

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.	Joho	lanto	.5
2.	Työa	asemaympäristön vaatimukset	.6
	2.1.	Laitteistolle asetetut vaatimukset	.6
	2.1.	Käytettävän työaseman suojaustaso	.6
	2.2.	Kulutuksentasausominaisuus	.6
	2.3.	Hibernaatio (horrostila)	.7
	2.4.	Suositukset	.8
	2.5.	Salasanavaatimukset	.9
	2.6.	Toimikorttia käyttävät tahot	.9
	2.6.	1. Outlook asetukset	10
3.	True	eCrypt asennusohje Windows käyttöjärjestelmille	13
4.	Suo	menkielisen kielipaketin asentaminen	16
LII	TE 1. T	PM modulin ja BitLocker levynsalauksen käyttöönotto	18

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.

TrueCrypt - Preferences					
Default Mount Options Mount volumes as read-only Mount volumes as removable media					
TrueCrypt Background Task Image: Enabled Image: Exit when there are no mounted volumes					
Actions to perform upon logon to Windows					
Auto-Dismount Dismount all when: Image: User logs off Image: Screen saver is launched Image: Entering power saving model Image: Auto-dismount volume after no data has been read/written to it for 60 Image: Force auto-dismount even if volume contains open files or directories					
 Windows Open Explorer window for successfully mounted volume ✓ Use a different taskbar icon when there are mounted volumes ✓ Preserve modification timestamp of file containers 					
Password Cache Cache passwords in driver memory Wipe cached passwords on exit Wipe cached passwords on auto-dismount					
More Settings OK Cancel					

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 Idap.fineid.fi. Hakemisto otetaan Outlookissa käyttöön sähköpostitilin asetuksista, Tiedosto->Tiliasetukset josta välilehti osoitteistot.

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

iă uusi tili	
Kansion tai osoitteiston laji Voit valita lisättävän kansion tai osoitteen lajin.	×
Internet-hakemistopalvelu (LDAP)	
Yhdistä LDAP-palvelimeen sähköpostiosoitteiden ja muiden tietojen etsimistä ja tarkistamista varten.	
🔘 Lisää <u>o</u> soitteistoja	
Yhdistä osoitteistoon sähköpostiosoitteiden ja muiden tietojen etsimistä ja tarkistamista varten.	
< Egelinen Seuraava	> Peruuta

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

Lisää uusi tili		—
Hakemistopalvelu Voit kirjoittaa hak	in (LDAP) asetukset kemistopalvelun tietojen käytössä vaadittavat asetukset.	× C
Palvelimen tiedot		
Kirjoita sen hakemistop määrittänyt sinulle.	palvelun nimi, jonka Internet-palveluntarjoaja tai järjestelmänvalvoja on	
Palvelimen <u>n</u> imi:	ldap.fineid.fi	
Kirjaustiedot		
🔲 T <u>ä</u> mä palvelin vaati	ii kirjautumisen	
<u>K</u> äyttäjänimi:		
S <u>a</u> lasana;		
Uaadi suojattua	a salasanan vahvistusta (Secure Password Authentication)	
	< Egelinen Seuraava >	Peruuta

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

Microsoft LDAP-hake	emisto	×
Yhteys Etsintä		
Näyttönimi		
<u>N</u> äyttönimi osoitte	eiston mukaisessa muodossa	
Varmennehake	emisto (fineid)	
Yhteyden tiedot		
Portti:	389	
K <u>ä</u> ytä SSL-yhteyttä		
	OK Peruuta K <u>ä</u> yt	tä

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

Tiliasetukset							
Kansiot ja osoitteistot Voit valita muutettavan tai poistettavan kansion tai osoitteiston alla olevasta luettelosta.							
Datatiedostot RSS-syötteet SharePoint-luettelot Internet-kalenterit Julkaistut kalenterit Osoitteistot							
🔟 Uusi 🚰 Muuta 🗙 Poista							
Nimi	Laji						
Outlook-osoitteisto	MAPI						
Varmennehakemisto	LDAP						
Varmennehakemisto (fineid)	LDAP						
			Sulie				

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

<u>ا گ</u>	/äestörekiste	erikeskus \	ARMENNEHA	AKU VARMENNEHAKEMISTOS	TA - Mi	crosoft	t Int	ernet Explor	er prov	ided by Pelast	usopisto		- 0	
9	http://vrk. f i	neid.fi/ce	tsearchB.asp?	state=search&issuercn=VRK+	CA+for	+ Quali	fied	+ Certificate	s&lastr	name=Hassin	en&firstname	=Marko&d	finuid=	
													Sulje ikku	na
VA	RMENNEHA	AKU VARI	MENNEHAKEN	IISTOSTA										
(II /0	joita nakuei t kävttää * -	nto alla ol merkkiä k	eviin kentiin. atkaisumerkk	tinä.										
ła	ku palautta	a maksim	issaan 100 v	armennetta.										
Va	rmenteen i	myöntäjä	(CA)											
6	VRK Gov.	CA for Ci	tizen Qualified	d Certificates										
0	VRK Gov.	CA for Ci	tizen Qualified	d Certificates - G2										
0	VRK CA f	or Qualifie	d Certificates											
0	VRK CA f	or Qualifie	d Certificates	- <u>G2</u>										
0	VRK CA f	or Service	Providers											
0	VRK CA f	or Service	Providers - G	<u>2</u>										
0	VRK CA f	or Healtho	are Service P	roviders										
C	VRK CA f	or Healtho	are Professio	onals Qualified Certificates										
Su	kunimi:			Etunimi:	Tunnu	s:								
H	assinen			Marko										
F	Lisää hakı	utuloksiin	myös allekirjo	pitusvarmenteet										
				Lataa sulkulista		Etsi v	arm	nenteet						
Ha	un tulokse	t												
ŧ	Sukunimi	Etunimi	Tunnus	Sähköposti		Käyt	tö	Lataa varn	nenne	Hex				
I	Hassinen	Marko	910582873	marko.hassinen@pelastusc	pisto.fi	<u>,</u>	Y	2000392	825	773B9279				
2	Hassinen	Marko	910582873	marko.hassinen@pelastusc	pisto.fi	<u>,</u>	Y	2000460	512	773C9AE0				
													100%	
													- 100 %	

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.

Tiedostoj	en lataaminen – Suojausvaroitus								
Haluatko tallentaa tai suorittaa tāmān tiedoston?									
Nimi: TrueCrypt Setup 7.1a.exe Tyyppi: Sovellus Lähde: www.truecrypt.org									
	Suorita <u>T</u> allenna Peruuta								
	Vaikka Internetistä ladatut tiedostot voivat olla hyödyllisiä, tämän tyyppiset tiedostot voivat vahingoittaa tietokonettasi. Jos et luota lähteeseen, älä suorita tai tallenna tätä ohjelmaa. Lisätietoja riskeistä								

Asennuksen ensimmäinen vaihe on lisenssiehtojen hyväksyminen, paina Next.

😰 TrueCrypt Setup 7.1a						
Please read the license terms You must accept these license terms before you can use, extract, or install TrueCrypt.						
IMPORTANT: By checking the checkbox below, you accept these license terms and signify understand and agree to them. Please click the 'arrow down' icon to see the rest of the lic	that you ense.					
TrueCrypt License Version 3.0 Software distributed under this license is distributed on an "AS IS" BASIS WITHOUT WARRANTIES OF ANY KIND. THE AUTHORS AND DISTRIBUTORS OF THE SOFTWARE DISCLAIM ANY LIABILITY. ANYONE WHO USES, COPIES, MODIFIES, OR (RE)DISTRIBUTES ANY PART OF THE SOFTWARE IS, BY SUCH ACTION(S), ACCEPTING AND AGREEING TO BE BOUND BY ALL TERMS AND CONDITIONS OF THIS LICENSE. IF YOU DO NOT ACCEPT THEM, DO NOT USE, COPY, MODIFY, NOR (RE)DISTRIBUTE THE SOFTWARE, NOR ANY PART(S) THEREOF.						
I. Definitions I. "This Product" means the work (including, but not limited to, source code, graphics, te I accept the license terms TrueCrypt Installer	exts, and 🔻					
Help < Back Next >	Cancel					

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

😰 TrueCrypt Setup 7.1a								
Wizard Mode Select one of the modes. If you are not sure which to select, use the default mode. • Install Select this option if you want to install TrueCrypt on this system.								
If you select this option, all files will be extracted from this package but nothing will be installed on the system. Do not select it if you intend to encrypt the system partition or system drive. Selecting this option can be useful, for example, if you want to run TrueCrypt in so-called portable mode. TrueCrypt does not have to be installed on the operating system under which it is run. After all files are extracted, you can directly run the extracted file 'TrueCrypt.exe' (then TrueCrypt will run in portable mode).								
TrueCrypt Installer]							

Seuraava ikkuna näyttää asennuksen etenemisen, paina Finish asennuksen valmistuttua.

TrueCrypt Setup 7.1a	
Installing Please wait while TrueCrypt is being installed.	
 Creating System Restore point Installing C: \Program Files\TrueCrypt\TrueCrypt User Guide.pdf Installing C: \Program Files\TrueCrypt\License.txt Installing C: \Program Files\TrueCrypt\TrueCrypt.exe Installing C: \Program Files\TrueCrypt\TrueCrypt Format.exe Installing C: \Program Files\TrueCrypt\truecrypt.sys Installing C: \Program Files\TrueCrypt\truecrypt.sys Installing C: \Windows\system32\Drivers\truecrypt.sys	*
TrueCrypt Installer	Cancel

Lopuksi asennusohjelma kertoo asennuksen onnistumisesta infoikkunalla.



Asennuksen jälkeen asennusohjelma tarjoaa ohjeistusta (englannin kielinen) luettavaksi:

TrueCrypt	Setup		X
?	If you have never used TrueCrypt before, we the chapter Beginner's Tutorial in the TrueCr want to view the tutorial?	recommend tha ypt User Guide. [t you read)o you
		Yes	<u>N</u> o

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-0.1.0for-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.

- O X -G ↓ Computer → OS (C:) → Program Files → TrueCrypt ▼ 4 Search TrueCrypt Q Organize 🔻 🖉 Open 🔻 Burn New folder = - 1 0 Name Date modified Type Size 👉 Eavorites XML Document 🧮 Desktop 🔮 Language.fi 18.3.2014 9:45 258 KB L Downloads 22.2.2014 12:32 License 24 KB Text Document 😻 Dropbox TrueCrypt Format 22.2.2014 12:32 1 573 KB Application 🖳 Recent Places 🎲 TrueCrypt Setup 22.2.2014 12:31 Application 3 386 KB iCloud Photos 🔁 TrueCrypt User Guide 22.2.2014 12:32 Adobe Acrobat D... 903 KB 🔢 TrueCrypt 22.2.2014 12:32 Application 1 481 KB 📄 Libraries 🚳 truecrypt.sys 22.2.2014 12:32 System file 227 KB Documents 22.2.2014 12:32 System file 226 KB 🚳 truecrypt-x64.sys al Music Pictures ^(興) Podcasts < 💽 Language.fi Date modified: 18.3.2014 9:45 Date created: 18.3.2014 9:31 XMI Document Size: 257 KB

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

2) Avaa True Crypt ja valitse Settings -> Language

TrueCrypt - Kieli (language)	x
English]
Suomi	
ı Aktiivinen kielipaketti	
Kielipaketin versio:	0.1.0
Matti Ruhanen	*
	-
Lataa Käännöspaketteja	
OK Per	ru

3) Nyt käyttöliittymän tulisi olla suomenkielinen.

True	Crypt								x
<u>T</u> altiot	<u>J</u> ärjestelmä	Favor <u>i</u> tes	T <u>v</u> ökalut	A <u>s</u> etukset	<u>O</u> hje			Kotisi	ivu
As	Taltio				Коко	Salausalgoritmi		Гууррі	4 III +
Taltio	L <u>u</u> o Taltio		Ta	ltion Ominaist	u <u>d</u> et,,	Т	yhjennä <u>V</u> ä	ilimuisti]
	I Älä	tallenna histo	riatietoja	Т	altio <u>n</u> Työka	▼ N	/alitse T <u>i</u> ed <u>V</u> alitse La	osto ite	
Y	<u>h</u> distä Laite	Auto	oyhdistä <u>L</u> ai	tteet P	oista Kaikki	Yhteydet	Poi	stu	

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:

🕞 🖀 Alusta TPM-suojauslaitteisto
Ota käyttöön TPM-suojauslaitteisto
Noudata seuraavia vaiheita:
Sulje tietokone alla olevan painikkeen avulla.
Käynnistä tietokone sulkemisen jälkeen.
Noudata käynnistyksen aikana näkyviin tulevia ohjeita.
Jatka ohjatun toiminnon käyttämistä automaattisesti kirjautumalla Windowsiin.
Lisätietoja TPM:n alustuksesta
Sammuta

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

% ⊦	łallitse TPM-suojauslaitteistoa
Luo	TPM-omistajasalasana
Käytä	i tätä salasanaa TPM-hallintatehtävissä.
•	Luo salasana <u>a</u> utomaattisesti (suositus) Tämä ohjattu toiminto luo salasanan sinulle.
•	Luo salasana <u>m</u> anuaalisesti Ohjattu toiminto auttaa salasanan luomisessa.
Miksi	tarvitsen TPM-omistaiasalasanan?
	Pe

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.

🕞 👔 Hallitse TPM-suc	vjauslaitteistoa
TPM-suojauslait	tteistoa alustetaan, odota
	Tämä voi kestää muutaman minuutin.

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 (Trusted Platform Module) -tur	vapiirin hallinta paikallisessa tietokoneessa	
1 Tiedosto T <u>o</u> iminto <u>N</u> äytä Ikl	kuna O <u>hj</u> e	- 8 ×
🐅 TPM-hallinta paikallisessa tietokon	TPM-hallinta paikallisessa tietokoneessa	Toiminnot
🎾 Komentojen hallinta	Yleiskatsaus ^ ^	TPM-hallinta paikallisessa tietokoneessa 🔺
	Windowstiatekonest jotka eleätiävät TPM (Trusted Platform Modula) euoisuslaittaiston tarjosvat	Alusta TPM
	laajennettuja suojausominaisuuksia sovelluksille. Tämä laajennus näyttää tiedot tietokoneen TPM:stä	 Ota TPM käyttöön
	ja saili jarjesteimanvalvojile laiteen maantysten tekemisen. Jarjesteimanvalvojat volvat myös tarkastella ja hallita laitteen ymmärtämiä komentoja.	Poista TPM käytöstä
		Muuta omistajasalasanaa
	Tila	Poista TPM
	TPM on käytössä ja se on otettu omistukseen.	Nollaa TPM-lukitus
		Näytä
		Uusi ikkuna tähän
	👔 Muuta TPM-omistajasalasanaa. 🚚	Q Päivitä
	👔 Poista omistus tyhjentämällä TPM ja palauta TPM tehdasasetuksiin. 🍃	2 Ohie
	VAROITUS: Jos puhdistat TPM:n, menetät kaikki TPM-avaimet ja niiden suojaamat tiedot.	
	TPM-valmistaian tiedot	
	Valmistaja: INTC Valmistajan versio: 4.1 Maantysversio: 1.2	
	Linkit ja resurssit	
	Mitä tarkoittaa TPM-alustus?	
	Milloin TPM pitää käynnistää tai sammuttaa?	
	Milloin omistajasalasanaa pitää muuttaa?	
	<u>Milloin TPM puhdistetaan?</u>	
	<u>Milloin TPM-lukitus nollataan?</u>	
	Missä on lisätietoja TPM-omistajasalasanasta?	
	Wuinka TPM-komennot estetään ja salitaan?	
	Wuinka TPM-komennon estämiseen liittyvä ryhmäkäytäntö määritetään?	
۰	Ø Missä on lisätietoja TPM-komennoista?	
Päivittää nykyisen valinnan.		

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.

Ohjauspaneeli (4) Reference BitLockeria Suojaa tietokone salaamalla levyllä olevat tiedot	
Näytä lisää tuloksia bitlo × Sammuta	

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

	läriestelmä ja suojaus ▶ Bitl ocker-asemansalaus
Ohjauspaneelin pääikkuna	Auta suojaamaan tiedostojasi ja kansioitasi salaamalla asemat
	BitLocker-asemansalaus auttaa estämään alla näkyvään asemaan tallennettujen tiedostojen luvattoman käytön. Voit käyttää tietokonetta normaalisti, mutta luvattomat käyttäjät eivät voi lukea tai käyttää tiedostojasi.
	Mitä BitLocker-asemansalauksesta tulisi tietää ennen sen käyttämistä?
	BitLocker-asemansalaus - Kiintolevyasemat
	C: C:
Katso myös	BitLocker-asemansalaus - BitLocker To Go
💡 TPM-hallinta	E: Ota BitLocker käyttöön
👂 Levynhallinta	Ei käytössä
Lue tietosuoiatiedot verkossa	

Klikkaa "Ota BitLocker käyttöön" valitsemastasi asemasta.

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

	x
🕞 🏘 BitLocker-asemansalaus (C:)	
Tarkistetaan tietokoneen kokoonpanoa	
BitLocker tarkistaa, että tietokone täyttää sen järjestelmävaatimukset. Tämä saattaa kestää joitakin minuutteja.	
BILLOCKET-asennus edeliyttaa, että järjesteimä on kytketty verkkovirtaan, ennen kuin muutoksia voidaan tehdä. Kytke tietokone verkkovirtaan ja suorita BitLocker-asennus uudelleen.	
Mitkä ovat BitLockerin järjestelmävaatimukset?	
	_
Peruu	ta

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.

	×
bitLocker-asemansalaus (C:)	
Tarkistetaan tietokoneen kokoonpanoa	
BitLocker tarkistaa, että tietokone täyttää sen järjestelmävaatimukset. Tämä saattaa kestää joitakin minuutteja.	
Mitkä ovat BitLockerin järjestelmävaatimukset?	
Pe	ruuta

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).

🚱 🏘 BitLocker-asemansalaus (C:)
Valmistellaan asemaa BitLockeria varten Bitlocker otetaan käyttöön aiemmin luodun aseman tai kiintolevyn varaamattoman vapaan tilan avulla.
 Tiedot Uusi järjestelmäasema luodaan aseman C: vapaasta tilasta. Uudella asemalla ei ole asemakirjainta.
Varoitus: Microsoft suosittelee, että varmuuskopioit tärkeät tiedot ja tiedostot ennen jatkamista. Varmuuskopion tekeminen Varmuuskopiointi- ja palautuskeskuksen avulla
🥼 Tämä saattaa kestää kauan sen mukaan, minkä kokoinen ja miten pirstoutunut asema on.
<u>Miten aseman valmistelu toimii?</u>
S <u>e</u> uraava Peruuta

Paina Seuraava.

🕞 🏘 BitLocker-asemansalaus (C:)
Valmistellaan asemaa BitLockeria varten
Älä katkaise virtaa tietokoneesta tai käynnistä tietokonetta uudelleen, ennen kuin tämä prosessi on tehty loppuun.
Pienennetään asemaa C:
Luodaan uusi järjestelmäasema
Valmistellaan asemaa BitLockeria varten
Tila:
Peruuta

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

🖉 🏘 BitLocker-asemansalaus (C:)
Aseman valmistelu on valmis
Tietokone on käynnistettävä uudelleen, jotta järjestelmäaseman valmistelu BitLockeria varten tehdään loppuun.
Tallenna ja sulje avoimet tiedostot tai ohjelmat ennen uudelleenkäynnistämistä.
Käynnistä uudelleen <u>n</u> yt

Paina "Käynnistä uudelleen nyt".

Salaus alkaa uudelleen käynnistyksen jälkeen määrityksillä:

	x			
🕞 🎭 BitLocker-asemansalaus (C:)				
BitLocker-asemansalauksen määritys				
Tälle tietokoneelle tehdään seuraavat valmistelut, jotta BitLocker voidaan ottaa käyttöön.				
✓ Valmistele asema BitLockeria varten				
Salaa asema				
Mitkä ovat Ritl ockerin järjestelmävaatimukset?				
with over one offering all stering volume volume stering stering stering volume stering sterin				
Seuraava Peruut	a			

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.

6	Regular BitLocker-asemansalaus (C:)
	Miten haluat tallentaa palautusavaimen? Palautusavain ei ole sama kuin PIN-tunnus tai käynnistysavain. Sen avulla voidaan käyttää tiedostoja ja kansioita, jos tietokoneessa ilmennyt ongelma estää tämän.
	Tallenna palautusavain USB-muistitikkuun
	Tallenna palautusavain tie <u>d</u> ostoon
	Tul <u>o</u> sta palautusavain
	Mikä palautusavain on?
	S <u>e</u> uraava Peruuta

USB muistitikku -valinnan jälkeen ohjattu toiminto kysyy avaimen tallennuspaikkaa:

Ta	allenna	palautusavain USB-muistitikkuun
	S.	Liitä USB-muistitikku tietokoneeseen, valitse se luettelosta ja napsauta Tallenna-painiketta.
		Siirrettävä levy (E:)
		Tallenna Peruuta

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

×
G the BitLocker-asemansalaus (C:)
Miten haluat tallentaa palautusavaimen?
Palautusavain ei ole sama kuin PIN-tunnus tai käynnistysavain. Sen avulla voidaan käyttää tiedostoja ja kansioita, jos tietokoneessa ilmennyt ongelma estää tämän.
Tallenna palautusavain USB-muistitikuun
→ Tallenna palautusavain tie <u>d</u> ostoon
→ Tul <u>o</u> sta palautusavain
Palautusavain on tallennettu.
Mikä palautusavain on?
S <u>e</u> uraava Peruuta

Paina "Seuraava".

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

🚱 🎭 BitLocker-asemansalaus (C:)	×				
Oletko valmis salaamaan tämän aseman?					
Valittu asema on C:					
Voit jatkaa työskentelyä aseman salaamisen aikana. Salaus vaikuttaa tio käyttää vapaata levytilaa salauksen aikana.	etokoneen nopeuteen, ja BitLocker				
🕼 Suorita BitLocker-järjestelmätarkistus					
Järjestelmätarkistus varmistaa, että BitLocker voi lukea palautus- ja salausavaimet oikein ennen aseman salaamista.					
Aseta tallennetun palautusavaimen sisältävä USB-muistilaite tietokoneeseen. BitLocker käynnistää tietokoneen uudelleen ennen salausta.					
Huomautus: Tämä tarkistus voi viedä jonkin verran aikaa, mutta sit poistamaan aseman lukituksen palautusavaimen avulla.	ä suositellaan, koska voit joutua				
	Jatka Peruuta				

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.

🍖 BitLo	cker-asemansalaus
	Salataan
	Asema C: 0.4 % valmis
	Sulje

Varsin pitkän kahvitauon jälkeen salaus on valmis.

🗛 BitLo	ocker-asemansalaus	
R	Aseman C: salaaminen on valmis.	
	Sulje	

Paina Sulje.

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

🚱 🗢 🖳 🕨 Tietokon	e 🕨		← ← Hae: Tie	etokone 🔎
Järjestä 🔻 Automaatti	inen toisto Poista Ominai	isuudet Järjestelmän ominaisuu	det »	u= ▼ 🗍 🔞
 ✓ Suosikit ▲ Ladatut tiedostot ■ Työpöytä Wimeisimmät sijainn 	 Kiintolevyasemat (1) Paikallinen levy (C:) 134 Gt vapaana / 148 Laitteet, joissa on siirrett 	Gt ävä tallennusväline (2)		
 ✓ Kirjastot ▷ Kuvat ▷ Musiikki ▷ Tiedostot ▷ Videot ▷ Nietokone ▷ Verkko 	DVD-RW-asema (D:)	Siirrettävä 882 Mt va	levy (E:) paana / 3,89 Gt	
Siirrettävä levy Siirrettävä levy	r (E:) Käytetty tila:	Koko yhteensä: 3,89 G Tiedostojärjestelmä: FAT3	it BitLocke	r-tila: Ei käytössä

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.

X
🕞 🐒 Hallitse TPM-suojauslaitteistoa
Poista TPM-suojauslaitteisto käytöstä Poista TPM-suojauslaitteisto käytöstä käynnistämättä tätä tietokonetta uudelleen antamalla TPM-omistajasalasana.
→ Minulla on omistajasalasanatiedosto
➔ Haluan kirjoittaa omistajasalasanan
Minulla ei ole TPM-omistajasalasanaa
Peruuta

Salasanatiedosto syötetään ohjattuun toimintoon joka poistaa TPM moduulin käytöstä.

	Test and		x
\bigcirc	🐒 Hallitse TPM-suo	jauslaitteistoa	
	Valitse TPM-om	istajasalasanan sisältävä tiedosto	
	<u>T</u> iedoston sijainti:	E:\TUTKIMUS-PC.tpm	
	Tämä tiedosto voi sijait USB-muistitikulla tai CD	a paikallisessa tietokoneessa tai siirrettävässä tietovälineessä (kuten -levyllä).	
		Poista TPM käytöstä	uuta