Pelastusopisto

D-sarja:
Muut julkaisut
[4/2014]

Salassa pidettävän tiedon välittäminen sähköpostitse pelastustoimessa suojaustasolla IV
Ylläpidon ohjeistus

Marko Hassinen

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

Pelastusopiston julkaisu

D-Sarja: Muut julkaisut

4/2014

ISBN: 978-952-5905-47-2 (pdf)

ISSN: 1795-9187

PELASTUSOPISTO

Salassa pidettävän tiedon välittäminen sähköpostitse pelastustoimessa suojaustasolla IV

Ylläpidon ohjeistus

Hassinen Marko, FT, Pelastusopisto

Toimintaohje 30 sivua, 1 liite

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.

Loppukäyttäjälle suunnatussa erillisessä ohjeistuksessa yksityiskohtaisesti ohjeistetaan miten salassa pidettävä materiaali voidaan turvallisesti lähettää sähköpostilla ja miten vastaanotettua materiaalia tulee käsitellä. Tämä ohjeistus antaa valmiudet tuottaa loppukäyttäjälle vaaditun mukainen tekninen ympäristö.

Tämä ohjeistus keskittyy 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.

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. Sähköisen allekirjoituksen ja salauksen avulla saadaan toteutettua kaikki mainitut kolme tietoturvan perusominaisuutta.

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).

Tämä ohjeistus pyrkii antamaan yksityiskohtaisen kuvan salassa pidettävän tiedon sähköpostikommunikoinnissa tarvittavan ohjelmiston sekä käyttöympäristön asentamisesta ja määritysten tekemisestä.

2. TYÖASEMAYMPÄRISTÖN VAATIMUKSET

Tahot, jotka eivät voi käyttää toimikorttia salassa pidettävän tiedon välittämiseen, voivat käyttää Viestintäviraston hyväksymää TrueCrypt ohjelmaa (versiot 7.0, 7.1 ja 7.1a). Asennusohje Windows käyttöjärjestelmille löytyy kappaleesta 3, suomenkielisen kielipaketin asennusohje kappaleesta 4 ja asennusohje MAC käyttöjärjestelmille on myös saatavilla (sähköpostitse marko.hassinen@pelastusopisto.fi). Huomaa, että ohjeessa esitetyt minimivaatimukset koskevat vain suojaustason 4 tiedon lähettämistä ja vastaanottamista, suojaustasolle 3 on erillisiä vaatimuksia.

2.1. Laitteistolle asetetut vaatimukset

True Crypt sovellusta käytettäessä materiaali on työasemassa selväkielisenä silloin kun säiliö (taltio) johon materiaali on tallennettu, on avoin. Näin ollen työasemaympäristön täytyy täyttää tietyt yleiset kriteerit, sekä materiaalin suojaustasoa vastaavat kriteerit. Alustana toimivalle laitteistolle, suojaustasosta riippumatta, on asetettu seuraavat vaatimukset (nsca.fi):

1. Käytettävän työaseman suojaustason tulee olla käsiteltävän tiedon mukainen, huomioiden että osion ollessa käytössä (mounted), tiedostot ovat salaamattomia.
2. Käytettävällä laitteella ei saa olla ns. kulutuksentasausominaisuutta (wear-level)
3. Windows-käyttöjärjestelmässä ei saa käyttää hibernaatiota.
4. On käytössä jokin menetelmä alustan eheyden (muuttumattomuuden) varmistamiseen.

Seuraavissa kappaleissa tarkastellaan tarkemmin näitä vaatimuksia ja niiden toteuttamistapoja ja kappaleessa 2.4 on suositukset tavoista joilla kriteerit helpoiten täytetään. Ainakin kappale 2.4 kannattaa lukea **ennen kuin mitään asennuksia/asetuksia tehdään.**

2.1. Käytettävän työaseman suojaustaso

Käsiteltäessä salassa pidettävää, suojaustasoluokiteltua tietoa, tulee käytettävän työaseman (ja sen ylläpitotoiminnan) täyttää käytettävän suojaustason mukaiset vaatimukset. ST4 tietoa käsiteltäessä, työaseman tulee olla ST4 vaatimusten mukainen ympäristö. Vaatimukset työaseman tietoturvamekanismeista sekä työaseman ylläpitotoimista löytyvät kansallisesta turvallisuusauditointikriteeristöstä (KATAKRI). Kattava ohjeistus ympäristöjen ja toiminnan saattamisesta ST4 tasolle on liian laaja tähän ohjeistukseen liitettäväksi.

2.2. Kulutuksentasausominaisuus

Kulutuksentasaus on yleinen tapa pidentää lähinnä EEPROM teknologiaan (Flash, SSD) perustuvien muistien käyttöikää. Koska tällainen muisti kestää rajallisen määrän luku/kirjoitusoperaatioita, kulutuksen tasauksella pyritään käyttöä hajauttamaan mahdollisimman tasaisesti koko muistialueelle.

Kulutuksen tasaus aiheuttaa riskin kun tietoja päivitetään muistille. Vanhoja tietoja ei välttämättä ylikirjoiteta, vaan uusi tieto saatetaan kirjoittaa toiseen muistin kohtaan vanhan jäädessä oleilemaan

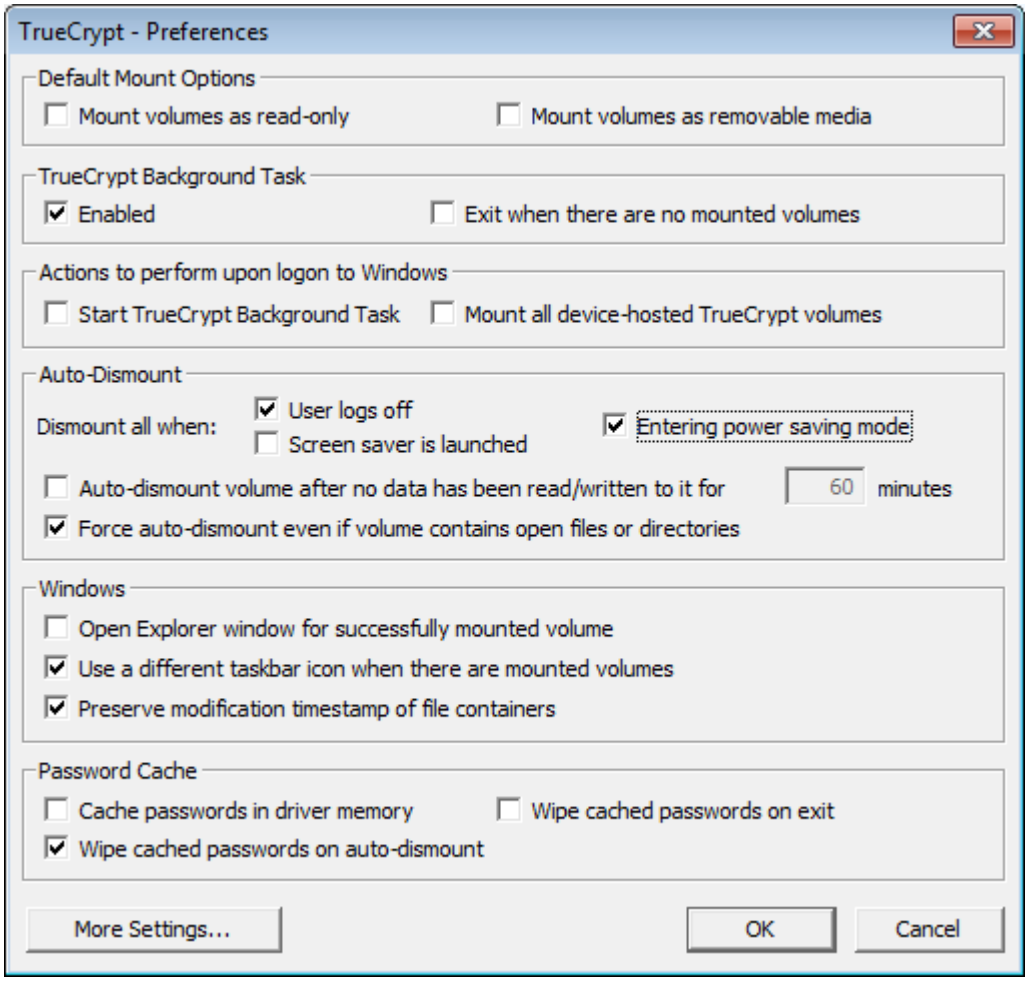
muistiin. Erityisen ongelmalliseksi tämä muodostuu osion (taltion) otsikkotietojen osalta, jos aiempi salasana on vaarantunut ja vaihdettu uuteen. Vanhan otsikon ja salasanan avulla taltion tietoihin pääsee käsiksi vaikka salasana olisi vaihdettu.

Edellä kuvatuin perustein sellaisten muistien, jotka käyttävät kulutuksen tasausta, käyttö TrueCrypt sovelluksen kanssa aiheuttaa tietoturvariskin. Selkeästi tällä on vaikutusta siirrettävien muistien (usb "tikkujen") käyttöön. Tällainen muistiväline on syytä luotettavasti salata vaikka taltio itsessään onkin salattu.

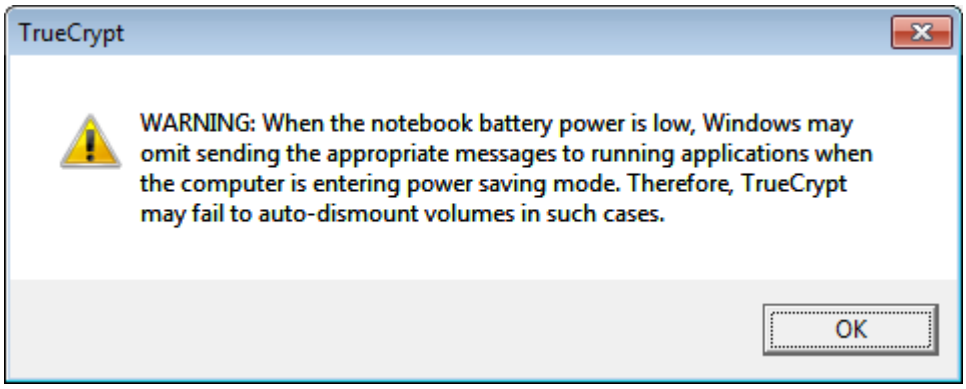
2.3. Hibernaatio (horrostila)

Windowsin hibernaatio (horrostila) toiminne saattaa altistaa tietoturvauhkalle. Hibernoituessaan kone tallentaa RAM muistin tilan hibernaatiotiedostoon, jolloin mm. True Cryptin käyttämät salasanat saattavat tallentua selväkielisenä (kuten myös mm. avoimena olevien tekstitiedostojen sisällöt jne.).

TC voidaan asettaa purkamaan (dismount) kaikkien avoimien osioiden (taltioiden) yhteydet horrostilaan mentäessä valinnalla Settings->Preferences (Asetukset->Ominaisuudet) rastittamalla kohdan Entering power saving mode (Siirryttäessä Virransäästötilaan) kohdasta Auto-Dismount (Automaattinen-yhteyden Poisto). Kuva alla.



Valinta antaa lisätietoikkunan (alla) jossa kerrotaan että tämä toiminne ei ole täysin varma kaikissa olosuhteissa. Lisäksi on syytä huomata, että esimerkiksi tekstinkäsittelyohjelmassa avoinna oleva salassa pidettävää tietoa sisältävä dokumentti jää edelleen selväkieliseen muotoon.



Toinen, ja varmempi vaihtoehto on poistaa hibernaatio (horrostila) kokonaan pois käytöstä. Ohjeet tämän tekemiseen löytyvät mm. Microsoftin sivuilta (http://support.microsoft.com/kb/920730):

Jos haluat poistaa horrostilan käytöstä, toimi seuraavasti:
1. Napsauta Käynnistä-painiketta ja kirjoita Aloita haku -ruutuun kom.
2. Napsauta haun tulosten luettelossa hiiren kakkospainikkeella Komentorivi-kohdetta ja valitse sitten Suorita järjestelmänvalvojana.
3. Kun Käyttäjätilien valvonnan kehote tulee näyttöön, valitse Jatka.
4. Kirjoita komentokehotteeseen powercfg.exe /hibernate off ja paina sitten ENTER-näppäintä.
5. Kirjoita exit ja sulje komentokehoteikkuna painamalla sitten ENTER-näppäintä.

Kolmas, ja ehkä suositeltavin ratkaisu on levysalaus, jossa luotettavalla salausmenetelmällä salataan levykapasiteetti kokonaisuudessaan (FDE, Full Disk Encryption). Kiintolevyn salaamiseen voidaan käyttää mm. käyttöjärjestelmän asennusvaiheessa tarjolla olevaa salausmenetelmää. Myös True Crypt on luvallinen salaustuote kiintolevyn salaamisessa (https://www.viestintavirasto.fi/attachments/NCSA-FIn_hyvaksymat_salausratkaisut_turvaluokitellulle_tiedolle.pdf).

Suositeltavin tapa Windows 7 ja 8 alustoilla on käyttää BitLocker tuotetta, yksityiskohdat seuraavassa kappaleessa.

2.4. Suositukset

Windows 7 ja 8 alustoilla voidaan parilla verraten yksinkertaisella operaatiolla toteuttaa yllä mainitut vaatimukset. Sinällään näillä toimenpiteillä ei kirjaimellisesti toteuteta annettuja vaatimuksia, vaan tuotetaan vastaavat suojaustoimet ja suojataan samat asiat kuin mitä alkuperäisillä vaatimuksilla on ajateltu.

Hibernaation ja kulutuksen tasauksen ongelmat voidaan poistaa luotettavalla levysalauksella. Windows maailmassa BitLocker niminen tuote toteuttaa levyn salauksen. Salauksessa tarvitaan luonnollisesti avain, jonka käyttäjä syöttää koneen käynnistyessä. Tämä ei ole käytettävyyden kannalta erityisen kätevää, mutta jos koneesta löytyy ns. luotettu alusta, TPM (Trusted Platform Module), voidaan avain (ja avaimet yleensäkin) tallentaa tälle alustalle. Tällä tavoin kone käynnistyessään pyytää avaimen alustalta eikä käyttäjän tarvitse sitä muistaa. TPM on erillinen piiri, jota ei onnistuneesti (hyökkäysmielessä) voi siirtää toisen koneeseen, joten salatun levyn siirto toiseen koneeseen ei auta hyökkääjää.

TPM käyttöönotto ja konfigurointi tapahtuu erillisestä hallintaohjelmasta, jonka voi käynnistää komentokehotteesta komennolla "tpm.msc". TPM moduulin käyttöön otto ja levyn BitLocker -salauksen ohjeet löytyvät liitteestä 1.

On hyvä huomata, että BitLocker toteuttaa myös neljännen annetuista vaatimuksista, eli se valvoo tietokoneen käyttöjärjestelmäasennuksen eheyttä. Suora lainaus Windows 7 ohjeesta: *"Jos salaat käyttöjärjestelmäaseman, BitLocker etsii tietokoneesta käynnistyksen aikana tilanteita, jotka voivat aiheuttaa tietoturvariskin (kuten BIOSiin tai käynnistystiedostoihin tehtyjä muutoksia). Jos havaitaan mahdollinen tietoturvariski, BitLocker lukitsee käyttöjärjestelmäaseman ja edellyttää erityistä BitLocker-palautusavainta, jotta aseman lukitus voidaan avata. Varmista, että luot palautusavaimen, kun otat BitLocker-salauksen käyttöön ensimmäisen kerran".*

2.5. Salasanavaatimukset

Suojaustasolla ST4 salasanan täytyy olla minimissään 21 merkkiä pitkä, alfanumeerisia merkkejä sisältävä, mahdollisimman satunnaiselta vaikuttava merkkijono. Salasanaa ei saa lähettää vastaanottajalle salaamattomalla sähköpostilla tai matkapuhelimella, vaan salasanan vaihdon tulee tapahtua kasvokkain tai muulla vastaavalle suojaustasolle hyväksytyllä menetelmällä. Tarkemmat ohjeet salasanan välittämisestä toiselle osapuolelle löytyvät loppukäyttäjän ohjeesta.

2.6. Toimikorttia käyttävät tahot

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

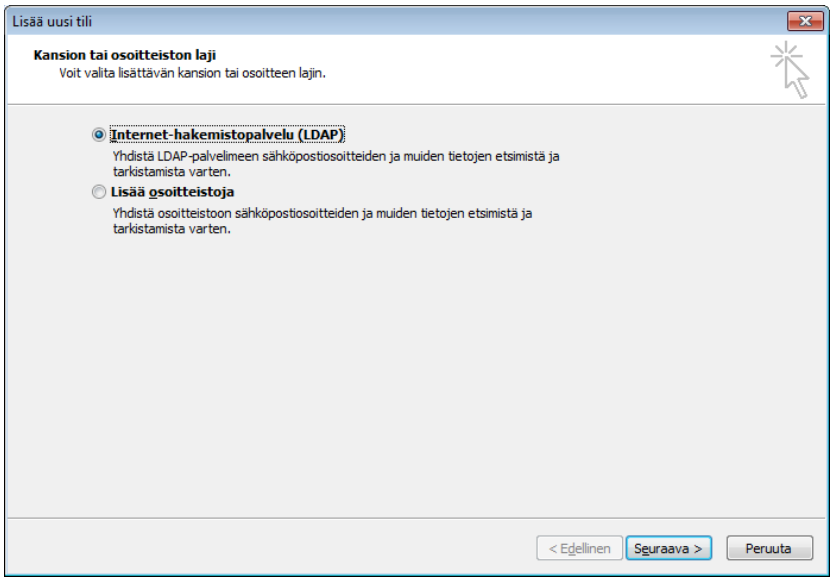
on luotettavan tahon myöntämä, voidaan myös olla suhteellisen varmoja että kyseisellä käyttäjällä (ja vain hänellä) on hallussaan julkiseen avaimeen liittyvä salainen avain.

Varmenteet tallennetaan varmennehakemistoon. Jotta varmennetta vastaavan salaisen avaimen haltijalle (henkilö, jolle varmenne on myönnetty) voidaan lähettää salattu ja 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.

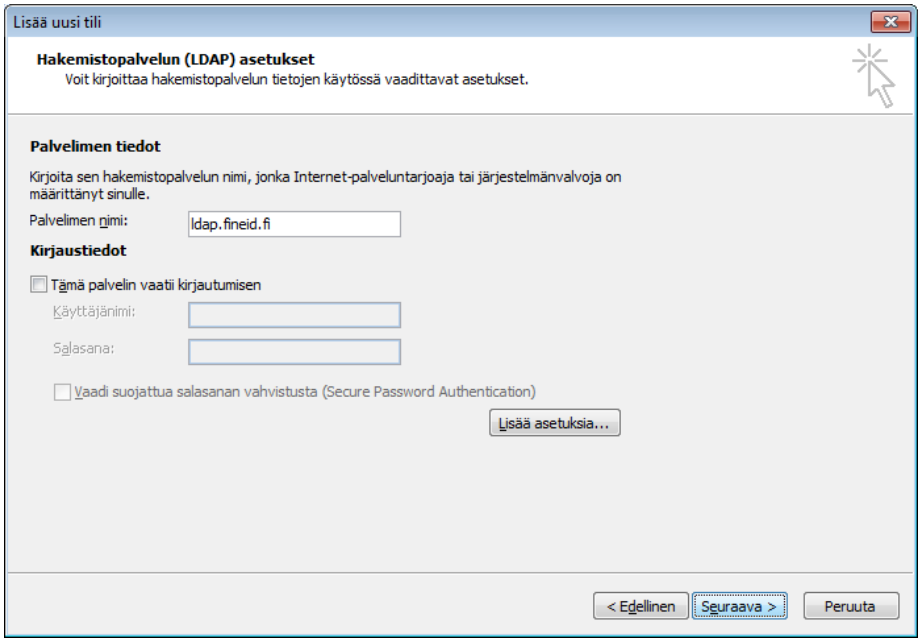
2.6.1. Outlook asetukset

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.

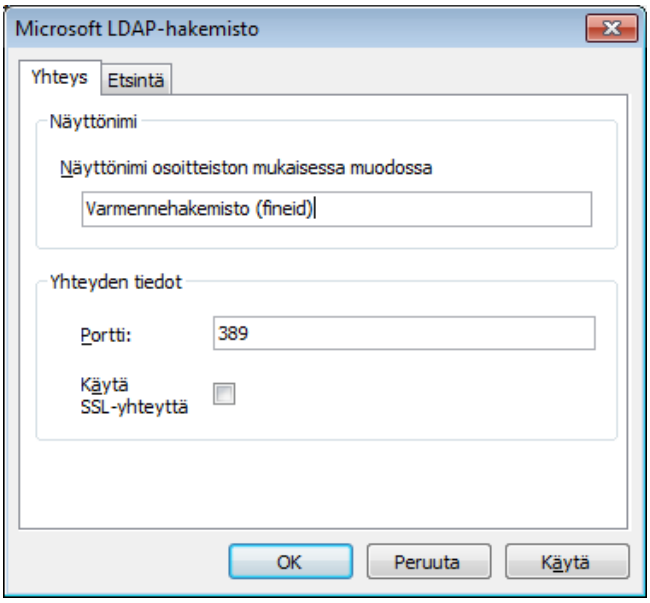
Varmennehakemisto lisätään (ellei sitä jo ole asetettu) Uusi… -painikkeella.



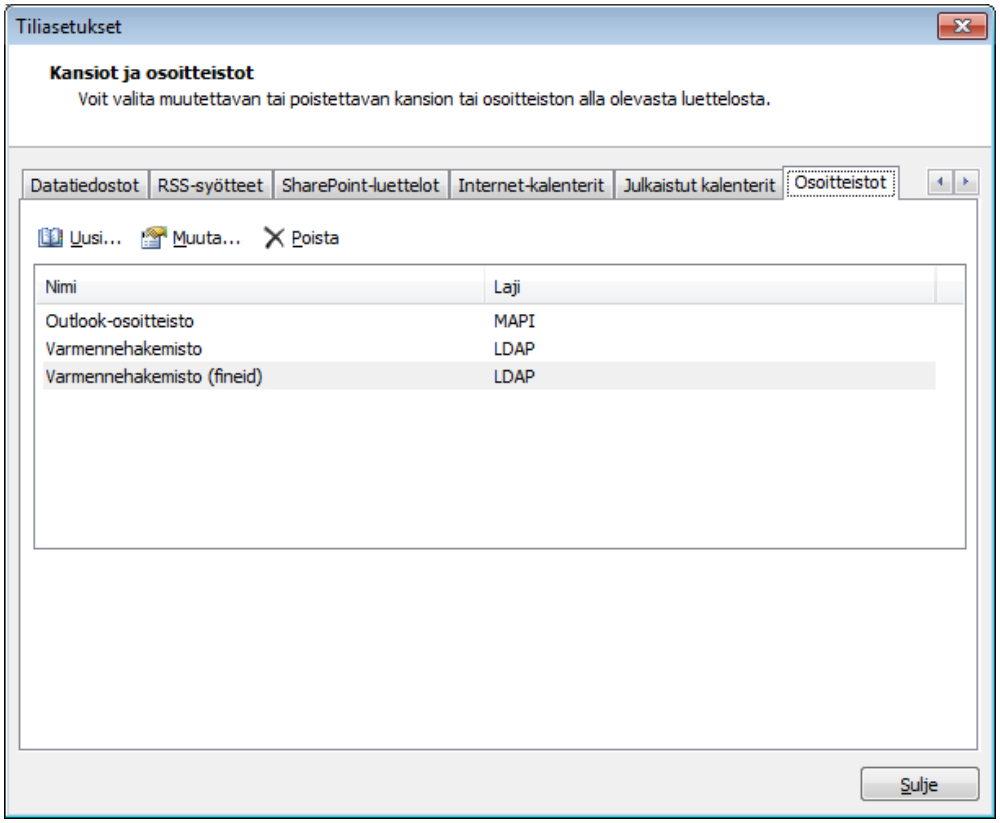
Sopiva valinta avautuvassa ruudussa on Internet-hakemistopalvelu (LDAP). Seuraavaksi annetaan varmennepalvelimen nimi, Väestörekisterikeskuksen kyseessä ollessa ldap.fineid.fi.



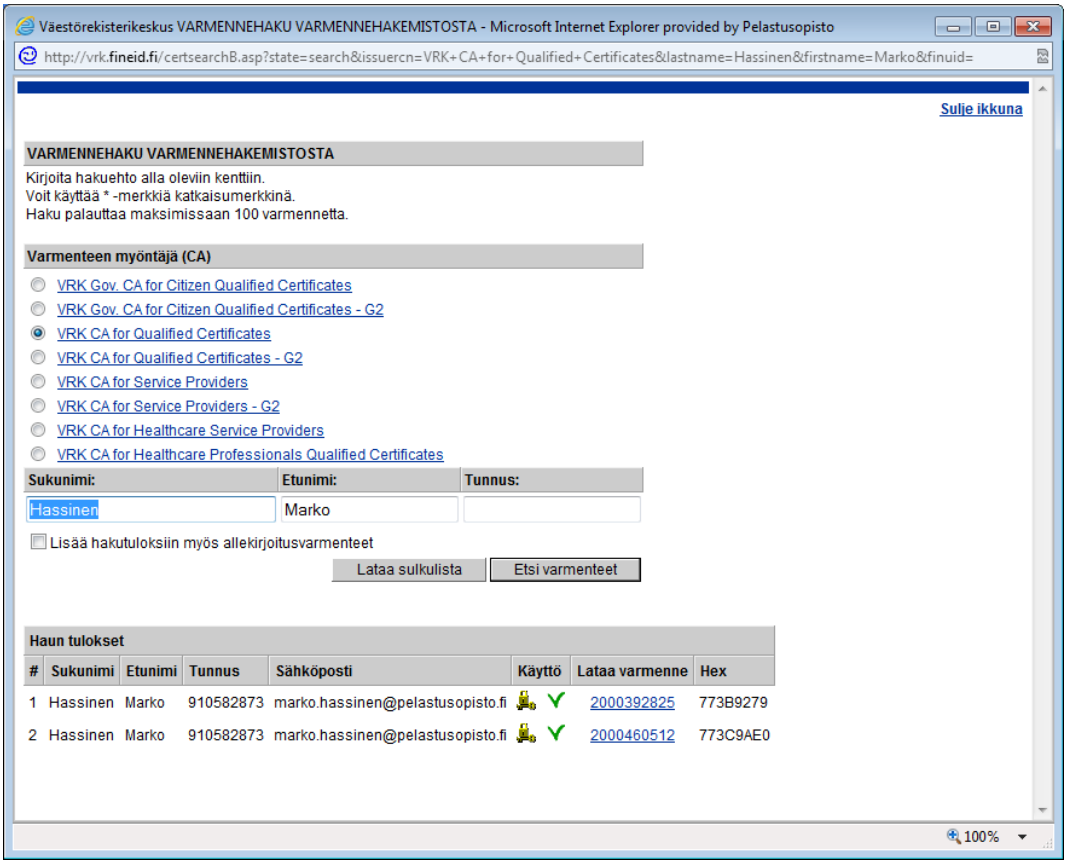
Lisää asetuksia -painikkeella hakemistolle voi mm. antaa haluamansa nimen:



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



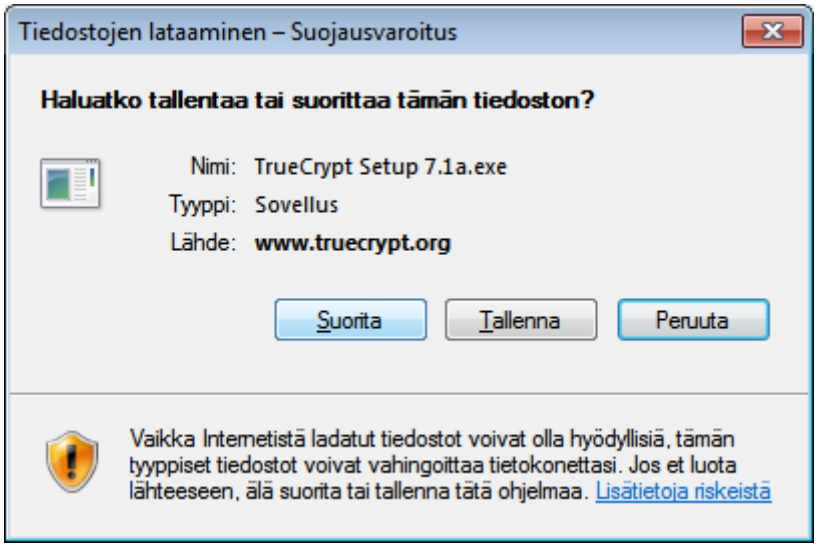
Yksittäisiä varmenteita voi hakea VRK:n sivulta, osoitteesta [http://vrk.fineid.fi/certsearchB.asp.](http://vrk.fineid.fi/certsearchB.asp)



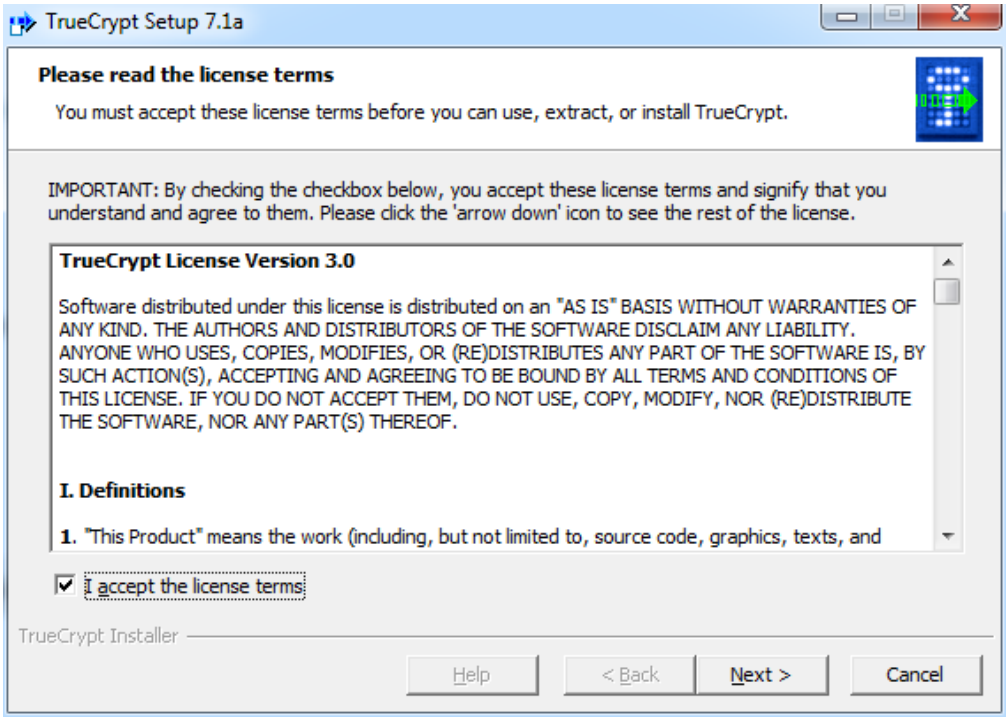
Organisaatiovarmenteet löytyvät listalta VRK CA for Qualified Certificates.

3. TRUECRYPT ASENNUSOHJE WINDOWS KÄYTTÖJÄRJESTELMILLE

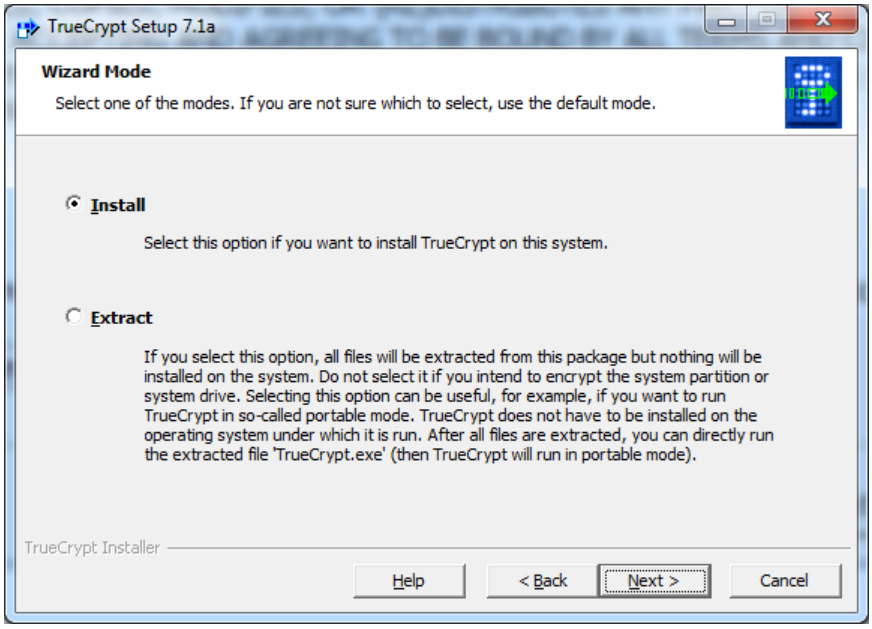
Asennuspaketti on ladattavissa osoitteesta: http://www.unicta.fi/truecrypt/. Internetistä ladatulla versiolla voidaan käsitellä ST4 tasolle luokiteltua tietoa, ST3 taso vaatii erillisiä toimenpiteitä. Asennuspaketti on suoritettava tiedosto, joka käynnistyy latausikkunan Suorita painikkeella tai tallennettua tiedostoa tuplaklikkaamalla.



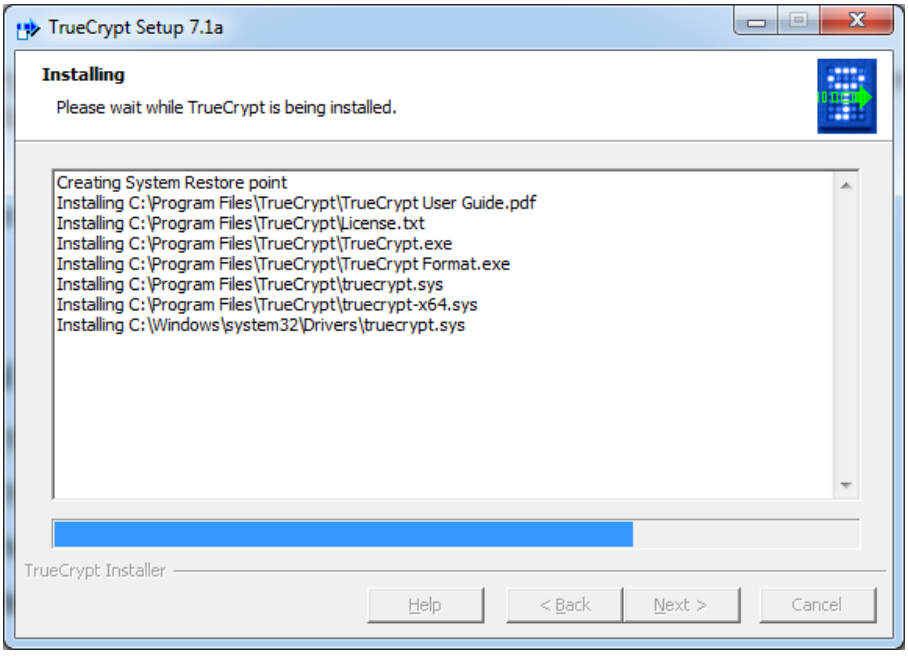
Asennuksen ensimmäinen vaihe on lisenssiehtojen hyväksyminen, paina Next.



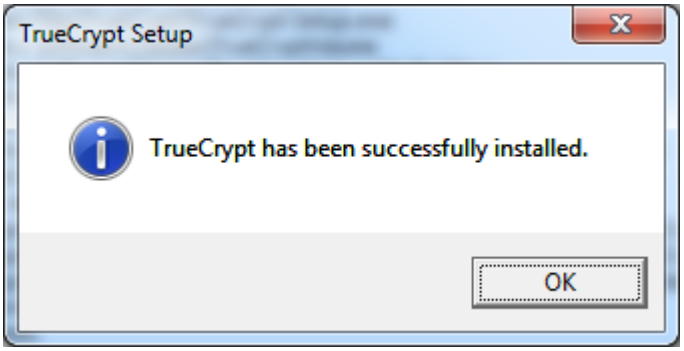
Seuraavassa ikkunassa valitaan asennustyyppi, Install on sopiva valinta, paina Next.



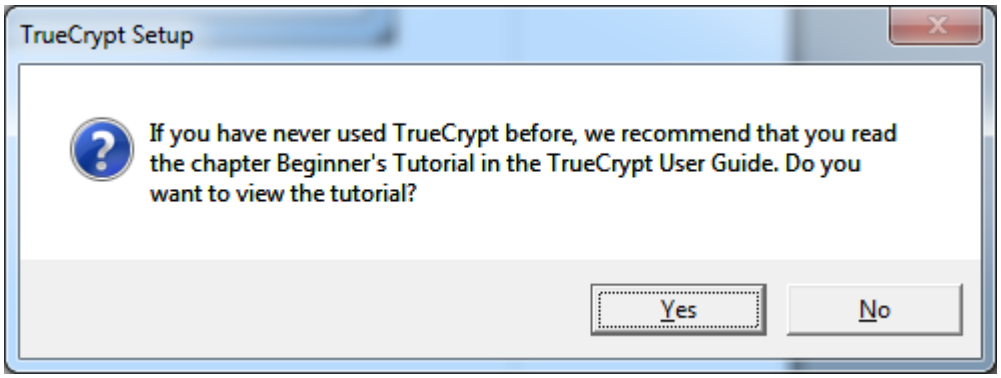
Seuraava ikkuna näyttää asennuksen etenemisen, paina Finish asennuksen valmistuttua.



Lopuksi asennusohjelma kertoo asennuksen onnistumisesta infoikkunalla.



Asennuksen jälkeen asennusohjelma tarjoaa ohjeistusta (englannin kielinen) luettavaksi:



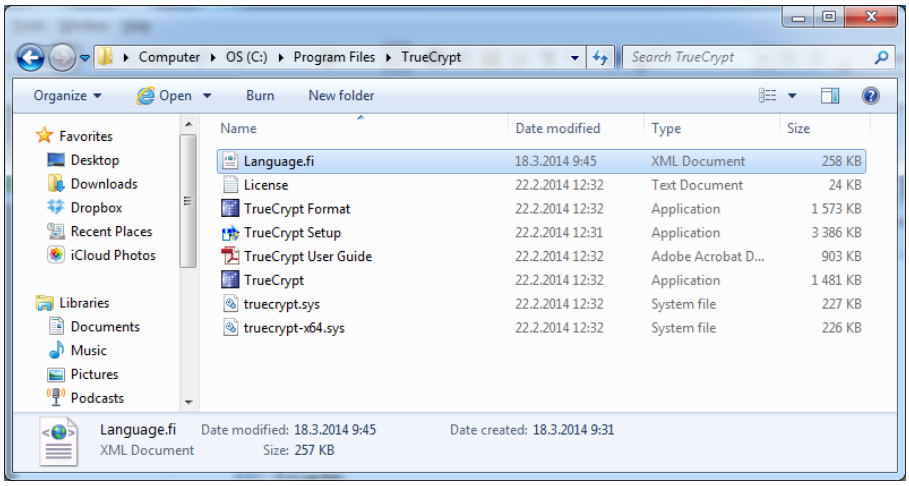
4. SUOMENKIELISEN KIELIPAKETIN ASENTAMINEN

Suomenkielisen ohjelmasta saa asentamalla kielipaketin, joka löytyy osoitteesta: http://www.unicta.fi/truecrypt/localizations. Kielipaketteihin pääsee myös TrueCryptistä valinnalla Settings->Language ja klikkaamalla avautuvasta ikkunasta tekstiä Download Language Pack. Asentaminen saattaa vaatia järjestelmän valvojan oikeuksia (Kirjoitusoikeus Program Files -kansioon), riippuen tietokoneen asetuksista.

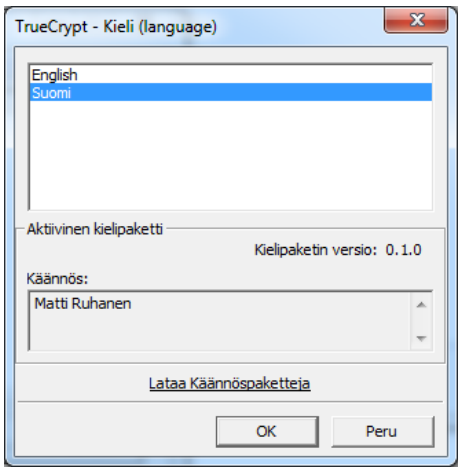
Asennus tapahtuu lataamalla .zip -päätteisen paketin, ohjeen kirjoittamishetkellä langpack-fi-0.1.0-for-truecrypt-7.1a yllä mainitusta osoitteesta (selaa sivua kohtaan Suomi). Paketti on pakattu ja täytyy purkaa esim. WinZip ohjelmalla. Mikäli koneeseen on asennettu WinZip tai vastaava, onnistuu purkaminen helpoiten hiiren oikealla painikkeella klikkaamalla tiedostoa ja valitsemalla WinZip -kohdasta Pura -komento. Windows 7:ssa purkamiseen tarvittava ohjelma on mukana käyttöjärjestelmässä.

Tuloksena on kaksi tiedostoa, Language.fi ja Readme.txt. Jälkimmäisessä tiedostossa on samat ohjeet kuin tässä Suomeksi.

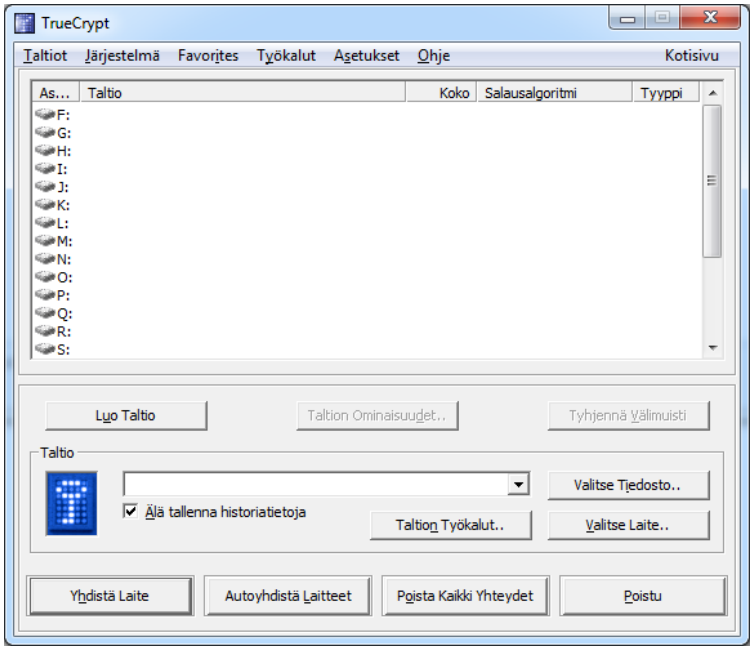
1) Kopioi Language.fi True Cryptin asennuskansioon (oletusarvoisesti C:\Program Files\TrueCrypt)



2) Avaa True Crypt ja valitse Settings -> Language



3) Nyt käyttöliittymän tulisi olla suomenkielinen.

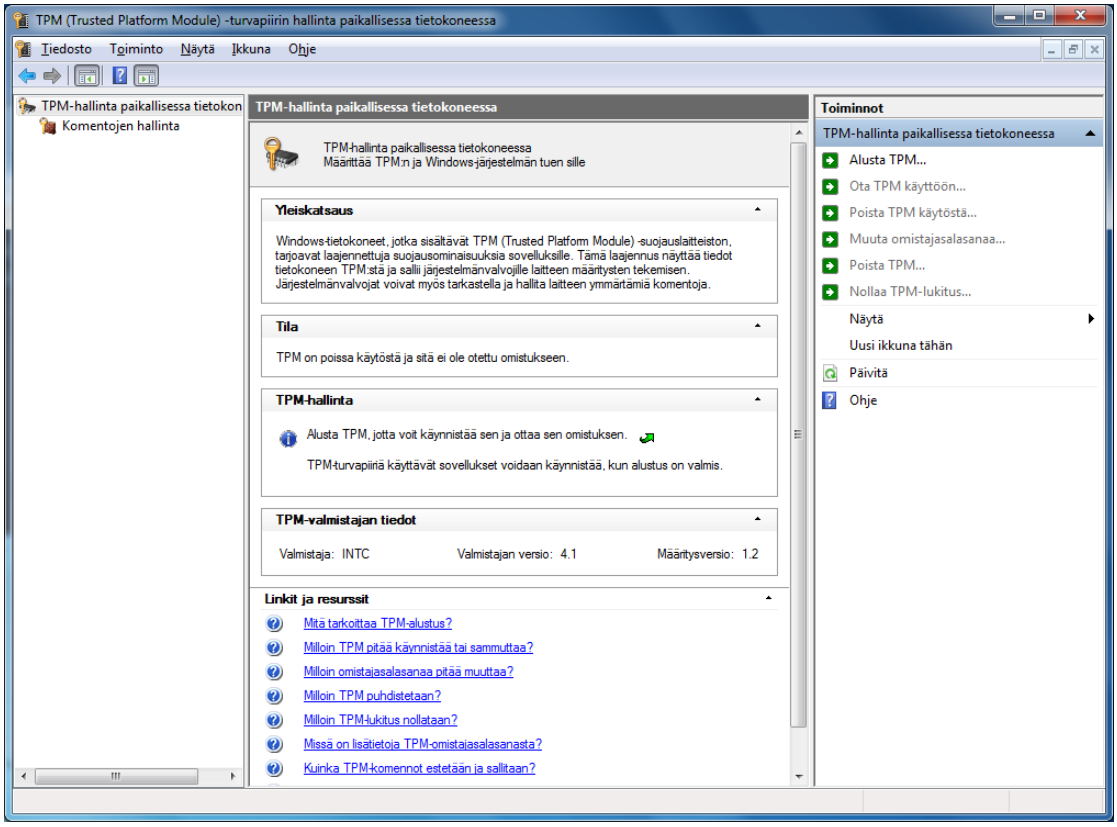


LIITE 1. TPM MODULIN JA BITLOCKER LEVYNSALAUKSEN KÄYTTÖÖNOTTO

BitLocker salaus on helpointa toteuttaa järjestelmissä, joissa on olemassa luotettu turvapiiri, ns. TPM komponentti (TPM, Trusted Paltform Module). TPM turvapiiri on pieni elektroninen komponentti, jonka muistisisältö on suojattu ulkopuolista (luvatonta) muokkaamista vastaan. TPM löytyy yleensä kaikista yrityskäyttöön myytävistä kannettavista ja se on myös joihinkin emolevyihin asennettavissa jälkikäteen.

TPM moduulin hallinnointiin on oma työkalu, joka käynnistyy kirjoittamalla komento tpm.msc windows komentokehotteeseen.

TPM saattaa olla oletusarvoisesti pois käytöstä vaikka koneessa moduuli olisikin asennettuna. Mikäli näin on, voidaan TPM ottaa käyttöön koneen BIOS asetuksista (kohta Security). TPM:n ollessa käytettävissä, hallinnointi yleensä näyttää kutakuinkin alla olevalta.

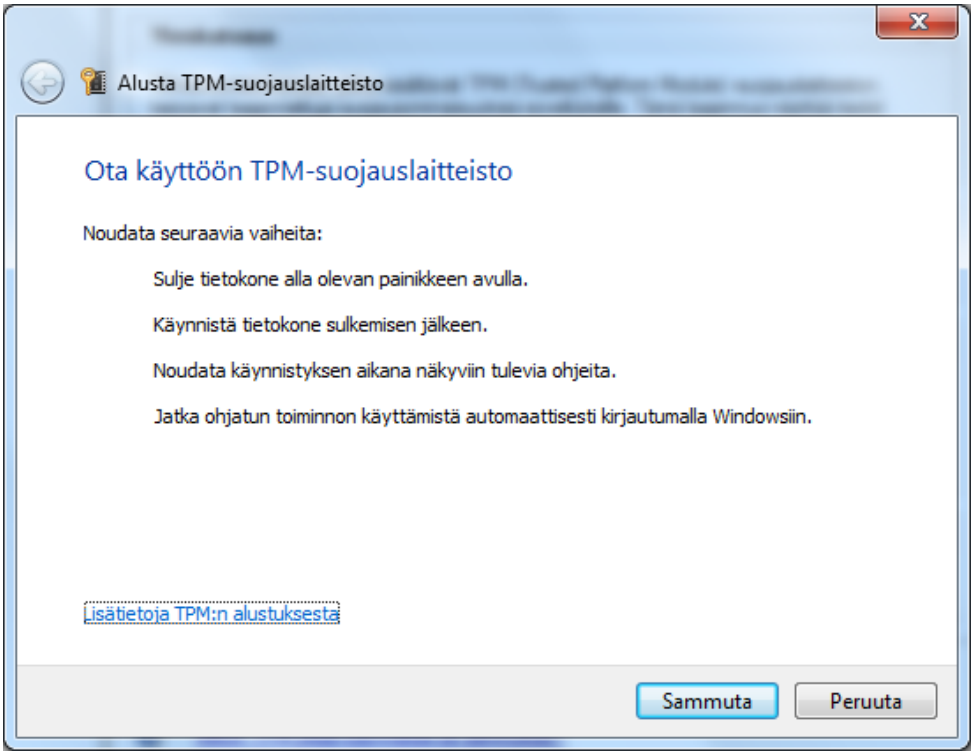


TPM aktivoidaan käyttöön alustamalla se "Alusta TPM" toiminnolla.

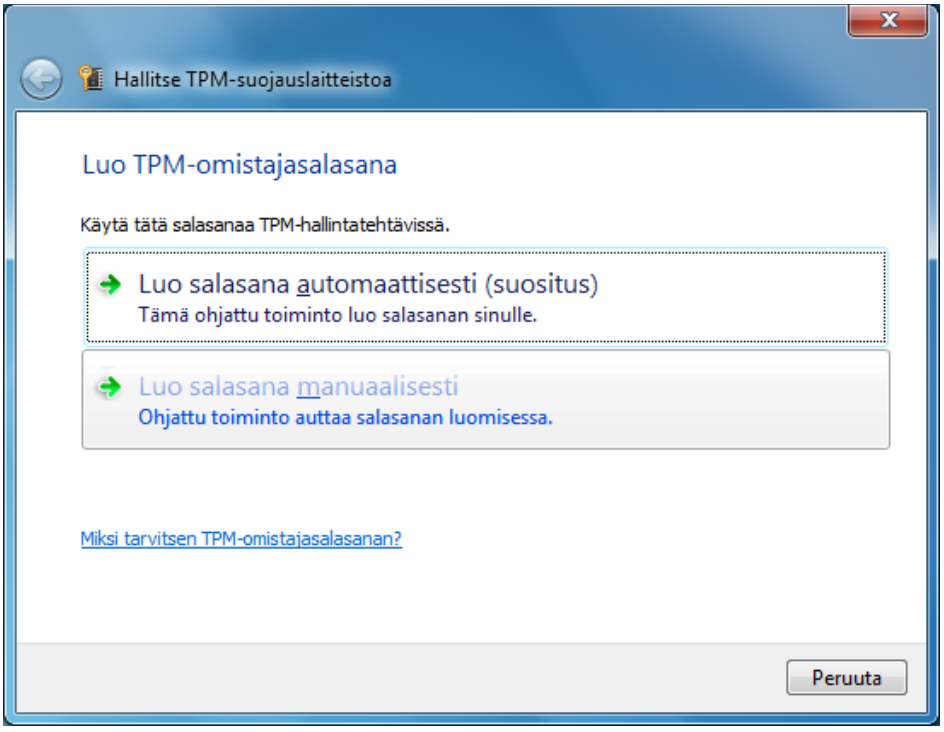
HUOM 1: Tämä toiminto sisältää koneen uudelleen käynnistyksen, tallenna kaikki tallentamattomat työt ennen aloittamista!

HUOM 2: Mikäli kone on ollut jo käytössä ja siinä on arvokasta tietoa, on syytä ottaa VARMUUSKOPIO ennen kuin levyä aletaan salata!

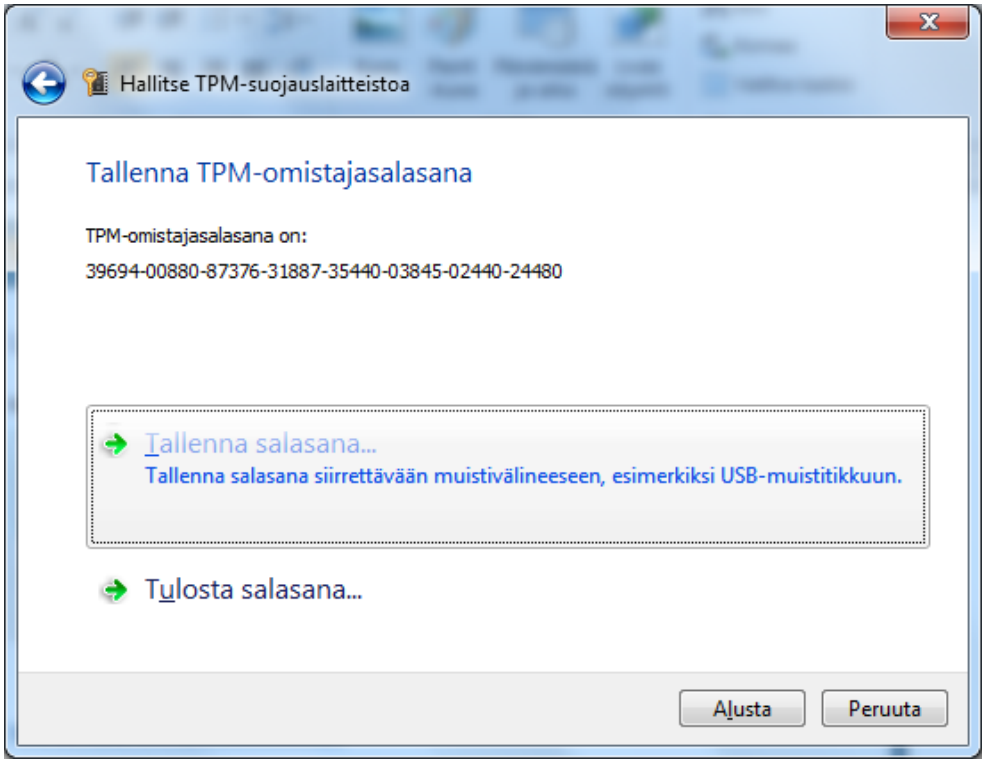
Toiminto käynnistää ohjatun alustuksen, kuvakaappaukset ja selitykset alla:



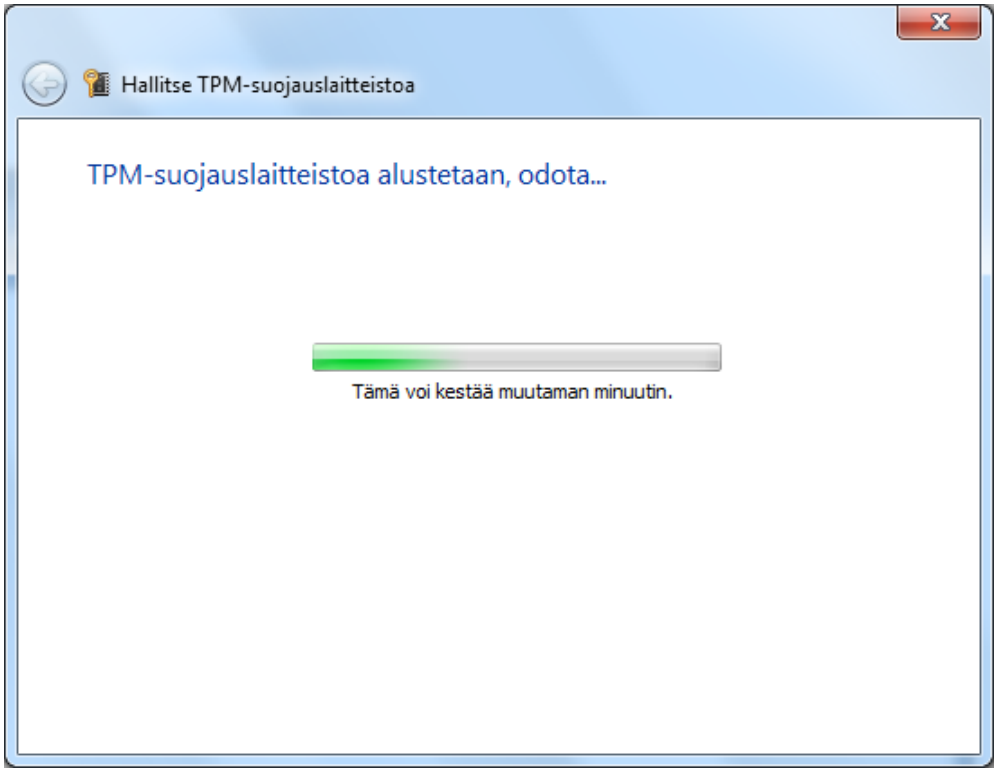
TPM käyttöönoton ensimmäinen vaihe asettaa koneen tilaan, jossa uudelleen käynnistys aktivoi TPM moduulin. Kone siis sammutettaan ja varsinainen käyttöönotto alkaa käynnistyksen yhteydessä.



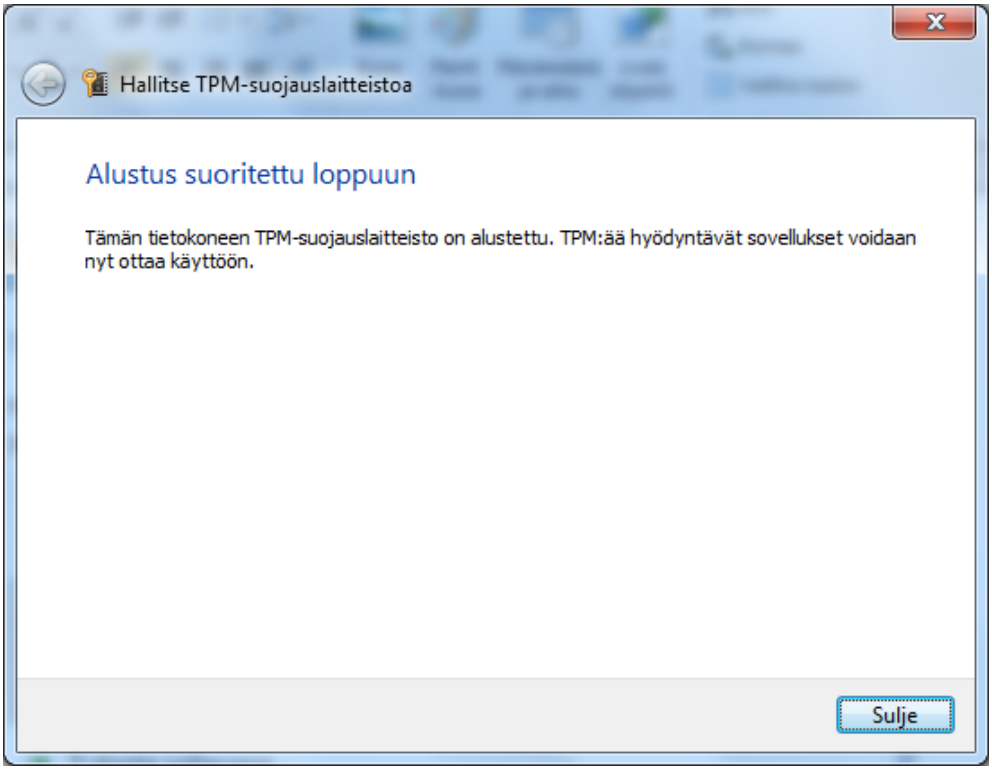
TPM turvapiirille luodaan omistajasalasana, joka on syytä tallentaa luotettavasti. Ohjatun toiminnan automaattisesti luoma salasana on hyvä vaihtoehto.



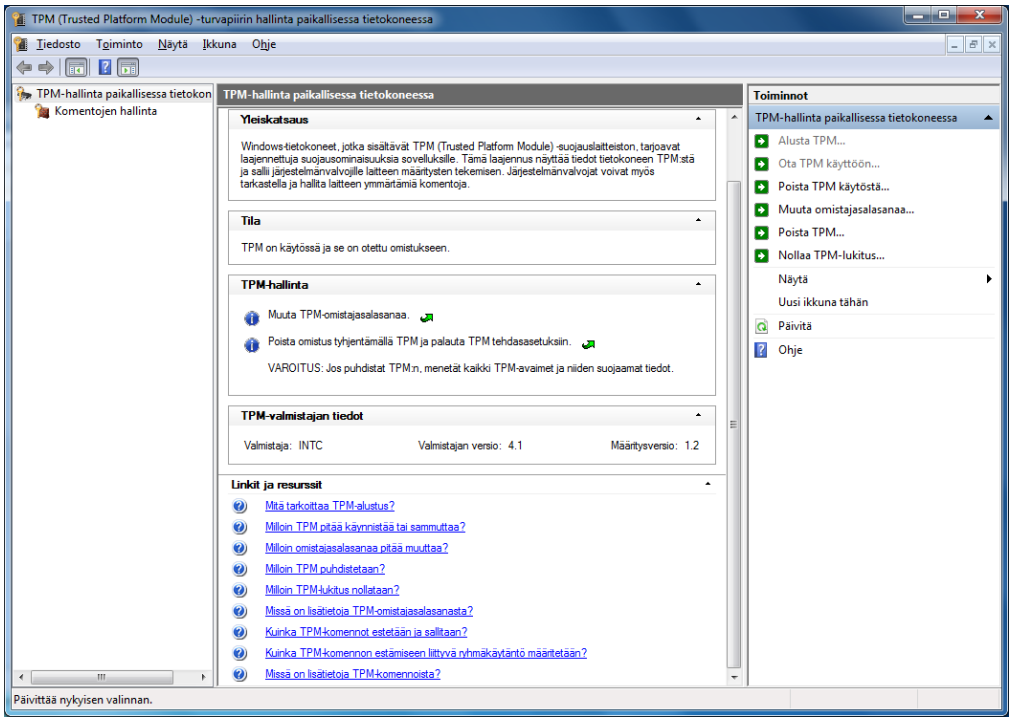
Toiminto näyttää salasanan ja se on myös syytä tässä vaiheessa tallentaa esimerkiksi muistitikulle.



Salasanan tallentamisen jälkeen TPM turvapiiri alustetaan, mikä vie hetken.

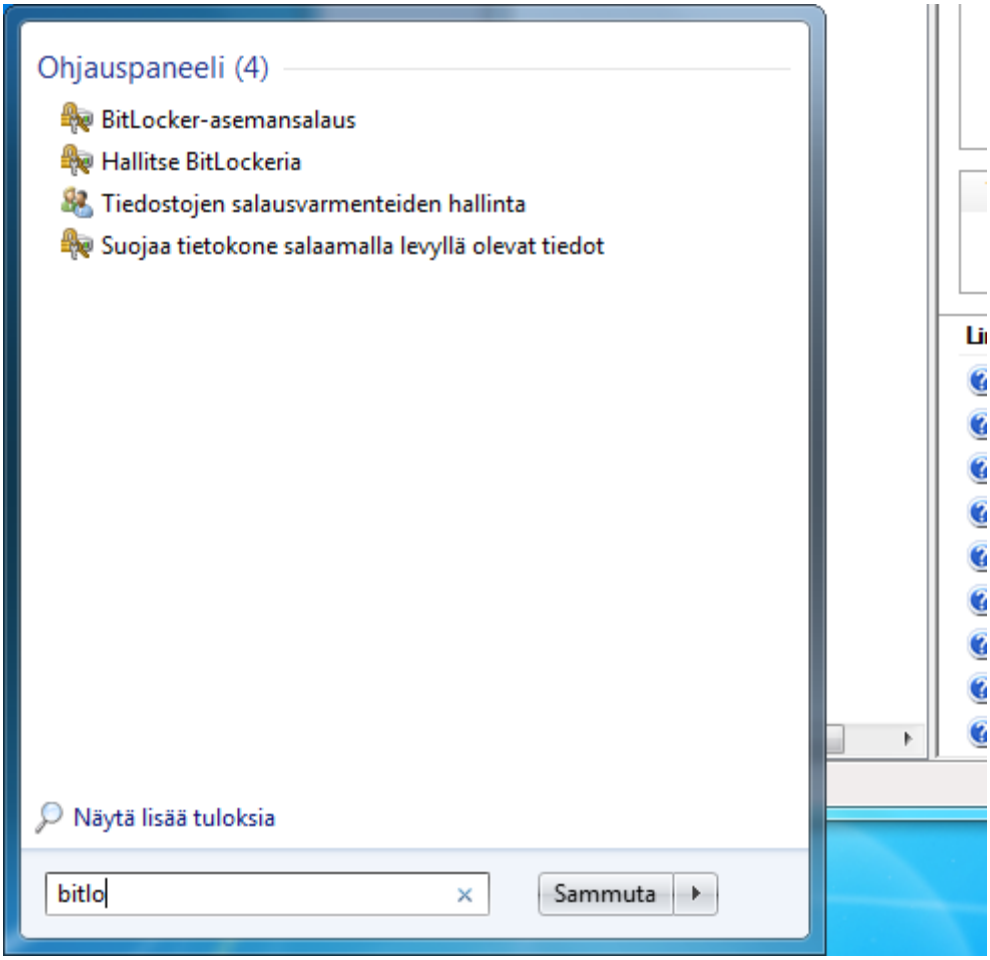


Kun alustus on valmis, on turvapiiri käytettävissä. Turvapiiri on vahvasti sidoksissa käytössä olevaan laitteistoon, eli sitä ei voi siirtää toiseen laitteistoon ja käyttää siellä onnistuneesti.

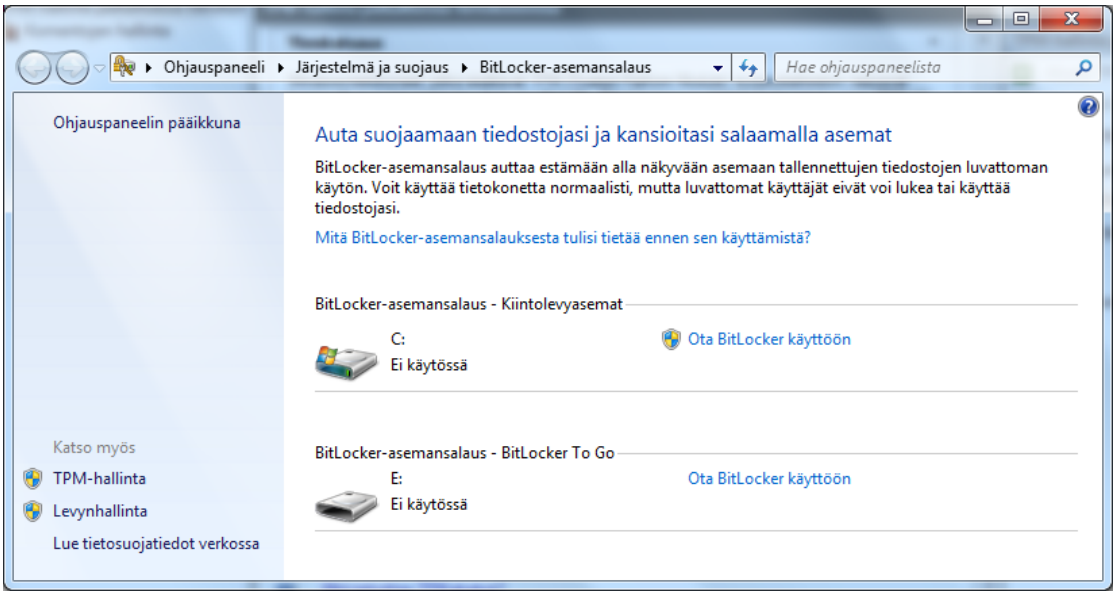


TPM hallinnointityökalu näyttää nyt että TPM on käytössä ja otettu omistukseen. Kun tämä on valmis, voidaan BitLocker ottaa käyttöön aseman salauksessa ja TPM hallinnoi siinä tarvittavia avaimia.

BitLocker voidaan ottaa käyttöön windows -kuvakkeesta kirjoittamalla hakukenttään BitLocker. Valitse kohta BitLocker-asemansalaus.

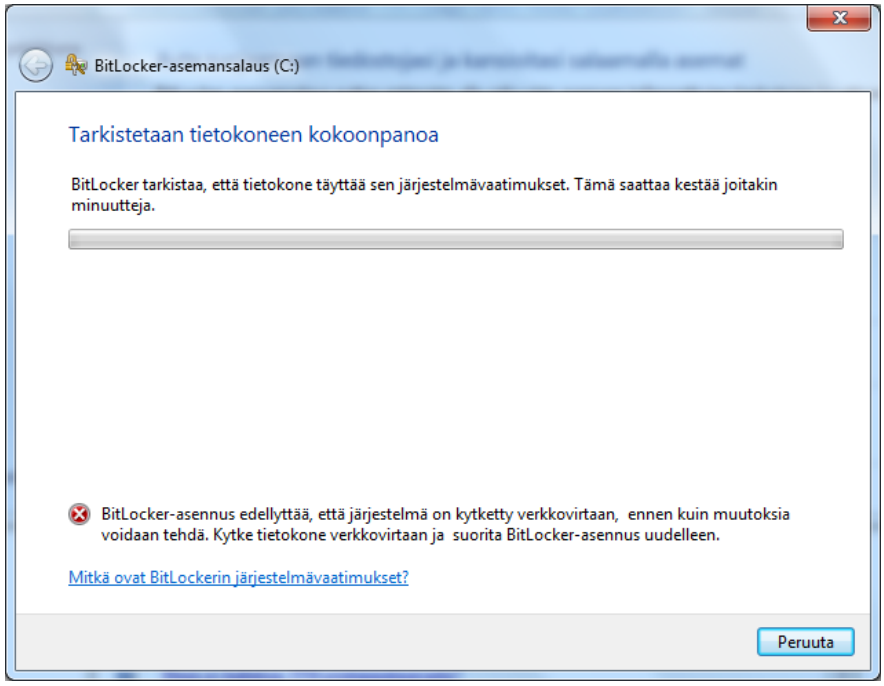


Avautuvasta ikkunasta voi aseman salauksen ottaa käyttöön asemakohtaisesti. Tässä esimerkissä salataan käyttöjärjestelmän sisältävä asema C:.

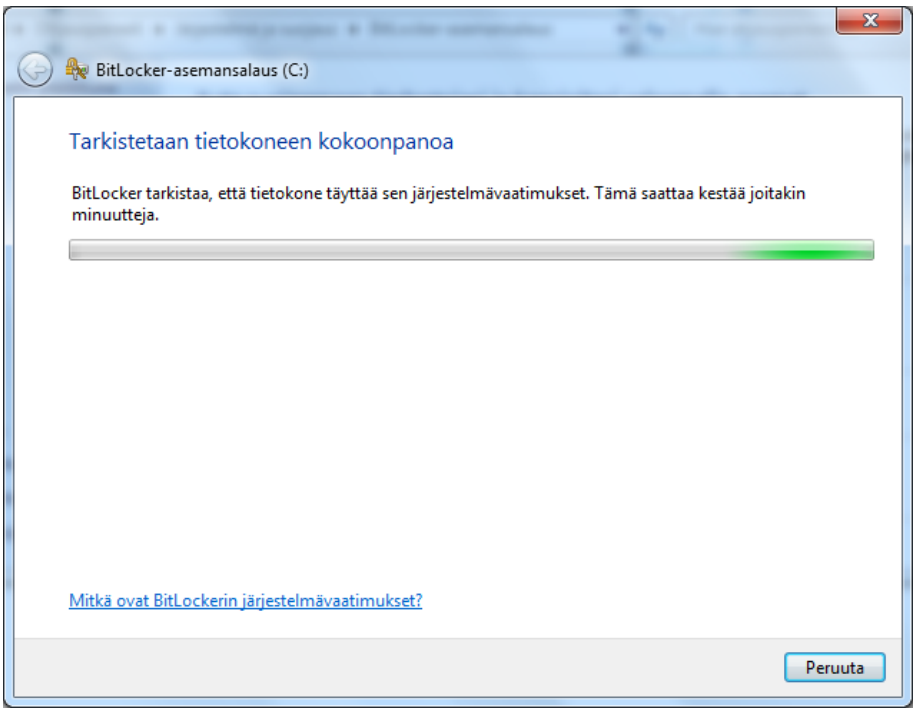


Klikkaa "Ota BitLocker käyttöön" valitsemastasi asemasta.

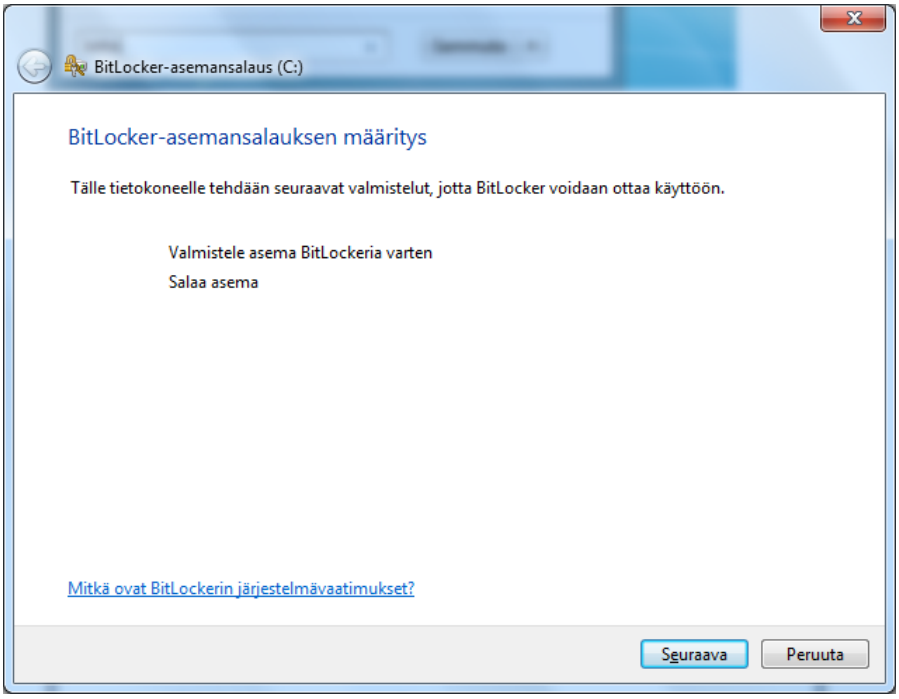
Salauksen käyttöönotto käynnistää ohjatun toiminnon, joka aluksi tarkastaa tietokoneen kokoonpanon.



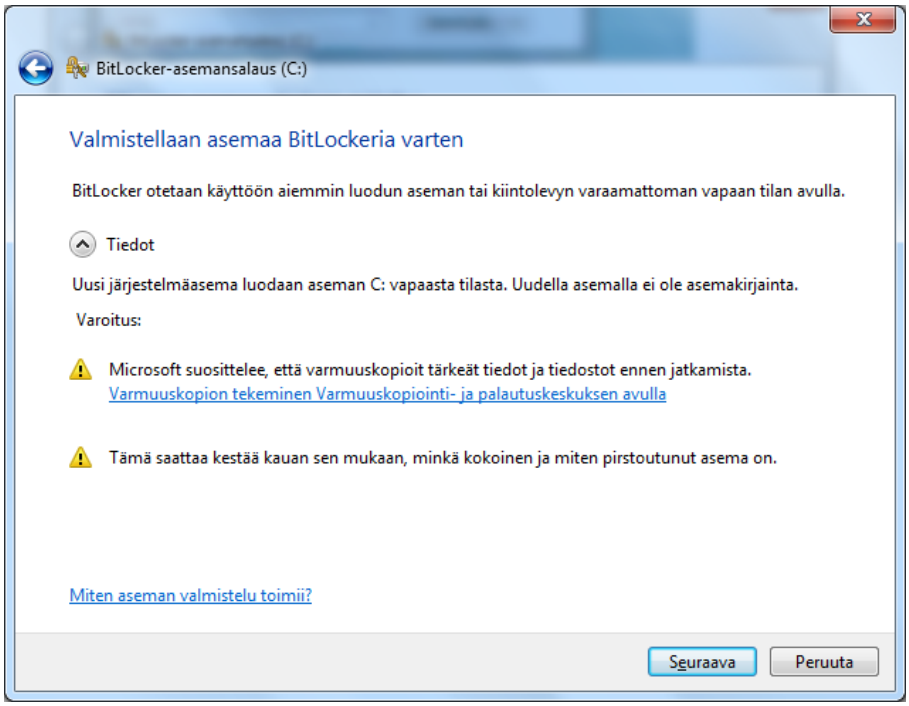
Tässä esimerkissä kannettava kone ei ollut verkkovirrassa, joten järjestelmä ei aloita levyn salausta (virran loppuminen kesken salauksen saattaa aiheuttaa ongelmia). Salaus kestää verraten pitkään (tosi pitkän kahvitauon verran), luonnollisesti levyn koosta, käyttöasteesta, koneen nopeudesta ja monista muista tekijöistä riippuen.



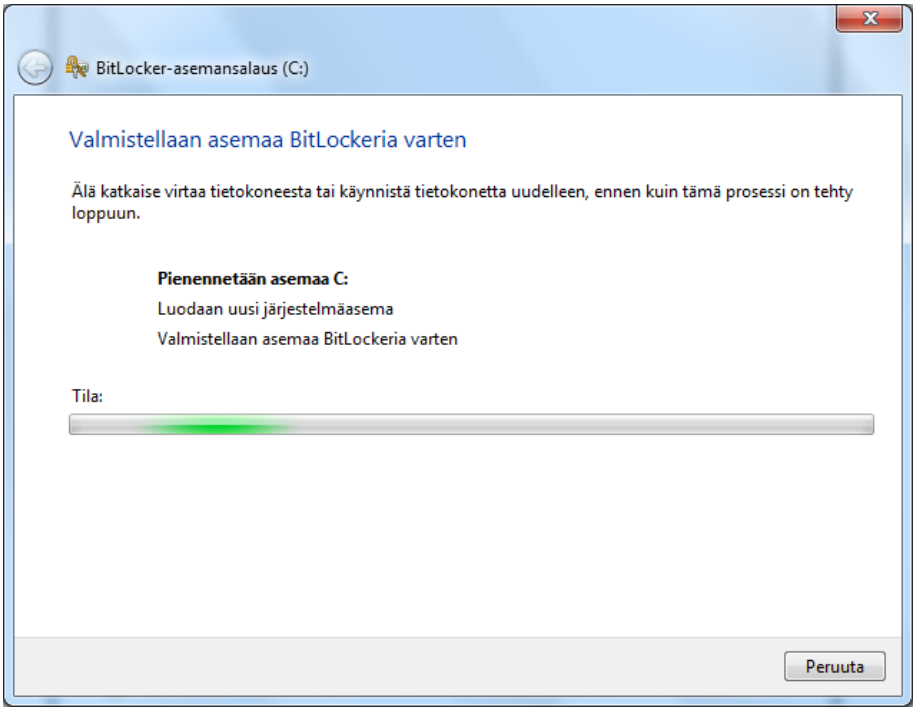
Tarkistuksen jälkeen järjestelmä alkaa varsinaisen salaustoiminnon.



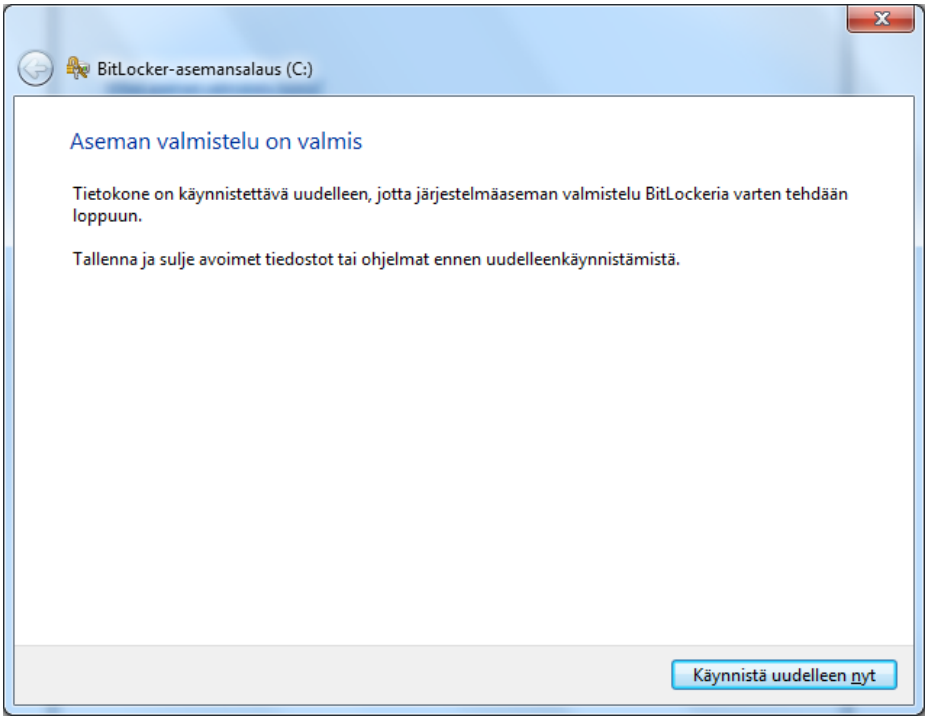
Paina Seuraava. Ohjattu toiminne vielä muistuttaa varmuuskopiosta ja kertoo että salauksessa voi mennä pitkäänkin (aseman tiedot samalla järjestellään uudelleen).



Paina Seuraava.

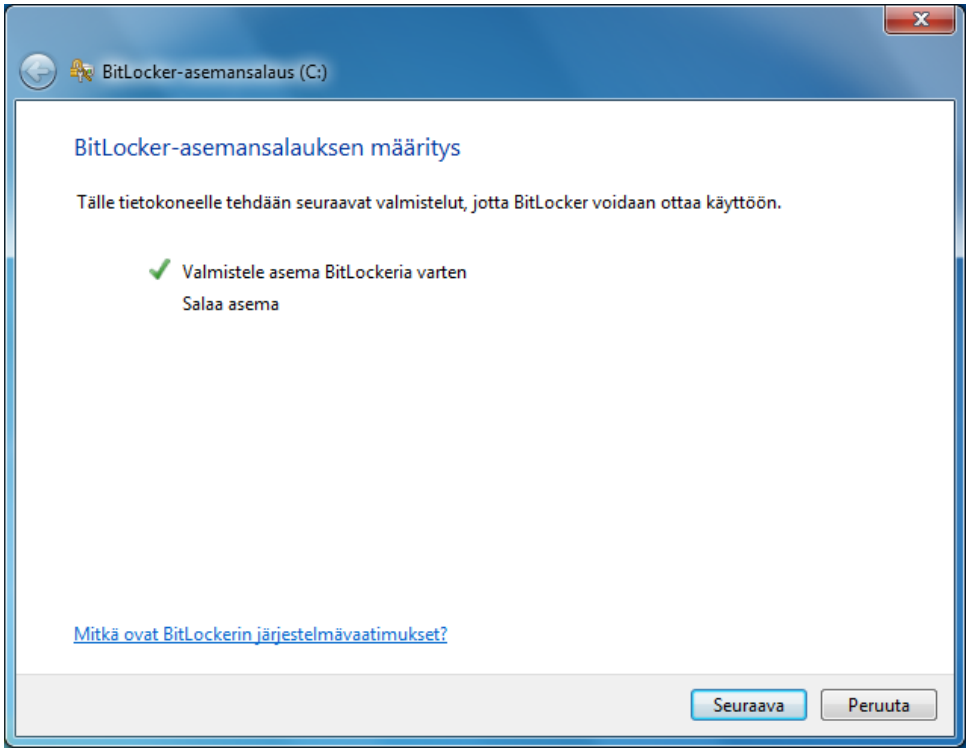


Valmistelu (defragmentointi) kestää kohtuullisen pitkään, loppuun se saadaan käynnistämällä kone uudelleen kun ohjattu toiminto niin pyytää.

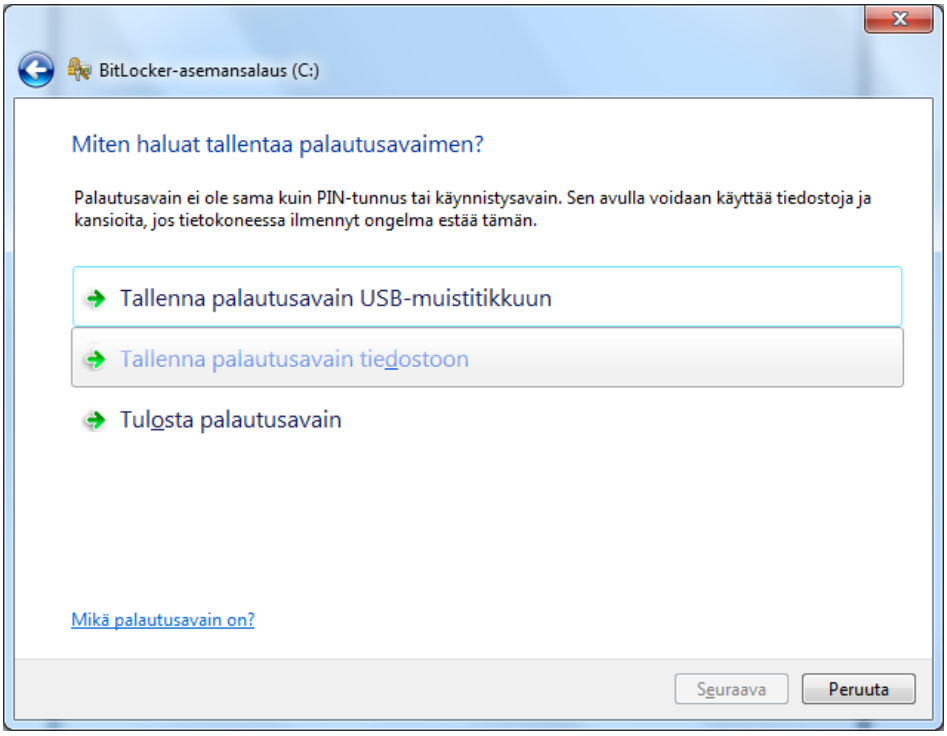


Paina "Käynnistä uudelleen nyt".

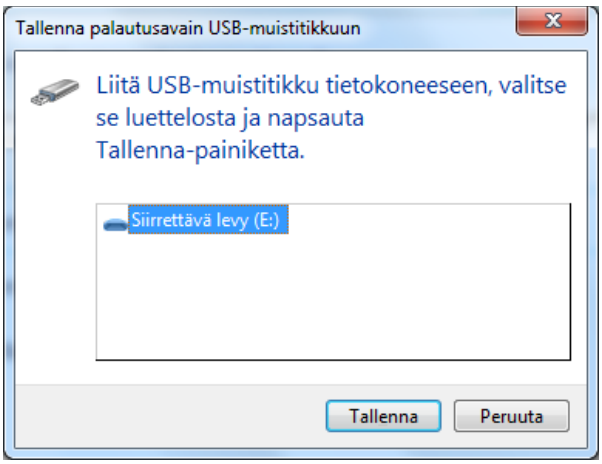
Salaus alkaa uudelleen käynnistyksen jälkeen määrityksillä:



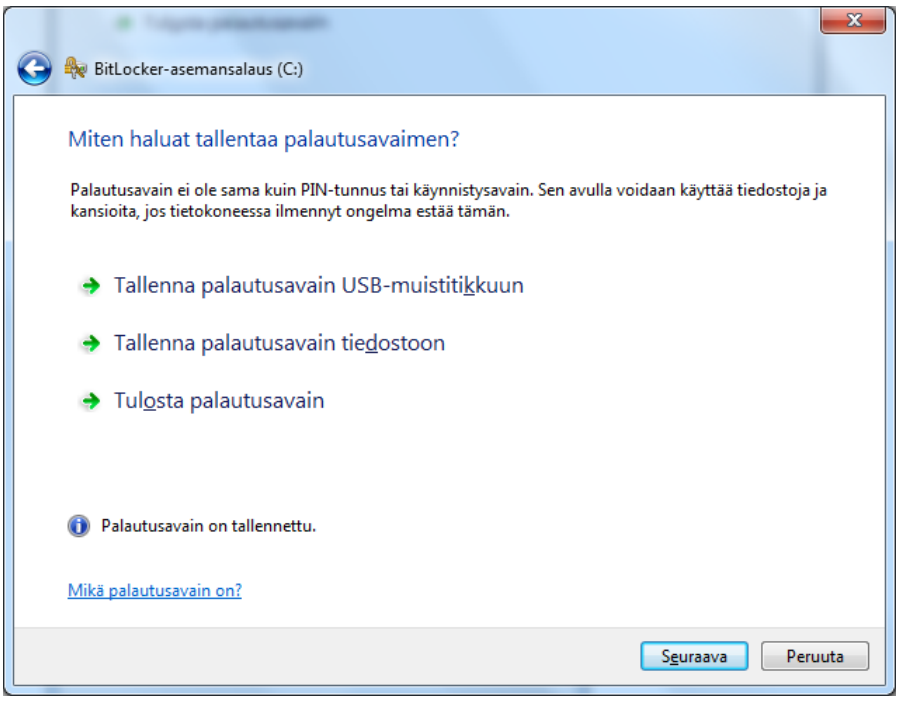
Salauksen avaamista varten (tilanteessa jossa se ei onnistu esimerkiksi laiteviasta johtuen) luodaan palautusavain. Se on syytä tallentaa paikkaan jossa se on turvassa, esimerkiksi usb muistille tai organisaation suojatulle palvelimelle.



USB muistitikku -valinnan jälkeen ohjattu toiminto kysyy avaimen tallennuspaikkaa:

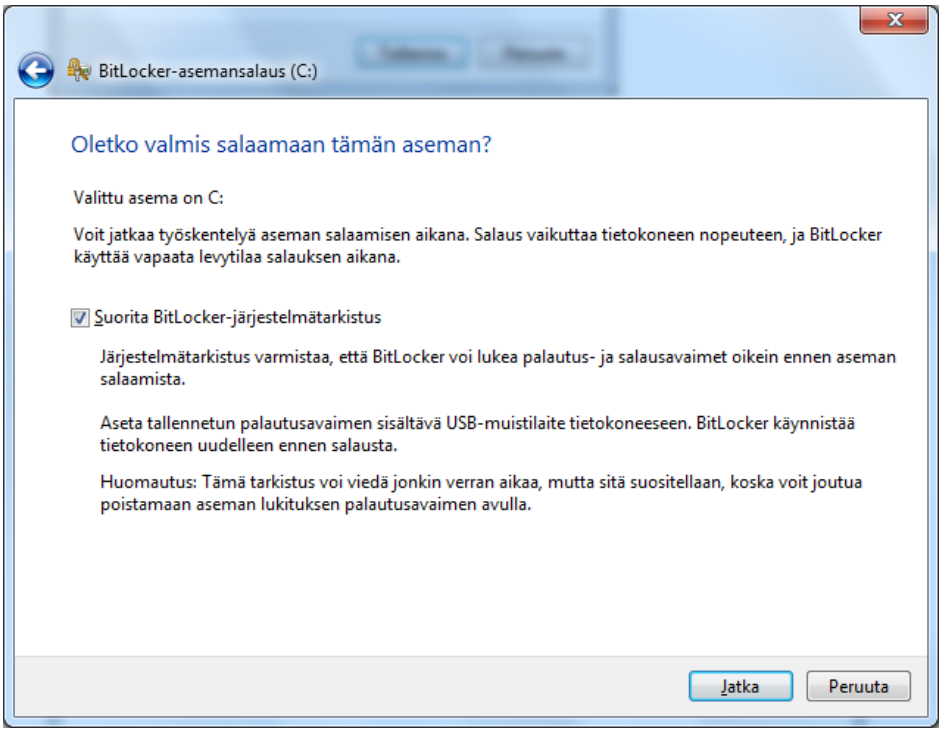


Valitse haluttu USB muisti ja paina "Tallenna". Tallennuksen jälkeen infoteksti "Palautusavain on tallennettu" kertoo avaimen olevan tallessa.

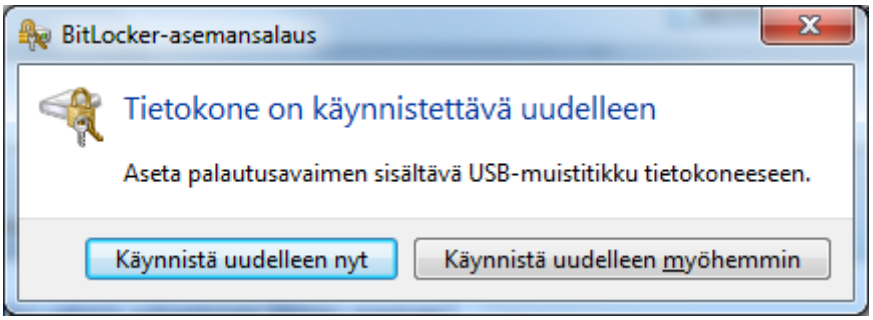


Paina "Seuraava".

Kun avaimen tallentamiseen liittyvät toimet ovat valmiit, voidaan salaus aloittaa. On suositeltavaa testata salaus- ja palautusavainten toiminta (valintaruutu Suorita BitLocker -järjestelmän tarkistus).

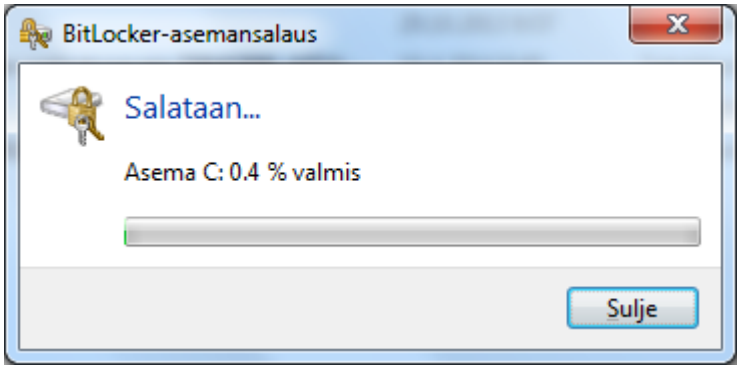


Mikäli valitsit järjestelmätarkistuksen, ohjattu toiminto pyytää palautusavaimen sisältävän muistitikun ja käynnistää koneen uudelleen. Mikäli et valinnut tarkistusta tämä vaihe ohitetaan.

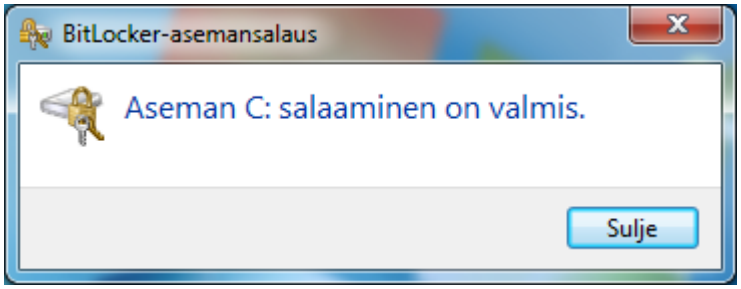


Paina "Käynnistä uudelleen nyt".

Itse salaus alkaa ja sitä voi suorittaa taustalla. Koneella voi periaatteessa tehdä asioita salauksen aikana, mutta voi olla hyvä antaa koneen tehdä asiansa rauhassa salauksen ajan.

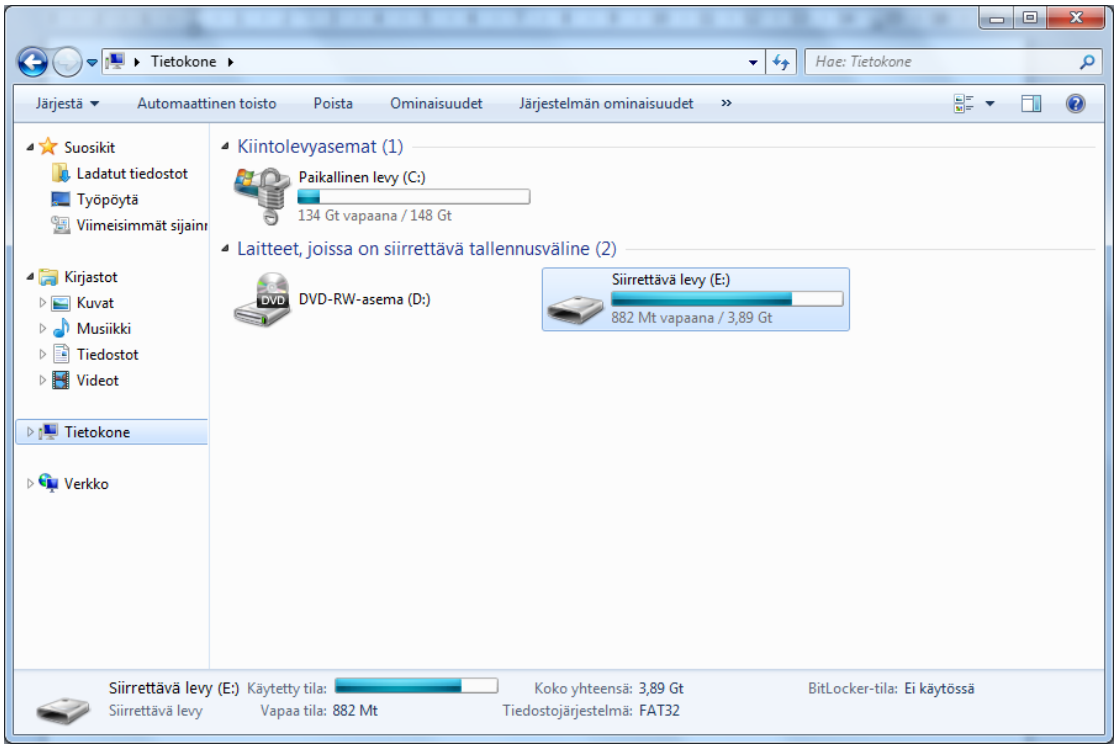


Varsin pitkän kahvitauon jälkeen salaus on valmis.



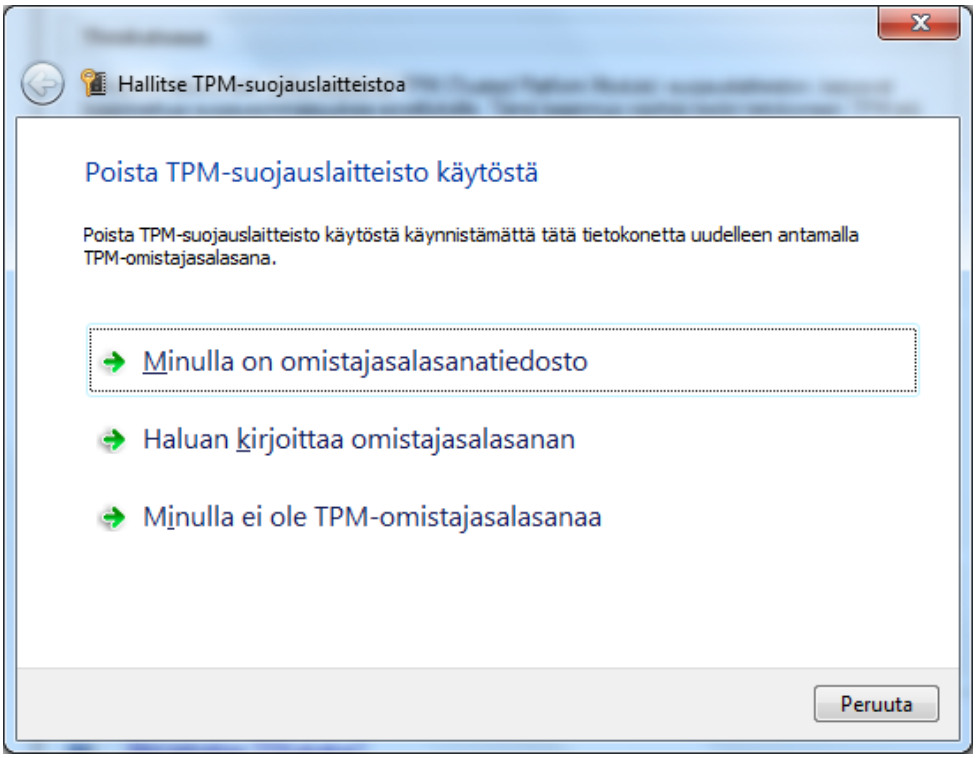
Paina Sulje.

Avattaessa resurssien hallinta nähdään nyt että asema on salattu (Tunnuksen päällä on lukon kuva).



TPM turvapiirin poistaminen käytöstä

TPM turvapiirin voi tarvittaessa poistaa käytöstä, tosin se ei ole suositeltavaa ainakaan jos levysalaus on käytössä. Poistaminen tapahtuu turvapiirin hallinnoinnin työkalulla (tpm.msc komentokehotteesta). Poistamiseen tarvitaan salasanatiedosto tai salasana täytyy kirjoittaa.



Salasanatiedosto syötetään ohjattuun toimintoon joka poistaa TPM moduulin käytöstä.