

## 7. Bitlocker & EFS - 1

Friday, November 21, 2025

19:33

### Bitlocker ja EFS (encrypting file system)

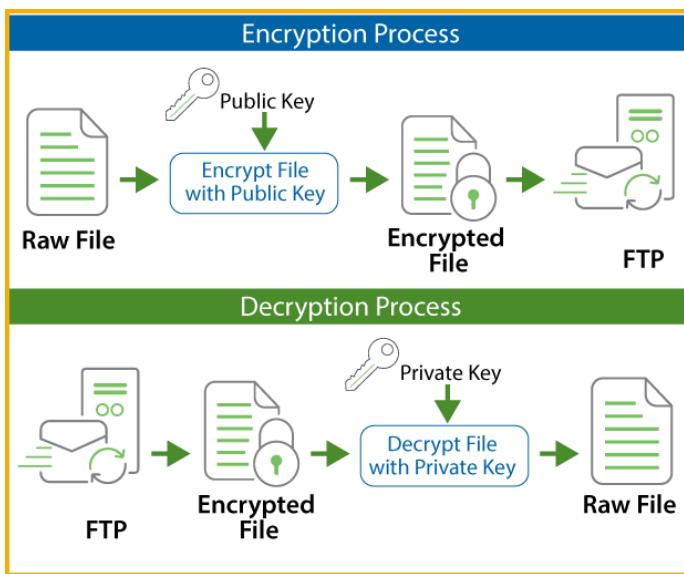
EFS eli Encrypted File System on Microsoft Windowsin ominaisuus, joka mahdollistaa tiedostojen ja kansioiden salauksen suoraan NTFS-tiedostojärjestelmässä. EFS on käyttäjäkohtainen salausmuoto, joka tekee tiedostoista lukukelvottomia ilman oikeaa salausavainta. Tämä suojaaa arkaluontoista tietoa luovuttamalta käytöltä, esimerkiksi jos laite varastetaan tai joutuu väriin käsiiin.

#### 🔒 BitLocker

- Mikä se on:** Kokonaisen levyn salausratkaisu Windowsissa. Salaa koko kiintolevyn, jolloin data on suojattu, vaikka levy irrotettaisiin ja yritettäisiin lukea toisessa koneessa.
- Vaikeustaso:** Peruskäytössä melko helppo (voit ottaa käyttöön GUI:sta tai PowerShellillä). Edistyneempiä juttuja ovat mm. TPM-integraatio, PIN-koodit, verkkoavaimet ja hallinta Group Policyllä.
- Merkitys IT-adminille:** Erittäin tärkeä yrityksissä, joissa on kannettavia tietokoneita. Suojaaa arkaluontoista dataa varkaustilanteissa.
- Voiko harjoitella VMware Workstationissa:** Kyllä, mutta huomioi että BitLocker vaatii TPM:n (Trusted Platform Module). VMware ei tarjoa fyysisää TPM:ää, mutta voit käyttää **TPM-emulointia** tai ottaa käyttöön BitLockerin ilman TPM:ää (Group Policy -asetus: *Allow BitLocker without a compatible TPM*). Tämä toimii hyvin testilabrassa.

#### 📁 EFS (Encrypting File System)

- Mikä se on:** Tiedostokohtainen salaus NTFS-tiedostojärjestelmässä. Käyttäjä voi salata yksittäisiä tiedostoja tai kansioita, jolloin vain kyseinen käyttäjä voi avata ne.
- Vaikeustaso:** Helppo aloittaa (hiiren oikea → Properties → Advanced → Encrypt contents). Vaikeampi puoli on sertifikaattien hallinta, avainten varmuuskopiointi ja palautus.
- Merkitys IT-adminille:** Tärkeä, mutta ei yhtä kriittinen kuin BitLocker. Käytännössä EFS sopii tilanteisiin, joissa halutaan suojata yksittäisiä tiedostoja käyttäjäkohtaisesti. Yrityksissä BitLocker on useammin käytössä, mutta EFS voi täydentää sitä.
- Voiko harjoitella VMware Workstationissa:** Kyllä, täysin mahdollista. Voit testata EFS:ää Windows 10 -asiakaskoneessa (VM2) ja hallita sertifikaatteja Windows Serveristä (VM1). Tämä on hyvä tapa oppia käytännön hallintaa.



- Helppous:** Molemmat ovat helppoja aloittaa, mutta syvemmälle mentäessä (TPM, sertifikaatit, GPO-hallinta) vaikeustaso nousee.
- Tärkeys IT-adminille:** BitLocker on kriittinen osa yrityksen tietoturvaa. EFS on hyödyllinen lisä, mutta ei yhtä laajasti käytetty.

#####
#####

### LABRA HARJOITUS - OHJE LUONNOS TYYPPI - START HERE;

#### BitLocker ilman TPM:ää Windows 10 -VM:ssä

Valmistelu: salli BitLocker ilman TPM:ää

- Avaa paikallinen Group Policy VM2:ssa:**
  - Käynnistä → kirjoita "gpedit.msc" → Enter.
- Siirry asetukseen:**
  - Computer Configuration → Administrative Templates → Windows Components → BitLocker Drive Encryption → Operating System Drives.
- Ota käyttöön asetus:**

- **Enable “Require additional authentication at startup”**
  - Avaa asetus → valitse **Enabled** → rastita **Allow BitLocker without a compatible TPM** → Apply → OK.
4. **Käynnistä VM2 uudelleen:**
- Varmista, että GPO-asetus aktivoituu.

#### Levyn salauksen käyttöönotto (C:)

1. **Avaa BitLocker-asetukset:**
  - Control Panel → BitLocker Drive Encryption → Turn on BitLocker (C:).
2. **Valitse todennusmenetelmä:**
  - **Valitse “Enter a password”** (koska TPM ei ole käytössä). Aseta vahva testisalasana.
3. **Tallenna palautusavain:**
  - **Save to a file ja Print the recovery key** (valitse vähintään tallennus tiedostoon).
  - Tallenna esim. D:-asemalle tai verkkojaolle, El samalle salattavalle C:-asemalle.
4. **Valitse salauslaajuus:**
  - **Encrypt used disk space only** (nopeampi labrassa).
5. **Salaus käyntiin:**
  - Hyväksy oletukset → Start encrypting. Odota, että valmistuu.

#### Testaus: varmista salauksen toimivuus

1. **Lukitus/avauksen testi:**
  - Käynnistä VM2 uudelleen.
  - Varmista, että käynnistykssä pyydetään salasanaa ja kirjautuminen onnistuu.
2. **Recovery key -testi (valinnainen):**
  - Syötä tahallaan väärä salasana → käytä “Recovery key” -vaihtoehtoa → anna tallennettu palautusavain.
  - Varmista, että Windows avautuu.

#### Hallinta PowerShellillä (valinnainen)

1. **Tarkista tila:**
  - Avaa PowerShell (Admin) → suorita:
    - `manage-bde -status C:`
2. **Lukitse/avaa komennolla:**
  - Lukitse: `manage-bde -lock C: -force`
  - Avaa: `manage-bde -unlock C: -RecoveryPassword <REKAVAINEN_GUID>`

## EFS (Encrypting File System) tiedostokohtainen salaus

#### Valmistelu: luu testikansio ja tiedosto

1. **Luo kansio:**
  - C:\EFS-Test (tai käyttäjäsi profiilin Documents-kansioon).
2. **Luo tekstitiedosto:**
  - hello.txt ja kirjoita sisälle “hello world”. Tallenna.

#### Salaus tiedostolle tai kansiolle

1. **Ominaisuudet-valinta:**
  - Hiiren oikea hello.txt → Properties → Advanced.
2. **Ota salaus käyttöön:**
  - **Rastita “Encrypt contents to secure data”** → OK → Apply.
  - Valitse “Apply changes to this file only” (tai koko kansio, jos haluat).
3. **Vahvistus:**
  - Tiedoston nimi voi muuttua vihertäväksi (NTFS EFS -värikoodi), merkkinä salauksesta.

#### Sertifikaatin ja avaimen varmuuskopioointi (pakollinen!)

1. **Avaa Sertifikaattien hallinta:**
  - Käynnistä → “certmgr.msc” (Current User -varasto).
2. **Etsi EFS-sertifikaatti:**
  - Personal → Certificates.
  - Sertifikaatin “Intended Purposes” näyttää “Encrypting File System”.
3. **Vie .PFX-muotoon (sisältää yksityisavaimen):**
  - Hiiren oikea EFS-sertifikaatti → All Tasks → Export.
  - Valitse **Yes, export the private key** → PFX.
  - Ota mukaan “Export all extended properties”.
  - Aseta **vahva salasana** PFX:lle.
  - Tallenna tiedosto turvalliseen sijaintiin (esim. C:\EFS-Backup\efs\_backup.pfx).
4. **Testaa varmuuskopio palauttamalla (valinnainen):**
  - Poista tilapäisesti EFS-sertifikaatti: Personal → Certificates → poista (vain labraa varten).
  - Yritä avata hello.txt → pitäisi epäonnistua (Access denied).
  - Palauta: hiiren oikea **efs\_backup.pfx** → Install → Current User → anna salasana → Finish.
  - Avaa hello.txt → toimii taas.

#### Käyttööikeustesti toisella käyttäjällä tai koneella

1. **Toisen käyttäjän testi samassa VM:ssä:**
  - Luo VM2:lle uusi paikallinen käyttäjä → kirjaudu sisään uutena käyttäjänä.
  - Yritä avata salattu hello.txt → ei avaudu (puuttuu vastaava EFS-sertifikaatti).
2. **Siirto toiseen VM:ään (VM1 tai toinen Win10):**
  - Kopioi hello.txt toiseen koneeseen.
  - Yritä avata → ei avaudu ilman alkuperäistä sertifikaattia.

- Tuo PFX ja asenna se kyseisen käyttäjän "Current User" -varastoon → avaus onnistuu.

## Yrityskäytön näkökulma ja vaikeustaso

- **BitLocker:**
  - **Tärkeys:** Korkea; suojaa koko levyn ja on standardi kannettavissa.
  - **Vaikeustaso:** Helppo aloitus, keskitaso hallinnassa (GPO, palautusavainten keruu, raportointi).
- **EFS:**
  - **Tärkeys:** Kohtalainen; hyvä käyttäjäkohtaiseen tiedostosuojaan, mutta vaatii avainhallinnan kurinalaisuutta.
  - **Vaikeustaso:** Helppo aloittaa, keskitaso sertifikaattien varmistuksessa ja palautuksessa.

#####

BitLocker Windows Serverissä on **levynsalausken työkalu**, jota käytetään suojaamaan dataa varkausilta ja luvattomalta käytöltä. IT-adminille se tuo hallittavuutta ja tietoturvaa, käyttäjälle se tarkoittaa, että data pysyy turvassa myös laitteen kadotessa. Riskit liittyvät avainten hallintaan ja TPM-haavoittuvuuksiin, mutta oikein toteutettuna se on erittäin hyödyllinen. Palautusavaimet voidaan säilyttää esimerkiksi Active Directoryssä tai Microsoft Endpoint Managerissa.

## ⌚ Miksi BitLocker Windows Serverissä?

- **Tietoturva:** Salaa koko levyn, jolloin data ei ole luettavissa ilman oikeaa avainta. Tämä suojaa erityisesti palvelimia ja kannettavia, jos levy varastetaan.
- **Compliance:** Monissa toimialoissa (esim. finanssi, terveydenhuolto) vaaditaan salattua dataa levyllä. BitLocker täyttää nämä vaatimukset.
- **Integraatio AD:n kanssa:** Palautusavaimet voidaan automaattisesti tallentaa Active Directoryyn, jolloin IT-admin voi palauttaa salauksen hallitusti.

## 🛡 Hyödyt IT-adminille

- **Keskitetty hallinta:** BitLocker voidaan hallita Group Policyllä, SCCM:llä tai Intunella. Tämä mahdollistaa automaattisen käyttöönoton ja seurannan.
- **Avainhallinta:** Palautusavaimet voidaan kerätä AD:hen tai pilvipalveluun, jolloin IT-admin voi auttaa käyttäjää ongelmatilanteessa.
- **Auditointi:** Mahdollistaa raportoinnin siitä, mitkä koneet ovat salattuja ja mitkä eivät.

## 👤 Mitä käyttäjän pitää tietää

- **Käynnistyksen PIN/salasana:** Jos TPM ei ole käytössä, käyttäjältä voidaan vaatia PIN tai salasana käynnistykseen.
- **Palautusavaimen merkitys:** Jos käyttäjä unohtaa PINin tai levy siirretään toiseen koneeseen, vain palautusavaimella voi avata levyn.
- **Normaalikäyttö:** Salaus on läpinäkyvä – käyttäjä ei huomaa sitä päivittäisessä työssä.

## ⚠️ Riskit ja poikkeamat

- **TPM-haavoittuvuudet:** TPM-moduuleissa on ollut haavoittuvuuksia (esim. CVE-2019-0090, CVE-2023-1017), jotka voivat paljastaa salausavaimia.
- **DMA-hyökkäykset:** Hyökkääjä voi yrittää päästää muistiin suoraan laitteiden kautta (esim. Thunderbolt).
- **Avainhallinnan puute:** Jos palautusavainta ei ole tallennettu AD:hen tai muualle, sen katoaminen voi tehdä datasta pysyvästi saavuttamatonta.
- **Käyttäjäkokemus:** Jos PIN unohtuu tai levy vioituu, käyttäjä ei pääse dataan ilman palautusavainta.

## 📁 Missä avaimet säilyvät?

- **Active Directory:** Palautusavaimet voidaan automaattisesti tallentaa AD:hen domain-ympäristössä.
- **Microsoft Endpoint Manager / SCCM:** Avaimet voidaan hallita keskitetysti pilvipalvelussa.
- **Paijallinen tallennus:** Käyttäjä voi tallentaa avaimen tiedostoon, USB-tikulle tai tulostaa sen. Tämä ei ole suositeltavaa ilman keskitettyä hallintaa.

## ✳️ Yhteenveto

- **Käyttö:** BitLocker suojaa levyä ja dataa, erityisen tärkeä palvelimissa ja kannettavissa.
- **Hyödyt:** IT-admin saa hallittavuutta, käyttäjä saa turvaa.
- **Riskit:** TPM-haavoittuvuudet, avainten katoaminen, DMA-hyökkäykset.
- **Säilytys:** Avaimet kannattaa tallentaa AD:hen tai hallintajärjestelmään, ei vain käyttäjän vastuulle.

## 🔑 Mikä on TPM?

- **TPM (Trusted Platform Module)** on erillinen mikrosiru, joka on asennettu emolevylle.
- Sen tehtävä on turvallisesti säilyttää salausavaimia ja suorittaa **kryptografisia operaatioita**.
- TPM:ää käytetään mm. BitLockerissa, jotta levyn salausavaimet eivät koskaan ole suoraan käyttöjärjestelmän muistissa, vaan ne pysyvät suojaussa laitteistossa.

## 🔒 Miksi BitLocker käyttää TPM:ää?

- **Automaattinen avaus:** TPM voi avata salatun levyn käynnistyksen yhteydessä, jos järjestelmä ei ole muuttunut (secure boot, boot chain).
- **Turvallisuus:** Avaimet eivät ole tallennettuna levylle tai käyttäjän hallussa, vaan TPM suojaa niitä.
- **Käyttäjäkokemus:** Käynnistys voi olla läpinäkyvä – käyttäjän ei tarvitse aina syöttää PINiä tai salasanaa.

## ⚠️ Miten haavoittuvuudet liittyvät BitLockeriin?

- Jos **TPM:ssä on haavoittuvuus**, hyökkääjä voi teoriassa murtaa sen suojauskuksen ja saada salausavaimen ulos.
- Esimerkkejä:
  - **Fyysiset hyökkäykset:** Hyökkääjä voi juottaa kiinni TPM-siruun ja yrittää lukea sen muistia.

- **Firmware-haavoittuvuudet:** TPM:n ohjelmistossa voi olla virheitä, jotka paljastavat avaimia.
- **Side-channel-hyökkäykset:** Hyökkääjä voi mitata sähköisiä signaaleja tai virrankulutusta ja päättää avaimia.
- Koska BitLocker luottaa TPM:ään avainten suojaamisessa, sen haavoittuvuus = riski BitLockerille.

## ⌚ Riskien hallinta

- **Lisäautentikointi:** BitLocker voidaan konfiguroida vaatimaan PIN tai USB-avain TPM:n lisäksi → hyökkääjä ei saa levyä auki pelkällä TPM:n manipuloinnilla.
- **Firmware-päivitykset:** TPM-valmistajat julkaisevat päivityksiä haavoittuvuuksiin. IT-adminin pitää huolehtia niiden asentamisesta.
- **Käyttö ilman TPM:ää:** BitLocker voidaan ottaa käyttöön ilman TPM:ää, mutta silloin avaimet tallennetaan muualle (esim. USB-tikulle tai syöttetään PINillä). Tämä voi olla vähemmän kätevä, mutta antaa enemmän hallintaa.

## 📁 Missä avaimet säilyvät?

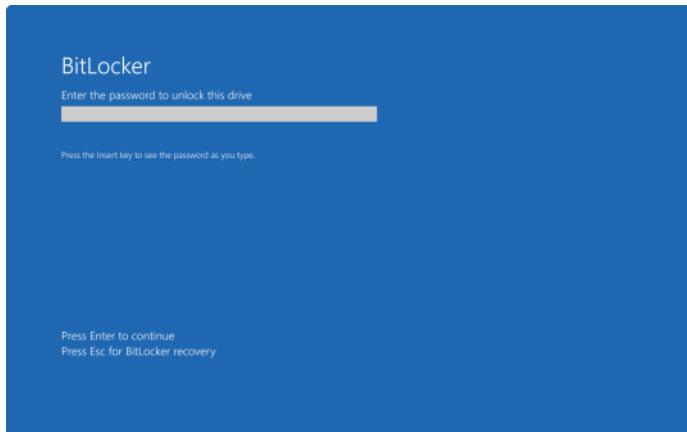
- **TPM:** Pääsääntöisesti BitLocker-avaimet.
- **Active Directory / Azure AD / Intune:** Palautusavaimet voidaan kerätä keskitetysti.
- **Käyttäjän hallussa:** Avaimet voidaan tallentaa tiedostoon, tulostaa tai USB-tikulle (riskialttiimpaa).

## 📋 Yhteenveto

- **TPM = laitteistopohjainen avainsäilö.**
- **BitLocker käyttää TPM:ää**, koska se tekee salauksesta läpinäkyvää ja turvallista.
- **Riskit liittyvät siihen, että jos TPM murretaan, BitLocker-avaimet voivat vuotaa.**
- **IT-adminin rooli:** varmistaa, että TPM on päivitetty, BitLocker on konfiguroitu oikein (PIN/USB + AD-avainkeruu), ja palautusavaimet säilytetään hallitusti.

#####

## Bitlocker (Windows server vs Pilvipalvelun intune) on jotakin eroja toisiinsa



## 💻 BitLocker Windows Serverissä (on-premises)

- **Teknologia:** Sama BitLocker-levyn salaus, joka on osa Windowsia.
- **Hallinta:**
  - IT-admin konfiguroi Group Policyllä (GPO) tai manuaalisesti.
  - Palautusavaimet voidaan tallentaa **Active Directoryyn** (AD DS).
- **Käyttö:**
  - Soveltuu palvelimiin ja työasemiin, jotka ovat domainissa.
  - IT-admin voi hakea palautusavaimen AD:stä, jos käyttäjä unohtaa PINin tai levy lukittuu.
- **Riski:** Jos avaimia ei ole tallennettu AD:hen tai varmuuskopioitu, data voi jäädä pysyvästi lukituksi.

## 🌐 BitLocker Intunen / Entra ID:n kautta (pilvihallinta)

- **Teknologia:** Sama BitLocker, mutta hallinta tapahtuu **Microsoft Endpoint Managerin (Intune)** ja **Entra ID:n** kautta.
- **Hallinta:**
  - Palautusavaimet tallennetaan automaattisesti **Entra ID:hen** (Azure AD).
  - Vain Intune/Entra ID -admin voi nähdä ja hallita avaimia.
- **Käyttö:**
  - Soveltuu erityisesti mobiileihin ja etäkäytössä oleviin laitteisiin.
  - Käyttäjä ei itse näe avaimia, vaan IT-admin hallitsee niitä keskitetysti.
- **Turva:** Jos kone varastetaan, varas ei voi purkaa levyä ilman avainta.
- **Data:** Jos kone hajoaa, käyttäjä voi palauttaa datansa pilvestä (OneDrive, SharePoint, Teams). Tämä on iso ero – pilvihallinta yhdistyy datan varmuuskopointiin.

## ⌚ Yhteinen idea vs. ero

- **Yhteistä:** Molemmissa BitLocker salaa levyn, suojaa dataa ja estää varkaita lukemasta sisältöä.
- **Ero:**
  - **Windows Server/AD:** Avaimet hallitaan on-premises AD:ssä, IT-admin voi hakea ne.
  - **Intune/Entra ID:** Avaimet hallitaan pilvessä, vain pilviadmin voi nähdä ne. Lisäksi pilvhallinta yhdistyy varmuuskopointiin ja mobiililaitteiden hallintaan.

## ⌚ Käytännön merkitys

- **Yrityksissä, joissa on paljon etäkäyttäjiä:** Intune + Entra ID on parempi, koska avaimet ja varmuuskopiot ovat pilvessä.
- **Perinteisessä domain-ypäristössä:** Windows Serverin BitLocker + AD-avainkeruu riittää.
- **Käyttäjälle:** Molemmissa tapauksissa varas ei voi purkaa levyn. Erona on se, mistä palautusavain löytyy (AD vs. Entra ID).

- **BitLocker itsessään on sama teknologia molemmissa (levyn salaus Windowsissa).**
- **Windows Server/AD-hallinta:** Avaimet tallennetaan yleensä Active Directoryyn, ja domain-admin voi hakea ne.
- **Intune/Entra ID -hallinta:** Avaimet tallennetaan pilveen (Entra ID), ja vain Intune/Entra ID -admin voi nähdä ja hallita niitä. Tämä vastaa sitä mitä sanoit "pitemmästä koodista" ja adminin yksinoikeudesta.
- **Varastettu kone:** Molemmissa malleissa levyn salaus ei voi purkaa ilman avainta, joten varas ei pääse dataan.
- **Datasiirto/varmuuskopio:** Pilvhallinnassa (Intune + OneDrive/SharePoint) käyttäjän data on helpommin palautettavissa, jos kone hajoaa. Tämä on se ero, jonka mainitsit.
- **Eli:** Idea on sama (BitLocker salaa levyn), mutta hallintamalli ja avainten säilytys eroavat: on-premises AD vs. pilvi (Intune/Entra ID).
  - *On jotakin samoja ja pientä eroavaa teoriaa.*

#####

## EFS - WINDOWS SERVER HARJOITUS - DEMO 1

Windowsin **Encrypting File System (EFS)** salaa tiedostot ja kansiot NTFS-levyllä siten, että vain käyttäjättili, jolla on **oikea salausavain** (joka liittyy käyttäjän salasanaan ja sertifiikaattiin), voi avata ja lukea sisällön. Jos Maija ei ole valtuutettu käyttäjä eikä hänen ole oikeaa avainta, hän ei pääse lukemaan tiedoston sisältöä, vaikka tietäisi Mattin salasanan.

## ⌚ Käytännön esimerkki

- Matti luo tiedoston hello.txt ja ottaa EFS-salauksen käyttöön.
- Windows luo FEK:n ja salaa tiedoston sisällön.
- FEK salataan Mattin julkisella avaimella.
- Kun Matti kirjautuu sisään omalla tilillään ja salasanallaan, hänen yksityinen avaimensa avaa FEK:n ja tiedosto näkyy normaalisti.
- Jos Maija yrittää avata tiedoston omalta tililtään, hän ei saa sisältöä näkyviin, ellei Matti ole lisännyt häntä valtuutetuksi käyttäjäksi tiedoston salausasetuksissa.

### Tässä on huomio koskien EFS asetuksensa:

#### ⌚ EFS ja käyttäjäkohtainen salaus

- EFS ei toimi niin, että voit itse asettaa erillisen "salasanan" tiedostolle tai kansiolle.
- Sen sijaan EFS käyttää **käyttäjätiliin sidottua sertifiakaattia ja avainparia**. Kun käyttäjä kirjautuu sisään omalla Windows-tilillään (ja salasanalla), hänen yksityinen avaimensa avaa tiedoston.
- Eli tiedoston avaaminen perustuu **Windowsin käyttäjätiliin ja sen avaimiin**, ei erilliseen koodiin, jonka voisi syöttää tiedoston avaamisen yhteydessä.

#### ⌚ Active Directory (AD DS) ja ryhmät

- Windows Server -ypäristössä, jossa on **Active Directory Domain Services (AD DS)**, EFS voidaan hallita keskitetysti.
- Voit määrittää, että tietty **käyttäjät tai ryhmät** lisätään tiedoston salausasetuksiin. Nämä useampi henkilö voi avata saman tiedoston omilla tunnuksillaan.
- Käytännössä tiedoston FEK (File Encryption Key) salataan jokaisen valtuutetun käyttäjän julkisella avaimella. Jokainen heistä voi purkaa sen omalla yksityisellä avaimellaan.

#### ⌚ Käytännön ero

- **Ei voi:** asettaa erillistä "salasanakenttää" tiedoston avaamiseen.
- **Voi:** lisätä valtuutettuja käyttäjiä (AD DS -käyttäjiä tai ryhmä) tiedoston salausasetuksiin.
- Tämä tarkoittaa, että jos haluat Maijan ja Mattin molempien voivan lukea tiedoston, sinun pitää lisätä Maija tiedoston salauksen käyttäjälistaan.

### Tämä on vain harjoitus demo ja videon mukaan, ja hyvä harjoitus:

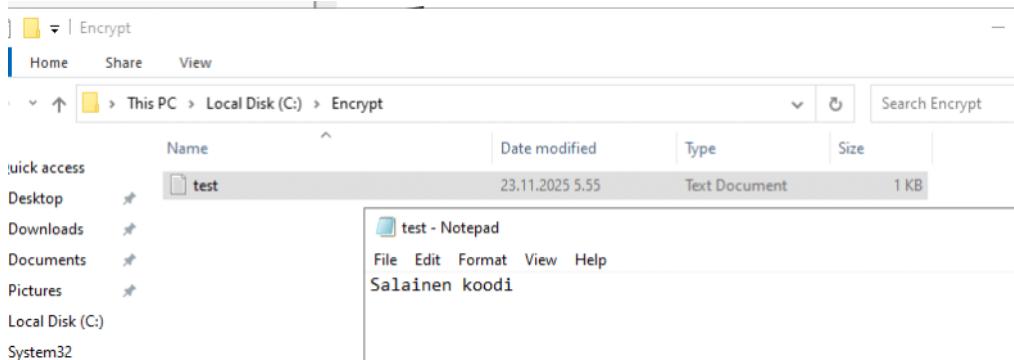
- Tämän linkin ja harjoitus ideana onkin kuinka asennettaan ja lukitaan enkryptaus (kryptaaminen suom. Salaaminen) - että testaa toisella tunnarilla esim. Jaettu C-levyn kansion alla ja toinen käyttäjä ei pysty avata sitä txt tiedostoa, mutta silti pääsee kansion alle.

[Learn how to setup the Encrypting File Service EFS in Windows Server 2022](#)



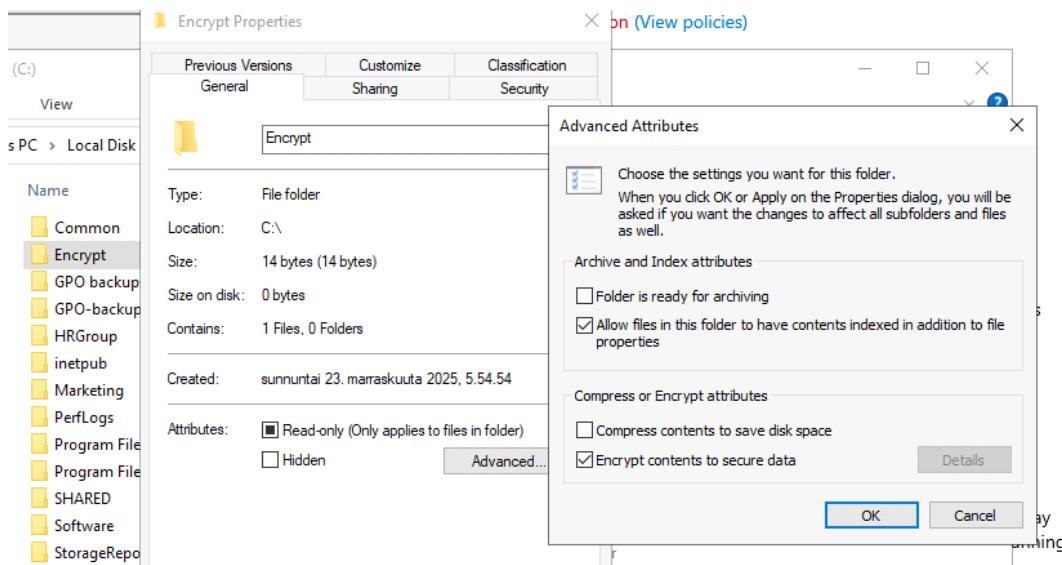
## OMA TOIMINTA - START HERE;

Ekana luodaan C:-levyn kansio ja txt - joku teksti riittää ja huom tämä on harjoitus ja ei tarvitse olla mitään salaista.



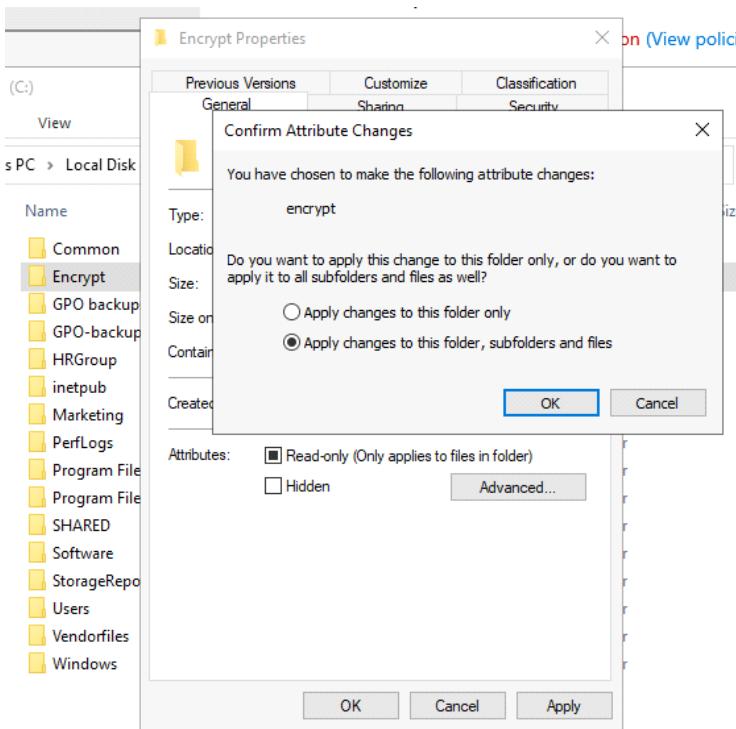
Avaa "encrypt" kansiosta kaksois klikkaus >> properties

Advanced alhaalta valitaan "encrypt contents to secure data" --> OK , ja Apply ja siitä tulee ilmoitus



Tämä ilmoitus tulee näkyviinsä, koska halutaan tehdä muutosta kansioon tai sitä alkansiolle (sub folder) ja siitä tiedostoille, eli "encrypt" kansioon mitä sen alla kuuluukaan.

- Jos valittaisi "apply changes to this folder only" - niin se tarkoittaa "encrypt" kansion sisäisiens tiedostot ei tule kryptatuksi.
- Harjoituksen kannalta tämä on ok.
- Apply ja OK



Kun tarkistellaan "advanced..." >> "details" - niin nähdään vähä lisätietoa/yksikohtaisempaa tietoa.

- Tässä on pari eri sertifikaattia

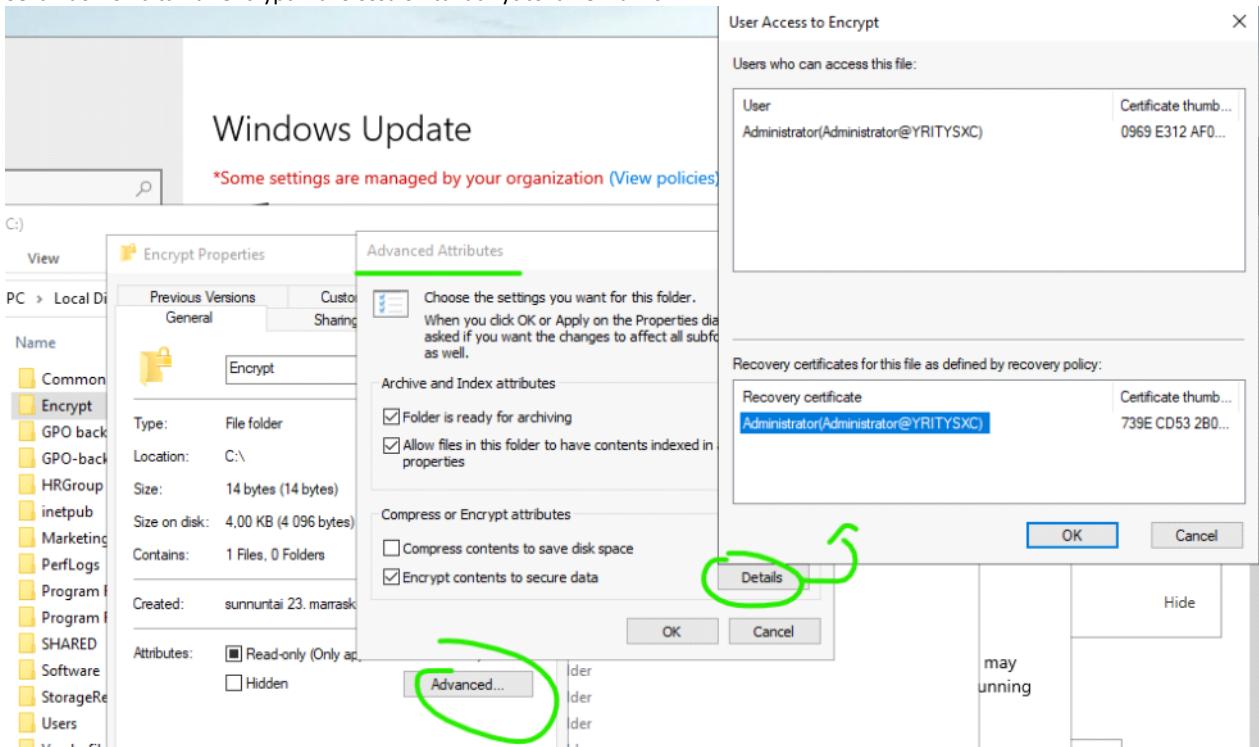
### Users who can access this file

- Tämä lista näyttää **ne käyttäjät, joiden julkinen avain on liitetty tiedoston salaukseen.**
- Käytännössä: kun tiedosto salataan, sen sisällön salausavain (FEK, *File Encryption Key*) salataan jokaisen valtuutetun käyttäjän julkisella avaimella.
- Nämä ollaan jokainen listassa oleva käyttäjä voi omalla yksityisellä avaimellaan purkaa FEK:n ja avata tiedoston.
- Tämä on se normaali käyttö: Matti salaa tiedoston ja lisää Maijan käyttäjäksi → molemmat voivat lukea tiedoston omilla tunnuksillaan.

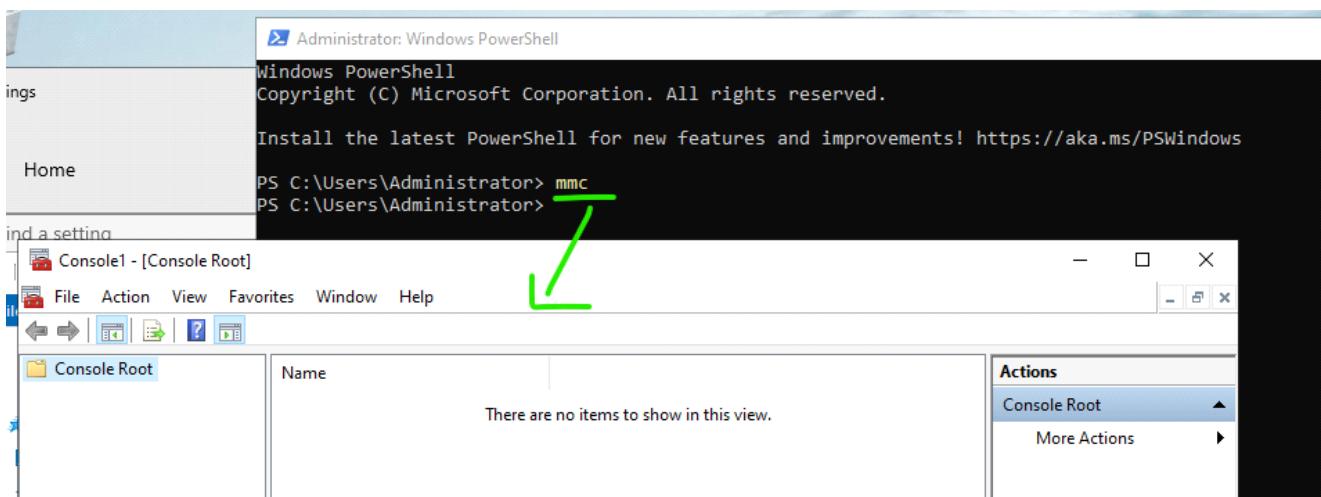
### Recovery certificates for this file (as defined by recovery policy)

- Tämä liittyy **EFS Recovery Agent -käytäntöön**, joka on erityisen tärkeä Windows Server / AD-ymäristössä.
- Recovery Agent on nimetty käyttäjä (yleensä domain admin), jonka sertifikaatti lisätään automaattisesti salattuihin tiedostoihin.
- Jos alkuperäinen käyttäjä (esim. Matti) menettää avaimensa tai salasana unohtuu, Recovery Agent voi silti purkaa tiedoston.
- Tämä on siis **varmuusmekanismi**: ettei käy niin, että tiedosto jää ikuisesti lukiutuksi, jos käyttäjän avain katoaa.

Sekä huomoina tämä "encrypt" kansiossa on tullut nyt tollainen lukko.

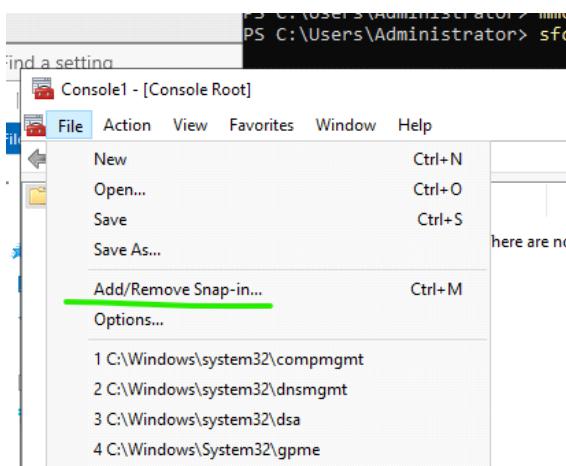


Seuraavaksi mennään "microsoft amangement console" työkaluun ja avaa cmd/powershell kautta komennolla >> mmc

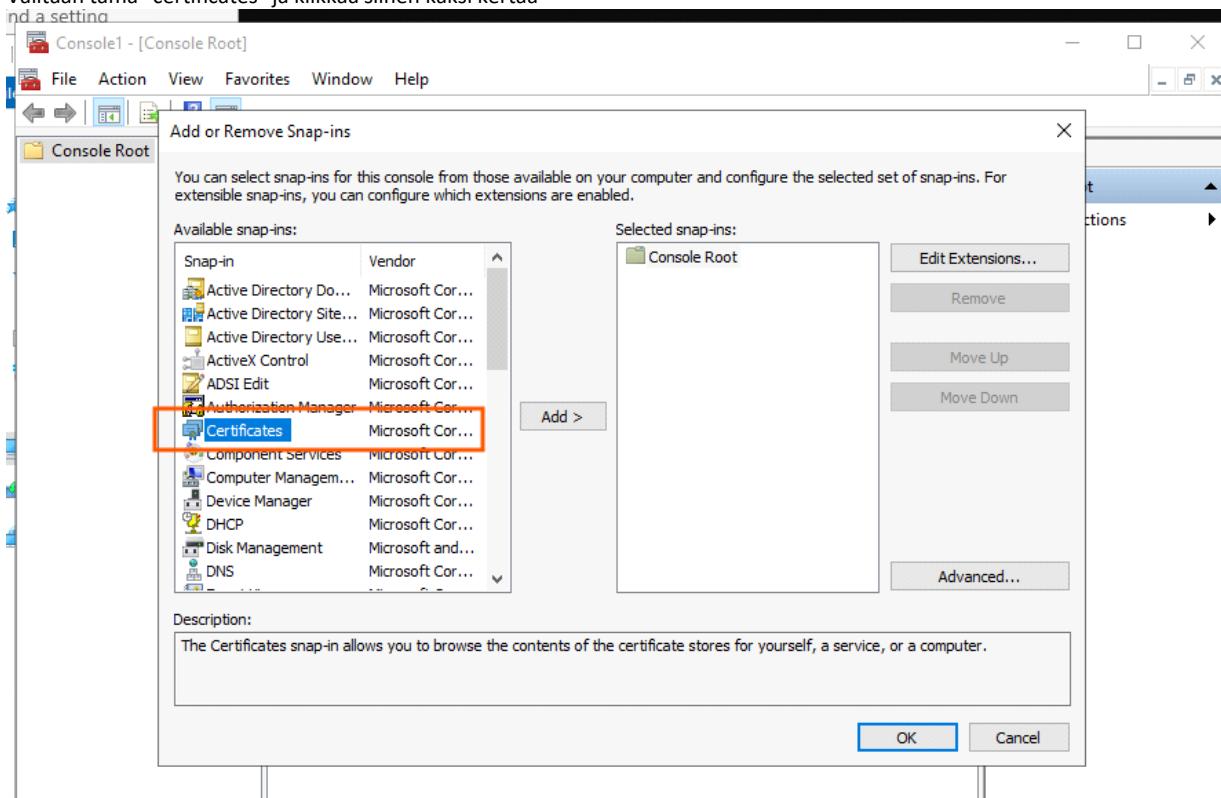


Valitse "File >> Add/remove snap-in.."

Tämän ideana on kuin nähdä jokaista sovellusta et vähä kuin mitä työkalua on tarjolla

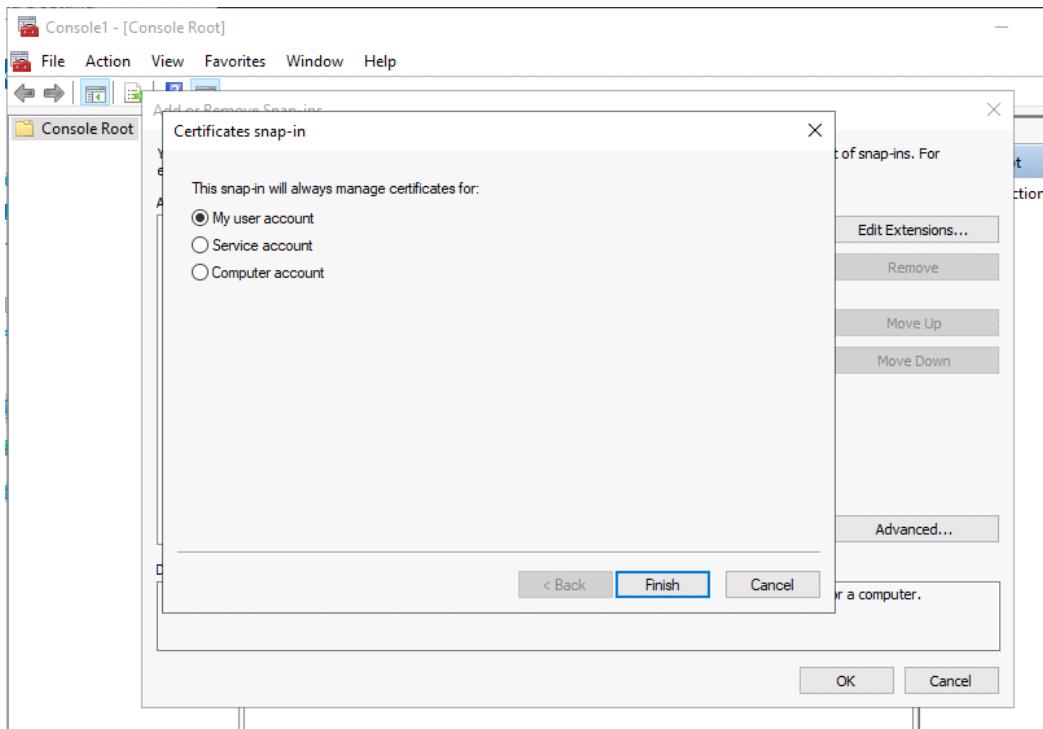


Valitaan tämä "certificates" ja klikkaa siihen kaksi kertaa



Valitaan "my user accounts" - koska kuin muotoilee uudestaan ja se on kuin admin EFS:ää varten

- Finish ja OK



Tästä nähdään se sertifikaatti on kuin automaattisesti luotu encrypttattuun tiedostoon varten

**MMC → Certificates (Current User) → Personal → Certificates**, näet ne sertifikaatit, jotka on liitetty juuri sinun käyttäjätiliisi (administrator). Tämä on se paikka, jossa EFS ja muut Windowsin salaus- ja tunnistautumismekanismit käyttävät avaimiaan.

- Muut sertifikaatit voivat liittyä sähköpostiin, tunnistautumiseen tai allekirjoituksiin.
- Tärkein huomio: **pidä EFS-sertifikaatista varmuuskopio**, muuten riskinä on datan menettäminen.

#### Muut sertifikaatit (esim. sähköposti, autentikointi, allekirjoitus)

- Personal-kansiossa voi olla myös muita sertifikaatteja, kuten S/MIME-sähköpostin salaukseen, digitaaliin allekirjoituksiin tai tunnistautumiseen.
- Jokainen sertifikaatti kertoo: *mihin tarkoitukseen se on myönnetty* (Usage: Encryption, Digital Signature, Authentication jne.).

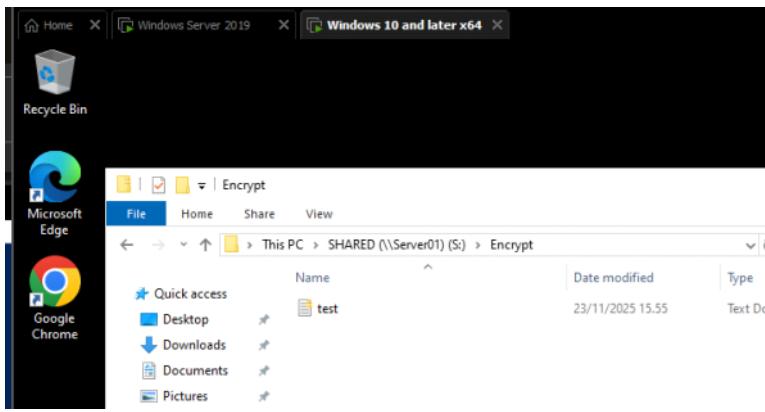
Actions	Certificates
More Actions	

Takaisin C-levyyn ja encrypt kansiosta tarkistettuna siinä on pieni lukko (keltainen lukko)

- Kun on administrator siis tunnuksella windows serverissä niin pääsee tarkistaa txt tiedostonsa, mitä siinä lukekaan.
- Jos kirjauduttaisiin toisella tunnuksella sisään niin voiko toinen käyttäjä lukea tästä txt tiedostoa?
  - Riittää avaa VM2

Huomioina tässä harjoituksessa siirsin VM1 (admin) siis Encrypt kansion tonne - SHARED kovalevyn ja tästä harjoitusta löytyy 5.2. S:\SHARED - ohje

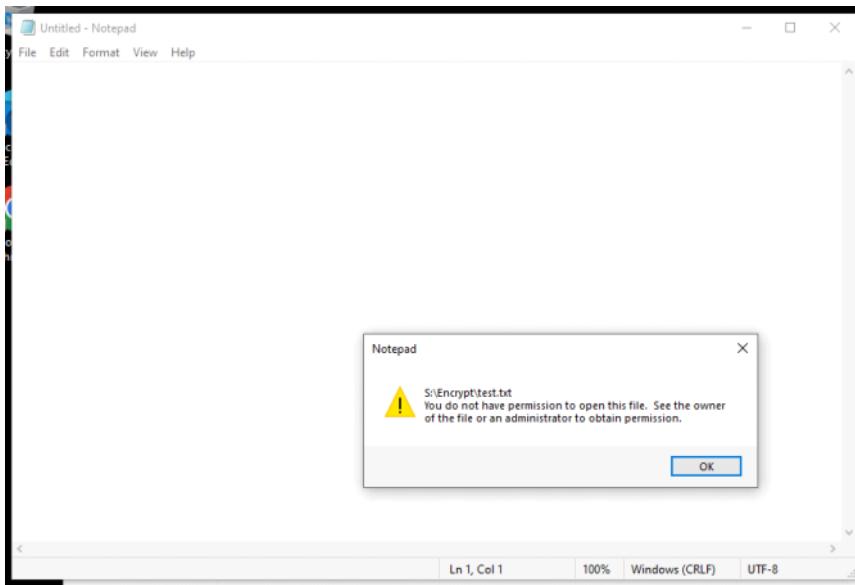
Tämä on VM2 tavallisen käyttäjän (Win10/11) näkymä, jos hän itse katsoo ja jos haluaa nähdä mitä encrypt kansion tiedostoja oon ja mitä siellä lukee



Perus ei ole oikeutta lukea ja päästä katsoo tämän txt tiedostoa.

Tämä päätee myös dekryptattua tiedostoa

Jos tämä käyttäjä (user1) haluaisi lukea tämän tiedoston niin jouduttaisiin lisämään ryhmään ja määrittää administrator oikeutta, jotta päästään lukea tämän enkryptattua / salattua tiedostoa.

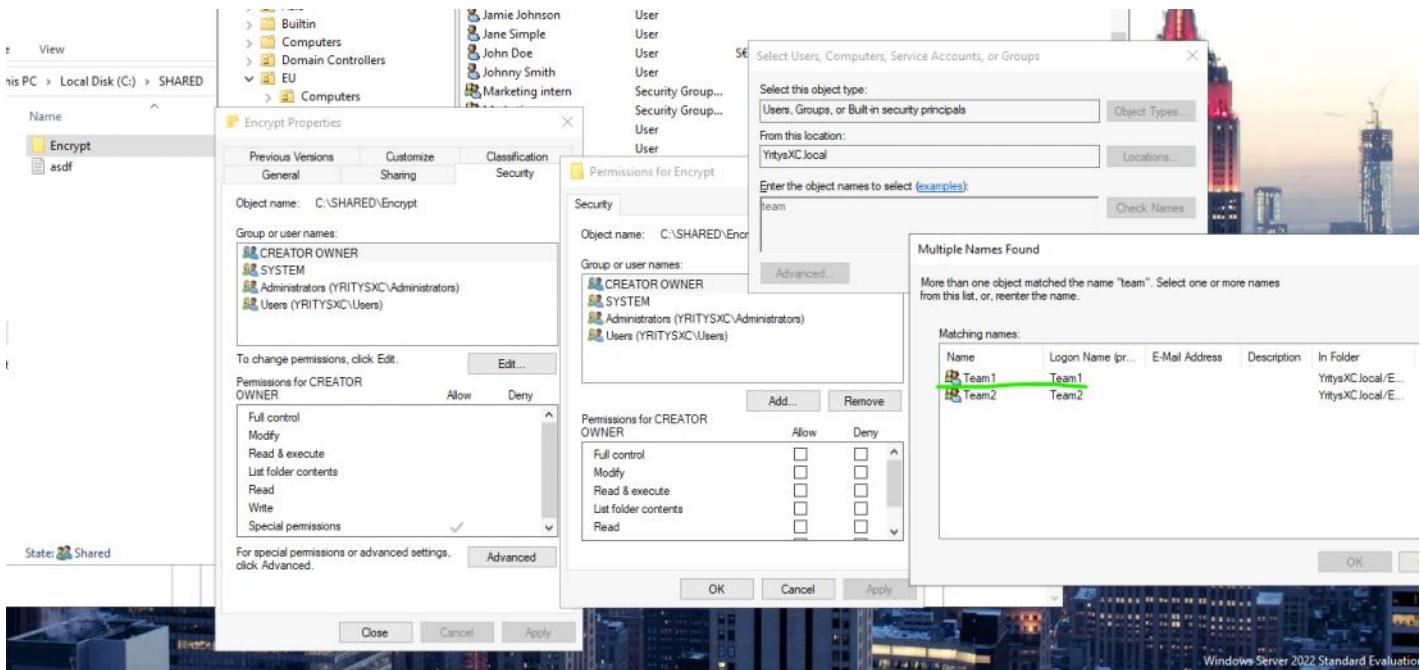


## OIKEUDEN ANTAMINEN - START HERE;

- **Tämä päätee kansion ominaisuudesta, että mikä se polku onkaan ja viittauksia::**
  - General-välilehti → Advanced → Encrypt contents to secure data → Tämä on se polku, jolla otat EFS-salausen käyttöön tiedostolle tai kansiolle. → Kun valitset tämän, Windows salaa sisällön käyttäjätilisi sertifikaatilla.
  - **Security-välilehti (NTFS-oikeudet)** → Täällä hallitaan käyttöoikeuksia: kuka voi avata tiedoston/kansion käyttöjärjestelmän tasolla. → Tämä ei itsessään salaa sisältöä, vaan estää/antaa pääsyn.
  - **Sharing-välilehti** → Tämä liittyy verkkjakoon: kuka voi käyttää resurssia verkon yli. → Ei liity salaukseen, vaan jakamiseen.
- **EFS-salaus = General-välilehti → Advanced → Encrypt contents to secure data**
- **NTFS-oikeudet = Security-välilehti**
- **Verkkjakaminen = Sharing-välilehti**

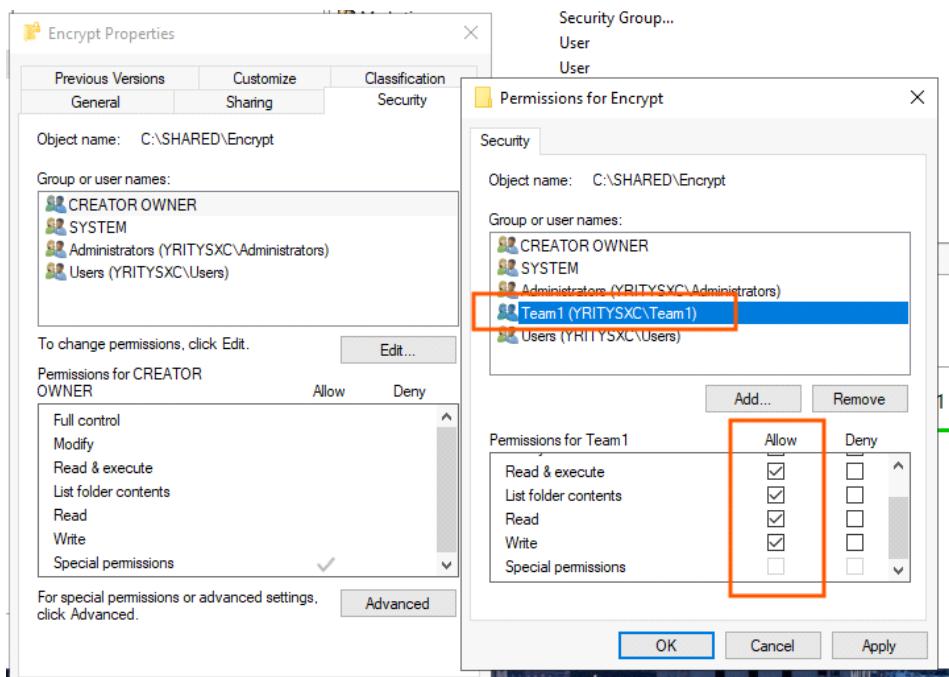
### Pieni skenaario / kuvaus:

- Kokeillaan luoda joku ryhmä, että miten tätä ryhmää annetaan "encrypt" kansion oikeus jotta vain nimetyt henkilöt voivat lukea tämän txt tiedoston. Lisäksi ryhmästä oikeudesta kokeillaan että voi lukea ja editoida.
- Muut käyttäjät ja ryhmät ei voi lukea ja editoida.

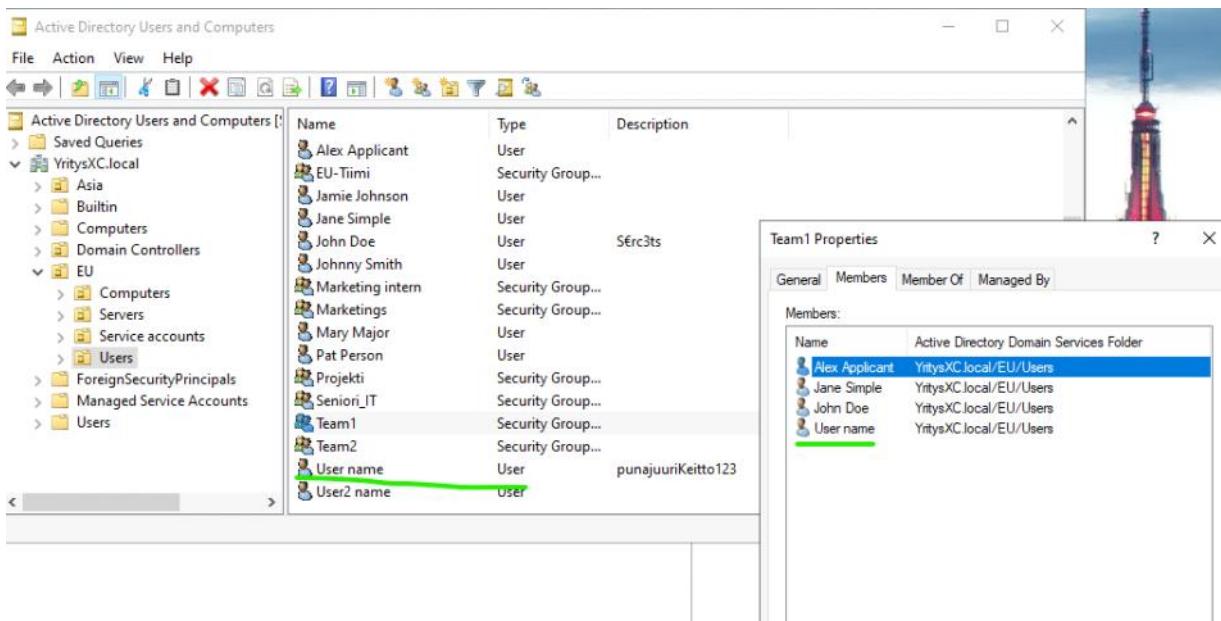
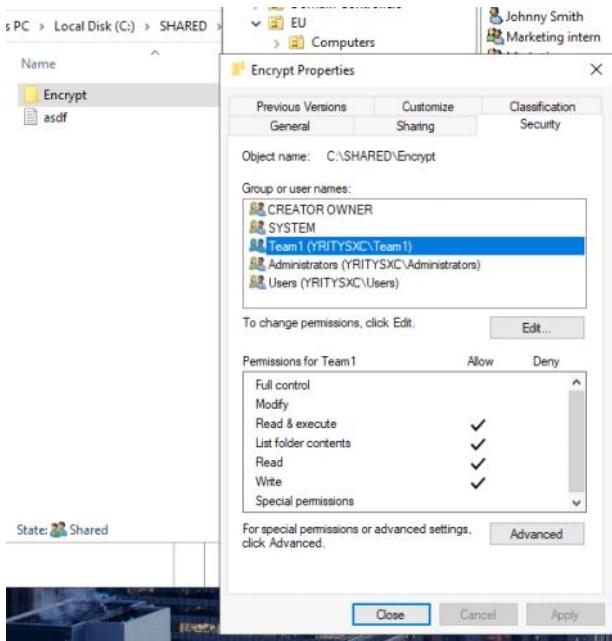


Oikeudesta määritetty:

- Read & execute
- List folder contents
- Read
- Write



Apply ja OK



Tässä oli muutamia pieniä säätöjä välissä, mutta vasta jälkeen katsottu osa videoita ja kkysytty tekoälyltä apua, että se on tiedostolle (txt) johon tulee ne oikeudet käyttäjään/ryhmän alle. Pari-muutamien säätöjä takana, josta kokeiltiin asettaa kansion EFS kautta joko shared/NTFS polkuun ryhmille se oikeus joko Full control ja jne , mutta todellinen vastaus on se tiedoston alle.

## Mini pohdinta ja koskien EFS asetuksesta - 1:

Pientä säätöä asetusten kanssa, mutta ideana on juuri se, että tiedoston **Details**-kohdasta voidaan lisätä käyttäjiä, joilla on oikeus avata ja muokata salattua tiedostoa. Tässä pohdinnassa ja asetusten säättämisessä on hyvä muistaa, että jokaisella käyttäjällä, jotka löytyvät Active Directoryn *Users*-kontista tai organisaatioyksiköiden (OU) alta – eli nimetyt henkilökunnan jäsenet – täytyy olla oma **EFS-sertifikaatti**. Tämä toimii vähän kuin henkilökohtainen tunniste: ilman sertifikaattia käyttäjää ei voi lisätä tiedoston salauksen piiriin, vaikka hänen olisi NTFS- tai share-oikeudet.

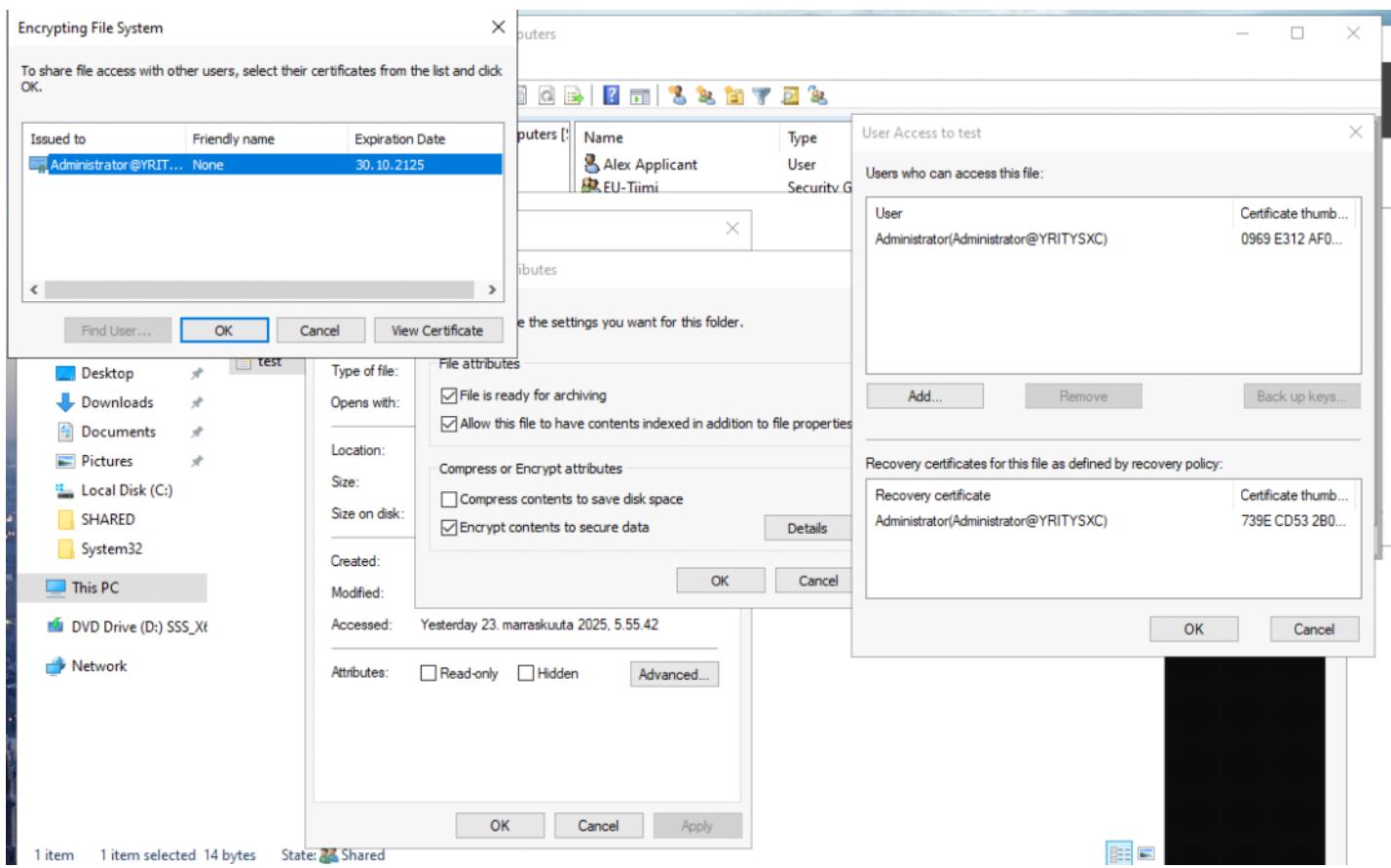
Koska EFS on tiedostokohtainen salausmenetelmä, sen kautta varmistetaan, että vain valtuutetut käyttäjät voivat avata sisällön. Kun käyttäjä lisätään Encrypting File Systemin alle, hänet voidaan sallia muokkaamaan tiedostoa (esim. txt). Sertifikaatti luodaan automaattisesti, kun käyttäjä ensimmäisen kerran salaa tiedoston tai kansion. Sertifikaatti sisältää **julkisen ja yksityisen avaimen parin**:

- **Julkinen avain** → käytetään tiedoston salausavaimen (FEK, File Encryption Key) salaamiseen.
- **Yksityinen avain** → käytetään FEK:n purkamiseen, jolloin tiedosto voidaan avata ja lukea normaalisti.

Jos käyttäjällä ei ole vielä luotu EFS-sertifikaattia, se voidaan **exportata/importata MMC:stä (.pfx-tiedosto)**. Exportin yhteydessä yksityinen avain täytyy suojaata salasanalla, jotta se pysyy turvallisena. Importointi onnistuu vain käyttäjän omaan profiiliin, ei ryhmälle. Tämä on tärkeä huomio: ryhmillä ei ole omaa sertifikaattia, joten EFS toimii vain yksittäisten käyttäjien tasolla.

Lisäksi Active Directory -ympäristössä kannattaa huomioida **Recovery Agent**. Tämä on hallinnollinen varmuusavaus, joka lisätään automaattisesti tiedostoihin organisaation EFS-politiikan mukaisesti. Recovery Agentin sertifikaatti mahdollistaa sen, että tiedosto voidaan palauttaa, vaikka alkuperäinen käyttäjä menettäisi avaimensa tai profiiliinsa korruptoituisi. Tämä on olennainen osa EFS:n hallintaa, erityisesti palvelinympäristössä.

Tästä ohjelmasta jatkuu harjoitus toiseen sivustoon, mutta välissä on pieni pohdinta koskien sertifikaattista on hyvä myös ottaa varmuuskopiointi.



## Harjoitus teema jatkuu toisessa sivussa (BITLOCKER & EFS - 2)