D-sarja:
Muut julkaisut
[3/2014]

Salassa pidettävän tiedon välittäminen sähköpostitse pelastustoimessa suojaustasolla IV

Marko Hassinen

Ohjeistus pelastustoimessa muodostuneen tai ulkopuolelta tulleen salassa pidettävän materiaalin välittämiseen sähköpostitse.

Pelastusopiston julkaisu

D-Sarja: Muut julkaisut

3/2014

ISBN: 978-952-5905-46-5 (pdf)

ISSN: 1795-9187

PELASTUSOPISTO

Salassa pidettävän tiedon välittäminen sähköpostitse pelastustoimessa suojaustasolla IV

Hassinen Marko, FT, Pelastusopisto

Toimintaohje 47 s.

Elokuu 2014

TIIVISTELMÄ

Pelastustoimessa syntyy salassa pidettävää materiaalia, jonka käsittelyä säätelevät useat lait ja ohjeistukset. Toimialan sisällä syntyvä salassa pidettävä materiaali on kuitenkin määrällisesti vähäistä verrattuna muilta toimialoilta ja viranomaisilta pelastustoimelle luovutettavaan salassa pidettävään materiaaliin. Koska suurin osa tästä materiaalista on sähköisessä muodossa ja sähköposti on luonteva tapa välittää tällaista materiaalia, tarvitaan ohjeistus tällaisen materiaalin turvalliseen välittämiseen sähköpostitse. Tässä ohjeistuksessa yksityiskohtaisesti ohjeistetaan miten salassa pidettävä materiaali voidaan turvallisesti lähettää sähköpostilla ja miten vastaanotettua materiaalia tulee käsitellä.

Ohjeessa otetaan huomioon niin toimikorttia käyttävät tahot kuin sellaiset joilla soveltuvaa toimikorttia ei ole käytettävissään. Tämä ohjeistus painottuu enemmän toimintaan ilman toimikorttia, koska ohjeistuksen kirjoitushetkellä toimikortin yleisyys pelastustoimialalla on verraten pieni. Tiedon välittämiseen ilman toimikorttia käytetään tässä ohjeistuksessa TrueCrypt nimistä ohjelmistoa. Ohjeistus perustuu suurelta osin Kyberturvallisuuskeskuksen NCSA -toiminnon antamaan ohjeistukseen sekä voimassa oleviin lakeihin, VAHTI -suosituksiin ja KATAKRI (Kansallinen Turvallisuusauditointikriteeristö) vaatimuksiin.

Tämä ohjeistus on osa kokonaisuutta, johon kuluu tämän ohjeen lisäksi Ylläpidon ohje, jossa kerrotaan miten tietojenkäsittely-ympäristö tulee rakentaa jotta se täyttää True Crypt sovelluksen käytölle asetetut vaatimukset. Ylläpidon ohjeessa on ohjelmiston asentamiseen ja kieliversioihin liittyvät ohjeet.

Käsillä oleva ohjeistus on osa Pelastusopiston TUPO -hankkeen (Pelastustoimen operatiivisten tietojärjestelmien tietoturvapolitiikka) tuloksia. Hankkeen on pääsääntöisesti rahoittanut Palosuojelurahasto. Kiitokset kuuluvat myös Pelastustoimen tietoteknisiä hankkeita koordinoivalle työryhmälle ohjeen kommentoinnista ja erityisesti Jukka Kangasvierelle avusta toimikorttiosion toiminnallisuuksien testaamisessa.

SISÄLLYSLUETTELO

1. JOHDANTO

Salassa pidettävä tieto tulee sähköpostitse kommunikoituna salata luotettavasti (luottamuksellisuus). Julkisen avaimen salausmenetelmiin perustuvalla toimikorttijärjestelyllä tällainen luottamuksellisuus voidaan tuottaa. Toimikortin käyttö vaatii infrastruktuurin, jossa vastaanottajalla on toimikortti ja lähettäjällä pääsy varmennejärjestelmään, jossa vastaanottajan toimikorttiin liittyvä varmennen on saatavilla.

Luottamuksellisuus voidaan toteuttaa myös salaisen avaimen menettelyllä, jossa lähettäjä ja vastaanottaja tuntevat jaetun salaisuuden (salasana). Olennaista luonnollisesti on, että tämä salaisuus ei ole asiaan kuulumattomien tahojen hallinnassa. Salaisen avaimen menettelyssä luottamuksellisuus perustuu jaetun salaisuuden salassa pysymiseen, mikä asettaa vaatimuksia salaisuuden (salasanan) jakeluun ja arvaamisen vaikeuteen. Toisin sanoen salaisuus tulee pystyä jakelemaan asiaan kuuluville tahoille luotettavasti ja salaisuuden tulee olla siinä määrin monimutkainen, ettei sitä pysty päättelemään tai arvaamaan (kokeilemaan kaikkia vaihtoehtoja).

Salassa pidettävän tiedon suojaamiseen sähköisessä ympäristössä liittyvät tavanomaiset tietoturvan perusominaisuudet, eli luottamuksellisuus, eheys ja kiistämättömyys.

Luottamuksellisuudella tarkoitetaan sitä, että viestin sisältö on tulkittavissa vain oikeutettujen tahojen toimesta. Sähköpostissa tämä tarkoittaa karkeasti ottaen sitä, että viestin sisällön tarkoituksen voi saada selville vain tarkoitettu vastaanottaja. Mahdollisesti matkan varrella viestin haltuunsa saava oikeudeton taho ei pysty tulkitsemaan viestin sisältöä.

Eheys tarkoittaa viestin muuttumattomuutta. Eheys pystytään tuottamaan erilaisilla tarkastussummilla (ns. hajautusfunktioilla). Sähköinen allekirjoitus toteuttaa eheyden vaatimuksen ja eheys voidaan toteuttaa myös jaetun salaisuuden (salasana) järjestelmissä. Eheysmekanismit käytännössä valvovat viestin muuttumattomuutta ja osaavat ilmoittaa että viesti ei ole alkuperäisessä muodossaan, mutta eivät pysty takaamaan viestin muuttumattomuutta. Viestin tahallista muuttamista, ns. "peukalointia" ei siis voida estää, mutta se voidaan havaita.

Kiistämättömyydellä tarkoitetaan sitoutumista jota ei voi jälkeenpäin kiistää. Perinteisesti sopimuksissa on tämä ominaisuus tuotettu omakätisellä allekirjoituksella. Vastaavasti se voidaan tuottaa julkisen avaimen menetelmillä (yleensä toimikortilla) tuotetulla digitaalisella allekirjoituksella. Kiistämättömyyttä ei voida toteuttaa jaettuun salaisuuteen perustuvissa menetelmissä. Sähköisen allekirjoituksen ja salauksen avulla saadaan toteutettua kaikki mainitut kolme tietoturvan perusominaisuutta.

Tässä ohjeessa pyritään antamaan olennainen tieto päivittäisen sähköpostiliikenteen hoitamiseen salassa pidettävän tiedon osalta. Tahot, jotka voivat käyttää Väestörekisterikeskuksen myöntämää varmenteellista toimikorttia, löytävät soveltuvat ohjeet kappaleesta 2 "Sähköposti toimikorttia käyttäen".

2. SÄHKÖPOSTI SALATTUA SÄILIÖTÄ KÄYTTÄEN

Tahot, jotka eivät voi käyttää toimikorttia salassa pidettävän tiedon välittämiseen, voivat käyttää Viestintäviraston hyväksymää TrueCrypt ohjelmaa (versiot 7.0, 7.1 ja 7.1a). Tässä oletetaan, että TrueCrypt ohjelma on asennettu käyttäjän työasemaan. Asennusohje löytyy erillisestä ohjeesta "Salassa pidettävän tiedon välittäminen sähköpostitse pelastustoimessa suojaustasolla IV, Ylläpidon ohjeistus", joka on saatavilla Pelastusopiston julkaisusarjasta. Myös MAC käyttöohje on olemassa ja saatavilla Pelastusopistolta.

Ensimmäinen kappale kuvaa sähköpostilla vastaanotetun säiliön tiedostojen avaamisen ja salassa pidettävän tiedon lähettämisen olemassa olevaa säiliötä käyttäen, sekä ohjeet salassa pidettävän tiedon sisältävän säiliön luomiseen. Kappaleet 2.3. ja 2.4 pitävät sisällään ohjeistuksen englanninkielisen version käytöstä (vastaanottaminen ja lähettäminen). Lyhyt johdanto tiedon salassa pidettävyyden arviointiin ja suojaustasoihin on kappaleessa 4.

2.1. Vastaanottaminen (suomenkielinen versio)

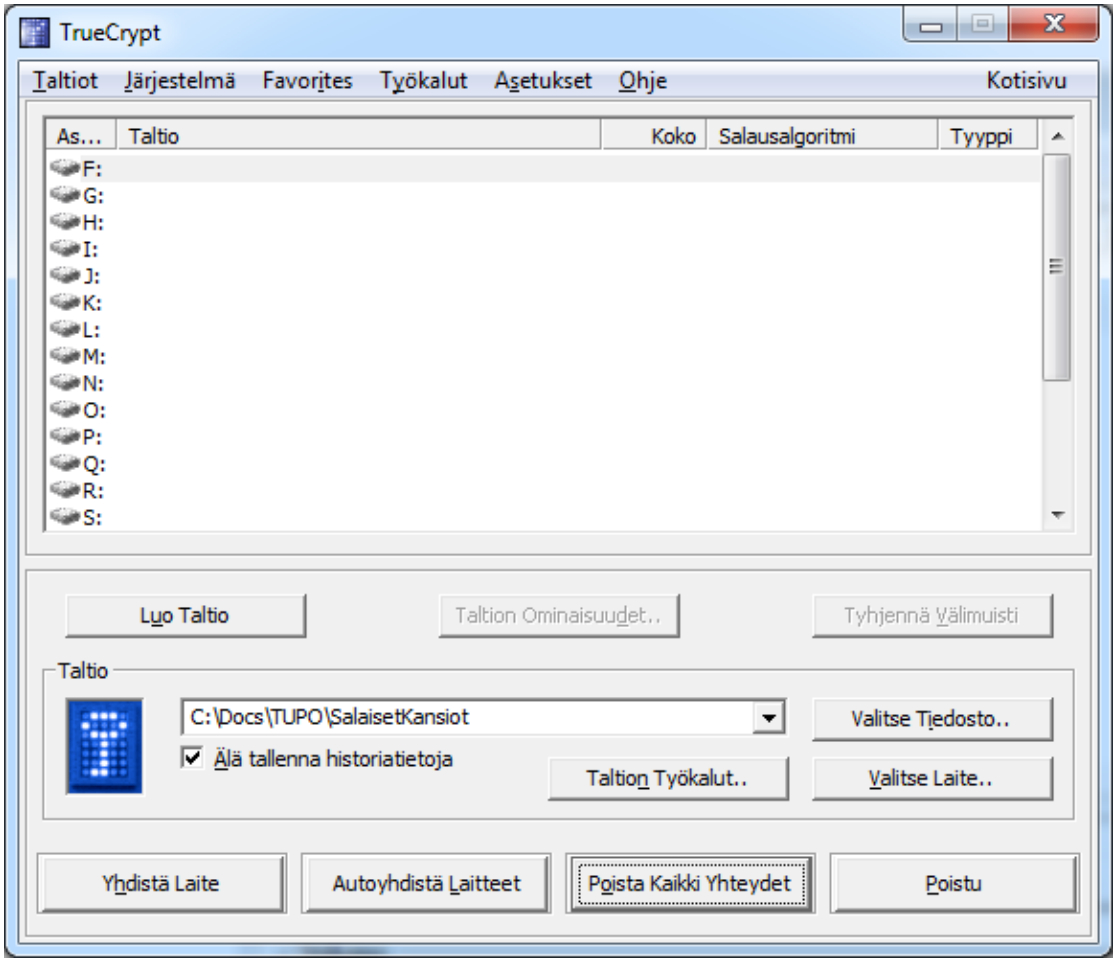
Salassa pidettävä tieto välitetään sähköpostin liitteenä TrueCrypt säiliönä. Tietoturvavaatimuksista (tarkemmat perustelut Ylläpidon ohjeessa) johtuen sähköpostin liitteenä vastaanotettu säiliö tulee poistaa sähköpostipalvelimen viestistä sen jälkeen kun se on tallennettu työasemaan. Säiliötä ei saa jättää palvelimen levylle.

1) Vastaanotettu liite (salattu säiliö) tallennetaan tiedostoksi levylle. Esimerkissä se on tallennettu nimellä C:\Docs\TUPO\SalaisetKansiot. Huomaa, ettei säiliöllä yleensä ole tiedostopäätettä.

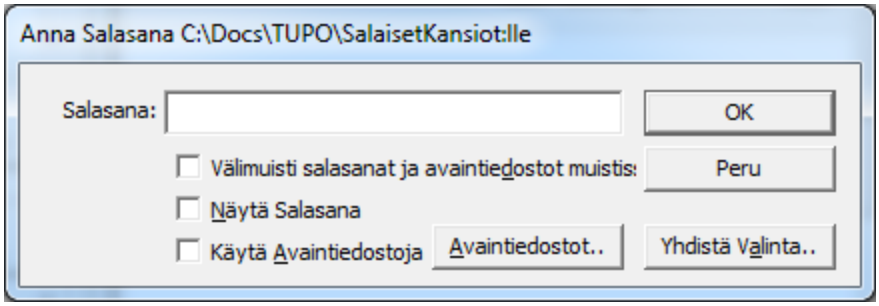
2) Tiedosto otetaan käyttöön TrueCrypt ohjelmalla seuraavasti:

a) Valitse haluamasi kirjain levyn tunnukseksi ohjelman listalta (esimerkissä valittu F:) Säiliö tulee näkymään koneessasi erillisenä levynä (kuten mm. muistitikut) kyseisellä tunnuksella.

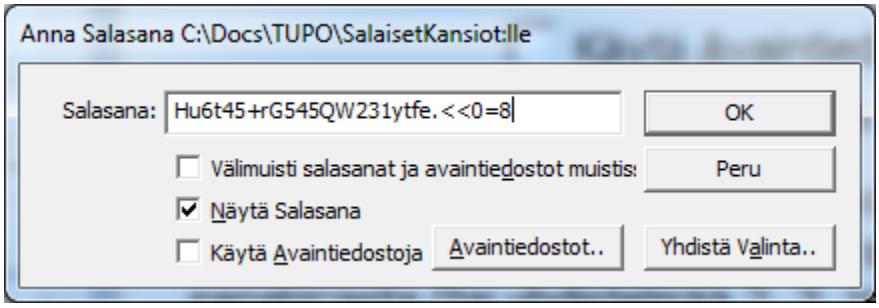
b) Valitse tiedosto Valitse Tiedosto -painikkeella. Tässä esimerkissä tiedosto on C:\Docs\TUPO\SalaisetKansiot.



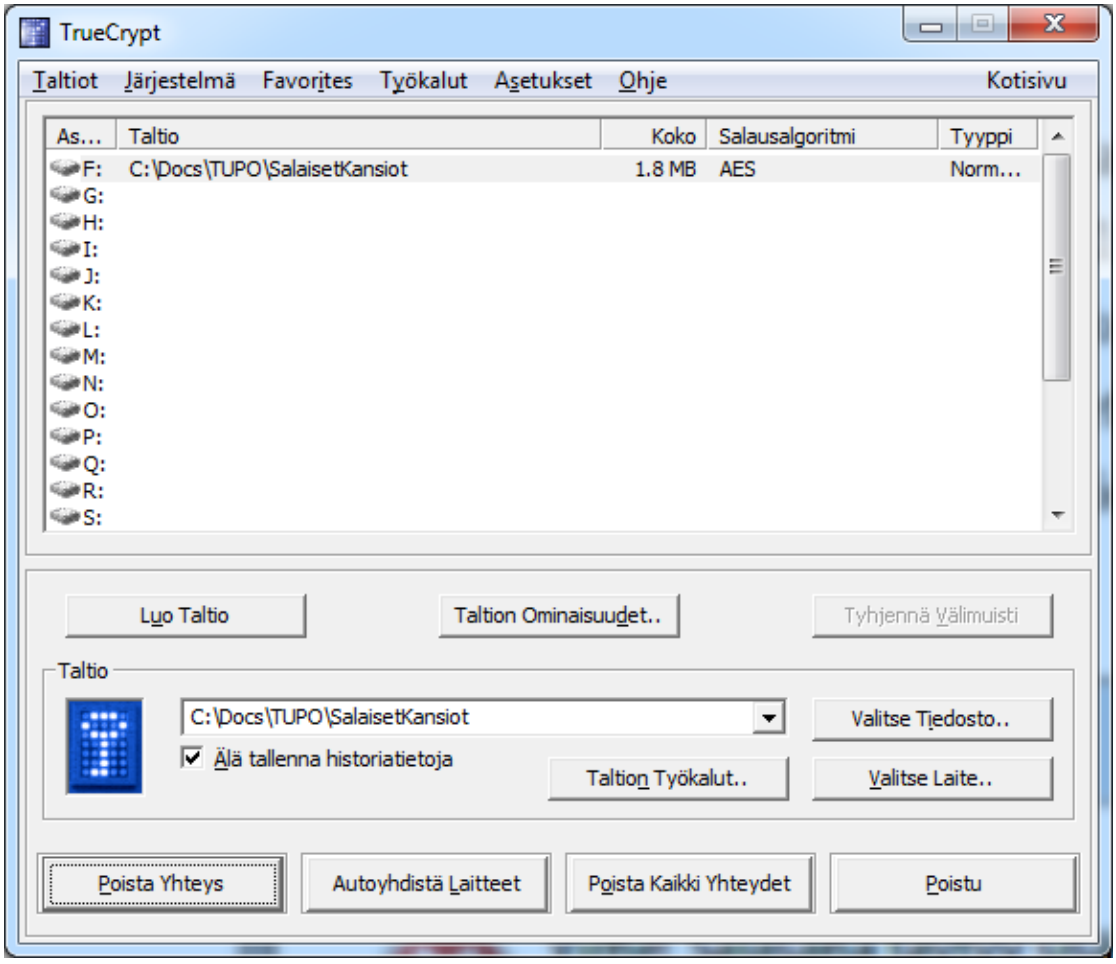
c) Paina Yhdistä Laite painiketta, jolloin ohjelma kysyy salasanaa.



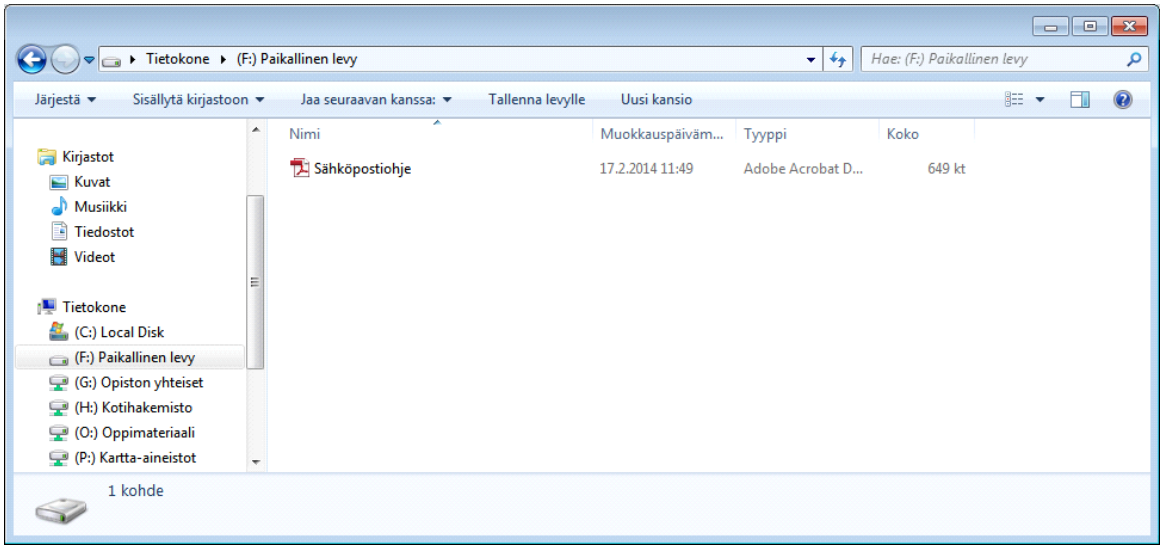
d) Syötettyäsi salasanan, paina OK painiketta. Saat kirjoittamasi salasanan tarvittaessa näkyviin Näytä Salasana valinnalla. Salasanan olet saanut tiedoston lähettäjältä, toivottavasti jollain muulla tavalla kuin sähköpostilla.



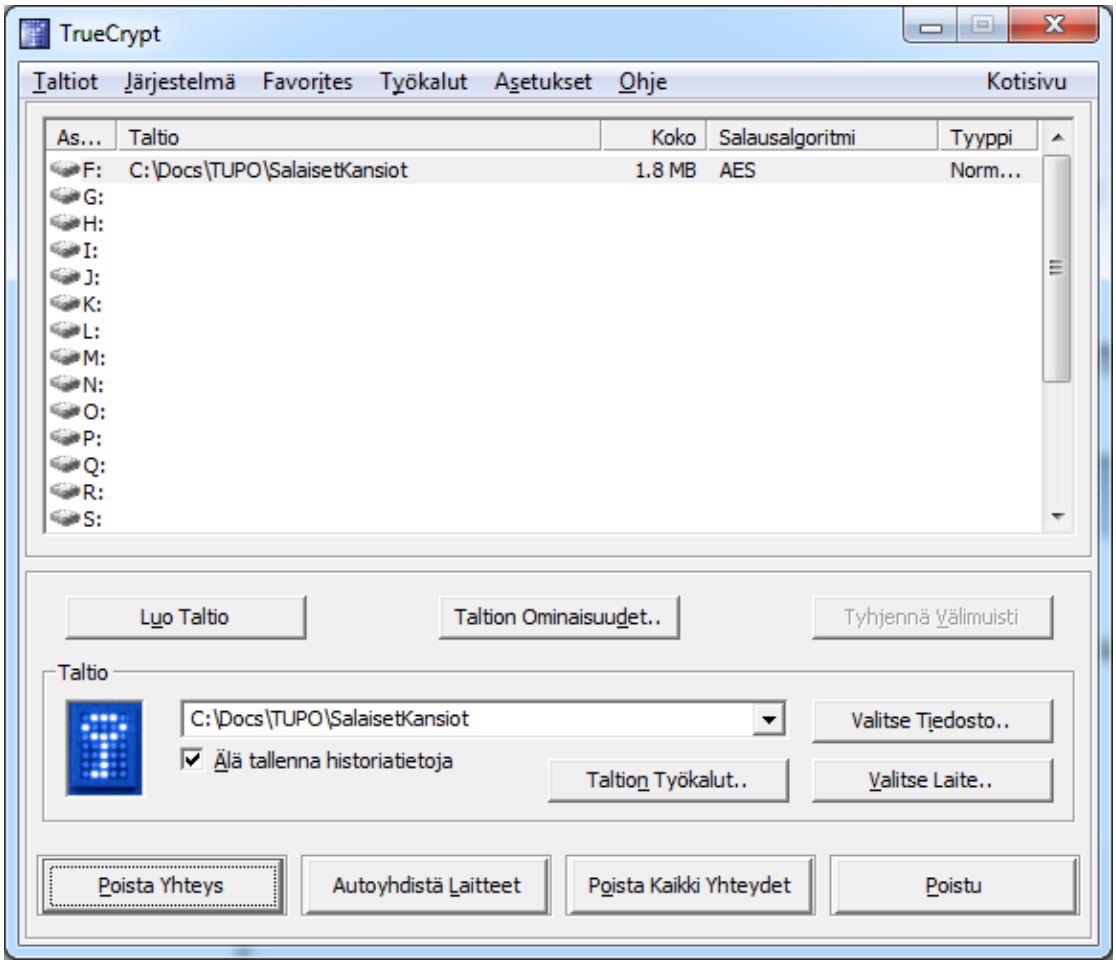
e) Onnistuneen "mounttamisen" jälkeen säiliö näkyy listalla. Säiliöstä kerrotaan tiedosto jossa se sijaitsee, säiliön koko ja käytetty salausalgoritmi (tässä AES, Advanced Encryption Standard).



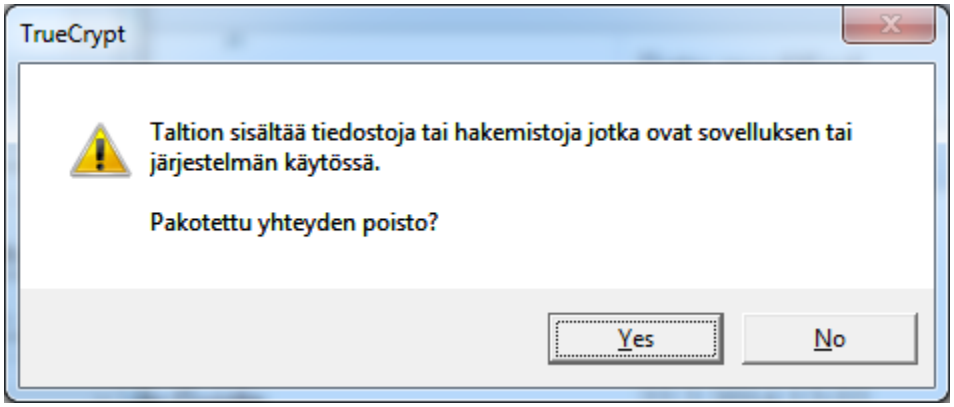
Säiliön tiedot ovat nyt käytettävissä normaalin levyn/ulkoisen muistin tavoin. Voit avata tiedostoja, muokata ja tallentaa tavanomaiseen tapaan.



f) Lopuksi säiliön käyttöönotto (mounttaus) on syytä purkaa, etenkin jos olet muokannut säiliön sisältöä. Tämä tapahtuu valitsemalla kyseinen asematunnus (tässä esimerkissä F:) ja painamalla Poista Yhteys painiketta. Mikäli sinulla on useampia säiliöitä käytössäsi, voit purkaa kaikki käyttöönotot kerralla Poista Kaikki Yhteydet -painikkeella.



Huomioi, että sovellukset, jotka lukitsevat tiedoston käyttöön (kuten Word tai Excel) asettavat lukon myös säiliössä olevaan tiedostoon. Tiedostot on syytä sulkea ennen käyttöönoton purkamista, muutoin saat varoituksen.



Mikäli tähän vastaat Kyllä, kaikki tallentamattomat muutokset kyseisten tiedostojen osalta häviävät ja tiedostot saattavat muuttua käyttökelvottomiksi (korruptoitua).

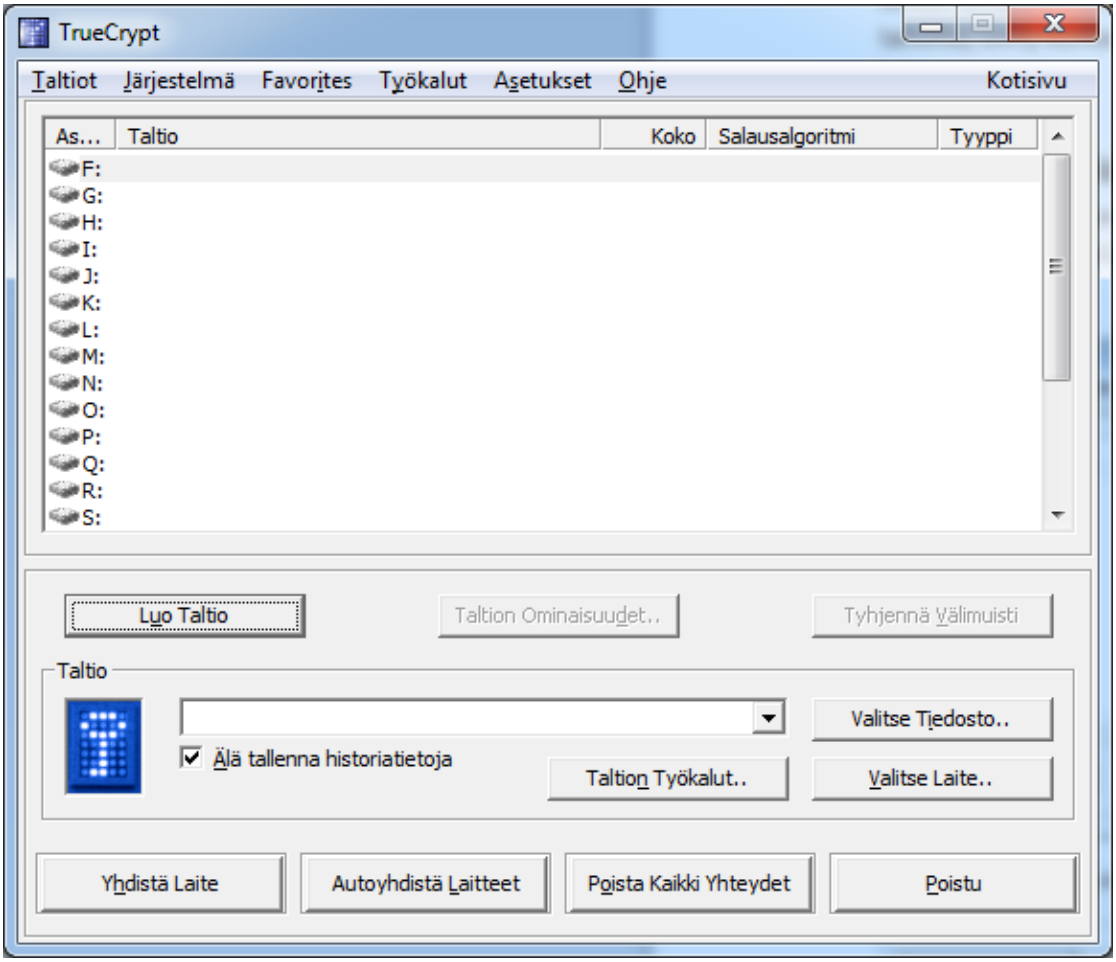
2.2. Lähettäminen (suomenkielinen versio)

Salassa pidettävän tiedon lähettäminen tapahtuu lähettämällä salattu säiliö sähköpostin liitetiedostona. Tässä on huomioitava, että itse viesti kulkee edelleen selkokielisenä (salaamattomana) ja näin ollen **itse viestissä ei saa olla salassa pidettävää tietoa**. Lähetetty viesti tallentuu sähköpostipalvelimen lähetettyihin viesteihin, joten myös lähetetystä säiliöstä jää kopio palvelimelle. Tämä kopio on tietoturvasyistä (tarkemmat perustelut Ylläpidon ohjeessa) syytä poistaa, eli lähetetyn viestin liitetiedostona oleva säiliö on poistettava viestistä kun viesti on lähtenyt.

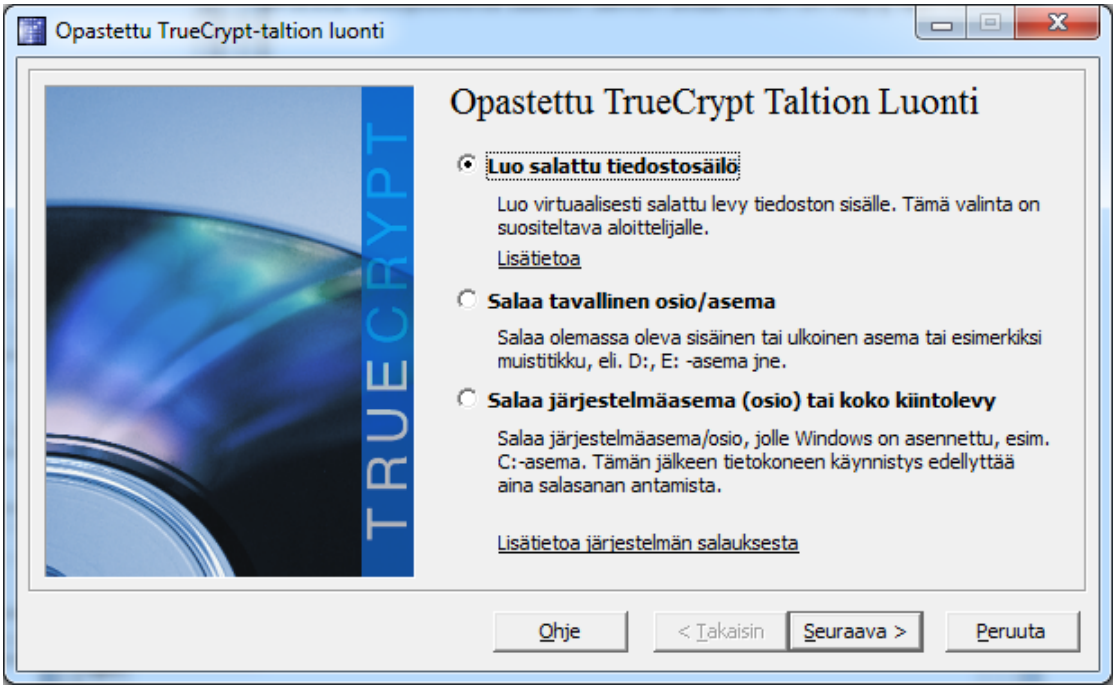
Mikäli sinulla on jo olemassa salattu taltio (olet sen itse luonut tai saanut joltain toiselta taholta) siirry kohtaan 2.2.3. Ulkopuolelta saadun säiliön avaaminen on käyty läpi kohdassa 2.1.

2.2.1. Salatun säiliön (taltion) luominen

Salattu säiliö luodaan valitsemalla asematunnus (kuvassa F:) ja Luo Taltio-painiketta painamalla.

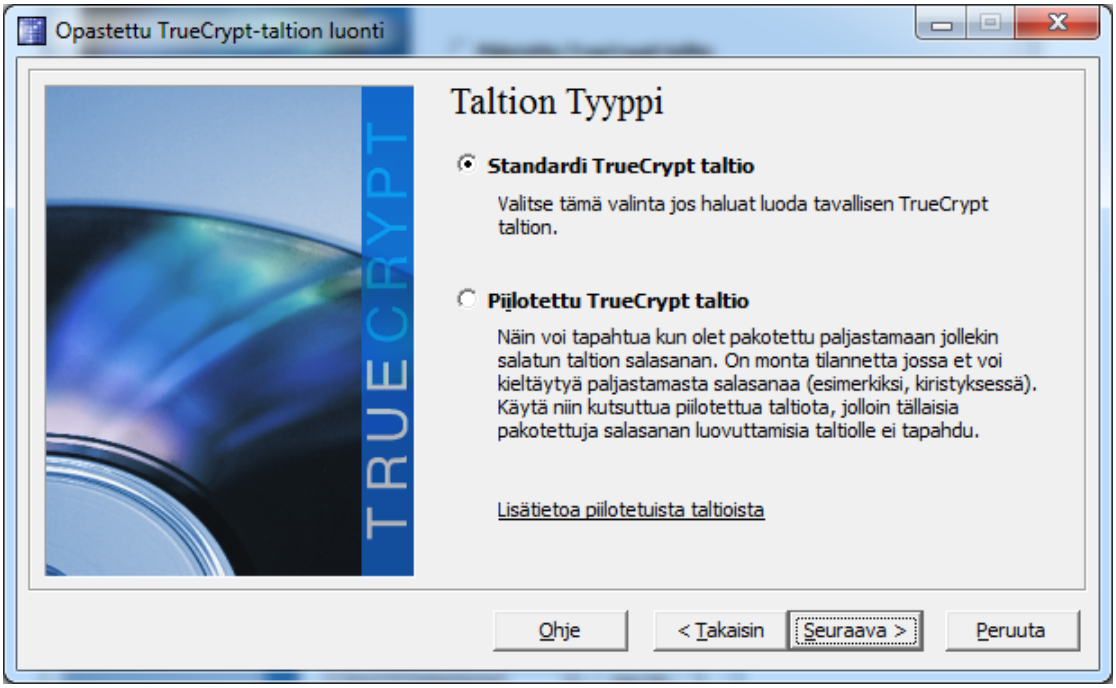


Sähköpostitiedonvälitykseen sopiva vaihtoehto avautuvassa dialogissa on ensimmäinen, Luo salattu tiedostosäiliö.

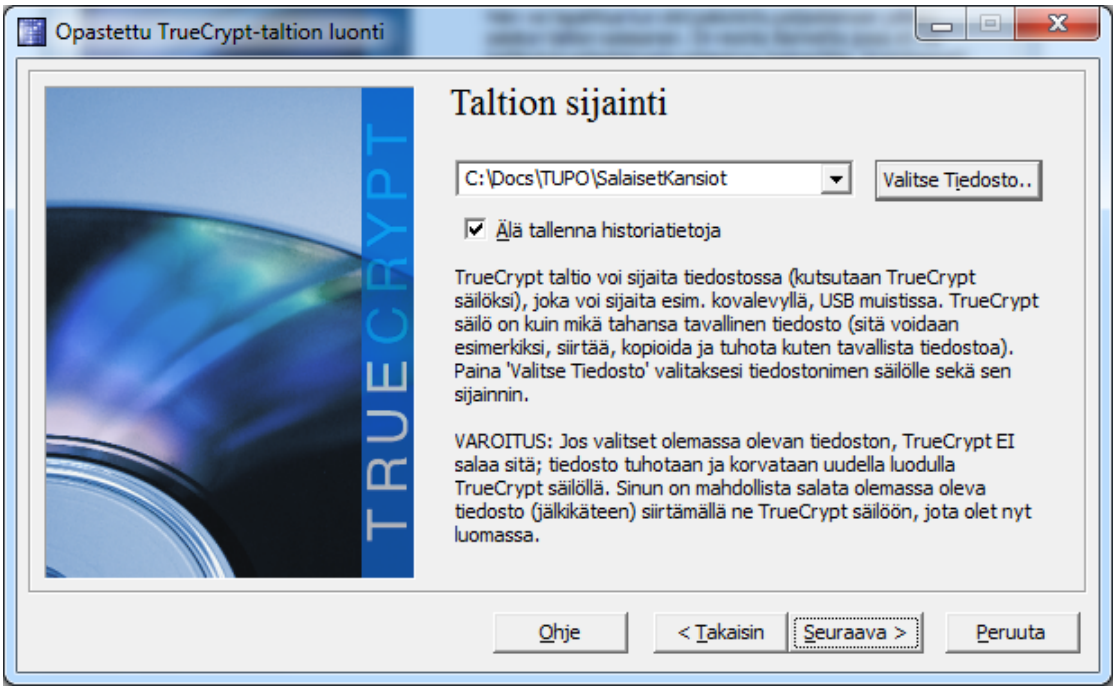


Seuraava -painikkeella pääsee seuraavaan ikkunaan jossa valitaan luotavan tiedoston tyyppi.

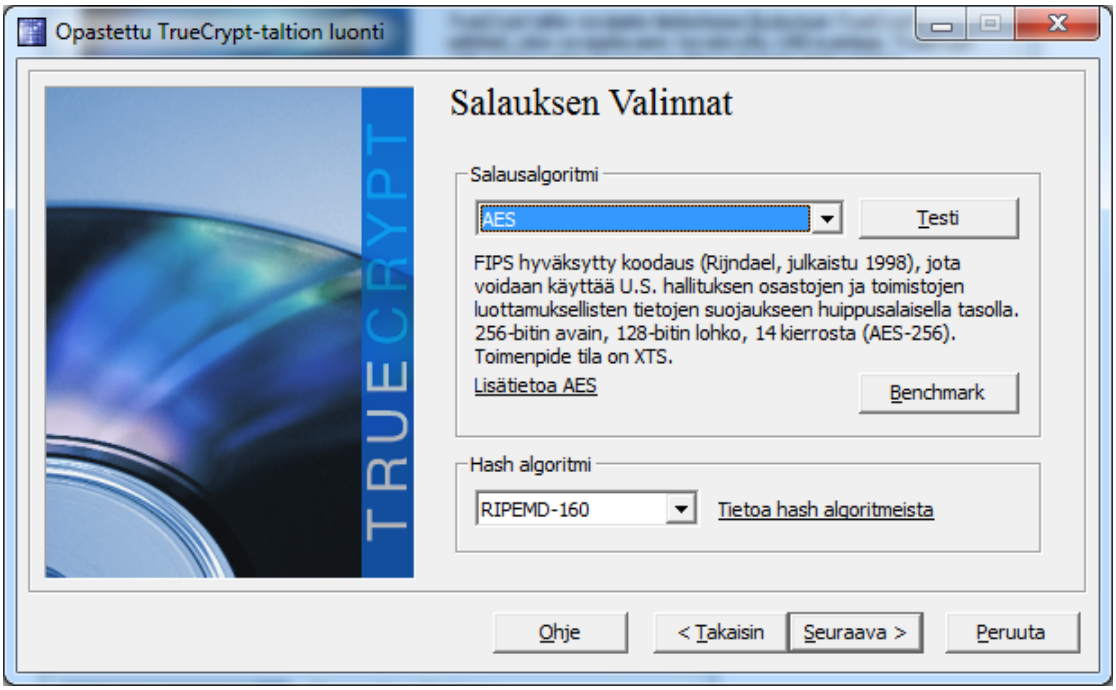
Oletusarvona oleva "Standardi TrueCrypt taltio" sopii sähköpostikäyttöön, joten ikkunasta voi jatkaa matkaa Seuraava -painikkeella.



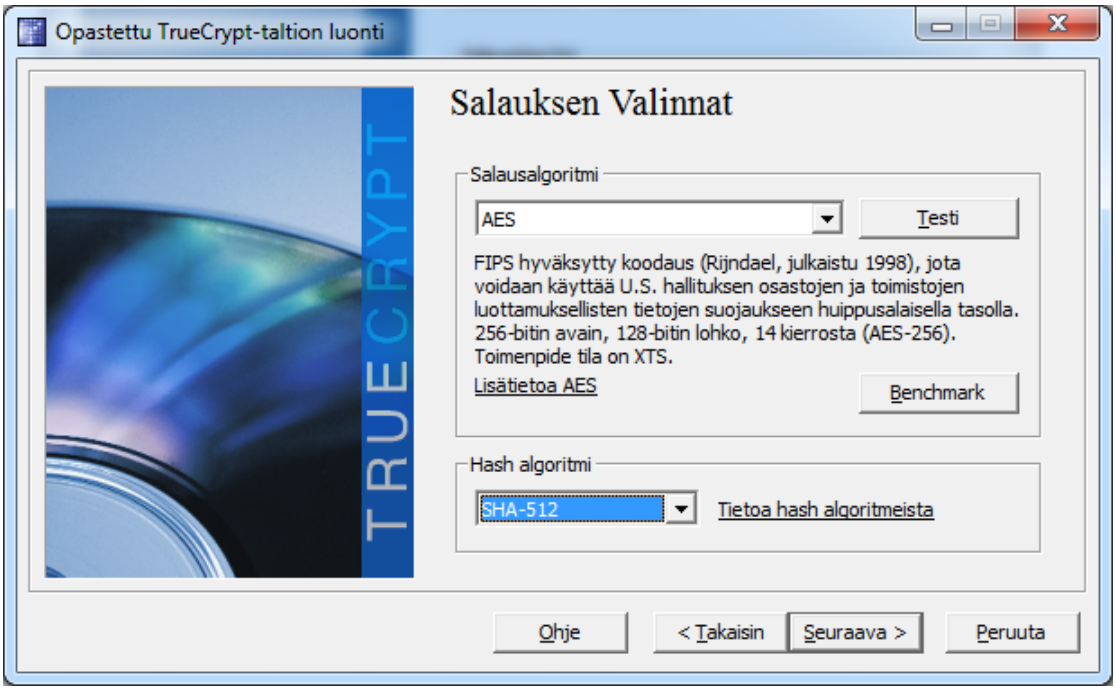
Seuraavassa ikkunassa valitaan tiedosto, johon salattu säiliö luodaan. Säiliön välittäminen sähköpostilla on käytännössä tämän tiedoston siirtämistä sähköpostin liitteenä.



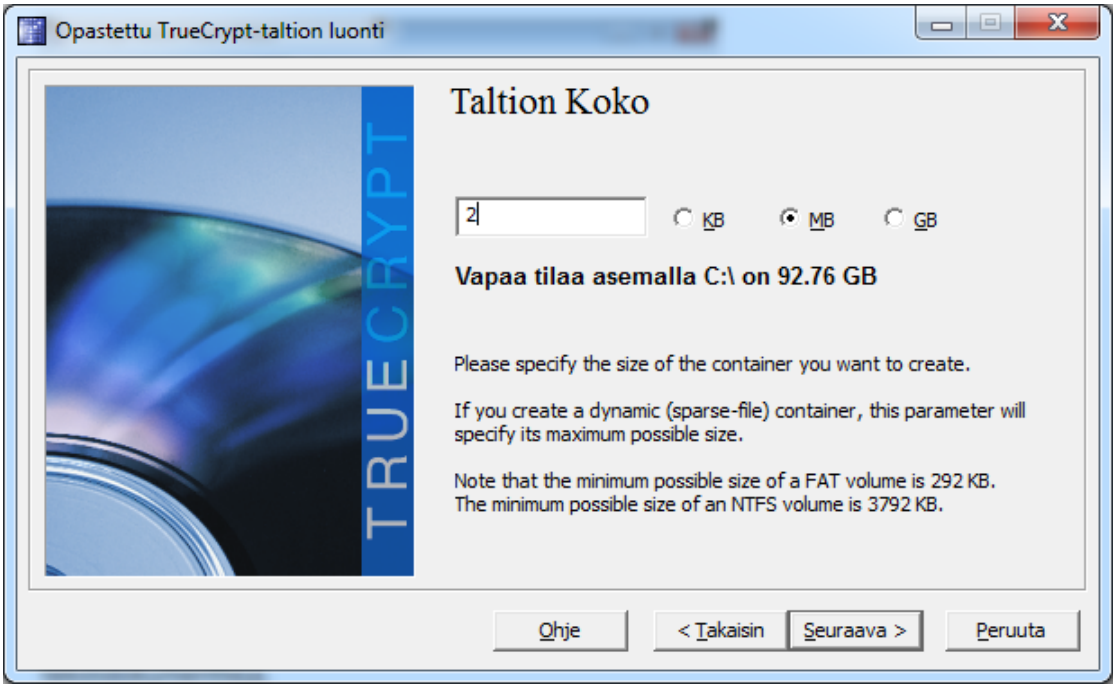
Tässä kohden voit luoda kokonaan uuden tiedoston tai valita olemassa olevan. On syytä huomioida, että jos valitset olemassa olevan tiedoston, sen sisältö hävitetään ja tilalle luodaan uusi tiedosto. Seuraava sivu "Salauksen Valinnat" antaa mahdollisuuden valita käytetty salausmenetelmä.



Oletusarvo "AES" on sopiva, mutta "RIPEMD-160" **EI OLE HYVÄKSYTTY** vaan hajautusalgoritmina (Hash algoritmi) tulee käyttää joko SHA-512 tai Whirlpool.



Valintojen jälkeen jatketaan Seuraava -painikkeella sivulle, jossa voidaan valita luotavan taltion (tiedoston) koko.

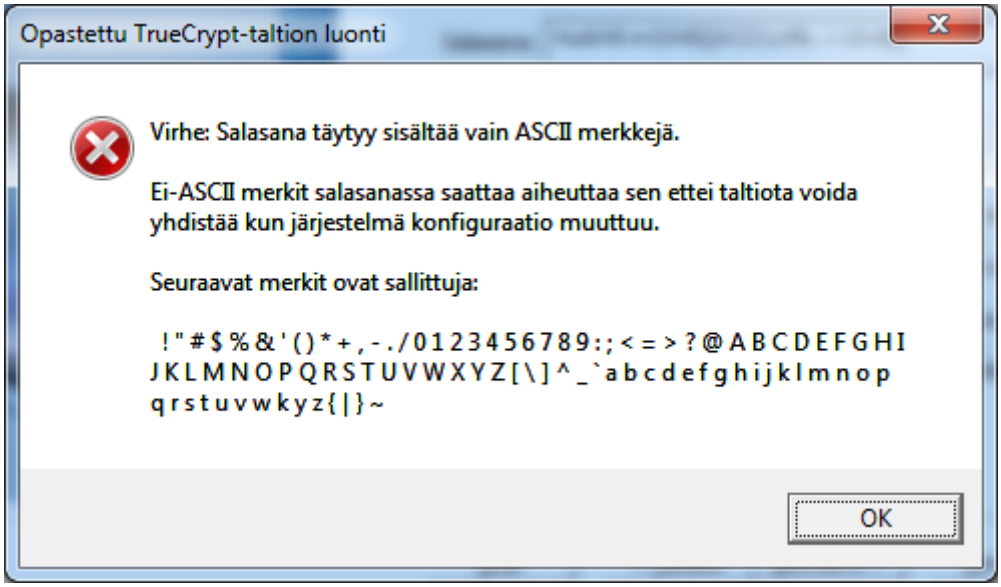


Tiedoston koon valinnassa on hyvä tiedostaa, että tiedostosta tulee valitun kokoinen, vaikka säiliö olisi tyhjä. 10 MB kokoiseen säiliöön mahtuu jo paljon tavaraa, mutta se on usealle sähköpostiohjelmalle liikaa. Näin ollen säiliötä ei kannata tehdä tarpeettoman suureksi, vaan

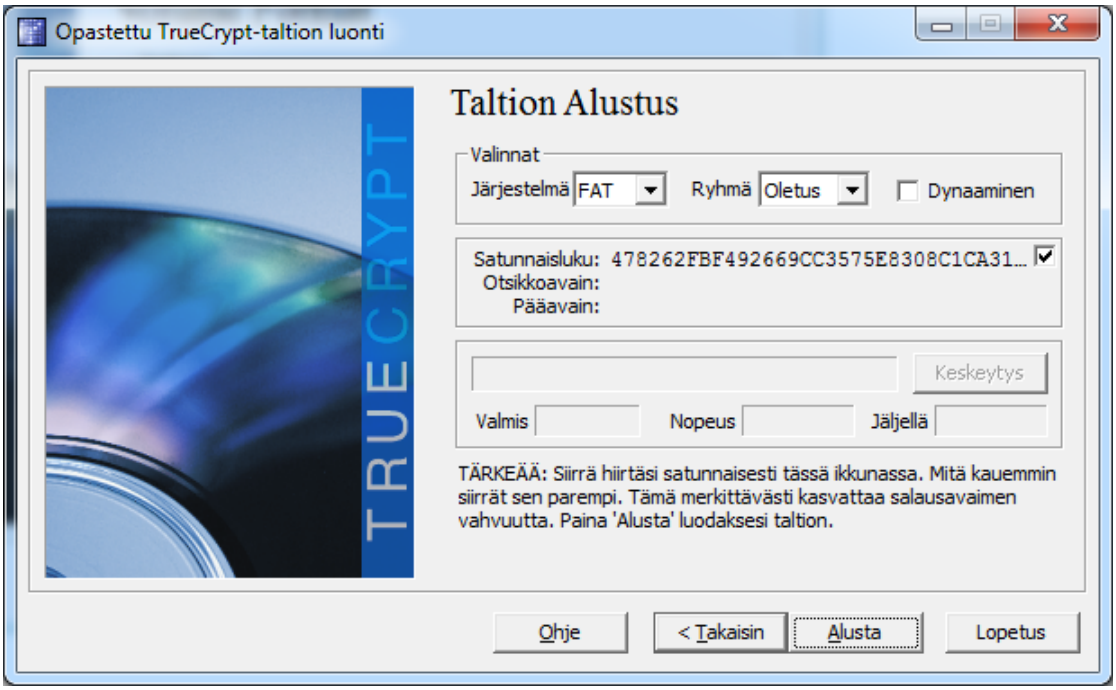
suhteuttaa koko tilan tarpeeseen. Lähtökohtaisesti esim. 5 MB riittää kohtuulliseen määrään tekstidokumentteja.

Salattu säiliö voidaan tehdä joko salasanan tai avaintiedoston avulla. Avaintiedostoa käytettäessä avainmateriaali otetaan tiedoston binäärisestä esityksestä. Tämä vaihtoehto vaatii sen, että jokaisella käyttäjällä on identtisesti sama tiedosto käytössään.

Sähköpostin välittämiseen salasana on ehkä toimivampi ratkaisu. Hyvän salasanan (esimerkissä Hu6t45+rG545QW231ytfe.<<0=8 on kohtuullisen satunnainen) perusvaatimus on että se on mahdollisimman vaikeasti ulkopuolisen arvattavissa. Salasanan **minimipituus on 21** alfanumeerista (isot ja pienet kirjaimet sekä numerot) merkkiä tasolla ST4. TrueCrypt vaatii ASCII merkkejä, joten merkkien joukko on rajattu. Mikäli salasanassa on epäkelpoja merkkejä, syntyy virheilmoitus:

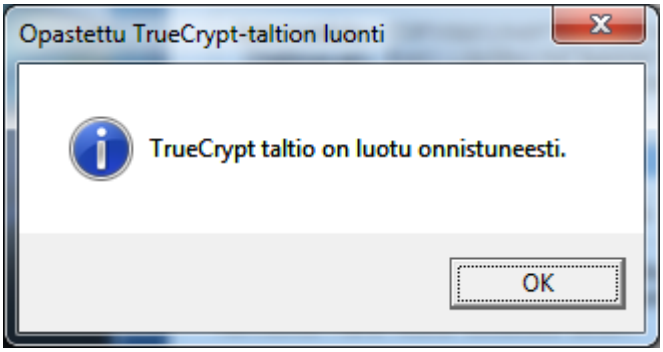


Salasanan vaatimukset salassa pidettävän tiedon välittämiseen löytyy kappaleessa 2.2.2.

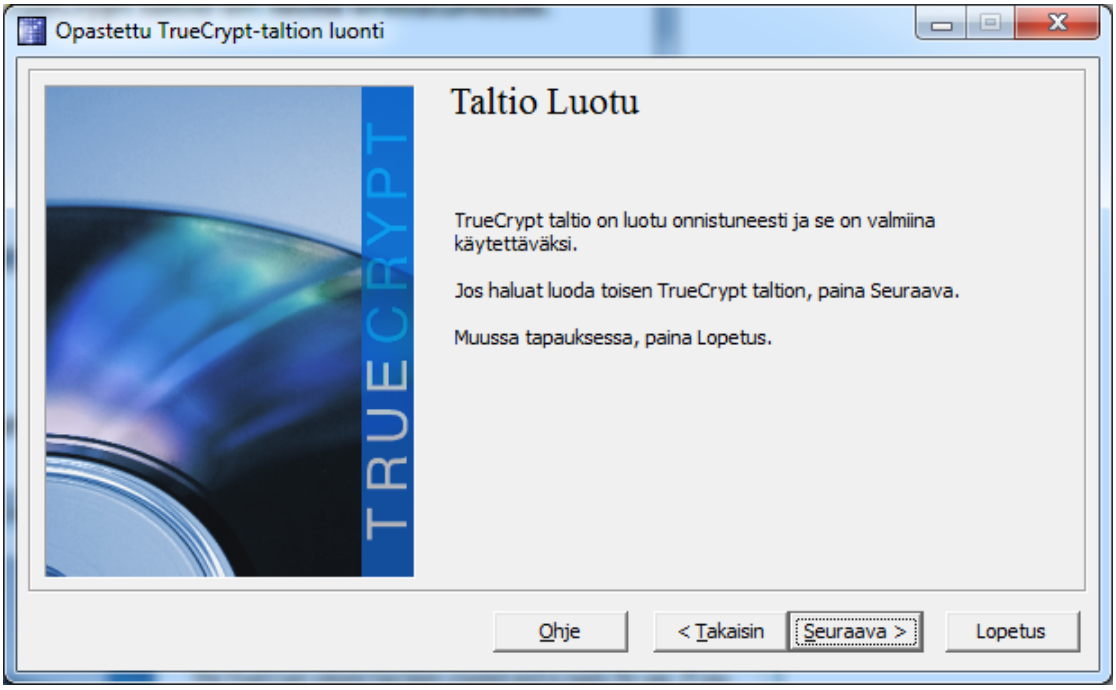


Seuraavaksi valitaan tiedostojärjestelmä, FAT (oletus) on sopiva valinta, eikä Ryhmä valintaan tarvitse koskea. Osion voi luoda myös kooltaan muuttuvaksi (dynaamiseksi), mutta se tuo mukanaan sekä suorituskykyongelmia että riskin osion korruptoitumisesta (tuhoutumisesta) tietyissä tilanteissa, joten sitä ei voi suositella. Parempi tapa on luoda useampi erikokoinen säiliö erilaisiin tarkoituksiin.

Samalla sivulla luodaan myös salausavainten generoinnissa tarvittavaa satunnaisuutta, minkä vuoksi ohjelma pyytää liikuttelemaan hiirtä ikkunan päällä. Tällä tavoin syntynyttä satunnaisuutta käytetään avainten alustuksessa. **ST4 tason minimivaatimus alustuksen vaatimalle satunnaisuudelle on hiiren liikuttelua 20 sekunnin ajan.** Oletusarvot ovat siis ok, ja matka jatkuu Alusta -painikkeen painamisella. Kun säiliö on valmis, tulee ruutuun ilmoitus:



Tämän jälkeen säiliö (taltio) on valmis:



Taltio on nyt valmis ja voidaan ottaa käyttöön. Katso ohje kohdassa 2.1, kohta 2).

2.2.2. Salasanavaatimukset ja salasanan välittäminen

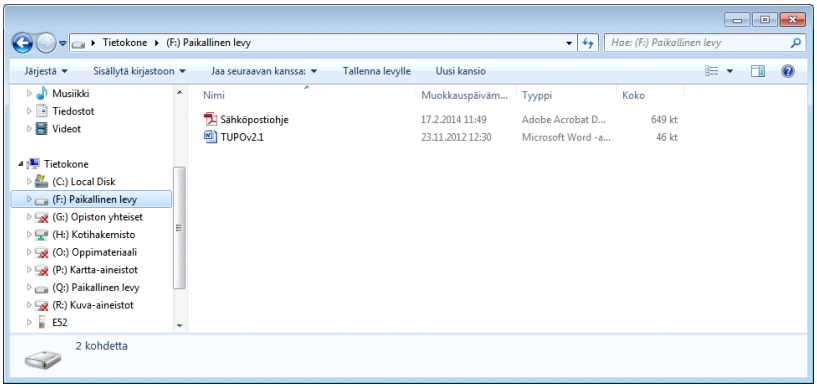
Suojaustasolla ST4 salasanan täytyy olla minimissään 21 merkkiä pitkä, alfanumeerisia merkkejä (isot ja pienet kirjaimet sekä numerot) sisältävä, mahdollisimman satunnaiselta vaikuttava merkkijono. Salasanaa ei saa lähettää vastaanottajalle salaamattomalla sähköpostilla tai matkapuhelimella tekstiviestinä, vaan salasanan vaihdon tulee tapahtua kasvokkain tai muulla vastaavalle suojaustasolle hyväksytyllä menetelmällä.

VAHTI 2/2010 ohjeen mukaan *Suojaustasoon IV luokiteltuun asiakirjaan sisältyviä tietoja voidaan eräissä tapauksissa käsitellä puhelimessa peitetysti*. Näin ollen salasanan voi harkinnan mukaan välittää tunnetulle henkilölle puhelimessa peitellysti. Mitä peitellysti tarkoittaa on soittajan itsensä päätettävä, mutta puhelinkeskustelussa on ainakin syytä pidättäytyä mainitsemasta mihin tarkoitukseen salasanaa käytetään. Tekstiviestistä jää aina digitaalisia jälkiä, joten salaamattoman tekstiviestin lähettäminen on turvattomampi tapa, varsinkin jos samaa päätelaitetta käytetään sähköpostin lukemiseen. Tällöin syntyy riski, että sekä salasana että käytetty säiliö ovat samassa laitteessa. Tällöin laitteen kadottaminen aiheuttaa vakavan tietoturvapoikkeaman.

2.2.3. Tiedostojen lisääminen säiliöön (taltioon)

Kun säiliö (taltio) on otettu käyttöön (Ohjeen kohta 2.1), tiedostoja voi lisätä, poistaa ja muokata kuten mille tahansa levylle (tai vaikkapa usb muistitikulla).

Levy näkyy valitulla tunnuksella (tässä F:) normaalisti tiedostojärjestelmässä:



Kun säiliö "irrotetaan" Poista yhteys -painikkeella (ohjeen kohta 2.1 f), se on lähetettävissä sähköpostilla normaalisti liitetiedostona.

2.3. *Vastaanottaminen (englanninkielinen versio)*

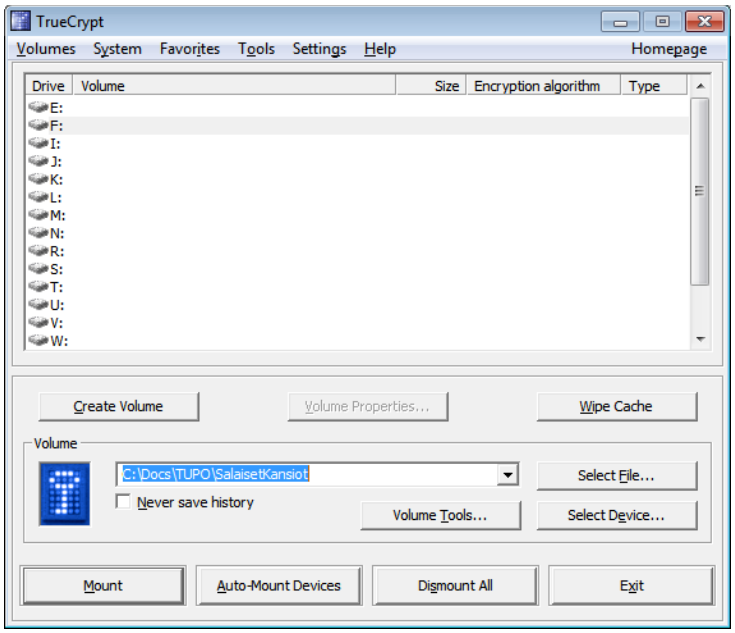
Tämä ohje on identtinen kappaleen 2.2 suomenkielisen version kanssa, lukuun ottamatta sovelluksessa käytettyä kieltä.

1) Vastaanotettu liite (salattu säiliö) tallennetaan tiedostoksi levylle. Esimerkissä se on tallennettu nimellä C:\Docs\TUPO\SalaisetKansiot. Huomaa, ettei säiliöllä yleensä ole tiedostopäätettä.

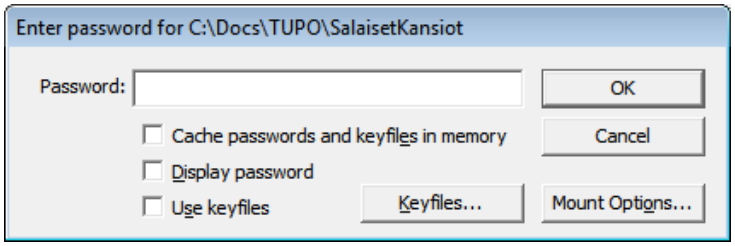
2) Tiedosto otetaan käyttöön TrueCrypt ohjelmalla seuraavasti:

a) Valitse haluamasi kirjain levyn tunnukseksi ohjelman listalta (esimerkissä valittu F:) Säiliö tulee näkymään koneessasi erillisenä levynä (kuten mm. muistitikut) kyseisellä tunnuksella.

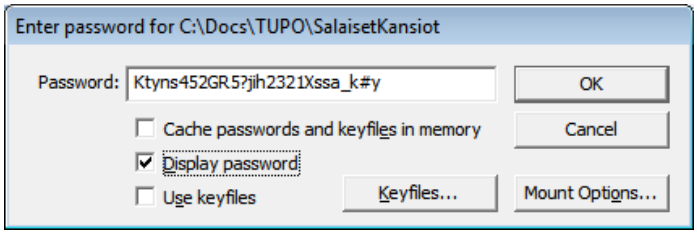
b) Valitse tiedosto Select File -painikkeella. Tässä esimerkissä tiedosto on C:\Docs\TUPO\SalaisetKansiot.



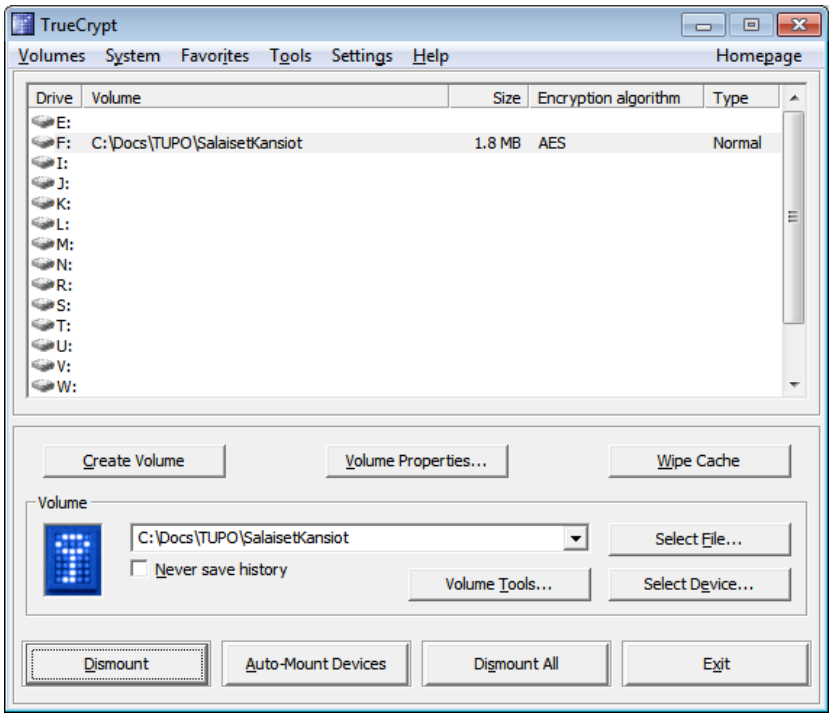
c) Paina Mount painiketta, jolloin ohjelma kysyy salasanaa.



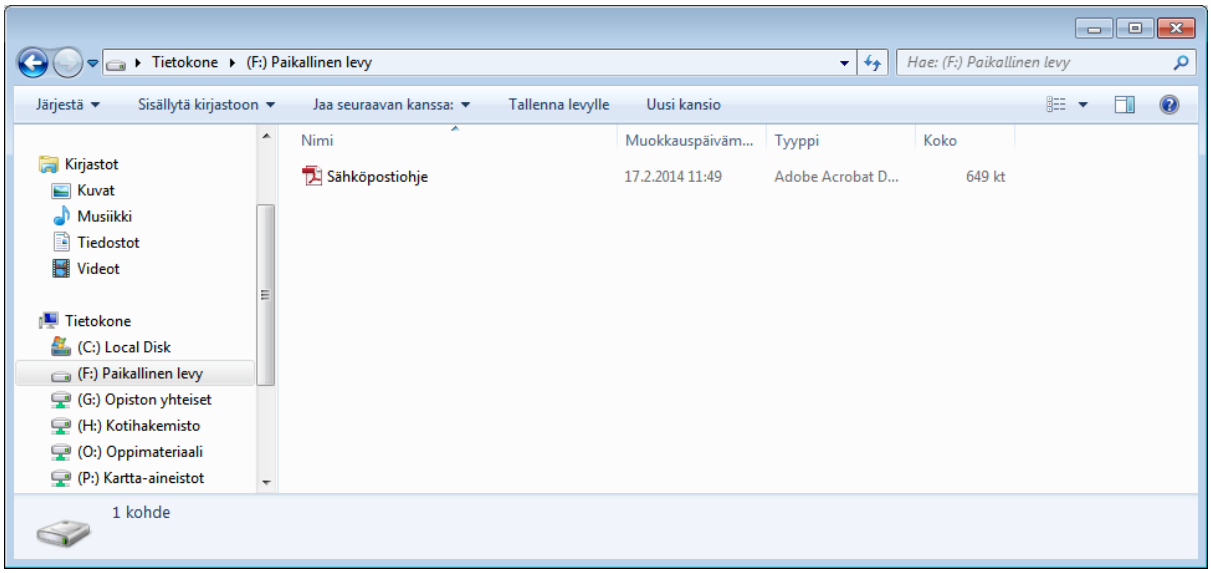
d) Syötettyäsi salasanan, paina OK painiketta. Saat kirjoittamasi salasanan tarvittaessa näkyviin Display password valinnalla. Salasanan olet saanut tiedoston lähettäjältä, toivottavasti jollain muulla tavalla kuin sähköpostilla.



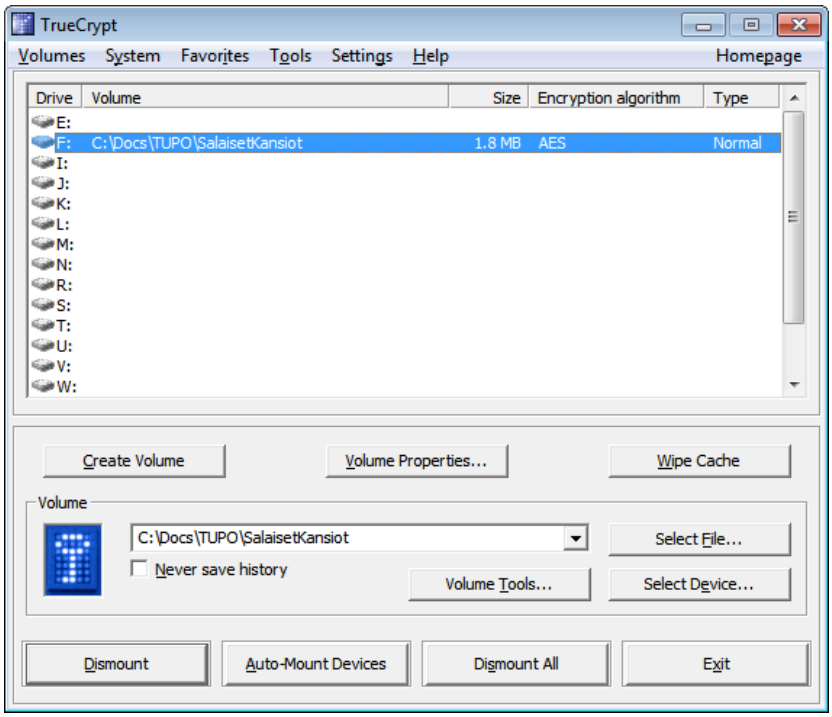
e) Onnistuneen "mounttamisen" jälkeen säiliö näkyy listalla. Säiliöstä kerrotaan tiedosto jossa se sijaitsee, säiliön koko ja käytetty salausalgoritmi (tässä AES, Advanced Encryption Standard).



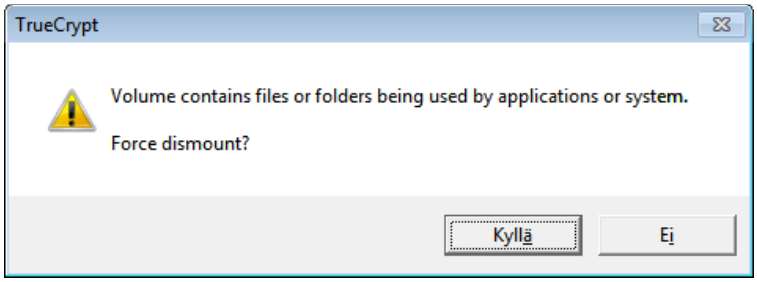
Säiliön tiedot ovat nyt käytettävissä normaalin levyn/ulkoisen muistin tavoin. Voit avata tiedostoja, muokata ja tallentaa tavanomaiseen tapaan.



f) Lopuksi säiliön käyttöönotto (mounttaus) on syytä purkaa, etenkin jos olet muokannut säiliön sisältöä. Tämä tapahtuu valitsemalla kyseinen asematunnus (tässä esimerkissä F:) ja painamalla Dismount painiketta. Mikäli sinulla on useampia säiliöitä käytössäsi, voit purkaa kaikki käyttöönotot kerralla Dismount all -painikkeella.



Huomioi, että sovellukset, jotka lukitsevat tiedoston käyttöön (kuten Word tai Excel) asettavat lukon myös säiliössä olevaan tiedostoon. Tiedostot on syytä sulkea ennen käyttöönoton purkamista, muutoin saat varoituksen.



Mikäli tähän vastaat Kyllä, kaikki tallentamattomat muutokset kyseisten tiedostojen osalta häviävät ja tiedostot saattavat muuttua käyttökelvottomiksi (korruptoitua).

2.4. Lähettäminen (englanninkielinen versio)

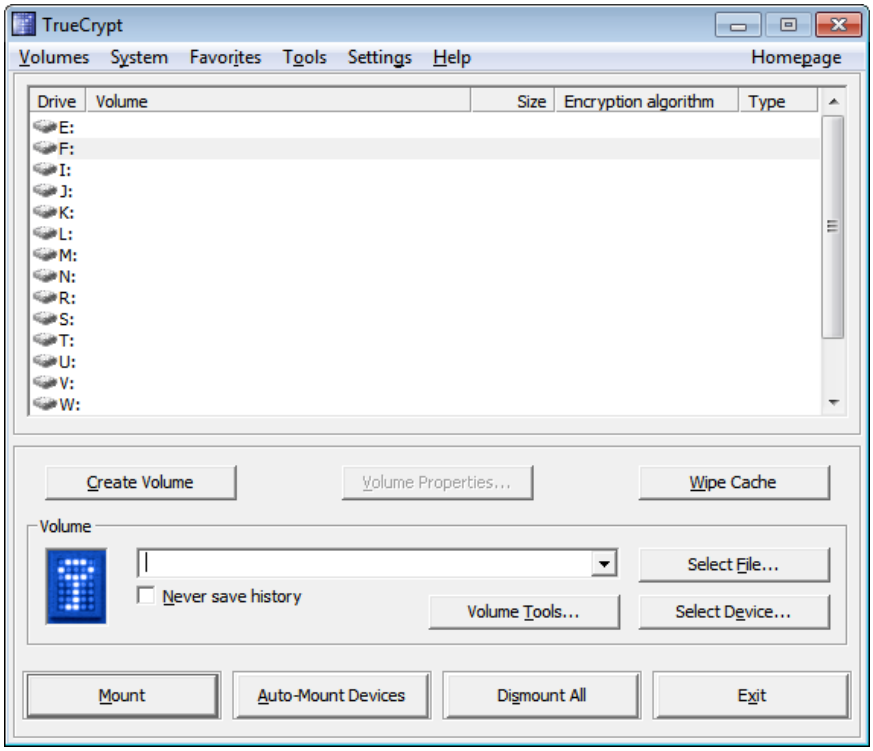
Salassa pidettävän tiedon lähettäminen tapahtuu lähettämällä salattu säiliö sähköpostin liitetiedostona. Tässä on huomioitava, että itse viesti kulkee edelleen selkokielisenä (salaamattomana) ja näin ollen **itse viestissä ei saa olla salassa pidettävää tietoa**. Lähetetty viesti tallentuu sähköpostipalvelimen lähetettyihin viesteihin, joten myös lähetetystä säiliöstä jää kopio palvelimelle. Tämä kopio on tietoturvasyistä (tarkemmat perustelut Ylläpidon ohjeessa) syytä

poistaa, eli lähetetyn viestin liitetiedostona oleva säiliö on poistettava viestistä kun viesti on lähtenyt.

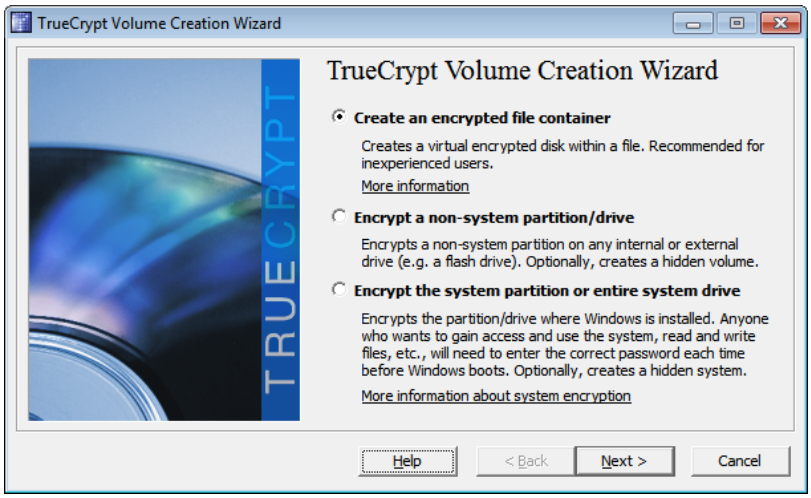
Mikäli sinulla on jo olemassa salattu säiliö (olet sen itse luonut tai saanut joltain toiselta taholta) siirry kohtaan 2.4.3. Ulkopuolelta saadun säiliön avaaminen on käyty läpi kohdassa 2.3.

2.4.1. Salatun säiliön luominen

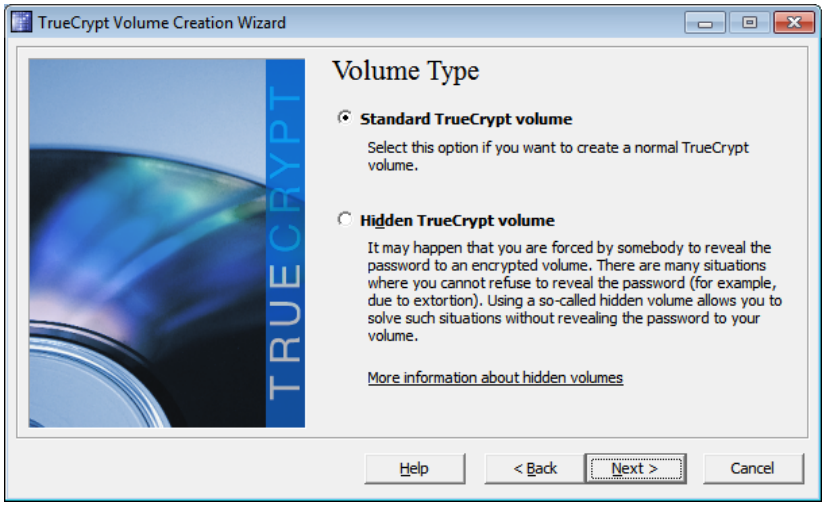
Salattu säiliö luodaan valitsemalla asematunnus (kuvassa F:) ja Create Volume -painiketta painamalla.



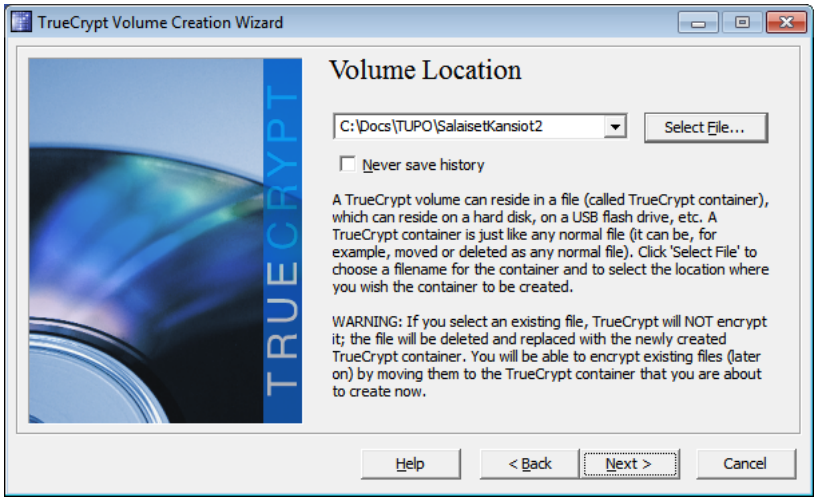
Sähköpostitiedonvälitykseen sopiva vaihtoehto avautuvassa dialogissa on ensimmäinen, Create an encrypted file container.



Next -painikkeella pääsee seuraavaan ikkunaan jossa valitaan luotavan tiedoston tyyppi.



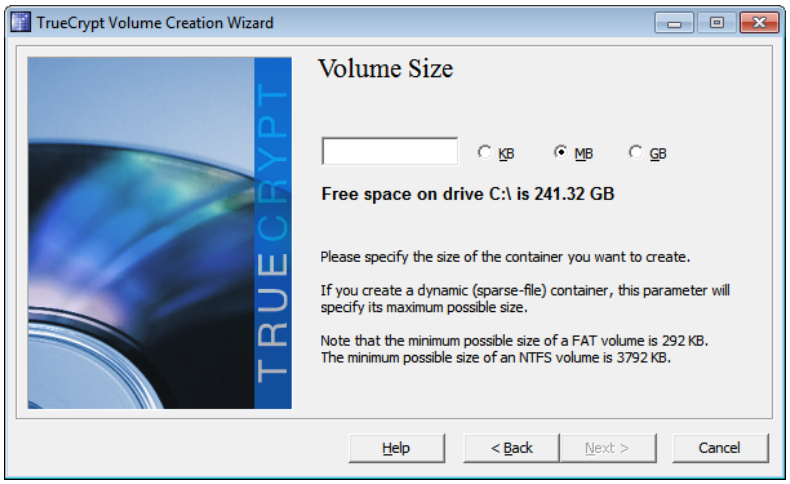
Oletusarvona oleva "Standard TrueCrypt volume" sopii sähköpostikäyttöön, joten ikkunasta voi jatkaa matkaa Next -painikkeella.



Seuraavassa ikkunassa valitaan tiedosto, johon salattu säiliö luodaan. Säiliön välittäminen sähköpostilla on käytännössä tämän tiedoston siirtämistä sähköpostin liitteenä. Tässä kohden voit luoda kokonaan uuden tiedoston tai valita olemassa olevan. On syytä huomioida, että jos valitset olemassa olevan tiedoston, sen sisältö hävitetään ja tilalle luodaan uusi tiedosto.

Oletusarvo "AES" on sopiva, mutta "RIPEMD-160" EI OLE HYVÄKSYTTY vaan hajautusalgoritmina (Hash algoritmi) tulee käyttää joko SHA-512 tai Whirlpool.

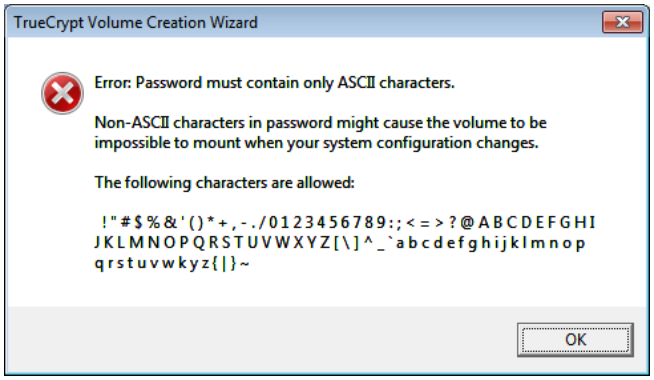
Valintojen jälkeen jatketaan Seuraava -painikkeella sivulle, jossa voidaan valita luotavan taltion (tiedoston) koko.



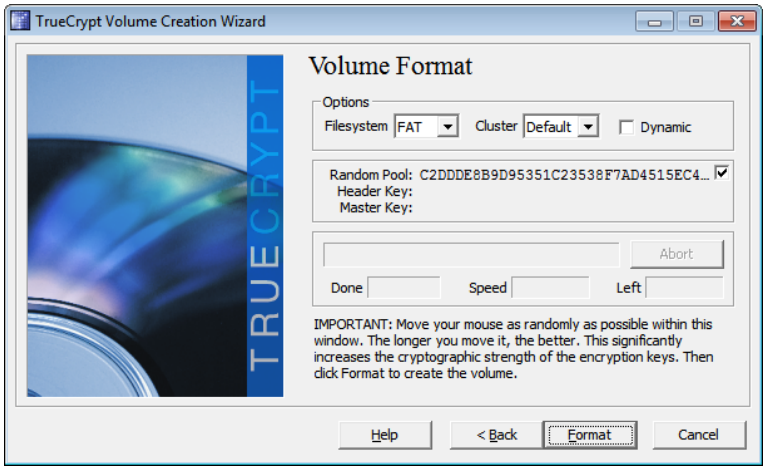
Tiedoston koon valinnassa on hyvä tiedostaa, että tiedostosta tulee valitun kokoinen, vaikka säiliö olisi tyhjä. 10 MB kokoiseen säiliöön mahtuu jo paljon tavaraa, mutta se on usealle sähköpostiohjelmalle liikaa. Näin ollen säiliötä ei kannata tehdä tarpeettoman suureksi, vaan suhteuttaa koko tilan tarpeeseen. Lähtökohtaisesti esim. 2 MB riittää suureen määrään tekstidokumentteja.

Salattu säiliö voidaan tehdä joko salasanan tai avaintiedoston avulla. Avaintiedostoa käytettäessä avainmateriaali otetaan tiedoston binäärisestä esityksestä. Tämä vaihtoehto vaatii sen, että jokaisella käyttäjällä on identtisesti sama tiedosto käytössään.

Sähköpostin välittämiseen salasana on ehkä toimivampi ratkaisu. Hyvän salasanan perusvaatimus on että se on mahdollisimman vaikeasti ulkopuolisen arvattavissa. Salasanan **minimipituus on 21 alfanumeerista (isot ja pienet kirjaimet sekä numerot) merkkiä tasolla ST4**. TrueCrypt vaatii ASCII merkkejä, joten merkkien joukko on rajattu. Mikäli salasanassa on epäkelpoja merkkejä, syntyy virheilmoitus:

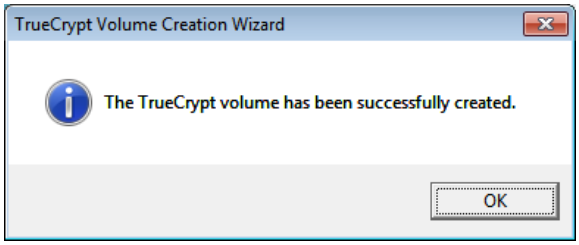


Salasanan vaatimukset salassa pidettävän tiedon välittämiseen löytyy kappaleessa 2.3.3.

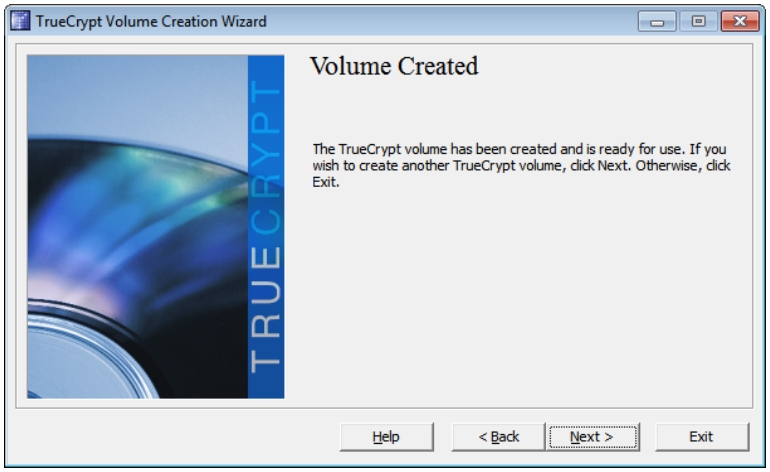


Seuraavaksi valitaan tiedostojärjestelmä, FAT (oletus) on sopiva valinta, eikä Cluster valintaan tarvitse koskea. Osion voi luoda myös kooltaan muuttuvaksi (dynaamiseksi), mutta se tuo mukanaan sekä suorituskykyongelmia että riskin osion korruptoitumisesta (tuhoutumisesta) tietyissä tilanteissa, joten sitä ei voi suositella. Parempi tapa on luoda useampi erikokoinen osio eri tarkoituksiin.

Samalla sivulla luodaan myös salausavainten generoinnissa tarvittavaa satunnaisuutta, minkä vuoksi ohjelma pyytää liikuttelemaan hiirtä ikkunan päällä. Tällä tavoin syntynyttä satunnaisuutta käytetään avainten alustuksessa. **ST4 tason minimivaatimus alustuksen vaatimalle satunnaisuudelle on hiiren liikuttelua 20 sekunnin ajan**. Oletusarvot ovat siis ok, ja matka jatkuu Format -painikkeen painamisella. Kun säiliö on valmis, tulee ruutuun ilmoitus:



Tämän jälkeen osio on valmis:



Osio on nyt valmis ja voidaan ottaa käyttöön. Katso ohje kohdassa 2.3, kohta 2).

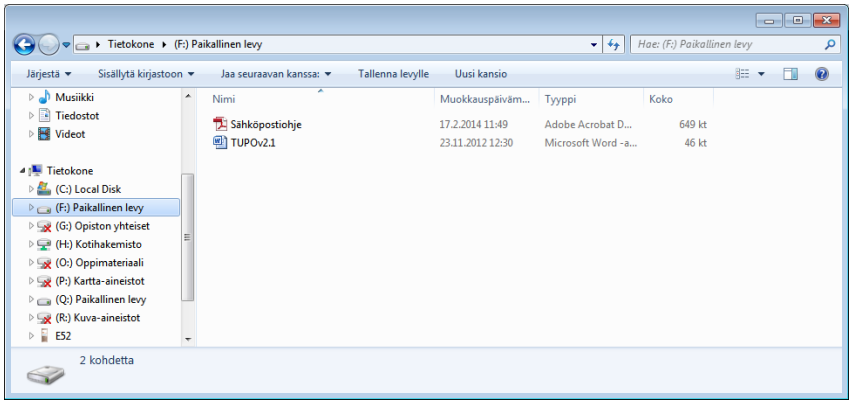
2.4.2. Salasanavaatimukset

Katso kohta 1.2.2.

2.4.3. Tiedostojen lisääminen säiliöön

Kun säiliö on otettu käyttöön (Ohjeen kohta 2.3), tiedostoja voi lisätä, poistaa ja muokata kuten mille tahansa levylle (tai vaikkapa usb muistitikulla).

Levy näkyy valitulla tunnuksella (tässä F:) normaalisti tiedostojärjestelmässä:



Kun säiliö "irroitetaan" Dismount -painikkeella (ohjeen kohta 2.3 f), se on lähetettävissä sähköpostilla normaalisti liitetiedostona.

3. SÄHKÖPOSTI TOIMIKORTTIA KÄYTTÄEN

Toimikorttia käytettäessä salassa pidettävän tiedon välittämiseen luottamuksellisuus perustuu vastaanottajan julkisella avaimella tehtyyn salaukseen. Julkisella avaimella tehdyn salauksen voi purkaa ainoastaan vastaavan salaisen avaimen sisältämän toimikortin avulla (Periaatteessa salainen avain voi olla muuallakin kuin toimikortilla, mutta tässä yhteydessä salaus puretaan toimikortilla).

Julkisen avaimen salaus mahdollistaa myös digitaalisen allekirjoituksen sekä vahvan tunnistautumisen. Digitaalisella allekirjoituksella voidaan tuottaa johdannossa esitetty kiistämättömyyden ominaisuus, koska voidaan olla varmoja että henkilön julkisella avaimella todennettava allekirjoitus on kyseisen henkilön tuottama.

Julkisen avaimen menettelyssä olennaisessa roolissa on varmenne, jolla julkisen avaimen omistajuus varmennetaan. Varmenne kertoo luotettavasti julkisen avaimen omistajan tiedot ja mikäli varmenne on luotettavan tahon myöntämä, voidaan myös olla suhteellisen varmoja että kyseisellä käyttäjällä (ja vain hänellä) on hallussaan julkiseen avaimeen liittyvä salainen avain.

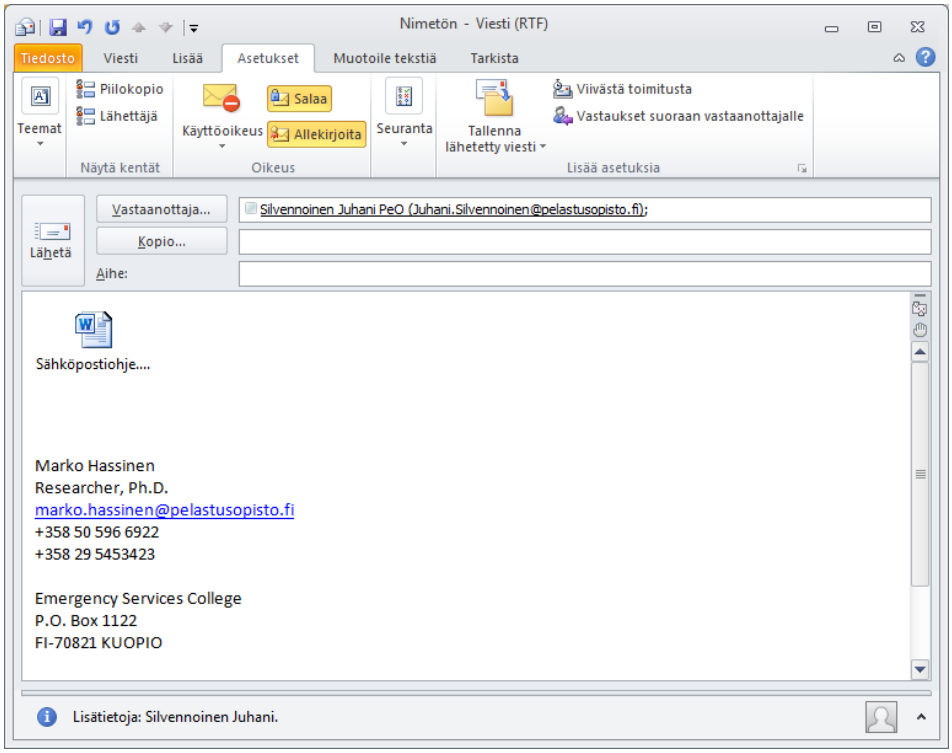
Varmenteet tallennetaan (yleensä) varmennehakemistoon. Jotta varmennetta vastaavan salaisen avaimen haltijalle (henkilö, jolle varmenne on myönnetty) voidaan lähettää salattu viesti, täytyy saada haltuun henkilön julkinen avain. Julkinen avain on osa varmennetta. Näin ollen viestin lähettäjällä täytyy olla pääsy varmennehakemistoon, jossa vastaanottajan organisaation varmenteet ovat.

Mikäli varmenteet on päätetty jättää hakemistosta pois, vaatii kommunikointi etukäteistoimenpiteitä, jotka on esitetty kohdassa "Esivalmistelut silloin kun varmennetta ei ole hakemistossa". Tämän ohjeen kirjoittamishetkellä (Elokuu 2014) pelastustoimen virkakortin varmenteet eivät ole hakemistosta saatavilla.

3.1.1. Salatun viestin lähettäminen Outlook -ohjelmalla

Salatun viestin lähettäminen Outlook ohjelmalla on hyvin yksinkertaista silloin, kun vastaanottajan varmennetiedot ovat ennestään sähköpostiohjelman tiedossa (ellei ole, katso kohta asetukset) tai ne löytyvät hakemistosta. Viestin kirjoittaminen ja liitteiden liittäminen tapahtuu normaaliin tapaan. Salaus (ja tarvittaessa allekirjoitus) tehdään Asetukset välilehdeltä valitsemalla tarvittavat Oikeus -kohdasta. Tämän jälkeen viesti lähetetään normaaliin tapaan Lähetä -painikkeella.

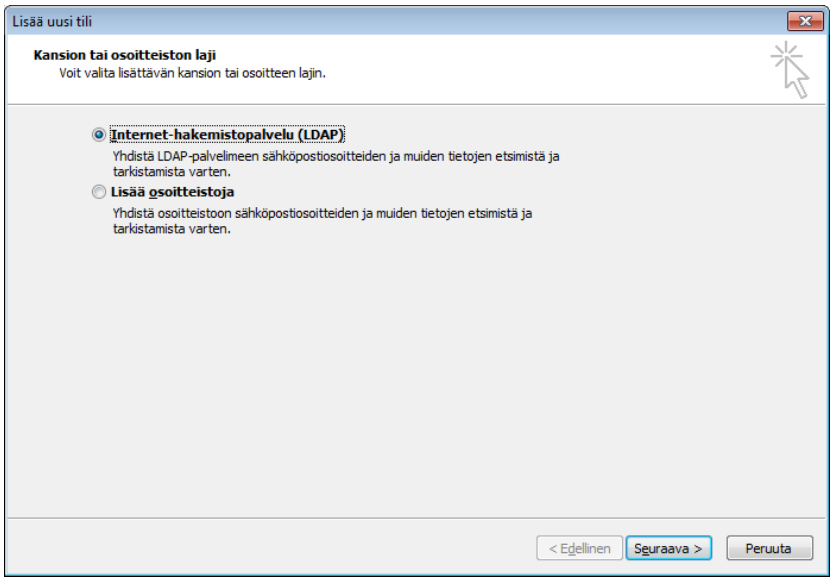
Yleensä Outlook vaatii että myös lähettäjällä on oma digitaalinen tunnus, eli molemmilla osapuolilla tulee olla toimikortti tai vastaava digitaalinen tunnus joka voi olla toteutettu myös ilman toimikorttia.



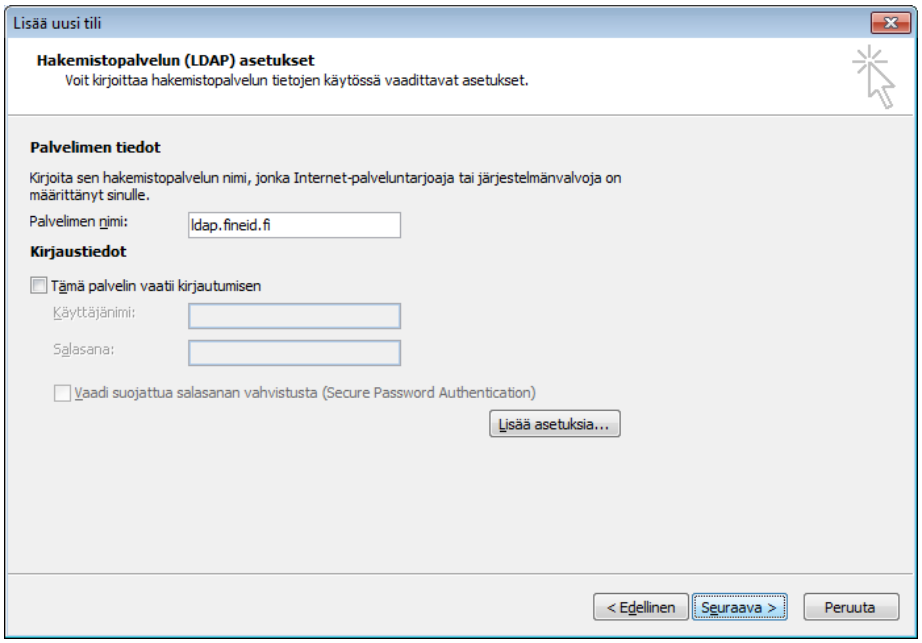
3.1.2. Outlook asetukset

Outlook tarvitsee yhden olennaisen asetuksen salatun sähköpostin käyttöön, eli varmennehakemiston sijainnin. Lähetettäessä salattua postia tarvitaan vastaanottajan varmenne ja vastaavasti vastaanotettaessa tarvitaan lähettäjän varmenne. Jotta nämä varmenteet olisivat saatavilla, on olemassa varmennehakemistoja (kuten Väestörekisterikeskuksen FINEID hakemisto). Tässä ohjeessa pitäydytään Väestörekisterikeskuksen toimikorttien käytössä ja niihin liittyvässä varmennehakemistossa, joka löytyy palvelimelta ldap.fineid.fi. Hakemisto otetaan Outlookissa käyttöön sähköpostitilin asetuksista, Tiedosto->Tiliasetukset josta välilehti osoitteistot.

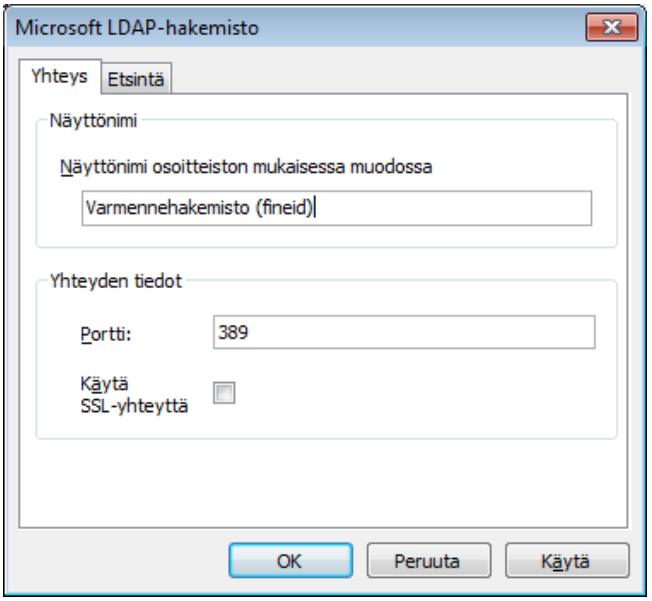
Varmennehakemisto lisätään (ellei sitä jo ole asetettu) Uusi… -painikkeella.



Sopiva valinta avautuvassa ruudussa on Internet-hakemistopalvelu (LDAP). Seuraavaksi annetaan varmennepalvelimen nimi, Väestörekisterikeskuksen kyseessä ollessa ldap.fineid.fi.

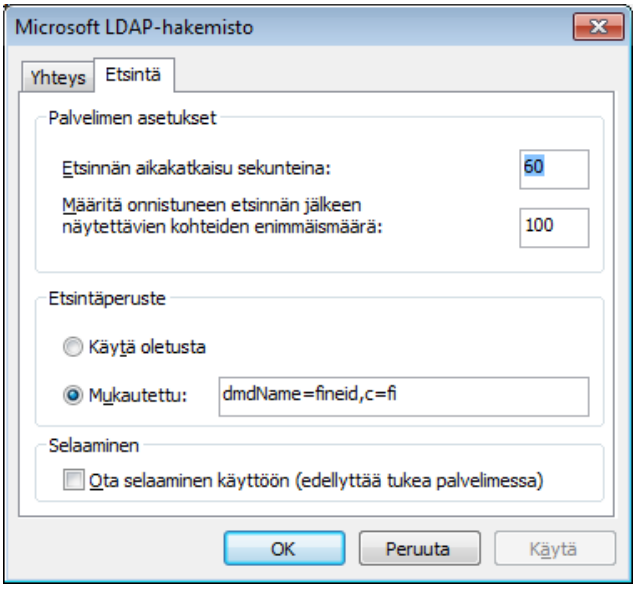


Lisää asetuksia -painikkeella hakemistolle voi mm. antaa haluamansa nimen:

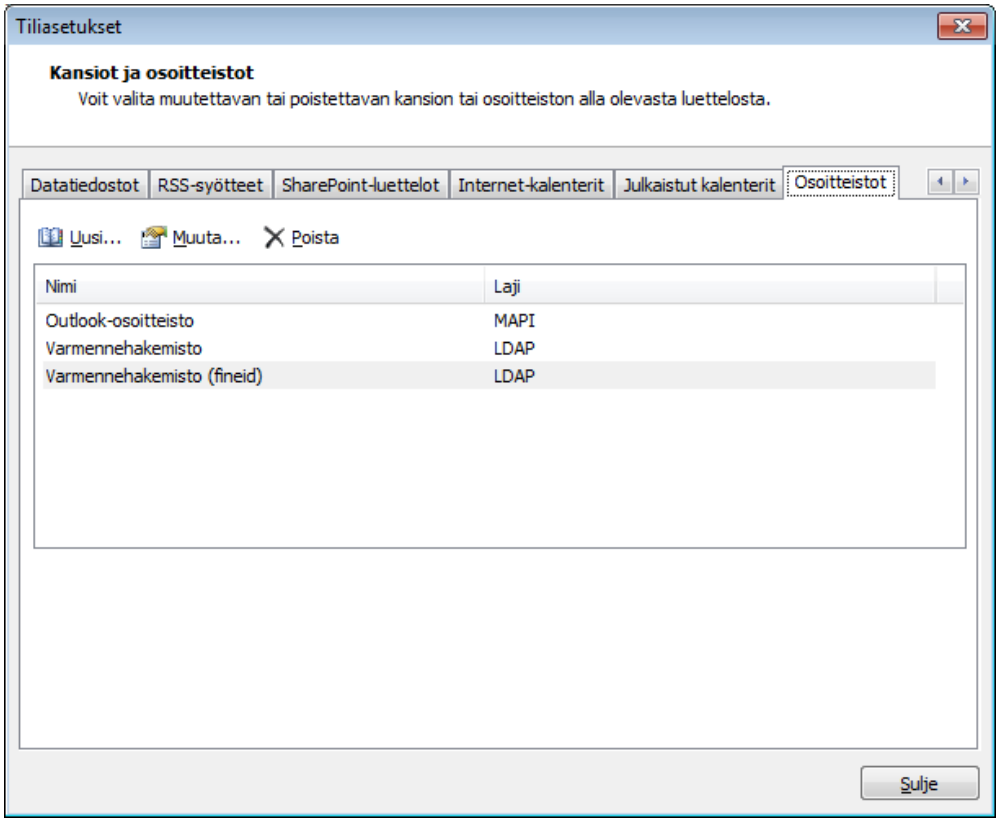


Varmennehakemiston lisättyään voi kyseisen varmentajan (tässä VRK) varmentamille henkilöille lähettää salattua (ja allekirjoitettua) sähköpostia.

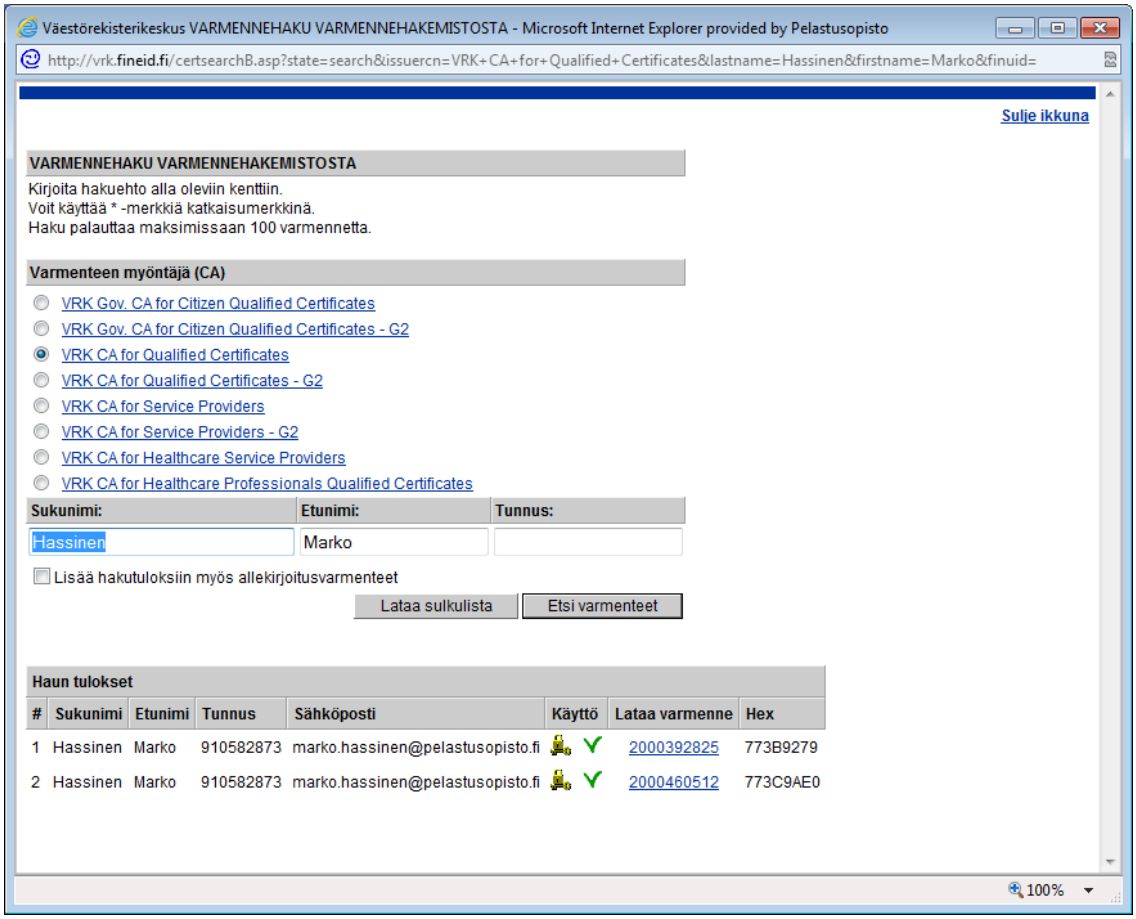
Käytettäessä Fineid hakemistoa, välilehdelle Etsintä on tarpeen laittaa mukautettu etsintäperuste, jotta vastaanottajan varmenne sieltä löytyy. Etsintäperuste on tässä tapauksessa dmdName=fineid,c=fi jolloin varmenteita haetaan oikeasta hakemistosta.



Tallenna asetukset painamalla OK, Seuraava, Valmis.



Yksittäisiä varmenteita voi hakea VRK:n sivulta, osoitteesta http://vrk.fineid.fi/certsearchB.asp



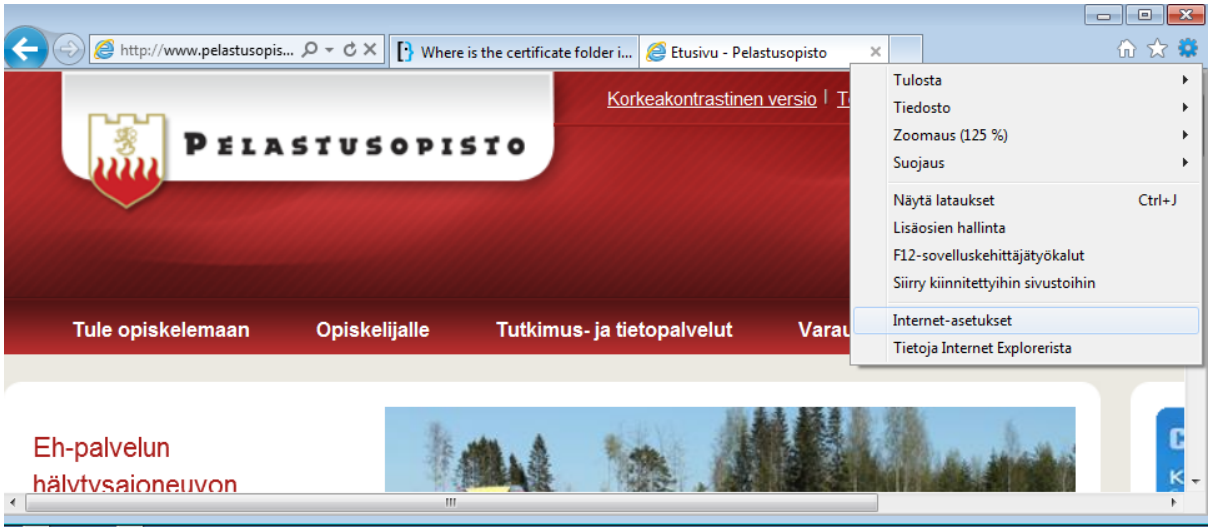
Organisaatiovarmenteet löytyvät listalta VRK CA for Qualified Certificates.

3.1.3. Esivalmistelut silloin kun varmennetta ei ole hakemistossa

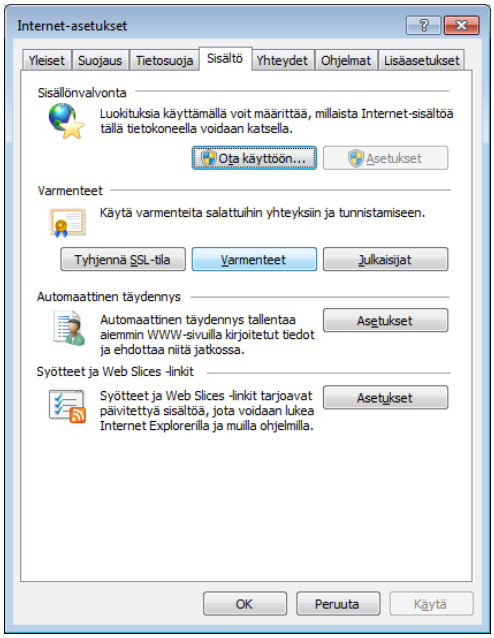
Jos vastaanottajan varmennetta ei löydy fineid hakemistosta, on varmenne saatava muulla tavoin. Käytännössä tämä vaatii sen, että vastaanottaja lähettää ensin viestin jonka liitteenä on hänen varmenteensa. Varmenteiden lähettäminen vaatii jonkin verran käsitöitä, kun varmenteet täytyy ensin paikallistaa, tallentaa tiedostoon ja muuttaa tiedosto sopivaan muotoon lähettämistä varten. Vastaanottajan on myös osattava asentaa varmenteet oman sähköpostiohjelmansa osoitekirjaan.

3.1.4. Varmenteen tallentaminen (export)

Varmennekortin ollessa lukijalaitteessa, ovat varmenteet tuotavissa tiedostoon (export). Varmenteiden tuomiseen on useita tapoja, mutta varmimmin toimiva tapa on avata selain (tässä Internet Explorer) ja sieltä internet-asetukset.

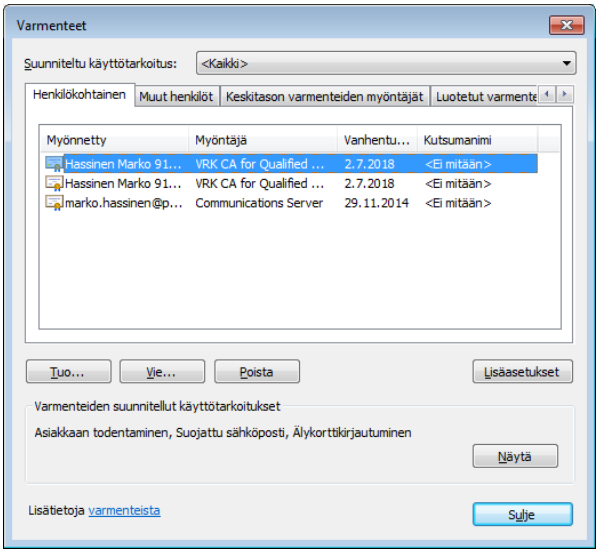


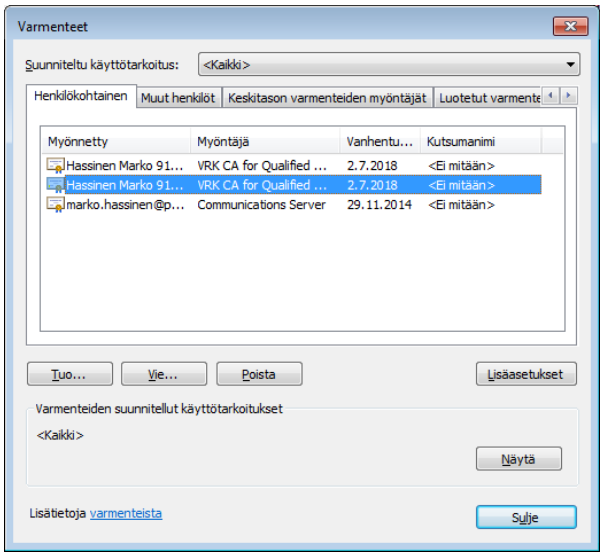
Internet-asetusten sisältö -välilehden Varmenteet -painikkeella saa esiin varmennelistauksen.



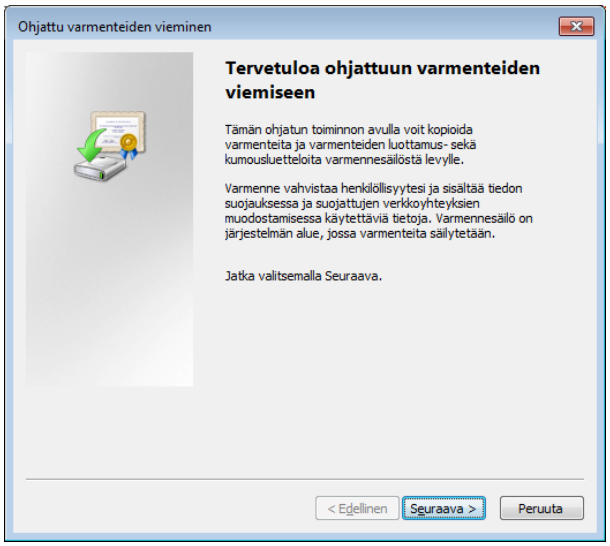
Omat varmenteet löytyvät "Henkilökohtainen" välilehdeltä. Näistä valitaan haluttu varmenne ja painetaan "Vie" -painiketta.

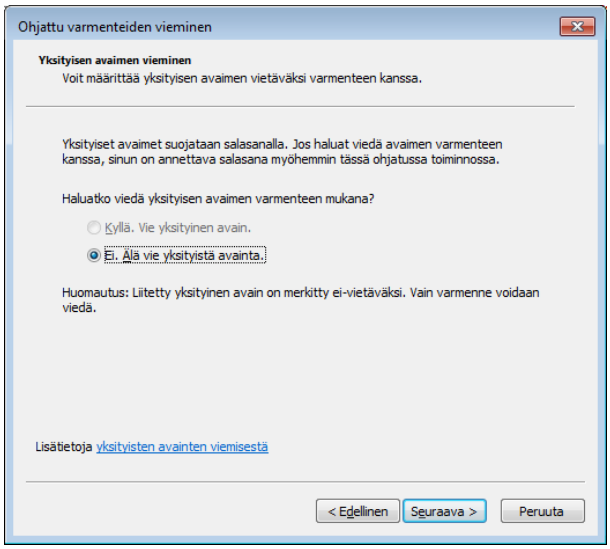
Varmenteita on kaksi (kts. alla oleva kuvat), joista molemmat on hyvä tallentaa (viedä).



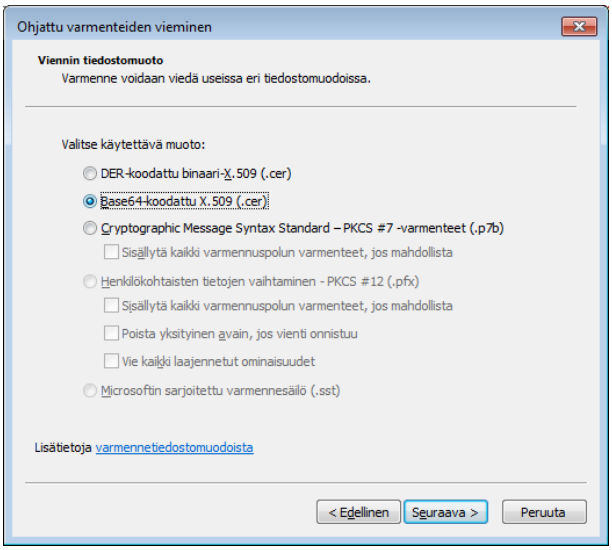


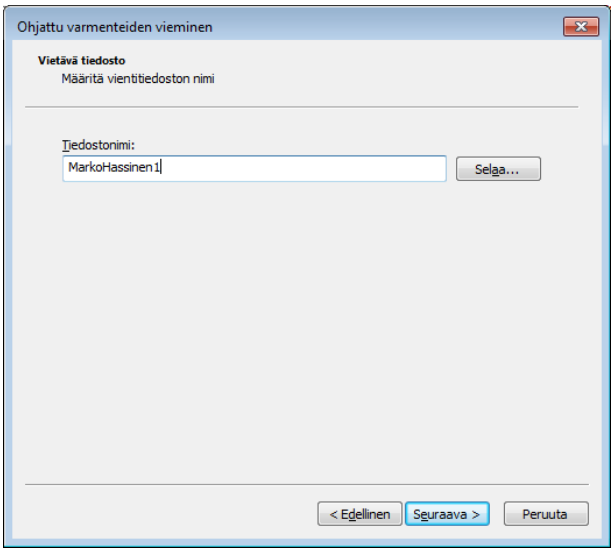
Tämä käynnistää ohjatun toiminnon, jonka kahdessa ensimmäisessä vaiheessa painetaan Seuraava painiketta (Yksityistä avainta ei voi viedä varmenteen mukana).



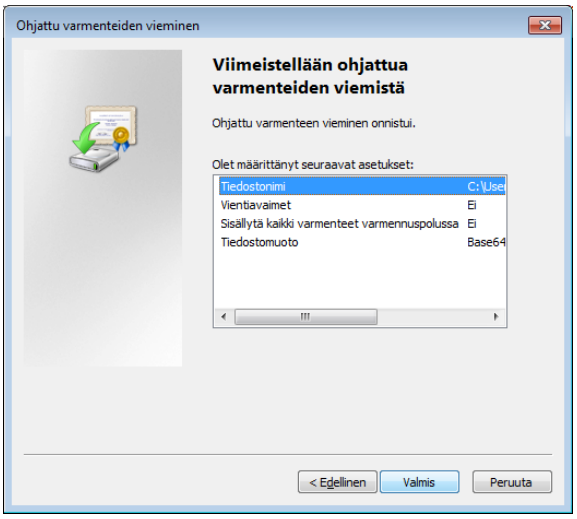


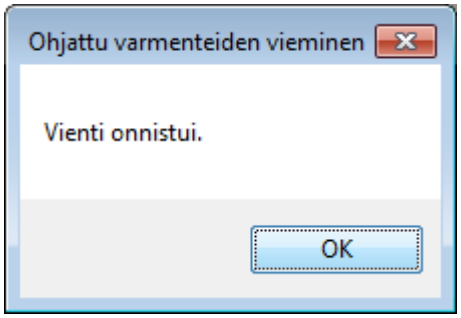
Seuraavassa vaiheessa valitaan muoto, johon varmenne tallennetaan. Jotta varmenne saadaan kulkemaan sähköpostin liitteenä, tulee valita Base64-koodattu muoto.



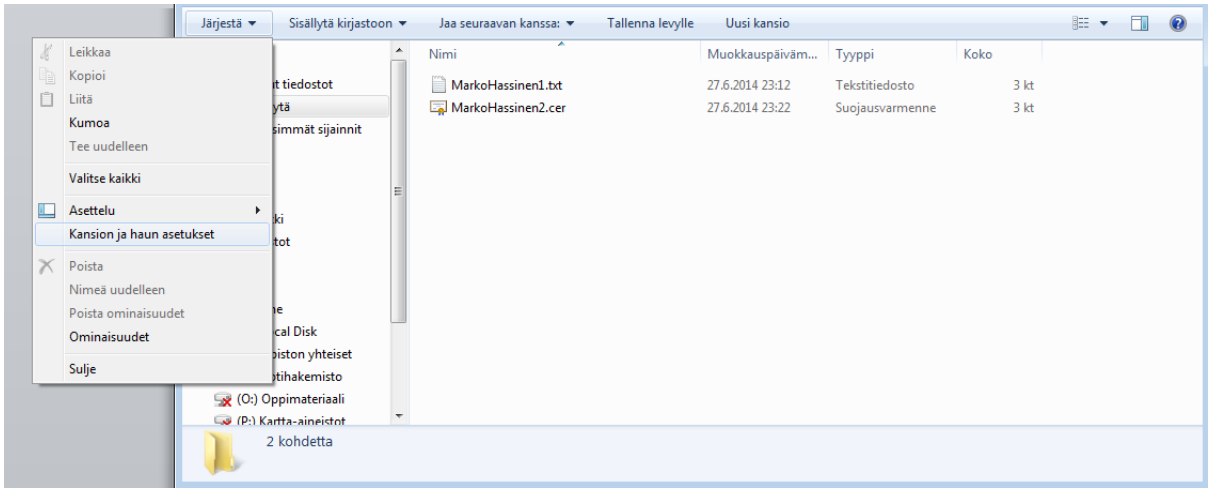


Muodon valinnan jälkeen paina Seuraava, anna tiedostolle nimi ja paina jälleen Seuraava. Lopuksi viimeisessä ikkunassa paina Valmis ja ohjattu toiminto ilmoittaa varmenteen viennin onnistumisesta.

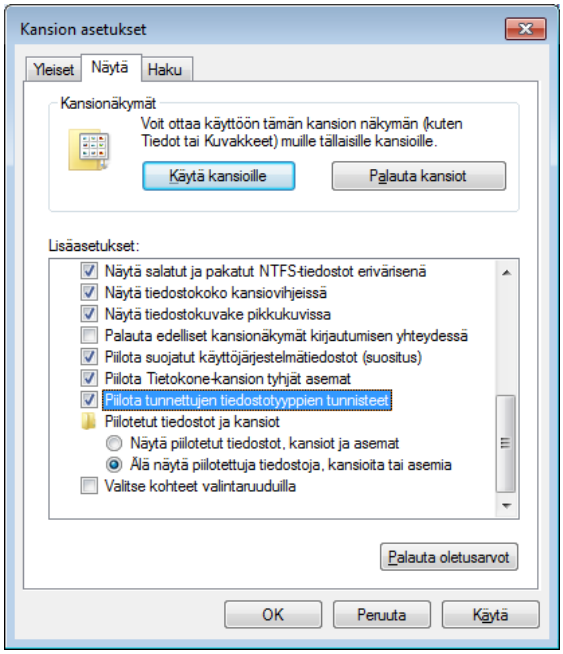




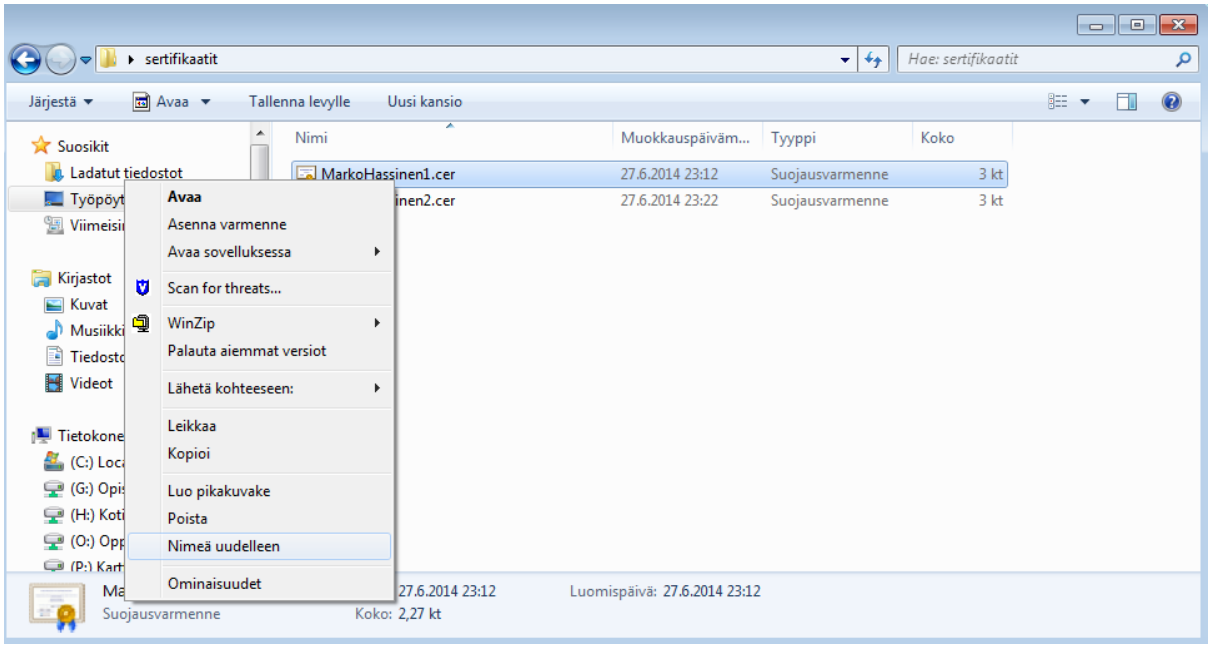
Jotta varmenteet saadaan kulkemaan Outlookin kanssa sähköpostitse, täytyy niiden tiedostopääte muuttaa .cer muodosta esimerkiksi .txt muotoon. Outlook pitää .cer päätteisiä tiedostoja tietoturvauhkana eikä suostu niitä lähettämään eikä vastaanottamaan. Base64 muoto on tekstiä, joten .txt pääte sopii tilanteeseen varsin hyvin. Tiedostopäätteen voi muuttaa vaikkapa resurssien hallinnasta, kun ensin muuttaa kansion asetukset siten että tunnettujen tiedostopäätteiden piilotus otetaan pois käytöstä. Tämä tapahtuu Windows 7:ssa siten, että valitaan Järjestä->Kansion ja haun asetukset.



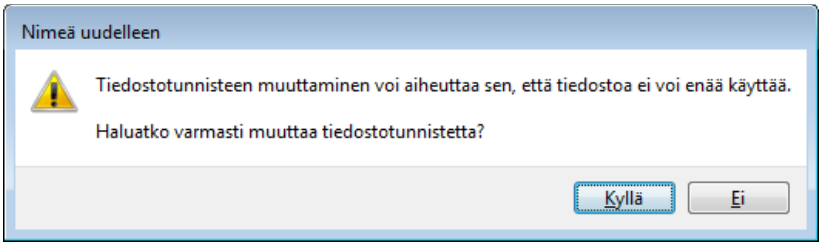
Seuraavaksi Näytä välilehdeltä poistetaan Piilota tunnettujen tiedostotyyppien tunnisteet kohdasta rasti.



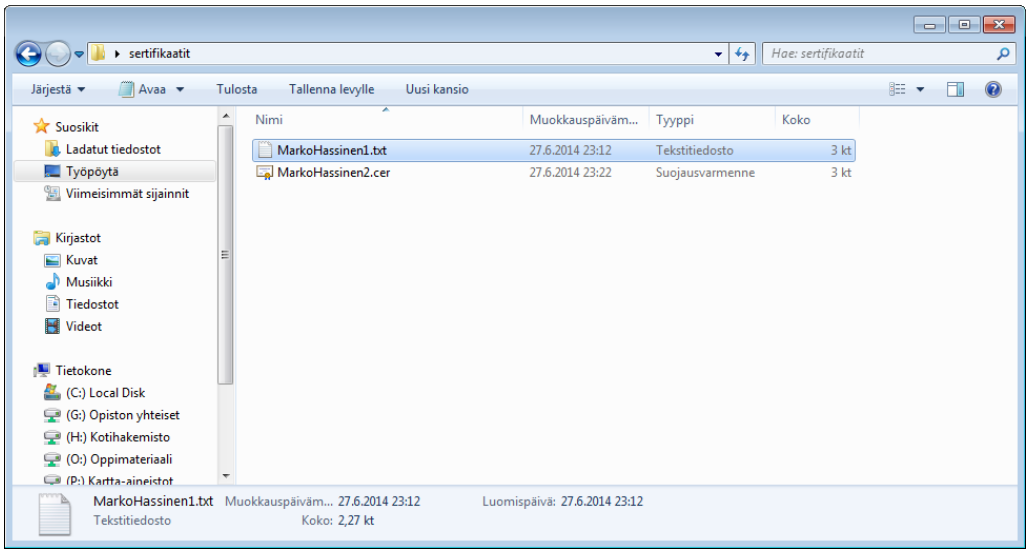
Tiedostopäätteen muuttaminen onnistuu valitsemalla tiedoston ja hiiren oikealla painikkeella avautuvasta valikosta Nimeä uudelleen.



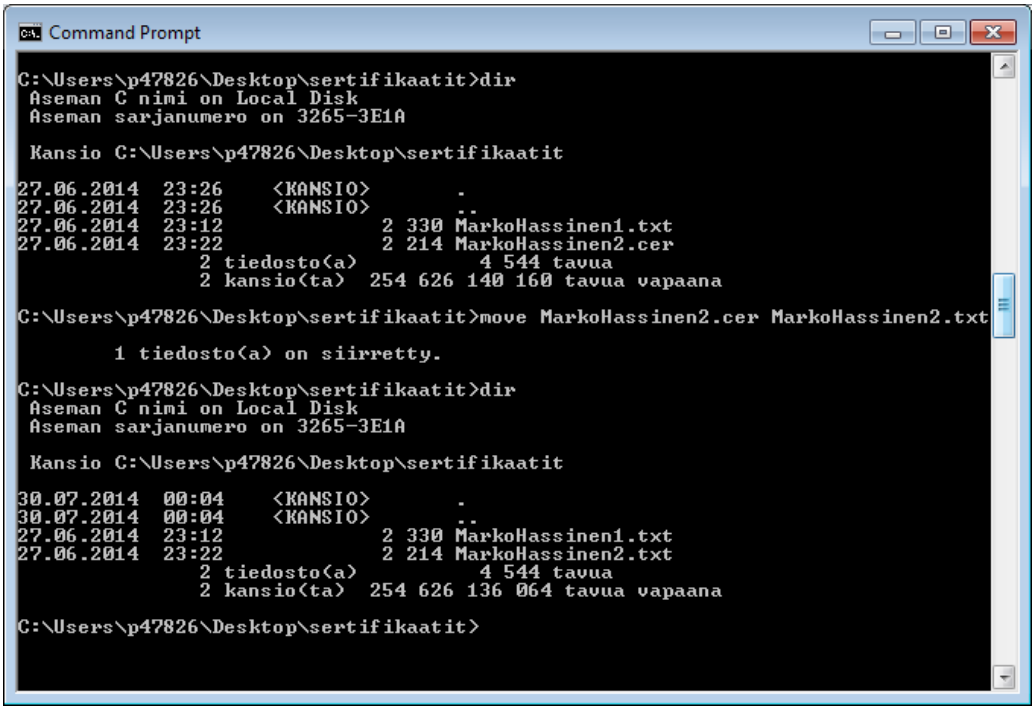
Avautuvaan dialogiin vastataan Kyllä.



Kun kaikki tarvittavat sertifikaatit ovat .txt muodossa voidaan ne lähettää normaalisti sähköpostin liitetiedostoina.



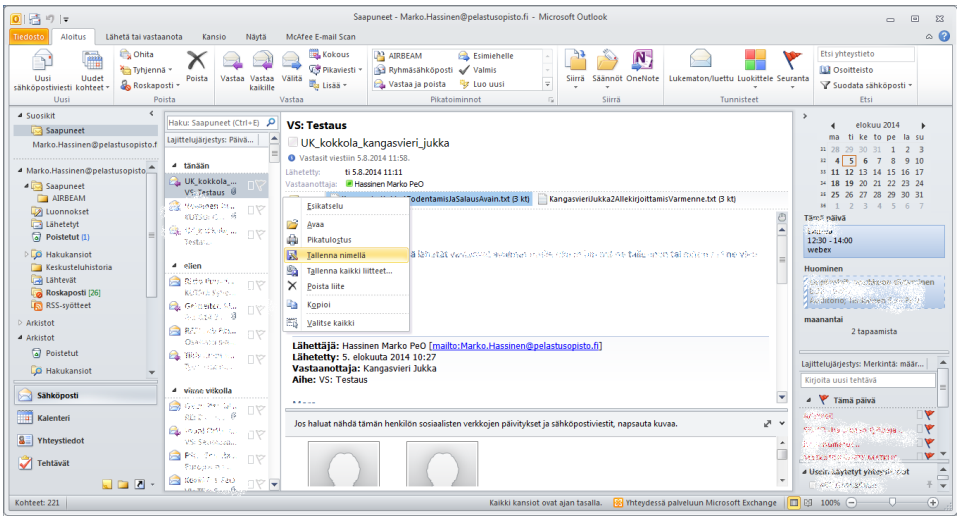
Saman nimeämismuutoksen voi toki tehdä muullakin tavalla, esimerkiksi komentokehotteesta move -komennolla:



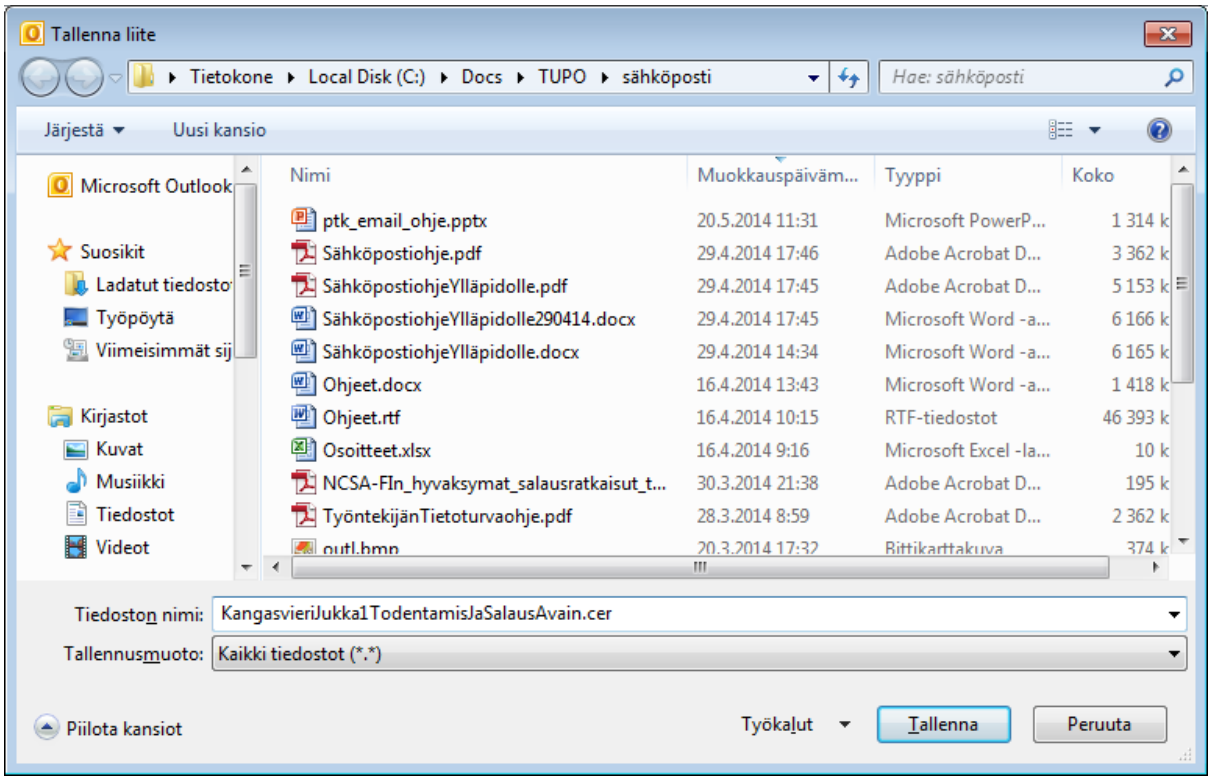
3.1.5. Varmenteen asentamien Outlookin osoitekirjaan

Edellä kuvatulla tavalla lähetetyt varmenteet voi vastaanottaja ottaa käyttöön. Prosessi on suurelta osin käänteinen edellä esitettyyn. Vastaanottaja tallentaa varmenteet omalle koneelleen, palauttaa alkuperäisen .cer tiedostopäätteen ja tuo varmenteet Outlookin osoitteistoon.

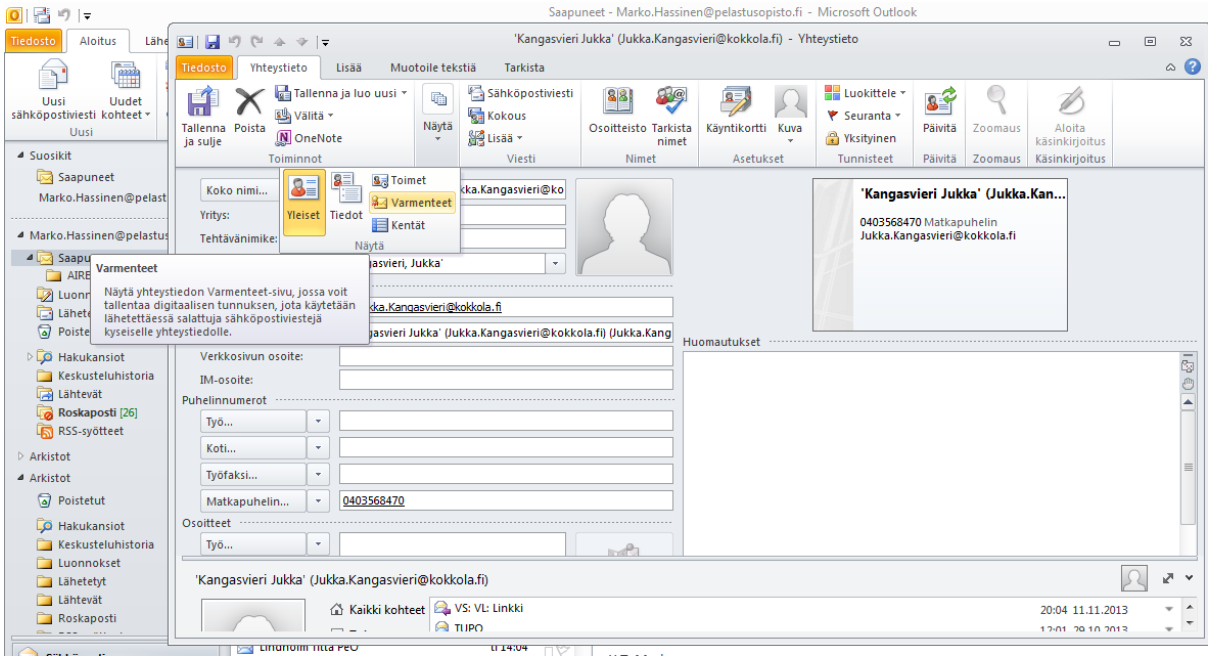
Tiedoston tallentaminen tapahtuu esim. valitsemalla liitteen ja hiiren oikealla painikkeella valinta Tallenna nimellä:



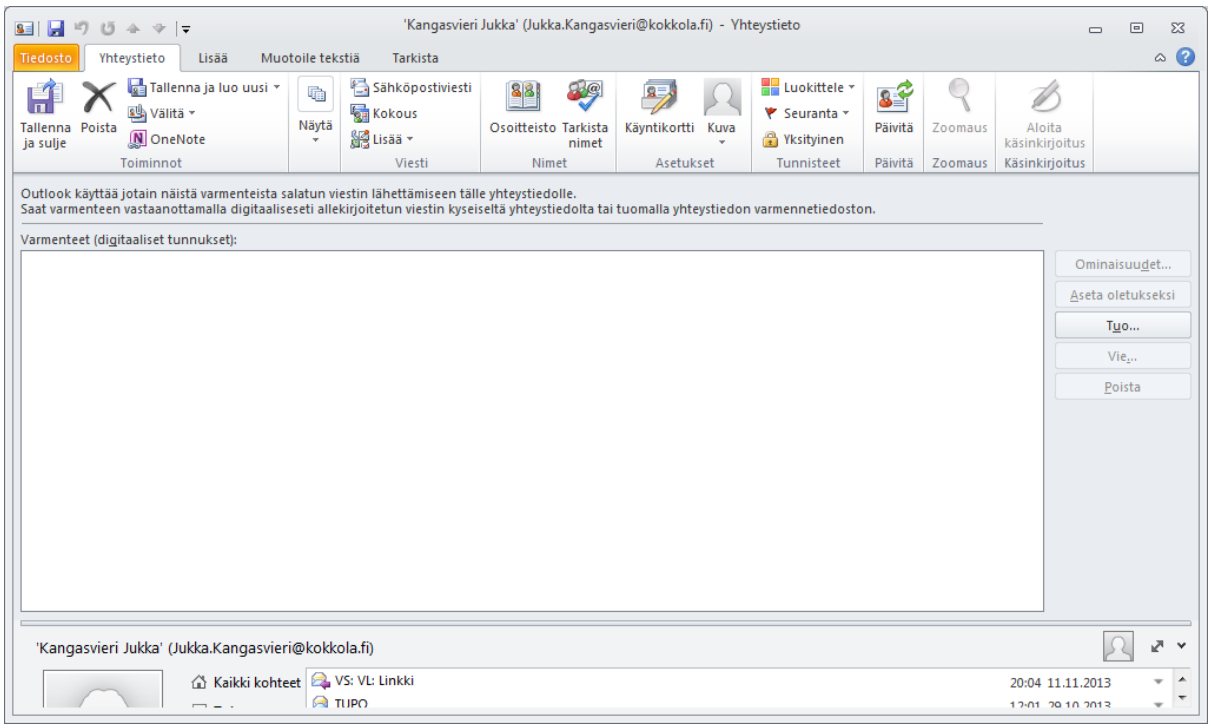
Seuraavassa vaiheessa voi tallennusdialogissa muuttaa tiedostopäätteen muotoon .cer siten, että ensin kohtaan "Tallennusmuoto" valitsee "Kaikki tiedostot" ja sitten muuttaa .txt päätteen muotoon .cer. Nyt varmennetiedosto on tuotavissa Outlookin osoitteistoon. Huomioi, että Outlookiin kannattaa tuoda vastapuolen molemmat varmenteet, jos ne ovat saatavilla.



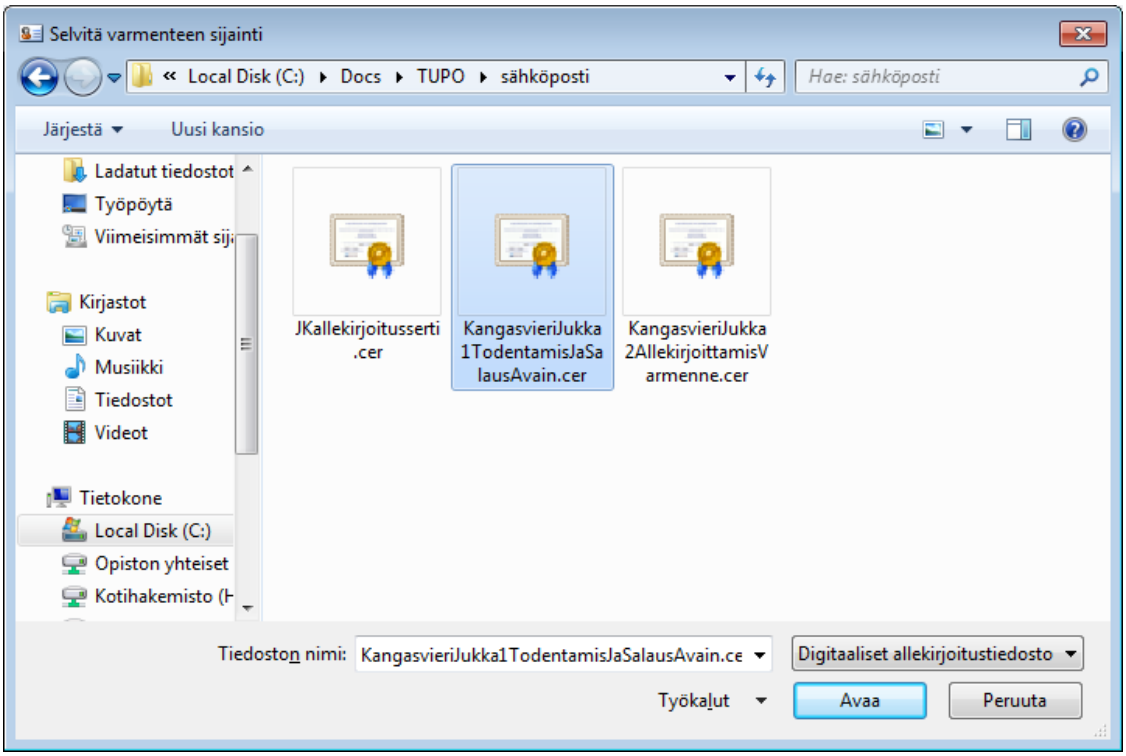
Varmenteet voidaan Outlookiin tallentaa käyttäjän yhteystietoihin. Avaa yhteystietokortti esimerkiksi osoitteistosta tuplaklikkaamalla henkilön nimeä. Mikäli henkilöä ei ole yhteystietoihin tallennettuna, valitse Yhteystiedot -> Uusi yhteystieto.



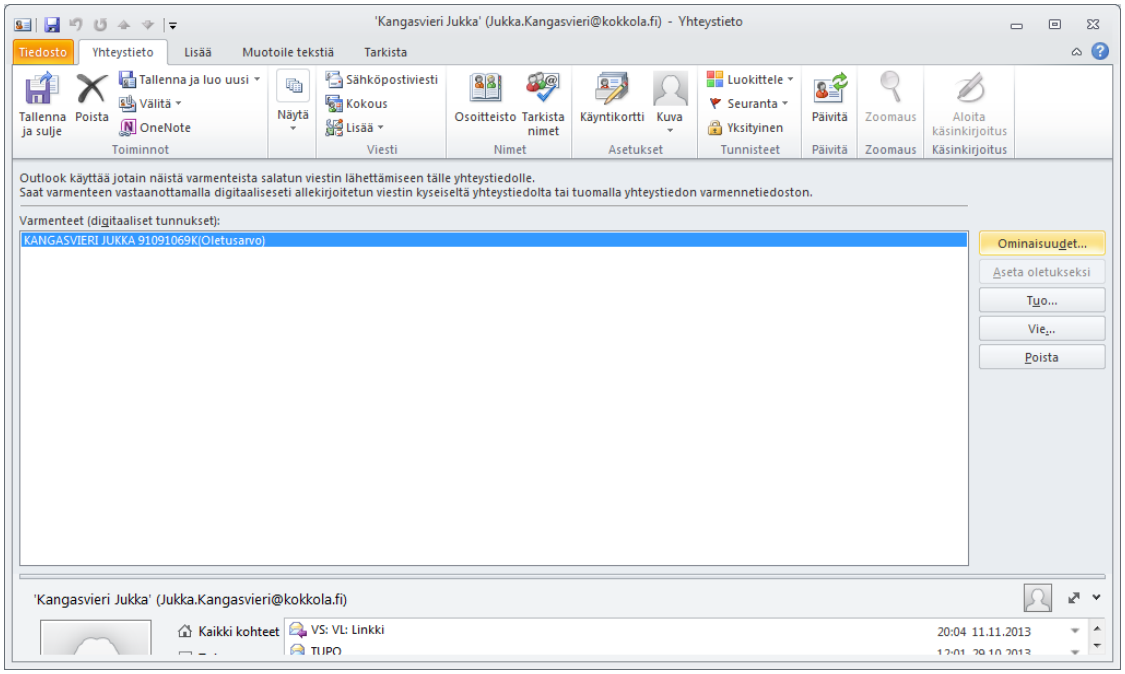
Yhteystietolomakkeelta löytyy kohta varmenteet (kts. yllä), jonne varmeteet tuodaan. Paina Tuo painiketta.



Tämän jälkeen valitse .cer päätteinen tiedosto hakemistosta jonne olet tallentanut varmenteet ja paina Avaa.

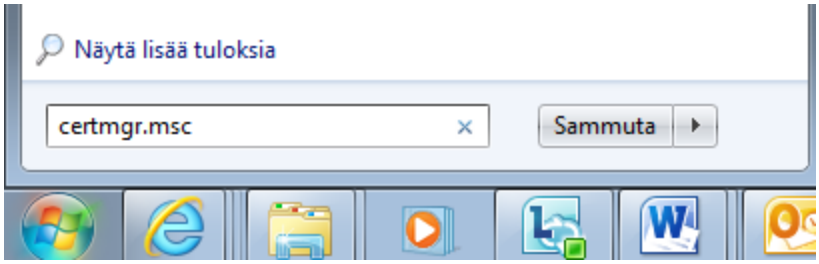


Varmenne ilmestyy varmennelistalle. Toista sama toisen varmenteen kanssa.

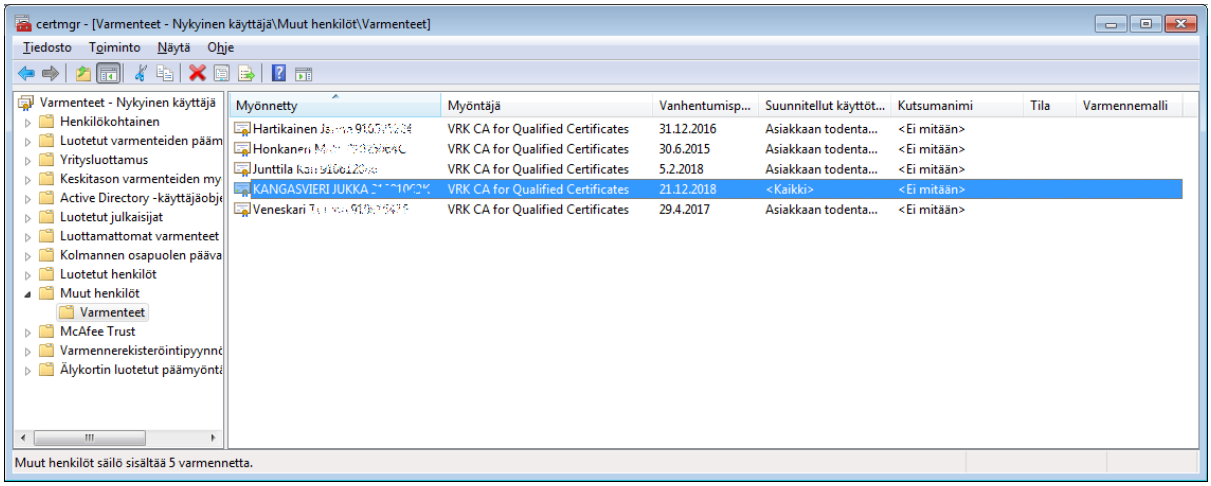


Kun molemmat varmenteet on tallennettu, paina Tallenna ja Sulje. Tämän jälkeen voit lähettää henkilölle salattuja ja allekirjoitettuja viestejä.

Varmenteita voi myös tarkastella certmgr.msc työkalulla, jolla järjestelmästä voi myös poistaa sinne tuotuja varmenteita. Työkalu käynnistyy, kun painaa Windowsin aloituspainiketta, kirjoittaa hakukenttään certmgr.msc ja painaa enter.

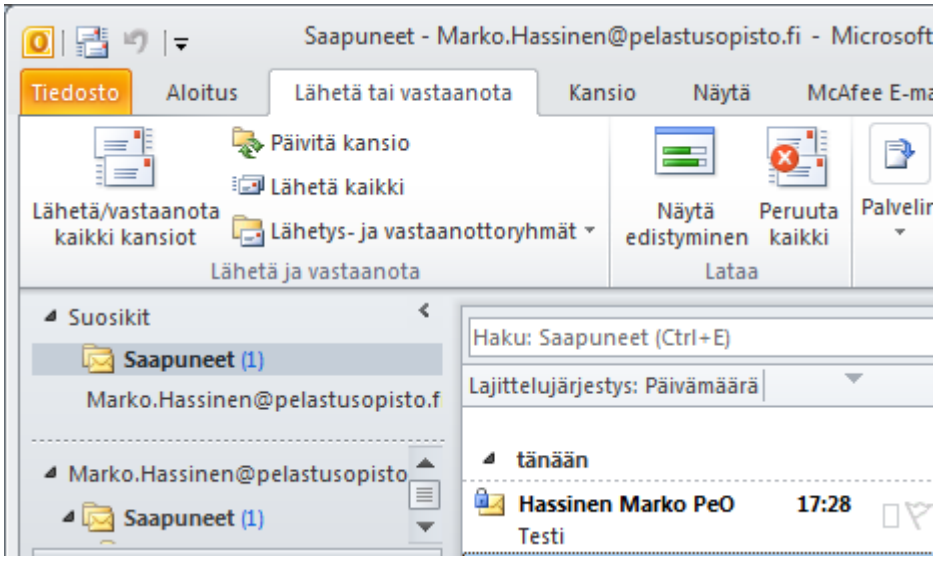


Alla olevassa kuvassa on tarpeettomia yksityiskohtia "sutattu" tarkoituksella.

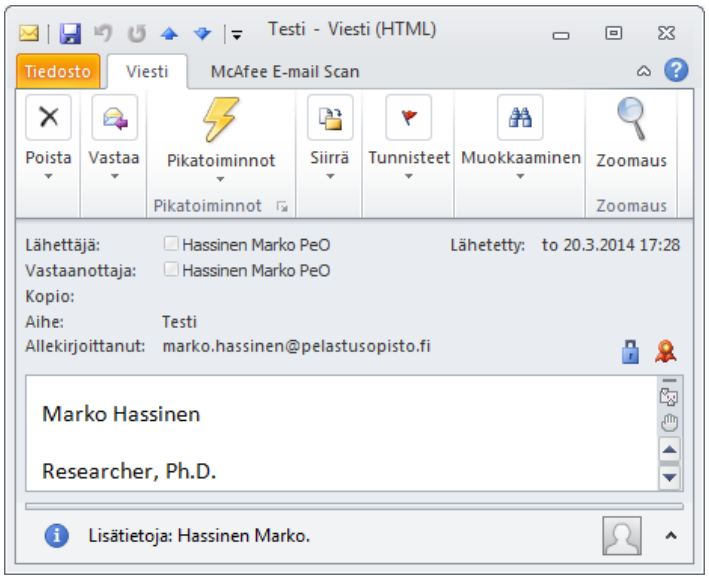


3.1.6. Salatun postin vastaanottaminen

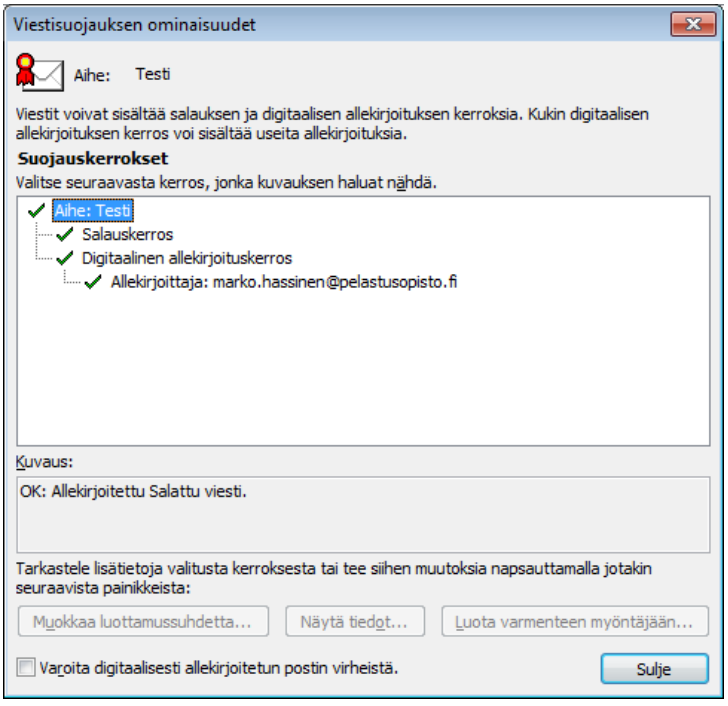
Saapuneista viesteistä salatun viestin tunnistaa kirjekuoren ja lukon kuvasta.



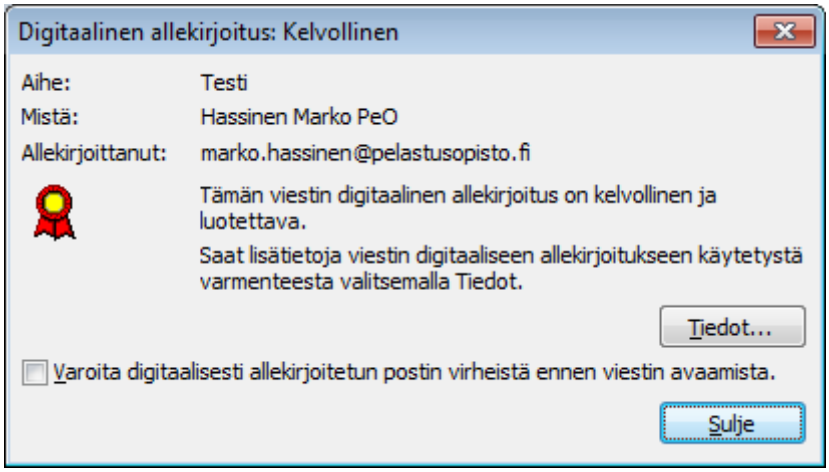
Viesti avautuu kuten salaamatonkin viesti, mikäli lähettäjän varmenne löytyy tiliasetuksissa määritellystä varmennehakemistosta.



Salauksen yksityiskohtia voi tarkastella viestissä olevasta sinisestä lukon kuvasta ja vastaavasti allekirjoitustietoja punaisesta kuvakkeesta.



Viestiin liittyvän allekirjoituksen kelvollisuutta voi tutkia tarkemmin halutessaan klikkaamalla viestin oikeasta yläkulmasta punaista kuvaketta  .

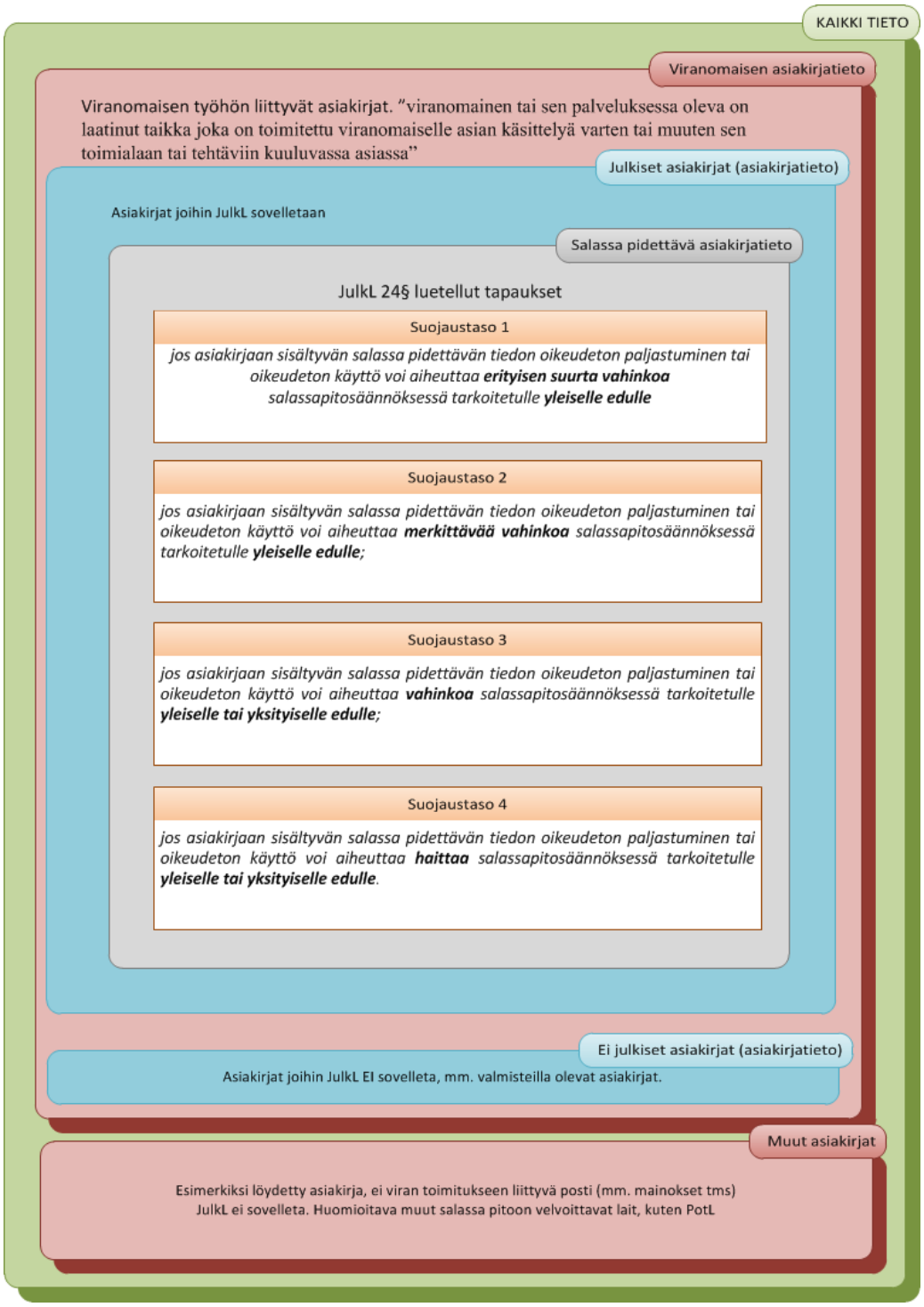


Avautuva dialogi kertoo, onko kyseinen allekirjoitus kunnossa.

4. SALASSAPITO PÄHKINÄN KUORESSA

Viranomaisen tiedot ovat lähtökohtaisesti julkisia. Laki viranomaisten toiminnan julkisuudesta määrittelee tapaukset, joissa viranomaisen tieto voi olla salassa pidettävää.

Salassa pidettävä tieto voidaan luokitella suojaustasoihin. Suojaustasomäärittely perustuu tiedon omistavan tahon arvioon tiedon oikeudettoman paljastumisen aiheuttamasta vahingosta.



Suojaustasoista lievin on ST4, jonka käsittely edellyttää ns. perustietoturvatasoa. ST4 ja ST3 tieto voidaan lähettää sähköpostilla vastaanottajalle salattuna tai muutoin suojattuna. ST2 ja ST1 tietoa ei

käytännössä voi sähköpostilla lähettää organisaatioiden välillä. ST1 ja ST2 voidaan lähettää viranomaisen verkon sisällä, tosin ST1 vain vahvasti salattuna. Tässä ohjeessa käytetty TrueCrypt on hyväksytty (ncsa.fi) tasoille ST2, ST3 ja ST4.

Salassa pidettävyyden määrittelevää lainsäädäntöä käsitellään yksityiskohtaisemmin julkaisussa "Salassa pidettävän tiedon tunnistaminen ja suojaustasoluokittelu pelastustoimessa".

5. SALASSA PIDETTÄVÄN TIEDON TALLENTAMINEN

5.1. Vastaanotetun materiaalin tallentaminen

Salassa pidettävän tiedon tallentamiseen on omassa omat vaatimuksensa. Mikäli tieto tallennetaan salatussa säiliössä samoin kuin sitä on edellä kerrotulla tavalla lähetetty, voidaan ST3 ja ST4 tason tieto tallentaa muistivälineelle (kiintolevy, siirrettävä muisti) tai viranomaisen verkon palvelimelle. ST3 tason tietoa tallennettaessa viranomaisen verkon palvelimelle, vaaditaan korotetun tietoturvallisuustason käsittely-ympäristöä.

ST2 ja ST1 tason tiedon tallentamisessa vaaditaan edellisen lisäksi vahvaa salausta ja korkean tietoturvallisuustason vaatimukset täyttävää ympäristöä. Tässä ohjeistuksessa ei kuitenkaan ole tarkoituksena ottaa kantaa ST1 ja ST2 tason vaatimuksiin, koska niiden välittämiseen sähköpostitse ei ole nähtävissä välittömiä tarpeita.

Tiedon tallentamisessa on myös otettava huomioon tiedon säilytysaikaan ja arkistointiin liittyvät säännökset, mikäli kyseessä on sellainen tieto joka viranomaisen täytyy arkistoida. Käytännössä tiedon omistaja vastaa arkistoinnista, joten toiselta viranomaiselta saadun tiedon arkistointi ei yleensä ole tarpeen. Mikäli asiasta on epäselvyyttä, varsinkin omassa organisaatiossa syntyneen tiedon osalta, on syytä tarkastaa asia organisaation arkistonmuodostussuunnitelmasta (katso kappale 4.10).

5.2. Vastaanotetun materiaalin luovuttaminen edelleen

Salassa pidettävästä materiaalista on hyvä muistaa, että salassa pidettävyyden määrittelee tiedon omistaja, joka on usein myös tiedon alun perin luonut taho. Salassa pidettävän tiedon luovuttava organisaatio on velvollinen varmistamaan, että vastaanottava taho on tietoinen tiedon käyttöön liittyvistä rajoitteista, mukaan lukien määräykset tiedon luovuttamisesta edelleen.

Pääsääntöisesti edelleen luovutus vaati tiedon omistajaorganisaation myöntymyksen. Haltuun toiselta organisaatiolta saatua salassa pidettävää tietoa ei siis saa luovuttaa kolmannelle osapuolelle ilman luovuttaja nimenomaista lupaa.

Lisäksi, vaikka lupa materiaalin luovuttamiseen olisikin, ei materiaalia saa luovuttaa ellei ole varma siitä että vastaanottaja myös tuntee materiaalin käsittelyyn liittyvät säännöt ja myös niitä noudattaa.

Sähköpostiliikenteessä tämä on syytä ottaa huomioon, ennen kuin sähköpostiviestejä edelleen lähetetään (forward).

6. LÄHTEET

ICT-varautumisen vaatimukset, VAHTI 2/2012

Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje, 30.11.2010

Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje, 10.2.2014, Ulkoasiainministeriö

KATAKRI: Kansallinen turvallisuusauditointikriteeristö. Versio II, 2011. Puolustusministeriö.

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)

Laki sähköisestä asioinnista viranomaistoiminnassa (24.1.2003/13)

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (7.8.2009/617)

Laki viranomaisten toiminnan julkisuudesta (621/1999)

Mäenpää, Olli: Julkisuusperiaate. WSOY 2008

NCSA-FI:n hyväksymät salausratkaisut. Viestintävirasto

Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010

Schneier Bruce: Applied Cryptography. 1996

Sisäasiainministeriön määräys salassa pidettävien tietoaineistojen luokittelusta ja käsittelystä, 2011

Sähköisen viestinnän tietosuojalaki (516/2004)

Teknisen ICT-ympäristön tietoturvataso-ohje. VAHTI 3/2012

Tietoturvallisuusasetus (681/2010)

Tunnistaminen julkishallinnon verkkopalveluissa, VAHTI 12/2006

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (TiTuA 681/2010)

Viestintävirasto, Kansallinen tietoturvaviranomainen NCSA-FI