

### 7.1.3. EFS - 4

Sunday, November 30, 2025 13:31

## 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:

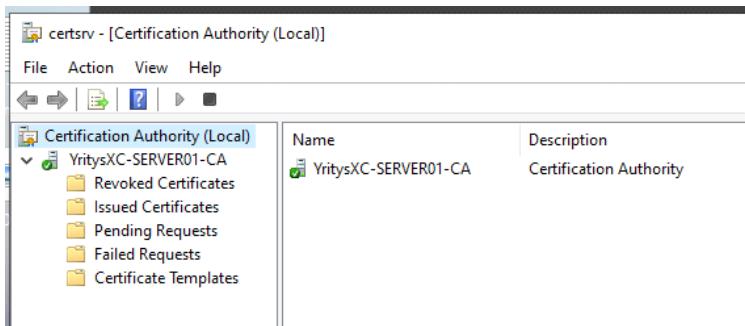
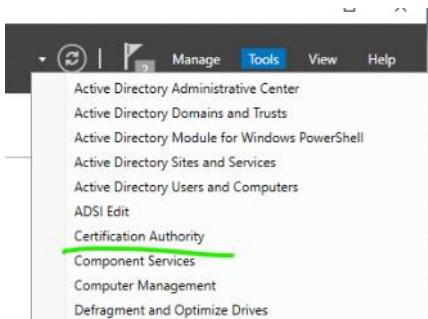
- 25. **Encrypting User Data with EFS in Active Directory** (Windows Server 2019)
- 26. **Setting up EFS with Group Policy and Certificate Authority** (Windows Server 2019)
- 27. **How to Backup and Restore EFS certificates** (Windows Server 2019)
- 18. **Configure EFS Data Recovery Agent using Group Policy** (Windows Server 2019)

Nyt jatkuu 18. video konfiguroidaa/määritetään EFS Data recovery agenttinsä käyttäen Group policy:ä

Tässä video on jotakin dejavu toistoa, mutta harjoituksen kannalta hyvä kertausta ja toistoa.

**TODAY IS: 30.11.2025**

windows serverin >> tools certification authority:stä



Tässä certificate templates nähdään mitä sertifikaatti ja muita tietoja on annettu ja just pääsee ensimmäisenä windows serveris tä ladattuna tämä wizard työkalunsa.

- Huom tässä "mylab basic" aikaisemmasta harjoituksesta ja säilytetään se

certsrv - [Certification Authority (Local)\YritysXC-SERVER01-CA\Certificate Templates]

File Action View Help

← → 🔍 🗁 🗃 🗑 ?

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...
<b>EFS Recovery Agent</b>	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting ...

Server Manager

certsrv - [Certification Authority (Local)\YritysXC-SERVER01-CA\Cert

File Action View Help

← → 🔍 🗁 🗃 🗑 ?

Certification Authority (Local)

- YritysXC-SERVER01-CA
  - Revoked Certificates
  - Issued Certificates
  - Pending Requests
  - Failed Requests
  - Certificate Templates**

Manage

- New
- ... Main Controller
- ... Server Computer
- ... Coordinate Certification Aut
- View

Tästä etsitään se "EFS recovery agent" listalta ja tehdään siitä duplikointi eli kopio

Certificate Templates Console

File Action View Help

← → 🔍 🗁 🗃 🗑 ?

Certificate Templates (Server01)

Template Display Name	Schema Version	Version	Intended Purposes
Administrator	1	4.1	
Authenticated Session	1	3.1	
Basic EFS	1	3.1	
CA Exchange	2	106.0	Private Key Archival
CEP Encryption	1	4.1	
Code Signing	1	3.1	
Computer	1	5.1	
Cross Certification Authority	2	105.0	
Directory Email Replication	2	115.0	Directory Service Email Replication
Domain Controller	1	4.1	
Domain Controller Authentication	2	110.0	Client Authentication, Server Authentic...
<b>EFS Recovery Agent</b>	6.1		
Enrollment Agent	4.1		
Enrollment Agent	5.1		
Exchange Enrollment	4.1		
Exchange Signature	6.1		
Exchange User	7.1		
IDCSP	8.1		

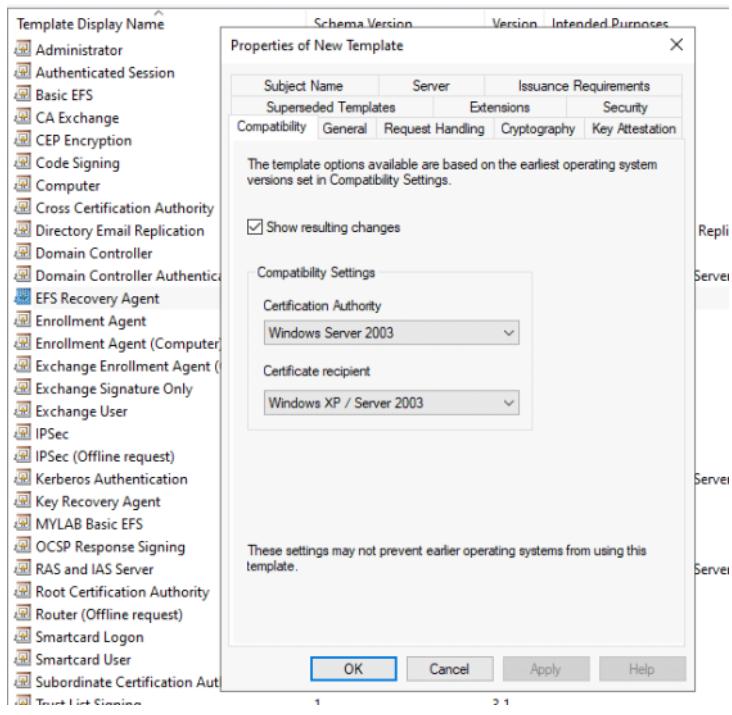
Duplicate Template

All Tasks

Properties

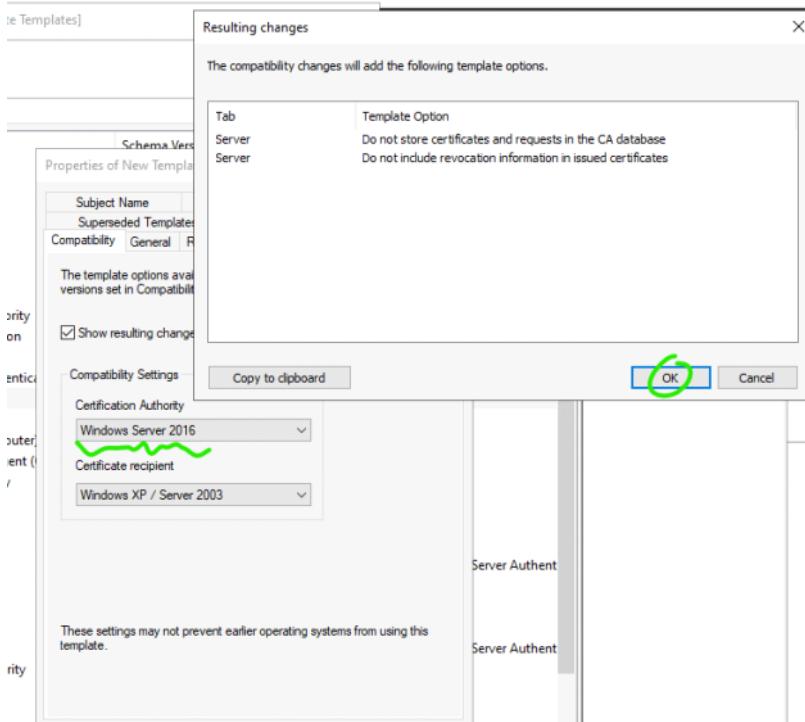
Help

BEFORE:

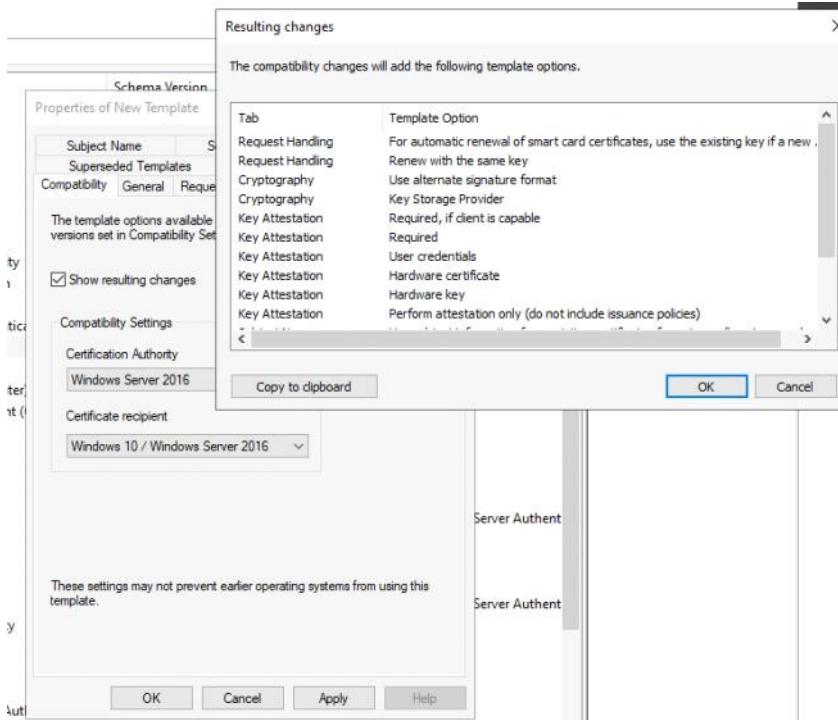


AFTER:

- Muutettiin vain windws server 2016 - niin ponnaataa ilmoitus ja klikkaa OOK
- Koska tässä demossa on windows 10 siksi otettiin tämä ja siksi tämä versio on vain tarjolla. Tämän vm1 onkin käytössä windwos server 2022



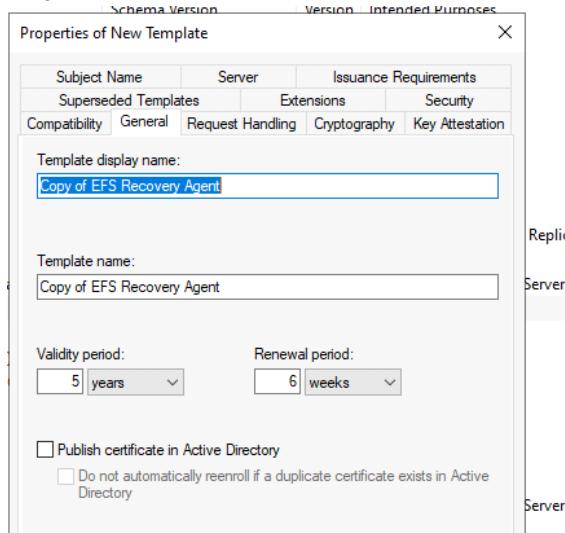
Sama alempi valikkosta muutettaan 2016 versio



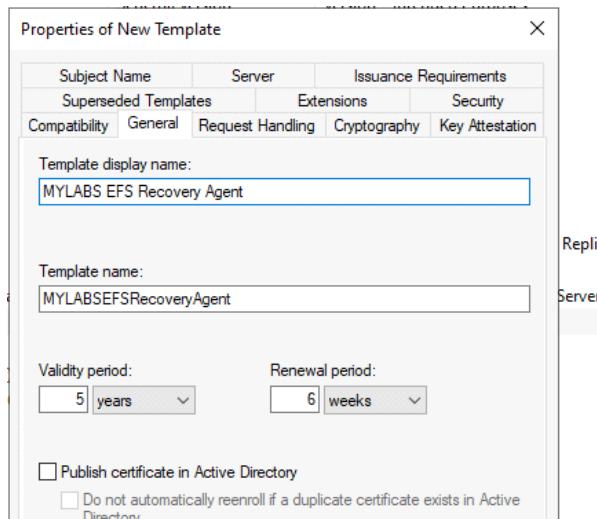
#### Seuraavaksi "General" polku

- Kirjoita uusi nimi ja itse saa keksiä

BEFORE:



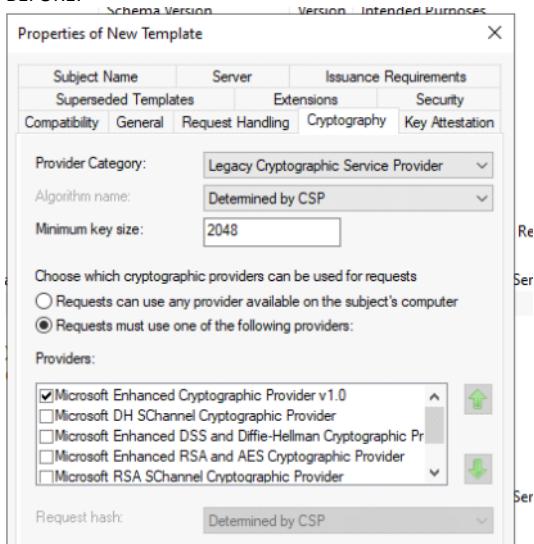
AFTER:



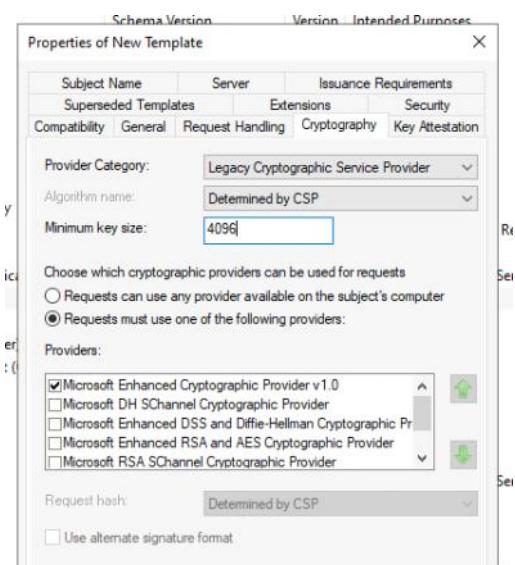
#### Seuraavaksi "Cryptography" polku

- Muutettaan vain se avain koko

BEFORE:

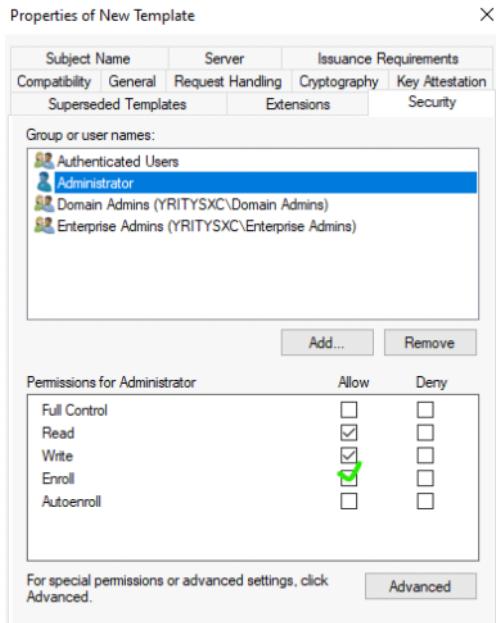


AFTER:



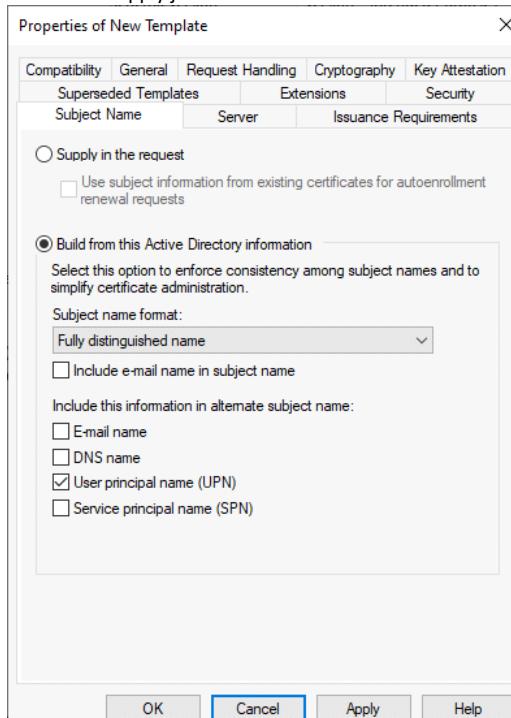
Seuraavaksi mennään "security" polkuun

- Tässä no oletuksena kaikki oikeudet ja käyttäjillä - siis valmiiksi, mutta administrator annettaan "enroll" oikeus lisää
- Eli lisää administratorille - enroll oikeus

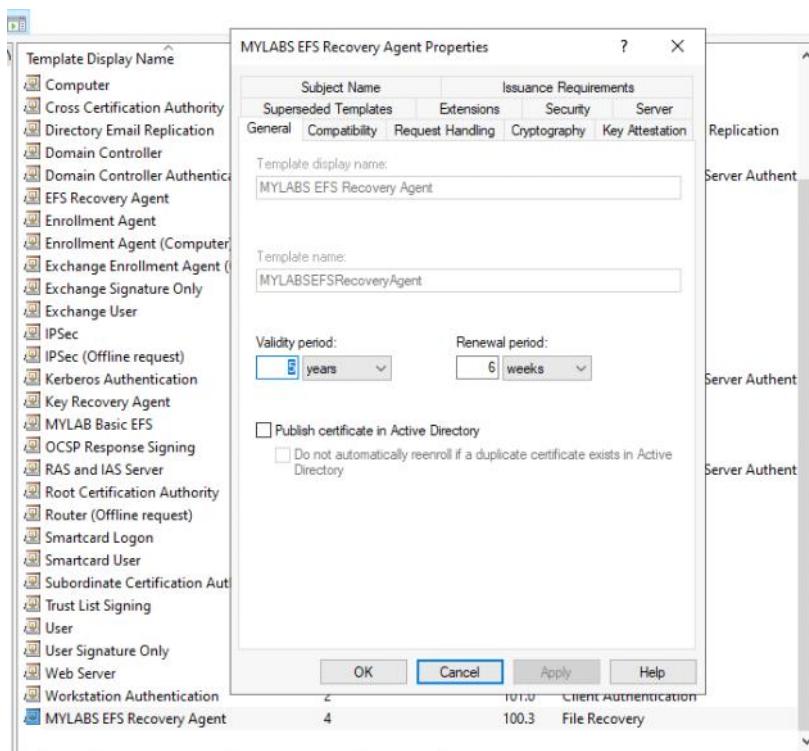


Seuraavaksi "subject name" - polkuun

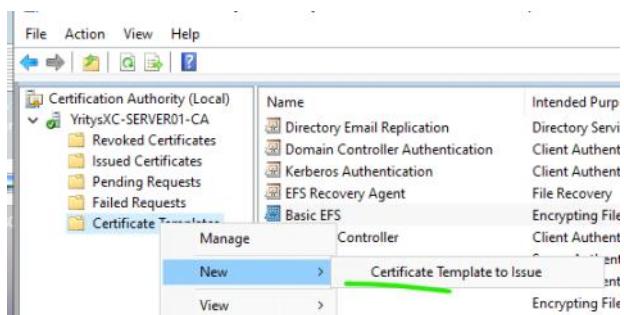
- Tarkistus UPN on päällä
  - Apply ja OK



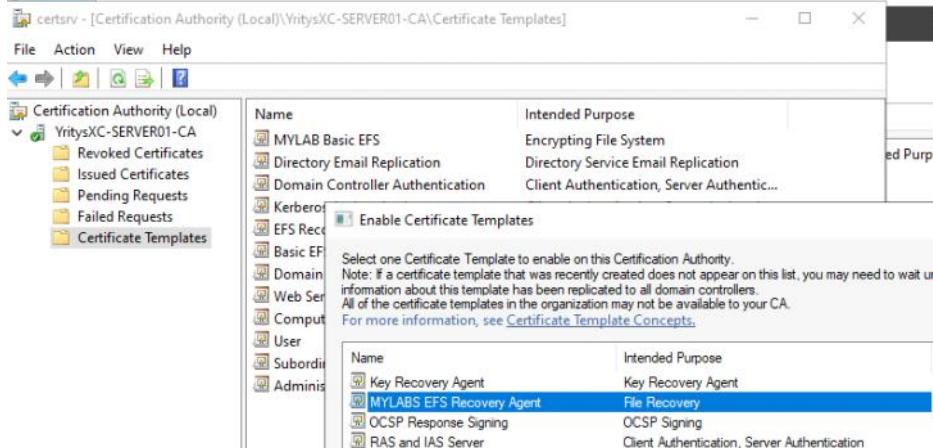
Sitten tämä tulee tähän listan alle, ja tästä voi jatkaa muokkaamista jos jotakin puuttuu tai halutaan erikseen muokata.



Eteenpäin ja seuraavaksi:

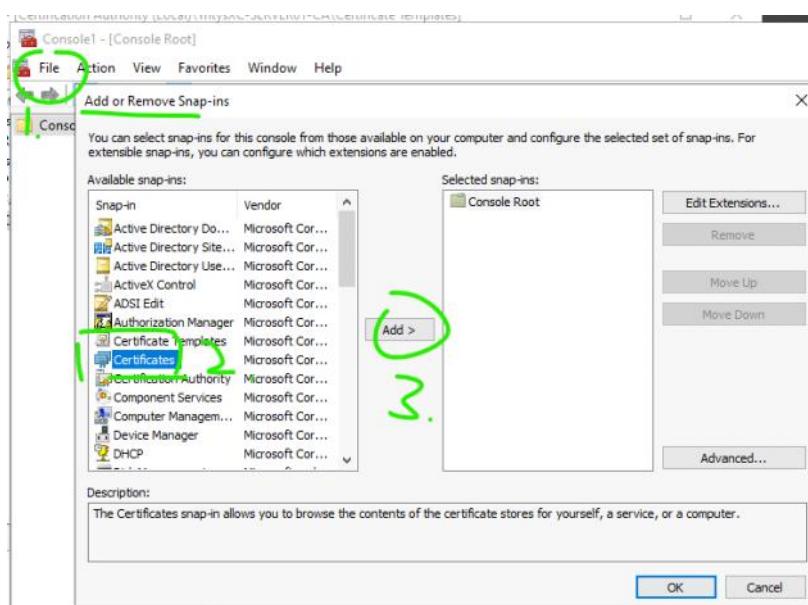


Eli valitaan meidän luoneen äskeittäisen mylabs efs recovery agentista ja se tulee täähän "certificate templates" listan alle.

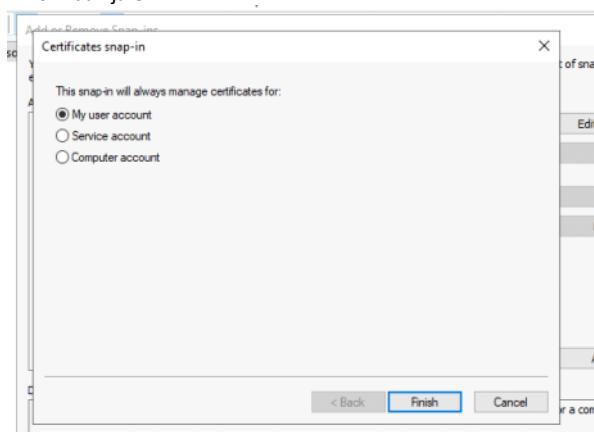


Seuraavaksi demostaan olemassa dns agency - luodaan issue tunnukselle sertifikaatille ja domain admin task Eli avataan "mmc"

"file" ja valitse "certificate" >> add >> ja "my current user"



Finish vaan ja OK



Tämä voi olla se recovery agentti mitä haluttaan, mutta pitää laajentaa näyttöä että tiedeteään se virallienn certifikaatti te mplate  
- Pientä sekanusta voi ja sekoitus voi tulla kantsii kakksois klikkaa ja lukea "details" polku vähä

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]							
File Action View Favorites Window Help		Actions					
		Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Sta...
Console Root	Certificates - Current User	Administrator	Administrator	29.8.2025	File Recovery	<None>	
Personal	Certificates	Administrator	YritysXC-SERVER01-CA	26.11.2027	File Recovery	<None>	EFS Recovery Agent
	Trusted Root Certificat	Administrator	Administrator	30.10.2025	Encrypting File Syst...	<None>	
	Enterprise Trust						
	Intermediate Certificat						
	Active Directory User						

Lisätään uusi certifikaatti ja ei valita noit ylempia kohtia

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]							
File Action View Favorites Window Help		Actions					
		Issued To	Issued By	Expiration Date	Intended Purposes	Fri	
Console Root	Certificates - Current User	Administrator	Administrator	29.8.2025	File Recovery	<N	
Personal	Certificates	Administrator	YritysXC-SERVER01-CA	26.11.2027	File Recovery	<N	
	Trusted Root Certificat	Administrator	Administrator	30.10.2025	Encrypting File Syst...	<N	
	Enterprise Trust						
	Intermediate Certificat						
	Active Directory User						
	Trusted Publishers						
	Untrusted Certificates						
	Third-Party Root Certi						
	Trusted People						
	Client Authentication						
	Other People						
	Certificate Enrollment						

All Tasks >	Request New Certificate...
Refresh	Import...
Export List...	Advanced Operations >
View >	
Arrow icons >	

Administrator Before You Begin

The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

Before requesting a certificate, verify the following:

- Your computer is connected to the network
- You have credentials that can be used to verify your right to obtain the certificate

Next Cancel

Certificate Enrollment

Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by your administrator	Active Directory Enrollment Policy
Configured by you	Add New

Next Cancel

Tätä me valittaa ja nenroll

Certificate Enrollment

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

	Status	Details
<input type="checkbox"/> Administrator	<span>STATUS: Available</span>	Details ▾
<input type="checkbox"/> Basic EFS	<span>STATUS: Available</span>	Details ▾
<input type="checkbox"/> EFS Recovery Agent	<span>STATUS: Available</span>	Details ▾
<input type="checkbox"/> MYLAB Basic EFS	<span>STATUS: Available</span>	Details ▾
<input checked="" type="checkbox"/> MYLABS EFS Recovery Agent	<span>STATUS: Available</span>	Details ▾
<input type="checkbox"/> User	<span>STATUS: Available</span>	Details ▾

Show all templates

Enroll Cancel

Certificate Enrollment

Requesting certificates. Please wait...

The enrollment server is being contacted to obtain the certificates you have requested.

**Active Directory Enrollment Policy**

	Status
<input checked="" type="checkbox"/> MYLABS EFS Recovery Agent	<span>STATUS: Enrolling...</span>

Cancel

Certificate Enrollment

Certificate Installation Results

The following certificates have been enrolled and installed on this computer.

**Active Directory Enrollment Policy**

	Status	Details
<input checked="" type="checkbox"/> MYLABS EFS Recovery Agent	<span>STATUS: Succeeded</span>	Details ▾

Finish

Siinä se viimeisenä onkin ja tuli listan alle.

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

File Action View Favorites Window Help

Back Forward Home Search Filter

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Template
Administrator	Administrator	29.8.2125	File Recovery	<None>		
Administrator	YritysXC-SERVER01-CA	26.11.2027	File Recovery	<None>		EFS Recovery Agent
Administrator	Administrator	30.10.2125	Encrypting File Syst...	<None>		
Administrator	YritysXC-SERVER01-CA	30.11.2027	File Recovery	<None>		MYLABS EFS Recovery Agent

Ainkin tästä nähdään valid from päivästä 30.11.2025 alkaen

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

File Action View Favorites Window Help

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Sta...	Certificate Template
Administrator	Administrator	29.8.2125	File Recovery	<None>		
Administrator	YritysXC-SERVER01-CA	26.11.2027	File Recovery	<None>		EFS Recovery Agent
Administrator	Administrator	30.10.2125	Encrypting File Syst...	<None>		
Administrator	YritysXC-SERVER01-CA	30.11.2027	File Recovery	<None>		MYLABS EFS Recovery Agent

**Certificate**

General Details Certification Path

**Certificate Information**

This certificate is intended for the following purpose(s):

- File Recovery

Issued to: Administrator

Issued by: YritysXC-SERVER01-CA

Valid from 30.11.2025 to 30.11.2027

You have a private key that corresponds to this certificate.

Issuer Statement

Nyt takaisin "certsrv" CA välilehteen ja avaa "issued certificates"

- Ja se on toi viimeisinä jonka otettiin

Certsrv - [Certification Authority (Local)\YritysXC-SERVER01-CA\Issued Certificates]

File Action View Help

Request ID	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Certificate Expiration Date
1	YRITYSXC\SERVER...	-----BEGIN CERTI...	Domain Controller (Domai...	3600000002e1f...	25.11.2025 7.29	25.11.2026 7.29
2	YRITYSXC\Administr...	-----BEGIN CERTI...	EFS Recovery Agent (EFSR...	3600000003634...	26.11.2025 9.25	26.11.2027 9.35
3	YRITYSXC\Administr...	-----BEGIN CERTI...	MYLABS EFS Recovery Age...	3600000004dac...	30.11.2025 9.19	30.11.2027 9.29

Certification Authority (Local)

- YritysXC-SERVER01-CA
  - Revoked Certificates
  - Issued Certificates
  - Pending Requests
  - Failed Requests
  - Certificate Templates

Nyt takaisin tähän taas, ja seuraavaksi pitää exportaa jotakin

- Eli otetaan se mylabs efs recovery agent ja polku "details"

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

File Action View Favorites Window Help

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Sta...	Certificate Template
Administrator	Administrator	29.8.2125	File Recovery	<None>		
Administrator	YritysXC-SERVER01-CA	26.11.2027	File Recovery	<None>		EFS Recovery Agent
Administrator	Administrator	30.10.2125	Encrypting File Syst...	<None>		
Administrator	YritysXC-SERVER01-CA	30.11.2027	File Recovery	<None>		MYLABS EFS Recovery Agent

**Certificate**

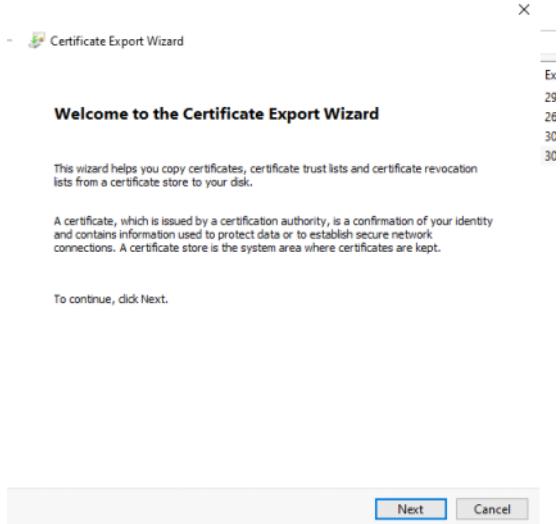
General Details Certification Path

Show: <All>

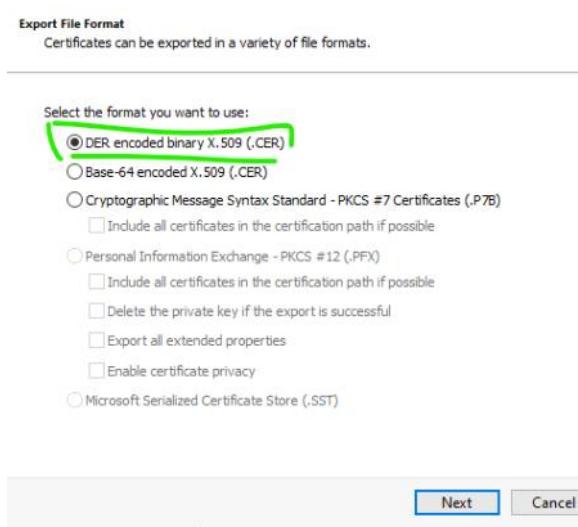
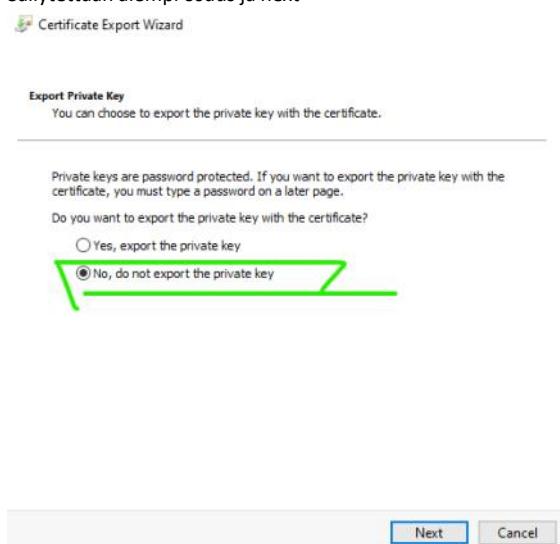
Field	Value
Version	V3
Serial number	3600000004dacfdc88547bb82...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	YritysXC-SERVER01-CA, Yrity...
Valid from	sunnuntaina 30. marraskuuta 20...
Valid to	tistaina 30. marraskuuta 2027 9...
Subject	Administrator_Users_YritysXC

Actions

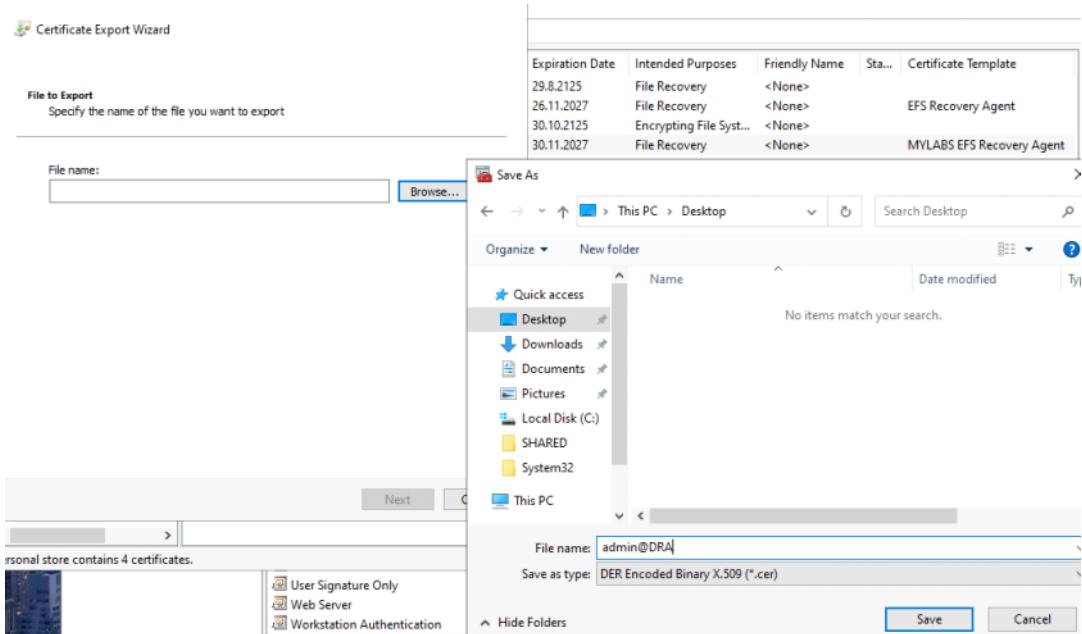
Copy to File...



Säilytettää alempi osuuus ja next



Tallennetaan ensimmäisenä desktopiin vaan ja joku nimike



## Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\Administrator\Desktop\admin
Export Keys	No
Include all certificates in the certification path	No
File Format	DER Encoded Binary X.509 (*.cer)

## Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\Administrator\Desktop\admin
Export Keys	No
Include all certificates in the certification path	No
File Format	DER Encoded Binary X.509 (*.cer)

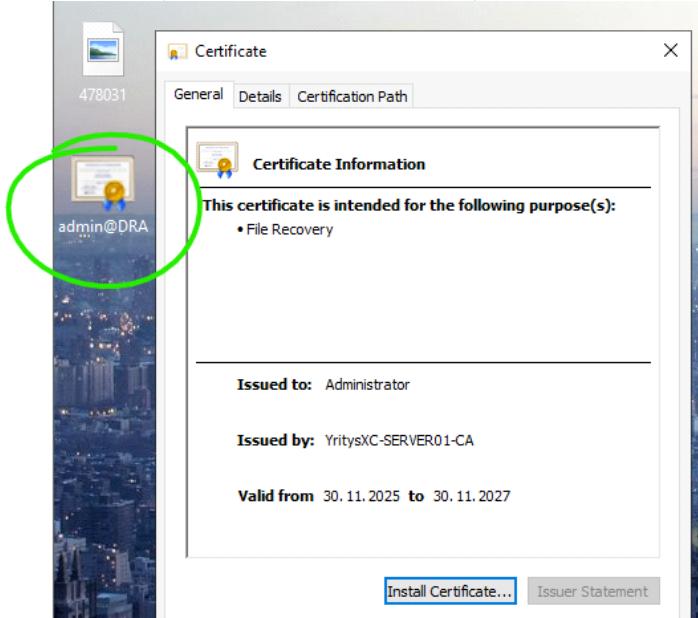
A message box from the 'Certificate Export Wizard' window says 'The export was successful.' with an 'OK' button.

25  
26  
30  
31

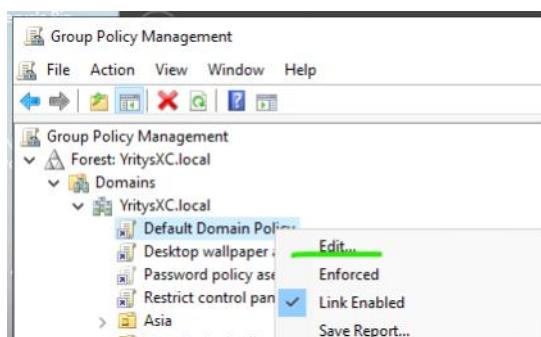


Nyt mennään desktopiin ja muistutuksena ollaan vm1 (windows serverissä kokoajan)

- Saattuu tähän tähän toimimaan ja eli toimi
- Seuraavaksi pitää saada tämä sertifikaatti lisättyä GPO asetuksensa mukaan



GPO:ssa konfiguroidaan ja määritetään tämä agenty recovery siihen jännästi ja muut gpo on varmistettava on poissa käytöstä e ttei se tule ristiriittaa ja sekoitusta.



Se on tois osa, ja koska siitä vähä rullaa oikealle niin näkee sen templates

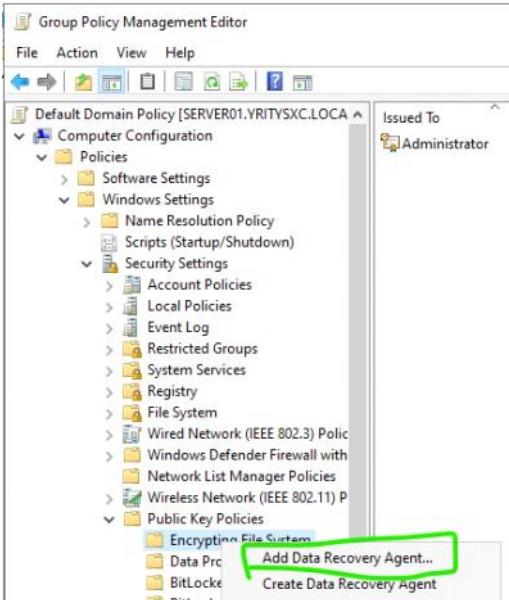
- Seuraavaksi eli pitää poistaa tois EFS recovery sertifikaatti

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate
administrator	Administrator	29.8.2025	File Recovery	<None>	Enabled	EFS Recovery

Pieni keskeytyminen tähän väliin ja jatkuu seuraavana päivänä.. Tai muu päivi

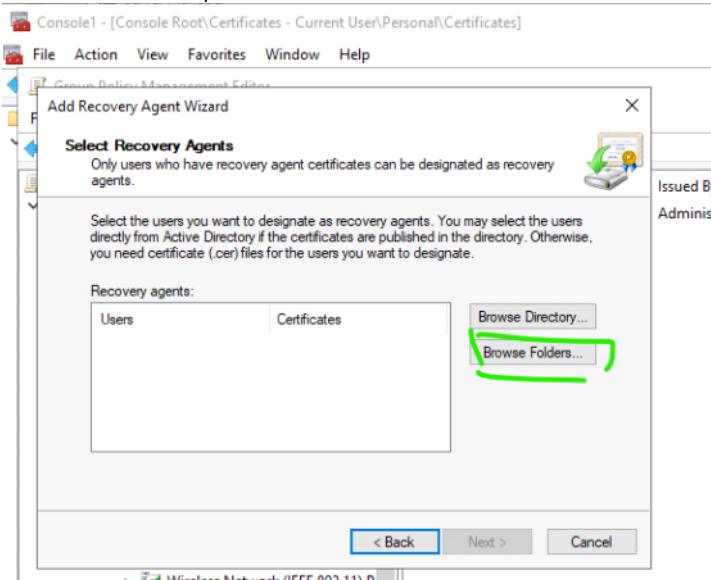
- Harjoitus jatkuu 2.12.2025 -->

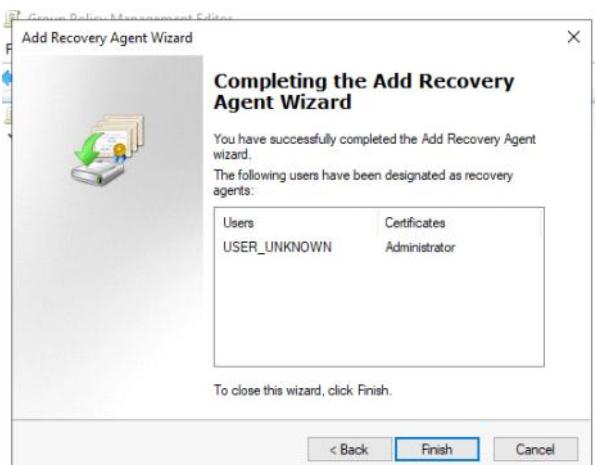
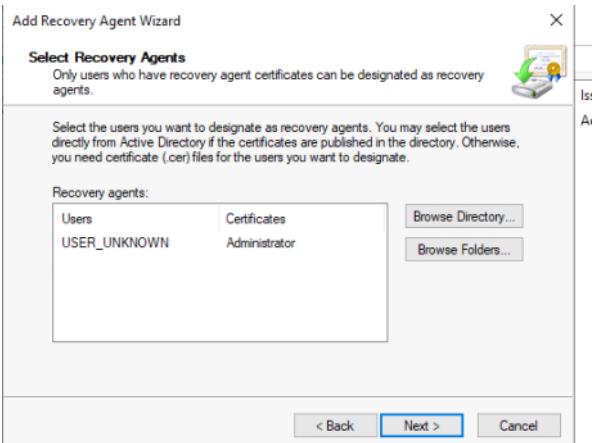
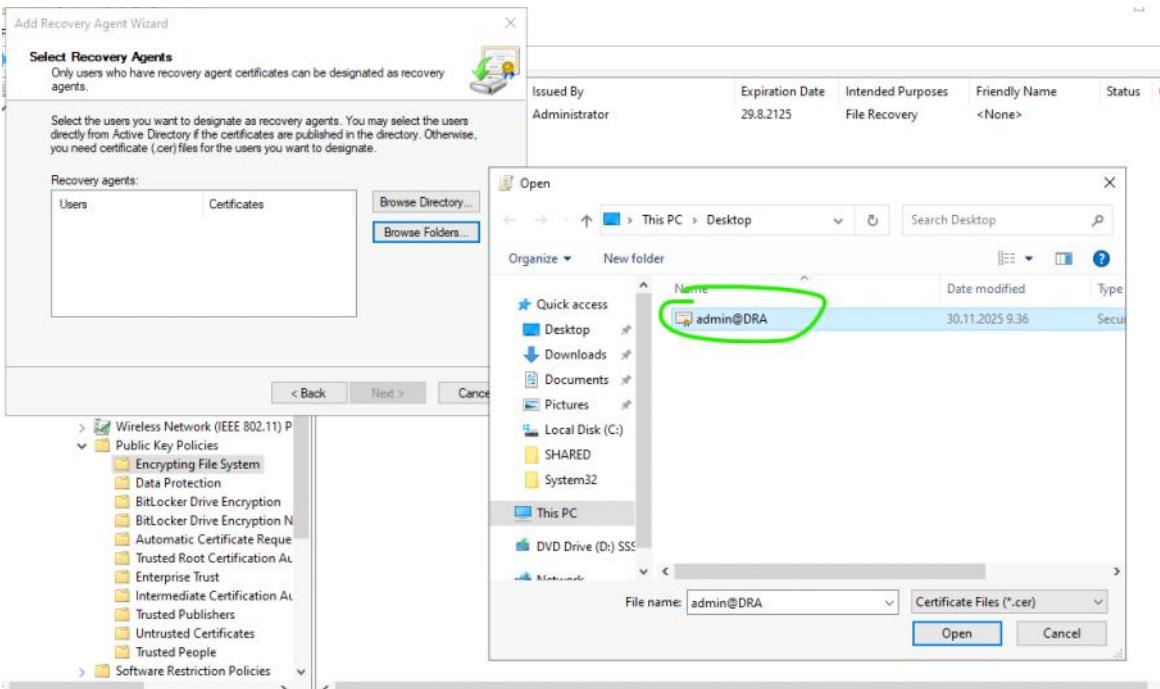
Tosiaan nyt positettaan tois "sertifikaatti" administrator tieto , ja koska halutan lisätä UUSI data recovery agent.



Tässä on kaksi vaihtoehtoa, joko direktoriossa tallella tai toisena kansiossa.

- Valitaan se alempi





Se tuli tähän näkyviinsä ja se ensimmäinen ja kaksoisklikkaus siihen, josta avautuu uusi ikkuna ja valitse "details"

Group Policy Management Editor

File Action View Help

Default Domain Policy [SERVER01.YRI]

Computer Configuration Policies Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) Security Settings Account Policies Local Policies Event Log Restricted Groups System Services Registry File System Wired Network (IEEE802.1X) Windows Defender Network List Manager Wireless Network (IEEE802.11) Public Key Policies Encrypting File System

Certificate

General Details Certification Path

Show: <All>

Field	Value
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Subject Alternative Name	Other Name:Principal Name=A..., 1.3.6.1.4.1.311.25.2
Key Usage	30 3e a0 3c 06 0a 2b 06 01 04... Key Encipherment (20)
Thumbprint	e11143cc755422416f8b26f30...
Extended Error Information	Revocation Status : OK. Effect...

Issued By: YritisXC-SERVER01-CA  
Administrator

Expiration Date: 30.11.2027  
29.8.2125

OK

Samalta thumbprint näyttää ainakin ja täsmennys

Group Policy Management Editor

Certificate

General Details Certification Path

Show: <All>

Field	Value
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Subject Alternative Name	Other Name:Principal Name=A..., 1.3.6.1.4.1.311.25.2
Key Usage	30 3e a0 3c 06 0a 2b 06 01 04... Key Encipherment (20)
Thumbprint	e11143cc755422416f8b26f30...
Extended Error Information	Revocation Status : OK. Effect...

Issued By: YritisXC-SERVER01-CA  
Administrator

Expiration Date: 30.11.2027  
29.8.2125

File Recovery File Recovery

Automatic Certificates

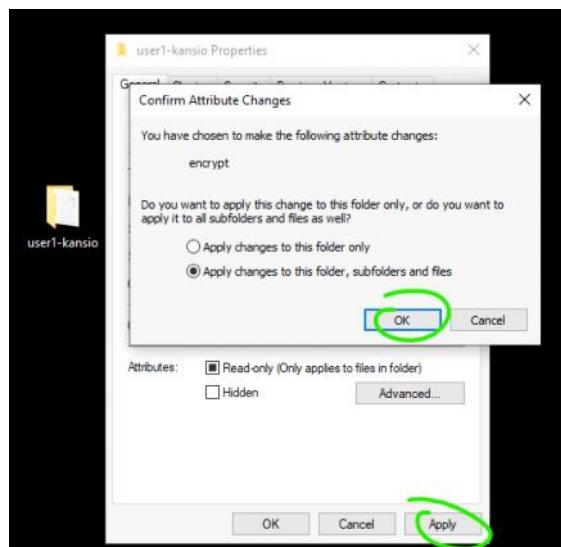
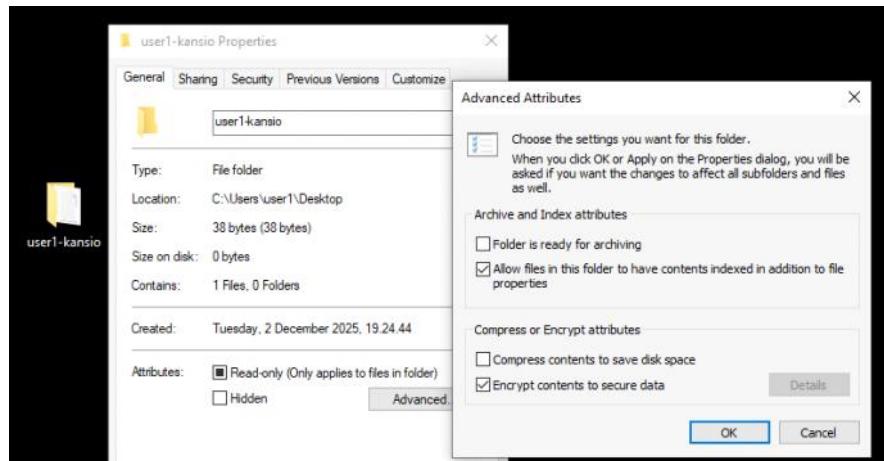
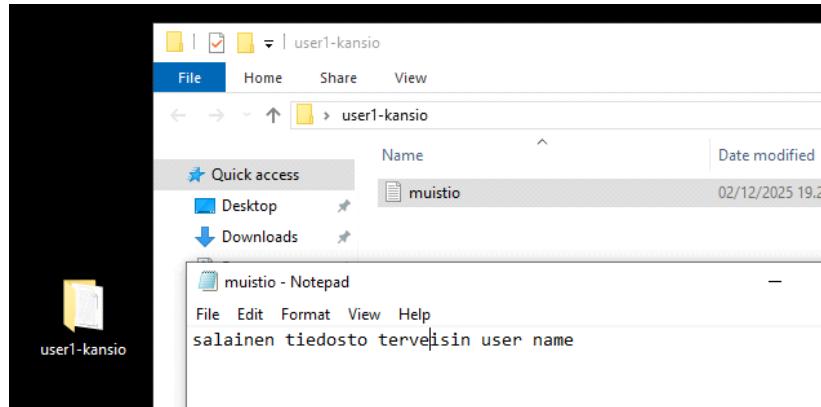
Certificates - [Certification Authority (Local)\YritisXC-SERVER01-CA\Issued Certificates]

Serial Number	Certificate Effective Date	Certificate Expiration Date
3600000002e1f...	25.11.2025 7.29	25.11.2026 7.29
3600000003634...	26.11.2025 9.25	26.11.2027 9.35
3600000004dac...	30.11.2025 9.19	30.11.2027 9.29

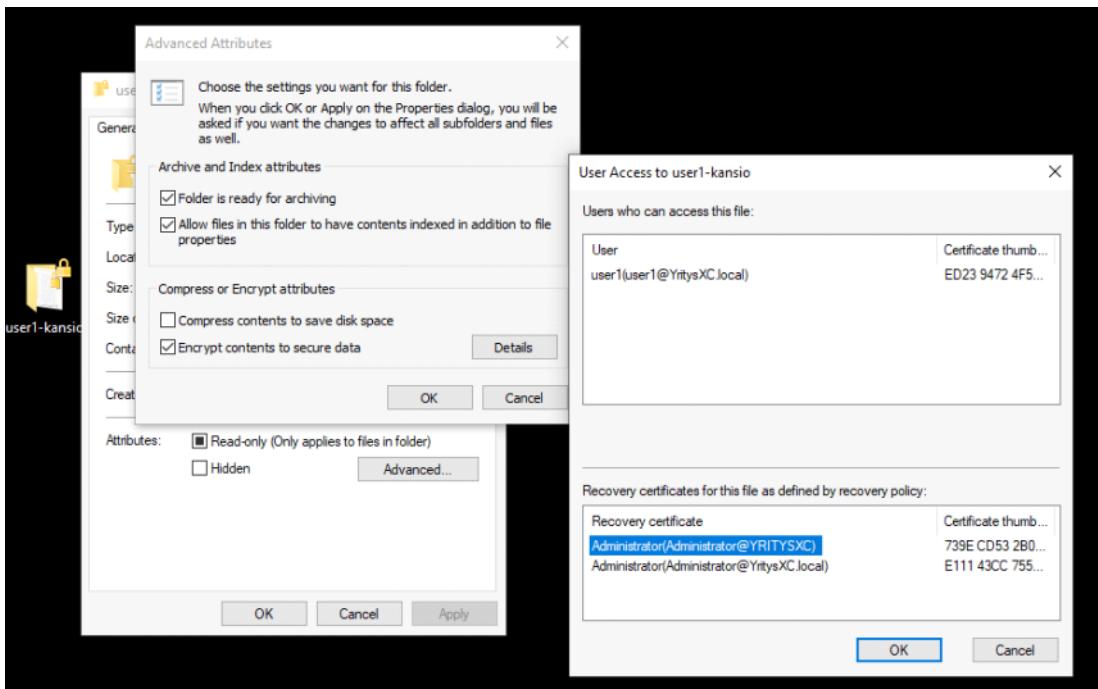
OK

Seuraavaksi upgrade policy (powershell , \$gpupdate /force) ja avataan toinen vm2 - win10/11 ja sama komento päivitystä

VM2:ssa luo sama encryptaus kansio ja joku txt - sana on vapaa



Kansio muuttui ja tuli lukko mukaan, sekä tarkistuksena (detail) että vain tämä käyttäjä on omistaja tähän kansioon.



Palauttamisen kannalta, josta pitää täsmennyä ton thumprint id mukaisesti.

A screenshot of a command-line interface (CLI) window titled 'Console1 - [Console Root]\Certificates - Current User\Personal\Certificates'. It displays a table of recovery certificates:

Recovery certificate	Certificate thumbprint
Administrator/Administrator@YRITYSX.local	739E CD53 2B03 B5F5 5CC4 57C2 ...
Administrator/Administrator@YritysXC.local	E111 43CC 7554 2241 6F8B 26F3 0...

Tämä on admin näkymä puoli ja windows serveristä:

A screenshot of the Microsoft Management Console (MMC) showing the 'Certificates' snap-in under 'Console1 - [Console Root]\Certificates - Current User\Personal\Certificates'. On the left is a tree view of certificate fields like Subject, Public key, and Thumpprint. On the right is a table of certificates:

Issued By	Expiration Date	Intended Purposes	Friendly Name	Status
YritysXC-SERVER01-CA	30.11.2027	File Recovery	<None>	
Administrator	29.8.2025	File Recovery	<None>	
YritysXC-SERVER01-CA	26.11.2027	File Recovery	<None>	
Administrator	30.10.2025	Encrypting File Syst...	<None>	

The 'Thumpprint' column for the second certificate is highlighted with a green box, showing the value '739ecd532b03b5f55cc457c2cd05156316bf46b0'.

Takaisin vm2:ja avaa mmc

Jotenkin siinä on se recovery agent sertifikaatti olemassa, mutta tämän kautta eli harjoitus on DONE.

## MINI YHTEENVETO JA POHDINTA - START HERE;

Tässä harjoituksessa siis tapahtui EFS sertifikaatti recovery agentti. Lyhyesti mitä tapahtui:

- VM2:n tavallinen käyttäjä salaa tiedoston omalla EFS-sertifikaatillaan, ja koska GPO:ssa on määritetty Recovery Agent (VM1:n Administrator), tiedoston salaukseen liitetään myös Administratorin RA-sertifikaatti. Näin VM1:n Administrator voi avata tiedoston ilman, että tarvitsee VM2:n käyttäjän sertifikaattia.
- Eli teoriassa ja käytännössä: **VM1:n Administrator toimii recovery agenttina itsessään, eikä VM2:n käyttäjän sertifikaattia tarvita palautukseen.**

### Mitä näet VM2:ssa (Win10/11)

- Kun loit EFS-salatuun kansioon ja tiedostoon, Windows käytti **käyttäjäkohtaisen EFS-sertifikaatin** (yleensä automaattisesti luotu, ellei AD CS:ää ole mukana).
- Kun tarkastelit tiedoston *Properties* → *Advanced* → *Details*, näit että tiedosto on salattu **Administrator-sertifikaatilla** (thumbprint alkaa 739E...).
- Tämä tarkoittaa: tiedoston salausavain on sidottu siihen sertifikaattiin, jotta juuri se identiteetti voi avata tiedoston.

## **Mitä näet VM1:ssa (Windows Server MMC)**

- Kun avasit MMC:n ja katsoit sertifikaatteja, löysit sertifikaatin nimellä **File Recovery** ja issuerina **Administrator**.
- Tämä on **EFS Recovery Agentin sertifikaatti**.
  - Recovery Agent on se varahenkilö, jonka avulla organisaatio voi purkaa EFS-salauksen, jos käyttäjä menettää oman avaimensa.
  - Recovery Agent määritellään Group Policyllä (GPO). Kun GPO on asetettu, kaikki uudet EFS-salaukset liittävät automaattisesti recovery agentin sertifikaatin tiedoston salaukseen.

## **Mitä tämä merkitsee harjoituksen kannalta**

- Se, että näet saman thumbprintin sekä tiedoston *Details*-kohdassa että MMC:ssä, tarkoittaa että **tiedosto on salattu niin, että sekä käyttäjän oma EFS-sertifikaatti että recovery agentin sertifikaatti voivat avata sen**.
- Käytännössä:
  - Käyttäjä (sinä VM2:ssa) voi avata tiedoston normaalisti.
  - Recovery Agent (Administrator VM1:ssa) voi myös avata sen, vaikka käyttäjän sertifikaatti katoaisi.
- Tämä on juuri se **EFS Recovery Agentin rooli** – varmistaa, että organisaatio ei menetä dataa, vaikka käyttäjän avain häviäisi.

## **Yhteenvedo**

- Ei ole **Certification Authority (CA)**, vaan **EFS Recovery Agentin sertifikaatti**.
- CA (varsinainen varmentaja) olisi erikseen, jos käytät AD CS:ää. Tässä harjoituksessa recovery agentin sertifikaatti on itse allekirjoitettu (issued by Administrator).
- Harjoituksen kannalta olet todistanut, että recovery agent toimii: tiedosto sisältää recovery agentin avaimen, ja siksi VM1:n Administrator voi palauttaa sen.

## **POHDINTA OSUUS JA TESTATTUA OSUUTTA SEURAAVASSA SIVUSSA (EFS - 5 POHDINTA)**