

7.1.2. EFS - 3

Thursday, November 27, 2025 14:41

HARJOITUS TEEMA JATKUU - START HERE;

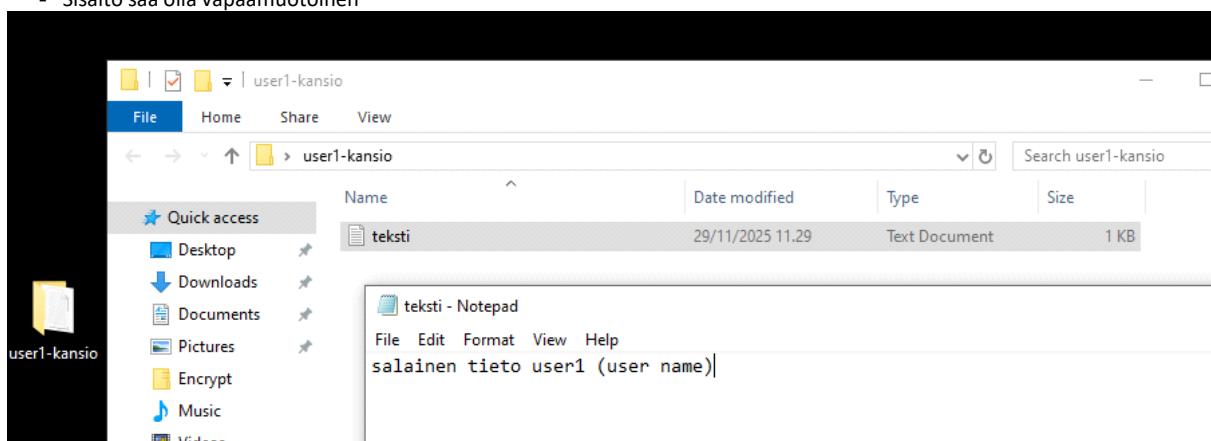
Tämä harjoitus jatkuu - tästä löytyy sama ohje ja video youtubestä.

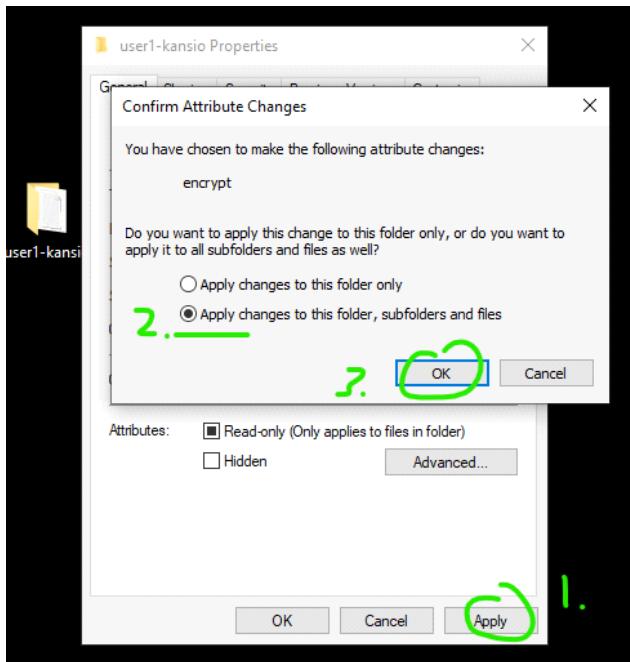
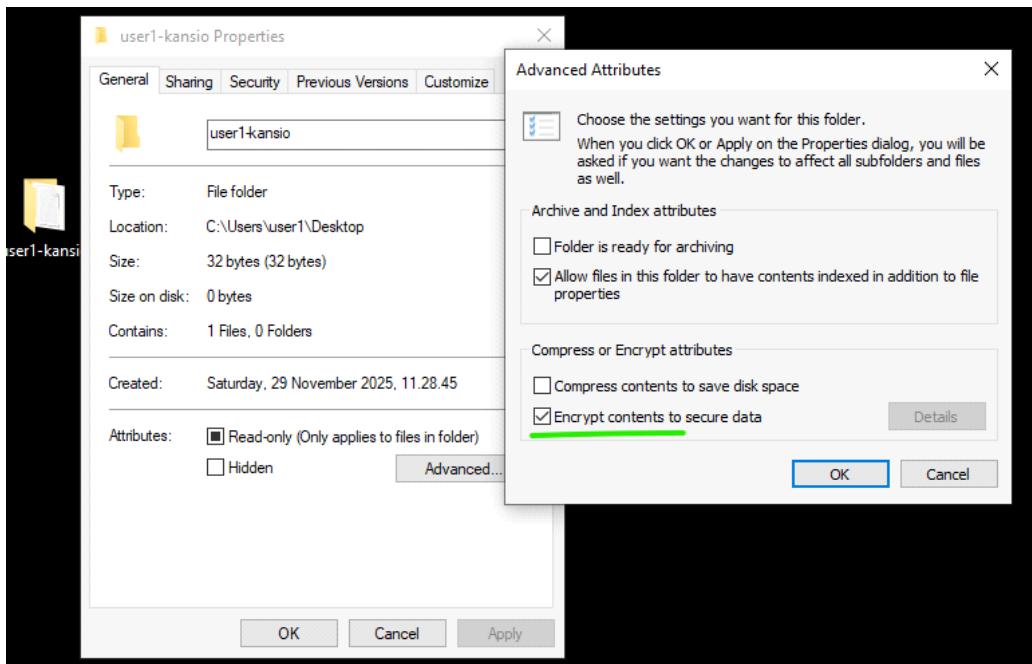


Nyt jatkuu 17. video eli backup ja varmuuskopiointi EFS sertifikaatti.

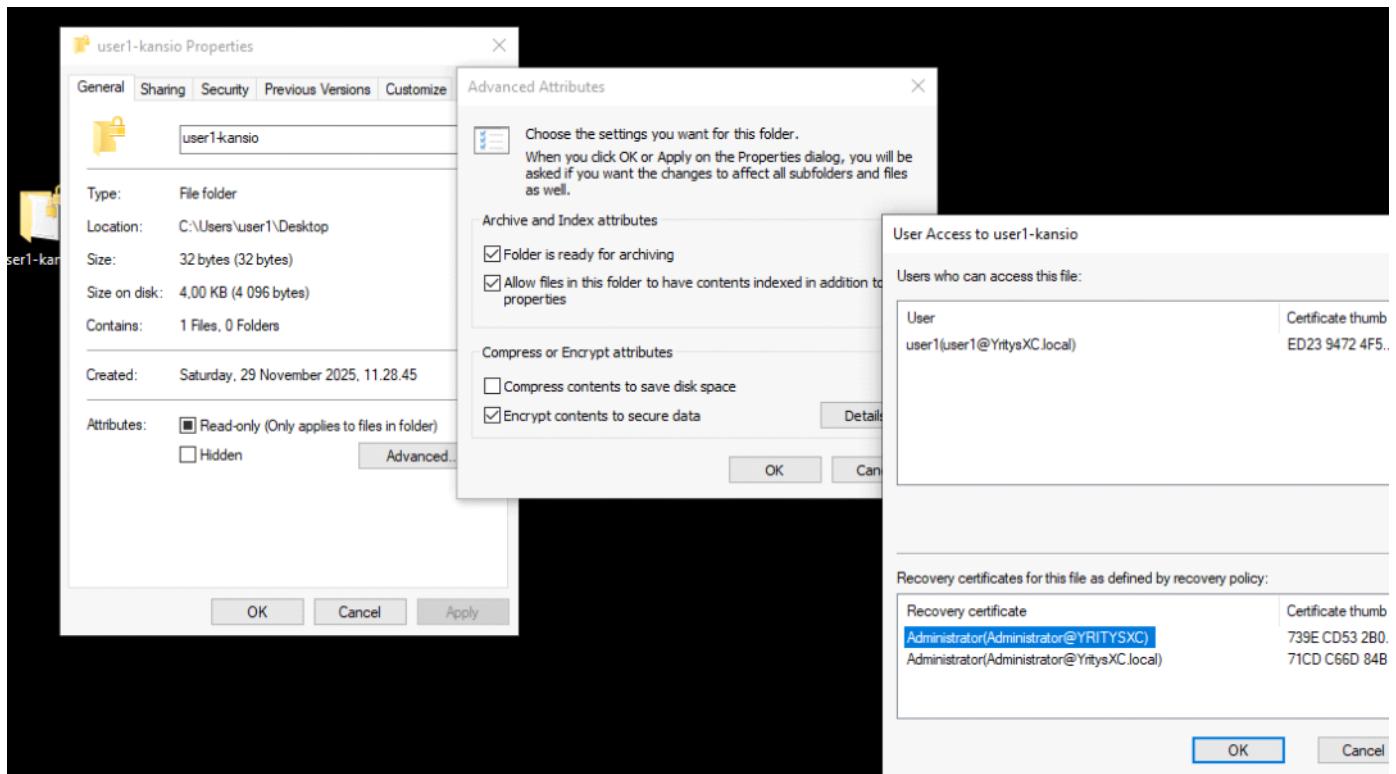
Tämä on vm2 (user) joku niistä ja desktop joku kansio - ja voi esim. Aloittaa tyhjästä ja encryppta sen kansio tyyppi ja sama kuin aikaisempi harjoitus

- Sisältö saa olla vapaamuotoinen



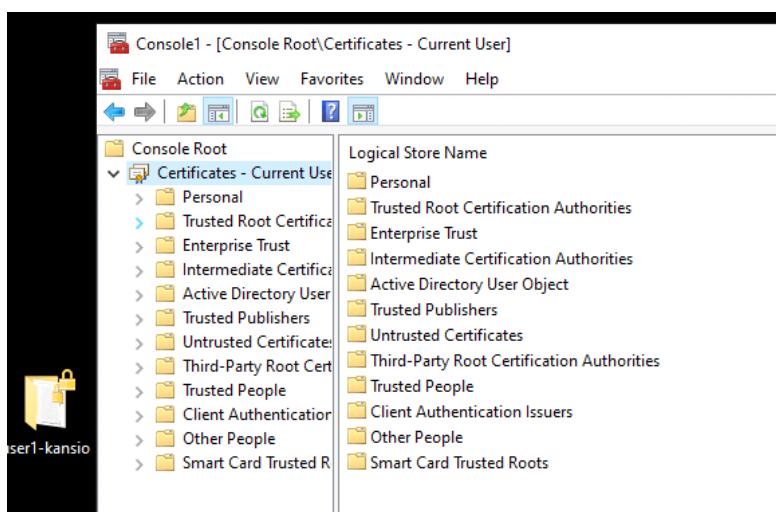


Detail tarkennus tästä kansiosta enkryptatusta tiedosta yksityiskohtaa ja lisätietona että täsmennyttä kuin omistaja on tämä käyttäjä.



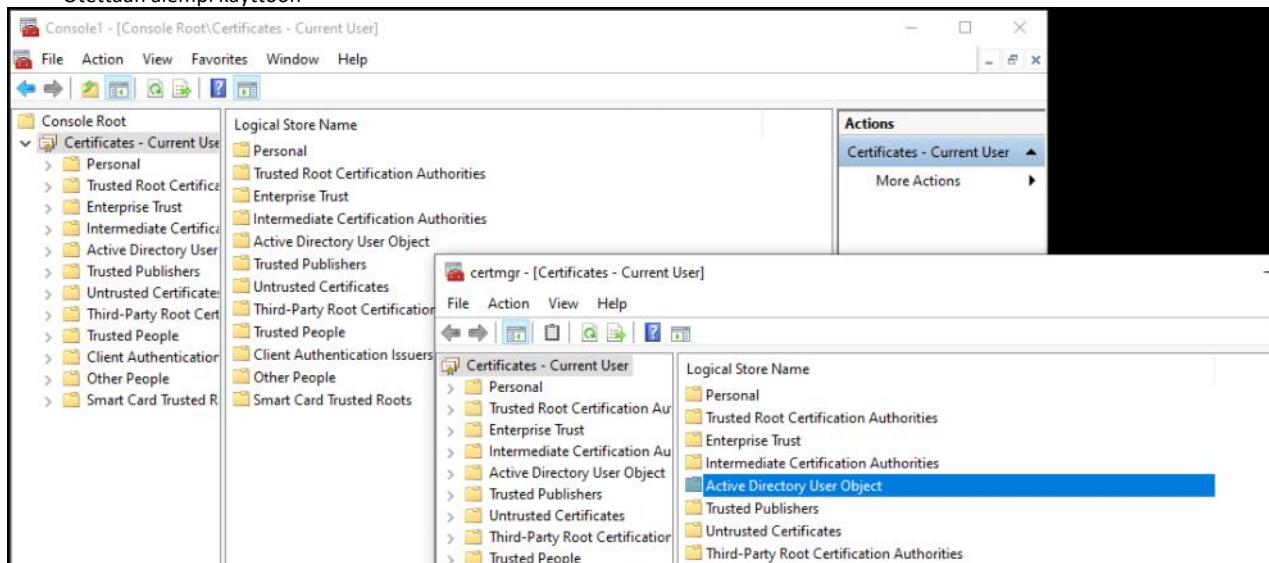
EFS back start toiminta nyt ja tarvitsee mmc.

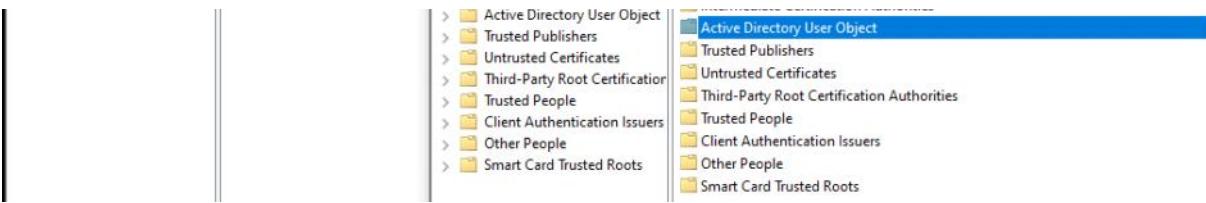
Tarvitaan tämä ja toinen



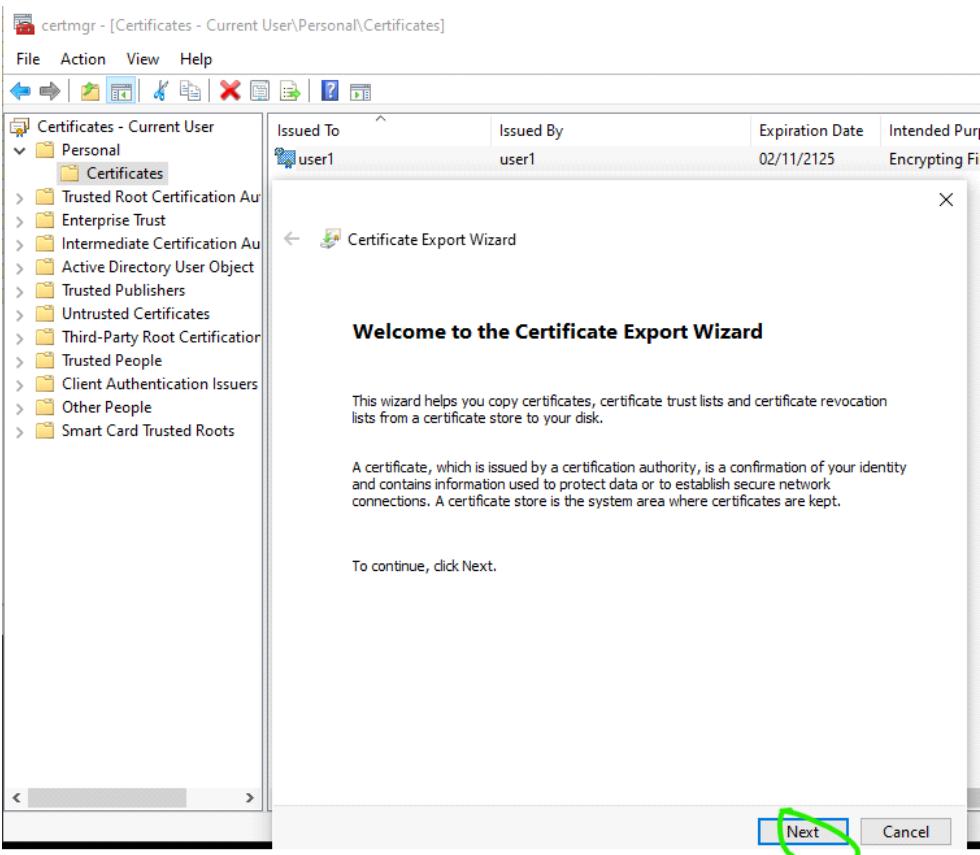
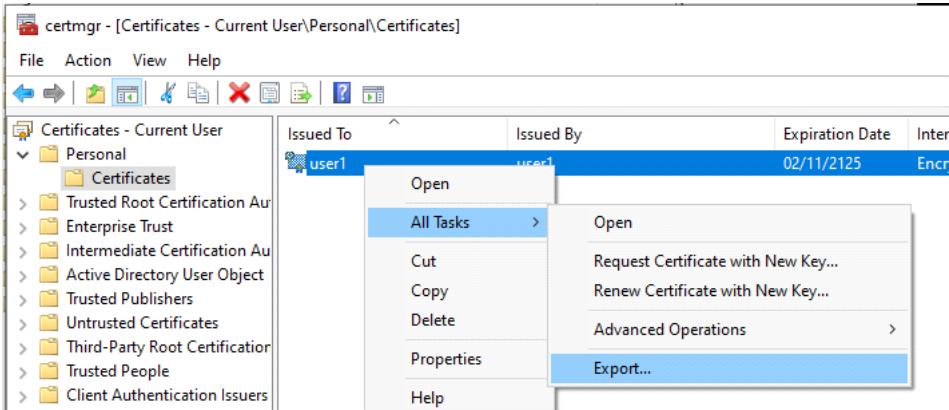
Tämä on sama idea mutta nimetty komento eri tavalla (win logo + R) ja haulla: certmgr.msc

- Otetaan alempi käyttöön





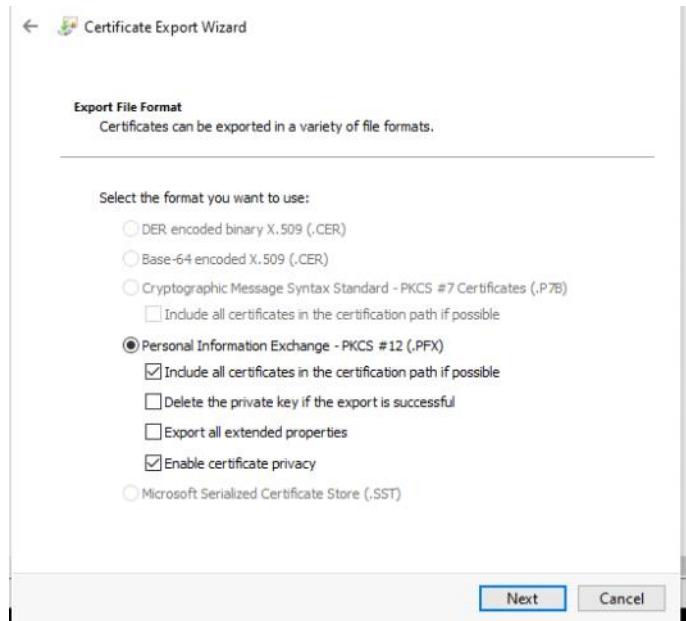
Eli tästä



Tästä saadaan backup private avain

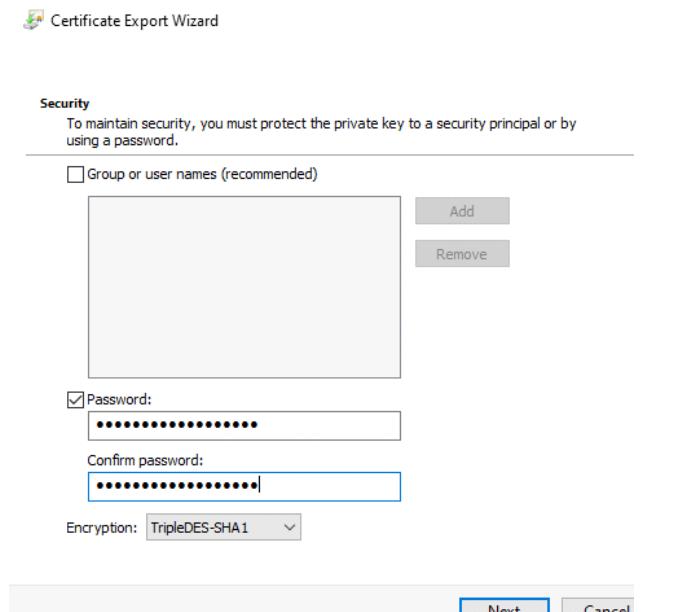


Ei kosketa mitään ja suoraan next

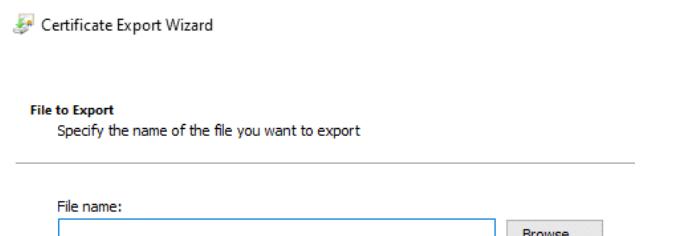


Salasana: punajuuriKeitto123

Kirjoita tarvittaessa johonkin ylös - mutta simppeli mieluiten



Klikkaa browse ja valitse se polku mihin tallennettaan, ja joku nimikke





File to Export

Specify the name of the file you want to export

File name:

C:\Users\user1\user1.pfx

[Browse...](#)

Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

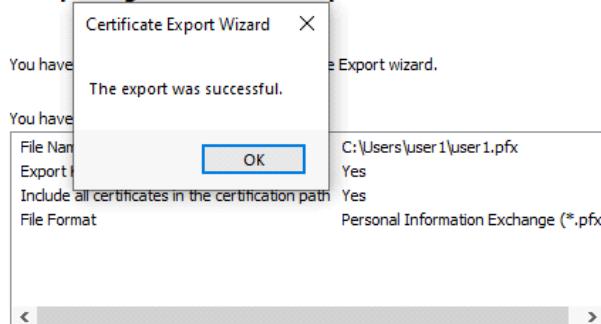
You have specified the following settings:

File Name	C:\Users\user1\user1.pfx
Export Keys	Yes
Include all certificates in the certification path	Yes
File Format	Personal Information Exchange (*.pfx)

[«](#) [»](#)



Completing the Certificate Export Wizard



Tarkistetaan se polku ja se export

This PC > Local Disk (C:) > Users > user1 >				▼	↻	Search user1
Name		Date modified	Type	Size		
3D Objects		05/11/2025 19.51	File folder			
Contacts		05/11/2025 19.51	File folder			
Desktop		29/11/2025 11.28	File folder			
Documents		05/11/2025 19.51	File folder			
Downloads		08/11/2025 14.52	File folder			
Favorites		05/11/2025 19.51	File folder			
Links		05/11/2025 19.51	File folder			
Music		05/11/2025 19.51	File folder			
OneDrive		07/11/2025 12.58	File folder			
Pictures		05/11/2025 20.00	File folder			
Saved Games		05/11/2025 19.51	File folder			
Searches		05/11/2025 19.53	File folder			
Videos		09/11/2025 15.15	File folder			
user1		29/11/2025 11.48	Personal Informati...	5 KB		

Takaisin "certmgr" välilehteen ja poistetaan tämä osuus:

certmgr - [Certificates - Current User\Personal\Certificates]

File Action View Help

Certificates - Current User

Personal

Certificates

Issued To: user1

Issued By: user1

Expiration Date: 02/11/2125

Intended Purposes: Encrypting File Syst...

Open

All Tasks

Cut

Copy

Delete

Certificates

You will not be able to read encrypted data using this certificate.
Do you want to delete this certificate?

Yes (highlighted with a green circle)

No

Ja varmistetaan se on poistettu, ja buuttaa kone (vm2)

Avataan ja testataan to desktop enkryptattu tiedosto ja avataan txt

- Huomataan ei ole oikeutta ja mitä ihmettää!!

File Home Share View

user1-kansio

teksti

Search user1-kansio

Quick access

Desktop

Downloads

Documents

Pictures

Encrypt

Music

user1-kansio

Videos

OneDrive

This PC

Network

Untitled - Notepad

File Edit Format View Help

Notepad

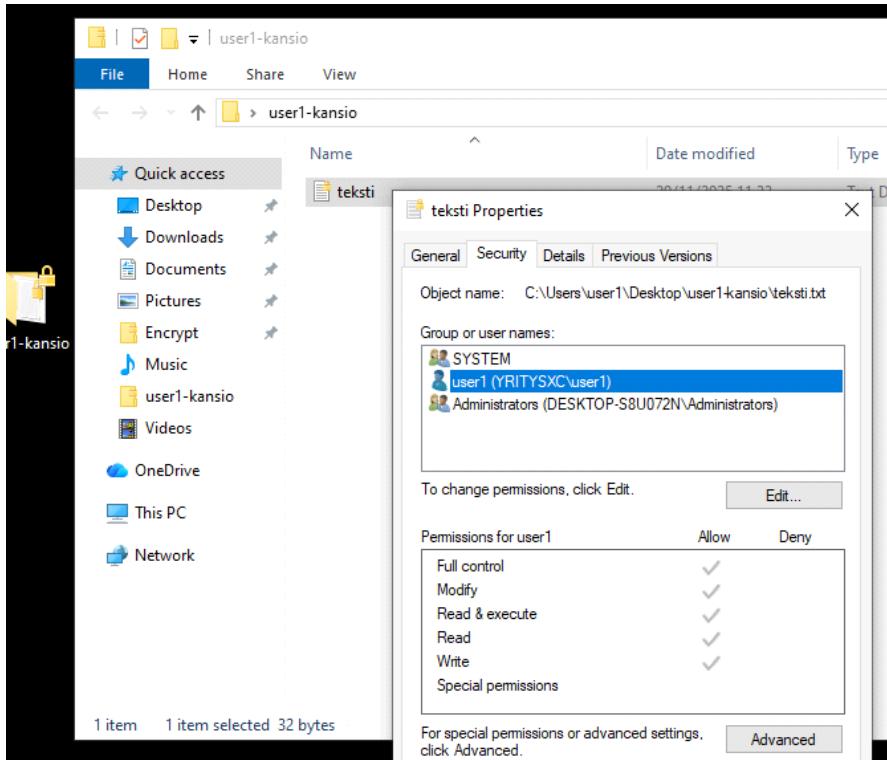
C:\Users\user1\Desktop\user1-kansio\teksti.txt

You do not have permission to open this file. See the owner of the file or an administrator to obtain permission.

OK

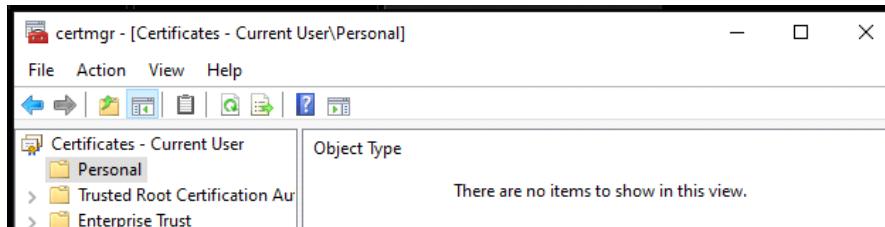
Avataan tämän txt ominaisuus (properties) ja security - polku

- Tästä huomataan käyttäjä itsensä on täys oikeus, mutta johtuen tästä sertifikaattista ja id:stä siksi varmaan tuli error

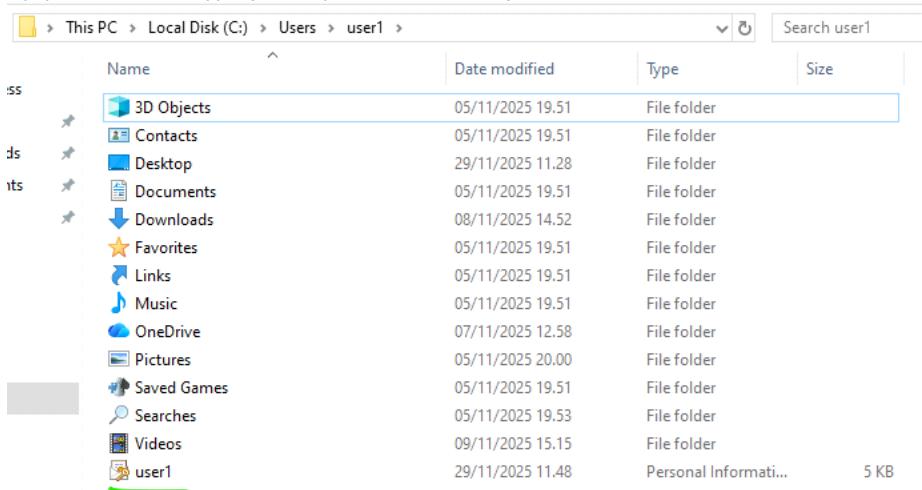


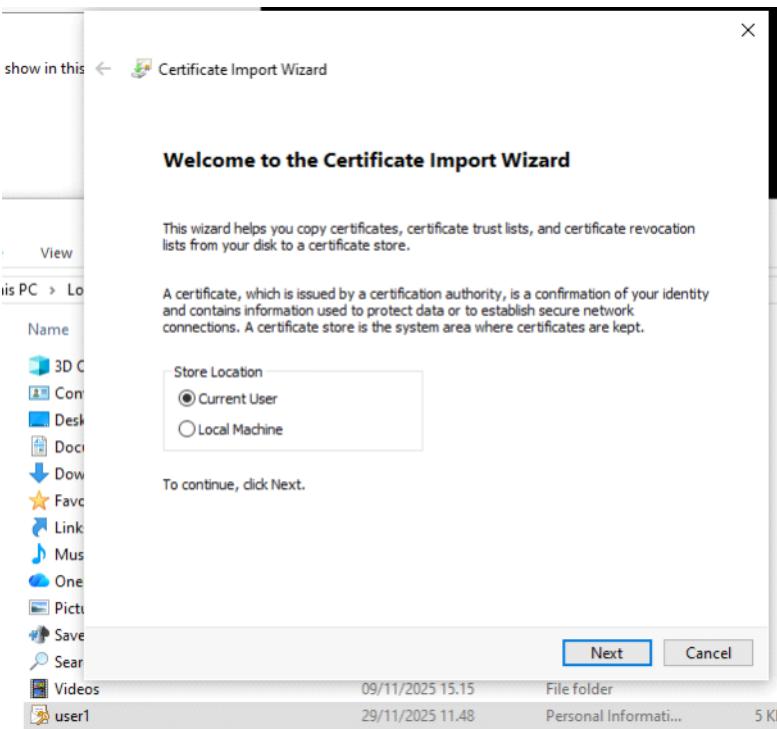
Seuraavaksi tarkistetaan to "certmgr.msc" js pika tarkistus

- Ja kyllä tyhjä

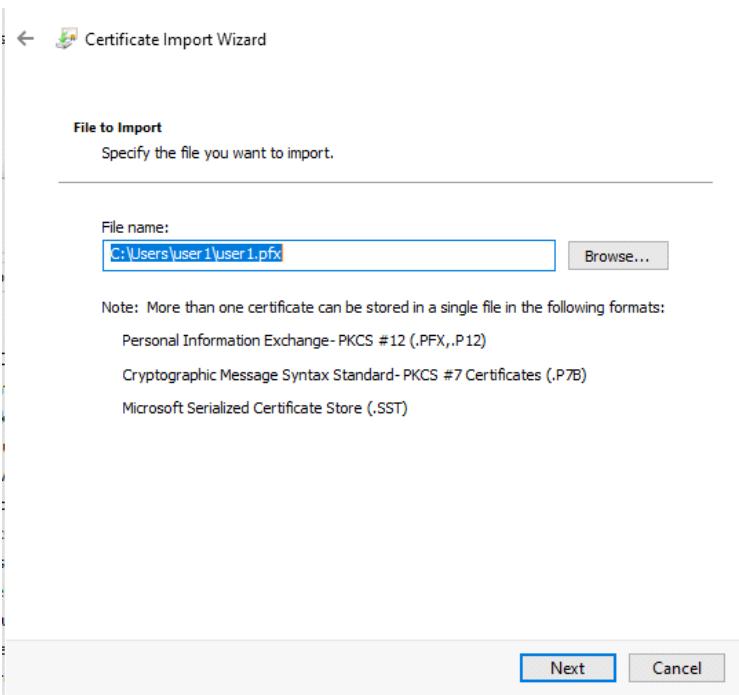


Nyt palataan local levyn , josta exportattiin se avain - ja kaksois klikaa siihen

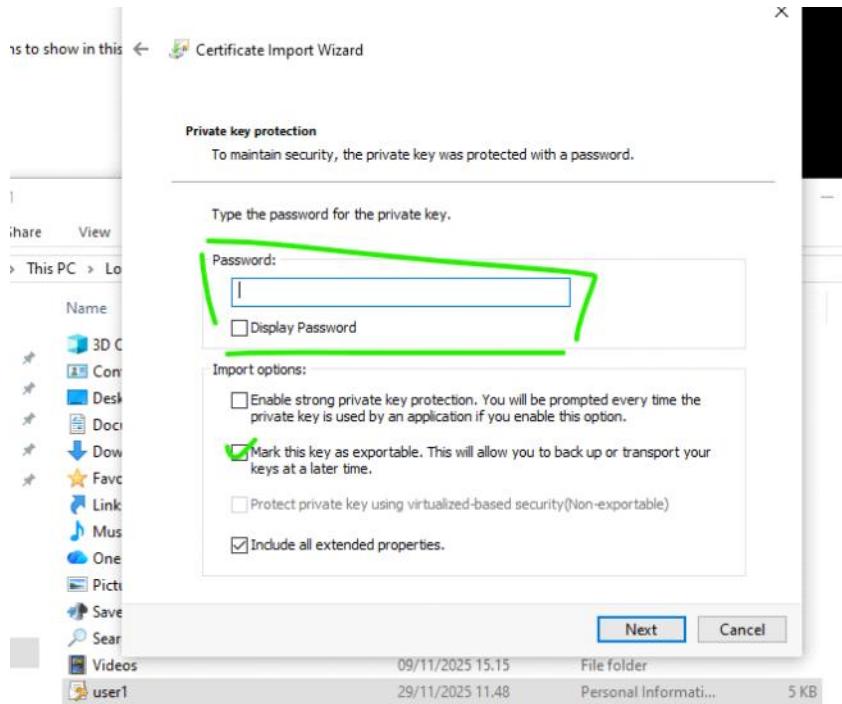




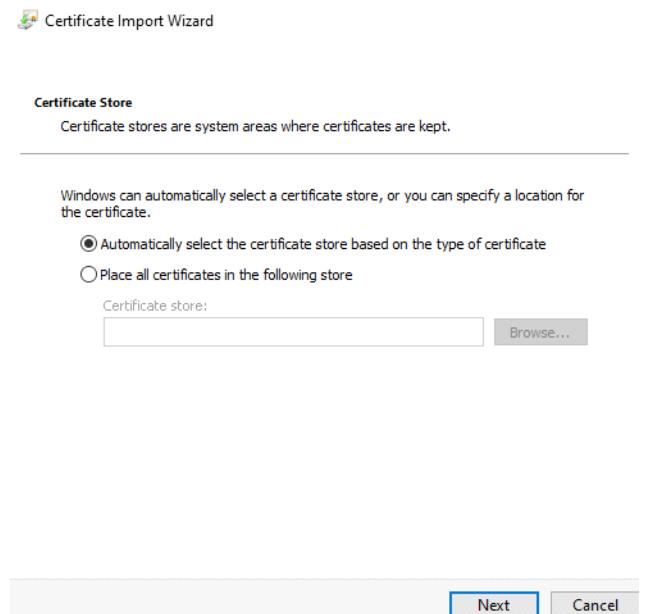
Tässä se kysyy mikä tiedosto , mutta oletuksena tässä harjoituksessa on vain tämä certifikaatti tieto niin vain tämä



Syötettää se salasana jonka aikaisempi exportattiin ja valittoi ruksi



Pidetään oletuksena ja next

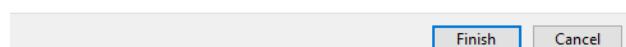


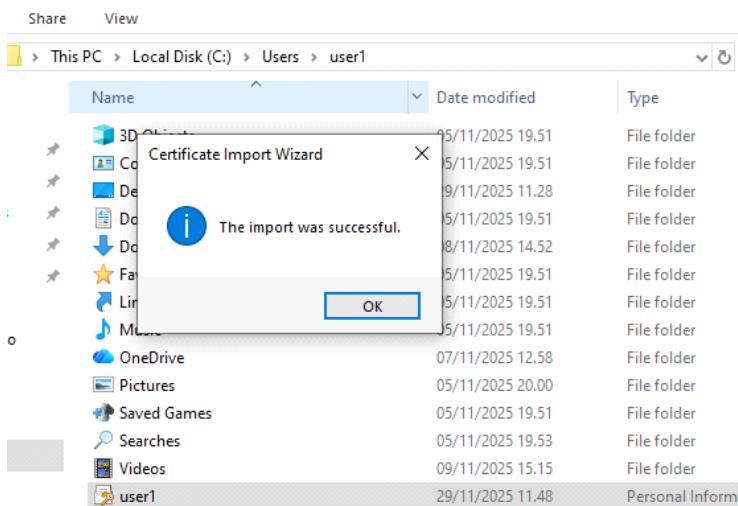
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

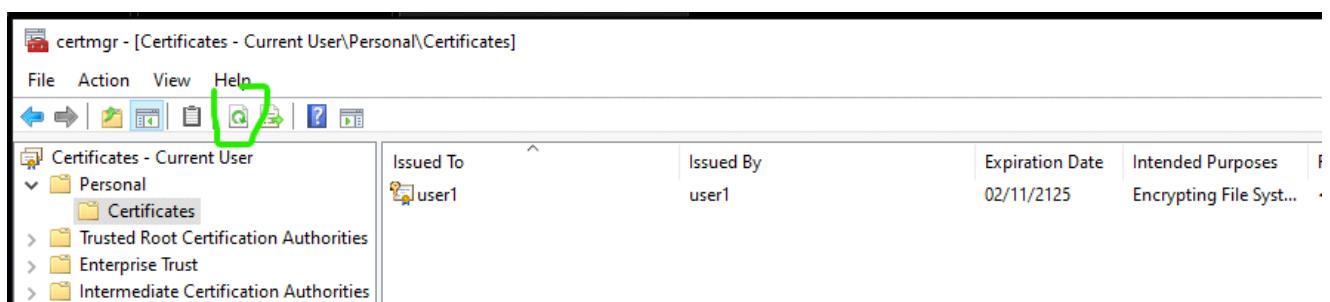
You have specified the following settings:

Certificate Store Selected	Automatically determined by the wizard
Content	PKCS#12
File Name	C:\Users\user1\user1.pfx



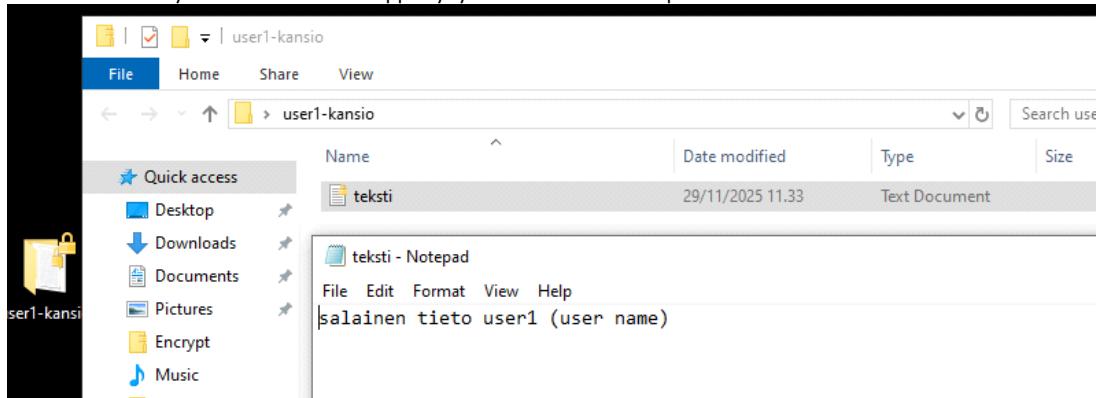


Tarkistetaan certmgr - ja yleensä ensimmäisenä näkymänä ei tule näkyviinsä, että on otettu varmuuskopiointi osuus ja siks kantsii päivittää tuosta (ympyröity käyttöliittymästä) niin se sen jälkeen tulee näkyviinsä.



Seuraavaksi tarkistetaan se desktop tiedosto ja huomataan, että on oikeus nyt editoida ja lukea sitä txt formaattia

- Tästä voidana nyt purkkaa se encrypt contents to secure data - eli takaisin normi txt formaattiin
- Sekä tästä nyt voidaan ikään kuin oppia lyhyesti miten saada backp efs certifikaattinsa



Tuossa videossa on toinen metodi vähä lopussa ([17. How to Backup and Restore EFS certificates](#)) että kuinka saa tällaisen efs certifikaattinsa ja backup prosessinsa, mutta sama idea.

Pieni teoria osa ja tästä harjoituksesta:

💡 Miksi et voinus avata tiedostoa vaikka NTFS-oikeudet olivat kunnossa?

- **EFS (Encrypting File System)** ei käytä NTFS-oikeuksia tiedoston sisällön salaamiseen.
- Kun teit *Encrypt contents to secure data*, Windows loi **EFS-sertifikaatin ja siihen liittyvän yksityisen avaimen** käyttäjällesi (User1).
- Salausavain tallennetaan käyttäjän sertifikaattivarastoon (certmgr).
- Kun poistit sertifikaatin (ja sen yksityisen avaimen), Windowsilla ei ollut enää mitään keinoa purkkaa tiedoston salausta.
- Siksi vaikka NTFS-Security-väliilehdellä näkyi *Full Control*, et voinus lukea tai muokata tiedostoa. NTFS sanoi "saat tehdä mitä haluat", mutta EFS sanoi "sinulla ei ole enää avainta".

💡 Mikä merkitys oli private key exportilla?

- Kun teit **export with private key**, loit käytännössä **varmuuskopion EFS-avaimestasi**.
- Tämä .pfx-tiedosto sisältää sekä sertifikaatin että yksityisen avaimen, suojaatuna salasanalla.
- Kun poistit alkuperäisen avaimen ja myöhemmin importoit sen takaisin (syöttämällä salasanan), Windows palautti EFS-avaimen käyttäjällesi.
- Heti kun avain oli taas käytettävissä, EFS pystyi purkamaan salauksen ja sait takaisin luku- ja muokkausoikeudet.

Pieni yhteenvetö ja pohdinta tässä välissä - START HERE;

Exportattu private key ei ole kansiokohtainen varmuuskopio, vaan käyttäjän EFS-avaimen varmuuskopio. Ilman tätä avainta tiedoston sisältö pysyy salattuna, vaikka administratorilla olisi täydet NTFS-oikeudet.

Jos salattu kansio siirretään esimerkiksi VM1 Windows Serverin administratorille, hän ei voi avata sitä ilman User1:n avainta .

- **HUOMIO:** EFS-sertifikaatti ja private key ovat aina käyttäjäkohtaisia.
- Vain User1 (tai se, jolla on exportattu avain ja sen salasana) voi avata tiedoston.
- Yritysympäristössä voidaan lisäksi määritää Data Recovery Agent, jolloin myös virallinen administrator voi avata tiedoston omalla recovery agentin avaimellaan. Ilman User1:n avainta tai recovery agenttia tiedosto pysyy salattuna.

EFS ei ole vain tekninen harjoitus, vaan siihen liittyy **hallinnollisia ja organisatorisia käytäntöjä**, jotka kannattaa dokumentoida.

Lisähuomio: Yrityksen näkökulmasta EFS-avainten hallinta on kriittistä erityisesti offboarding-tilanteissa.

- Jos käyttäjä poistuu organisaatiosta ilman että hänen EFS-avaimensa on varmuuskopioitu, salattuihin tiedostoihin ei enää päästää käsiksi.
- Administrator ei voi avata tiedostoja ilman käyttäjän avainta, ellei organisaatiossa ole määritetty Data Recovery Agentia tai käytössä ole AD CS:n key archival -toiminto.
- Tämä koskee yhtä lailla pieniä, keskisuuria ja suuria kansainvälisiä yrityksiä: jokaisessa tapauksessa on oltava selkeä prosessi avainten varmuuskopioinnille, palautukselle ja hallinnalle. Exportattu avain (.pfx) on erittäin arkaluonteinen, ja sen hallinta kuuluu tietoturvapolitiikan piiriin.

Mitä muuta kannattaa huomioida

- **Offboarding (työntekijän poistuminen):**
 - Jos käyttäjä lähtee yrityksestä, hänen EFS-avaimensa voi kadota ellei sitä ole varmuuskopioitu.
 - Ilman avainta yritys menettää pysyvästi pääsyn salattuihin tiedostoihin.
 - Siksi **pakollinen käytäntö**: ennen offboardingia varmistetaan, että käyttäjän EFS-sertifikaatti ja private key on talletettu hallitusti (esim. PKI + Key Archival tai Recovery Agent).
- **Administratorin rooli:**
 - Normaallilla adminilla ei ole automaattista pääsyä EFS-tiedostoihin.
 - Yrityksen tulee määritää **Data Recovery Agent (DRA)** Group Policyyllä, jotta hallittu palautus on mahdollista.
 - DRA:n avaimet pitää säilyttää turvallisesti (esim. HSM, suojaudu varasto), koska ne avaavat kaikkien käyttäjien salatut tiedostot.
- **Käytännön poliittiat:**
 - **Key Archival:** AD CS voi arkistoida käyttäjien EFS-avaimet automaattisesti, jolloin ne voidaan palauttaa myöhemmin.
 - **Dokumentointi:** jokaisessa organisaatiossa tulisi olla selkeä ohjeistus, miten EFS-avaimia käsitellään, varmuuskopioidaan ja palautetaan.
 - **Tietoturva:** exportattu avain (.pfx) on erittäin arkaluonteinen. Jos se annetaan adminille, hän voi avata käyttäjän tiedostot. Tämä pitää huomioida tietosuojakäytännöissä.
- **Yrityksen koon vaikutus:**
 - **Pienet yritykset:** usein ei ole PKI:tä, joten käytännön ratkaisu on varmuuskopioida avaimet manuaalisesti ja säilyttää ne turvallisesti.
 - **Keskisuuret yritykset:** kannattaa ottaa käyttöön AD CS ja määritää Recovery Agent.
 - **Suuret/kansainväliset yritykset:** yleensä käytössä on PKI, HSM ja tiukat prosessit avainten hallintaan, sekä auditointi ja compliance-vaatimukset (esim. GDPR, ISO 27001).

Jos käyttäjä unohtaa avaimen tai salasanan

- Ilman private keytä ja sen salasanaa tiedosto on käytännössä menetetty.
- Administrator ei voi ”arvata” tai murtaa salasanaa — EFS on suunniteltu estämään juuri sen.
- Exportattu avain (.pfx) on ainoa tapa palauttaa pääsy, ellei organisaatiossa ole Recovery Agentia.

Jos Recovery Agent on määritetty

- Kun Recovery Agent (DRA) on asetettu Group Policyyllä, jokainen EFS-salattu tiedosto salataan **kahdella avaimella**: käyttäjän omalla ja agentin avaimella.
- Tällöin administrator voi käyttää DRA:n private keytä ja avata tiedoston, vaikka käyttäjä olisi unohtanut oman avaimensa tai salasanansa.
- Tämä on se ”turvaverkko”, jota yrityksissä yleensä vaaditaan, jotta tiedot eivät katoa käyttäjän virheen takia.

Jos Recovery Agentia ei ole

- Vain käyttäjän oma avain toimii.
- Jos käyttäjä unohtaa salasanan eikä avainta ole varmuuskopioitu, tiedosto on pysyvästi salattu.
- Administrator ei voi tehdä mitään — tämä on EFS:n tietoturvaperiaate.

Neuvo yrityksille

- **Pakollinen käytäntö:** määritä Recovery Agent AD-ympäristössä.
- **Key Archival:** käytä AD CS:n key archival -toimintoa, jolloin käyttäjien avaimet tallentuvat automaattisesti PKI:hin.
- **Prosessi:** offboardingissa varmista, että käyttäjän avaimet ovat tallessa.
- **Tietoturva:** exportattujen avainten salasanat pitää hallita turvallisesti (esim. HSM, salattu varasto).

Jos käyttäjä unohtaa avaimen eikä Recovery Agentia ole, tiedosto on menetetty. Jos Recovery Agent on käytössä, administrator voi avata tiedoston hallitusti. Tämä on se syy, miksi **EFS ilman Recovery Agentia ei ole suositeltava ratkaisu yrityksissä**.

#####
#####

EFS:n tarkoitus verrattuna moderneihin vaihtoehtoihin

- **EFS (Encrypting File System)** suojaa NTFS-tiedostoja levyllä käyttäjän sertifikaatilla ja yksityisellä avaimella.
- Se on tehokas mutta rajattu: suojaa paikallisia tiedostoja käyttäjäkohtaisesti, ei ratkaise jakamista, synkronointia tai yhteistyötä.
- **Pilvipalvelut ja modernit työkalut** (OneDrive/SharePoint, Google Drive, iCloud, BitLocker, Microsoft Information Protection) ratkaisevat laajemmat tarpeet: käyttöoikeudet, jakaminen, elinkaaren hallinta, auditointi, DLP, laitehäviöt.

Milloin EFS on tarpeellinen ja milloin ei

- **Paikallinen työasema tai on-prem palvelin:**
 - Tarpeellinen, jos tiedostoja pitää suojaa myös järjestelmänvalvojalta tai offline-varkauksilta.
 - Ei vältämätön, jos BitLocker jo suojaa koko levyn ja riski on vain laitteen katoaminen.
- **Jaetut kansiot ja yhteistyö:**
 - Ei suositeltava: EFS sitoo tiedoston käyttäjän avaimiin, mikä vaikeuttaa jakamista.
 - Käytä NTFS-oikeuksia + BitLocker, tai Rights Management (MIP/RMS) jos halutaan salaus yli käyttäjien.
- **Pilvitallennus (Microsoft 365, Google Workspace, AWS S3):**
 - Käytä pilvialustan ACL-oikeuksia, DLP-sääntöjä, sensitivity-labeleita ja KMS-avaimia.
 - EFS ei lisää arvoa pilviympäristössä.

Varmuuskopiointi ja avainten hallinta

- **Onko EFS-avainten varmuuskopiointi pakollista?**
 - Kyllä, jos EFS on käytössä. Ilman varmuuskopioita (tai Recovery Agentia) tiedot voivat kadota pysyvästi.
- **Kuinka usein?**
 - Ei päivittäin/kuukausittain, vaan **avaimen luontihetkellä ja aina sertifikaatin uusinnan yhteydessä**.
 - Jos käytössä on AD CS key archival + Recovery Agent, manuaalisia exportteja ei tarvita.
- **Manuaalinen export (.pfx):**
 - Tee varmuuskopio avaimesta ja säilytä se salasanalla suojauduttuna turvassa (esim. salattu vault).
 - Älä säilytä samaan koneeseen.

Käyttöjärjestelmät ja alustat

- **Windows on-prem:** EFS NTFS:lle, BitLocker koko levylle. Recovery Agent GPO:lla.
- **Windows + Microsoft 365:** Suosi sensitivity-labeleita, SharePoint/OneDrive-oikeuksia, DLP:tä. EFS vain erityistapauksissa.
- **macOS/iOS:** FileVault koko levylle, ei EFS-vastinetta.
- **Linux:** LUKS, gpg, eCryptfs.
- **Pilvi (AWS/Google/Microsoft):** Käytä KMS/CMK, IAM-oikeuksia, DLP/RMS. EFS ei ole relevantti.

Käytännön poliitikat

- **Tietoluokittelu:**
 - Arkalouonteiset tiedot pilveen hallittuihin sijainteihin (SharePoint/Teams/Drive).
 - Paikallisesti vain jos pakko → BitLocker + EFS + Recovery Agent.
- **Avainten hallinta:**
 - Recovery Agent pakollinen GPO:lla.
 - AD CS key archival jos PKI käytössä.
 - Jos ei PKI:tä → manuaalinen export ja säilytys turvassa.
- **Jakaminen:**
 - Älä käytä EFS:ää jaetuissa kansioissa. Käytä NTFS-oikeuksia tai pilvialustan ACL:ia.
 - Jos halutaan salaus yli käyttäjien → käytä Rights Management (MIP/RMS).
- **Offboarding:**
 - Tarkista että avaimet ovat tallessa (DRA tai key archival).
 - Siirrä tiedot hallittuihin sijainteihin ennen tilin sulkemista.
- **Testaus:**
 - Tee säännöllinen palautustesti (esim. neljännesvuosittain) DRA:lla tai key archivalilla.
- **Käyttäjille (ei-tekniset):**
 - Yksinkertainen sääntö: pidä arkalouonteiset tiedot yrityksen pilvessä, älä omalla työpöydällä.

Todennäköisyys ja tarve

- **EFS:n käyttö:** Harvinainen pilvi-ensimmäisissä organisaatioissa. Tarpeellinen vain jos NTFS-dataa pitää suojaata käyttäjäkohtaisesti.
- **Vaihtoehdot:** BitLocker + pilvialustan hallinta ovat lähes aina riittäviä.

Suositus

- **Yritykselle:**
 - BitLocker kaikille laitteille.
 - Pilvessä: sensitivity-labelit, ACL:t, DLP.
 - EFS vain erityistapauksissa, ja **vain jos Recovery Agent on määritetty**.
 - Dokumentoitu prosessi: avainten varmuuskopiointi, offboarding, palautustestit.

Voiko administrator purkaa EFS-avaimen?

- **Normaali administrator (local/domain admin)** ei voi purkaa tai "murtaa" käyttäjän EFS-avainta.
- Avaimet ovat sidottu käyttäjän henkilökohtaiseen sertifikaattiin ja private keyhin.
- Salaus perustuu vahvaan kryptografiaan, eikä admin voi ohittaa sitä pelkillä NTFS-oikeuksilla tai hallintaoikeuksilla.
- **Poikkeus: Recovery Agent (DRA)**
 - Jos organisaatiossa on määritetty *Data Recovery Agent Group Policy*llä, tiedosto salataan sekä käyttäjän avaimella että recovery agentin avaimella.
 - Tällöin administrator, jolla on recovery agentin private key, voi avata tiedoston.
 - Tämä on ainoa hallittu tapa, jolla admin voi päästää käsiksi EFS-salattuihin tiedostoihin ilman käyttäjän omaa avainta.

- **Key Archival AD CS:ssä**

- Jos käytössä on Active Directory Certificate Services (AD CS) ja key archival, käyttäjän EFS-avaimet voidaan arkistoida PKI:hin.
 - Administrator voi palauttaa avaimen arkistosta, mutta tämä vaatii hallitun prosessin ja oikeudet PKI-järjestelmään.

Yhteenveto

- **Ilman Recovery Agentia tai key archivalia:** administrator ei voi purkaa EFS-avainta eikä avata tiedostoja.

- **Jos Recovery Agent on käytössä:** administrator voi avata tiedoston omalla agentin avaimellaan.

- **Jos key archival on käytössä:** administrator voi palauttaa käyttäjän avaimen PKI:stä ja avata tiedoston.

#####

Tosi työelämän tilanteessa

EFS:n merkitys käytännössä

- **Ei akuuttinen tai välttämätön:** Useimmissa yrityksissä EFS ei ole ensisijainen suojausratkaisu, koska BitLocker ja pilvipalveluiden käyttöoikeusmallit (ACL, DLP, sensitivity labels) kattavat jo suurimman osan tarpeista.
- **Hyvä tietää:** EFS on kuitenkin tärkeä ymmärtää, koska se suojaa tiedoston sisällön käyttäjäkohtaisesti – jopa järjestelmänvalvoja ei pääse siihen käsiksi ilman avainta.
- **Harvoin käytetty:** Moni organisaatio ei ota EFS:ää käyttöön juuri sen hallinnollisen hankaluuden takia (avainten varmuuskopiointi, Recovery Agentin määrittäminen, käyttäjän unohtamat salasanat).

Huono puoli

- Jokainen EFS-salattu tiedosto on sidottu käyttäjän omaan avaimen hallintaan.
- Jos käyttäjä unohtaa avaimen tai salasana ei ole tallessa, tiedosto on menetetty – ellei Recovery Agentia ole määritetty.
- Käytännössä tämä tarkoittaa, että **administrator joutuu kysymään User1:ltä avainta** aina, kun tiedosto pitää avata, jos Recovery Agentia ei ole olemassa.

Yhteenveto

- **EFS ei ole kriittinen** nykypäivän pilvi- ja BitLocker-maailmassa, mutta se on hyvä tuntea.
- **Käyttö on harvinaista**, ja jos sitä käytetään, se vaatii selkeän prosessin: avainten varmuuskopiointi, Recovery Agentin määrittäminen ja offboarding-käytännöt.
- Ilman näitä hallintakeinoja EFS muuttuu helposti “riskiksi” – tiedostoja voi kadota, jos käyttäjä ei ole saatavilla.

EFS on enemmän **tekninen erikoisuus ja hyvä tietää** kuin jokapäiväinen työkalu. Yrityksissä, joissa on moderni pilvi- ja BitLocker-strategia, EFS:n käyttöä kannattaa harkita vain erityistapauksissa.

Pilvipalvelu ja Windows EFS

EFS-salattu kansio ja pilvi (Windows/Microsoft)

- **EFS toimii vain NTFS-tiedostojärjestelmässä paikallisella koneella.** Kun siirrä EFS-salatun kansion pilveen (esim. OneDrive, SharePoint, Azure Files), tiedosto pysyy salattuna, mutta pilvipalvelu ei ymmärrä EFS-salausta.
- **Avattavuus:**
 - Käytännössä sinun täytyy **ladata tiedosto takaisin Windows-työasemalle**, jossa käyttäjän EFS-avain on käytettävissä.
 - Pilvipalvelun selaimessa tai mobiilisovelluksessa tiedosto ei avaudu, koska niissä ei ole EFS-avainta.
- **Ainoa keino:** kyllä, käytännössä tiedosto pitää avata Windows-koneessa, jossa on oikea käyttäjäprofiili ja private key.
- **Yrityskäytäntö:** tästä syystä EFS ei ole suosittelu pilvitetiedostojen suojausmenetelmä. Pilvessä käytetään mieluummin **Microsoft Information Protection (MIP/AIP)**, **sensitivity labels**, **DLP-politiikat** ja **BitLocker palvelinpuolella**.

Vaihtoehtoiset työkalut ja menetelmät

Jos halutaan EFS:n kaltaista per-tiedosto tai per-kansio salausta, on olemassa muita ratkaisuja:

- **Windows / Microsoft:**
 - **BitLocker:** koko levyn tai volyymin salaus, hallittavissa AD/Intune kautta.
 - **Azure Information Protection (AIP) / Microsoft Purview:** tiedostokohtainen salaus ja käyttöoikeuksien hallinta, toimii myös pilvessä.
 - **OneDrive/SharePoint sensitivity labels:** tiedostot ja kansiot voidaan suojaa automaattisesti, myös pilvessä.
- **Kolmannen osapuolen työkalut:**
 - **VeraCrypt:** avoimen lähdekoodin levysalaus, voi luoda salattuja kontteja/kansioita.
 - **AxCrypt, Boxcryptor:** tiedostokohtainen salaus, integroituu pilvipalveluihin.
 - **GPG/PGP:** tiedostojen salaus avaimilla, toimii kaikilla alustoilla.
- **macOS/iOS:**
 - **FileVault:** koko levyn salaus.
 - **Disk Utility encrypted image:** voi luoda salattuja kansioita.
- **Linux:**
 - **LUKS/dm-crypt:** levysalaus.
 - **eCryptfs/EncFS:** kansio- ja tiedostokohtainen salaus.
 - **GPG:** yksittäisten tiedostojen salaus.

Yhteenveto

- Jos siirrä EFS-salatun kansion pilveen, se pitää avata **Windows-koneessa, jossa on oikea avain** – pilvi ei tue EFS:ää.

- Pilvessä kannattaa käyttää **pilvialustan omia salaus- ja käyttöoikeustyökaluja** (MIP, sensitivity labels, DLP).

- Vaihtoehtoisia työkaluja on paljon (BitLocker, VeraCrypt, AxCrypt, GPG), ja ne voivat olla joustavampia kuin EFS, etenkin pilviympäristössä.

