

## 7.1.4. EFS - 5 Pohdinta

Wednesday, December 3, 2025 19:44

### POHDINTA OSUUS JA TESTATTUA OSUUTTA

- **EFS-salattu tiedosto pysyy sidottuna siihen NTFS-taltion kontekstiin, jossa se on salattu.** Kun yrität siirtää sen USB:lle tai verkkoasemalle, salaus ei vältämättä säily tai tiedosto ei ole avattavissa, koska EFS ei toimi FAT/ExFAT-levyillä eikä SMB-jaoissa samalla tavalla.
- **Recovery Agent (Administrator)** voi avata tiedoston vain, jos se on edelleen NTFS-taltiolla ja tiedoston salaukseen on liitetty RA:n sertifikaatti. Siirto toiseen ympäristöön ilman NTFS-tukea katkaisee tämän.
- **Administrator ei tarvitse käyttäjän salasanaa eikä käyttäjän sertifikaattia** – RA:n oma private key riittää, jos tiedosto on salattu niin, että RA on mukana.
- Jos tiedosto on salattu vain käyttäjän omalla avaimella eikä RA ole mukana, silloin se jää käytännössä "lukituksi" käyttäjän taakse. Silloin ainoa tapa avata on, että käyttäjä itse purkaa sen tai antaa oman avaimensa.
- Recovery Agent toimii vain NTFS-taltiolla, ei siirrettynä USB:lle tai verkkoasemalle. Administrator voi avata tiedoston vain, jos RA-sertifikaatti on liitetty salaukseen.

### EFS-harjoittelun periaatteet seuraavaa kertaa varten

- **Laajuus:** EFS salaa tiedostot NTFS-tiedostojärjestelmän tasolla käyttäjän sertifikaatilla. Se ei ole tarkoitettu FAT/exFAT-levylle, moniin SMB-kopiointiskenarioihin tai "siirrettäväin kassakaappeihin".
- **Avaimet ja käyttö:** **Käyttäjän avain** purkaa salauksen läpinäkyvästi käyttäjälle; **Recovery Agentin (RA)** avain purkaa, jos RA oli mukana salauksen aikana. Ilman RA:ta ylläpitäjät eivät voi palauttaa.
- **Siirrettävyyden rajat:** EFS-tiedostojen siirtäminen pois NTFS:stä voi poistaa tai rikkota salauksen. SMB-kopioissa tiedosto voi salautua uudelleen tai epäonnistua. EFS soveltuu parhaiten paikalliseen NTFS-taltion suojaamiseen.
- **Vastuiden eroteltu:** EFS suojaa sisältöä; **NTFS-oikeudet** hallitsevat käyttöoikeuksia; **BitLocker** suojaa koko levyn tai laitteen.

### Vaiheittainen suunnitelma selkeään, toistettavaan labraan

1. **Perusasetukset GPO:ssa ja RA:ssa**
  - **Määritä RA:** Konfiguroi EFS Recovery Agents GPO:ssa ennen kuin käyttäjät salaavat mitään.
  - **Varmista RA:n läsnäolo:** Testitiedostossa tarkista Details → Recovery Agents ja varmista, että RA-sertifikaatin thumbprint vastaa MMC:ssä näkyvää.
2. **Käyttäjän salausprosessi**
  - **Luo testitiedostot NTFS:ään:** Käytä paikallista kansioita (esim. C:\EFS-Lab).
  - **Salaa:** Properties → Advanced → Encrypt; varmista, että käyttäjän sertifikaatti näkyy kohdassa "Users who can access".
3. **Recovery-todistus**
  - **Simuloi avaimen menetys:** Poista käyttäjän EFS-sertifikaatti (varmuuskopioi ensin PFX:ksi), aja cipher /k.
  - **Aava RA:na:** Kirjaudu sisään Administratorilla samalle koneelle, varmista että RA-sertifikaatilla on private key, korja NTFS-oikeudet tarvittaessa, avaa tiedosto ja vahvista efsinfo /r.
4. **Dokumentointitodisteet**
  - **Kaappaan todisteet:** Kuvakaappaukset Details-dialogista, MMC-sertifikaateista ja komentoista (efsinfo /c, efsinfo /r).
  - **Kirjaamalla thumbprintit ja GPO-linkit:** Merkitse RA-thumbprint, GPO-nimi/OU-scope ja testin ajankohta.

### Siirrettävyyys ja "kassakaappi"-vaihtoehdot verrattuna EFS:ään

- **BitLocker (suositeltu siirrettävyteen):**
  - **Käyttötapaus:** Koko levyn tai taltion salaus, joka kulkee laitteen mukana (USB, ulkoiset levyt).
  - **Hyöty:** Data pysyy salattuna siirrettäessä; yksinkertaisempi kuin EFS "kassakaappi"-skenaarioihin.
- **Salatut kontit (ZIP/7z, VHD/VHDX):**
  - **Käyttötapaus:** Luo NTFS-muotoinen VHD/VHDX, liitä se ja salaa BitLockerilla; säilytä tiedostot sisällä.
  - **Hyöty:** Siirrettävä "safe", joka säilyttää NTFS:n ja salauksen.
- **Pilvi (SharePoint/OneDrive) yrityskontrolleilla:**
  - **Käyttötapaus:** Keskitetty tallennus DLP:llä, auditoinnilla ja Sensitivity Labelseilla (Purview/AIP).
  - **Hyöty:** Poliittikopohjainen suojaus ja tietosuoja, parempi yhteistyöön kuin EFS.
- **SMB-jaot (Windows-palvelimella):**
  - **Käyttötapaus:** Keskitetty NTFS + palvelinpuolen suojaus.
  - **Hyöty:** EFS SMB:n yli on epävarmaa; käytä mieluummin palvelinpuolen salausta, NTFS-ACL:ia ja BitLockeria.

### Loppukäyttäjän ohjeet (selkeästi)

- **Salaa vain paikallisella NTFS:llä:** Älä odota, että EFS "seuraa" tiedostoa USB:lle tai verkkoasemalle.
- **Jos siirrät dataa, käytä BitLockeria:** Salaa USB-levy tai NTFS-VHD "kassakaappi" ja kopioi tiedostot sinne.
- **Varmuuskopioi EFS-avaimesi:** Exportoi PFX ja säilytä turvallisesti (salasanalla suojaattuna, adminin hallinnassa).
- **Älä jaa avaintasi:** PFX ei kuulu muille; palautus on RA:n tehtävä, ei käyttäjän avaimen jakaminen.

### Ylläpitäjän politiikka ja infrastruktuurin tarkistuslista

- **Esikonfiguroi RA GPO:ssa:** Varmista RA ennen kuin käyttäjät salaavat.
- **Avainten elinkaari:**
  - **Varmuuskopiot:** Automatisoi EFS-avainten exportointi turvalliseen säilytykseen.
  - **Offboarding:** Varmista RA-peitto ja kerää käyttäjän PFX vain virallisen prosessin kautta.

- **Suosi BitLockeria siirrettävissä medioissa:** Mandatoi BitLocker USB:lle ja työasemien levyille.
- **Palvelinpuolen kontrollit:** NTFS-ACL:t, auditointi ja BitLocker palvelinlevyllä; vältä EFS:ää SMB-jaoissa.
- **Pilvihallinta:** Käytä Sensitivity Labelseja, DLP:ää ja auditointia SharePointissa/OneDrivessa.
- **Dokumentointi:** Pidä runbook RA-thumbprintestä, sertifikaattivarastoista ja palautusprosesseista; testaa säännöllisesti.

## ISO 27001/27000 -näkökulma

- **Pääsynhallinta ja vähimmän oikeuden periaate:** Selkeät roolit käyttäjille vs. RA-yläpitäjille; auditoi palautukset.
- **Kryptografiapolitiikka:** Dokumentoi milloin käytetään EFS:ää, BitLockeria tai pilvisalausta; sisällytä avainten hallinta ja varmuuskopiot.
- **Tietojen luokittelu:** Merkitse tiedot (julkinen, sisäinen, luottamuksellinen) ja sovella vastaavat tekniset kontrollit.
- **Toipumissuunnitelmat:** Testatut EFS-palautusprosesseit ja vaihtoehdot, jos RA ei ollut käytössä; logaa ja tarkista palautukset.
- **Pilvi ja toimittajat:** Varmista, että SharePoint/OneDrive täyttää salaus-, DLP- ja tietosuoja-vaatimukset.

### Miksi ZIP ei toimi EFS:n kanssa

- Kun pakkaat EFS-salatun kansion tai tiedoston ZIP-arkistoon (tai 7z, RAR jne.), pakkausohjelma lukee tiedoston **selväkielisenä** ja kirjoittaa sen arkistoon ilman EFS-salausta.
- Lopputulos: ZIP-tiedosto ei ole enää EFS-suojattu, vaan sen sisältö on tavallinen tiedosto arkiston sisällä.
- Jos haluat suojaata ZIP-tiedoston, sinun täytyy käyttää **ZIP-ohjelman omaa salausominaisuutta** (esim. AES-256-salattu ZIP), mutta se ei liity EFS:ään.

### Testisi vahvistaa tämän

- Kun loit salatun kansion ja sisäisen .txt-tiedoston, EFS toimi paikallisesti NTFS:llä.
- Kun yritit siirtää tai pakata sen ZIP:iin, salaus ei enää seurannut mukana → tämä on odotettu käytös.

### Muistiinpanona

- **EFS toimii vain NTFS-taltioilla.**
- **Siirto USB:lle, verkkoasemalle tai ZIP-pakettiin ei säilytä EFS-salausta.**
- Jos haluat "kassakaappi"-tyypisen siirrettävän ratkaisun, käytä **BitLockeria** (koko levy tai VHD) tai **ZIP/7z-salausia**, mutta ne ovat eri teknologiaa kuin EFS.

- EFS-salaus ei säily siirrettäessä tiedostoja ZIP-arkistoon, verkkoasemalle tai FAT/USB-tikulle – vain NTFS-taltiolla EFS toimii.

## Käyttäjä ja Administrator näkökulmat (tekoäly ohje):

### Mitä EFS tekee ja mitä se ei tee

- **EFS** salaa tiedostot **NTFS-taltioilla käyttäjän sertifikaatilla**. Salaus on sidottu käyttäjän profiiliin ja private keyhin.
- **Ei toimi** **FAT/exFAT-levyllä, ZIP-paketeissa tai useimmissa SMB-jaoissa**. Jos siirräät tiedoston pois NTFS:stä, salaus ei säily.
- **Ei suojaa** tiedoston nimeä, metatietoja tai **NTFS-oikeuksia**. Se suojaa vain tiedoston sisällön.
- **Ei korvaa** **BitLockeria**. BitLocker suojaa koko levyn, EFS vain yksittäisiä tiedostoja/kansioita.

### Mitä sallitaan ja mitä ei

- **Sallittua:** Käyttäjä voi salata omia tiedostojaan NTFS-taltiolla, ja Recovery Agent voi avata ne, jos RA on määritetty GPO:ssa.
- **Ei sallittua:** Käyttäjän avaimen jakaminen muille (esim. exportoitu PFX ilman valvontaa) – tämä rikkoo tietoturvaa.
- **Ei mahdollista:** Purkaa EFS-salausta ilman käyttäjän private keytä tai Recovery Agentin avainta. Kryptografia perustuu vahvaan standardiin (RSA + AES), eikä sitä voi "murtaa" käytännössä.

### Sertifikaatti avaimena

- Käyttäjän **EFS-sertifikaatti** on käytännössä ainoa keino avata tiedosto, jos Recovery Agentia ei ole mukana.
- Recovery Agentin sertifikaatti on **varmistuskeino**: jos käyttäjä unohtaa avaimensa tai lähtee organisaatiosta, RA voi avata tiedoston.
- Ilman kumpaakaan avainta tiedosto on menetetty – ei ole realistista "hakkeroida" EFS:ää.

### Voiko joku purkaa EFS:n ilman avainta?

- **Normaalisti ei.** EFS käyttää vahvaa kryptografiaa, eikä sitä voi käytännössä murtaa brute force -menetelmillä.
- **Ainoa realistinen riski:** jos käyttäjän avain (PFX) tai Recovery Agentin avain vuotaa, tai jos koneella on haittaohjelma, joka nappaa avaimen muistista.
- **Tietoturvan näkökulmasta:** suojaa avaimet, käytä vahvoja salasanoja PFX-exporteissa, ja varmista että Recovery Agent on määritetty.

### Mitä pitäisi muistaa jatkossa

- **EFS toimii vain NTFS-taltiolla.**
- **Recovery Agent on väältämätön organisaatioissa.** Ilman RA:ta tiedostot voivat jäädä ikuisesti lukkoon.
- **Käyttäjän sertifikaatti on henkilökohtainen.** Jos se katoaa eikä RA ole mukana, tiedosto on menetetty.
- **Ei ole kiertotietä.** Kryptografia on suunniteltu niin, että ilman avainta ei voi purkaa.
- **Tietoturva ja ISO 27001:** avainten hallinta, varmuuskopiot, vähimmän oikeuden periaate ja toipumissuunnitelmat ovat osa hyvää käytäntöä.

- **EFS:n purkaminen onnistuu vain käyttäjän omalla sertifikaatilla tai Recovery Agentilla. Muut keinot eivät ole realistisia.** Tämä on se ydinasia, joka loppukäyttäjän ja ylläpitäjän pitää ymmärtää.

## Efin käyttö tuotannossa ja organisaatioissa

- **Yleinen asema:** EFS on edelleen Windowsin ominaisuus, mutta sen käyttö tuotannossa on tyypillisesti rajattua. Moni organisaatio suosii BitLockeria (levy/taltio), DLP:ää ja pilvi-salausta (Purview/AIP) sekä NTFS-oikeuksia ja keskitettyä hallintaa jaettuihin tietoihin.
- **Missä EFS:ää käytetään:** Paikallisen, käyttäjäkohtaisen datan suojaus työasemalla tai tietyissä palvelinskenaarioissa, joissa tiedosto ei liiku

NTFS-taltion ulkopuolelle ja RA on määritetty GPO:lla.

- **Missä EFS ei ole suosittu:** Siirrettävä “kassakaappiskenaariot” (USB, exFAT/FAT, ZIP, SMB-jaot), jaettu yhteistyööskentely, organisaatioiden, joissa halutaan yhtenäinen, siirrettävä salaus ja keskitetty valvonta.

## Lyhyt vertailu: efs vs vaihtoehdot

Ratkaisu	Käyttötarkoitus	Siirrettävyys	Hallinta ja valvonta	Tyypillinen käyttö
EFS	Tiedosto/kansio NTFS:llä, käyttäjäkohtainen	Heikko (ei FAT/exFAT/ZIP/SMB varmuudella)	RA/GPO, rajattu	Paikallinen data-at-rest
BitLocker	Koko levy/taltio	Vahva (USB, VHD, laitteet)	Keskitetty, policyt	Endpointit, USB, palvelimet
Purview/AIP (Sensitivity Labels)	Tiedostokohtainen suoja ja poliittika	Vahva (kulkee tiedoston mukana)	DLP, auditointi, identiteetit	Pilvi ja M365-yhteistyö
NTFS ACL + Server-side	Pääsynhallinta ja lokitus	Riippuu tallennusratkaisusta	Hyvä (keskitetty)	Jaetut kansiot, palvelinvolymit

## Tietoturva, kyberturvallisuus ja eettinen hakkerointi

- **Hyökkäyspinta:** EFS:n “murtaminen” ilman avaimia ei ole realistista; käytännön hyökkäykset kohdistuvat avaimen hankintaan (PFX-vuoto, heikko salasana), DPAPI-suojaan käyttäjäkoneella, tai muistista/endpointilta kaappaamiseen, kun käyttäjä on kirjautunut.
- **Eettinen hakkerointi:** Testaa avainten suojausta, varmuuskopiointia/escrow’ta, RA-prosessia, pääsynhallinta, lokitusta, ja endpoint-kovennusta. Itse EFS-krypton kiertäminen ei ole testin fokus; fokus on avainten hallinnan ja prosessien heikkoudet.
- **Todennäköisyys (karkeasti):** EFS-spesifisä murtotilanteita on harvoin; suurin riski on avainvuoto tai endpoint-kompromissi. Organisaatioissa, jotka eivät käytä RA:ta tai avainhallintaa, lukittujen tiedostojen riski on silti käytännössä korkea.

## Mitä saa ja ei saa tehdä

- **Saa/kuuluu:**
  - Käyttää EFS:ää vain NTFS-taltiolla, RA määritettynä GPO:ssa.
  - Varmuuskopioida käyttäjän EFS-avaimet turvallisesti (salattu PFX, escrow).
  - Dokumentoida RA-thumbprintit, OU-scope, ja testata palautus säännöllisesti.
- **Ei saa/ei kannata:**
  - Luottaa EFS:ään siirrettävässä mediassa (USB/FAT/exFAT), ZIP:ssä tai SMB-jaossa odottaen salauksen säilyvän.
  - Jakaa käyttäjän PFX:ää muille tai säälyttää sitä heikolla salasanalla.
  - Unohtaa RA-konfigurointi ennen kuin käyttäjät aloittavat salauksen.

## ISO 27001 -konteksti (ytimekkäästi)

- **Cryptographic controls:** Määrittele selkeästi, milloin käytetään EFS:ää, BitLockeria ja AIP:ää; hallitse avainten elinkaari, varmuuskopiot, escrow ja auditointi.
- **Access control:** Vähimmän oikeuden periaate, RA-roolien rajaus, palautustapahtumien lokitus ja hyväksyntä.
- **Asset & classification:** Luokittele data ja kohdenna tekniset kontrollit (BitLocker endpointille, AIP tiedostolle, NTFS ACL ja palvelinpuolen suoja jaettuihin).
- **Business continuity:** Testatut EFS-palautusprosessit; fallback-ratkaisut (BitLocker/AIP) siirrettävyteen.

## Käytännön johtopäätös

- EFS on hyödyllinen paikallisessa, käyttäjäkohtaisessa suojaussa NTFS:llä, mutta ei siirrettävyteen.
- Organisaatioissa perusratkaisu on: BitLocker endpointille ja siirrettäville medioille, NTFS ACL + palvelinpuolen suoja ja lokitus jaetuissa, sekä AIP/Purview tiedoston mukana kulkevaan suojaan ja yhteistyöhön.
- EFS:ää käytetään, kun se sopii tarpeeseen ja RA/GPO/avainten hallinta on kunnossa; muuten se korvataan yllä mainituilla vaihtoehdolla.

## Windows ja Apple:

EFS (Encrypting File System) on saatavilla **vain Windows Pro-, Enterprise- ja Education-versioissa** (sekä Windows 10 että 11). **Windows Home** -versiossa EFS ei ole käytettävissä. MacOS:lla (Apple) ei ole EFS:ää lainkaan – siellä käytetään muita salausratkaisuja, kuten **FileVault** koko levyn salaukseen.

### Windows 10 ja 11 -versiot

- **Windows Home:** Ei sisällä EFS:ää. Käyttäjät voivat käyttää BitLockeria vain, jos laitevalmistaja on sen esiasentanut, mutta EFS ei ole vaihtoehto.
- **Windows Pro:** Sisältää EFS-ominaisuuden. Käyttäjä voi salata yksittäisiä tiedostoja ja kansioita NTFS-taltiolla.
- **Windows Enterprise:** Sisältää EFS:n lisäksi laajennetut hallintaominaisuudet (Group Policy, Recovery Agent, avainten hallinta).
- **Windows Education / Pro Education:** Sisältää EFS:n, käytännössä samat ominaisuudet kuin Enterprise, mutta lisensointi on suunnattu oppilaitoksiin.

### macOS (Apple)

- macOS ei tue EFS:ää.
- Apple tarjoaa **FileVault**-ominaisuuden, joka salaa koko levyn (Full Disk Encryption).
- FileVault perustuu XTS-AES-128 salaukseen ja suojaa koko käyttäjäprofiilin ja datan, mutta ei yksittäisiä tiedostoja samalla tavalla kuin EFS.
- Jos halutaan tiedostokohtainen salaus Macilla, käytetään yleensä kolmannen osapuolen ohjelmia (esim. VeraCrypt, salatut ZIP/7z-arkistot) tai macOS:n sisäisiä avainketju- ja salausratkaisuja.

## KYSYTTÄ TEKOÄLYLTÄ APUA JA HAETTU LISÄTIETOA:

- Ei ole kikkaa/tempua, josta esim. Administrator (VM1) ettei purkaisi VM2 EFS exportatun certifikaatti tiedonsa.
- Recovery agent voi vain täsmentää ja jos tarkistaa sen thumbprint avaimen koodinsa.
  - Recovery Agent voi täsmentää ja tarkentaa itsensä thumbprintin kautta, mutta vain niissä tiedostoissa, joissa RA oli mukana salaukseen.

### 100 % varma vastaus

- Ei ole olemassa mitään "kikkaa" tai takaporttia, jolla Windowsin Administrator voisi purkaa käyttäjän exportoidun PFX-tiedoston ilman sen salasanaa.
- **Ainoa keino** avata käyttäjän EFS-salattuja tiedostoja on:
  1. Käyttäjän oma sertifikaatti + private key (PFX, salasana tiedossa).
  2. **Recovery Agent (RA)**, jos se oli määritetty GPO:ssa **ennen** kuin tiedosto salattiin.

### Recovery Agentin rooli

- RA ei ole "vain assistentti" vaan virallinen varmistusmekanismi.
- Kun RA on määritetty, jokainen uusi EFS-salattu tiedosto sisältää myös RA:n julkisen avaimen.
- Tämä tarkoittaa, että RA:n private keyllä (Administratorin hallussa) tiedosto voidaan avata, vaikka käyttäjän oma avain olisi kadonnut.
- Jos RA ei ollut mukana salauksen hetkellä → tiedosto on sidottu vain käyttäjän avaimiin → ilman PFX-salasanaa tiedosto jää lukkoon.

### Ei kiertotietä

- Kryptografia on suunniteltu niin, että ilman avainta ei ole realistista purkaa salausta.
- Ei ole olemassa toimivaa "hakkerointimenetelmää" tai Windowsin sisäistä kikkaa, jolla voisi ohittaa tämän.
- Käytännössä: **jos RA ei ollut määritetty ja käyttäjä ei anna salasanaa, tiedosto on menetetty.**

## JOTAKIN OMAA TESTEJÄ & OMA MUISTIINPANONA JA OMA NÄKÖKULMA:

- **Testi VM2:lla:**
  - Salaus tehty kansioon ja sen sisällä olevaan .txt-tiedostoon.
  - Yritetty pakata (.zip) → salaus ei säilynyt. Sama pätee yksittäiseen .txt-tiedostoon.
  - Siirto C-levylle tai verkkoasemalle/tikulle ei onnistunut salauksen säilyttämisen kannalta.
- **Exportattu sertifikaatti:**
  - VM2:n käyttäjä voi exportoida oman avaimensa PFX-tiedoston salasanalla, ja ainakin se voi siirtää jakaa esim. Jaettuun levylle (S:- levy)
    - Tästä esim. Administrator (VM1) pääsee käsiksi PFX tiedoston alle, ettei voi yrittää avata salasanansa
  - Vain käyttäjä itse tietää salasanan → edes Administrator ei voi purkaa ilman Recovery Agentia.
- **Oma muistiinpanona, omalta näkökulmalta harjoituksen osalta harjoitelusta ja tekoälyltä kysytty apua:**
  - Jos käyttäjä haluaisi salata ja enkrypdata kokonaisen kansion, ettei alla on salaisia tiedostoja niin keinoja on varmasti paljon kuten encrypdata sitä kansiota joko onedrive pilvipalvelujen alle, hard disk eli mahdollinen toiselle kovalevylle/tikun alle.
  - En usko tätä kauheasti käytettää nyky maailmassa ja tulevaisuudessaan, mutta osat ehkä saattaa käyttää. Tärkeänä on ymmärtää sen EFS käytön teorian ja loogisen idean miten se toimii, ettei hahmottaa tietoturvan/kyberturvallisuuden ja ISO 27000 vaatimuksensa.
  - Ylläpitäjälle ja loppukäyttäjälle tämä on ylimääräinen lisätyö, koska suojaatun kansion sen jälkeen kukaan ei kuitenkaan muista ettei tällaista on suorittanut ja miksi, ettei mihin varten.
    - Ainoastaan jää jälki ja muistio MMC, josta järjestelmänvalvoja ja käyttäjä itsensä voi käydä käyttöliittymästä konfiguroimassa ja monitoroida sitä järjestelmänsä tarvittaessa.
- **Koskien recovery agenttia - periaatteessa tämä on vain administrator työkalu, josta voi tarkistaa mmc työkalun alta ja löytyykö certifikaattien tietoja just ID:n perusteella (thumbprint)**
  - **MMC Certificates** = Microsoft Management Consolesen *Certificates-snap-in*
  - Kun käyttäjä encrypttaa kansion EFS:llä, Windows liittää tiedoston metatietoihin sekä käyttäjän oman avaimen ettei **recovery agentin avaimen**. **Administrator** ei saa tätä tietoa käyttäjältä, vaan se täsmentyy automaattisesti thumbprintin muodossa. Näin hallinto voi avata tiedoston riippumatta käyttäjän läsnäolosta.
  - Encryptattun kansion ja exportatun EFS sertifikaatti, josta vain se käyttäjä itse tietää sen salasansa.
  - Periaatteessa tämän metodi salausmenetelmä toimii kuin käyttäjän kassakaappina itsensä, ettei vain hänen olemassa oleva avain ja koodin kautta voi purkkaa sen EFS sertifikaattin salasansa ja päästääkseen encrypttatuun kansion. Jos muita käyttäjät ja kuten administrator tai joku henkilökunta haluaa avatessaan sen kansion ja sertifikaattin salasansa - niin se on mahdotonta eli