaihtaa koneen nimeä eikä työryhmää. Tästä syystä koneen nimi ja työryhmä tarkastettiin aiemmin.

Windows Server 2003 -CA:n asennus jatkuu CA Type -sivulta, jossa valitaan **Stand-alone root CA**; lisäksi laitetaan rasti **Use custom settings to gene-**

rate the key pair and CA certificate. Public and Private Key Pair -sivulla tehdään seuraavat valinnat:

- CSP: Microsoft Strong Cryptographic Service Provider
- Allow the CSP to interact with the desktop: Ei valita!
- Hash algorithm: SHA-1
- Key length: 4096.

Siinä tapauksessa, että HSM-laite on asennettu järjestelmään, valitaan CSP-kohdassa se CSP, joka asennettiin HSM-laitteen yhteydessä. Lisäksi pitää valita **Allow this CSP to interact with the desktop**. Jos HSM-laitetta ei ole asennettu, edellinen asetus ja **Use an existing key** -asetus jätetään tyhjiksi.

CA Identifying Information -sivulla tehdään seuraavat valinnat:

- Common Name for this CA: RNKO Root CA
- Distinguished name suffix: O=RNKO,C=FI
- Validity Period: 20 Years.

Common name for this CA on nimi, jolla CA tunnetaan. Distinguished name suffix on aktiivihakemistonimeä vastaava LDAP-nimi. Tämän asetuksen voi myöhemminkin tehdä Certutil-ohjelmalla. Validity period on CA:n sertifikaatin voimassaoloaika. Jos koneeseen on jossakin vaiheessa jo asennettu Certificate Services -palvelu sekä myös poistettu tämä asennus, tulee ilmoitus, halutaanko aikaisemman asennuksen yksityinen avain kirjoittaa yli. Jos avainta ei tarvita tai sen on varmuuskopioitu, voidaan hyväksyä ylikirjoitus. Jos halutaan suorittaa varmuuskopiointi ja keskeyttää asennus, ei hyväksytä ylikirjoitusta.

Seuraavaksi asennuksessa CSP luo julkisen ja yksityisen avaimen. Avaimet tallennetaan system-tilin profiiliin, jos HSM-laitetta ei ole asennettu. Jos laite on asennettu, tallentuvat avaimet kyseiseen laitteeseen. Sertifikaatti valmistetaan rekisteriasetusten pohjalta, koska kone ei kuulu aktiivihakemistoympäristöön eivätkä näin ollen sertifikaattipohjat ole käytössä. Seuraavat laajennokset (key usage extensions) määritellään sertifikaattiin eri allekirjoituksia varten:

- Digital signature (Digitaalinen allekirjoitus)
- Certificate signing (Sertifikaatin allekirjoitus)

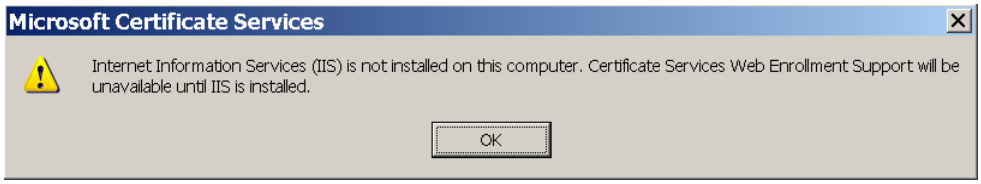
- Certificate offline CRL signing (Offline sulkulistan allekirjoitus)
- Certificate CRL signing (Sulkulistan allekirjoitus).

Jos kone olisi liitetty toimialueeseen, laajennokset periytyisivät aktiivihakemiston CA-pohjasta (CA template).

Certificate database Settings -sivun asetukset määrittävät, minne tietokanta ja log-tiedosto tallennetaan. Tallennuksen tulee tapahtua paikalliselle NTFS-levylle seuraavasti:

- Certificate database: D:\CertDB
- Certificate database log: D:\CertLog
- CA configuration: D:\CAConfig.

Jos Certificate Services on asennettu jo aikaisemmin ja nyt esim. palautetaan asennus varmuuskopiosta, *Preserve existing certificate database* -kohta rastittamalla voidaan määrittää asennus käyttämään jo olemassa olevaa tietokantaa. Ilman rastia mahdollinen jo olemassa oleva tietokanta tuhoutuu. Logit ja tietokanta on myös mahdollista siirtää toiseen paikkaan. *Store configuration information in a shared folder* -kohdassa määritellään paikka, josta konfiguraatiot jaetaan asiakkaille. Tässä tapauksessa, kun CA toimii offline-tilassa, asetuksella ei ole merkitystä, mutta se pitää kuitenkin määritellä. Oletusmääritys on C:\CAConfig, joka muutetaan arvoksi D:\CAConfig alkumäärityksien mukaan. Polku voitaisiin antaa myös UNC-nimenä, esim. \\Localhost\CAConfig. Jos palvelimeen ei ole asennettu verkkokorttia, annetaan polku paikallisesti, ei UNC-nimenä. Asennus pyytää mahdollisesti tässä vaiheessa asennusmedian, normaalisti CD-levyn jatkaakseen asennusta, joten media tulee varata käyttöön jo ennen asennuksen aloitusta. Jos IIS-palvelinta ei asenneta, kuten tässä tapauksessa ei tarvitse tehdä, tulee ilmoitus:



Kuva 27. IIS ei käytettävissä -ilmoitus

Sertifikaatteja ei siis voi anoa web-selaimella juuri-CA-palvelimelta. Tämän jälkeen sertifikaattipalvelun asennus on valmis. [1, s. 121-122; 3, s. 64-68.]

Windows Server 2008 CA:n Certificate Services -asennus jatkuu seuraavasti:

- Select Role Services -sivulla valitaan Certificatin Authority -valintaruutu.
- Specify Setup Type -sivulla valitaan Standalone.
- Specify CA Type -sivulla valitaan Root CA -valinta.
- Set up Private Key -sivulla valitaan Create A New Private Key.

Configure Cryptography For CA -sivulla tehdään seuraavat valinnat:

- Select a cryptographic service provicer (CSP): RSA#Microsoft Software Key Storage Provider
- Key character length: 2048
- Select the hash algorithm for signing certificates issued by this CA: sha256.

Configure CA Name -sivulla tehdään seuraavat valinnat:

- Common name for this CA: RNKO Root CA
- Distinguished name suffix: O=RNKO,C=FI.

Set Validity Period -sivulla vaihdetaan voimassaoloaika 20 vuodeksi (20 years) ja Configure Certificate Database -sivulla valitaan:

- Certificate database: D:\CertDB
- Certificate database log: D\CertLog.

Confirm Installation Selections -sivulla valitaan Install-painike tietojen tarkastamisen jälkeen. Lopuksi tulee Installation Results -sivu, josta valitaan Close, kun ollaan varmistuttu asennuksen onnistumisesta. [6, s. 123-124.]

17.4 Juuri-CA:n sertifikaatin tarkastus

Sertifikaattipalvelun asennuksen ja sertifikaatin luonnin jälkeen kannattaa syntynyt sertifikaatti tarkastaa certutil-komennoilla:

certutil -ca.cert RNKOCA01.cer

Tällä komennolla nähdään siis itse sertifikaatti.

Seuraavalla komennolla voi tarkastaa asennuksessa annetut tiedot:

certutil RNKOCA01.cer

Kannattaa tarkistaa varsinkin että, sertifikaatin voimassaoloaika on 20 vuotta:

Signature Algorithm:
Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
Algorithm Parameters:
05 00
Issuer:
CN= RNKOCA01
DC=RNKO
DC=FI

NotBefore: 29.12.2008 17:26
NotAfter: 29.12.2028 17:26

CA:n konfiguraation voi tarkasta komennolla:

certutil -cainfo

Listauksesta kannattaa tarkastaa lähinnä CA:n tyyppi, jonka tulee olla Standalone Root CA:

CA type: 3 -- Stand-alone Root CA
ENUM_STANDALONE_ROOTCA -- 3

Tietokannan ja logien sijainnin voi tarkastaa komennolla:

certutil -getreg | find /I "Directory"

Listauksesta näkyy polut:

ConfigurationDirectory REG_SZ = \\rnkoca01\CertConfig
DBDirectory REG_SZ = D:\CertDB
DBLogDirectory REG_SZ = D:\CertLog
DBTempDirectory REG_SZ = D:\CertLog
DBSystemDirectory REG_SZ = D:\CertLog

Edellisillä komennoilla voitiin tarkastaa juuri-CA:n sertifikaatti. Kun juuri-CA on kunnossa, voidaan määritellä asetuksia, jotka tulevat voimaan asiakkaille, joille juuri-CA myöntää sertifikaatit. Asetukset perustuvat seuraaviin tietoihin:

- Kaikki asiakkaat ja palvelimet ovat Windows Server 2003/2008- tai Windows XP/Vista/7 -koneita ja ne kuuluvat rnko.fi-toimialueeseen.
- WWW-palvelin, jossa sulkulistat ja sertifikaatit julkaistaan, on nimeltään www.rnko.fi. Palvelimelle on määritelty virtuaalihakemisto nimeltään PKI, josta julkaisu tapahtuu. Palvelin näkyy sekä sisäisille että ulkopuolisille asiakkaille.
- Juuri-CA:n alapuolella olevan käytäntö-CA:n sertifikaatti on voimassa 10 vuotta. Toisin sanoen juuri-CA myöntää sertifikaatin, joka on voimassa 10 vuotta.
- Juuri-CA:n sertifikaatti ja sulkulistat kopioidaan siirrettävälle medialle, josta ne voidaan julkaista aktiivihakemistossa. [3, s. 68-69.]

17.5 Aktiivihakemiston nimiavaruuden määrittäminen juuri-CA:n rekisteriin

Seuraavaksi määritellään asetukset, jotka tulevat myönnettävien sertifikaattien mukana asiakkaille. Asiakkaita voivat olla seuraavan tason CA:t tai loppuasiakkaat kuten koneet ja käyttäjät. Nämä asetukset tulee tehdä erittäin huolella, koska ne vaikuttavat loppuasiakkaiden sertifikaattien toimintaan.

Juuri-CA ei ole toimialueen jäsen, joten se ei voi tässä vaiheessa julkaista sulkulistaa eikä CA:n sertifikaattia aktiivihakemistoon. Asetukset julkaistaan myöhemmin aktiivihakemistossa, joten aktiivihakemiston julkaisupaikka määritellään tässä vaiheessa rekisteriin:

certutil -setreg ca\DSConfigDN CN=Configuration,DC=rnko,DC=fi

CN=Configuration,DC=rnk,DC=fi on juuritoimialueen (root domain) LDAP-nimi. Asetus kertoo Configuration-säiliön (container) sijainnin aktiivihakemistossa. Sertifikaattipalvelu on käynnistettävä uudelleen rekisterimuutoksen jälkeen esim. komentokehotteessa komennoilla **net stop CertSvc** ja **net start CertSvc** tai yhdellä komennolla **net stop CertSvc & net start CertSvc**. Jos juuri-CA on myöntänyt sertifikaatteja tai julkaissut sulkulistan jo aikaisemmin, täytyy toimenpiteet suorittaa uudelleen tämän rekisterimuutoksen jälkeen! Tämähän ei ole tarpeellista juuri nyt, kun juuri-CA asennetaan parhaillaan. [3, s. 69-70.]

17.6 Juuri-CA:n sulkulistan jakelupisteen määrittäminen

CRL-laajennos tulee kaikkiin juuri-CA:n myöntämiin sertifikaatteihin, joten se on erittäin kriittinen asetus sertifikaattien toiminnan kannalta. Asetus mahdollistaa sulkulistan tarkastamisen. Ennen sulkulistan muuttamista kannattaa voimassa olevat asetukset tarkastaa, jotta ne voi tarvittaessa palauttaa.

certutil -getreg ca\CRLPublicationURLs

Komennon antama listaus kannattaa ottaa muistiin.

C:\>certutil -getreg ca\CRLPublicationURLs

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\RNKO Root CA\CRLPublicationURLs:

CRLPublicationURLs REG_MULTI_SZ =
0: 65:C:\WINDOWS\system32\CertSrv\CertEnroll\%3%8%9.crl
CSURL_SERVERPUBLISH -- 1
CSURL_SERVERPUBLISHDELTA -- 40 (64)

1: 8:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10
CSURL_ADDTOCRLCDP -- 8

2: 6:http://%1/CertEnroll/%3%8%9.crl
CSURL_ADDTOCERTCDP -- 2
CSURL_ADDTOFRESHESTCRL -- 4

3: 6:file://\\%1\CertEnroll\%3%8%9.crl
CSURL_ADDTOCERTCDP -- 2
CSURL_ADDTOFRESHESTCRL -- 4

CertUtil: -getreg command completed successfully.

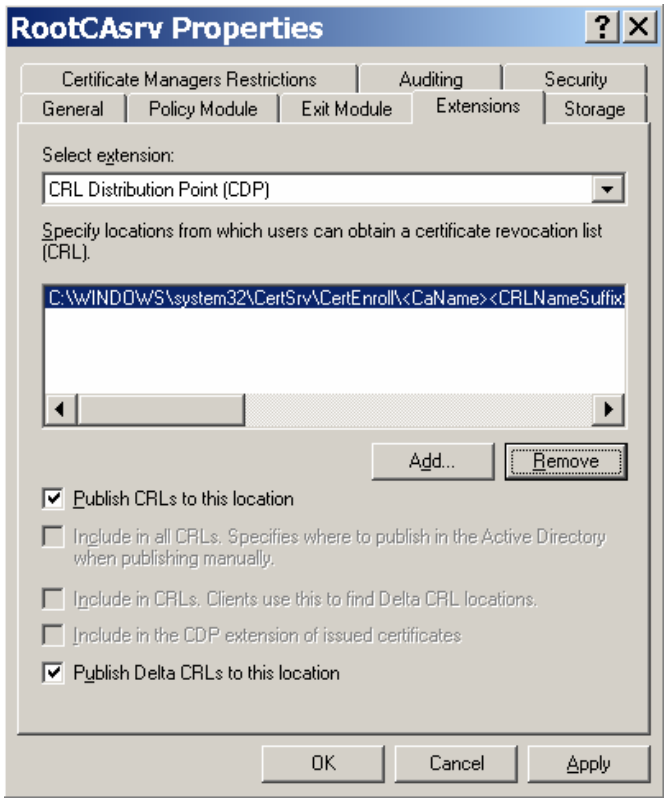
Listauksessa näkyy ensimmäisellä rivillä rekisteriavain, jossa polut on määritelty. Tämä avain kannattaa varmuuskopioida. Listassa olevat %-muuttujat on esitelty liitteessä 3. Seuraavaksi polut määritellään uudelleen Certification Authority -työkalulla. Työkalu löytyy Administrative Tools -valikosta. Työkalussa valitaan juuri-CA aktiiviseksi ja tämän jälkeen valitaan valikosta Action

ja sieltä Properties ja edelleen Extensions-välilehti. Välilehdeltä poistetaan kaikki muut polut listasta, paitsi paikallinen polku. Paikallinen polku jakelupisteeseen on säilytettävä, koska se on ainoa, jota offline-tilassa oleva sertifikaattipalvelin voi käyttää. Polku on seuraavanlainen:

C:\Windows\System32\CertSrv\CertEnroll\RNKOCA01.crl

Tämä jakelupiste ei tule myönnettävien sertifikaattien laajennokseen, siis tämä polku on vain juuri-CA:ta varten, sitä ei ilmoiteta asiakkaille. Polkujen poistamiseksi Extensions-välilehdellä Select extension -kohdassa valitaan CRL Distribution Point (CDP). Specify location from which users can obtain a certificate revocation list (CRL) -kohdassa valitaan LDAP-polku, napsautetaan Remove ja lopuksi valitaan Yes. Tämä toistetaan kaikille muille, paitsi paikalliselle jakelupisteelle.

Kuva 28 näyttää ikkuna näkymän poistojen jälkeen.



Kuva 28. Sulkulistan jakelupisteen polkujen lisääminen

Seuraavaksi lisätään seuraavan taulukon (taulukko 4) mukaiset http- ja ldap-polut.

Taulukko 4. Sulkulistan julkaisupisteet

PROTOKOLLA (ACCESS PROTOCOL)	**SULKULISTAN JULKAISUPISTE (CRL DISTRIBUTION POINT)**
PAIKALLINEN	C:\WINDOWS\SYSTEM32\CERTSRV\CERTENROLL\%3%8.CRL
HTTP	HTTP://WWW.RNKO.FI/PKI/%3%8.CRL
LDAP	LDAP://LDAPSRV/CN=%7%8,CN=%2,CN=CDP,CN=PUBLIC KEY SERVICES,CN=SERVICES,%6%10

Lisääminen tapahtuu valitsemalla kuvan ikkunassa Add-painike ja kirjoittamalla polku ja painamalla Insert. Polussa voidaan käyttää avuksi liitteen 3 muuttujia. LDAPSRV on LDAP-palvelimen nimi. Lopuksi painetaan OK ja toimenpide toistetaan seuraavalle julkaisupisteelle. Tämän jälkeen aktivoidaan ikkunasta paikallinen polku ja varmistetaan että, vain Publish CRLs to this location -kohdassa on rasti. Valitaan seuraavaksi http-polku ja varmistetaan, että vain Include in the CDP extension of issued certificates -kohdassa on rasti. Viimeiseksi valitaan LDAP-polku ja varmistetaan, että Include in the CDP extension of issued certificates ja Include in all CRLs -kohdissa on rasti. Seuraavassa taulukossa (taulukko 5) on koottuna edellä mainitut valinnat.

Taulukko 5. Sulkulistan polkujen määritykset

SULKULISTAN JULKAISUPOLUN MÄÄRITYS	**FILE**	**HTTP**	**LDAP**
PUBLISH CRLS TO THIS LOCATION SULKULISTA JULKAISTAAN TÄSTÄ PISTEESTÄ AUTOMAATTISESTI	✓		
INCLUDE IN ALL CRLS MÄÄRITTÄÄ SIJAINNIN, KUN JULKAISTAAN MANUAALISESTI AKTIIVIHAKEMISTOSSA			✓
INCLUDE IN CRLS ASIAKKAAT LÖYTÄVÄT LISÄSULKULISTAN (DELTA CRL) TÄÄLTÄ			
INCLUDE IN THE CDP EXTENSION OF ISSUED CERTIFICATES POLKU JULKAISTAAN MYÖNNETTÄVIIN SERTIFIKAATTEIHIN		✓	✓
PUBLISH DELTA CRLS TO THIS LOCATION LISÄSULKULISTA JULKAISTAAN TÄSTÄ PISTEESTÄ			
INCLUDE IN THE IDP EXTENSION OF ISSUED CRLS EI-WINDOWS -ASIAKKAILLE VOIDAAN KERTOA SULKULISTAN TYYPPI (ESIM. KONE- JA KÄYTTÄJÄSERTIFIKAATIT)			

Publish CRLs to this location -valintaa ei voi valita LDAP-polkuun, koska juuri-CA ei ole kytketty verkkoon ja näin ollen se ei voi automaattisesti julkaista

sulkulistaa aktiivihakemistoon. Sama pätee myös Publish Delta CRLs to this location -valintaan; juuri-CA-palvelimestahan ei edes julkaista lisäsulkulistaa. Lopuksi painetaan Apply-painiketta ja saadaan ilmoitus, että palvelu pitää käynnistää uudelleen. Tähän ilmoitukseen vastataan No. Ikkuna jätetään auki ja palvelun uudelleenkäynnistys tehdään vasta seuraavan kohdan jälkeen. [3, s. 70-75.]

17.7 Juuri-CA:n sertifikaatin jakelupisteen konfigurointi

Nämä asetukset ovat edellisten tavoin kriittisiä sertifikaattien toiminnan kannalta. Määrityksiä jatketaan edellisestä kohdasta Extensions-välilehdellä. Valitaan Authority Information Access (AIA) kohdassa Select Extension. Specify locations from which users can obtain the certificate for this CA -ikkunassa poistetaan kaikki muut polut, paitsi paikallinen polku samalla tavalla kuin aikaisemmin. Tämän jälkeen lisätään polut taulukon 6 mukaan.

Taulukko 6. CA:n sertifikaatin julkaisupisteen polut

PROTOKOLLA (ACCESS PROTOCOL)	**CA:N SERTIFIKAATIN JULKAISUPISTE (AIA DISTRIBUTION POINT)**
PAIKALLINEN	C:\WINDOWS\SYSTEM32\CERTSRV\CERTENROLL\%1_%3%4.CRT
HTTP	HTTP://WWW.RNKO.FI/PKI/%1_%3%4.CRT
LDAP	LDAP://LDAPSRV/CN=%7,CN=AIA,CN=PUBLIC KEY SERVICES,CN=SERVICES,%6%11

LDAPSRV on LDAP-palvelimen nimi. Seuraavaksi määritellään ikkunan alalaidassa olevat ominaisuudet poluille seuraavana olevan taulukon mukaan.

Taulukko 7. CA:n sertifikaatin julkaisupisteen polkujen määritykset

SERTIFIKAATIN JULKAISUPOLUN MÄÄRITYS	FILE	HTTP	LDAP
INCLUDE IN THE AIA EXTENSION OF ISSUED CERTIFICATES POLKU LISÄTÄÄN SERTIFIKAATTIEN AIA-LAAJENNOKSIIN.		✓	✓
INCLUDE IN THE ONLINE CERTIFICATE STATUS PROTOCOL (OCSP) EXTENSION OCSP-LAAJENNOKSEN KÄYTTÖ.			

OCSP-laajennoksia voidaan käyttää suoraan Windows Server 2008 -ympäristössä, jossa kyseiset laajennokset ovat käytössä suoraan ilman lisäosien asennusta. Windows Server 2003 -ympäristössä vaaditaan erillisten lisäosien asennus. Laajennokset mahdollistavat reaaliaikaisen sertifikaattien tarkastuksen OCSP-palvelimelta.

Lopuksi painetaan OK ja vastataan uudelleenkäynnistykseen Yes. Tarkistetaan vielä komentokehotteesta, että CRL-julkaisupisteet ovat muuttuneet:

certutil -getreg ca\CRLPublicationURLs

Sekä myös CA:n sertifikaatin julkaisupisteen polku:

certutil -getreg ca\CACertPublicationURLs

Julkaisupisteet voidaan muuttaa vaihtoehtoisesti koneen rekisteriin myös suoraan komentokehotteessa certutil-komennolla ilman graafista käyttöliittymää. Seuraava komento muuttaa sulkulistan polun:

certutil -setreg CA\CRLPublicationURLs
"1:%WINDIR%\system32\CertSrv\CertEnroll\%3%8%9.crl\n
8:http://www.rnko.fi/pki/%3%8%9.crl\n10:LDAP:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10"

Seuraava komento muuttaa CA:n sertifikaatin julkaisupolun:

certutil -setreg CA\CACertPublicationURLs
"1:%WINDIR%\system32\CertSrv\CertEnroll\%1_%3%4.crt\n

2:LDAP:///CN=%7,CN=AIA,CN=Public Key Servces,CN=Services,
%6%11\n2:http://www.rnko.fi/pki/%1_%3%4.crt"

Komentojen poluissa on ennen polkua annettu numeroarvo. Esimerkiksi sulkulistan http-polun alussa on numero 2 ja ldap-polun alussa on numero 10. Näillä numeroarvoilla voidaan tehdä poluille samat määritykset, jotka tehtiin Certification Authority -työkalulla aiemmin. Numero 2 http-polun edessä siis tarkoittaa samaa kuin *include in the cdp extension of issued certificates* Certification Authority -työkalun Extensions-välilehdellä. Numero 10 ldap-polun edessä tarkoittaa arvoja *Include in all CRLs* ja *Include in the CDP extension of issued certificates*. *Include in all CRLs -määritys vastaa arvoa 8 ja Include in the CDP extension of issued certificates* -määritys vastaa arvoa 2. Kun nämä arvot lasketaan yhteen, saadaan tulokseksi 10. Taulukko 8 sisältää sulkulistan julkaisupolun määrityksiä vastaavat arvot ja taulukko 9 näyttää sertifikaatin julkaisupolun määrityksiä vastaavat arvot.

Taulukko 8. CA:n sertifikaatin julkaisupisteen polkujen määritysten numeroarvot

SULKULISTAN POLUN MÄÄRITYS	**NUMERO-ARVO**
PUBLISH CRLS TO THIS LOCATION	1
INCLUDE IN ALL CRLS	2
INCLUDE IN CRLS	4
INCLUDE IN THE CDP EXTENSION OF ISSUED CERTIFICATES	8
PUBLISH DELTA CRLS TO THIS LOCATION	64
INCLUDE IN THE IDP EXTENSION OF ISSUED CRLS	128

Taulukko 9. CA:n sertifikaatin julkaisupisteen polkujen määritysten numeroarvot

SERTIFIKAATIN POLUN MÄÄRITYS	**NUMERO-ARVO**
AUTOMATICALLY PUBLISH CA CERTIFICATE TO THIS LOCATION	1
INCLUDE IN THE AIA EXTENSION OF ISSUED CERTIFICATES	2
INCLUDE IN THE ONLINE CERTIFICATE STATUS PROTOCOL (OCSP) EXTENSION	4

Jos käskyistä halutaan tehdä komentojono, on %-merkit korvattava %%-merkeillä. Lisäksi huomiota kannattaa kiinnittää \n-merkkiin, joka on loppumerkki muuttujalle (multivalued attribute). Muuttujat siis erotellaan edellisessä esimerkissä \n-merkillä, ei välilyönnillä. Lisäksi kannattaa huomioida, ettei lainausmerkkien sisällä ole yhtään välilyöntiä. Komentojen suoritusten jälkeen tulee Certificate Services -palvelu käynnistää uudelleen. Tämä voidaan tehdä komentokehotteessa antamalla käskyt **net stop CertSvc** ja **net start CertSvc** kuten jo aikaisemminkin todettiin. Luonnollisesti käskyjen jälkeen kannattaa tarkistaa julkaisupisteiden uudet polut edellisen esimerkin mukaan certutil-ohjelmalla. [3, s. 75-77.]

17.8 Juuri-CA:n sulkulistan julkaisuajan määrittäminen

Seuraavaksi määritellään, millaisella jaksotuksella sulkulista julkaistaan. Tässä esimerkissä sulkulista julkaistaan kaksi kertaa vuodessa. Käynnistetään Certification Authority -työkalu Administrative Tools -valikosta. Seuraavaksi aktivoidaan Revoked Certificates -säiliö ja valitaan Action-valikosta Properties-valinta. CRL Publication Interval -kohtaan kirjoitetaan 180 Days ja valitaan OK.

Asetukset voidaan antaa vaihtoehtoisesti myös certutil-ohjelmalla. Suositeltavaa onkin tehdä asetuksista komentojono. Seuraavat komennot kannattaa tallentaa komentojonoksi:

```
certutil -setreg CA\CRLPeriodUnits 180
certutil -setreg CA\CRLPeriod "Days"
certutil -setreg CA\CRLDeltaPeriodUnits 0
net stop certsvc
net start certsvc
```

Komennot kirjoitetaan tai kopioidaan leikepöydän kautta Muistioon ja tallennetaan tiedostoon, jolle annetaan cmd-tarkennin. Suorittamalla komentojono voidaan käskyt suorittaa ja saada kaikki määritykset kerralla tehtyä. [3, s. 80.]

17.9 Myönnettävien sertifikaattien voimassaoloajan konfigurointi

Certutil-ohjelmalla määritetään myönnettäville sertifikaateille voimassaoloaika. Tätä ei pidä sekoittaa juuri-CA:n oman sertifikaatin voimassaoloaikaan, joka määriteltiin asennuksen yhteydessä CAPolicy.inf-tiedostossa. Seuraavat komennot määrittelevät myönnettäville sertifikaateille 10 vuotta voimassaoloaikaa. Palvelu tulee käynnistää uudelleen rekisterimuutoksen jälkeen.

```
certutil -setreg ca\ValidityPeriodUnits 10
certutil -setreg ca\ValidityPeriod "Years"
net stop certsvc & net start certsvc
```

Käskyistä kannattaa tehdä komentojono. [3, s. 81; 6, s. 118.]

17.10 Sulkulistan uudelleenjulkaisu

Koska julkaisupolut ovat muuttuneet, tulee sulkulista julkaista uudelleen. Käynnistetään Certification Authority -työkalu Administrative Tools -valikosta. Aktivoidaan Revoked Certificates -säiliö valitaan Action-valikosta All Tasks ja edelleen Publish. Lisäsulkulistaa ei tässä esimerkissä ole julkaistu, joten se ei ole valittavissa. Lopuksi valitaan OK.

C:\WINDOWS\system32\certsrv\CertEnroll-hakemistoon syntyy uusi sulkulista nimeltä RNKO Root CA.crl. Uudelleenjulkaisu voidaan tehdä vaihtoehtoisesti komentokehotteessa komennolla:

```
certutil -CRL
```

[3, s. 82.]

17.11 Julkaistun sulkulistan varmistaminen

Sulkulistan julkaisupolku nähdään komennolla:

```
certutil -dynamicfilelist
```

Annetaan seuraavaksi certutil-komennon parametriksi edellisen listauksen polku ja sulkulistan nimi:

certutil “C:\WINDOWS\system32\certsrv\CertEnroll\RNKO Root CA.crl”

Komennossa tulee käyttää lainausmerkkejä, koska sulkulistan nimi sisältää välilyöntejä. Varmistetaan seuraavaksi, että julkaisuaika on oikein kohdassa Next Update sekä Published CRL Locations -kohdassa ei lue DC=UnavailableConfigDN. Jos kuitenkin näin käy, niin aikaisemmassa konfiguraatiossa on tullut virhe mahdollisesti certutil -setreg ca\DSConfigDN CN=Configuration,DC=rnko,DC=fi -komennossa. Kyseinen komento siis määritti rekisteriasetuksen, jossa määritellään Configuration-säiliön sijainti aktiivihakemistossa. Mahdollisesti certutil -CRL -komento, jolla määriteltiin sulkulistan uudelleenjulkaiseminen, on jäänyt antamatta tai vastaava toimenpide Certification Authority -työkalulla on jäänyt tekemättä.

Listauksen tulisi olla seuraavanlainen:

Published CRL Locations
    [1]Locations
        Distribution Point Name:
            Full Name:
URL=ldap://LDAPSRV/CN=RNKO%20Root%20CA,CN=rnkoca01,CN=CDP,
CN=Public%20Key%20Services,CN=Services,**CN=Configuration**,
DC=rnko,DC=fi?certificateRevocationList?base?**objectClass=cRLDistributionPoint**

CN-arvojen tulee olla samat kuin certutil -setreg ca\DSConfigDN CN=Configuration,DC=rnko,DC=fi -komennossa annetut. Lisäksi objectClass-komponentti tulee olla oikein määritelty. %20-merkit ovat välilyöntejä.

Juuri-CA:n konfigurointi on hyvin pitkälle mahdollista tehdä pelkästään komentojonona. Komentojono ajetaan CAPolicy.inf-tiedoston luonnin ja Sertificate Services -palvelun asennuksen jälkeen. Vaikka palvelimen asennus käy komentojonolla todella nopeasti, tarkistuskomennot kannattaa joka tapauksessa antaa ja tutkia huolella komentojen antamat listaukset. Seuraavalla komentojonolla voidaan siis konfiguroida palvelin huomattavasti nopeammin kuin se tässä esimerkissä tehtiin. Komentojonoon on lisätty auditointikomento, josta kerrotaan seuraavassa kappaleessa. [3, s. 82-83.]

Komentojono, jolla juuri-CA voidaan asentaa automaattisesti:

REM --- Määritellään LDAP-polku
certutil -setreg CA\DSConfigDN CN=Configuration,DC=rnko,DC=fi

REM --- Määritellään sulkulitan julkaisuajat kaksi kertaa vuodessa---
certutil -setreg CA\CRLPeriodUnits 26
certutil -setreg CA\CRLPeriod “Weeks"
certutil -setreg CA\CRLDeltaPeriodUnits 0
certutil -setreg CA\CRLDeltaPeriod “Days"

REM --- Määritellään sulkulistan julkaisupaikat myönnettävien sertifikaattien CDP-laajennoksiin ---
certutil -setreg CA\CRLPublicationURLs
“1:%windir%\system32\CertSrv\CertEnroll\%%3%%8%%9.crl\n10:ldap:///CN=%%7%%8,CN=%%2,CN=CDP,CN=Public Key Services,CN=Services,%%6%%10\n
8:http://www.rnko.fi/pki/ %%3%%8%%9.crl"

REM --- Määritellään sertifikaattien julkaisupaikat myönnettävien sertifikaattien AIA-laajennoksiin ---
certutil -setreg CA\CACertPublicationURLs
“1:%windir%\system32\CertSrv\CertEnroll\%%1_%%3%%4.crt\n2:ldap:///CN=%%7,CN=AIA,CN=Public Key Services,CN=Services,%%6%%11\n2:http://www.rnko.fi/pki/%%1_%%3%%4.crt"

REM --- Määritellään auditointi-asetuksiin kaikki toiminnot ---
certutil -setreg CA\AuditFilter 127

REM --- Määritellään myönnettävien sertifikaattien voimassaoloaika ---
certutil -setreg CA\ValidityPeriodUnits 10
certutil -setreg CA\ValidityPeriod “Years"

REM --- Käynnistetään Certificate-palvelu uudelleen ---
net stop certsvc & net start certsvc
certutil -crl [1, s. 123; 3, s. 146-148.]

17.12 Auditoinnin määrittäminen

Palvelimen asetusten määrittely vaatii vielä auditoinnin määrittelemisen. Auditoinnilla tarkoitetaan palvelimen tapahtumien kirjaamista loki-tiedostoon myöhempää tarkastelua varten. Auditointi voidaan määritellä Certification Authority -työkalulla CA-palvelimessa. Palvelimen ominaisuuksien Auditing-välilehdellä rastitetaan kaikki tapahtumat. Nopeampi tapa tehdä määritys on tehdä se certutil-työkalulla:

certutil -setreg CA\AuditFilter 127

Tämänkin komennon jälkeen palvelu tulee käynnistää uudelleen, ennen kuin asetukset ovat voimassa. Jotta auditointi toimii, tulee vielä Object Access -asetus määritellä tietoturva-asetuksissa niin, että auditoidaan onnistuneet ja epäonnistuneet toiminnot. Tämä tehdään Administrative Tools -valikon Local Security Policy -työkalulla. Polku on Security Settings\Local Policies\Audit Policy. Samalla kannattaa määritellä myös muut auditoinnit tietoturvamääritysten mukaan:

- Account Logon: Success, Failure
- Account Management: Success, Failure
- Directory Service Access: Failure
- Logon Events: Success, Failure
- **Object Access**: Success, Failure
- Policy Change: Success, Failure
- Privilege Use: Failure
- Process Tracking: No auditing
- System Events: Success, Failure.

CNG tuo mahdollisuuden tallentaa avaimet esim. tietokoneen TPM-piiriin. Avainten eristys ja hallinta tapahtuu uuden rajapinnan kautta; tätä rajapintaa ei tueta Windows Server 2003- tai XP-ympäristöissä. Tämän uuden rajapinnan kautta tapahtuu myös CNG:n auditointi. Jos uusien algoritmien auditointi otetaan käyttöön, annetaan komento:

auditpol /set /subcategory:”other system events” /success:enable /failure:enable

Näiden toimenpiteiden jälkeen juuri-CA on valmis myöntämään sertifikaatteja. Tuotantoympäristöön liittäminen vaatii vielä erinäisiä lisätehtäviä, kuten

tietoturva-asetusten määrittäminen. Näitä määrityksiä ei käydä läpi tässä työssä. [1, s. 123-124; 6, s. 13-17.]

18 KÄYTÄNTÖ-CA:N ASENTAMINEN

18.1 Asetukset

Käytäntö-CA asennetaan seuraavien asetusten mukaan:

- CA:n tyyppi: Standalone Subordinate CA
- CA:n nimi: RNKO Policy CA.
- CA:n koneen nimi: RNKOCA02.
- CA:n sertifikaatin voimassaoloaika: 10 vuotta.
- CA:n sertifikaatin avaimen pituus: 2048 bittiä.
- Sulkulistat julkaistaan puolen vuoden välein.
- Lisäsulkulistoja ei julkaista.
- CPS julkaistaan osoitteessa www.rnko.fi/cps/cps.htm.
- CPS:n OID-tunnus on 1.3.6.1.4.1.311.509.3.1
- Koneessa on kaksi peilattua levyosiota tai asemaa, jotka näkyvät C- ja D-asematunnuksilla. C-asema on käyttöjärjestelmää varten ja D-asema tietokantaa ja loki-tiedostoja varten. [1, s. 125.]

Lisäksi ympäristöön määritellään seuraavat asetukset:

- Kaikki koneet ovat vähintään Windows XP- tai Windows Server 2003 -käyttöjärjestelmällä varustettuja koneita.
- WWW-palvelimen osoite on www.rnko.fi ja palvelimelle on tehty virtuaalihakemisto nimellä pki. Palvelimelle on pääsy sekä ulko- että sisäverkosta.
- Käytäntö-CA:n alapuolella olevien myöntäjä-CA-koneiden sertifikaatit ovat voimassa viisi vuotta.
- Palvelimelle määritellään auditointi, jotta voidaan myöhemmin seurata palvelinkoneen tapahtumia.
- Palvelimen sertifikaatti ja julkaisulista julkaistaan www-palvelimessa (www.rnko.fi/pki). [6, s.130.]

18.2 Asennus työryhmään

Organisaation käytäntö-CA asennetaan työryhmän jäseneksi samalla tavoin kuin tehtiin aikaisemmin juuri-CA:lle. Käytäntö-CA on kytketty irti verkosta eikä silläkään ole yhteyttä domainin ohjauskoneeseen. Edelleen koneen nimeksi tulee valita sopiva nimi, jota ei käytetä muissa koneissa; nimi julkaistaan myöhemmin aktiivihakemistossa. Siis tässä vaiheessa määritetään koneen nimi ja työryhmä, koska myöhemmin niitä ei voi enää muuttaa. Asennuksen jälkeen kannattaa tehdä tarkastus **net config workstation** -komennolla. Koneen nimi sekä logon domain tulee olla samannimiset kuten jo juuri-CA:n asennuksessa todettiin. [3, s. 84.]

18.3 CAPolicy.inf-tiedoston konfigurointi

CAPolicy.inf-tiedosto on määriteltävä myös käytäntö-CA -palvelimella. CPS määritellään tällä tasolla, kun kyse on kolmitasoisesta hierarkiasta. CPS määritellään omalla OID-tunnuksella. CPS siis määrittää, mitä käytännön toimenpiteitä CA suorittaa ja noudattaa. CPS-määritykset ovat voimassa siinä CA:n koneessa, jossa CPS on määritelty, sekä kaikissa tämän koneen alapuolella olevissa CA-koneissa. Jos käytössä on useampi CPS, tulee jokaista CPS:ää varten asentaa oma käytäntö-CA-palvelin. Jokainen CPS tunnistetaan omasta OID-tunnuksesta. Tässä CPS on RNKO_CPS-käytännön (policy) alla. Lisäksi määritellään AllIssuancePolicy-käytäntö, jolla varmistetaan, että kaikki myöntämiskäytännöt ovat voimassa. Siis sertifikaatit voidaan myöntää automaattisesti tai myöntäminen tapahtuu manuaalisesti esimerkiksi, vasta kun henkilö on tunnistettu vaikkapa henkilökortin avulla. Kannattaa huomioida, että jokainen käytäntö tunnistetaan omasta OID-tunnuksesta.

Tiedostossa määritellään myös notice-teksti ja www-osoite RNKO_CPS-käytännön alla. Notice-teksti tulee näkyviin, kun asiakas napsauttaa hiirellä Issuer Statement -painiketta CA:n sertifikaatissa. More Info -painike avaa dokumentin tekstin, jonka osoite määritellään URL-kohdassa.

Kuten jo alkuasetuksissa mainittiin, yksityisen avaimen pituus on 2048 bittiä, CA:n sertifikaatti on voimassa 10 vuotta sekä sulkulistat julkaistaan kaksi kertaa vuodessa eli 26 viikon välein eikä lisäsulkulistoja ei julkaista. Alla on malli CAPolicy.inf-tiedostosta:

[Version]
Signature="$Windows NT$"

[PolicyStatementExtension]
Policies= AllIssuancePolicy,RNKO_CPS

[AllIssuancePolicy]
OID = 2.5.29.32.0

[RNKO_CPS]
OID=1.3.6.1.4.1.311.509.3.1
NOTICE=RNKO Certificate Practice Statement
URL=http://www.rnko.fi/CPS/CPS.htm

[certsrv_server]
RenewalKeyLength=2048
RenewalValidityPeriodUnits=10
RenewalValidityPeriod=years
CRLPeriod=weeks
CRLPeriodUnits=26
CRLDeltaPeriodUnits=0
CRLDeltaPeriod=days
DiscreteSignatureAlgorithm=1
[1, s. 125; 6, s.126].

18.4 Juuri-CA:n sertifikaatin ja sulkulistan noutaminen

Ennen käytäntö-CA -sertifikaattipalvelimen asennusta noudetaan juuri-CA:sta sertifikaatti sekä uusin sulkulista. Nämä asennetaan käytäntö-CA:n trusted root store -sertifikaattisäiliöön. Tällä varmistetaan, että käytäntö-CA luottaa juuri-CA:han sekä sulkulistan tarkastus onnistuu. Sertifikaatin ja sulkulistan noutaminen täytyy tehdä manuaalisesti esim. usb-tikun avulla. Juuri-CA-koneessa kopioidaan sertifikaatti usb-tikulle certutil-ohjelmalla:

certutil -ca.cert ”x:\rnkoca01_RNKO Root CA.crt”

X: on usb-aseman tunnus. Jos juuri-CA:n sertifikaatti on uusittu, pitää kopioida kaikki sertifikaatit samalla. Tämä onnistuu copy-komennolla:

copy %systemroot%\system32\certsrv\certenroll*.crt x:\

Sulkulista kopioidaan certutil-ohjelmalla:

certutil -GetCRL “x:\RNKO Root CA.crl”

Tiedostot viedään manuaalisesti usb-tikulla käytäntö-CA-palvelimeen.

Vienti voidaan suorittaa käytäntö-CA-palvelimessa Certificates-työkalulla tai certutil-ohjelmalla. Sertifikaattitiedoston nimi on rnkoca01_RNKO Root CA.crt ja sulkulista on nimeltään RNKO Root CA.crl. Jos sertifikaatti olisi uusittu kerran, olisivat nimet rnkoca01_RNKO Root CA(1).crt ja RNKO Root CA(1).crl. Siis suluissa oleva numero näyttää, kuinka monesti sertifikaatti on uusittu.

Sertifikaatti ja sulkulista viedään Certificates-työkalulla. Ensin työkalu täytyy luoda mmc-konsolissa. Valitaan Start > Run ja kirjoitetaan mmc ja painetaan ENTER. Seuraavaksi valitaan File-valikosta Add/Remove Snap-in ja edelleen Add. Tämän jälkeen valitaan Certificates ja valitaan edelleen Add. Avautuvasta ikkunasta valitaan Computer account ja sitten Next. Seuraavaksi valitaan Local computer ja Finish. Lopuksi painetaan Close ja OK. Työkalu sertifikaatin viemistä varten on valmis. Työkalun voi tallentaa File-valikosta, jolloin seuraavalla kerralla ei työkalua tarvitse enää tehdä uudelleen. Tämän jälkeen voidaan tuoda itse sertifikaatti. Napsautetaan ikkunassa Certificates-kuvaketta ja valitaan View-valikosta Options. Rastitetaan Physical certificate stores -valinta ja kuitataan OK. Pääikkunassa kaksoisklikataan Certificates (Local Computer) -kuvaketta, edelleen kaksoisklikataan Trusted Root Certification Authorities ja tämän jälkeen kaksoisklikataan Registry. Klikataan seuraavaksi hiiren kakkospainikkeella Certificates ja valitaan All Tasks ja edelleen Import ja sitten Next. Varmistetaan, että usb-muistitikku, jossa on juuri-CA:n sertifikaatti ja sulkulista, on kytketty koneeseen. Valitaan ikkunasta Browse ja etsitään juuri-CA:n sertifikaatti rnkoca01_RNKO Root CA.crt ja valitaan Open. Valitaan Place all certificates in the following store -valinta ja klikataan Next. Sertifikaatin tallennuspaikka (Trusted Root Certification Authorities\Registry) on automaattisesti oikein joten painetaan Finish. Sulkulista tuodaan samalla tavalla, paitsi tiedostoa valittaessa valitaan RNKO Root CA.crl -tiedosto. Jos juuri-CA:n sertifikaatti on uusittu, pitää em. komentosarja uusia; siis kaikki sertifikaatit on tuotava kuten jo aikaisemmin mainittiin.

Joskus sertifikaatteja on vaikea löytää, jolloin niitä kannattaa etsiä etsi-toiminnolla. Tällöin avataan Certificates-työkalu. Klikataan hiiren kakkos-painikkeella pääikkunassa Certificates-kuvaketta. Valitaan Find Certificates, annetaan valintakriteeri ja valitaan lopuksi Find Now. Valintakriteerejä kannattaa kokeilemalla kokeilla ja tutkia tulosta.

Vaihtoehtoisesti sertifikaatin voi tuoda nopeasti certutil-ohjelmalla seuraavalla komennolla:

certutil -addstore -f Root ”x:\rnkoca01_RNKO Root CA.crt”

Sulkulistan voi tuoda komennolla:

certutil -addstore -f Root ”x:\RNKO Root CA.crl”

Root on sertifikaatin sijoituspaikka ja x: on usb-muistitikun asematunnus. Jos sertifikaatteja on useampia, voi sertifikaatit ja sulkulistat tuoda komento-jonossa. Tällöin luodaan komentojono, jonka sisältö on:

for %A in (x:*.crt) do certutil -addstore -f Root %A
for %A in (x:*.crl) do certutil -addstore -f Root %A

Ensimmäinen komento tuo x:-asemasta kaikki sertifikaatit (.crt-tiedostot) ja toinen vastaavasti kaikki sulkulistat (.crl-tiedostot). Valitsin -f pakottaa tuo-maan sertifikaatin, vaikka se olisikin jo aikaisemmin tuotu.

Tuonnin jälkeen kannattaa tarkistaa, että tuonti tapahtui oikeaan paikkaan ja sertifikaatin ja sulkulistan versionumerot ovat samat. Tarkistus tapahtuu ko-mennolla:

certutil -verifystore root

Lisäksi kannattaa tarkastaa, että Application Policies- ja Issuance Policies -kohdissa molemmissa lukee All. [3, s. 85-91; 6, s.126.]

18.5 Käytäntö-CA:n asennus ja sertifikaatin luonti

Käytäntö-CA-koneeseen kirjaudutaan paikallisella Administrator-oikeudet omaavalla tunnuksella. Tästä tunnuksesta tulee **CA Administrator** asen-nuksen yhteydessä; oikeudet voidaan myöhemmin delegoida toiselle käyttä-jätunnukselle tarvittaessa. Koneen kello ja päiväys kannattaa tarkistaa tässä

vaiheessa. Seuraavaksi lisätään Certificate Services -komponentti. Komponentin lisääminen tapahtuu samalla tavalla kuin juuriCA-palvelimen asennuksessa ohjauspaneelissa.

Myöskään käytäntö-CA-koneeseen ei ole suotavaa asentaa muita palveluita tietoturvan takia. IIS-palvelin kannattaa myös jättää asentamatta. Käytäntö-CA-koneessa offline-sertifikaatit voidaan anoa Certification Authority -työkalulla kuten juuri-CA-koneessakin.

Certificate Services -komponentin lisäämisen jälkeen ei voida enää vaihtaa koneen nimeä eikä työryhmää.

Ohjattu toiminto jatkuu Windows Server 2003 CA:n asennuksessa CA Type -ikkunassa, jossa valitaan **Stand-alone subordinate CA**; lisäksi rastitetaan kohta **Use custom settings to generate the key pair and CA certificate.**

Public and Private Key Pair -sivulla valitaan seuraavat asetukset:

- CSP: Microsoft Strong Cryptographic Service Provider
- Allow the CSP to interact with the desktop: Ei valita!
- Hash algorithm: SHA-1
- Key length: 2,048.

Siinä tapauksessa, jos HSM-laite on asennettu järjestelmään, valitaan CSP-kohdassa se CSP, joka asennettiin HSM-laitteen yhteydessä. Jos HSM-laite on asennettu, valitaan vielä asetus **Allow this CSP to interact with the desktop**. Jos HSM-laitetta ei ole asennettu **Allow this CSP to interact with the desktop**- ja **Use an existing key** -asetukset jätetään tyhjiksi.

CA Identifying Information -sivulla tehdään seuraavat valinnat:

- Common Name for this CA: RNKO Policy CA
- Distinguished name suffix: O=RNKO,C=FI
- Validity Period: Determine by Parent CA (valittu jo valmiiksi).

Common name for this CA on nimi, jolla CA tunnetaan. Distinguished name suffix on aktiivihakemistonimeä vastaava LDAP-nimi, jonka voi myöhemminkin määritellä Certutil-ohjelmalla. Validity period on CA:n sertifikaatin voimassaoloaika, joka määritellään juuri-CA-palvelimen asetuksissa. Jos koneeseen on jossakin vaiheessa jo asennettu Certificate Services -palvelu

sekä myös poistettu tämä asennus, tulee ilmoitus halutaanko aikaisemman asennuksen yksityinen avain kirjoittaa yli. Jos avainta ei tarvita tai sen on varmuuskopioitu, voidaan hyväksyä ylikirjoitus. Jos halutaan suorittaa varmuuskopiointi ja keskeyttää asennus, ei hyväksytä ylikirjoitusta.

Certificate database Settings -sivun asetukset määrittävät, minne tietokanta sekä log-tiedosto tallennetaan. Tallennuksen tulee tapahtua paikalliselle NTFS-levylle samalla tavalla kuin juuri-CA:n asennuksessa:

- Certificate database: D:\CertDB
- Certificate database log: D:\CertLog
- CA configuration: D:\CAConfig.

Certificate database- ja Certificate database log -kohdat määrittävät, minne tietokanta sekä log-tiedosto tallennetaan. Tallennuksen tulee tapahtua paikalliselle NTFS-levylle. Certificate database -ruutuun kirjoitetaan D:\CertDB ja Certificate database log -ruutuun kirjoitetaan D:\CertLog. Hakemistot kannattaa luoda ja valita Browse-painikkeella. Jos Certificate Services on asennettu jo aikaisemmin ja nyt esim. palautetaan asennus varmuuskopiosta, *Preserve existing certificate database* -kohta rastittamalla voidaan asentaa asennus käyttämään jo olemassa olevaa tietokantaa. Ilman rastia mahdollinen olemassa oleva tietokanta tuhoutuu. *Store configuration information in a shared folder* -kohdassa määritellään paikka, josta konfiguraatiot jaetaan asiakkaille. Tässä tapauksessa, kun CA toimii offline-tilassa, asetuksella ei ole merkitystä, mutta se pitää kuitenkin määritellä. Oletusmääritys on C:\CAConfig, joka muutetaan hakemistoksi D:\CAConfig. CA Certificate Request -sivulla valitaan Save the request to a file ja Request file -kohtaan kirjoitetaan esim. x:\PolicyCA.reg. Tiedosto tallennetaan usb-muistitikulle ja sillä haetaan sertifikaatti juuri-CA-koneelta.

Asennus pyytää mahdollisesti seuraavaksi vaiheessa asennusmedian (CD-levy asemaan) jatkaakseen asennusta.

Seuraavaksi tulee ilmoitus, että sertifikaatti tulee pyytää juuri-CA-palvelimelta syntyneellä sertifikaattihakemuksella (.reg-tiedosto). Tämän jälkeen asennus on valmis.

IIS-palvelinta ei asenneta, kuten tässä tapauksessa ei tarvitse tehdä, tulee ilmoitus, ettei sertifikaatteja voi anoa www-sivujen kautta.

Jos IIS-palvelin on asennettu, tulee ilmoitus palvelun pysäyttämisestä. Lopuksi painetaan Finish-painiketta ja Usb-muistitikku viedään juuri-CA-koneeseen, josta käytäntö-CA:n sertifikaatti anotaan. [1, s. 125-129; 3, s. 91-95.]

Windows Server 2008 CA:n asennus jatkuu Certificate Services -roolin lisäämisen jälkeen seuraavasti:

- Specify Setup Type -sivulla valitaan Standalone.
- Specify CA Type -sivulla valitaan Subordinate CA -valinta.
- Set up Private Key -sivulla valitaan Create A New Private Key.

Configure Cryptography For CA -sivulla tehdään seuraavat valinnat:

- Select a cryptographic service provicer (CSP): RSA#Microsoft Software Key Storage Provider
- Key character length: 2048
- Select the hash algorithm for signing certificates issued by this CA: sha256.

Configure CA Name -sivulla tehdään seuraavat valinnat:

- Common name for this CA: RNKO Policy CA
- Distinguished name suffix: O=RNKO,C=FI.

Request Certificate From A Parent CA -sivulla sertifikaattipyyntö tallennetaan tiedostoksi USB-muistille esimerkiksi nimellä PolicyCA.req. Tämän jälkeen Configure Certificate Database -sivulla kirjoitetaan:

- Certificate database: D:\CertDB
- Certificate database log: D\CertLog.

Confirm Installation Selections -sivulla valitaan Install-painike tietojen tarkastamisen jälkeen. Seuraavaksi tulee Installation Results -sivu, josta valitaan Close.

Seuraavaksi sertifikaattipyyntö vielä tarkistetaan ennen toimittamista juuri-CA:lle. [6, s. 127-128.]

18.6 Sertifikaattipyynnön varmistus

Osa käytäntö-CA:n sertifikaatin ominaisuuksista tulee periytymällä ylemmältä CA:lta ja osa CAPolicy.inf-tiedostosta. Jotta ominaisuudet CAPolicy.inf-tiedostosta ovat tulleet oikein, kannattaa ne tarkastaa ennen sertifikaattipyynnön toimittamista juuri-CA:lle. Tarkastus tehdään certutil-komennolla:

Certutil PolicyCA.req

Certutil-komennon parametriksi annetaan CA:n asennuksessa syntynyt certifikaattipyyntötiedosto (.req). Listauksesta tarkastetaan, että Certificate Policies -otsikko löytyy. Otsikon alla tulee olla All Issuance policies -käytäntö sekä RNKO_CPS-käytäntö, joka näkyy OID-tunnuksena 1.3.6.1.4.1.311.509.3.1. Certificate Policies -kohdan alapuolelta tulee siis löytyä seuraavanlainen listaus:

Certificate Policies
[1]Certificate Policy:
Policy Identifier=All issuance policies
[2]Certificate Policy:
Policy Identifier=1.3.6.1.4.1.311.509.3.1
[2,1]Policy Qualifier Info:
Policy Qualifier Id=User Notice
Qualifier:
Notice Text=RNKO Certificate Practice Statement
[2,2]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
http://www.rnko.fi/CPS/CPS.htm

Listauksesta voi olla joskus hankala löytää haluttu rivi, joten komennon voi antaa esimerkiksi muodossa:

Certutil PolicyCA.req | find /I ”Policy Identifier”;

Komennolla siis etsitään rivi, jossa lukee Policy Identifier. Jos listaus puuttuu, tällöin tulee tarkastaa että %systemroot%-hakemistossa on varmasti tiedosto nimeltä CAPolicy.inf ja sen sisältö on sama kuin aikaisemmin kuvattiin. Pienikin kirjoitusvirhe saattaa aiheuttaa, ettei käytäntö tule voimaan. [3, s. 95-96.].

18.7 Sertifikaattipyynnön tekeminen juuri-CA:ssa

Sertifikaattipyyntö, joka on req-tiedostona muistitikulla, toimitetaan juuri-CA-koneeseen. Pyyntö tehdään Certification Authority -työkalulla. Juuri-CA-koneeseen kirjaudutaan CA administrator -tunnuksella. Administrative Tools -valikosta käynnistetään Certification Authority -työkalu. Varmistetaan ensin, ettei CA hyväksy sertifikaatteja automaattisesti. Tämä on kyllä oletuksena ja tulisi säilyttää näin edelleenkin. Tarkistaminen tapahtuu aktivoimalla koneen nimi ja valitsemalla Action-valikosta Properties. Seuraavaksi valitaan Policy Module -välilehti, josta edelleen valitaan Properties-painike. Valintamerkin tulee olla ylemmässä kohdassa (Set the certificate request status to pending. The administrator must explicitly issue the certificate), joka määrää, että ylläpitäjä tutkii sertifikaattipyynnön ja myöntää tämän perusteella hakijalle sertifikaatin.

Seuraavaksi tehdään varsinainen sertifikaattipyyntö. Varmistetaan, että koneen nimi on aktiivinen ja valitaan Action-valikosta All Tasks ja edelleen Submit new request. Avataan hakemistoikkuna usb-muistitikulta ja valitaan PolicyCA.req-tiedosto ja valitaan Open. Valitaan seuraavaksi Pending Requests -säiliön kuvake. Tarkastetaan sertifikaatin ominaisuudet vielä varmuuden vuoksi aktivoimalla sertifikaatti ja valitsemalla Action-valikosta All tasks ja edelleen Export Binary Data. Alasvetovalikosta valitaan Binary Request ja lopuksi OK.

Tarkistetaan seuraavat asiat:

- Subject:
  CN= RNKO Policy CA
  DC=RNKO
  DC=FI
- Public Key Length: 2048 bits
- Basic Constraints
  Subject Type=CA
- Certificate Policies
  [1] Certificate Policy:
  Policy Identifier=1.3.6.1.4.1.1204.509.3.1
  [1,1]Policy Qualifier Info:
  Policy Qualifier Id=User Notice
  Qualifier:

Notice Text=RNKO Certificate Practice Statement
[1,2]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
http://www.rnko.fi/CPS/CPS.htm

- Signature matches Public Key
- [1]Certificate Policy:
  Policy Identifier=All issuance policies
- Jos Windows 2008 -ympäristössä on otettu käyttöön CNG-algoritmit, tarkistetaan vielä, että allekirjoitusalgoritmi on SHA256RSA:
  Algorithm ObjectId: 1.2.840.113549.1.1.11 sha256RSA . [1, s. 128; 6, s. 128-129.]

Subject-kohdassa tulee olla CA:n nimi. Julkisen avaimen pituus tulee olla 2048 bittiä. Basic Constraints -kohdassa tarkastetaan, että sertifikaatti on määritelty CA:lle, eikä esimerkiksi käyttäjälle, koneelle tai palvelulle. Certificate Policies -kohdassa tarkastetaan, että OID, Notice Text ja CPS:ään viittaava polku ovat oikein. Katsotaan vielä, että allekirjoitus vastaa julkista avainta. Seuraavaksi tarkastetaan, että myöntämiskäytäntö on oikein. Siis All issuance policies pitää sisällään kaikki muut myöntämiskäytännöt. Myöntämiskäytäntöjä on eri tasoja, joilla ilmaistaan kuinka sertifikaatti on myönnetty asiakkaalle. Esimerkiksi jotkin sertifikaatit myönnetään vain henkilökohtaisesti, jolloin vaaditaan henkilöllisyystodistus. Jotkin sertifikaatit voidaan myöntää automaattisesti; riittää että käyttäjä kirjautuu ja antaa salasanansa. Tämän jälkeen hän saa sertifikaatin. Menettelytapa, kuinka käyttäjä saa sertifikaatin, voidaan ilmaista sertifikaatissa myöntämiskäytännöllä. Jos Windows Server 2008 -ympäristössä on otettu käyttöön CNG-algoritmit, tarkistetaan lopuksi vielä, että allekirjoitusalgoritmi on SHA256RSA [1, s.127; 6, s.128-129.]

Jos asetukset eivät ole oikein, pitää käytäntö-CA:n sertifikaattipalvelu asentaa uudelleen ja ennen asennusta tarkastaa CAPolicy.inf-tiedoston sisältö.

Seuraavaksi suljetaan ikkuna ja aktivoidaan uudelleen Pending Requests -säiliön kuvake, valitaan Action-valikosta All Tasks ja edelleen Issue. Tämä toimenpide myöntää sertifikaatin. Seuraavaksi aktivoidaan Issued Certificates -kuvake ja klikataan sertifikaatti aktiiviseksi, valitaan Action-valikosta Open. Tämän jälkeen tarkastetaan General-välilehdeltä, että kohdassa *This*

certificate is intended for the following purpose(s) lukee All issuance policies ja All application policies. Valitaan Details-välilehti ja varmistetaan, että CRL Distributions -ja Authority Information Access -kentissä ovat ne polut, jotka aikaisemmin konfiguroitiin. Myös muut kentät kannattaa silmäillä läpi virheiden varalta; myöntäjä on juuri-CA, sertifikaatin voimassaoloaika on oikein jne. Jos kaikki tiedot ovat oikein, siirrytään seuraavaan kohtaan, jossa sertifikaatti viedään sertifikaattisäiliöstä tiedostoksi. [1, s. 3, s. 96-98.]

18.8 Käytäntö-CA:n sertifikaatin tallennus tiedostoksi

Jatketaan edellisestä kohdasta sulkematta ikkunaa. Valitaan Details-välilehdellä Copy to file ja edelleen Next. Valitaan Cryptographic Message Syntax Standard - PKCS#7 Certificates (.P7B) ja lisäksi laitetaan valintamerkki kohtaan *Include all certificates in the certification path if possible*. Valitaan Next. Tallennus tapahtuu usb-muistitikulle halutulla nimellä esim. x:\PolicyCA, jolloin tiedostolle tulee tarkennin .p7b. Seuraavaksi valitaan Next, Finish ja klikataan OK-painiketta kahdesti. Tästä jatketaan aktivoimalla Issued Certificates -kuvake ja aktivoidaan oikealla näkyvä sertifikaatti ja valitaan edelleen Action-valikosta All Tasks. Avautuvasta valikosta valitaan Export Binary Data. Valintaruudussa on oletuksena Binary Certificate, joka hyväksytään. Valitaan alapuolelta *Save binary data to a file* ja painetaan OK. Tallennetaan syntyvä DER-koodattu tiedosto usb-muistitikulle sopivalla nimellä esim. PolicyCA.cer. Tarkennin tulee myös kirjoittaa. Lopuksi suljetaan ikkuna. Ennen sertifikaatin asennusta käytäntö-CA-palvelimeen, tarkastetaan sertifikaatin luottoketju. [3, s. 99; 6, s.129-130.]

18.9 Käytäntö-CA:n sertifikaatin luottoketjun tarkastaminen

Ennen sertifikaatin asennusta käytäntö-CA-palvelimeen sertifikaatista kannattaa tarkastaa, että luottoketju on muodostunut oikein. Luottoketjun tarkastaminen suoritetaan certutil-komennolla seuraavasti:

```
certutil -verify x:\PolicyCA.cer
```

Tarkastamista helpottaa ErrorStatus-kohtien etsiminen tekstistä. Kohdat löydetään komennolla:

```
certutil -verify x:\PolicyCA.cer | findstr /c:dwErrorStatus
```

Listauksesta tulee tarkistaa, että ErrosStatus-kohdat ovat nollia:

CertContext[0][0]: dwInfoStatus=102 **dwErrorStatus=0**
CertContext[0][1]: dwInfoStatus=10c **dwErrorStatus=0**
[3, s. 100].

18.10 Sertifikaatin asentaminen käytäntö-CA-palvelimeen

Seuraavaksi sertifikaatti asennetaan käytäntö-CA-palvelimeen. Siirrytään käytäntö-CA-palvelimen ääreen ja käynnistetään Administrative Tools -valikosta Certification Authority. Aktivoidaan koneen kuvake ja valitaan Action-valikosta All Tasks ja edelleen install CA Certificate. Valitaan usb-muistitikulta PolicyCA.p7b ja valitaan tämän jälkeen Open. Aikaisemmin koneeseen asennettiin juuri-CA:n sertifikaatti. Jos näin ei olisi tehty, tulisi nyt ilmoitus, ettei juuritason sertifikaatti ole luotettu (root certificate is not trusted). Aktivoidaan koneen kuvake ja valitaan Action-valikosta All Tasks ja edelleen Start Service. Palvelun käynnistyksen voi tehdä myös komentokehotteessa komennolla net start certsvc. Palvelun käynnistyttyä kuvakkeen merkki muuttuu punaisesta vihreäksi. [3, s. 100-101; 6, s.130.]

Sertifikaatin voi asentaa vaihtoehtoisesti komentokehotteessa:

certutil -installcert x:\PolicyCA.p7b
net start certsvc [3, s. 101-102]

Usb-muistitikulla oleva sertifikaattipyyntö (PolicyCA.req-tiedosto) tulisi tietoturvan vuoksi tuhota.

Loput määritykset ajetaan komentojonosta. Asetukset käsiteltiin juuri-CA:n asennuksen yhteydessä. Lopuksi asennus kannattaa tarkistaa, kuten juuri-CA:n asennuskin tarkastettiin.

REM --- Määritellään LDAP-polku
certutil -setreg CA\DSConfigDN CN=Configuration,DC=rnko,DC=fi

REM --- Määritellään sulkulitan julkaisuajat kaksi kertaa vuodessa---
certutil -setreg CA\CRLPeriodUnits 26
certutil -setreg CA\CRLPeriod "Weeks"
certutil -setreg CA\CRLDeltaPeriodUnits 0
certutil -setreg CA\CRLDeltaPeriod "Days"

REM --- Määritellään sulkulistan julkaisupaikat myönnettävien sertifikaattien CDP-laajennoksiin ---
certutil -setreg CA\CRLPublicationURLs
"1:%windir%\system32\CertSrv\CertEnroll\%%3%%8%%9.crl\n
10:ldap:///CN=%%7%%8,CN=%%2,CN=CDP,CN=Public Key Services,CN=Services,%%6%%10\n2:http://www.rnko.fi/pki/ %%3%%8%%9.crl"

REM --- Määritellään sertifikaattien julkaisupaikat myönnettävien sertifikaattien AIA-laajennoksiin ---
certutil -setreg CA\CACertPublicationURLs
"1:%windir%\system32\CertSrv\CertEnroll\%%1_%%3%%4.crt\n
2:ldap:///CN=%%7,CN=AIA,CN=Public Key Services,CN=Services,
%%6%%11\n2:http://www.rnko.fi/pki/%%1_%%3%%4.crt"

REM --- Määritellään auditointi-asetuksiin kaikki toiminnot ---
certutil -setreg CA\AuditFilter 127

REM --- Määritellään myönnettävien sertifikaattien voimassaoloaika ---
certutil -setreg CA\ValidityPeriodUnits 5
certutil -setreg CA\ValidityPeriod "Years"

REM --- Windows 2008 -palvelimissa voidaan ottaa käyttöön diskriitti allekirjoitus ---
certutil -setreg CA\csp\DiscreteSignatureAlgorithm 1

REM --- Käynnistetään Certificate-palvelu uudelleen ---
net stop certsvc & net start certsvc
certutil -crl
[1, s. 123; 6, s.131.]

18.11 Auditoinnin määrittäminen

Viimeisenä tehtävänä on vielä auditoinnin määrittäminen. Sertifikaattipalvelimen kaikki tapahtumat määriteltiin jo tallennettavaksi lokiin edellisessä komentojonossa:

certutil -setreg CA\AuditFilter 127

Tämän lisäksi määritellään Administrative Tools -valikon Local Security Policy -työkalulla onnistuneet ja epäonnistuneet tapahtumat auditoitavaksi kuten

tehtiin juuri-CA:n asennuksessa. Jos myös uusien CNG-algoritmien auditointi otetaan käyttöön, annetaan komento:

auditpol /set /subcategory:”other system events” /success:enable /failure:enable

Käytäntö-CA-palvelimen asennus on nyt valmis. Tuotantoympäristöön asentaminen vaatii vielä lisätoimenpiteitä lähinnä tietoturvan osalta; näitä toimenpiteitä ei käydä läpi tämän työn puitteissa. [1, s. 123-124.]

19 MYÖNTÄJÄ-CA:N ASENTAMINEN

Myöntäjä-CA:n tehtävä on automatisoida sertifikaattien myöntäminen. Suuremmassa ympäristössä päivittäin myönnetään sertifikaatteja lukuisa määrä. Tehtävän helpottamiseksi ja kustannuksien säästämiseksi voidaan tehtävä automatisoida hyvin pitkälle. Ryhmäkäytäntö-asetukset määrittävät hakevatko asiakkaat sertifikaatteja automaattisesti vai pitääkö sertifikaatti hakea manuaalisesti. Aktiivihakemisto-ympäristössä ryhmäkäytäntö-asetukset tulee tehdä erikseen toimialueen ohjauskoneille sekä muille työasemille ja palvelimille.

Ennen myöntäjä-CA-palvelimen asennusta on varmistettava tai päätettävä seuraavat asiat:

- Käyttöjärjestelmän versio on Windows Server 2003- tai 2008 Enterprise Edition ja asennus on suoritettu C-asemalle.
- Koneen aika ja päiväys ovat oikein.
- Palvelin on liitetty toimialueeseen.
- Asentajalla on local administrator-, enterprise administrator- ja root domain administrator -oikeudet.
- Tiedostojako (file and print sharing) on CA-koneessa päällä.
- Myöntäjä-CA luottaa juuri-CA:han.
- Myöntäjä-CA:n tulee pysyä noutamaan käytäntö-CA:n sertifikaatti ja sulkulista.
- CA:n tyyppi: Enterprise Subordinate CA
- CA:n nimi: RNKO Issuing CA
- CA:n koneen nimi: RNKOCA3
- CA:n sertifikaatin avaimen pituus: 2048 bittiä

- CA:n sertifikaatin voimassaoloaika: 5 vuotta
- CA jakaa sertifikaatteja, joiden voimassaoloaika on maksimissaan 2 vuotta.
- Sulkulistat julkaistaan joka kolmas päivä ja lisäsulkulistat julkaistaan joka 12 tunti.
- Jos asennetaan Windows 2008 -CA, käytetäänkö CNG-algoritmeja?
- Levyjärjestelmänä kaksi peilattua levyä sekä RAID 5 -levyjärjestelmä. C- ja D-asemat ovat peilattuja; C-asemalla on käyttöjärjestelmä, D-asemalla CA-koneen loki-tiedostot ja RAID 5 -levyllä, joka näkyy E-asemana, CA:n tietokanta.

19.1 Sertifikaattien ja sulkulistojen noutaminen juuri-CA- ja käytäntö-CA-palvelimilta

Myöntäjä-CA:n asentamisessa tarvitaan sekä juuri- että käytäntö-tasojen palvelimien sertifikaatit ja sulkulistat. Koska em. palvelimet eivät ole verkossa, täytyy sertifikaatit ja sulkulistat hakea manuaalisesti. Tämä tehtiin jo aiemmin, kun käytäntö-CA-palvelimeen noudettiin juuri-CA:n sertifikaatti certutil-ohjelmalla:

certutil -ca.cert “x:\rnkoca01_RNKO Root CA.crt”

Sulkulista haettiin komennolla:

certutil -GetCRL ”x:\RNKO Root CA.crl”

Sertifikaatit ja sulkulistat voidaan myös kopioida %system-root%\system32\certsrv\certEnroll\ -hakemistosta suoraan usb-tikulle. Myös selaimella voidaan tehdä nouto, jos web-palvelin on asennettu CA-palvelimiin. Tässä tapauksessa näin ei ole, joten tämä mahdollisuus puuttuu. Käytäntö-CA:n sertifikaatti ja sulkulista kopioidaan usb-tikulle. Tämän jälkeen usb-tikulla on molempien palvelimien sertifikaatit ja sulkulistat.

19.2 Juuri-CA- ja käytäntö-CA-palvelimien sertifikaattien ja sulkulistojen julkaiseminen aktiivihakemistossa

Seuraavalla komentojonolla julkaistaan juuri-CA- ja käytäntö-CA-palvelimien sertifikaatit ja sulkulistat aktiivihakemistossa. Komentojono kopioi kaikki sertifikaatit ja sulkulistat, ei pelkästään uusimpia. Myöntäjä-CA -koneeseen kir-

jaudutaan juuritoimialueen Administrator-tunnuksella. Tilin tulee myös kuulua Enterprise Administrators -ryhmään.

```
@echo off
x:
cd \
REM juuri-CA:n sertifikaattien julkaiseminen:
for %%c in ("rnkoca01*.crt") do certutil -dspublish -f "%%c" RootCA
REM käytäntö-CA:n sertifikaatin julkaiseminen:
for %%c in ("rnkoca02*.crt") do certutil -dspublish -f "%%c" SubCA
REM juuriCA:n sulkulistan julkaiseminen:
for %%c in ("RNKO*.crl") do certutil -dspublish -f "%%c"
REM käytäntö-CA:n sulkulistan julkaiseminen:
for %%c in ("RNKO*.crl") do certutil -dspublish -f "%%c"
gpupdate /force
```

Julkaiseminen tapahtuu certutil-ohjelman dspublish-valitsimella. F-valitsin (force) tarvitaan, koska säiliörakenne ei ehkä ole olemassa aktiivihakemistossa, tällöin se luodaan. Sertifikaatin julkaisemisessa toiseksi viimeinen parametri on sertifikaatin nimi ja viimeinen parametri on julkaisupaikka; rootca tarkoittaa, että sertifikaatti julkaistaan root CA storessa ja subca tarkoittaa, että sertifikaatti julkaistaan subordinate CA storessa. Sulkulistan julkaisemisessa viimeinen parametri on sulkulistan nimi. Gpupdate-komennolla saadaan ryhmäkäytäntö voimaan välittömästi. Seuraavan kerran kun ryhmäkäytäntö ajetaan asiakaskoneisiin, sertifikaatit lisätään trusted root CA- ja intermediate CA -säiliöihin automaattisesti.

Tässä esimerkissä voisi käyttää alla olevia yksittäisiä certutil-komentoja kopioinnissa, koska uusittuja sertifikaatteja tai sulkulistoja ei vielä ole.

```
certutil -dspublish -f "rnkoca01_RNKO Root CA.crt" RootCA
certutil -dspublish -f "rnkoca02_RNKO Policy CA.crt" SubCA
certutil -dspublish -f "RNKO Root CA.crl"
certutil -dspublish -f "RNKO Policy CA.crl"
```

Julkaisemisessa on muutama huomioitava asia, joihin kannattaa kiinnittää huomiota. Ensiksi, kun myöhemmin jossakin vaiheessa CA:n sertifikaatit uusitaan, täytyy ne julkaista uudestaan aktiivihakemistossa. Myös uuden sulkulistan julkaisu aiheuttaa uuden sulkulistan julkaisun myös aktiivihakemistoon.

Toiseksi, kun asiakaskoneella testataan sertifikaatin luonti, tarkastetaan ettei tule virhettä issuer distribution point (IDP). Tällöin sulkulistassa oleva julkaisupolku ei täsmää todellisen julkaisupolun kanssa. Kolmanneksi huomioitavaa on, että julkaisu tapahtuu certutil-ohjelmalla, joka korvaa Windows 2000 Resource Kit:in Dsstore-ohjelman; tätä Dsstore-ohjelmaa ei saa käyttää Windows Server 2003- tai 2008 -ympäristössä! [1, s. 132; 2, s. 2, s. 110-113; 6, s.133.]

19.3 Juuri-CA- ja käytäntö-CA-palvelimien sertifikaattien ja sulkulistojen julkaiseminen www-palvelimella

Tässä esimerkissä käytetään www-palvelimena Microsoftin IIS-palvelinta. Oletuksena koneeseen on jo asennettu www-palvelu ja yrityksen sivut on julkaistu palvelimelta. Sertifikaattien ja sulkulistojen julkaiseminen www-saitin kautta tapahtuu seuraavasti:

- Kirjaudutaan paikallisena Administratorina koneeseen, johon IIS on asennettu.
- Käynnistetään Internet Information Services (IIS) -konsoli Administrative Tools -valikosta.
- Valitaan palvelimen kuvakkeen alta Web Sites ja klikataan hiiren kakkospainikeella yrityksen web-saitin päällä, valitaan New - Virtual Directory.
- Ensimmäiseksi annetaan alias-nimi saitille, joka on tässä esimerkissä pki. Tällöin julkaisupolku tulee aikaisemman esimerkin mukaan http://www.rnko.fi/pki. Polun tulee olla ehdottomasti sama kuin sertifikaatissa ja sulkulistassa.
- Seuraavaksi valitaan kansio, jonne sertifikaatit ja sulkulistat tallennetaan. Polku voisi olla esim. d:\pki.
- Seuraavassa ikkunassa määritellään oikeuksiksi read-oikeudet; muita oikeuksia ei tarvitse antaa. Lopuksi painetaan Finish-painiketta.
- Kopioidaan juuri-CA:n ja käytäntö-CA:n sertifikaatit ja sulkulistat usb-muistista d:\pki-hakemistoon. [1, s. 133; 2, s. 2, s. 114.]

19.4 Julkaistujen sertifikaattien ja sulkulistojen oikeudet

Aktiivihakemiston sekä www-palvelimen oikeudet tulee tarkastaa, jotta asiakkaat voivat tarvittaessa tehdä sertifikaattien ja sulkulistojen tarkastuksen.

Virtuaalihakemiston http://www.rnko.fi/pki oikeudet määritellään niin, että anonyymikäyttö on sallittu (allow anonymous access). Tällöin asiakkaat näkevät hakemiston sisällön riippumatta ensisijaisesta autentikointimenetelmästä. Oletuksena anonyymikäyttö on sallittu, mutta se kannattaa tarkastaa virtuaalihakemiston ominaisuuksista: klikataan hiiren kakkospainikkeella virtuaalihakemiston päällä ja valitaan Properties, Directory Security -välilehdeltä valitaan Edit-painike ja tarkistetaan, että Allow Anonymous Access -valintaruudussa on valintamerkki.

Jos halutaan, että asiakkaat, jotka eivät kuulu toimialueeseen, voivat tehdä LDAP-kyselyitä sertifikaateista ja sulkulistoista, täytyy Everyone-ryhmälle antaa lukuoikeudet toimialueen objekteihin. Tämä tehdään ADSIEdit-ohjelmalla, joka asennetaan Support Tools -paketista Windows Server 2003/2008 -asennuslevyltä. Tässä esimerkissä tämä ei ole tarpeellista. [2, s. 113.]

19.5 Juuri-CA- ja käytäntö-CA-palvelimien sertifikaattien ja sulkulistojen julkaisemisen varmistaminen aktiivihakemistossa

Sertifikaattien ja sulkulistojen julkaisemisen varmistaminen oikeassa paikassa voidaan tehdä Active Directory Sites and Services -konsolilla. Tämä tapahtuu seuraavasti:

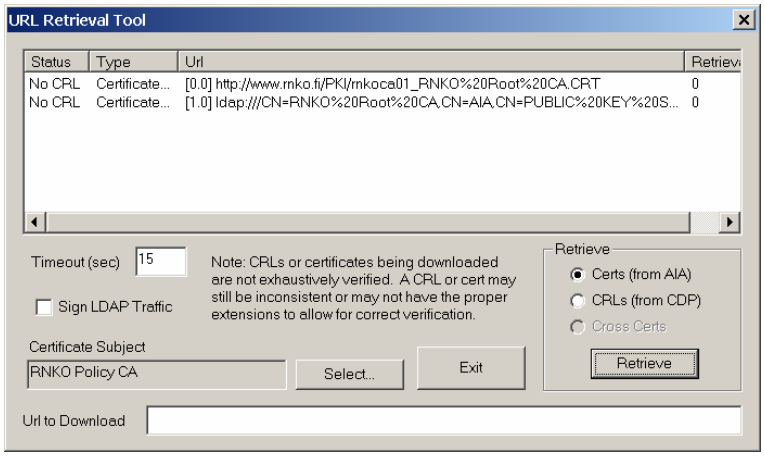
- Kirjaudutaan toimialueen ohjauskoneeseen juuritoimialueen Administrator-tunnuksella; tunnuksen tulee kuulua myös Enterprise Administrators -ryhmään.
- Käynnistetään Active Directory Sites and Services -työkalu Administrative Tools -valikosta. Käynnistys voidaan tehdä myös komentokehotteesta komennolla *dssite.msc*.
- Valitaan View-valikosta *Show Services Node*.
- Valitaan Services ja tämän alta Public Key Services.
- Tarkistetaan, että sertifikaatit löytyvät AIA-säiliöstä ja objektit sulkulistoille löytyvät CRL-säiliöstä. Jos julkaisemisessa on tapahtunut virhe, täytyy julkaisu tehdä uudelleen. Saattaa olla myös, että aktiivihakemistoympäristössä replikointi ei ole vielä tapahtunut, joten objektit eivät vielä ole näkyvissä. Tässä ikkunassa voidaan myös poistaa tarpeettomat vanhat objektit.

Saman tarkastuksen voisi tehdä myös AdsiEdit.msc-konsolilla, jonka voi asentaa Support Tools -työkalupaketista. Tämä operaatio siis tarkasti, että julkaisu tapahtui oikeassa paikassa. Seuraavaksi pitää tarkastaa, että julkaistiin oikeaa tietoa. [2, s. 114-115.]

19.6 Juuri-CA- ja käytäntö-CA-palvelimien sertifikaattien ja sulkulistojen tietojen tarkastaminen

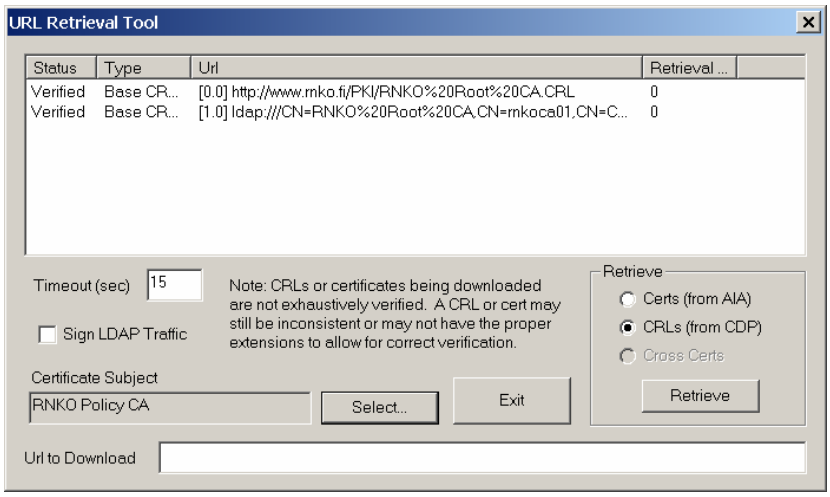
Tarkistaminen, että aktiivihakemistossa julkaistu tieto on oikeaa, tapahtuu seuraavasti:

- Kirjaudutaan koneeseen, joka on aktiivihakemiston jäsen jollakin toimialueen käyttäjän tunnuksella. Riittää, että käyttäjätunnuksella on lukuoikeudet aktiivihakemistossa julkaistuihin sertifikaatteihin ja sulkulistoihin.
- Komentokehotteessa annetaan komento:
  certutil -url x:\”rnkoca02_RNKO Policy CA.crt”
- Avautuvassa ikkunassa (kuva 29) valitaan Certs (from AIA) ja painetaan Retrieve-painiketta; tällöin nähdään sertifikaatit.
- Tämän jälkeen valitaan CRLs (from CDP) ja painetaan Retrieve-painiketta; tällöin nähdään sulkulistat (kuva 30).



Kuva 29. Julkaistun sertifikaatin polun tarkistus käytäntö-CA:n sertifikaatista

Tässä esimerkissä sulkulistoja ei ole, koska juuri-CA:n CAPolicy.inf-tiedostossa CRL distribution points on jätetty tyhjäksi.



Kuva 30. Julkaistun sulkulistan polun tarkistus käytäntö-CA:n sertifikaatista

Certutil -url -komento toimii X.509V3-sertifikaattien kanssa. Komentoa voi käyttää myös käyttäjien sertifikaattien tarkastamisessa. Sertifikaatit ja sulkulistat voidaan tarkastaa vain DER-koodatuista sertifikaateista. Jos sulkulistassa on virhe, on se korjattava palvelimella, jossa sulkulista on määritelty. Sulkulista on attribuuttina jokaisessa myönnettävässä sertifikaatissa, joten tämän asetuksen tulee olla ehdottomasti oikein. [2, s. 115-117.]

19.7 CAPolicy.inf-tiedoston valmistelu

Ennen sertifikaatti-palvelun asentamista valmistellaan CAPolicy.inf-tiedosto. Alla on esimerkkitiedosto:

```
[Version]
Signature="$Windows NT$"
[certsrv_server]
Renewalkeylength=2048
RenewalValidityPeriodUnits=5
RenewalValidityPeriod=years
CRLPeriod=3
CRLPeriodUnits=days
CRLDeltaPeriod=12
CRLDeltaPeriodUnits=hours
DiscreteSignatureAlgorithm=1
LoadDefaultTemplates=0
```

Yksityisen avaimen pituus on 2048 bittiä. Käytäntö-CA-palvelimen myöntämät sertifikaatit ovat voimassa viisi vuotta. Sulkulistat julkaistaan joka kolmas päivä. Lisäsulkulistat julkaistaan 2 kertaa vuorokaudessa eli joka 12 tunti. [1, s. 133-134.]

Jos asennetaan Windows Server 2008 -palvelin ja halutaan ottaa käyttöön Suite B -yhteensopiva ympäristö, tulee myös versio 3:n mukaiset sertifikaattipohjat ottaa käyttöön. Oletuksena CA:n asennuksessa otetaan käyttöön aikaisemmat sertifikaattipohjat (versiot 1 ja 2). Version 3 sertifikaattipohjat saadaan käyttöön määrittelemällä LoadDefaultTemplates=0 -rivi. Diskreetit allekirjoitusalgoritmit saadaan tarvittaessa käyttöön DiscreteSignatureAlgorithm=1 -määritelmällä.

CAPolicy.inf-tiedosto tallennetaan Windowsin asennuskansioon, esim. C:\Windows, kuten aikaisemmissakin asennuksissa tehtiin.

19.8 Myöntäjä-CA:n asennus

Asennettavassa koneessa tulisi olla levyjärjestelmänä kaksi peilattua levyä sekä RAID 5 -levyjärjestelmä. C- ja D-asemat ovat peilattuja; C-asemalla on käyttöjärjestelmä, D-asemalla CA-koneen loki-tiedostot ja RAID 5 -levyllä CA:n tietokanta. RAID-5 -levy näkyy E-asemana. Levyasemien tarkastuksen lisäksi kannattaa tarkastaa, että kone on varmasti toimialueen jäsen sekä ajan ja päiväyksen oikeellisuus. Sertifikaattien myöntämisessä voi tulla ongelmia, jos koneiden kellot poikkeavat toisistaan kovin paljon.

Asentajan käyttäjätilin tulee olla Enterprise Admins- ja juuritoimialueen Domain Admins -ryhmissä sekä Administrators-ryhmässä. Tämä koskee nimenomaan ensimmäisen CA-koneen asennusta. Muissa CA-koneiden asennuksissa ei tarvitse olla Domain Admins -ryhmän jäsenenä. Asentajalla tulee olla siis pääsy aktiivihakemiston configuration-osioon.

Myöntäjä-CA-koneeseen kirjaudutaan siis Administrator-, Enterprise Admins- ja Domain Admins -oikeudet omaavalla tunnuksella. Tästä tunnuksesta tulee **CA Administrator** asennuksen yhteydessä; oikeudet voidaan myöhemmin delegoida toiselle käyttäjätunnukselle tarvittaessa.

Jos sertifikaatteja myönnetään selaimen kautta, tulee luonnollisesti IIS asentaa. Se tapahtuu aikaisemmin kuvatulla tavalla.

IIS-palvelimen jälkeen lisätään Certificate Services -komponentti. Tämä tapahtuu hyvin pitkälle samoin kuin aikaisempien CA-koneiden asennuksessa ohjauspaneelissa. Kannattaa muistaa, että lisäyksen jälkeen ei voida enää vaihtaa koneen nimeä eikä työryhmää.

Certificate Services -palvelun asentaminen **Windows Server 2003** -palvelimessa käynnistetään ohjaspaneelista aikaisemmin kuvatulla tavalla.

- CA:n tyypiksi tulee Enterprise Subordinate CA
- Rastitetaan myös kohta Use custom settings to generate the key pair and CA certificate.

Public and Private Key Pair -sivulla valitaan seuraavat asetukset:

- CSP: Microsoft Strong Cryptographic Service Provider
- Allow the CSP to interact with the desktop: Disabled
- Hash algorithm: SHA-1
- Key length: 2,048.

Siinä tapauksessa, jos HSM-laite on asennettu järjestelmään, valitaan CSP-kohdassa se CSP, joka asennettiin HSM-laitteen yhteydessä. Jos HSM-laite on asennettu, valitaan vielä asetus **Allow this CSP to interact with the desktop**. Jos HSM-laitetta ei ole asennettu **Allow this CSP to interact with the desktop**- ja **Use an existing key** -asetukset jätetään tyhjiksi.

CA Identifying Information -sivulla tehdään seuraavat valinnat:

- Common Name for this CA: RNKO Issuing CA
- Distinguished name suffix: O=RNKO,C=FI.

Kuten aikaisemmin jo todettiin, Common name for this CA on nimi, jolla CA tunnetaan ja Distinguished name suffix on aktiivihakemistonimeä vastaava LDAP-nimi.

Certificate database Settings -sivun asetukset määrittävät, minne tietokanta sekä log-tiedosto tallennetaan. Tallennuksen tulee tapahtua paikalliselle NTFS-levylle samalla tavalla kuin juuri-CA:n asennuksessa:

- Certificate database: E:\CertDB
- Certificate database log: D:\CertLog.

CA Certificate Request -sivulla valitaan Save the request to a file ja Request file -kohtaan kirjoitetaan esim. x:\IssuingCA.reg. Tiedosto tallennetaan usb-muistitikulle ja sillä haetaan sertifikaatti käytäntö-CA-koneelta.

Seuraavaksi tulee ilmoitus IIS-palvelun väliaikaisesta pysäyttämisestä, jos palvelu on asennettu samaan koneeseen. Tämän jälkeen asennus pyytää mahdollisesti seuraavaksi vaiheessa asennusmedian (CD-levy asemaan) jatkaakseen asennusta. Tarvittaessa hakemistoksi valitaan \i386-hakemisto. Myös mahdollisesti Service Pack -tiedostojen media pyydetään.

Seuraavaksi tulee ilmoitus, että asennus ei ole vielä valmis. Sertifikaatti tulee pyytää käytäntö-CA-palvelimelta asennuksessa syntyneellä sertifikaattihakemuksella (.reg-tiedosto). Jos www-palvelin on asennettu samaan koneeseen, hyväksytään vielä Active Server Pages -sivujen käyttöönotto ja suljetaan kaikki ikkunat. Jos palvelinta ei ole asennettu, tulee ilmoitus ettei sertifikaatteja voi anoa selaimen kautta, ennen kuin www-palvelu on asennettu koneeseen.

Windows Server 2008 -palvelimessa Certificate Services -komponentti lisätään Administrative Tools -valikon Server Managerin kautta lisäämällä rooli, kuten jo aikaisemmin käytiin läpi. Roles Summary -kohdasta valitaan Add Roles. Select Server Roles -sivulla valitaan Active Directory Certificate Services -valintaruudun lisäksi myös Certification Authority Web Enrollment -valintaruutu, jos sertifikaatteja halutaan myöntää myös selaimen kautta. Näin normaalisti tehdään ja tämä vaatii Web Server (IIS) -roolin valitsemista. Roolien valinnan jälkeen painetaan Add Required Role Services -painiketta.

Windows 2008 CA:n asennus jatkuu Certificate Services -roolin lisäämisen jälkeen seuraavasti:

- Specify Setup Type -sivulla valitaan Enterprise.
- Specify CA Type -sivulla valitaan Subordinate CA -valinta.
- Set up Private Key -sivulla valitaan Create A New Private Key.

Configure Cryptography For CA -sivulla tehdään seuraavat valinnat:

- Select a cryptographic service provicer (CSP): RSA#Microsoft Software Key Storage Provider
- Key character length: 2048

- Select the hash algorithm for signing certificates issued by this CA: sha256.

Configure CA Name -sivulla tehdään seuraavat valinnat:

- Common name for this CA: RNKO Issuing CA
- Distinguished name suffix: O=RNKO,C=FI.

Request Certificate From A Parent CA -sivulla sertifikaattipyyntö tallennetaan tiedostoksi USB-muistille esimerkiksi nimellä IssuingCA.req. Tämän jälkeen Configure Certificate Database -sivulla kirjoitetaan:

- Certificate database: E:\CertDB
- Certificate database log: D\CertLog.

Sivulla näkyvät roolit hyväksytään ja Confirm Installation Selections -sivulla valitaan Install-painike tietojen tarkastamisen jälkeen. Seuraavaksi tulee Installation Results -sivu, josta valitaan Close.

Asennuksen yhteydessä syntynyt sertifikaattipyyntö toimitetaan käytäntö-CA -palvelimelle. Toimenpiteet ovat hyvin pitkälle samat kuin aikaisemmin käytäntö-CA:n asennuksessa. Certification Authority -työkalulla lähetetään ja hyväksytään sertifikaattipyyntö seuraavasti:

- Aktivoidaan RNKO Policy CA ja valitaan Action-valikosta All Tasks ja edelleen valitaan Submit new request.
- Tiedoston nimeksi kirjoitetaan x:\IssuingCA.req.
- Seuraavaksi valitaan Action-valikosta All Tasks ja valitaan Export Binary Data; alasvetovalikosta valitaan Binary Request.
- Varmistetaan, että subject-nimi on RNKO Issuing CA:
  Subject:
  CN= RNKO Issuing CA
  O=RNKO
  C=FI
- Varmistetaan, että julkisen avaimen pituus on 2048 bittiä:
  Public Key Length: 2048 bts
- Varmistetaan, että Basic Constraints -kohdassa Subject Type=CA:
  Basic Constraints
  Subject type=CA

- Windows 2008 -asennuksessa tarkastetaan, että allekirjoitusalgoritmi on SHA256RSA:
  Algorithm ObjectId: 1.2.840.113549.1.1.11 sha256RSA
- Varmistetaan, että allekirjoitus on sama kuin julkisessa avaimessa:
  Signature matches Public Key.
- Suljetaan ikkuna ja aktivoidaan pending SubCA certificate -kuvake ja valitaan Action-valikosta All Tasks ja edelleen Issue.
- Aktivoidaan seuraavaksi Issued Certificates ja kaksoisklikataan myönnettyä sertifikaattia.
- Valitaan Details-välilehti ja edelleen Copy to File.

Myönnetty sertifikaatti tallennetaan USB-muistitikulle PKCS #7 Certificates (.P7B) -muodossa esimerkiksi nimellä IssuingCA.p7b. (Valitaan myös Include all certificates in the certification path if possible). Myönnettyä sertifikaattia kaksoisklikataan hiirellä ja tarkastetaan seuraavat tiedot:

- voimassaoloaika
- avaimen pituus
- sertifikaattikäytännöt (mihin sertifikaattia voi käyttää).

Tässä vaiheessa voidaan juuri-CA- ja käytäntö-CA -palvelimet halutessa sammuttaa. USB-muistitikku viedään myöntäjä-CA-palvelimeen takaisin ja saatetaan asennus Certification Authority -työkalulla loppuun :

- Aktivoidaan RNKO Issuing CA -kuvake ja valitaan Action-valikosta All Tasks ja edelleen Install CA Certificate.
- Select File to Complete CA Installation -ikkunassa kirjoitetaan x:\IssuingCA.p7b.
- Lopuksi käynnistetään palvelu valitsemalla Action-valikosta All Tasks ja edelleen Start Service.

Sertifikaatti voidaan asentaa myös komentokehotteessa komennolla:

certutil -installcert IssuingCA.p7b

[1, s. 134-138; 2, s. 118-124; 6, s.136-139.]

19.8.1 Myöntäjä-CA-koneen konfigurointi

Loput CA:n asetuksista ajetaan komentojonosta. Komentojonoon on määritelty lähinnä seuraavat asetukset:

- Koneet kuuluvat RNKO.FI-toimialueeseen.
- WWW-palvelin on nimeltään www.rnko.fi. Palvelimeen on tehty virtuaalihakemisto nimeltä pki, jonne kopioidaan kaikkien CA-koneiden sertifikaatit sekä sulkulistat.
- WWW-palvelin on verkossa osoitteessa www.rnko.fi/pki sekä sisäverkon että ulkoverkon asiakkaille.
- Myöntäjä-CA myöntää sertifikaatit asiakkaille maksimissaan kahdeksi vuodeksi. Asiakkaita voivat olla käyttäjät, koneet, palvelut ja verkkolaitteet.
- Asiakkaat hakevat sulkulistat ja sertifikaatit ensisijaisesti aktiivihakemistosta, toissijaisesti www-palvelimelta ja viimeisenä palvelimen tiedostojaosta.
- Huomioitavaa on, että ympäristön koneiden käyttöjärjestelmä on joko Windows XP/Vista/7 tai Windows Server 2003/2008.

```
REM --- Määritellään Configuration-osion LDAP-osoite ---
certutil -setreg CA\DSConfigDN CN=Configuration,DC=RNKO,DC=FI

REM --- Määritellään sulkulistan julkaisusykli ---
certutil -setreg CA\CRLPeriodUnits 3
certutil -setreg CA\CRLPeriod "Days"
certutil -setreg CA\CRLDeltaPeriodUnits 12
certutil -setreg CA\CRLDeltaPeriod "Hours"

REM --- Määritellään sulkulistan julkaisupisteen URL-osoitteet
certutil -setreg CA\CRLPublicationURLs "65:%windir%\system32\CertSrv\
CertEnroll\%%3%%8%%9.crl\n79:ldap:///CN=%%7%%8,CN=%%2,
CN=CDP,CN=Public Key Services,CN=Services,%%6%%10\n6:
http://www.rnko.fi/pki/%%3%%8%%9.crl\n6:http://%%1/
CertEnroll/%%3%%8%%9.crl\n0:file://\\%%1/CertEnroll\%%3%%8%%9.crl"

REM --- Määritellään sertifikaattien julkaisupisteen URL-osoitteet
certutil -setreg CA\CACertPublicationURLs "1:%windir%\system32\
CertSrv\CertEnroll\%%1_%%3%%4.crt\n3:ldap:///CN=%%7,
CN=AIA,CN=Public Key Services,CN=Services,%%6%%11\n2:
http://www.rnko.fi/pki/%%1_%%3%%4.crt\n2:http://%%1/
CertEnroll/%%1_%%3%%4.crt \n0:file://\\%%1\CertEnroll/
%%1_%%3%%4.crt "
```

```
REM --- Määritellään auditointi-asetukset ---
certutil -setreg CA\AuditFilter 127

REM --- Määritellään diskriitit allekirjoitukset Windows Server 2008 -ympäristössä ---
certutil -setreg CA\csp/DiscreteSignatureAlgorithm 1

REM --- Määritellään myönnettäville sertifikaateille maksimi voimassaoloaika
certutil -setreg CA\ValidityPeriodUnits 2
certutil -setreg CA\ValidityPeriod "Years"

REM --- Käynnistetään sertifikaatti-palvelu uudelleen ---
net stop certsvc & net start certsvc
certutil -crl
```

Komentojonon suorituksen jälkeen kannattaa kopioida kaikki sertifikaatit usb-muistiin komennolla:

```
copy /y %windir%\system32\certsrv\certenroll\*.cr? x:\
```

Hakemistossa tulisi olla kaksi sertifikaattia ja yksi sulkulista:

- RNKO Issuing CA.crl
- RNKO Issuing CA+.crl
- RNKOCA03.rnko.fi_RNKO Issuing CA.crt

[1, s. 138-139; 6, s. 139-141.]

19.8.2 Auditointi-asetusten määrittely

Kuten käytäntö-CA:n asennuksessa, auditointi tulee vielä määritellä tietoturva-asetuksissa. Määritykset tehdään sen organisaatioyksikön ryhmäkäytännön asetuksissa, johon myöntäjä-CA kuuluu. [1, s. 139-140.]

19.8.3 Luottoketjun ja sertifikaattien tarkastus

Myöntäjä-CA:n täytyy pystyä tarkastamaan luottoketju yläpuolella oleviin CA-koneisiin sekä niiden sulkulistat. Jos näin ei ole, CA:n käynnistyksessä tulee virheilmoitus. Luottoketju tarkastetaan komennolla:

```
certutil -verify ”RNKOCA03.rnko.fi_RNKO Issuing CA.crt”
```

Komento kannattaa antaa muodossa:

certutil -verify ”RNKOCA03.rnko.fi_RNKO Issuing CA.crt” |findstr /c:dwErrorStatus

Listauksesta tutkitaan, että jokainen dwErrorStatus-arvo on nolla.

Myös sulkulistojen julkaisupisteet kannattaa tarkastaa. Tarkastaminen tapahtuu komennolla:

certutil -URL ” RNKOCA03.rnko.fi_RNKO Issuing CA.crt”

Varmuudeksi kannattaa vielä ladata sulkulista paikalliselle koneelle tarkastusta varten. HTTP-protokollalla lataaminen on helppoa, mutta jos julkaisupiste on tavoitettavissa pelkästään LDAP-protokollalla, annetaan komento:

certutil -store -split ldap:///CN= RNKOCA03 ,CN= Issuing CA, CN=CDP, CN=Public Key Services, CN=Services,CN=Configuration,DC= rnko, DC=fi? CertificateRevocationList ?base?objectClass=cRLDistributionPoint

Tuloksena syntyy tiedosto nimeltään Blob0_0.crl, jota kaksoisklikkaamalla saadaan tiedosto auki.

Vastaavat asiat voidaan tehdä myös PKI Health -työkalulla, joka on saatavissa Windows Server 2003 Resource Kit -työkaluista. Työkalut voi ladata Microsoftin saitilta ilmaiseksi. Windows Server 2008 -palvelimessa tämä työkalu asentuu automaattisesti Certificate Services -roolin asennuksen yhteydessä. Työkalu tutkii kaikki polut, jotka on mainittu sertifikaatin laajennoskentissä (AIA- ja CDP-kentät), ja raportoi, ovatko sertifikaatit ja sulkulistat saatavilla. Lisäksi raportoidaan sertifikaattien ja sulkulistojen päättymispäivämäärät. Työkalu käynnistetään Windows Server 2003/2008 -palvelimessa, joka on toimialueen metsän jäsen. Työkalu käynnistetään komennolla pkiview.msc Start-valikon Run-linkistä. Ikkunassa näkyy jokainen CA ja CRL and AIA location -kohdassa ovatko linkit ja sertifikaatit kunnossa. [2, s. 125-126; 6, s. 146.]

19.8.4 Sertifikaattipohjien ja arkistoinnin käyttöönotto

Kun sertifikaattipalvelimet on asennettu, määritellään seuraavaksi sertifikaattipohjat sertifikaateille, jotka halutaan myöntää asiakkaille. Sertifikaattipohjat määritellään Certificate Template -työkalulla, joka käynnistetään antamalla komentokehotteessa (tai Start-valikon Run-komento) komento certtmpl.msc. Versio 1:n pohja voidaan päivittää versioon 2 tai 3 tekemällä siitä kopio. Päi-

vitys täytyy tehdä silloin, kun halutaan muuttaa pohjan ominaisuuksia; versio 1:n pohjan ominaisuuksia ei voida muuttaa. Versio 3 -pohjat ovat käytössä Windows Server 2008 -palvelimessa, kun halutaan käyttää CNG-salausta. Sertifikaattipohjan päivittäminen uudemmaksi tapahtuu klikkaamalla hiiren kakkospainikkeella halutun sertifikaattipohjan päällä ja valitsemalla pikavalikosta Duplicate Template -valinta. Windows Server 2008 -palvelimessa kysytään, kumpi pohja luodaan, versio 2 vai versio 3. Jos halutaan luoda versio 2 -pohja, valitaan ikkunasta valinta *Windows 2003 Server, Enterprise Edition* ja jos halutaan luoda versio 3 -pohja, valitaan *Windows Server 2008, Enterprise Edition*. General-välilehdellä annetaan pohjalle nimi ja valitaan sertifikaatin voimassaoloaika. Extensions-välilehdellä voidaan määritellä sovelluskäytännöt (Application Policies). Jos esimerkiksi version 2 pohja kopioitiin User-pohjasta, on pohjassa sovelluskäytännöt Encrypting File System, Secure Email ja Client Authentication. Edit-painiketta painamalla ja tämän jälkeen painamalla Add-painiketta voidaan lisätä esimerkiksi Smart Card Logon -sovelluskäytäntö. Tällöin tällä sertifikaattipohjalla myönnetyillä sertifikaateilla voi salata tiedostoja, käyttää salattua sähköpostia, autentikoitua ja kirjautua toimikortilla.

Sertifikaatti voidaan näin tarvittaessa myöntää useampaa käyttötarkoitusta varten. Superseded Templates -välilehdellä voidaan määritellä ne sertifikaattipohjat, jotka tämä uusi pohja korvaa. Edellisessä tapauksessa valittaisiin User-sertifikaattipohja. Security-välilehdellä määritellään käyttäjät tai ryhmät, jotka voivat hakea sertifikaattia kyseisellä sertifikaattipohjalla. Käyttäjälle tai ryhmälle tulee antaa read- ja enroll-oikeudet. Jos lisäksi annetaan vielä autoenroll-oikeus, voidaan sertifikaatti myöntää automaattisesti. Jos halutaan, että sertifikaatti myönnetään manuaalisesti, laitetaan rasti Issuance Requirements -välilehden kohtaan *CA certificate manager approval*. Tällöin anottava sertifikaatti tallentuu Certification Authority -työkalun Pending Requests -säiliöön odottamaan ylläpitäjän toimenpiteitä. Saman välilehden kohta *This number of authorised signatures* määrittää kuinka monta allekirjoitusta sertifikaattihaku tarvitsee ennen myöntämistä. Lisäksi määritellään myöntämis- ja sovelluskäytännöt, jotka myöntäjän sertifikaatissa tulee olla, jotta myöntäminen onnistuu. Automaattisessa sertifikaatin myöntämisessä nämä kohdat jätetään täyttämättä. Edellä kuvatuilla periaatteilla tehdään tarvittava määrä sertifikaattipohjia organisaation tarpeen mukaan.

Jos asiakkaiden yksityisten avainten arkistointi halutaan ottaa käyttöön, tehdään ympäristöön avaimen palautusagentille tili, jolle määritellään tarvittavat oikeudet sertifikaatin hakemiseksi. Tämän jälkeen sallitaan avainten arkistointi myöntäjä-CA-palvelimessa. Lopuksi vielä määritellään tarvittaviin sertifikaattipohjiin automaattinen arkistointi.

Tilin luonnin jälkeen siis annetaan luodulle avaimen palautusagentin tilille oikeudet hakea Key Recovery Agent -sertifikaattia. Tämä sertifikaatti pitää olla käyttäjällä, jotta hän voi palauttaa käyttäjien yksityiset avaimet tietokannasta takaisin käyttäjille. Oikeudet annetaan Certificate Templates -työkalulla. Ikkunan oikeassa laidassa klikataan hiiren kakkospainikkeella Key Recovery Agent -sertifikaattipohjaa ja valitaan Properties. Tämän jälkeen valitaan Security-välilehti ja tällä välilehdellä lisätään luotu käyttäjätili listaan ja lopuksi annetaan Read- ja Enroll-oikeudet. Autoenroll-oikeutta ei kannata antaa, koska sertifikaattia ei tulisi myöntää automaattisesti, vaan ylläpitäjä myöntää sen manuaalisesti tietoturvasyistä.

Nyt siis luodulla tilillä on oikeus hakea avaimen palautusagentin sertifikaattia. Hakeminen on helpoin tehdä web-selaimen kautta ottamalla yhteys myöntäjä-CA-palvelimen www-palvelimeen. Avaimen palautusagentti avaa organisaation www-sivut selaimeensa kirjoittamalla osoitteeksi https://rnkoca03/CertSrv. SSL-salaus tulee rakentaa www-palvelimeen, muussa tapauksessa yhteys otetaan salaamattomana kirjoittamalla osoite http://rnkoca03/CertSrv. Sivulta valitaan linkki Request a certificate. Uudelta sivulta valitaan advanced certificate request. Seuraavalta sivulta valitaan Create and submit a request to this CA. Certificate Template -kohdasta valitaan Key Recovery Agent. Tarvittaessa avaimen pituutta voi kasvattaa oletusarvosta 2048 bittiä. Lisäksi valitaan kohta Enable strong private key protection, jolloin annetaan salasana, joka tarvitaan käsiteltäessä yksityistä avainta. Sertifikaattipyyntö lähetetään Submit painikkeella. Ylläpitäjä (Certificate manager) myöntää tämän jälkeen sertifikaatin Certificate Authority -työkalulla. Tämän myöntämisen jälkeen avaimen palautusagentti avaa selaimeensa uudestaan www-sivut kirjoittamalla https://rnkoca03/CertSrv. Sivulta valitaan linkki View the status of a pending certificate request. Sertifikaatti asennetaan Install-valinnalla. Jos ylläpitäjä ei ole vielä hyväksynyt sertifikaattipyyntöä, sivulla on linkki josta voi tarkastella sertifikaattihakua; lähinnä perua haun.

Seuraavaksi sallitaan avainten arkistointi myöntäjä-CA-palvelimessa. Tämä tehdään myöntäjä-CA:n Certification Authority -työkalulla valitsemalla CA-koneen kuvake hiiren kakkospainikkeella ja valitsemalla edelleen Properties. Recovery Agents -välilehdellä valitaan kohta *Archive the key* ja tämän jälkeen Add-painikkeella valitaan avaimen palautusagentin sertifikaatti.

Lopuksi käydään lisäämässä sertifikaattipohjiin yksityisen avaimen automaattinen arkistointi. Tämä tehdään Certificate Templates -työkalulla. Työkalun saa auki siis kirjoittamalla komentokehotteessa certtmpl.msc tai Certification Authority -työkalussa klikkaamalla hiiren kakkospainikkeella Certificate Templates -kuvaketta ja valitsemalla Manage. Avautuvassa ikkunassa kaksoisklikataan sertifikaattipohjaa ja valitaan Request Handling -välilehti. Välilehdeltä valitaan *Archive subject's encryption private key*.

Lopuksi kannattaa testata hakemalla sertifikaatti automaattisesti sekä manuaalisesti testikäyttäjälle. Myönnetyt sertifikaatit kannattaa avata ja tutkia, että kaikki asetukset ovat oikein. Lisäksi kannattaa testata yksityisen avaimen palautus tietokannasta.

20 TULOKSET

Osa PKI-järjestelmän kustannuksistaa aiheutuu itse palvelinkoneista. Mitä suurempi ympäristö, sen enemmän tarvitaan palvelinkoneita. Varsinkin, jos organisaation metsä muodostuu useammasta puusta, joista jokainen sijaitsee omassa nimiavaruudessaan. Siis jokaisessa puussa, jossa on oma nimiavaruus, tarvitaan omat CA-palvelimet. Myös hierarkiatasoja vähentämällä voidaan ympäristöä yksinkertaistaa ja hieman vähentää koneiden määrää. Koneiden määrän vähentäminen on kuitenkin marginaalista, koska juuri-CA- ja käytäntö-CA-palvelimet voidaan asentaa yhteen koneeseen virtuaaliympäristöön. Jos käytetään pelkästään yksitasoista mallia, jolloin yksi kone suorittaa kaikkien CA-koneiden roolin, tingitään tietoturvasta. Yksitasoisessa mallissa tulisikin CA:n avaimet tallentaa HSM-laitteeseen, koska CA-konetta ei voida poistaa verkosta. Tämä lisää käytännössä kustannuksia huomattavasti, joten yksitasoinen malli tulee kysymykseen ainoastaan tilanteessa, jossa ei tarvita tietoturvaa.

Kaksitasoinen malli toimii useimmissa organisaatioissa. Organisaatiolla voi olla toimipaikkoja hyvinkin laajalla maantieteellisellä alueella. Kolmitasoista

mallia tarvitaan, jos halutaan määritellä esimerkiksi eri toimipaikkoihin erilaiset sovellus- tai myöntämiskäytännöt. Tällöin käytäntö-CA-palvelimella voidaan määritellä mitä sertifikaatteja alapuolella olevat myöntäjä-CA-palvelimet voivat jakaa ja millä tavalla käyttäjät tunnistetaan. Koko ympäristöä ei tarvitse asentaa uudelleen eikä kaikkia sertifikaatteja uusia, jos jonkin palvelimen avain paljastuu; tässä mallissa siis voidaan laittaa tarvittaessa usean myöntäjä-CA:n sertifikaatit sulkulistalle ja jättää osa myöntäjä-CA-palvelimista verkkoon.

Tietoturvan kasvattaminen lisää tasoja ja myös koneiden määrää. Kuten jo aikaisemmin mainittiin, juuri-CA- ja käytäntö-CA-koneita voidaan ajaa samalla virtuaalikoneella, mikä vähentää kustannuksia. Jos koneesta otetaan kiintolevy talteen ja tallennetaan se varmaan paikkaan, voidaan konetta käyttää toisissa tehtävissä. Tällöin tulee kuitenkin huolehtia tilanteesta, jossa joko juuri-CA- tai käytäntö-CA-palvelin joudutaan käynnistämään. Tällainen tilanne tulee ainakin sertifikaattien uusinnassa ja sulkulistojen julkaisussa. Riskinä on myös tämän laitteiston hajoaminen ja korvaaminen uudella; saadaanko uusi täsmälleen samanlainen laitteisto? Palvelimet tuleekin varmuuskopioida joka tapauksessa niin, että palauttaminen onnistuu myös uuteen laiteympäristöön. Virtuaaliympäristöllä voidaan kuitenkin tätä laitteistoriskiä pienentää, koska se ei ole suoraan laiteriippuvainen. Toisaalta virtuaaliympäristö vaatii tehokkaamman koneen.

Koneiden määrää lisää myös vikasietoisuus. Samojen palveluiden tulisi olla saatavissa myös varapalvelimelta. Jokainen asennus vaatii myös käyttöjärjestelmälisenssin, vaikka ympäristönä olisikin virtuaalikone. Lisäksi vikasietoinen levyjärjestelmä on lisäkustannus. Offline-palvelimiin voidaan asentaa ohjelmistopohjainen RAID 1, jolloin säästytään vikasietoisen levyohjaimen hankkimiselta. Levyjen peilaus voidaan siis tehdä Windowsin tukemalla ohjelmallisella peilauksella. Tietokannan sijoittaminen nopealle vikasietoiselle RAID 5- tai RAID 0+1 -levylle tuo lisäkustannuksia. Tällöin ratkaisun tulee olla laitteistopohjainen, mikä on ohjelmistopohjaista huomattavasti kalliimpi. Vikasietoisuuteen luetaan myös OCSP-palvelimen asennus. Koska palvelimen asennus käytännössä vaatii vikasietoisen klusterin rakentamisen, tulee tarkkaan miettiä, tarvitaanko reaaliaikaista sertifikaattien tarkastamista. Monissa ympäristöissä sulkulistoilla saavutetaan tarvittava tietoturva kustannustehokkaasti.

Lisäkustannuksia tuovat myös varmuuskopiointilaitteet. Varmuuskopiointilaitteina voi käyttää mm. nauha-asemaa, vaihdettavaa kiintolevyä tai usb-muistia.

Tietoturva tuo myös lisäkustannuksia HSM-laitteiden tai toimikorttien kautta. HSM-laitteet ovat erittäin kalliita laitteita, mutta näiden kustannuksia voidaan vähentää käyttämällä yhtä HSM-laitetta verkon kautta useammalla CA-palvelimella. Tiedonsiirto verkossa HSM-laitteen ja palvelimen välillä kulkee salatussa muodossa. Toimikortti on huomattavasti halvempi ratkaisu, mutta huonoin puoli on, että kortin tulee olla koko ajan lukijalaitteessa. Lisäksi avaimet on suojattu huonommin kuin HSM-laitteessa.

Fyysinen tietoturva tuo myös omat kustannuksensa. CA-koneet tulee suojata fyysisesti niin, ettei kuka tahansa pääse koneen ääreen. Kone tulee sijoittaa vähintäänkin lukittuun kaappiin, johon vain asiaan kuuluvilla henkilöillä on pääsy.

Varmennepolitiikan ja varmennekäytännön laatiminen, julkaisu ja toteuttaminen tuovat lisäkustannuksia. Varmennekäytäntölausuma on juridinen dokumentti, joten dokumentin laatiminen jo sinänsä vaatii mahdollisesti kalliin lainopillisen avustajan käyttöä. Lisäksi dokumentti pitää julkaista palvelimella. Jos organisaatiolla ei ole ulkopuolisia asiakkaita, voidaan näistä kuluista säästää. Varmennekäytäntö määrittää toimenpiteet, joilla asiakas tunnistetaan sertifikaattia myönnettäessä. Jos tunnistaminen tehdään samalla kun käyttäjä tunnistetaan käyttäjätunnuksen luonnin yhteydessä, voidaan ylimääräistä työtä vähentää ja näin säästää kustannuksissa.

PKI-ympäristön suunnittelu, asennus ja hallinnointi on suuri kustannus organisaatiolle. PKI-ympäristön lisäksi tarvitaan tietoa Windows- ja aktiivihakemistoympäristöistä. Hyvällä suunnittelulla voidaan säästää kustannuksissa hyvinkin paljon, joten suunnitteluun kannattaa ehdottomasti panostaa ja tarvittaessa ostaa sitä konsulttipalveluna. Asennukset tulee tehdä huolella dokumentoiden. Asennuksen jälkeen on vielä testausvaihe, jonka lopputuloksena dokumentoidaan toimiva ympäristö. Tarvittaessa asennuspalvelukin kannattaa ostaa, jos yrityksessä ei ole tarvittavaa osaamista. Ylläpito tuo jatkuvia kustannuksia. Ylläpito sisältää mm. CA-koneiden konfigurointien muutokset, ylläpitäjien roolien määrittämisen, sertifikaattien ja sulkulistojen hallinnan, yksityisten avainten noutamisen tietokannasta, varmuuskopioinnin,

palautuksen, lokien tutkimisen, CA-koneen yleisen ylläpidon sekä vianetsinnän. Ylläpidonkin voi ostaa, mutta tällöin tulee miettiä kuinka nopeasti voidaan reagoida esimerkiksi tietoturvaloukkauksiin; lisäksi tulee muistaa, että ylläpitäjän tulee olla ehdottoman luotettava. Joka tapauksessa tieturvalokeja tulee seurata päivittäin, jotta tarvittaviin toimenpiteisiin voidaan ryhtyä välittömästi. Yleisessä ylläpidossa kannattaa huomioida, että virus- ja haittaohjelmien päivitykset sekä tietoturvapäivitykset pitää testata ennen niiden asennusta. Testaamattomat päivitykset saattavat aiheuttaa jopa järjestelmän toimimattomuuden, joten testauksessa ei kannata säästää. Lisää tietoturvaa saadaan roolien erottamisella, mutta tämä lisää kustannuksia lisääntyvinä henkilöiden palkkakuluina.

Ylläpitoa voidaan vähentää myös pidentämällä sertifikaattien voimassaoloaikaa. Tällöin sertifikaatteja ei tarvitse uusia niin usein. Avaimen pituus ja käytettävä algoritmi pääasiassa vaikuttavat siihen, kuinka pitkäksi ajaksi sertifikaatti voidaan myöntää. Juuri-CA- ja käytäntö-CA -palvelimissa sertifikaatin voimassaoloaika voi olla pitkä, koska palvelin ei ole verkossa eikä näin ollen ole hyökkäyksen kohteena.

Palvelinten sertifikaatit ja sulkulistat julkaistaan yleensä www-palvelimessa. Julkaisussa voidaan käyttää organisaation olemassa olevaa palvelinta, joten konekustannuksissa voidaan säästää, mutta ylläpitokustannukset lisääntyvät sertifikaattien ja sulkulistojen hallinnoinnin myötä. Pidentämällä sulkulistojen julkaisuväliä, saadaan ylläpitokustannuksissa säästetyksi. Toisaalta jos julkaisuväli pitenee liikaa, kärsii tietoturva, kun asiakkaat eivät saa tarpeeksi nopeasti tietoa poistetuista sertifikaateista. Lisäksi kannatta huomioida, että jos lisäsulkulista julkaistaan harvoin, kasvaa sen fyysinen koko ja sitä kautta suorituskyky kärsii.

Sertifikaattien automaattinen myöntämiskäytäntö tuo säästöjä ylläpitokustannuksista. Tällöin sertifikaattien manuaalinen myöntäminen jää pois. Kaikkia sertifikaatteja ei kuitenkaan voi myöntää automaattisesti, mutta toimialueen perussertifikaatit kuten EFS-salaus tai sähköposti voidaan myöntää automaattisesti. Jos yrityksen aktiivihakemistoympäristö on suuri, voi tämä tuoda huomattaviakin kustannussäästöjä ylläpitotyön vähenemisenä sekä lisäksi automatisointi vähentää virheiden määrää.

21 YHTEENVETO

Erilaisissa tietoverkkojen palveluissa tarvitaan yhä enemmän tiedon salausta ja käyttäjien tunnistusta. Julkisen avaimen järjestelmä eli PKI tarjoaa tähän tarvittavat työkalut.

Tiedon salauksessa käytetään sekä symmetristä että epäsymmetristä salausta. Itse tieto salataan symmetrisellä salauksella, jolloin tiedon lähettäjällä ja vastaanottajalla tulee olla hallussaan sama avain. Tällä avaimella tieto salataan lähetettäessä sekä salaus puretaan vastaanotettaessa. Ongelma symmetrisessä salauksessa on avaimen siirtäminen turvallisesti vastaanottajalle. Ratkaisu on epäsymmetrisen salauksen käyttö symmetrisen avaimen siirrossa. Epäsymmetrisessä salauksessa on käytössä kaksi avainta (avainpari), julkinen avain ja yksityinen avain. Tieto salataan julkisella avaimella ja tiedon salauksen purkaminen onnistuu vain avainparin yksityisellä avaimella. Käytännössä symmetrinen avain salataan vastaanottajan julkisella avaimella ja vastaanottaja purkaa salauksen omalla yksityisellä avaimella. Näin symmetrinen avain on saatu siirrettyä turvallisesti vastaanottajalle. Symmetrisessä salauksessa käytettäviä algoritmeja ovat mm. DES, 3DES ja AES. Epäsymmetrisessä salauksessa käytettäviä algoritmeja ovat mm. RSA ja Diffie-Hellman-avaimenvaihtoprotokolla sekä DSA, jota käytetään vain todentamiseen. Todentamisessa lähettäjä allekirjoittaa viestin omalla yksityisellä avaimellaan ja vastaanottaja tarkastaa allekirjoituksen lähettäjän julkisella avaimella. PKI-järjestelmässä CA:n tehtävä on varmistaa, että julkinen avain on oikean henkilön, koneen tai palvelun avain.

Windows Server 2008 tuo mukanaan uusia salausalgoritmeja, Suite B -algoritmit. Suite B on NSA:n uusi määritys, jolla lisätään turvaa uusien salausalgoritmien, kuten elliptisten käyrien, avulla. Suite B sisältää AES-salausalgoritmit 128- ja 256-bittisillä avaimenpituuksilla symmetristä salausta varten, SHA-2-tiivistealgoritmit (SHA-256, SHA-384 ja SHA-512), Elliptic Curve Diffie-Hellman (ECDH) julkisen avaimen salausta varten ja Elliptic Curve Digital Signature Algorithm (ECDSA) allekirjoitusta varten. Windows Server 2008 -käyttöjärjestelmän tietoturvauudistukset tunnetaan nimellä CNG eli Cryptography Next Generation.

PKI on toimintamalli, jossa tieto salataan avoimissa tietoverkoissa epäsymmetristä salausta käyttäen. Järjestelmä luo salauksen tarvitsemat avainparit

sekä ylläpitää avainhakemistoja ja sulkulistoja. PKI on yhdistelmä ohjelmistoja, salaustekniikoita ja palveluita, jotka mahdollistavat tietoturvaratkaisujen rakentamisen; sertifikaattien, julkisten avainten ja yksityisten avainten hallinnan. Järjestelmä tarvitaan nimenomaan siksi, että viestin lähettäjä saa haltuunsa vastaanottajan julkisen avaimen ja voi olla varma siitä, että tätä julkista avainta vastaava yksityinen avain kuuluu viestin vastaanottajalle.

Sertifikaatti eli varmenne on työkalu tunnistamista ja tiedon salaamista varten. Se on standardoitu tapa kytkeä julkinen avain tiettyyn identiteettiin, joka voi olla esimerkiksi henkilö, työasema tai palvelin. Sertifikaatin myöntää varmentaja (CA). CA allekirjoittaa sertifikaatin omalla salaisella avaimellaan, jolloin sertifikaatin sisältöä ei päästä huomaamatta muuttamaan. Sertifikaattia ei voida käyttää ikuisesti, koska muutoin mahdollisella hyökkääjällä on paljon aikaa murtaa yksityinen avain. Sertifikaateilla on tietyn mittainen elinkaari ja ne vanhenevat elinkaaren lopussa. Elinkaarta voidaan pidentää myöntämällä sertifikaatti uudelleen. CA:lla on myös oma sertifikaattinsa, johon sen toiminta perustuu. Yleensä CA myöntää itselleen oman sertifikaatin tai se on hankittu joltakin toiselta luotetulta taholta. CA julkaisee sulkulistaa, jossa ilmoitetaan sertifikaatit, jotka eivät ole enää voimassa.

Windowsin palvelinkäyttöjärjestelmän sertifikaattipalvelulla voidaan rakentaa koko CA-hierarkia tai asentaa se pelkästään yhteen koneeseen. Normaalisti PKI-ympäristö sisältää monta CA-palvelinkonetta. Ensimmäinen vaihe PKI-järjestelmän luonnissa on asentaa CA. Ensimmäinen CA, joka asennetaan on juuri-CA. Juuri-CA voi olla kahta eri tyyppiä: enterprise tai standalone. Normaalissa hierarkisessa rakenteessa tyyppi on standalone. Jos koko hierarkia rakennetaan yhteen koneeseen, on tyyppi enterprise. Hierarkisen CA-rakenteen muodostavat juuri-CA sekä yksi tai useampi väli-CA. Juuri-CA myöntää sertifikaatit väli-CA:ille, jotka edelleen myöntävät sertifikaatit joko toisille väli-CA:ille tai loppukäyttäjille. Väli-CA:t jaetaan vielä käytäntö-CA- ja myöntäjä-CA -palvelimiin. Normaalisti myöntäjä-CA jakaa sertifikaatit loppukäyttäjille ja käytäntö-CA toisille CA-palvelimille. Luottoketjun ansiosta väli-CA:t voivat myöntää loppukäyttäjille sertifikaatteja. Väli-CA:t voidaan määritellä niin, että ne jakavat vain tietyntyyppisiä sertifikaatteja. Esim. väli-CA jakaa sertifikaatteja tiettyyn nimiavaruuteen kuten rnko.fi tai jaettavat sertifikaatit ovat käytössä vain EFS-salauksessa tai älykorteissa. Yksitasoisessa mallissa on vain yksi CA-kone. Se asennetaan enterprise juuri-CA

-koneeksi, joka on toimialueen jäsen ja jakaa sertifikaatit asiakkaille. Tämän CA-koneen tehtävä on siis toimia juuri-CA:n ja väli-CA:n rooleissa. Tämä malli tuo kustannussäästöjä muihin malleihin verrattuna mutta on tietoturvaltaan huonompi. Kaksitasoisessa mallissa on juuri-CA sekä väli-CA, johon on yhdistetty käytäntö-CA:n ja myöntäjä-CA:n roolit. Kolmitasoisessa mallissa em. roolit ovat omissa koneissaan. Tietoturvan takia vain loppukäyttöön myöntävät CA-palvelimet ovat online-tilassa. Muut palvelimet, kuten juuri-CA ja käytäntö-CA ovat offline-tilassa eli ainakin irrotettuina verkosta mutta mahdollisesti myös sammutettuina.

Organisaation tarpeet määrittelevät käytettävät PKI-sovellukset. Yleisesti käytettyjä sovelluksia ovat mm. 802.1x-autentikointi, digitaalinen allekirjoitus, EFS-salaus, SSL, IPSec, salattu sähköposti, älykortit, ohjelmistojen allekirjoitus ja VPN.

Organisaatiolla tulisi olla määriteltynä tietoturvakäytäntö, jossa määritellään tietoturvavaatimukset PKI:n suunnittelua ja käyttöä varten. Lisäksi organisaation tulee määrittää mm. PKI:n ylläpitäjät, minimoida riskit ongelmien tullessa, määrittää sertifikaattien voimassaoloaika ja julkaisupaikka, tehdä ympäristöstä vikasietoinen, miettiä tarvitaanko ristiinsertifiointia toisen organisaation kanssa ja tarvittaessa määritellä oma CPS. CPS-dokumentissa organisaatio kertoo omat velvollisuutensa sertifikaattien myöntäjänä. CPS tarvitaan nimenomaan, jos organisaatio myöntää sertifikaatteja ulkopuolisille käyttäjille.

Suurissa yrityksissä voidaan myöntää jopa tuhansia sertifikaatteja käyttäjille ja koneille. Tällöin sertifikaattipohjat (certificate templates) helpottavat sertifikaattien myöntämistä. Sertifikaattipohjia on kolmea eri versiota. Version 1 pohjat tulivat käyttöön Windows 2000 -ympäristössä. Windows Server 2003 -ympäristöön lisättiin version 2 pohjat ja version 3 pohjat Windows Server 2008 -ympäristöön. Windows Server 2003 -ympäristössä voidaan käyttää version 1 ja 2 pohjia ja Windows Server 2008 -ympäristössä ovat käytössä kaikki pohjat. Version 3 pohjat sisältävät uudet CNG-salaukset, jotka perustuvat elliptisiin käyriin. Version 1 pohjia ei voi editoida, joten käytännössä näistä pohjista kopioidaan version 2 ja 3 pohjat, joita voidaan muokata halutulla tavalla. Pohjaan voidaan määrittää asetus, jolla sertifikaatti jaetaan automaattisesti käyttäjälle. Käyttäjä on siis kirjautunut toimialueella omalla käyttäjätunnuksella ja salasanalla, tämän jälkeen käyttäjä voi saada sertifi-

kaatin automaattisesti esim EFS-salausta varten. Sertifikaattipohjassa määritellään, kenelle myönnetään jokin tietty sertifikaatti automaattisesti; tämän lisäksi määritellään ryhmäkäytännöllä (Group Policy) varsinainen sertifikaatin haku. Sertifikaatin automaattinen myöntäminen perustuu siis sertifikaattipohjan ja ryhmäkäytännön asetuksiin. Automaattisesti jaetut sertifikaatit perustuvat versioiden 2 tai 3 pohjiin ja version 1 sertifikaatit pitää jakaa manuaalisesti. Manuaalisesti sertifikaatin voi hakea web-selaimella, certificates-työkalulla tai certreq-komentokehotetyökalulla.

Joskus tulee myös tilanne, että sertifikaatti täytyy ottaa pois käytöstä. Tällöin sertifikaatti laitetaan sulkulistalle. Syitä tähän voivat olla, että tietokone poistetaan käytöstä, työntekijä lähtee yrityksestä tai yksityinen avain on paljastunut. Sulkulista voi olla *full CRL* -tyyppinen tai *Delta CRL* -tyyppinen. *Full CRL* -lista pitää sisällään täydellisen listauksen sulkulistasta, joka julkaistaan oletuksena kerran viikossa. *Delta CRL* -lista pitää sisällään vain lisäykset, jotka julkaistaan oletuksena kerran päivässä. Ne ovat lisäyksiä jotka ovat tulleet *full CRL* -listan julkaisun jälkeen. Sertifikaattia käytettäessä voidaan sen voimassaolo tarkastaa. Tarkastaminen tapahtuu paikasta, jossa sulkulista on julkaistu. Julkaisupaikka löytyy itse tarkastettavan sertifikaatin kentistä. Julkaisupaikka on normaalisti web-palvelin tai aktiivihakemisto. Windows Server 2008 -käyttöjärjestelmässä on mahdollista määritellä OCSP-palvelin, jolta asiakas tarkistaa sertifikaatin voimassaolon reaaliaikaisesti. Tällöin ei tarvitse julkaista erillistä sulkulistaa. Aktiivihakemistoympäristössä myös palvelinten sertifikaatit julkaistaan aktiivihakemistossa. Tällöin toimialueen asiakkaat saavat palvelinten sertifikaatit ja sulkulistat automaattisesti ryhmäkäytännön avulla.

CA-palvelimella on normaalisti monta ylläpitäjää ja heillä jokaisella on oma roolinsa. Jakamalla roolit usealle henkilölle saadaan tietoturvaa kasvatetuksi. Ylläpitäjällä voi olla jokin tai vaikkapa kaikki seuraavista rooleista:

- **CA administrator** on vastuussa tilien hallinnoinnista ja avainparien luomisesta.
- **Certificate manager** on vastuussa sertifikaattien hallinnoinnista.
- **Auditor** on vastuussa loki-tietojen ylläpidosta ja tarkastamisesta.
- **Backup operator** on vastuussa PKI-järjestelmän tietojen varmuuskopioinnista.

CA-palvelimelle tehtävistä toimenpiteistä tulee tehdä dokumentointi. Lisäksi tulee määritellä varmuuskopiointi palvelimen tärkeistä asetuksista ja tietokannasta. Auditointi tulee määritellä, jotta myöhemmin voidaan tarkastella palvelimella suoritettuja toimenpiteitä.

Käyttäjille myönnetyt sertifikaatit ja niihin liittyvät yksityiset avaimet voidaan halutessa arkistoida CA:n tietokantaan. Tällöin avaimen kadotessa voidaan käyttäjän avain palauttaa tietokannasta. Jos näin käy, tulee käyttäjän sertifikaatti laittaa sulkulistalle ja luoda hänelle uusi sertifikaatti ja avaimet. Vanhalla avaimella käyttäjä saa salatut tiedostot auki, tiedostot salataan uudelleen uudella avaimella.

Sertifikaattipalvelimen levyjärjestelmä tulisi miettiä ja valita käytön mukaan. Offline-tilassa toimiva palvelin ei tarvitse niin tehokasta levyjärjestelmää kuin online-tilassa toimiva. Molemmissa tiloissa käyttöjärjestelmä tulisi erottaa tietokannasta ja loki-tiedostoista. Myös levytilaa tulee varata riittävästi.

Ennen PKI-ympäristön asentamista pitäisi tarkastaa **tietoturvakäytäntö** (security policy) ajan tasalle PKI:ta varten ja varmistaa että sellainen yleensäkin on olemassa. Tietoturvakäytännön tehtävä on informoida sekä sopia pelisäännöt koko yrityksen henkilöstölle työtehtävissä, kuinka tietoturva otetaan huomioon ja sitä sovelletaan. Lisäksi tulisi luoda **varmennepolitiikka** (certificate policy, CP), jossa kuvataan varmentajan keskeiset toimintaperiaatteet hyvin yleisellä tasolla. Varmennepolitiikkaa yksityiskohtaisempi kuvaus löytyy **varmennekäytäntölausumasta** (certificate practice statement - CPS). Varmennekäytäntölausuma on julkinen dokumentti. Siinä kuvataan erittäin tarkasti toimet ja tehtävät, jotka CA tekee tietoturva- ja varmennekäytäntöjen ylläpitämiseksi.

OID on ainutkertainen standardoitu (ISO/IEC 8824) numerosarja, jolla voidaan yksilöidä muun muassa organisaatioita, esineitä, laitteita, koodistoja, asiakirjoja ja ohjelmistoja maailmanlaajuisesti. PKI-järjestelmässä OID-tunnuksella voidaan yksilöidä esim. sertifikaattipohjat ja CPS. Jos PKI-sovelluksia käytetään ulkopuolisen organisaation kanssa, tulee OID-tunnukset hakea julkiselta OID-hallinnoijalta, jolloin voidaan varmistua, että tunnukset ovat yksilöllisiä Internetissä. Julkisia OID-tunnuksia myöntävät mm. IANA, ANSI ja eri maiden omat organisaatiot. Jos PKI-sovellukset ovat

yrityksen sisäisessä käytössä, voidaan käyttää Windowsin jo olemassa olevia tunnuksia.

Joskus organisaation sertifikaattien tulee olla luotettuja myös toisissa organisaatioissa. Tällaisia tilanteita voivat olla esimerkiksi salatun sähköpostin käyttö organisaatioiden välillä tai jos ohjelmistokoodi on allekirjoitettu toisen organisaation sertifikaatilla. Alla on lueteltu tapoja, joilla luottosuhde voidaan rakentaa:

- Varmenneluottolista (CTL / Certificate trust list)
- yhteinen juuri-CA
- ristiinsertifiointi (cross-certification)
- pätevä alaisuussuhde (qualified subordination)
- silta-CA (Bridge CA).

CA-palvelimen asennus on monivaiheinen tehtävä. Esim. juuri-CA:n asentaminen sisältää seuraavat vaiheet:

- asennus työryhmään
- capolicy.inf-tiedosto
- juuri-CA:n asennus ja sertifikaatin luonti
- juuri-CA:n sertifikaatin tarkastus
- aktiivihakemiston nimiavaruuden määrittäminen juuri-CA:n rekisteriin
- juuri-CA:n sulkulistan jakelupisteen määrittäminen
- juuri-CA:n sertifikaatin jakelupisteen konfigurointi
- juuri-CA:n sulkulistan julkaisuajan määrittäminen
- myönnettävien sertifikaattien voimassaoloajan konfigurointi
- sulkulistan uudelleenjulkaisu
- julkaistun sulkulistan varmistaminen
- auditoinnin määrittäminen.

Windows Server 2003- ja Windows Server 2008 -ympäristöjen suunnittelu ja asennus tapahtuu hyvin pitkälle samoilla periaatteilla. Suurin ero ympäristöjen välillä on mahdollisuus käyttää Suite B -algoritmeja Windows Server 2008 -ympäristössä.

LÄHDELUETTELO

[1] Brian Komar, Windows Server 2003 PKI and Certificate Security, Microsoft Press.

[2] Orin Thomas, Tony Northrup, Implementing and Administering Security in a Microsoft Windows Server 2003 Network, Microsoft Press.

[3] Windows Server 2003: Deployment Whitepapers: Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure, http://technet.microsoft.com/en-us/library/cc772670(WS.10).aspx.

[4] Windows Security –yhteisön kotisivut [verkkodokumentti]. Saatavissa: http://www.windowsecurity.com/articles/Microsoft-PKI-Quick-Guide-Part1.html
http://www.windowsecurity.com/articles/Microsoft-PKI-Quick-Guide-Part2-Design.html
http://www.windowsecurity.com/articles/Microsoft-PKI-Quick-Guide-Part3.html. [Viitattu 25.12.2010].

[5] Windows Server 2003 PKI Operations Guide –verkkodokumentti. Saatavissa:
http://technet.microsoft.com/en-us/library/cc787594(WS.10).aspx. [Viitattu 25.12.2010].

[6] Brian Komar, Windows Server 2008 PKI and Certificate Security, Microsoft Press.

[7] Request for Comments: RFC 2459 -dokumentti. [Viitattu 25.12.2010]. Saatavissa: www.ietf.org/rfc/rfc2459.txt.

[8] Microsoft Technet: Security Watch: PKI Enhancements in Windows [verkkodokumentti]. Saatavissa:
http://technet.microsoft.com/fi-fi/magazine/2007.08.securitywatch(en-us).aspx. [Viitattu 25.12.2010].

Sertifikaattipohjat (versio 1 ja 2):

Nimi	Käyttötarkoitus
Administrator	Allows user authentication, EFS encryption, secure e-mail, and certificate trust list signing.
Agent (Offline request)	the subject name in the request.
Authenticated Session	Authenticates a user to a Web server. The private key is used to sign the authentication request.
Basic EFS	Encrypts and decrypts data by using EFS. The private key is used to decrypt the file encryption key (FEK) that is used to encrypt and decrypt the EFS-protected data.
CA Exchange	Used to store keys that are configured for private key archival.
CEP Encryption	Allows the holder to act as a registration authority (RA) for Simple Certificate Enrollment Protocol (SCEP) requests.
Code Signing	Used to digitally sign software.
Cross Certification Authority.	Permits your organization to define qualified subordination constraints when issuing certificates to CAs outside of your organization's CA hierarchy.
Computer	Provides both client and server authentication abilities to a computer account. The default permissions for this template allow enrollment only by computers running Windows 2000 and Windows Server 2003 family operating systems that are not domain controllers.
Directory Email Replication	Allows domain controllers to use secure Simple Mail Transfer Protocol (SMTP) for replication.
Domain Controller	Authentication Used to authenticate Active Directory computers and users.
EFS Recovery Agent	Allows the subject to decrypt files previously encrypted with EFS.
Enrollment Agent	Used to request certificates on behalf of another subject.
Exchange Enrollment	Used to request certificates on behalf of another subject and supply
Exchange Signature Only	Used by Exchange Key Management Service to issue certificates to Microsoft Exchange Server users for digitally signing e-mail.
Exchange User	Used by Exchange Key Management Service to issue certificates to Exchange users for encrypting e-mail.
IPSEC	Provides certificate-based authentication for computers by using IP Security (IPSec) for network communications.
IPSEC (Offline request)	Used by IPSec to digitally sign, encrypt, and decrypt network communication when the subject name is supplied in the request.
Key Recovery Agent	Allows a CA to implement key archival and recovery. The Key Recovery Agent certificate is used to encrypt and decrypt the certificate and private key in the CA database.

RAS and IAS Server	Enables Remote Access Services (RAS) and Internet Authentication Services (IAS) servers to authenticate their identities to other computers.
Router (Offline request)	Used by a router when requested through SCEP from a certification authority that holds a Certificate Enrollment Protocol (CEP) Encryption certificate.
Smartcard Logon	Authenticates a user with the network by using a smart card.
Smartcard User	Identical to the Smartcard Logon template, except that it can also be used to sign and encrypt e-mail.
Trust List Signing	Allows the holder to digitally sign a trust list.
User	Used by users for e-mail, EFS, and client authentication.
User Signature Only	Allows users to digitally sign data.
Web Server	Authenticates the Web server to connecting clients. The connecting clients use the public key to encrypt the data that is sent to the Web server when using Secure Sockets Layer (SSL) encryption.
Workstation	Enables client computers to authenticate their identities to Authentication servers.

Sertifikaattipalvelun tapahtuma-ID:t (Event IDs)

772. The Certificate Manager denied a pending certificate request.
773. Certificate Services received a resubmitted certificate request.
774. Certificate Services revoked a certificate.
775. Certificate Services received a request to publish the certificate revocation list.
776. Certificate Services published the certificate revocation list (CRL).
777. A certificate request extension changed.
778. One or more certificate request attributes changed.
779. Certificate Services received a request to shut down.
780. Certificate Services backup started.
781. Certificate Services backup completed.
782. Certificate Services restore started.
783. Certificate Services restore completed.
784. Certificate Services started.
785. Certificate Services stopped.
786. The security permissions for Certificate Services changed.
787. Certificate Services retrieved an archived key.
788. Certificate Services imported a certificate into its database.
789. The audit filter for Certificate Services changed.
790. Certificate Services received a certificate request.
791. Certificate Services approved a certificate request and issued a certificate.
792. Certificate Services denied a certificate request.
793. Certificate Services set the status of a certificate request to pending.
794. The Certificate Manager settings for Certificate Services changed.
795. A configuration entry changed in Certificate Services.
796. A property of Certificate Services changed.
797. Certificate Services archived a key.
798. Certificate Services imported and archived a key.
799. Certificate Services published the CA certificate to Active Directory.
800. One or more rows has been deleted from the certificate database.
801. Role separation enabled.

Muuttujat (replacement tokens)

TOKEN NAME	DESCRIPTION	WINDOWS 2000 MAP VALUE	WINDOWS SERVER 2003 MAP VALUE
SERVERDNSNAME	THE DNS NAME OF THE CA SERVER	%1	% 1
SERVERSHORTNAME	THE NETBIOS NAME OF THE CA SERVER	%2	% 2
CANAME	THE NAME OF THE CA	%3	% 3
CERT_SUFFIX	THE RENEWAL EXTENSION OF THE CA	%4	N/A
CERTIFICATENAME		N/A	% 4
DOMAIN_NAME	THE LOCATION OF THE DOMAIN ROOT IN ACTIVE DIRECTORY	%5	N/A
(NOT USED)		N/A	% 5
CONFIGURATION-CONTAINER	THE LOCATION OF THE CON-FIGURATION CONTAINER IN ACTIVE DIREC-TORY	%6	% 6
CATRUNCATEDNAME	THE "SANITIZED" NAME OF THE CA, 32 CHARAC-TERS WITH A HASH ON THE END	%7	% 7
CRLNAMESUFFIX	THE RENEWAL EXTENSION FOR THE CRL	%8	% 8

DELTACRLALLOWED	%9
CDPOBJECTCLASS	% 10
CAOBJECTCLASS	% 11

Näitä muuttujia käytetään mm. CAPolicy.inf-tiedostossa sekä Certification Authority -konsolissa määrittelemään CA-laajennokset (CA Extensions)