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.		Johda	anto		6			
2.		Sähk	öpos	ti salattua säiliötä käyttäen	7			
	2.1. Vastaanottaminen (suomenkielinen versio)							
	2.2	2.	Lähe	ttäminen (suomenkielinen versio)1	1			
		2.2.1	•	Salatun säiliön (taltion) luominen1	1			
		2.2.2	•	Salasanavaatimukset ja salasanan välittäminen1	8			
		2.2.3	•	Tiedostojen lisääminen säiliöön (taltioon)1	8			
	2.3	3.	Vast	aanottaminen (englanninkielinen versio)2	0			
	2.4	1 .	Lähe	ttäminen (englanninkielinen versio)2	2			
		2.4.1	•	Salatun säiliön luominen2	3			
		2.4.2	•	Salasanavaatimukset2	7			
		2.4.3	•	Tiedostojen lisääminen säiliöön2	7			
3.		Sähk	öpos	ti toimikorttia käyttäen2	7			
		3.1.1	•	Salatun viestin lähettäminen Outlook -ohjelmalla2	8			
		3.1.2	•	Outlook asetukset	9			
	:	3.1.3	•	Esivalmistelut silloin kun varmennetta ei ole hakemistossa	2			
		3.1.4	•	Varmenteen tallentaminen (export)3	2			
		3.1.5		Varmenteen asentamien Outlookin osoitekirjaan3	7			
		3.1.6		Salatun postin vastaanottaminen4	1			
4.		Salas	sapit	o pähkinän kuoressa4	4			
5.		Salas	sa pi	dettävän tiedon tallentaminen4	6			
	5.1	L.	Vast	aanotetun materiaalin tallentaminen4	6			
	5.2	2.	Vast	aanotetun materiaalin luovuttaminen edelleen4	6			
6.	I	Lähte	eet	4	7			

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.

True	Crypt							х
<u>T</u> altiot	<u>J</u> ärjestelmä	Favor <u>i</u> tes	Työkalut	A <u>s</u> etukset	<u>O</u> hje		Koti	sivu
As	Taltio				Koko	Salausalgoritmi	Тууррі	
Sec:								
С. С								
See 1:								=
С								
Set:								
Sec. 10.								
© 0:								
œQ:								
≪R: ≪S:								-
1								
		1					1	-
	L <u>u</u> o Taltio		Tal	tion Ominaisu	u <u>d</u> et,,	T	/hjennä <u>V</u> älimuisti	
- Taltio								
	C:\Doo	s\TUPO\Sala	isetKansiot			▼ V	alitse Tiedosto	
✓ Älä tallenna historiatietoja								
				1.	altio <u>n</u> Työka	ilut	Valitse Laite	
Y	hdistä Laite	Aut	oyhdistä <u>L</u> ait	teet P	oista Kaikki	Yhteydet	Poistu	

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

Anna Salasana C:\Docs\TUPO\SalaisetKansiot:lle	
Salasana:	ОК
Välimuisti salasanat ja avaintie <u>d</u> ostot muistis:	Peru
─ <u>N</u> äytä Salasana	
Käytä <u>A</u> vaintiedostoja <u>A</u> vaintiedostot	Yhdistä V <u>a</u> linta

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.

Anna Salasana C:\Docs\TUPO\SalaisetKansiot:lle						
Salasana: Hu6t45+rG545QW231ytfe	Hu6t45+rG545QW231ytfe.<<0=8 OK					
🔽 Välimuisti salasanat ja	Välimuisti salasanat ja avaintie <u>d</u> ostot muistis:					
✓ Näytä Salasana						
🗌 Käytä <u>A</u> vaintiedostoja	<u>A</u> vaintiedostot	Yhdistä V <u>a</u> linta				

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

True(Crypt								x
<u>T</u> altiot	<u>J</u> ärjestelmä	Favor <u>i</u> tes	T <u>y</u> ökalut	A <u>s</u> etukset	<u>O</u> hje			Kotis	ivu
As	Taltio				Koko	Salausalgo	ritmi	Тууррі	
 F: G: H: J: J: K: L: M: O: P: Q: R: S: 	C:\pocs\TUP	O\SalaisetKar	nsiot		1.8 MB	AES		Norm	H
Taltio	L <u>u</u> o Taltio		Ta	ltion Ominaisu	u <u>d</u> et		Tyhjer	nnä <u>V</u> älimuisti	
	C:\Docs\TUPO\SalaisetKansiot Valitse Tiedosto Zälä tallenna historiatietoja Taltion Työkalut Valitse Laite								
<u> </u>	oista Yhteys	Aut	oyhdistä <u>L</u> ait	tteet	<u>o</u> ista Kaikki	Yhteydet		Poistu	

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

							×
🕒 🔾 🗢 🗀 🕨 Tietokone 🕨 (f	-:) Pa	ikallinen levy		▼ ↓ ↓ ↓	Hae: (F:) Paikalli	nen levy	Q
Järjestä 🔻 Sisällytä kirjastoor	•	Jaa seuraavan kanssa: 🔻 🛛 Tallenna levylle	Uusi kansio			•	?
_	*	Nimi	Muokkauspäiväm	Тууррі	Koko		
🥽 Kirjastot 📄 Kuvat		🔁 Sähköpostiohje	17.2.2014 11:49	Adobe Acrobat D	649 kt		
🚽 Musiikki							
Tiedostot							
	=						
📜 Tietokone							
🏭 (C:) Local Disk							
👝 (F:) Paikallinen levy							
🖵 (G:) Opiston yhteiset							
🚽 (H:) Kotihakemisto							
⋥ (0:) Oppimateriaali							
🕎 (P:) Kartta-aineistot	-						
1 kohde							

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.

TrueC	rypt								x
<u>T</u> altiot	<u>J</u> ärjestelmä	Favor <u>i</u> tes	T <u>y</u> ökalut	A <u>s</u> etukset	<u>O</u> hje			Kotis	ivu
As	Taltio				Koko	Salausalgori	tmi	Тууррі	A
Sector Secto	C:\Docs\TUP	0\SalaisetKar	nsiot		1.8 MB	AES		Norm	
G: Generation:									
🥯 I:									=
≪#]: ≪#K:									_
œL:									
M:									
0 :									
P:									
₩. 									
S:									Ŧ
	L <u>u</u> o Taltio		Ta	ltion Ominaisu	uu <u>d</u> et		Tyhjennä <u>V</u>	älimuisti	1
						_			-
	C:\Doc	:s\TUPO\Sala	isetKansiot				Valitse Tie	dosto	
	. <u>A</u> lä	tallenna histo	riatietoja	т	altion Työka	alut	Valitse L	aite	
							_		
[1			
Po	oista Yhteys	Aut	oyhdistä <u>L</u> ait	tteet P	<u>o</u> ista Kaikki	Yhteydet	Po	oistu	
Ľ									

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.

TrueCrypt	x
4	Taltion sisältää tiedostoja tai hakemistoja jotka ovat sovelluksen tai järjestelmän käytössä. Pakotettu yhteyden poisto?
	Yes <u>N</u> o

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.

True	Crypt							x
<u>T</u> altiot	<u>J</u> ärjestelmä	Favor <u>i</u> tes	Työkalut	A <u>s</u> etukset	<u>O</u> hje		Kotis	ivu
As	Taltio				Koko	Salausalgoritmi	Тууррі	4 III >
Taltio	L <u>u</u> o Taltio		Ta	ltion Ominais	u <u>d</u> et,,	Tyhj	iennä <u>V</u> älimuisti	
	⊠ <u>Ä</u> lä	tallenna histo	riatietoja	T	altio <u>n</u> Työka		tse Tiedosto alitse Laite	
Y	hdistä Laite	Auto	oyhdistä <u>L</u> ait	tteet F	' <u>o</u> ista Kaikki	Yhteydet	<u>P</u> oistu	

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

Opastettu TrueCrypt-taltion luonti	
	Opastettu TrueCrypt Taltion Luonti
	Luo salattu tiedostosäilö
	Luo virtuaalisesti salattu levy tiedoston sisälle. Tämä valinta on suositeltava aloittelijalle.
	Lisätietoa
	🔘 Salaa tavallinen osio/asema
	Salaa olemassa oleva sisäinen tai ulkoinen asema tai esimerkiksi muistitikku, eli. D:, E: -asema jne.
	🔿 Salaa järjestelmäasema (osio) tai koko kiintolevy
L R	Salaa järjestelmäasema/osio, jolle Windows on asennettu, esim. C:-asema. Tämän jälkeen tietokoneen käynnistys edellyttää aina salasanan antamista.
	Lisätietoa järjestelmän salauksesta
	<u>O</u> hje < <u>T</u> akaisin <u>S</u> euraava > <u>P</u> eruuta

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

Opastettu TrueCrypt-taltion luonti	
	Taltion Tyyppi
	Standardi TrueCrypt taltio Valitse tämä valinta jos haluat luoda tavallisen TrueCrypt taltion.
	Piįlotettu TrueCrypt taltio Näin voi tapahtua kun olet pakotettu paljastamaan jollekin salatun taltion salasanan. On monta tilannetta jossa et voi kieltäytyä paljastamasta salasanaa (esimerkiksi, kiristyksessä). Käytä niin kutsuttua piilotettua taltiota, jolloin tällaisia pakotettuja salasanan luovuttamisia taltiolle ei tapahdu.
L R	<u>Lisätietoa piilotetuista taltioista</u>
	<u>O</u> hje < <u>T</u> akaisin <u>Seuraava ></u> <u>P</u> eruuta

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

Opastettu TrueCrypt-taltion luonti	
	Taltion Tyyppi
	Standardi TrueCrypt taltio
	Valitse tämä valinta jos haluat luoda tavallisen TrueCrypt taltion.
	O Pijlotettu TrueCrypt taltio
	Näin voi tapahtua kun olet pakotettu paljastamaan jollekin salatun taltion salasanan. On monta tilannetta jossa et voi kieltäytyä paljastamasta salasanaa (esimerkiksi, kiristyksessä). Käytä niin kutsuttua piilotettua taltiota, jolloin tällaisia pakotettuja salasanan luovuttamisia taltiolle ei tapahdu.
	Lisätietoa piilotetuista taltioista
	<u>O</u> hje < <u>T</u> akaisin <u>Seuraava ></u> <u>P</u> eruuta

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

Opastettu TrueCrypt-taltion luonti	
	Taltion sijainti
TRUECRYP	C:\Docs\TUPO\SalaisetKansiot ✓ ✓ Älä tallenna historiatietoja TrueCrypt taltio voi sijaita tiedostossa (kutsutaan TrueCrypt säilöksi), joka voi sijaita esim. kovalevyllä, USB muistissa. TrueCrypt säilö on kuin mikä tahansa tavallinen tiedosto (sitä voidaan esimerkiksi, siirtää, kopioida ja tuhota kuten tavallista tiedostoa). Paina 'Valitse Tiedosto' valitaksesi tiedostonimen säilölle sekä sen sijainnin. VAROITUS: Jos valitset olemassa olevan tiedoston, TrueCrypt El salaa sitä; tiedosto tuhotaan ja korvataan uudella luodulla TrueCrypt säilöllä. Sinun on mahdollista salata olemassa oleva tiedosto (jälkikäteen) siirtämällä ne TrueCrypt säilöön, jota olet nyt luomassa.
	<u>O</u> hje < <u>T</u> akaisin <u>S</u> euraava > <u>P</u> eruuta

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.

Opastettu TrueCrypt-taltion luonti	
	Salauksen Valinnat Salausalgoritmi AES Iesti FIPS hyväksytty koodaus (Rijndael, julkaistu 1998), jota voidaan käyttää U.S. hallituksen osastojen ja toimistojen luottamuksellisten tietojen suojaukseen huippusalaisella tasolla. 256-bitin avain, 128-bitin lohko, 14 kierrosta (AES-256). Toimenpide tila on XTS. Lisätietoa AES Benchmark Hash algoritmi Tietoa hash algoritmeista
	<u>O</u> hje < <u>T</u> akaisin <u>S</u> euraava > <u>P</u> eruuta

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

Opastettu TrueCrypt-taltion luonti	
	Salauksen Valinnat
	Salausalgoritmi Testi AES Image: Testi FIPS hyväksytty koodaus (Rijndael, julkaistu 1998), jota voidaan käyttää U.S. hallituksen osastojen ja toimistojen luottamuksellisten tietojen suojaukseen huippusalaisella tasolla. 256-bitin avain, 128-bitin lohko, 14 kierrosta (AES-256). Toimenpide tila on XTS. Lisätietoa AES Benchmark
L H	Hash algoritmi
	<u>Q</u> hje < <u>T</u> akaisin <u>S</u> euraava > <u>P</u> eruuta

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

Opastettu TrueCrypt-taltion luonti	x
Image: Construction doting Taltion Koko Image: Construction doting Image: Construction doting Image: Constructing doting doting Image: Constructing do	
Note that the minimum possible size of a FAT volume is 292 KB. The minimum possible size of an NTFS volume is 3792 KB. Ohje < Takaisin Qhje < Takaisin	

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.

F	Opastettu TrueCrypt-taltion luonti	
	TBUECBAPT	Taltion Salasana: Salasana: Hu6t45+rG545QW231ytfe.<<0=8 Vahvista: Hu6t45+rG545QW231ytfe.<<0=8 Käytä Avaintiedostoja Najytä Salasana On erittäin tärkeää että valitset hyvän salasanan. Sinun tulee välttää sellaisia jotka sisältävät vain yhden sanan joka voidaan löytää sanakirjasta (tai yhdistelmää 2, 3, tai 4 vastaavia sanoja). Sen ei pidä sisältää mitään nimeä tai syntymäpäivää. Ei pidä olla helposti arvattavissa. Hyvä salasana on satunnainen yhdistelmä isoja ja pieniä kirjaimia, numeroita, ja erikoismerkkejä kuten @ ^ = \$ * + jne. Suosittelemme valitsemaan salasanaan useamman kuin 20 merkkiä (mitä pitempi sitä parempi). Maksimi pituus on 64 merkkiä.
		Ohje < Takaisin Seuraava > Peruuta

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:

Opastettu	TrueCrypt-taltion luonti
8	Virhe: Salasana täytyy sisältää vain ASCII merkkejä. Ei-ASCII merkit salasanassa saattaa aiheuttaa sen ettei taltiota voida yhdistää kun järjestelmä konfiguraatio muuttuu. Seuraavat merkit ovat sallittuja: !"#\$%&'()*+,/0123456789:;<=>?@ABCDEFGHI JKLMNOPQRSTUVWXYZ[\]^_`a bcdefghijklmnop qrstuvwkyz{ }~
	ОК

Opastettu TrueCrypt-taltion luonti	
TBUECBYPT	Valinnat Järjestelmä FAT Ryhmä Oletus Dynaaminen Satunnaisluku: 478262FBF492669CC3575E8308C1CA31 Otsikkoavain: Pääavain: Valmis Nopeus Jäljellä TÄRKEÄÄ: Sirrä hiirtäsi satunnaisesti tässä ikkunassa. Mitä kauemmin siirrät sen parempi. Tämä merkittävästi kasvattaa salausavaimen vahvuutta. Paina 'Alusta' luodaksesi taltion.
	<u>O</u> hje < <u>T</u> akaisin <u>A</u> lusta Lopetus

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:

🗲 🗢 🖛 🕨 Tietokone 🔸 (F	:) Pa	ikallinen levy		• 4 ₇ 1	Hae: (F:) Paikali	inen levy	/	
Järjestä 🔻 Sisällytä kirjastoon	-	Jaa seuraavan kanssa: 👻 🛛 Tallenna levylle	Uusi kansio			823	•	2
🛚 🌙 Musiikki	^	Nimi	Muokkauspäiväm	Тууррі	Koko			
Tiedostot		🔁 Sähköpostiohje	17.2.2014 11:49	Adobe Acrobat D	649 kt			
🖻 🛅 Videot		TUPOv2.1	23.11.2012 12:30	Microsoft Word -a	46 kt			
🖳 Tietokone								
🏭 (C:) Local Disk								
🗅 👝 (F:) Paikallinen levy								
🕞 🙀 (G:) Opiston yhteiset	=							
🛛 🖵 (H:) Kotihakemisto								
🖻 🙀 (O:) Oppimateriaali								
P 👷 (P:) Kartta-aineistot	8							
(Q) Forcontent levy (Q) Forcontent levy (Q) Forcontent levy								
▷ 📔 E52	-							
2 kohdetta								

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.

TrueC	rypt							E	- 0	×
Volumes	System	Favor <u>i</u> tes	T <u>o</u> ols	Settings	<u>H</u> elp				Home	gage
Drive GE: GE: GI: GI: GI: GI: GI: GI: GI: GI	Volume					Size	Encryption	algorithm	Туре	H
Volume	Create Volur	ne ocs\TUPO\Sa ever save his	alaisetKar tory	⊻olume I Isiot	Properties Vol	5 ume <u>T</u> ool:	.	<u>Wi</u> pe Select Select I	Cache t <u>F</u> ile D <u>e</u> vice	
	<u>M</u> ount	A	uto-Moun	t Devices		Di <u>s</u> moun	nt All		E <u>x</u> it	

c) Paina Mount painiketta, jolloin ohjelma kysyy salasanaa.

Enter password for C:\Docs\TUPO\SalaisetKansiot								
Password:		ОК						
Cache passwords and	Cancel							
Use keyfiles	Keyfiles	Mount Options						

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.

Enter password for C:\Docs\TUPO\SalaisetKansiot								
Password: Ktyns452GR5?jih2321Xssa_k#y OK								
Cache passwords and Display password	Cache passwords and keyfiles in memory							
U <u>s</u> e keyfiles	Keyfiles	Mount Options						

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

TrueC	rypt								- 0	×
Volumes	S <u>y</u> stem	Favor <u>i</u> tes	T <u>o</u> ols	Settings	<u>H</u> elp				Homep	age
Drive	Volume					Size	Encryption	n algorithm	Туре	
9 F: 9 J: 9 J: 9 J: 9 J: 9 J: 9 M: 9 M: 9 K: 9 M: 9 K: 9 V: 9 V:	C: \Docs\TL	IPO \SalaisetK	ansiot			1.8 MB	AES		Normal	III
<u>(</u>	<u>O</u> reate Volur	ne		<u>V</u> olume I	Propertie	s		<u>W</u> ipe	Cache	
Volume	c:\p □ №	ocs\TUPO\Sa ever save his	alaisetKar tory	isiot	Vo	lume <u>T</u> ool	▼ s	Select	t <u>F</u> ile D <u>e</u> vice	
	Dismount	A	uto-Moun	t Devices		Dismour	nt All		E <u>x</u> it	

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

						×
🔾 🗢 🖘 Tietokone 🕨 (F:)	lae: (F:) Paikalli	nen levy	٩			
Järjestä 🔻 Sisällytä kirjastoon 🔹	🔹 Jaa seuraavan kanssa: 💌 Tallen	nna levylle Uusi kansio				0
A	Nimi 🔨	Muokkauspäiväm	Тууррі	Koko		
🥽 Kirjastot 📄 Kuvat	🔁 Sähköpostiohje	17.2.2014 11:49	Adobe Acrobat D	649 kt		
🎝 Musiikki						
Videot						
E Tietokone						
🛖 (P:) Kartta-aineistot 🗸						
1 kohde						

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.

TrueCrypt	- • ·
<u>V</u> olumes System Favor <u>i</u> tes T <u>o</u> ols Settings <u>H</u> elp	Home <u>p</u> age
Drive Volume Size Encryption algorithm	Туре
E: CUDeceVT IPO/Selaice#/appint 1.8 MP AES	Normal
	Norma
	=
≪™M: ≪≣a N•	
S:	
₩U:	
₩V:	-
	,
<u>C</u> reate Volume <u>V</u> olume Properties <u>Wip</u>	e Cache
Volume	
C:\Docs\TUPO\SalaisetKansiot	ect File
Never save history	
Volume Tools Selec	t D <u>e</u> vice
Dismount Auto-Mount Devices Dismount All	Evit
	<u>L'Vir</u>

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.

TrueCrypt		- 23
1	Volume contains files or folders being used by applications or system. Force dismount?	
	Kyll <u>ä</u> E <u>i</u>	

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.

TrueC	rypt								- 0	×
Volumes	System	Favor <u>i</u> tes	T <u>o</u> ols	Settings	<u>H</u> elp				Home	age
Drive	Volume					Size	Encryption a	algorithm	Туре	_
€:								-		
Sin F:										
······································										
≪ж:										-
See L:										-
See N:										
≪≥R:										
S:										
≪ v :										
🥯 W:										Ŧ
(Create Volur	ne		Volume I	Propertie	s		Wipe	Cache	
				1			_			
Volume	-									
							-	Select	t <u>F</u> ile	
		ever save his	tory							
					Vo	ume <u>T</u> ool	s	Select [Device	
					1				F (1)	
	Mount	A	uto-Moun	t Devices		Dismour	nt All		Exit	

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.

TrueCrypt Volume Creation Wizard	
	Volume Location
	C:\pocs\TUPO\SalaisetKansiot2 Select <u>File</u>
	Never save history
	A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.
TRL	WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.
	Help < Back Next > Cancel

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.

TrueCrypt Volume Creation Wizard	
TRUECBYPT	Encryption Algorithm Encryption Algorithm FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS. More information on AES Benchmark Hash Algorithm RIPEMD-160 Information on hash algorithms
	Help < Back Next > Cancel

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.

TrueCrypt Volume Creation Wizard	
TRUECRYPT	Volume Size CKB MB CGB Free space on drive C:\ is 241.32 GB Please specify the size of the container you want to create. If you create a dynamic (sparse-file) container, this parameter will specify its maximum possible size. Note that the minimum possible size of a FAT volume is 292 KB. The minimum possible size of an NTFS volume is 3792 KB.
	Help < Back Mext > Cancel

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.

TrueCrypt Volume Creation Wizard	
TRUECBYPT	Volume Password Password: $hyTR56 #gtBhEEddpo0980!!q$ Confirm: $hyTR56 #gtBhEEddpo0980!!q$ Uge keyfiles Display password X is very important that you choose a good password. You should an adictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ $h = s^{*} +$ etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum possible length is 64 characters.
	Help < Back Next > Cancel

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.

TrueCrypt Volume Creation Wizard	
CRYPT	Volume Format Options Filesystem FAT Cluster Default Dynamic Random Pool: C2DDDE8B9D95351C23538F7AD4515EC4 Random Key: Master Key:
TRUE	Abort Done Speed Left IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then dick Format to create the volume. Help < Back Eormat Cancel

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:

G v → Tietokone → (F	F:) P	aikallinen levy		▼ 4 ₂	Hae: (F:) Paikallii	nen levy	<u>×</u>
Järjestä 🔻 Sisällytä kirjastoon	•	Jaa seuraavan kanssa: 🔻 🛛 Tallenna levylle	Uusi kansio			800 -	0
🖻 🎝 Musiikki	*	Nimi	Muokkauspäiväm	Тууррі	Koko		
Tiedostot		🔁 Sähköpostiohje	17.2.2014 11:49	Adobe Acrobat D	649 kt		
🖻 🛅 Videot		TUPOv2.1	23.11.2012 12:30	Microsoft Word -a	46 kt		
↓ Titetokone ▶ G(2) Coal Disk ▶ G(2) Coal Disk ▶ G(2) Paikallinen levy ▶ G(2) Opiton yhteiset ▶ G(2) Arita-sineistot ▶ G(2) Kuva-sineistot ▶ G(2) Kuva-sineistot ▶ G(2) Z	E F						
2 kohdetta							

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.

🛐 🛃 🍠 😈 🐟 🗇 🛛 🗢 🕅	- e X
Tiedosto Viesti Lisää Asetukset Muotoile tekstiä Tarkista	۵ 😮
Image: Second	nitusta suoraan vastaanottajalle ia a
Vastaanottaja Silvennoinen Juhani PeO (Juhani. Silvennoinen @pelastusopisto.fi) Lähetä Kopio	
Sähköpostiohje	() () () () () () () () () () () () () (
Marko Hassinen Researcher, Ph.D. <u>marko.hassinen@pelastusopisto.fi</u> +358 50 596 6922 +358 29 5453423	=
Emergency Services College P.O. Box 1122 FI-70821 KUOPIO	V
1 Lisätietoja: Silvennoinen Juhani.	A .

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

\/		+ - + +	مالم منابلة منام
varmennenakemisto lisataa	in (ellel sita jo ole	e asetettu) Ousi	-ратліккееца.

iă uusi tili	
Kansion tai osoitteiston laji Voit valita lisättävän kansion tai osoitteen lajin.	
Internet-hakemistopalvelu (LDAP)	
Yhdistä LDAP-palvelimeen sähköpostiosoitteiden ja muiden tietojen et tarkistamista varten.	tsimistä ja
🔘 Lisää osoitteistoja	
Yhdistä osoitteistoon sähköpostiosoitteiden ja muiden tietojen etsimis tarkistamista varten.	stä ja
	< Edellinen 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 ha	un (LDAP) asetukset akemistopalvelun tietojen käytössä vaadittavat asetukset.	×
Palvelimen tiedot		
Kirjoita sen hakemisto määrittänyt sinulle.	opalvelun nimi, jonka Internet-palveluntarjoaja tai järjestelmänvalvoja on	
Palvelimen <u>n</u> imi:	ldap, fineid, fi	
Kirjaustiedot		
🔲 T <u>ä</u> mä palvelin vaa	ıtii kirjautumisen	
<u>K</u> äyttäjänimi:		
S <u>a</u> lasana;		
Vaadi suojattu	ia salasanan vahvistusta (Secure Password Authentication)	
	Lisää asetuksia	
	< Edellinen Seuraava > Peru	Juta

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

Microsoft LDAP-hak	emisto	×
Yhteys Etsintä		
Näyttönimi		
Näyttönimi osoitt	eiston mukaisessa muodossa	
Varmennehak	emisto (fineid)	
Yhteyden tiedot		
Portti:	389	
K <u>ä</u> ytä SSL-yhteyttä		
	OK Peruuta K <u>ä</u> y	tä

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.

Microsoft LDAP-hakemisto	×
Yhteys Etsintä	
Palvelimen asetukset	
Etsinnän aikakatkaisu sekunteina:	60
Määritä onnistuneen etsinnän jälkeen näytettävien kohteiden enimmäismäärä:	100
Etsintäperuste	
◯ Käy <u>t</u> ä oletusta	
Mukautettu: dmdName=fineid,c=fi	
Selaaminen	
Ota selaaminen käyttöön (edellyttää tukea p	alvelimessa)
OK Peruuta	K <u>ä</u> ytä

Tallenna asetukset painamalla OK, Seuraava, Valmis.

Tiliasetukset				×
Kansiot ja osoitteistot Voit valita muutettavan tai poistettava	an kansion tai osoitteiston alla	olevasta luettelosta.		
Datatiedostot RSS-syötteet SharePoint-	uettelot Internet-kalenterit	Julkaistut kalenterit	Osoitteistot	4 >
🗓 Uusi 🚰 Muuta 🗙 Poista				
Nimi	Laji			
Outlook-osoitteisto	MAPI			
Varmennehakemisto	LDAP			
Varmennehakemisto (fineid)	LDAP			
			<u>S</u> u	lje

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

<u>@</u> \	/äestörekiste	erikeskus \	ARMENNEHA	AKU VARMENNEHAKEMISTOS	TA - Mie	crosoft I	nternet Expl	orer prov	ided by Pelas	tusopisto			x
0	http://vrk. f i	neid.fi/cer	tsearchB.asp?	state=search&issuercn=VRK+	CA+for+	+ Qualifi	ed+Certifica	tes&lasti	name=Hassin	en&firstname:	=Marko&finuid=	:	8
											Sulje	ikkuna	1
v													
Kir	ioita hakuel	hto alla ol	eviin kenttiin.	1131031A									
Vo	it käyttää * -	merkkiä k	atkaisumerkk	tinä.									
На	ku palautta	a maksim	iissaan 100 v	armennetta.									
Va	rmenteen r	nyöntäjä	(CA)										
C	VRK Gov.	CA for Ci	tizen Qualifie	d Certificates									
C	VRK Gov.	CA for Ci	tizen Qualifie	d Certificates - G2									
۲	VRK CA f	or Qualifie	d Certificates	1									
0	VRK CA f	or Qualifie	d Certificates	<u>- G2</u>									
	VRK CA f	or Service	Providers										
		or Service	Providers - G	i <u>Z</u> Irouidara									
		or Healthc	are Service P	nole Qualified Certificates									
Su	kunimi:	orricaline	arer rolessi	Etunimi:	Tunnus	s:							
E	assinen			Marko				1					
	Lieää baki	itulokeiin	myös allakiri	oitusvormenteet									
	LISda IIdku	luioksiin	inyus alleniiji	Lataa culkulista		Etcivor	montoot	1					
				Lataa sulkulista	<u> </u>	Etai vai	menteet						
Ha	aun tulokse	t											
#	Sukunimi	Etunimi	Tunnus	Sähköposti		Käyttö	Lataa va	rmenne	Hex				
1	Hassinen	Marko	910582873	marko.hassinen@pelastus	opisto.fi	🏨 V	20003	92825	773B9279				
2	Hassinen	Marko	910582873	marko.hassinen@pelastus	opisto.fi	<u>i</u> , v	20004	<u>60512</u>	773C9AE0				
													Ŧ
											a 1	00%	•

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).

Internet-asetukset	? 🗙
Yleiset Suojaus Tietosuoja Sisältö Yhteydet Ohjelmat Lisä	iasetukset
Sisällönvalvonta Luokituksia käyttämällä voit määrittää, millaista Interne tällä tietokoneella voidaan katsella.	t-sisältöä
😵 Ota käyttöön 🧕 🛞 Asetuk	set
Varmenteet	
Käytä varmenteita salattuihin yhteyksiin ja tunnistamise	een.
Tyhjennä SSL-tila Varmenteet Julkaisija	at
Automaattinen täydennysAutomaattinen täydennys tallentaaAsetukse	et
aiemmin WWW-sivuilla kirjoitetut tiedot ja ehdottaa niitä jatkossa.	
Syötteet ja Web Slices -linkit	
Syötteet ja Web Sikces -linkit tarjoavat päivitettyä sisältöä, jota voidaan lukea Internet Explorerilla ja muilla ohjelmilla.	et
	Käytä
OK Peruuta	Ngyta

I dial I a a			1
nkilokohtainen Muut her	ikilöt Keskitason varment	teiden myöntäjä	it Luotetut varmen
Myönnetty	Myöntäjä	Vanhentu	Kutsumanimi
Hassinen Marko 91	VRK CA for Qualified	2.7.2018	<ei mitään=""></ei>
🙀 Hassinen Marko 91	VRK CA for Qualified	2.7.2018	<ei mitään=""></ei>
<u>I</u> uo	Poista		Lisäaset
<u>Tuo</u> <u>Vi</u> e menteiden suunnitellut k	Poista		Lisäaset

Varmenteet			×
Suunniteltu käyttötarkoitus:	<kaikki></kaikki>		•
Henkilökohtainen Muut hen	kilöt Keskitason varment	eiden myöntäjä	t Luotetut varmente
Myönnetty	Myöntäjä	Vanhentu	Kutsumanimi
Hassinen Marko 91	VRK CA for Qualified	2.7.2018	<ei mitään=""></ei>
🚟 Hassinen Marko 91	VRK CA for Qualified	2.7.2018	<ei mitään=""></ei>
marko.hassinen@p	Communications Server	29.11.2014	<ei mitään=""></ei>
<u>T</u> uo <u>V</u> ie	<u>P</u> oista		Lisäasetukset
Varmenteiden suunnitellut kä <kaikki></kaikki>	iyttötarkoitukset		
			Näytä
Lisätietoja <u>varmenteista</u>			Sulje

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

Ohjattu varmenteiden viemir	nen 🗧	Ohjattu varmenteiden vieminen
	Tervetuloa ohjattuun varmenteiden viemiseen	Yksityisen avaimen vieminen Voit määrittää yksityisen avaimen vietäväksi varmenteen kanssa.
	Tämän ohjatun toiminnon avulla voit kopioida varmenteita ja varmenteiden luottamus- sekä kumousluetteloita varmenesäilöstä levylle. Varmenne vahvistaa henkilöllisvytesi ja sisältää tiedon	Yksityiset avaimet suojataan salasanalla. Jos haluat viedä avaimen varmenteen kanssa, sinun on annettava salasana myöhemmin tässä ohjatussa toiminnossa.
	suojauksessa ja suojattujen verkkoyhteyksien muodostamisessa käytettäviä betoja. Varmennesällö on järjestelmän alue, jossa varmenteita säilytetään.	Haluatko viedā yksityisen avaimen varmenteen mukana? <u>Kyllā. Vie yksityinen avain.</u> <u>E. Aļa vie yksityistā avainta.</u>
	Jatka valitsemalla Seuraava.	Huomautus: Liitetty yksityinen avain on merkitty ei-vietäväksi. Vain varmenne voidaan viedä.
		Lisätietoja <u>vksitvisten avainten viemisestä</u>
	< Edellinen Seuraava > Peruuta	< Edelinen Seuraava > Peruuta

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

Ohjattu varmenteiden vieminen	Ohjattu varmenteiden vieminen
Viennin tiedostomuoto Varmenne voidaan viedä useissa eri tiedostomuodoissa.	Vietävä tiedosto Määritä vientitiedoston nimi
Valitse käytettävä muoto:	Tjedostonimi:
◎ DER-koodattu binaari-X.509 (.cer)	MarkoHassinen1 Selaa
Base64-koodattu X.509 (.cer)	
Cryptographic Message Syntax Standard – PKCS #7 -varmenteet (.p7b)	
Sis <u>ä</u> llytä kaikki varmennuspolun varmenteet, jos mahdollista	
<u>H</u> enkilökohtaisten tietojen vaihtaminen - PKCS #12 (.pfx)	
Sisällytä kaikki varmennuspolun varmenteet, jos mahdollista	
Poista yksityinen <u>a</u> vain, jos vienti onnistuu	
🗌 Vie kaikki laajennetut ominaisuudet	
O Microsoftin sarjoitettu varmennesäilö (.sst)	
Lisätietoja <u>varmennetiedostomuodoista</u>	
< Edellinen Seuraava > Peruuta	< Edelinen Seuraava > Peruuta

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

Ohjattu varmenteiden vieminen			Ì
	Viimeistellään ohjattua varmenteiden viemistä		
	Ohjattu varmenteen vieminen onnistui.		
	Olet määrittänyt seuraavat asetukset:		
	Tiedostonimi	C:\Use	
	Vientiavaimet	Ei	
	Sisällytä kaikki varmenteet varmennuspolussa	6	
	Tiedostomuoto	Base64	
	4	•	
	< Edellinen Valmis	Peruuta	
		. c. sutu	



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.

		Järjestä 🔻	Sisällytä kirjastoo	י ו	Jaa seuraavan kanssa: 🔻	Tallenna levylle	Uusi kansio					0
X	Leikkaa			^	Nimi		Muokkauspäiväm	Тууррі	Koko			
4	Kopioi		it tiedostot		MarkoHassinen1.txt		27.6.2014 23:12	Tekstitiedosto		3 kt		
	Liita		ytä		📮 MarkoHassinen2.cer		27.6.2014 23:22	Suojausvarmenne		3 kt		
	Tee uudelleen		simmät sijainnit									
	Valitse kaikki			=								
	Asettelu	•	ki									
	Kansion ja haun ase	etukset	tot									
X	Poista											
	Nimeä uudelleen											
	Poista ominaisuude	et	1e									
	Ominaisuudet		cal Disk									
	Sulje		oiston yhteiset otihakemisto									
_		🙀 (0:) O	ppimateriaali									
		🤜 (P:) Ka	rtta-aineistot	*								
		2	kohdetta									

Seuraavaksi Näytä välilehdeltä poistetaan Piilota tunnettujen tiedostotyyppien tunnisteet kohdasta rasti.

Kansion asetukset	×
Yleiset Näytä Haku	
Kansionäkymät Voit ottaa käyttöön tämän kansion näkymän (kuten Tiedot tai Kuvakkeet) muille tällaisille kansioille. Käytä kansioille Palauta kansiot	
Lisäasetukset:	
 Näytä salatut ja pakatut NTFS-tiedostot erivärisenä Näytä tiedostokoko kansiovihjeissä Näytä tiedostokuvake pikkukuvissa Palauta edelliset kansionäkymät kirjautumisen yhteydessä Piliota suojatut käytöjärjestelmätiedostot (suositus) Piliota Tietokone-kansion tyhjät asemat Piliota tunnettujen tiedostotyyppien tunnisteet Pilotatut tedostot ja kansiot Näytä pillotetut tiedostot, kansiot ja asemat Näytä pillotettu ja tiedostoja, kansiotta tai asemia Valitse kohteet valintaruuduilla 	▲ E
Palauta oletusarv	rot
OK Peruta Kāy	tä

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

C v l v se	rtifikaatit			✓ 4 ₁	Hae: sertifikaatit		٩
Järjestä 🔻 💼	Avaa 🔻 Tallenna levylle U	lusi kansio				:≡ - [. ?
쑦 Suosikit	^ Nimi	*	Muokkauspäiväm	Тууррі	Koko		
📙 Ladatut tiedo	stot 🗔 MarkoHass	inen1.cer	27.6.2014 23:12	Suojausvarmenne	3 kt		
 Työpöyt Wiimeisin Kirjastot Kuvat Musiikki Tiedosto Videot 	Avaa Asenna varmenne Avaa sovelluksessa → Scan for threats WinZip → Palauta aiemmat versiot Lähetä kohteeseen: →	inen2.cer	27.6.2014 23:22	Suojausvarmenne	3 kt		
🖳 Tietokone 🏝 (C:) Loci 🖵 (G:) Opi:	Leikkaa Kopioi Luo pikakuvake						
🚍 (H:) Koti	Poista						
🖵 (0:) Opp	Nimeä uudelleen						
Ma	Ominaisuudet	27.6.2014 23:12 Luo	mispäivä: 27.6.2014 23:12	2			
Suojausv	/armenne Koko:	2,27 kt					

Avautuvaan dialogiin vastataan Kyllä.

Nimeä	uudelleen
	Tiedostotunnisteen muuttaminen voi aiheuttaa sen, että tiedostoa ei voi enää käyttää. Haluatko varmasti muuttaa tiedostotunnistetta?
	<u>Kyllä</u> <u>E</u> i

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

						E		×
😋 🔍 🗢 📕 🕨 sertifikaatit				• 4 ₇	Hae: sertifikaatit			٩
Järjestä 🔻 📗 Avaa 🔻	Tulost	ta Tallenna levylle Uusi kansio				8== •	-	0
🔶 Suosikit	*	Nimi	Muokkauspäiväm	Тууррі	Koko			
🚺 Ladatut tiedostot		MarkoHassinen1.txt	27.6.2014 23:12	Tekstitiedosto	3 kt			
📃 Työpöytä		🔄 MarkoHassinen2.cer	27.6.2014 23:22	Suojausvarmenne	3 kt			
📃 Viimeisimmät sijainnit								
S Mitchel								
Kinjastot	=							
Musiikki								
Tiedostot								
Videot								
🖳 Tietokone								
🏭 (C:) Local Disk								
G:) Opiston yhteiset								
(H:) Kotihakemisto								
(0:) Oppirriateriaan	-							
MarkoHassinen1.txt Tekstitiedosto	t Muo	kkauspäiväm 27.6.2014 23:12 Koko: 2,27 kt	Luomispäivä: 27.6.2014 23:12					

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

Command Prompt	×
C:\Users\p47826\Desktop\sertifikaatit>dir Aseman C nimi on Local Disk Aseman sarjanumero on 3265-3E1A	-
Kansio C:\Users\p47826\Desktop\sertifikaatit	
27.06.2014 23:26 <kansio> . 27.06.2014 23:26 <kansio> . 27.06.2014 23:12 2 330 MarkoHassinen1.txt 27.06.2014 23:22 2 214 MarkoHassinen2.cer 27.06.2014 23:22 4 544 tavua 2 tiedosto(a) 4 544 tavua 2 kansio(ta) 254 626 140 160 tavua vapaana</kansio></kansio>	
C:\Users\p47826\Desktop\sertifikaatit>move MarkoHassinen2.cer MarkoHassinen2.txt	=
1 tiedosto(a) on siirretty.	
C:\Users\p47826\Desktop\sertifikaatit>dir Aseman C nimi on Local Disk Aseman sarjanumero on 3265-3E1A	
Kansio C:\Users\p47826\Desktop\sertifikaatit	
30.07.2014 00:04 (KANSIO) 30.07.2014 00:04 (KANSIO) 27.06.2014 23:12 2 330 MarkoHassinen1.txt 27.06.2014 23:22 2 214 MarkoHassinen2.txt 2 tiedosto(a) 4 544 tavua 2 kansio(ta) 254 626 136 064 tavua vapaana	
C:\Users\p47826\Desktop\sertifikaatit>	
	-

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:

0 📑 🤊 📼			Sai	apuneet - Marko.Hassinen@pelastusopisto.fi -	Microsoft Outlook		
Tiedosto Aloitus Lähetä tai	vastaanota Ka	nsio Näytä	McAfee E-mail Scan				۵ 🚱
Uusi Uudet sähköpostiviesti kohteet •	hita hjennā • oskaposti •	Vastaa Vastaa kaikille	Alitä Kokous Vältä Visää *	Image: State	Siirrä Säännöt OneNote	Lukemator/luettu Luokittele Seurar	- Etsi yhteystieto III Osoitteisto ▼ Suodata sähköposti ~
Uusi	Poista		astaa	Pikatoiminnot	ia Siirra	lunnisteet	ETSI
Subsikit Saapuneet Marko.Hassinen@pelastusopi Marko.Hassinen@pelastusopist	sto.f	uneet (Ctrl+E) 🔎	VS: Testaus UK_kokkola_ Vastasit viestiin 5/ Lähetetty: ti 5/8.	kangasvieri_jukka 8.2014 11:58. 2014 11:11			 elokuu 2014 ma ti ke to pe la su 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 21 31 44 15 16 17
Gaspuneet AIRBEAM Luonnokset Lähetetyt O Poistetut (1)	E Contraction Cont	kola 07 aus 0 c 6 kola 07	Vastaanottaja: Ha Esikatselu Avaa Pikatulogtus	ssinen Marko PeO	KangasvieriJukka2Allekirjoittan	nisVarmenne.txt (β kt) ⊘	→ 18 19 20 21 22 23 24 ⇒ 25 26 27 28 29 30 31 → 1 2 3 4 5 6 7 Tăm5 păivă Lourno 12:30 - 14:00
 Ge Hakukansiot Keskusteluhistoria Lähtevät Koskaposti [26] RSS-syötteet Arkistot 	A elien Constant	77-5- 07 55%- 12.3 07	Tallenna nimellä Tallenna kalkki Poista liite Koploi Yalltse kaikki	s a late at a version of the second sec	ada da ngana binang sa tain at	ମା ଭିଷି ମଧ୍ୟରି ୩୦ ମନ୍ଦି ମହା ବରିବେ 🚃	webex Huominen Scherologi ochtron Serviciaen Scharong Leiskowa Sirickon maanantai
Arkistot Poistetut Hakukansiot Sähköposti	Carrier Carrier Carrier Carrier Carrier Viene v	in see	Lähettäjä: Hassi Lähetetty: 5. elo Vastaanottaja: Aihe: VS: Testau	nen Marko PeO [<u>mailto:Marko.Hassinen@</u> ikuuta 2014 10:27 Kangasvieri Jukka s	pelastusopisto.fi]		2 tapaamista
Kalenteri	BED RED Control VSISE	90 8	Jos haluat nähdä ta	imän henkilön sosiaalisten verkkojen päivityks	et ja sähköpostiviestit, napsauta ku		artaniel V Martines Control Carlos V De control Carlos V
🏹 Tehtävät	PR. 7 Faropi Resilin	90	\bigcirc				A Usein adytetyt ymersie oot a Usein adytetyt ymersie oot af foreigituus +
Kohteet: 221				Kaikki kansid	ot ovat ajan tasalla. 🛛 😣 Yhteydess	sä palveluun Microsoft Exchange 🛛 🔲	100% —

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.

O Tallenna liite									
V V V V V V V V V V V V V V V V V V V	e → Local Disk (C:) → Docs → TUPO → sähköp	osti 👻 😽	Hae: sähköposti	م					
Järjestä 🔻 Uusi kansio				≣ ▼ 🔞					
0 Microsoft Outlook	Nimi	Muokkauspäiväm	Тууррі	Koko 🔺					
	🖭 ptk_email_ohje.pptx	20.5.2014 11:31	Microsoft PowerP	1 314 k					
🗙 Suosikit	🔁 Sähköpostiohje.pdf	29.4.2014 17:46	Adobe Acrobat D	3 362 k					
📕 Ladatut tiedosto ^{, 🚝}	🔁 SähköpostiohjeYlläpidolle.pdf	29.4.2014 17:45	Adobe Acrobat D	5 153 k ≡					
📃 Työpöytä	👜 SähköpostiohjeYlläpidolle290414.docx	29.4.2014 17:45	Microsoft Word -a	6 166 k					
🖫 Viimeisimmät sij	👜 SähköpostiohjeYlläpidolle.docx	29.4.2014 14:34	Microsoft Word -a	6 165 k					
	👜 Ohjeet.docx	16.4.2014 13:43	Microsoft Word -a	1 418 k					
🥽 Kirjastot	👜 Ohjeet.rtf	16.4.2014 10:15	RTF-tiedostot	46 393 k					
📔 Kuvat	🔊 Osoitteet.xlsx	16.4.2014 9:16	Microsoft Excel -la	10 k					
🌙 Musiikki	🔁 NCSA-FIn_hyvaksymat_salausratkaisut_t	30.3.2014 21:38	Adobe Acrobat D	195 k					
Tiedostot	🔁 TyöntekijänTietoturvaohje.pdf	28.3.2014 8:59	Adobe Acrobat D	2 362 k					
Videot	a outl.bmp	20.3.2014 17:32	Bittikarttakuva	374 k 👻					
Tiedosto <u>n</u> nimi: Kanga	svieri Jukka 1 Todentamis Ja Salaus Avain.cer			-					
Tallennus <u>m</u> uoto: Kaikki	tiedostot (*.*)								
) Piilota kansiot		Työka <u>l</u> ut ▼	<u>T</u> allenna	Peruuta					

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

0 📑 🤊 -		Saapu	neet - Marko.Hassine	n@pelastusopisto.fi -	Microsoft Outlook	
Tiedosto Aloitus Lähe	si 🚽 🕫 (* 🔺 🔶 🖵	'Kangasvieri	Jukka' (Jukka.Kangasv	vieri@kokkola.fi) - Yh	teystieto	
	Tiedosto Yhteystieto Lisää	i Muotoile tekstiä Tarkista				۵ 🕜
Uusi Uudet sähköpostiviesti kohteet – Uusi	Tallenna ja sulje Toiminnot	Jo uusi * Initia Sähköpostiviesti	Sooitteisto Tarkista nimet	Käyntikortti Kuva Asetukset	■ Luokittele × * Seuranta × @ Yksityinen Tunnisteet Päivitä Zoomaus	Aloita käsinkirjoitus Käsinkirjoitus
Saapuneet Marko.Hassinen@pelast	Koko nimi Yritys: Tehtävänimike:	S. Toimet Ka.Kangasvieri@ko ka.Kangasvieri@ko ka.Kangasvieri@ko	R		'Kangasvieri Jukka' (Jukka 0403568470 Matkapuhelin Jukka.Kangasvieri@kokkola.fi	1.Kan
AIRE AIRE Luonr Lähetet Poiste AIRE Näytä yhteys tallentaa dig lähetettäessi kyseiselle yht	tiedon Varmenteet-sivu, jossa voit itaalisen tunnuksen, jota käytetään ä salattuja sähköpostiviestejä teystiedolle.	asvieri, Jukka' v ka.Kangasvieri@kokkola.fi jasvieri Jukka' (Jukka.Kangasvieri@kokko	pla.fi) (Jukka.Kang	iomautukset	<u>K</u>	
Þ 🗭 Hakukansiot 📄 Keskusteluhistoria ট্টি Lähtevät	Verkkosivun osoite: IM-osoite: Puhelinnumerot					5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5
Roskaposti [26]	Туö 💌					
Arkistot	Koti 💌					
Arkistot	Työfaksi 💌					=
Poistetut	Matkapuhelin 040	3568470				
💢 Hakukansiot	Osoitteet					
🚞 Keskusteluhistoria	Työ 💌		and a			
🗀 Luonnokset 📄 Lähetetyt	'Kangasvieri Jukka' (Jukka.Ka	angasvieri@kokkola.fi)				<u> </u>
Lähtevät Roskaposti		ikki kohteet 🥰 VS: VL: Linkki . MIJPO				20:04 11.11.2013
A		ti 14:04				

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

🖭 🛃 🖑 🕐 🔶 'Kangasvieri Jukka' (Jukka,Kangasvieri@kokkola.fi) - Yhteystieto									
Tiedosto Yhteystieto Lisää Muot	toile tekstiä 🛛 Tarkista							۵ 🕜	
Tailenna ja luo uusi * Tailenna Poista ja sulje OneNote Toiminnot Outlook käyttää jotain näistä varmenteista sa	Näytä viesti Jatun viestin Jähettämiseen täll	Osoitteisto Tarkista nimet Nimet	Käyntikortti Kuv Asetukset	a Luokittele ▼ ▼ Seuranta ▼ a Yksityinen Tunnisteet	Päivitä Päivitä	Zoomaus Zoomaus	Aloita käsinkirjoitus Käsinkirjoitus		
Varmenteet (digitaaliset tunnukset):	iaat varmenteen vastaanottamalla digitaaliseseti allekirjoitetun viestin kyseiseltä yhteystiedolta tai tuomalla yhteystiedon varmennetiedoston. √armenteet (digitaaliset tunnukset):								
							Or	ninaisuu <u>d</u> et	
								ta oletukseksi	
								T <u>u</u> o	
								Vie <u>.</u>	
								<u>P</u> oista	
'Kangasvieri Jukka' (Jukka.Kangasvieri	'Kangasvieri Jukka' (Jukka.Kangasvieri@kokkola.fi)							Ω	
🛆 Kaikki kohtee	et 🚑 VS: VL: Linkki 🎮 TUPO						20:04 11.11.2	013	

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



Varmenne ilmestyy varmennelistalle. Toista sama toisen varmenteen kanssa.

😰 🛛 🛃 🦈 🤯 🖙 🐨 Kangasvieri Jukka' (Jukka.Kangasvieri@kokkola.fi) - Yhteystieto								- 0 %	
Tiedosto Yhteystieto Lisää Muo	toile tekstiä Tarkista							۵ (
Tallenna poista ja sulje Dutthok Kärttää intain päistä varmenteista si	Näytä Viesti Näytä Viesti	Osoitteisto Tarkista nimet Nimet	Käyntikortti Kuva Asetukset	Luokittele * Seuranta * Ksityinen Tunnisteet	Päivitä Päivitä	Q Zoomaus Zoomaus	Aloita käsinkirjoitus Käsinkirjoitus		
Saat varmenteen vastaanottamalla digitaalise	Jutioo käyttää jotain näistä varimenteistä salaitun viestin lähettämiseen talle yhteystiedolle. laat varmenteen vastaanottamalla digitaaliseseti allekirjoitetun viestin kyseiseltä yhteystiedolta tai tuomalla yhteystiedon varmennetiedoston.								
KANGASVIERI JUKKA 91091069K(Oletusarvo)							On	ninaisuu <u>d</u> et	
							Ase	ta oletukseksi	
								T <u>u</u> o	
								Vie <u>.</u>	
								<u>P</u> oista	
'Kangasvieri Jukka' (Jukka.Kangasvieri	i@kokkola.fi)							<u>∩</u> 2 ×	
🖾 Kaikki kohte	et 🚑 VS: VL: Linkki						20:04 11.11.2		

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.

🧟 certmgr - [Varmenteet - Nykyinen käyttäjä\Muut henkilöt\Varmenteet]											
<u>T</u> iedosto T <u>o</u> iminto <u>N</u> äytä O <u>h</u> j	<u>T</u> iedosto T <u>o</u> iminto <u>N</u> äytä O <u>hj</u> e										
🙀 Varmenteet - Nykyinen käyttäjä	Myönnetty	Myöntäjä	Vanhentumisp	Suunnitellut käyttöt	Kutsumanimi	Tila	Varmennemalli				
Henkilökohtainen	Hartikainen Jaseva 91.05/5234	VRK CA for Qualified Certificates	31.12.2016	Asiakkaan todenta	<ei mitään=""></ei>						
Luotetut varmenteiden pääm	Honkanen Math (506504C	VRK CA for Qualified Certificates	30.6.2015	Asiakkaan todenta	<ei mitään=""></ei>						
Vritysluottamus	Junttila Kan 9166120-2	VRK CA for Qualified Certificates	5.2.2018	Asiakkaan todenta	<ei mitään=""></ei>						
Keskitason varmenteiden my	KANGASVIERI JUKKA 21 TO1052K	VRK CA for Qualified Certificates	21.12.2018	<kaikki></kaikki>	<ei mitään=""></ei>						
Active Directory - Rayitajaobje	🙀 Veneskari 7.01 vo. 910626425	VRK CA for Qualified Certificates	29.4.2017	Asiakkaan todenta	<ei mitään=""></ei>						
Eucleur juikaisjat											
Kolmannen osapuolen pääva											
Luotetut henkilöt											
a 📔 Muut henkilöt											
Carmenteet											
McAfee Trust											
Varmennerekisteröintipyynné											
Alykortin luotetut päämyönti											
۰ III ا											
Muut henkilöt säilö sisältää 5 varmenn	netta.										

3.1.6. Salatun postin vastaanottaminen

Saapuneista viesteistä salatun viestin tunnistaa kirjekuoren ja lukon kuvasta.

🚺 📑 🤊 🚽 🛛 Saapuneet - Ma	arko.Hassinen	@pelastusopi	sto.fi - Microsoft
Tiedosto Aloitus Lähetä tai vastaa	nota Kan	sio Näytä	McAfee E-ma
Lähetä/vastaanota kaikki kansiot	ottoryhmät 🕶	Näytä edistyminen	Peruuta kaikki
Lähetä ja vastaanota		Lataa	a
▲ Suosikit <	Hakur Saanuu	neet (Ctrl+F)	
Saapuneet (1)	Tiaka. Saapai	icer (etti) ej	1
Marko. Hassinen@pelastusopisto.f	Lajittelujärjes	tys: Päivämäärä	ă 👘 🔻
 Marko.Hassinen@pelastusopisto Saapuneet (1) 	 ▲ tänään ▲ Hassiner Testi 	n Marko PeO	17:28 □Ÿ

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.

Viestisuojauksen ominaisuudet	×
Aihe: Testi	
Viestit voivat sisältää salauksen ja digitaalisen allekirjoituksen kerroksia. Kukin digitaalisen allekirjoituksen kerros voi sisältää useita allekirjoituksia.	
Suojauskerrokset	
Valitse seuraavasta kerros, jonka kuvauksen haluat nähdä.	
 Alhe: Test Salauskerros Digitaalinen allekirjoituskerros Allekirjoittaja: marko.hassinen@pelastusopisto.fi 	
Kuvaus:	
OK: Allekirjoitettu Salattu viesti.	
Tarkastele lisätietoja valitusta kerroksesta tai tee siihen muutoksia napsauttamalla jotakin seuraavista painikkeista:	
Muokkaa luottamussuhdetta Näytä tiedot Luota varmenteen myöntäjä	än
Varoita digitaalisesti allekirjoitetun postin virheistä. Sul	je

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

Digitaalinen alle	kirjoitus: Kelvollinen
Aihe: Mistä: Allekirjoittanut:	Testi Hassinen Marko PeO marko.hassinen@pelastusopisto.fi
유	Tämän viestin digitaalinen allekirjoitus on kelvollinen ja luotettava. Saat lisätietoja viestin digitaaliseen allekirjoitukseen käytetystä varmenteesta valitsemalla Tiedot.
🔲 <u>V</u> aroita digita	<u>T</u> iedot alisesti allekirjoitetun postin virheistä ennen viestin avaamista. <u>Sulje</u>

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.

KAIKKI TIETO
Viranomaisen asiakirjatieto
Viranomaisen työhön liittyvät asiakirjat. "viranomainen tai sen palveluksessa oleva on laatinut taikka joka on toimitettu viranomaiselle asian käsittelyä varten tai muuten sen toimialaan tai tehtäviin kuuluvassa asiassa" Julkiset asiakirjat (asiakirjatieto)
Asiakiriat jojihin lulki sovelletaan
Salassa pidettävä asiakirjatieto
JulkL 24§ luetellut tapaukset
Suojaustaso 1
jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle
Suojaustaso 2
jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle ;
Supjaurtare 2
jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle ;
Supjaurtare 4
jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa haittaa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle.
Ei julkiset asiakirjat (asiakirjatieto) Asiakirjat joihin JulkL El sovelleta, mm. valmisteilla olevat asiakirjat.
Muut asiakirjat
Esimerkiksi löydetty asiakirja, ei viran toimitukseen liittyvä posti (mm. mainokset tms) JulkL ei sovelleta. Huomioitava muut salassa pitoon velvoittavat lait, kuten PotL

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