

7.1.1 EFS - 2

Sunday, November 23, 2025 19:29

HARJOITUS TEEMA JATKUU - START HERE;

Tämä harjoitus jatkuu - tästä löytyy sama ohje ja video youtubestä.

The screenshot shows a list of four Microsoft WebCast videos from the Windows Server 2019 channel:

- Video 15: "Encrypting User Data with EFS in Active Directory" (Duration: 10:30)
- Video 16: "Setting up EFS with Group Policy and Certificate Authority" (Duration: 16:03)
- Video 17: "How to Backup and Restore EFS certificates" (Duration: 16:47)
- Video 18: "Configure EFS Data Recovery Agent using Group Policy" (Duration: 8:5K views)

Num. 15 on ainakin ensimmäisen konffausta steppi miten se menee , ja testaa toisella käyttäjällä avattessaan sitä txt tiedostoa. Sekä mahdollinen koskien toisella käyttäjällä on oikeus konffata omansa salaus kansion ja sisältyen sisäisen tiedostonsa.

Tämä harjoitus jatkuu num. 16 ja siitä 18 asti - kuitenkin tästä jatkuu **GPO policy EFS kanssa aja sertifikaatti autentikointi**.

Windows serveristä avaa ja etsi "certification authority" josta löytyy sertifikaatti dataa ja ikään kuin sopimuksia.

- Jos tästä ei ole esiasennettu niin kannattaa ladata (server manager >> Manage >> add roles and features wizard >> Server roles: **AD Certificate services**)

⌚ Mikä AD CS on ja miksi se on tärkeää

- Active Directory Certificate Services (AD CS) tarjoaa organisaatiolle oman **sertifikaattiviranomaisen (CA)**.
- Sen avulla voidaan myöntää, hallita ja perusttaa digitaalisia sertifikaatteja, joita käytetään mm.:
 - Käyttäjien ja koneiden todennukseen (smart card, Kerberos, VPN).
 - Salaustratkaisuihin kuten **EFS (Encrypting File System)** ja **BitLocker Network Unlock**.
 - Palveluiden suojaamiseen (IIS, RDP, Wi-Fi, VPN).
 - Hybridimallissa myös sisäisten ja ulkoisten palveluiden yhdistämiseen.

📁 AD CS ja EFS

- EFS voi toimia ilman AD CS:ää, mutta silloin avainten hallinta ja palautus on hankalampaa.
- AD CS mahdollistaa **Key Recovery Agent (KRA)** -sertifikaattien käytön, jolloin yritys voi palauttaa salattuja tiedostoja jos käyttäjä menettää avaimensa.
- Ilman CA:ta EFS on riskialttimpi, koska avaimen katoaminen = tiedostojen menetyks.

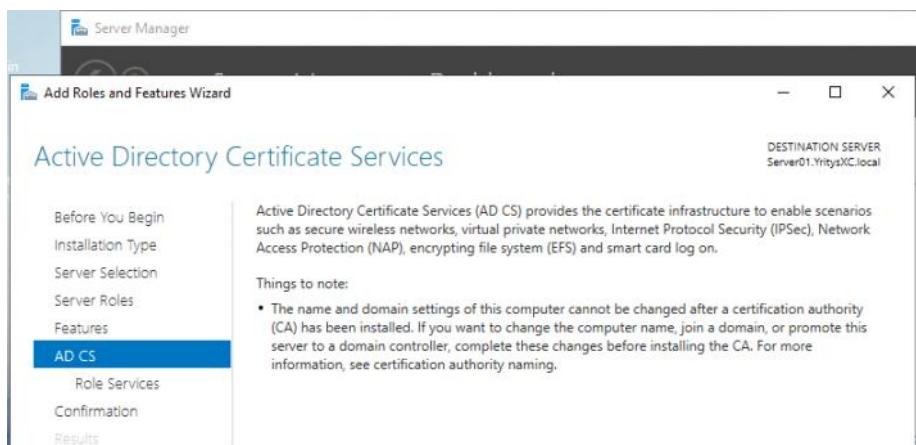
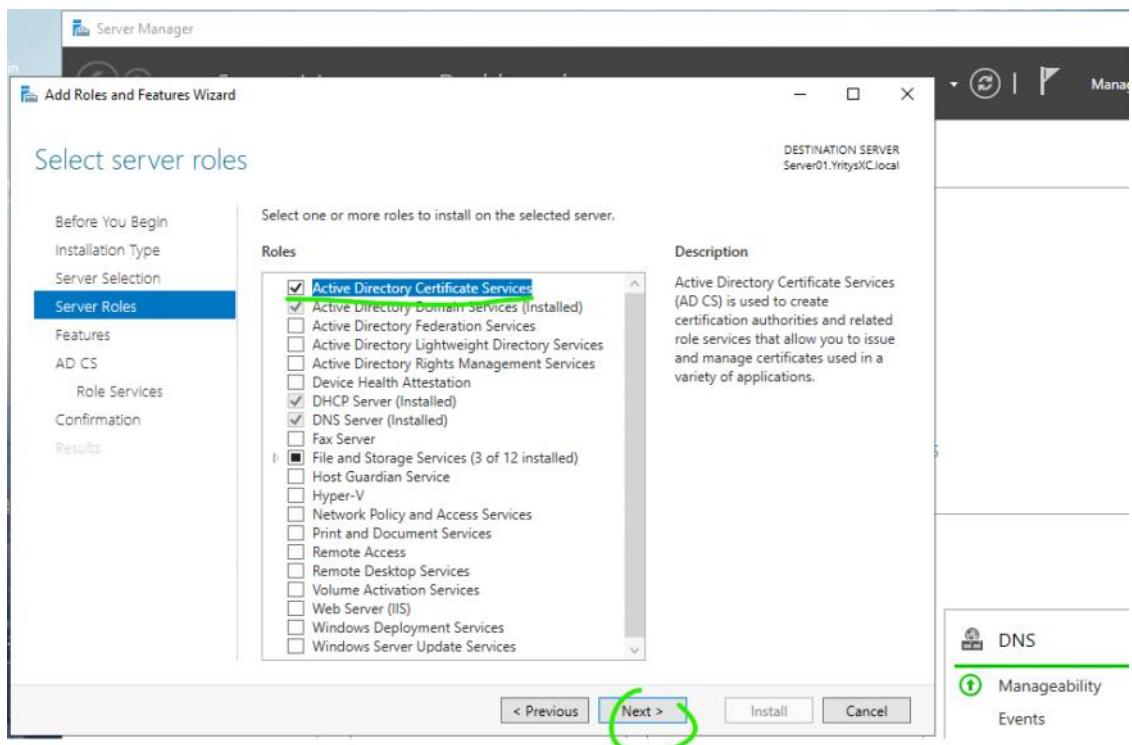
🏢 Käytötarve eri kokoisissa organisaatioissa

Organisaatiotyyppi	AD CS:n merkitys	Käyttöesimerkkejä
Pieni yritys	Ei aina väittämätön. Usein riittää kolmannen osapuolen SSL-sertifikaatit ja peruskäyttäjien salaus.	VPN-sertifikaatit, EFS palautus vain jos halutaan varmistaa tiedostojen säilyvyys.
Keskisuuri yritys	Suositeltava. Kasvava määrä palveluita ja käyttäjiä → oma CA helpottaa hallintaa.	Wi-Fi todennus, RDP, sisäiset web-palvelut, EFS avainten palautus.
Suuri yritys	Käytännössä väittämätön. Tarvitaan keskitetty sertifikaattien hallinta.	Automaattinen sertifikaattien jakelu GPO:lla, hybridimallit (Azure AD + on-prem), PKI-integraatiot.
Hybridimalli (cloud + on-prem)	AD CS integroituu Azure AD:hen ja MDM-ratkaisuihin.	Sertifikaatit mobiililaitteille, VPN ja Wi-Fi, sisäiset palvelut.
Fyysinen on-prem ympäristö	AD CS on klassinen ratkaisu.	Kaikki sisäiset palvelut, EFS, BitLocker Network Unlock.

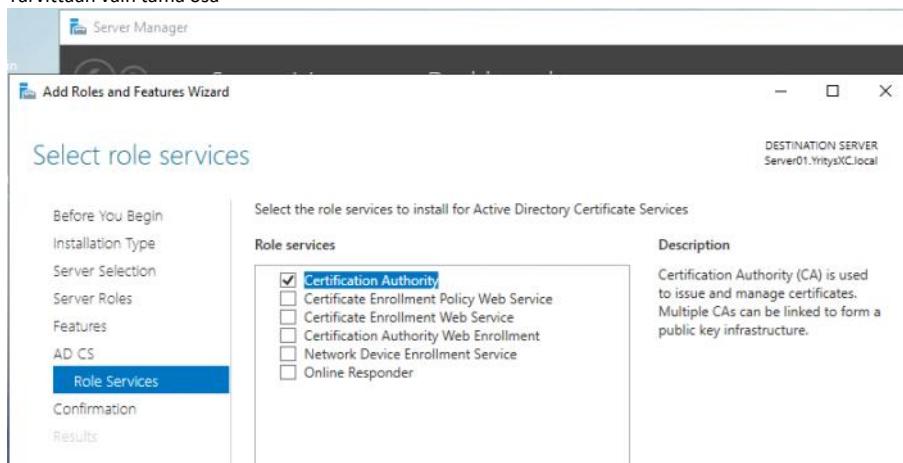
⌚ Yhteenveto

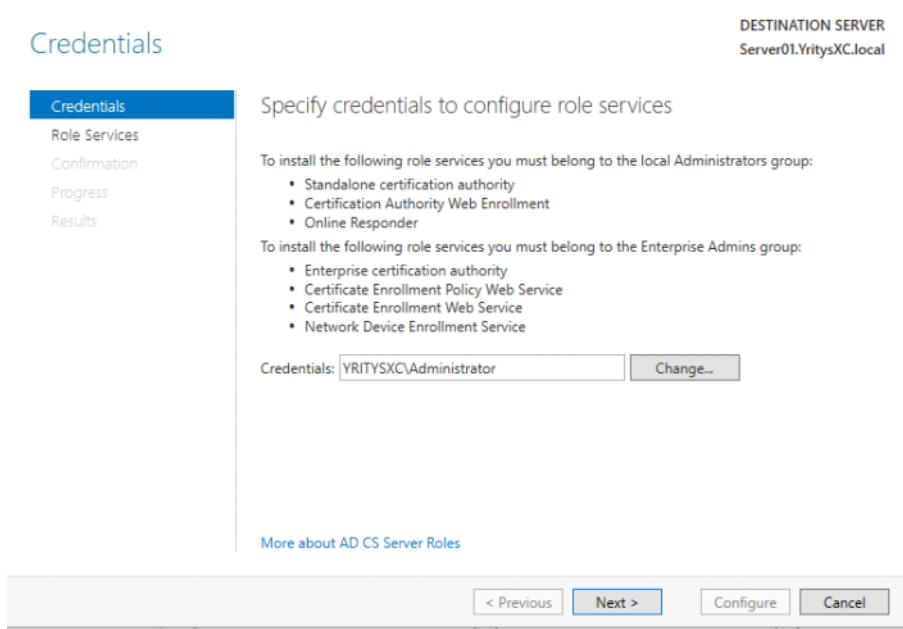
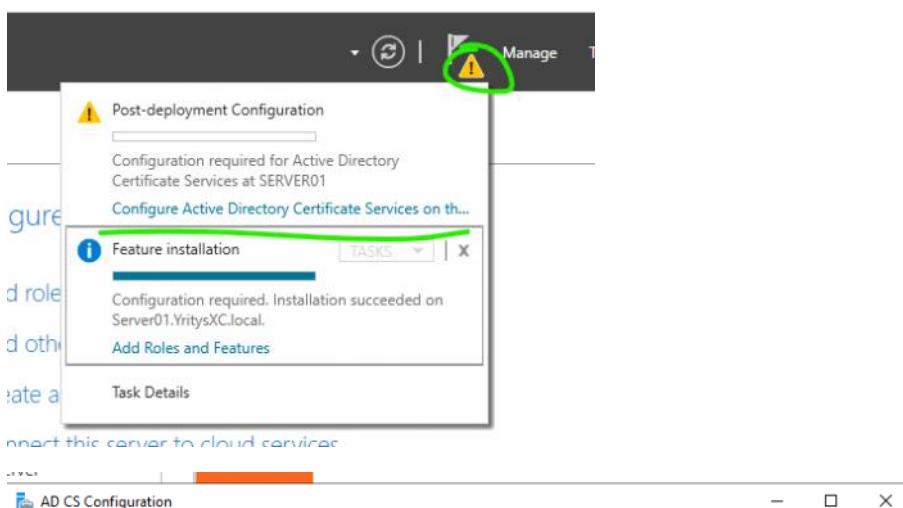
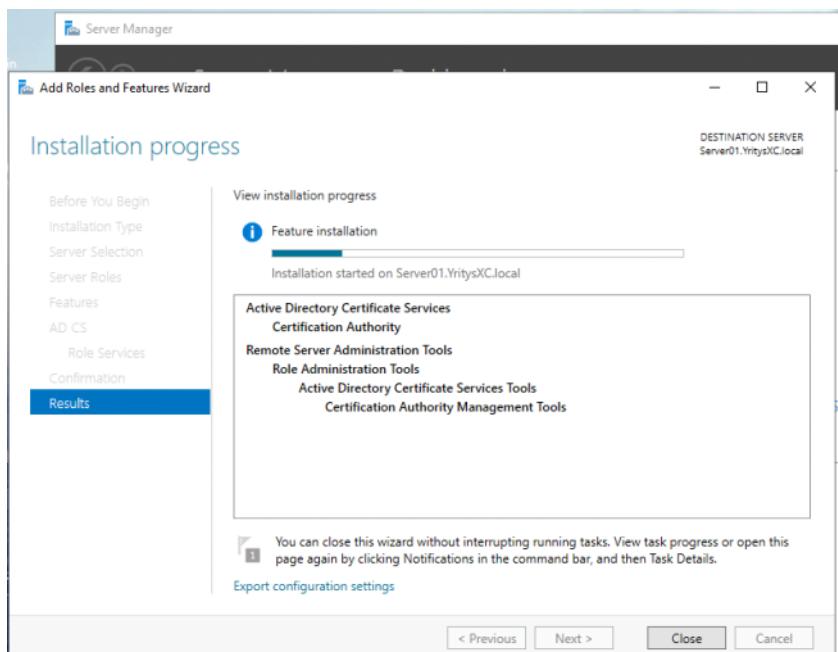
- Pienessä firmassa AD CS ei ole pakollinen, mutta tuo turvaa EFS:n ja sisäisten palveluiden hallintaan.
- Keskisuurissa ja suurissa yrityksissä AD CS on käytännössä standardi, koska sertifikaattien hallinta ilman omaa CA:ta on vaikeaa.
- **EFS:n kanssa** AD CS ei ole teknisesti pakollinen, mutta se tekee avainten palautuksesta ja hallinnasta realistista.
- **Hybridimallissa** AD CS yhdistyy pilvipalveluihin ja tuo hallittavuutta.

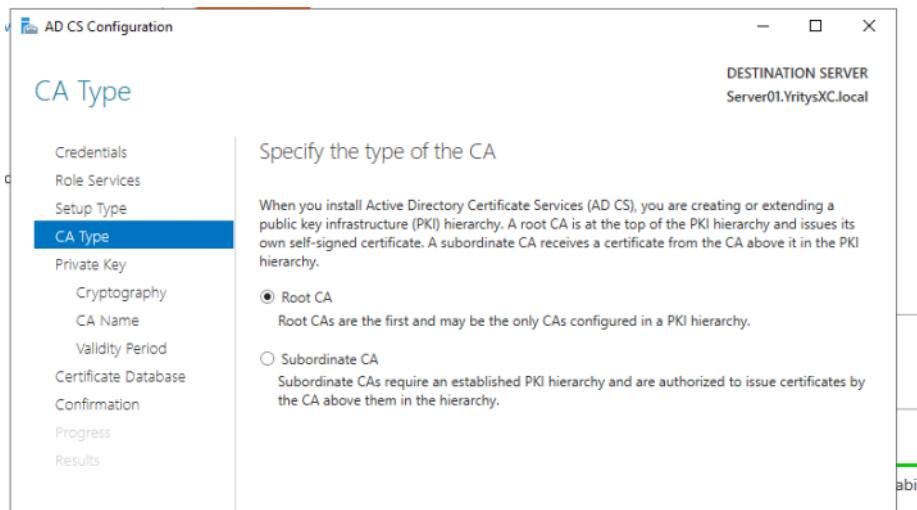
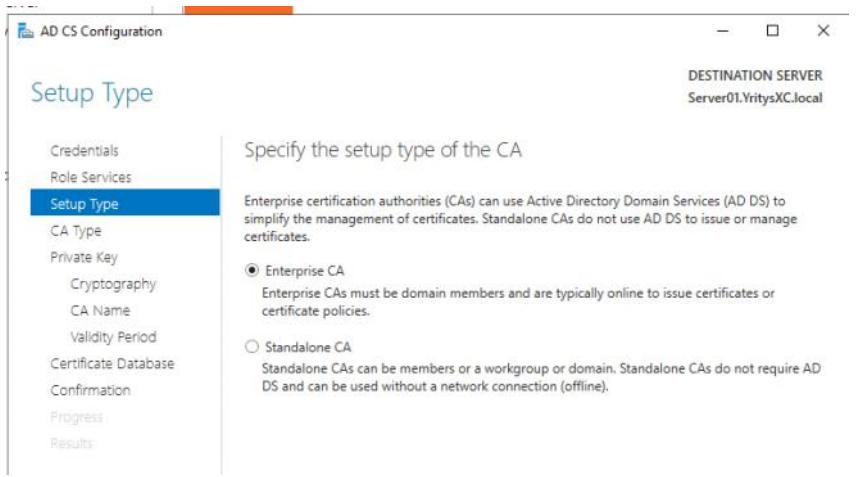
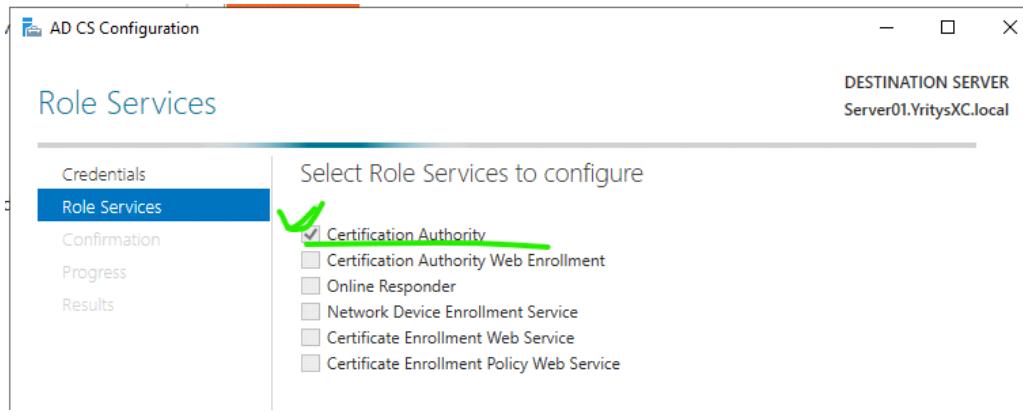
- Noissa aikaisemmassa asetuksissa ei ole mitään kummalista, että suoraan next ja "role-based or feature-based installation"
- Features - suoraan NEXT

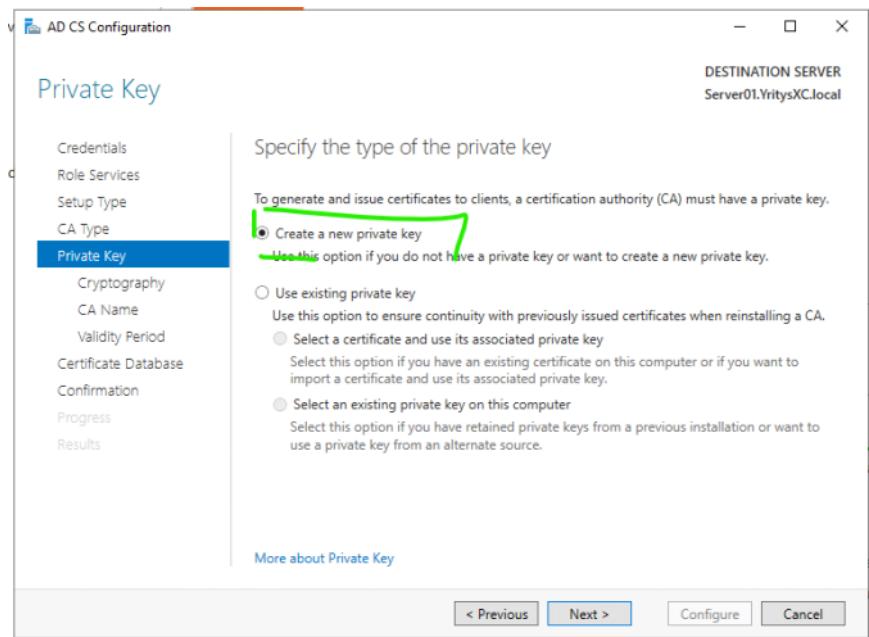


- Tarvitaan vain tämä osa

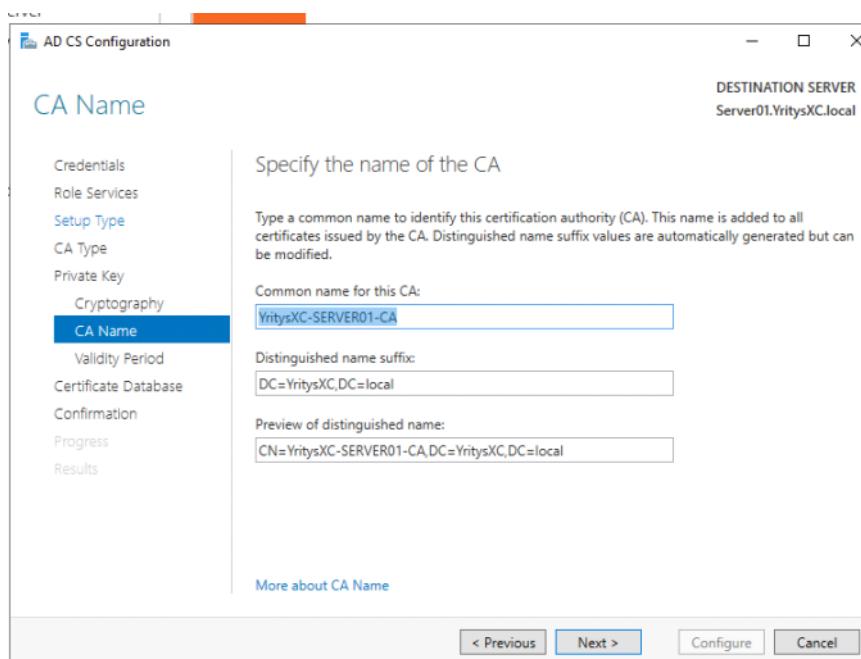
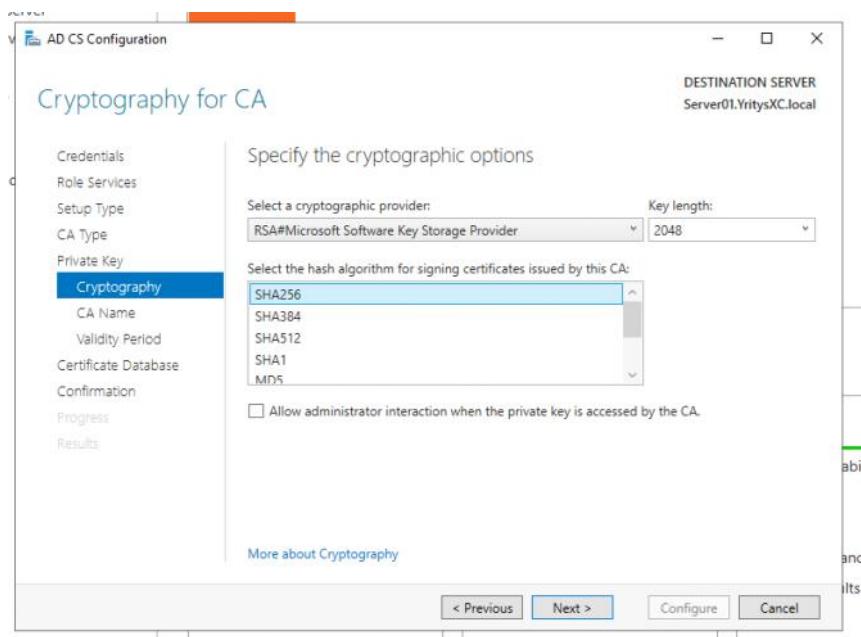




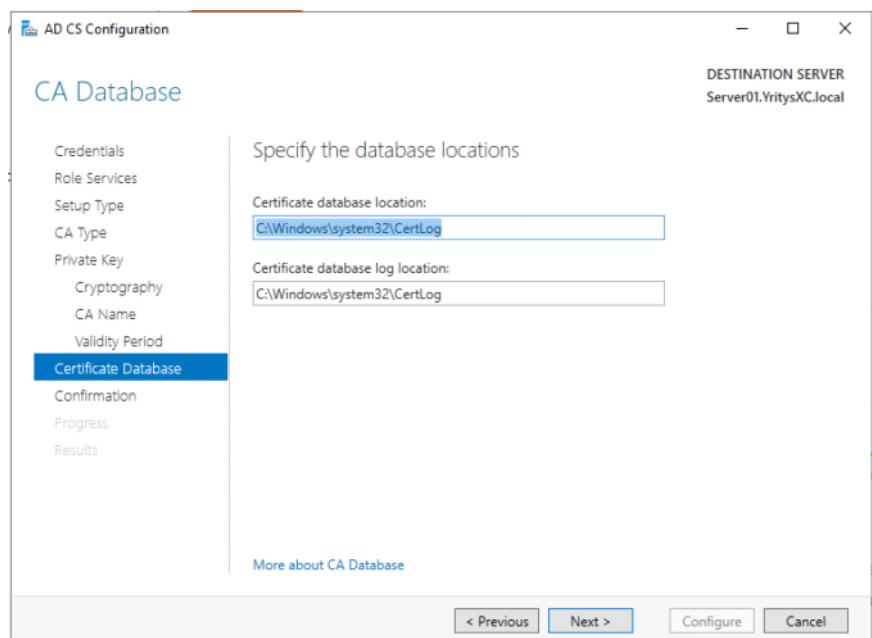
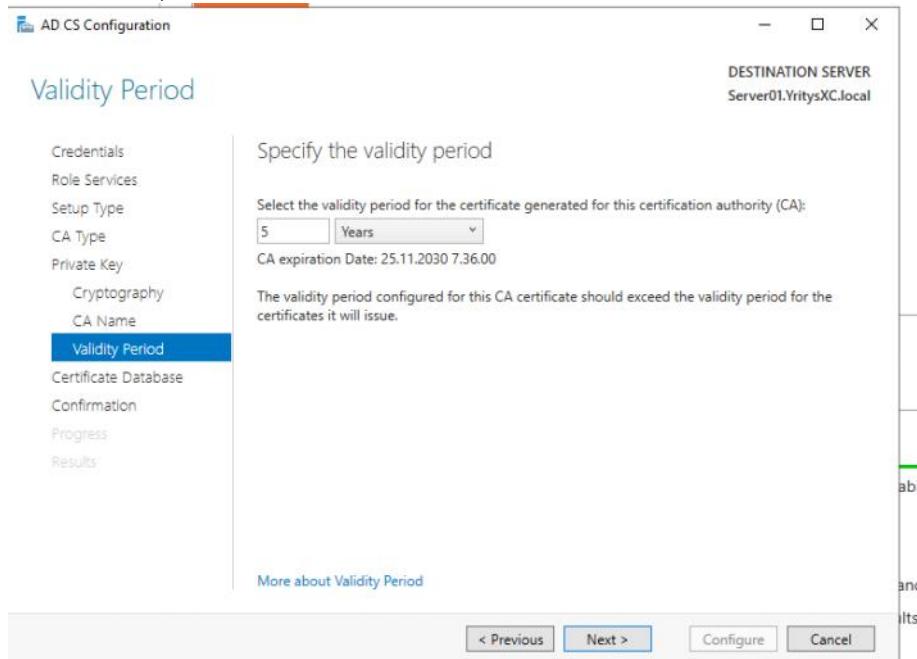




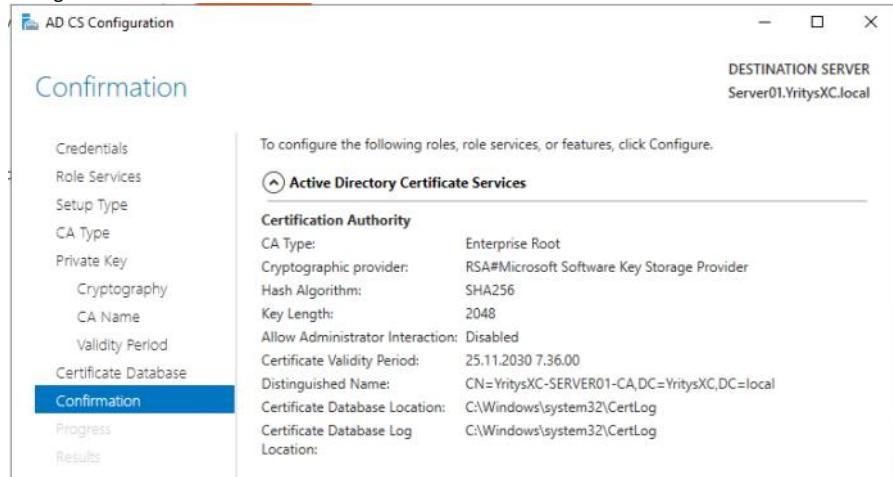
Valitaan oletuksena tämä

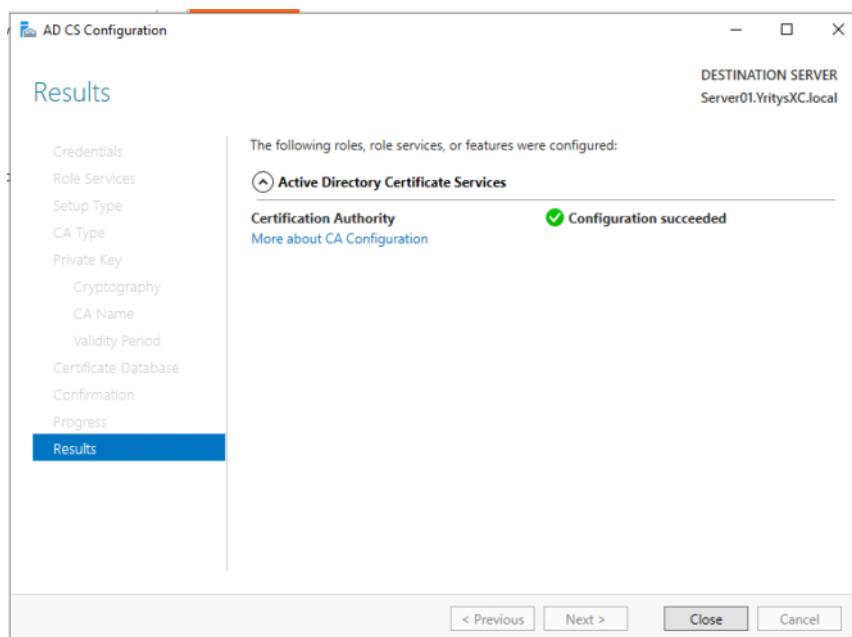
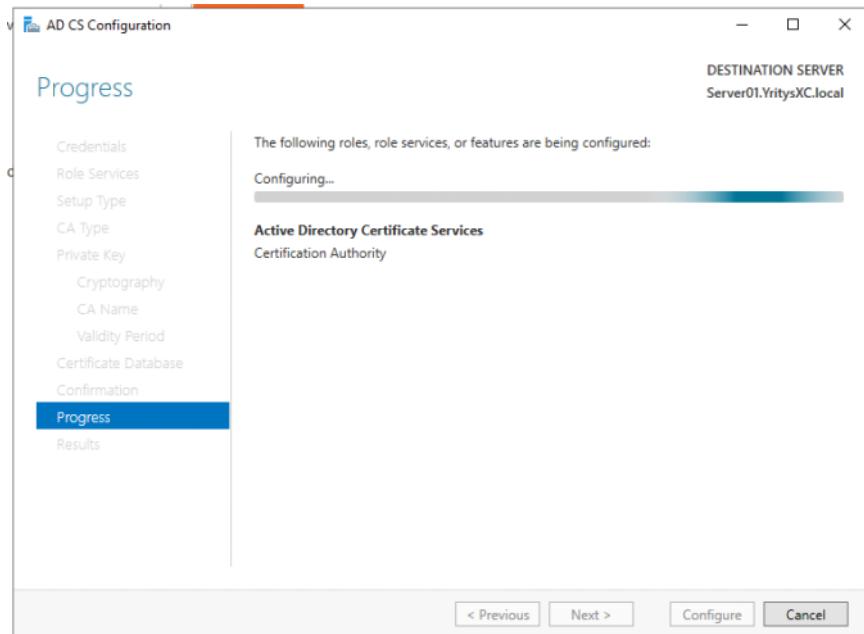


Voisin laittaa 10v , mutta mennään oletus 5v



- Configure seuraavaksi



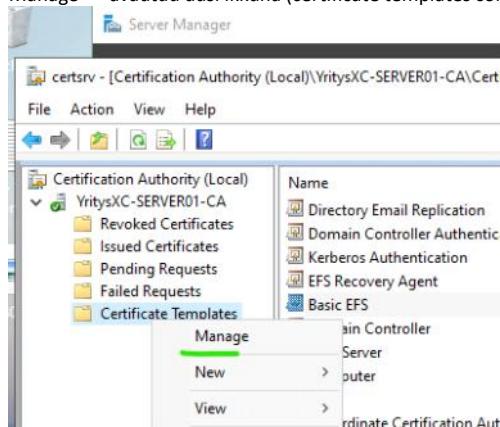


- DONE!!

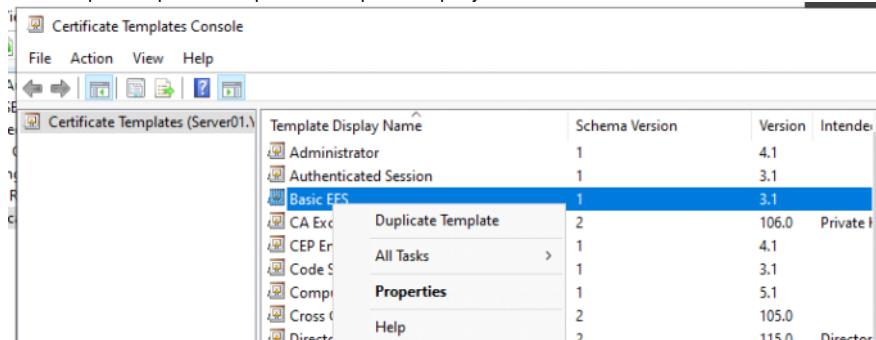
The screenshot shows the 'Active Directory Administrative Center' interface. The left navigation pane includes options like Active Directory Administrative Center, Active Directory Domains and Trusts, Active Directory Module for Windows PowerShell, Active Directory Sites and Services, Active Directory Users and Computers, ADSI Edit, Certification Authority (which is selected and highlighted with a green underline), Component Services, Computer Management, and Defragment and Optimize Drives. The main pane shows the 'certsrv - [Certification Authority (Local)]' window with a table of certificates. The table has columns for Name and Description. One entry is visible: 'Name' is 'YritysXC-SERVER01-CA' and 'Description' is 'Certification Authority'. The table also includes icons for Revoked Certificates, Issued Certificates, Pending Requests, Failed Requests, and Certificate Templates.

Tässä nähdään on olemassa Basic EFS, ja tehtävässä/harjoituksessa luodaan "custom EFS" muotoinen teema.

Manage >> avautuu uusi ikkuna (certificate templates console)

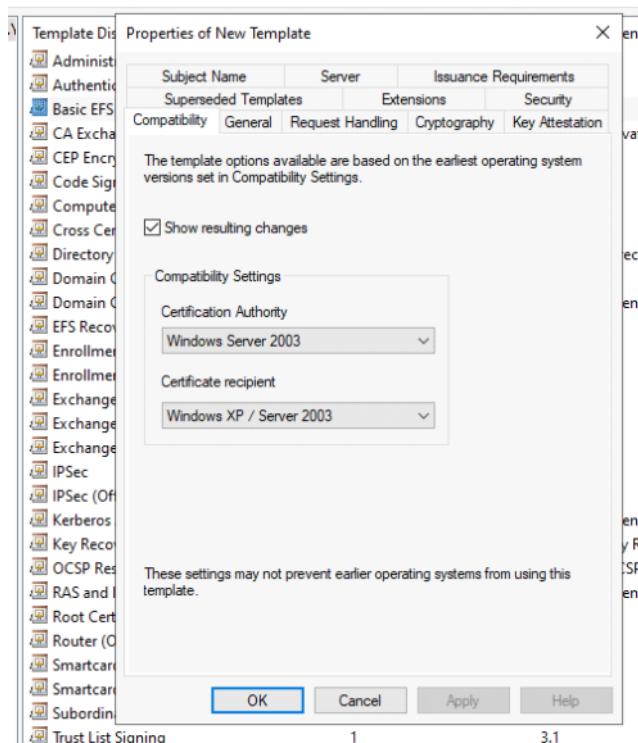


Tehdään pieni duplicate template - eli kopio tästä pohjasta kuin



Tämä on ensimmäinen oletus näkymänsä ja tästä valitetaan osa muutoksia

- Certification authority: Windows server 2016
 - Siinä ponnahtaa ilmoitus ja OK vaan
- Sama idea certification recipient: windows server 2016
 - Sama ponnahtaa ilmoitus ja OK



Template Dis Properties of New Template

Subject Name	Server	Issuance Requirements
Superseded Templates	Extensions	Security
Compatibility	General	Request Handling Cryptography Key Attestation

The compatibility changes will add the following template options.

Tab	Template Option
Server	Do not store certificates and requests in the CA database
Server	Do not include revocation information in issued certificates

Actions

- Certificate
- More
- Basic EFS

Resulting changes

The compatibility changes will add the following template options.

Tab	Template Option
Request Handling	For automatic renewal of smart card certificates, use the existing key if a new .
Request Handling	Renew with the same key
Cryptography	Use alternate signature format
Cryptography	Key Storage Provider
Key Attestation	Required, if client is capable
Key Attestation	Required
Key Attestation	User credentials
Key Attestation	Hardware certificate
Key Attestation	Hardware key
Key Attestation	Perform attestation only (do not include issuance policies)

Actions

- Certificate
- More
- Basic EFS

Copy to clipboard OK Cancel

Root Cert

Properties of New Template

Subject Name	Server	Issuance Requirements
Superseded Templates	Extensions	Security
Compatibility	General Request Handling Cryptography Key Attestation	

The template options available are based on the earliest operating system versions set in Compatibility Settings.

Show resulting changes

Compatibility Settings

Certification Authority: Windows Server 2016

Certificate recipient: Windows 10 / Windows Server 2016

These settings may not prevent earlier operating systems from using this template.

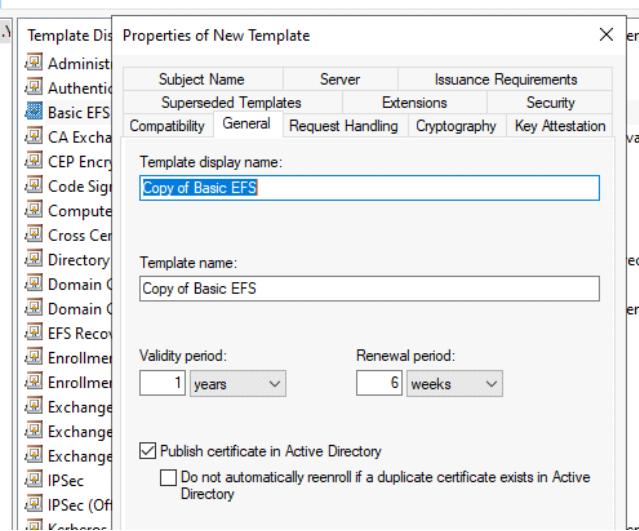
OK Cancel Apply Help

1 3.1

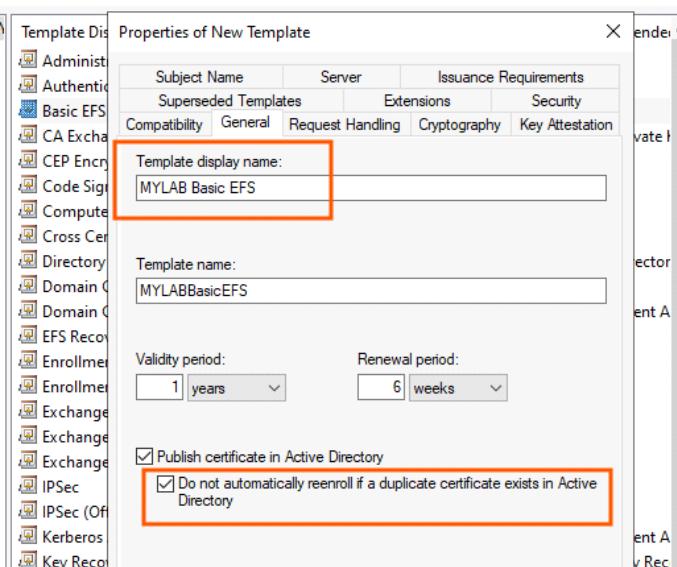
Seuraavaksi "General" polkuun

Assign - template display nimi - eli nimi muutos

BEFORE:



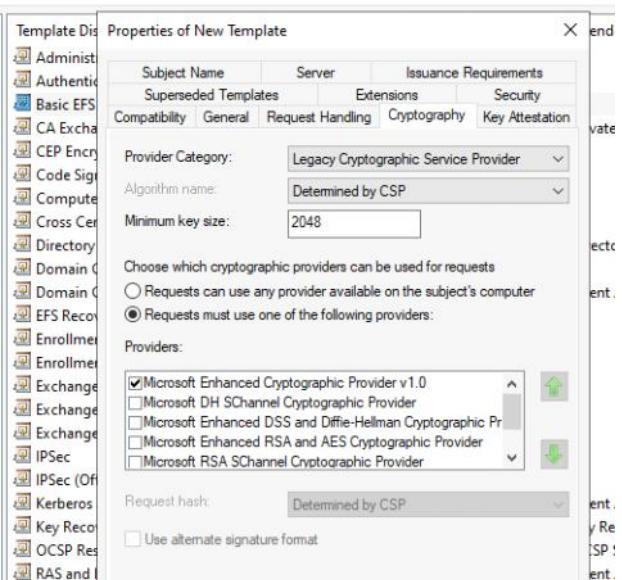
AFTER:



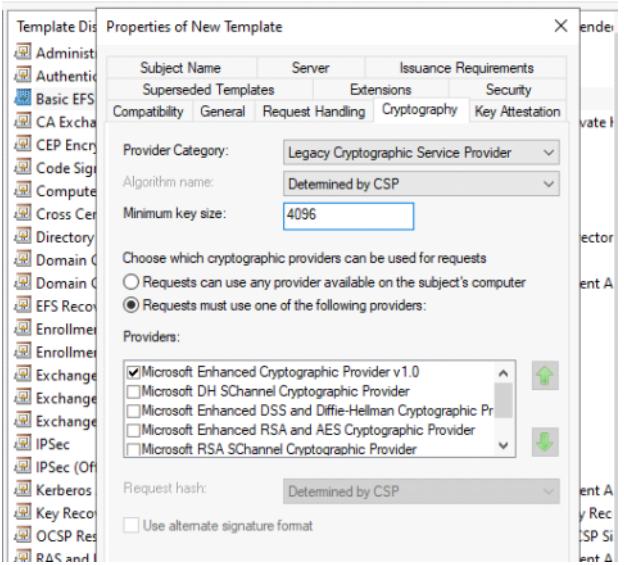
Seuraavaksi "cryptography" polkuun

Täältä haluttaan muuttaa se avain koko

BEFORE: 2048

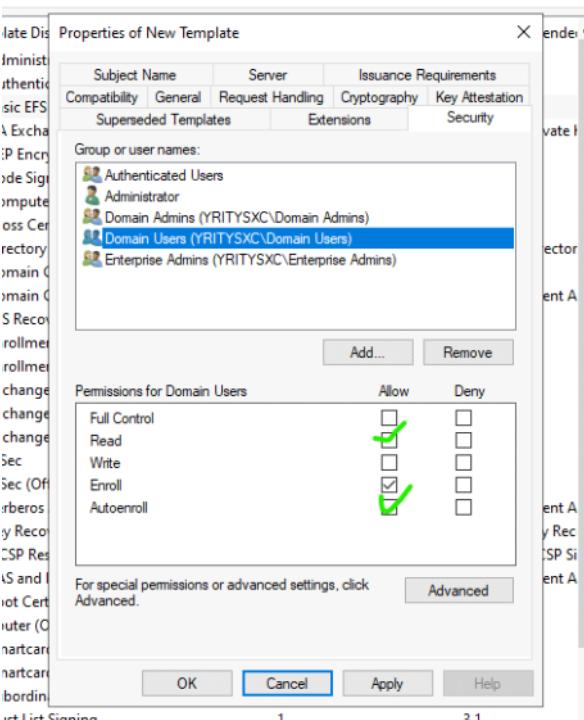


AFTER:



Seuraavaksi "security" polkuun

Määritettään tälle käyttäjälle vähä lisä oikeutta (ruksi mukaan)



Kaikki on kunnossa, sitten "Apply" ja "OK" - asetusket.

Viimeisenä se tulee tuohon listan alle, sekä jos on muutettavaa tietoa niin kaksois klikkaus ja "properties" niin avaa saman näkymänsä kuin aikaisemmin konfiguroitut/määritettyt asetukset.

- Vain nimeämässä "template display name" ei voi muuttaa paitsi ellei poista täitä kokonaista sertifikaatti tietoa

Certificate Templates Console

File Action View Help

The screenshot shows a table of certificate templates with columns: Template Display Name, Schema Version, Version, and Intended Purposes. The 'MYLAB Basic EFS' template is selected.

Template Display Name	Schema Version	Version	Intended Purposes
Code Signing	1	3.1	
Computer	1	5.1	
Cross Certification Authority	2	105.0	
Directory Email Replication	2	115.0	Director
Domain Controller	1	4.1	
Domain Controller Authentication	2	110.0	Client A
EFS Recovery Agent	1	6.1	
Enrollment Agent	1	4.1	
Enrollment Agent (Computer)	1	5.1	
Exchange Enrollment Agent (Offline requ...)	1	4.1	
Exchange Signature Only	1	6.1	
Exchange User	1	7.1	
IPSec	1	8.1	
IPSec (Offline request)	1	7.1	
Kerberos Authentication	2	110.0	Client A
Key Recovery Agent	2	105.0	Key Rec
OCSP Response Signing	3	101.0	OCSP Si
RAS and IAS Server	2	101.0	Client A
Root Certification Authority	1	5.1	
Router (Offline request)	1	4.1	
Smartcard Logon	1	6.1	
Smartcard User	1	11.1	
Subordinate Certification Authority	1	5.1	
Trust List Signing	1	3.1	
User	1	3.1	
User Signature Only	1	4.1	
Web Server	1	4.1	
Workstation Authentication	2	101.0	Client A
MYLAB Basic EFS	4	100.3	Encrypting File System

Seuraavaksi halutaan luoda kuin olemassa oleva sertifikaatti tieto ja julkaisata sitä

Certificate Authority (Local)

YritysXC-SERVER01-CA

- Revoked Certificates
- Issued Certificates
- Pending Requests
- Failed Requests
- Certificate Templates**

Manage Controller

New > Certificate Template to Issue

View > Certificate Template to Issue

Valitaan template mikä ja mille, ja valitetaan äskettäinen luotu "MYLAB"

Certification Authority (Local)

YritysXC-SERVER01-CA

Select one Certificate Template to enable on this Certification Authority.

Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.

All of the certificate templates in the organization may not be available to your CA.

For more information, see [Certificate Template Concepts](#).

Name	Intended Purpose
Exchange User	Secure Email
IPSec	IP security IKE intermediate
IPSec (Offline request)	IP security IKE intermediate
Key Recovery Agent	Key Recovery Agent
MYLAB Basic EFS	Encrypting File System
OCSP Response Signing	OCSP Signing
RAS and IAS Server	Client Authentication, Server Authentication
Router (Offline request)	Client Authentication
Smartcard Logon	Client Authentication, Smart Card Logon
Smartcard User	Secure Email, Client Authentication, Smart Card Logon

OK Cancel

Ja se tulee täähän listan alle ja näkyviinsä

The screenshot shows the Windows Certificates snap-in window titled 'certsrv - [Certification Authority (Local)\YritysXC-SERVER01-CA\Certificate Templates]'. The left pane displays a tree view of certificates under 'Certification Authority (Local) \ YritysXC-SERVER01-CA \ Certificate Templates'. The right pane lists certificate templates with their names and intended purposes:

Name	Intended Purpose
MYLAB Basic EFS	Encrypting File System
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System

Seuraavaksi kohti GPO asetuksia:

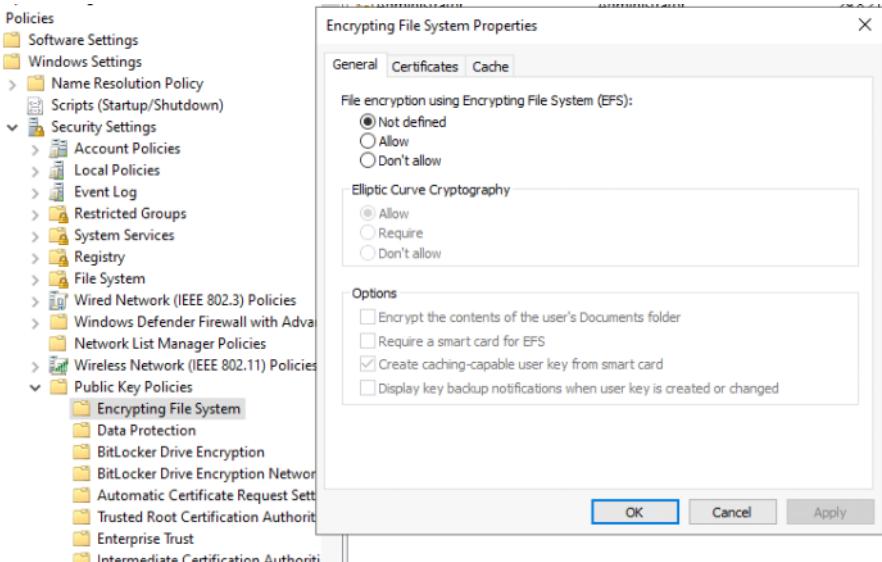
Tästä GPO asetuksesta tullaan muokkaa "default domain policy" alle.

The screenshot shows the 'Group Policy Management' console window. In the left pane, under 'Forest: YritysXC.local \ Domains \ YritysXC.local', the 'Default Domain Policy' is selected. A context menu is open over it, with the 'Edit...' option highlighted.

Sitten mennään tällaiseen polkuun ja oikea klikkaus ja valitse "properties"

The screenshot shows the 'Group Policy Management Editor' window. The left pane shows the policy structure under 'Default Domain Policy [SERVER01.YRITYSC.LOCAL] Policies \ Computer Configuration \ Policies \ Security Settings \ Encrypting File System'. A context menu is open over the 'Encrypting File System' folder, with the 'Properties' option highlighted.

BEFORE:



TÄHÄN VÄLIIN KESKEYTYS KOSKA EI TIEDETÄ JOS KONFIGUROIDAAN TÄMÄ ASETUS - NIIN EI KERRO MITÄ TAPAHTUU SEURAAVAKSI:

- EFS:n (Encrypting File System) GPO-asetukset tuoo kokoajan vähän hämmentäviä asetuksia

Vaihtoehdot: Not Defined, Allow, Don't Allow

- **Not Defined**
 - Tämä tarkoittaa, että kyseinen GPO ei otta kantaa EFS:ään.
 - Käyttäjät voivat edelleen käyttää EFS:ää, jos se on sallittu paikallisesti tai muissa käytännöissä.
 - Käytännössä: ei muutosta oletuskäytätyymiseen.
- **Allow**
 - Sallii käyttäjien käyttää EFS:ää tiedostojen ja kansioiden salaamiseen.
 - Tämä on se asetus, jos haluat että EFS on käytettäväissä domainissa.
 - Yhdessä AD CS:n kanssa voit hallita avainten varmuuskopointia ja palautusta.
- **Don't Allow**
 - Estää EFS:n käytön kokonaan.
 - Käyttäjät eivät voi salata tiedostoja/kansioita EFS:llä.
 - Tämä voi olla järkevää, jos organisaatio käyttää muita salausratkaisuja (esim. BitLocker) tai haluaa välttää EFS:n hallinnan monimutkaisuutta.

Asetus: Display key backup notifications when user key is created or changed

- Kun käyttäjä luo uuden EFS-avaimen (esim. ensimmäisen kerran kun hän salaa tiedoston), Windows voi näyttää **ilmoitusta**, että avain tulisi varmuuskopioida.
- Sama tapahtuu, jos avain **muuttuu** (esim. käyttäjäprofiiliin uudelleenluonti, avaimen resetointi).
- Ilmoitus ohjaa käyttäjää varmuuskopioimaan avaimen (esim. tallentamaan sen sertifikaattina tai käyttämään CA:n Key Recovery Agentia).
- Ilman varmuuskopiota: jos avain katoaa, salatut tiedostot menetetään. Tämä on se kriittinen riski EFS:ssä.

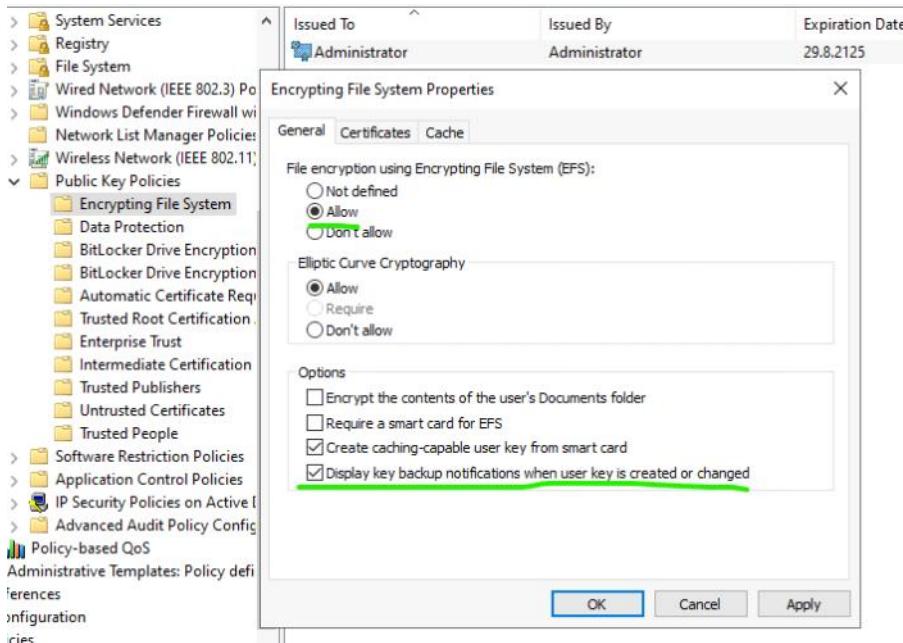
Käytännön merkitys

- **Pienessä firmassa:** jos EFS sallitaan, kannattaa ehdottomasti ottaa tämä ilmoitus käyttöön → käyttäjät muistavat varmuuskopioida avaimensa.
- **Keskisuri/suuri yritys:** yleensä hallitaan keskitetysti AD CS:n kautta, jolloin avainten varmuuskopointi hoidetaan automaattisesti Key Recovery Agentin avulla.
- **Jos asetat Don't Allow:** ilmoitus ei ole relevantti, koska EFS ei ole käytössä.

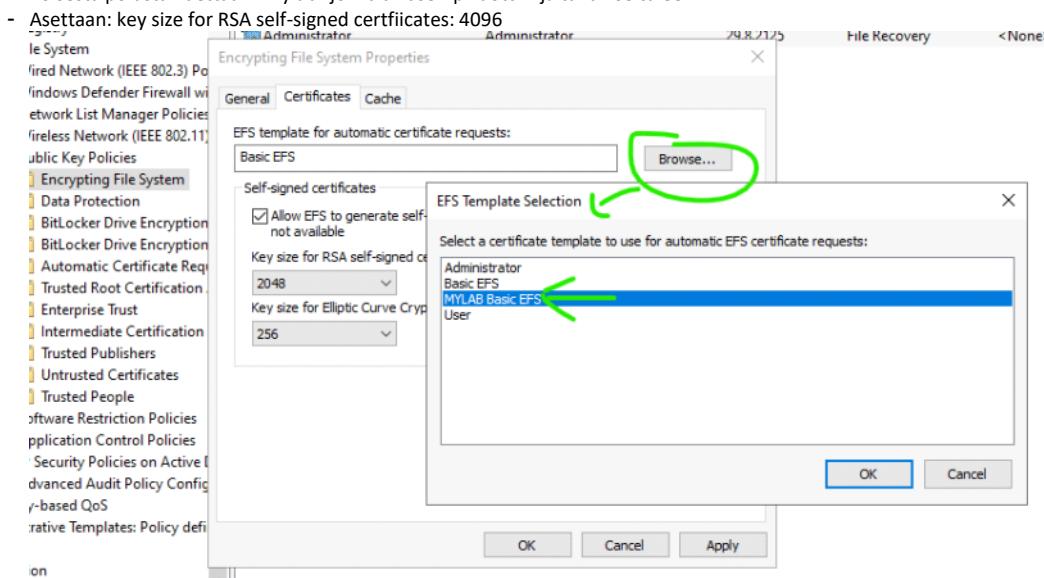
- **Not Defined** = ei muutosta, EFS toimii oletusten mukaan.
- **Allow** = EFS sallitaan.
- **Don't Allow** = EFS estetään.
- **Display key backup notifications...** = käyttäjälle tulee muistutus varmuuskopioida avain, jotta salatut tiedostot eivät katoa avaimen hävitessä.

HARJOITUS DEMO JATKUU - START HERE;

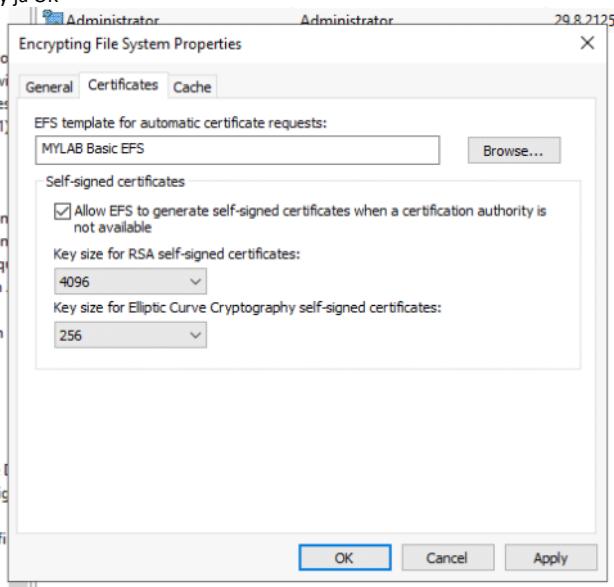
Asettaan olevat asetukset eli tämä:



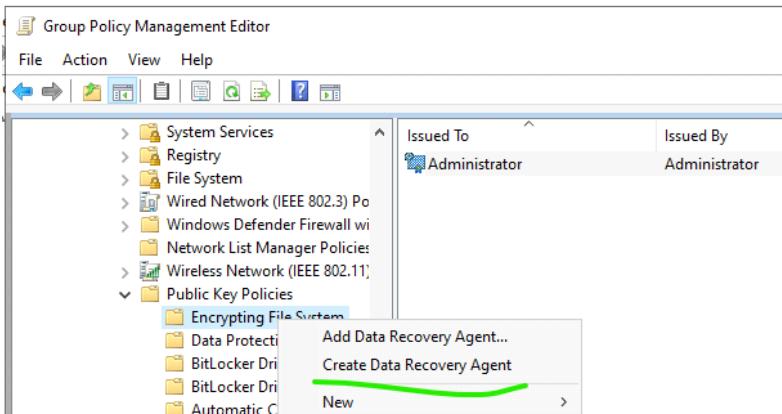
Toisesta polusta haetaan "mylab" jonka aikasempi luottiin ja tähän se tulee



- Apply ja OK



Seuraavaksi luodaan data recovery agentti



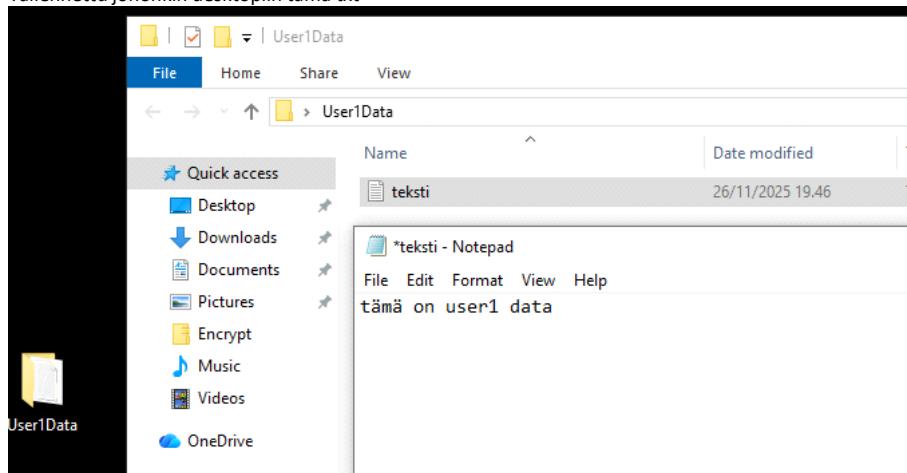
Se loi ponnahduksensa uuden sertifikaatti tiedon samantien ja pieni hämäys:

Group Policy Management Editor

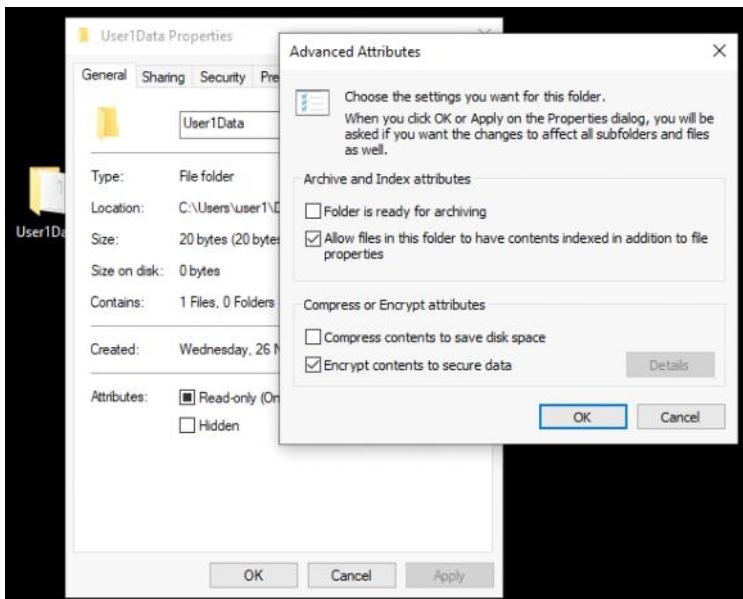
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
Administrator	Administrator	29.8.2125	File Recovery	<None>		EFS Recovery ...
Administrator	YritysXC-SERVER01-CA	26.11.2027	File Recovery	<None>		

Tämä on aikalailla valmis ja ok - seuraavaksi avataan VM2 - WIn10/11 työasema

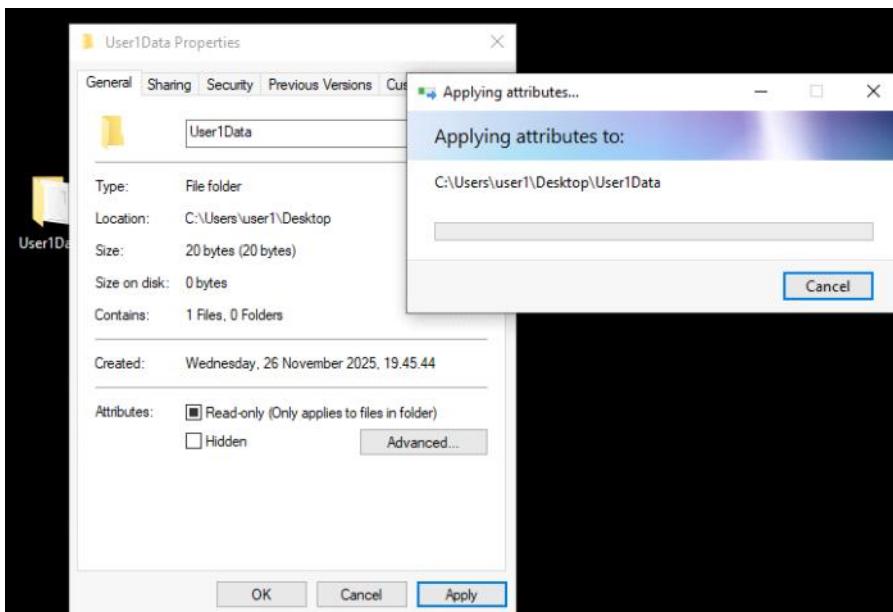
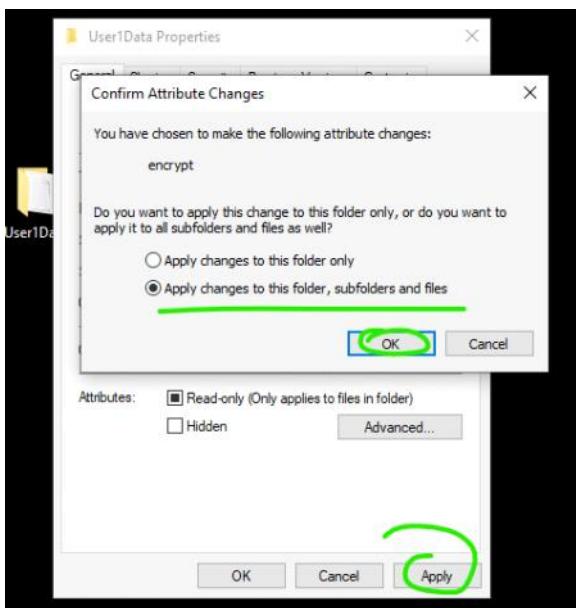
Tallennettu johonkin desktopiin tämä txt



Seuraavaaksi määritetään käsiö salausmenetelmään



Apply ja sen jälkee ponnahta ilmoitus

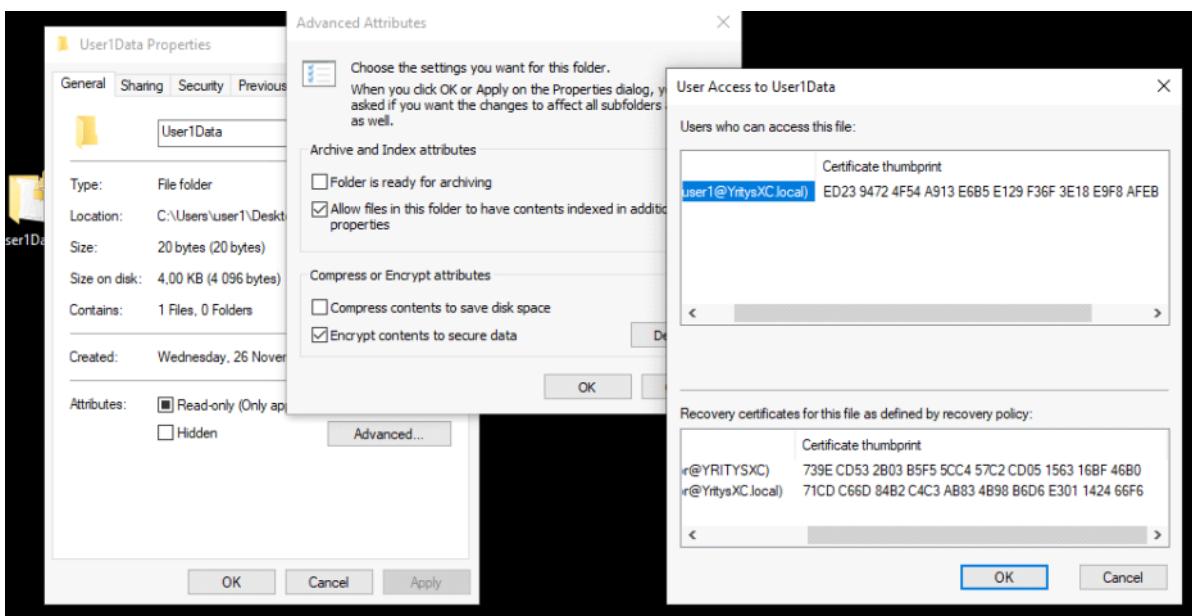
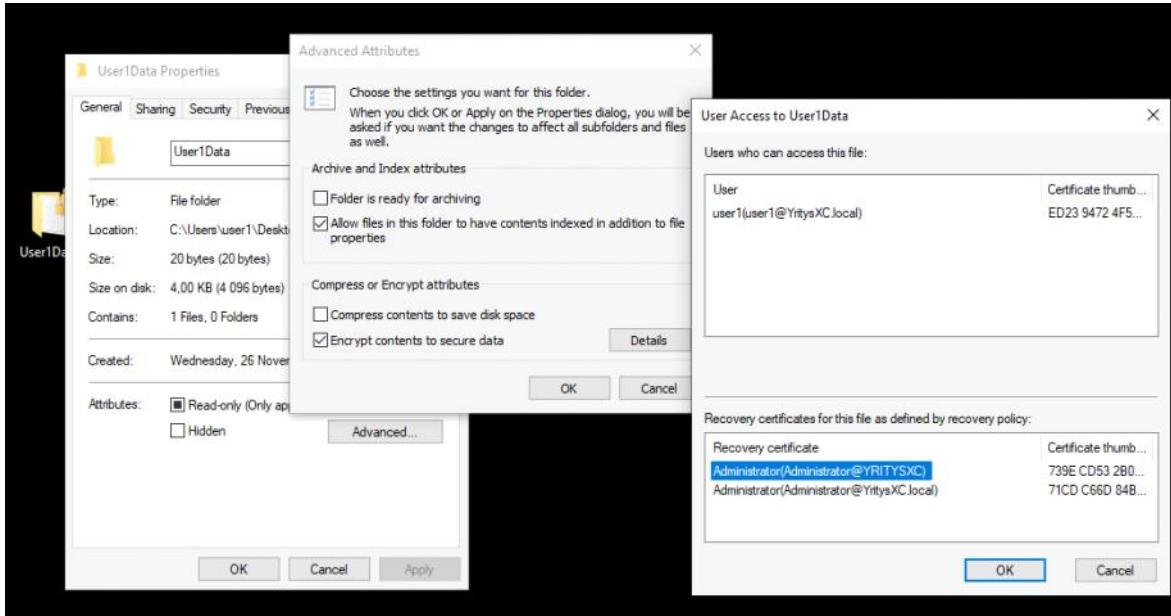


Saatiin ilmoitus , että tämä on back up tiedosto enryptattu tiedosto/avain.



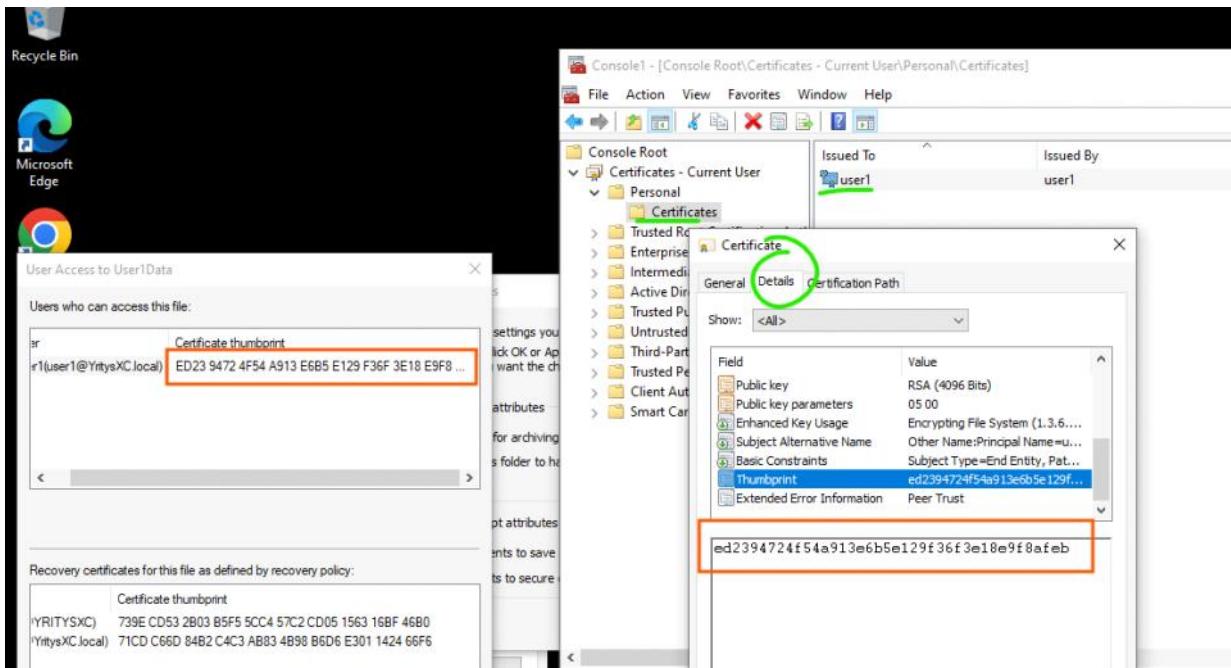
Tässä nähdään se salauskansio johon määritetään on tullut muutosta ja tarkistellaan lisätietoa.

- User1 (on vain oikeus tähän kansioon ja tiedostoon)
- Alhaalla on recovery policies - josta on kaksi tietoa
 - Ekana on määritetty administrator ad:sta
 - Mutta näitä thumbprint datasta voidaan tehdä vertailu ja tarkisut kennelle ne kuuluukaan.



Avataan mmc (win + r)

- Tästä voidaan täsmennää se thumbprint data
- Joo tähän kuitenkin pitäisi tulla näkyviinsä se lukeva "MYLABS" sertifikaatti tiedote kuitenkin



Jos mennään takaisin windows serverinsä ja tästä pitäisi tulla näkyviinsä toisen vm2 windows 10/11 määritetyn salauksen sertifikaatti tiedote

Request ID	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Certificate Expiration Date
2	YRITYSX\SERVER01\\$	-----BEGIN CERT...	Domain Controller (...)	3600000002e1f...	25.11.2025 7.29	25.11.2026 7.29
3	YRITYSX\Administrator	-----BEGIN CERT...	EFS Recovery Agent ...	360000003634...	26.11.2025 9.25	26.11.2027 9.35

Miksi VM2:n EFS-salattu kansio ei näy VM1:n CA:ssa

- Kun käyttäjä VM2:lla salaa tiedoston EFS:llä, Windows luo tai käyttää hänen omaa EFS-sertifikaattiaan.
- Jos domainissa ei ole määritetty **Enterprise CA:ta** (Active Directory Certificate Services), käyttäjä voi saada itse allekirjoitetun EFS-sertifikaatin paikallisesti.
- Tällöin CA:lla (VM1:llä) ei ole mitään tietoa siitä, että VM2:n käyttäjä loi sertifikaatin → siksi se ei näy *Issued Certificates*-listassa.

Milloin sertifikaatti näkyy CA:ssa

- Jos domainissa on **Enterprise CA** ja GPO on määritetty niin, että EFS-sertifikaatit haetaan CA:ltä, silloin VM2:n käyttäjä saa sertifikaatin CA:ltä.
- Tällöin CA kirjailee sen *Issued Certificates*-listaan.
- Tämä edellyttää, että:
 - AD CS on asennettu ja konfiguroitu Enterprise CA:ksi.
 - GPO:ssa on määritetty EFS-sertifikaattien automaattinen enrolointi.
 - Käyttäjä on domainissa ja saa sertifikaatin CA:ltä, ei paikallisesti.

Käytännön ero

- Ilman CA → käyttäjät luovat itse allekirjoitetut EFS-sertifikaatit, eivätkä ne näy CA:ssa.
- CA + GPO → käyttäjien EFS-sertifikaatit myönnetään CA:ltä ja näkyvät *Issued Certificates*-listassa.
- Tämä on se syy, miksi VM2:n salaus ei ilmestynyt VM1:n CA-konsoliin.

Yhteenvetö

- Ei ole virhe, että VM2:n EFS-salattu kansio ei näy VM1:n CA:ssa.
- Se näkyisi vain, jos EFS-sertifikaatti olisi haettu VM1:n Enterprise CA:ltä.
- Jos haluat, että kaikki domainin EFS-sertifikaatit hallitaan CA:n kautta, sinun pitää ottaa käyttöön **autoenrollment GPO** ja varmistaa, että AD CS on Enterprise CA, ei vain standalone.

Miksi VM2:n EFS-salattu kansio ei näy VM1:n CA:ssa

- EFS-salauksen yhteydessä käyttäjä käyttää omaa EFS-sertifikaattiaan.
- Jos CA (VM1) ei ole määritetty **Enterprise CA:ksi** ja GPO:lla ei ole ohjattu EFS-sertifikaattien automaattista enrolointia, käyttäjä voi luoda itse allekirjoitetun sertifikaatin → tämä ei koskaan näy CA:n *Issued Certificates*-listassa.
- Vain CA:sta haetut sertifikaatit kirjautuvat sinne.
- Eli: se, että VM2:n salaus ei ilmestynyt VM1:n listalle, ei ole virhe, vaan normaali tilanne jos autoenrollment ei ole käytössä.

Onko tämä vakava asia?

- Ei vakava:** tiedosto on silti salattu ja toimii käyttäjälle.

- **Vakava vasta jos:** organisaatio haluaa keskitetyn hallinnan ja palautusmahdollisuuden (Recovery Agent). Silloin sertifikaattien pitää tulla CA:ita.
- Ilman CA:ta riski on, että jos käyttäjä menettää avaimensa, tiedostoja ei voi palauttaa.

Työelämässä IT-adminin näkökulmasta

- Päivittäinen työ: ei tarvitse joka päivä tarkista EFS-sertifikaatteja.
- **Kuukausittainen/ylläpito:** isommissa organisaatioissa varmistetaan, että autoenrollment toimii ja Recovery Agent on määritetty.
- **Normi hyvä tietää:** ymmärtää, miksi sertifikaatti ei näy CA:ssa ja mitä se tarkoittaa.
- **Nice to know:** testilabroissa ja pienissä ympäristöissä tämä on enemmän oppimista kuin kriittistä hallintaa.
- **Pakollinen osaamisalue:** isoissa yrityksissä, joissa EFS/PKI on käytössä, adminin pitää tietää miten varmistaa että sertifikaatit tulevat CA:ita ja että palautus toimii.

Yhteenveto

- Ei kaada maailmaasi, eikä ole vakava virhe.
- Tämä on enemmän oppimisen paikka: **EFS-sertifikaatti ei näy CA:ssa ellei autoenrollment ole käytössä.**
- Työelämässä tämä on "hyvä tietää" ja "nice to know" pienissä ympäristöissä, mutta **välttämätön ymmärtää** isoissa organisaatioissa, joissa PKI ja EFS ovat osa tietoturvaliikkeitä.

OMA PIENI YHTEENVETO - VÄLISSÄ / POHDINTA - START HERE;

Onkin harjoitusmenetelmä tässä tehtynä, että VM2 Windows 10/11 -käyttäjän samassa DNS-ympäristössä ja VM1 Windows Serverin administrator tarkistetuna EFS-sertifikaatti ei näykään CA:ssa automaattisesti, vaikka videon mukaan pitäisi. Harjoituksen kannalta kuitenkin pitäisi IT-adminina tietää ja ymmärtää tämän teknisen toiminnan periaate: EFS-sertifikaatti syntyy käyttäjälle, mutta se ei aina tule näkyviin CA:n *Issued Certificates*-listalle, ellei autoenrollment ja Enterprise CA ole määritetty. Tämä ero on tärkeä ymmärtää, koska ilman CA:ta käyttäjä voi luoda itse allekirjoitetun sertifikaatin, joka ei ole hallittavissa keskitetyisti.

Yleensä tällaisen salausmenetelmän käyttö Windows 10/11 -kansioissa on nykymaailmassa vähentynyt, mutta se on edelleen yksi tapa suojaa tiedostoja. Sertifikaattina ja avaimen purkamisen EFS on enemmän 'legacy-ratkaisu', jota voi vielä kohdata, mutta useimmiten yritykset käyttävät muita menetelmiä tiedostojen suojaamiseen ja jakamiseen. Käytännössä organisaatiot hyödyntävät BitLocker-levysalausta, pilvipalveluiden sisäänrakennettua salausta (OneDrive, SharePoint, Teams) tai PKI-pohjaisia ratkaisuja, jotka ovat helpommin hallittavia ja tukevat myös tiedostojen jakamista organisaatioiden välillä.

IT-adminin näkökulmasta tämä on hyvä oppimisharjoitus: vaikka EFS ei ole enää jokapäiväinen työkalu, sen toimintaperiaatteiden ymmärtäminen auttaa hahmottamaan, miten sertifikaatit, CA ja avainten hallinta toimivat yhdessä. Tämä tieto ei välttämättä ole kriittistä pienessä yrityksessä, mutta suuremmissa ja hybridimallin ympäristöissä se on osa PKI-kokonaisuutta, joka tukee todennusta, salattua viestintää ja tiedostojen palautusta. Näin ollen EFS + CA on enemmän 'hyvä tietää ja ymmärtää' -osaamista, joka auttaa adminia hahmottamaan kokonaiskuvaa, vaikka käytännön työssä painopiste on siirtynyt BitLocker- ja pilvipalveluratkaisuihin

Pohdintaa EFS + CA:sta

- **EFS:n vahvuus**
 - Helppo tapa salata yksittäisiä tiedostoja ja kansioita Windowsissa.
 - Integroitu NTFS:ään ja AD:hen → käyttäjäkohtainen salaus.
 - CA:n avulla voidaan hallita avaimia ja palauttaa tiedostoja (Recovery Agent).
- **EFS:n heikkous nykypäivässä**
 - Ei sovella tiedostojen jakamiseen organisaatioiden välillä → salaus on sidottu käyttäjän sertifikaattiin.
 - Jos avain katoaa eikä CA:ta ole, tiedosto menetetään.
 - Pilvipalvelut (OneDrive, SharePoint, Teams) tarjoavat jo sisäänrakennettua salausta ja käyttöoikeuksien hallintaa, usein helpommin hallittavassa muodossa.
- **CA:n rooli**
 - Enterprise CA tuo hallittavuutta: sertifikaattien jakelu, palautus, todennus.
 - Isoissa organisaatioissa edelleen kriittinen, koska PKI on perusta monelle ratkaisulle (VPN, Wi-Fi, RDP, sisäiset web-palvelut).
 - Pienissä organisaatioissa voi olla "overkill", jos käytössä on vain pilvipalvelut ja BitLocker.

Nykymaailman vertailu

- **Windows 10/11**
 - EFS toimii edelleen, mutta Microsoft ohjaa enemmän BitLocker-levysalaukseen ja pilvipalveluiden käyttöön.
 - EFS on enemmän "legacy" tai erikoistilanteiden työkalu.
- **Pilvipalvelut**
 - OneDrive/SharePoint/Teams salaa tiedostot automaattisesti palvelinpäädessä.
 - Käyttöoikeudet hallitaan AD/Azure AD:n kautta.
 - Käytännössä helpompa ja turvallisempaa kuin EFS, jos tiedostoja jaetaan organisaatioiden välillä.
- **Organisaatioiden välinen tiedostonjakko**
 - EFS ei ole siihen tarkoitettu.
 - Jos haluat jakaa salatun PDF/TXT/koodin toiselle yritykselle, käytännöllisempiä ratkaisuja ovat:
 - **Azure Information Protection (AIP)** → tiedoston suojaus ja käyttöoikeuksien hallinta.
 - **Password-protected ZIP/PDF** → yksinkertainen mutta toimiva tapa.
 - **PKI-pohjainen salaus** → jos molemmilla organisaatioilla on CA ja sovittu sertifikaattien vaihto.