LAUREA AMMATTIKORKEAKOULU Uuden edellä

Eri tietoturvaluokan palveluympäristöjen käyttö samalla päätelaitteella

Penttinen, Jyri

2013 Leppävaara

Laurea-ammattikorkeakoulu
Leppävaara

Eri tietoturvaluokan palveluympäristöjen käyttö samalla päätelaitteella

Jyri Penttinen
Tietojärjestelmäosaamisen koulutusohjelma
Opinnäytetyö
Toukokuu, 2013

Sisällys

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Tietojärjestelmäosaamisen koulutusohjelma

Jyri Penttinen

Eri tietoturvaluokan palveluympäristöjen käyttö samalla päätelaitteella

Vuosi 2013 Sivumäärä 68

Tässä opinnäytetyössä tutkitaan miten useita eri tietoturvaluokan palveluympäristöjä voidaan käyttää samalla päätelaitteella. Tutkimuksessa päätelaitteen tekninen ratkaisu suunnitellaan kansallisen turvallisuusauditointikriteeristön asettamien vaatimusten perusteella. Päätelaitteen toteutuksessa otetaan huomioon auditointikriteeristön tietoturvallisuuden osa-alueiden vaatimukset.

Tutkimuksen teoriaosuudessa esitellään yleisesti KATAKRI:n piirteitä ja tutkimukseen liittyviä osa-alueita. Tutkimuksessa hyödynnettiin Jay Nunamakerin monimenetelmällistä tietojärjestelmän kehittämistutkimusta. Tutkimuksen aikana kirjallisten lähteiden ja tieteellisten julkaisujen ohella tietoa kerättiin asiantuntijahaastatteluilla. Käytännön simuloinnin ja kenttätestien merkitys korostui, sillä tutkimusongelmaan ei ollut saatavilla valmista ratkaisua. Tutkimuksen tavoitteena on tuottaa konkreettinen, käyttäjäystävällinen ja kustannustehokas ratkaisu.

Tutkimuksessa esitetty tekninen ratkaisu toteutettiin Microsoftin komentorivipohjaisen laitehallintaan käytettävän Devcon-ohjelmiston avulla. Passiivisen ympäristön käytön estävä komento määriteltiin käyttöjärjestelmän salaamattomaan käynnistyssektoriin. Devcon-työkalua hyödyntävä komento estää yhteyden muiden ympäristöjen kiintolevyille, kun loppukäyttäjä valitsee käytettävän ympäristön.

Tutkimuksessa esitetyn ratkaisun käyttöönoton myötä on mahdollista saavuttaa merkittäviä kustannussäästöjä. Laitekustannusten lisäksi säästetään lisenssikustannuksissa. Tutkimuksessa esitetty ratkaisu on auditoitu tutkimusprosessin aikana Puolustusvoimissa ja sen käytölle on myönnetty tuotantokäyttölupa. Ratkaisun avulla on asennettu tuotantoympäristöön useita satoja päätelaitteita.

Tutkimustuloksia voidaan hyödyntää laajasti eri organisaatioissa, joissa on käytössä useita eri tietoturvaluokan ympäristöjä. Organisaatioissa voidaan siirtyä esitetyn ratkaisun myötä usean eri päätelaitteen käytöstä yhteen päätelaitteeseen.

Asiasanat: tietoturvallisuus, työasema, käyttöjärjestelmä, kansallinen turvallisuusauditointikriteeristö, turvallisuusauditointi

Laurea University of Applied Sciences **Abstract**
Leppävaara
Master Degree in Information Systems

Jyri Penttinen

How to use different security level IT service environments using the same data terminal equipment

Year 2013 Pages 68

This Master's Thesis investigates how to use different security level IT service environments using the same device (Data terminal equipment). In this study the requirements were defined according to the Finnish national security audit criteria called KATAKRI. Implementation was defined to cover the KATAKRI-based information security sections.

This research work has been conducted using Jay Nunamaker's multimethodological information system (IS) research framework. Nunamaker's multimethodological IS research framework integrates theory building, observation, experimentation and system developing. The framework fits to the imminent investigation problem due to the fact that there was no previous solution available. The main objective of this study was to find concrete, user-friendly and cost-effective solution.

The main challenge during this investigation was how to separate different physical hard disks from each other. Technical solution was accomplished using the DevCon command-line device manager utility software created by Microsoft. DevCon script was defined in the non-encrypted master boot record. It separates different hard disks automatically during the starting process of the operating system when end-user chooses the environment to be used.

The solution represented in this research enables considerable cost savings. The reducing amount of devices and licenses acts as a basis for cost savings. The technical solution at hand has been approved in a security audit conducted during the research process. Production authorization was approved by the Finnish Defense Forces. Hundreds of computers have been installed to production environment using the developed technical solution.

Research results can be utilized widely in various companies and organizations that are using several security level IT environments. There is no more need to have a physical computer for each environment. Instead of that this technical solution presents possibility to change over to a "single computer policy".

Keywords: information security, computer, operating system, national security audit criteria, security audit

Sanasto ja lyhenteet

AES	Advanced Encryption Standard
Altiris	Symantecin valmistama työasemien hallintajärjestelmä
BIOS	Basic Input-Output System
Bluetooth	Langaton tiedonsiirtotekniikka
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAA	Crypto Approval Authority
Deployment Solution	Symantecin työasemien mallinnus- ja asennusjärjestelmä
DEVCON	Microsoftin komentorivipohjainen laitehallintasovellus
DOS	Disk Operating System
FDE	Full Disk Encryption
Firmware	Laiteohjelmisto
FIPS	Federal Information Processing Standard
IPS	Intrusion prevention system
KATAKRI	Kansallinen turvallisuusauditointikriteeristö
Key-logger	Ohjelma, joka tallentaa näppäimistön painallukset
MBR	Master Boot Record
Multiboot	Usean käyttöjärjestelmän päätelaitteen käynnistymisprosessi
NBRT	Norton Bootable Recovery Tool
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTLDR	Windows-käyttöjärjestelmän lataamiseen käytettävä tiedosto
Sata	Serial AT Attachment
STIV	Suojaustaso IV
STIII	Suojaustaso III
STII	Suojaustaso II
STI	Suojaustaso I
WLAN	Wireless local area network
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä

1 Johdanto

Turvaluokitellut ympäristöt ovat yleistyneet niin yritysmaailmassa kuin valtionhallinnossa. Tietoturvallisuuteen ja tietoturvaluokitellun materiaalin käsittelyyn kiinnitetään entistä enemmän huomiota ja tietoturvan kehittämisestä on tullut organisoidumpaa. Suomessa esimerkiksi Valtionhallinnon tietoturvallisuuden johtoryhmän tuottamia VAHTI-ohjeita käytetään hallinnon lisäksi hyväksi kansainvälisessä tietoturvatyössä niin yritysmaailmassa kuin kunnissa (Vahti-ohje 2011). Eri tietoturvaluokiteltujen ympäristöjen turvallisuuden todentamiseen on kehitelty kansallinen turvallisuusauditointikriteeristö KATAKRI. Se toimii turvallisuusviranomaisten yhteisenä kriteeristönä, jolla varmistetaan organisaation turvallisuuden taso (Puolustusministeriö 2011).

Eri tietoturvaluokan tiedon käsittelysäännöissä sekä päätelaitteiden laitekokoonpanoille ja konfiguraatioille asetetuilla vaatimuksilla on eroja. Suojaustasovaatimusten erojen vuoksi eri tietoturvaluokan ympäristöissä käytetään usein fyysisesti eri päätelaitteita. Loppukäyttäjällä on kuitenkaan harvoin todellinen tarve työskennellä eri ympäristöissä samanaikaisesti. Ei ole kustannustehokasta hankkia jokaiseen ympäristöön omaa fyysistä päätelaitetta, jos todellisuudessa pääsääntöisesti työskennellään yhdessä palveluympäristössä kerrallaan. Tässä tutkimuksessa tutkitaan, miten eri tietoturvaluokan palveluympäristöjä voidaan käyttää tietoturvallisesti samalla päätelaitteella. Kokemusteni ja havaintojeni perusteella omassa työympäristössäni tietoturvaluokiteltujen erillisympäristöjen päätelaitteet ovat usein pitkiä aikoja käyttämättöminä. Tutkimuksen yhtenä tavoitteena on kehittää käyttäjäystävällinen tekninen ratkaisu, jonka avulla voidaan saavuttaa merkittäviä kustannussäästöjä niin päätelaite- kuin ohjelmistokustannuksissa. Loppukäyttäjä ei tarvitse enää eri tietoturvaluokan ympäristölle omaa fyysistä päätelaitetta, vaan eri ympäristöjen käyttö tapahtuu samalla päätelaitteella. Tutkimuksessa käsitellään myös, minkä suojaustason ympäristöjä on mahdollista käyttää samalla päätelaitteella.

1.1 Tutkimuksen tavoitteet

Tutkimuksen tavoitteena on luoda tekninen ratkaisu, joka täyttää kansallisen turvallisuusauditointikriteeristön tietoturvallisuuden osa-alueiden asettamat vaatimukset. Tutkimuksessa kehitettävän ratkaisun myötä on mahdollista saavuttaa merkittäviä taloudellisia säästöjä. Sillä voidaan siirtyä usean päätelaitteen käytöstä yhteen päätelaitteeseen. Kustannussäästöjä saadaan niin päätelaite- kuin lisenssikustannuksissa. Ensisijaisesti tutkimustuloksia voidaan hyödyntää organisaatioissa, joissa on käytössä eri tietoturvaluokan ympäristöjä ja joiden tietoturvapolitiikka ja strategia noudattaa kansallista turvallisuusauditointikriteeristö KATAKRI:a.

Tutkimuksen yhtenä tavoitteena on toteuttaa käyttäjäystävällinen ratkaisu. Päätelaiteratkaisun vaatimukseksi määriteltiin, että eri ympäristöjen kiintolevyt ovat kiinni koneen rungossa samanaikaisesti. Käyttäjän ei tarvitse irrottaa tai vaihtaa kiintolevyjä päätelaitteeseen siirtyessään työskentelemään toiseen palveluympäristöön. Omien kokemusteni perusteella päätelaitteen liitännät eivät kestä jatkuvaa kiintolevyjen irrottamista ja kiinnittämistä. Lisäksi teknisen toteutuksen tulee olla helppokäyttöinen, jotta tietoteknisesti kaikentasoisilla loppukäyttäjillä on mahdollista käyttää päätelaitetta tietoturvallisesti. Tutkimuksessa esitettävän ratkaisun turvallisuus on todennettava turvallisuusviranomaisen toteuttamalla auditoinnilla ennen tuotantoympäristöön implementointia.

1.2 Tutkimuskysymys ja tutkimuksen rajaus

Tutkimuksessa etsitään keinoja eri tietoturvaluokan palveluympäristöjen tietoturvalliseen käyttämiseen samalla päätelaitteella. Tutkimuksessa tavoitellussa ratkaisussa eri ympäristöjen kiintolevyt ovat kiinni samanaikaisesti päätelaitteessa. Kehitettävä ratkaisumalli on tarkoitettu Windows- käyttöjärjestelmille. Laboratoriotesteissä käytetään Windows XP- ja Windows 7 – käyttöjärjestelmiä. Päätelaitteella käytettävien palveluympäristöjen kiintolevyt salataan hyväksytyllä kiintolevynsalausohjelmistolla. Windows 8-käyttöjärjestelmää ei laboratoriotesteissä käytetty, sillä se ei ollut tutkimusta tehtäessä laajamittaisessa käytössä yritysmaailmassa. Lisäksi päätelaitteen toteutuksen tulee olla loppukäyttäjälle helppokäyttöinen ja käyttäjäystävällinen.

Tutkimusta tehtäessä useat organisaatiot ovat etsineet vaatimukset täyttävää virtualisoitua päätelaiteratkaisua samaan tutkimusongelmaan. Toistaiseksi tietoturvallisuusvaatimukset täyttävää ja tuotantokäyttöön soveltuvaa virtualisoitua päätelaiteratkaisua ei ole löytynyt. Tämän vuoksi tutkimuksessa eri ympäristöt asennetaan fyysisesti eri kiintolevyille tai massamuisteille. Tavoitteena on kehittää tuotantokäyttöön soveltuva valmis ratkaisu, jolla saavutetaan välittömiä kustannussäästöjä todellisessa organisaatiossa. Käytettävissä olleiden resurssien vuoksi virtualisoitu ratkaisu rajattiin tutkimuksen ulkopuolelle. Teknisen ratkaisun kehityksessä tutkimuksen edetessä otetaan huomioon loppukäyttäjiltä saatu palaute päätelaitteen käytettävyydestä tuotantokäytössä. Tutkimuksessa esitettävän ratkaisun tietoturvallisuuden taso ja mahdolliset riskit todennetaan tutkimuksen yhteydessä kansallisen turvallisuusviranomaisen toteuttamalla auditoinnilla. Auditointikriteeristönä käytetään kansallista turvallisuusauditointikriteeristö KATAKRI:a ja sen 2011 julkaistua versiota 2.0.

2 Tutkimusmenetelmät ja tutkimusprosessin eteneminen

Tutkimuksen tavoitteena oli toteuttaa tekninen ratkaisu, joka mahdollistaa eri tietoturvaluokan palveluympäristöjen käytön samassa päätelaitteessa. Tutkimusongelmaa lähestyttiin aluksi hankkimalla aiheeseen liittyvää teoriatietoa ja mahdollisia valmiita olemassa olevia ratkaisuja. Hankittua teoriatietoa kehitettiin omien kokemusten, käytännön havainnointien ja testaamisen avulla. Aiheeseen liittyvien julkaisujen ja kirjallisuuden lisäksi tietoa ja kokemuksia hankittiin asiantuntijahaastatteluilla. Lopputuotteen vaatimusmäärittelyn perustana toimi kansallinen turvallisuusauditointikriteeristö KATAKRI.

2.1 Monimenetelmällinen tietojärjestelmän kehittämistutkimus

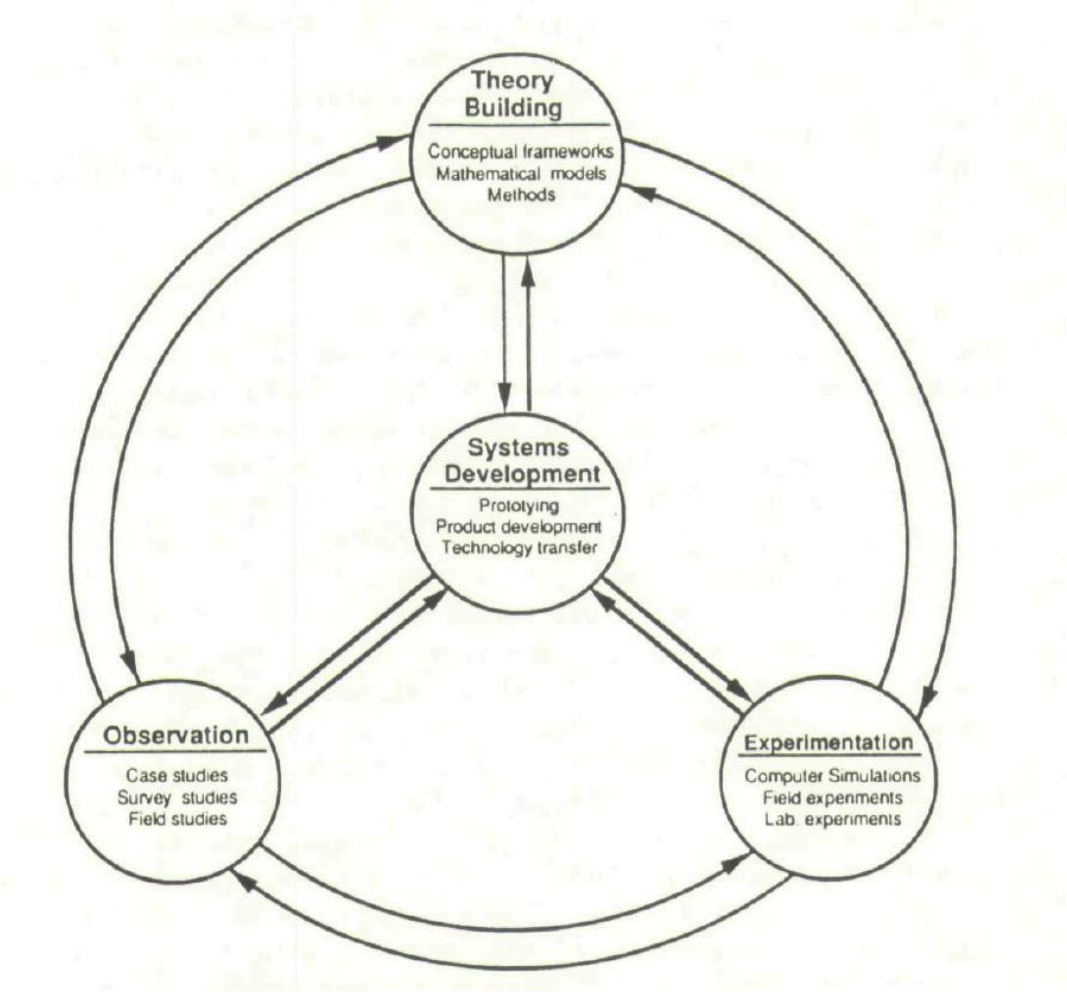
Tutkimusprosessissa käytettiin useita eri tutkimusmenetelmiä kuten simulaatiota, kenttätestausta, tapaustutkimusta sekä grounded -teoriaa. Olemassa olevaa ratkaisua tutkimusongelmaan tai vastaavaa julkista tutkimusta ei ollut saatavilla. Tämän vuoksi havainnointi, simulaatiot ja laboratoriotestit olivat keskeisiä ratkaisua kehitettäessä. Teoriatieto ja vaatimusmäärittelyt puolestaan loivat perustan kokeille.

Tutkimuksessa käytettiin Jay Nunamakerin monimenetelmällistä tietojärjestelmän kehittämistutkimuksen mallia. Nunamakerin, Chen ja Purdinin (1991) mukaan tietojärjestelmän kehittämistutkimus integroi yhteen teorian rakentamisen, havainnoinnin, observoinnin, testaamisen sekä järjestelmän kehittämisen. Nunamakerin (2010) mukaan tutkimusprosessi alkaa teorian, omien kokemusten ja tiedon keräämisellä. Saadun teoriatiedon pohjalta suoritetaan käytännön testaamista ja simulointia. Observoinnilla havainnollistetaan hankittua teoriatietoa. Hankitun teoriatiedon, käytännön testaamisen sekä observoinnin pohjalta rakennetaan prototuote (Nunamaker ym. 1991).

Nunamakerin monimenetelmällinen tietojärjestelmän kehittämistutkimuksen malli valittiin tutkimusmenetelmäksi, sillä se sopi parhaiten tutkimukseen, jossa rakennetaan tekninen ratkaisumalli aikaisemmin ratkaisemattomaan ongelmaan. Tutkimuksessa testaamisen ja teoriatiedon yhdistäminen käytännön tuotekehitystyöhön palvelivat tutkimukselle asetettuja tavoitteita parhaiten. Nunamakerin monimenetelmällinen tietojärjestelmän kehittämistutkimuksen malli on kuvattu kuviossa 1.

Van Akenin ja Hevnerin (2004) mukaan tietojärjestelmätieteen tutkimuksen tulos on johonkin organisaation tärkeään ongelmaan rakennettu IT-artefakti. Ongelmakentän ja liiketoimintastrategian määrittävät ympäristötekijät - kuten ihmiset, organisaatio sekä teknologia. IT-artefakti täyttää tavoitteen, kun se ratkaisee ongelman ja parantaa nykyisiä käytäntöjä tai ratkaisuja innovatiivisesti. (Hevner, March, Park & Ram 2004.) Van Akenin (2004) mukaan ongelman ymmärtäminen on puolet ratkaisusta. Seuraava askel on kehittää ja testata vaihtoeh-

toisia ratkaisuja. Tässä tutkimuksessa pyrittiin tiedonhankintavaiheessa kartoittamaan mahdollisia ratkaisumalleja ja sen jälkeen soveltamaan niitä käytännön testeillä. Tutkimusongelma oli syntynyt oman työyhteisön kautta ja päätelaitteiden kasvavien kustannusten vähentämiseksi etsittiin kustannustehokasta ratkaisua teknisen toteutuksen kautta.



Kuvio 1. Monimenetelmällinen tutkimusmallikehys (Nunamaker, Chen & Purdin 1990)

Teorian rakentaminen tarjoaa Nunamakerin ym. (1991, 94) mukaan perustiedon ja suuntaviivoja tietojärjestelmätutkimukselle. Käytännön testaamisen ja havainnoinnin myötä kehittyy uutta tutkimukselle soveltuvaa teoriaa. Havainnointia on usein käytetty, mikäli aiheesta on olemassa vain vähän tutkittua tietoa. Havainnointi sisältää tapaustutkimusta, kenttätutkimusta sekä käytännön testaamista. Teoria antaa yleensä tutkimukselle suuntaa, mutta on usein riittämätön operatiivisen tutkimusongelman ratkaisemiseksi (Nunamaker 2010, 322). Sen vuoksi käytännön havainnointi, olemassa olevan teorian soveltaminen ja edelleen kehittäminen on tärkeää. Tässä tutkimuksessa havainnointi yhdistettiin hankittuun teoriatietoon, omiin näkemyksiin sekä alan asiantuntijoiden kokemuksiin tutkittavasta aihealueesta. Tutkimusongelmaan pyrittiin toisin sanoen löytämään paras mahdollinen ratkaisu lähestymällä sitä monimenetelmällisesti eri näkökulmista.

Kokeellisuus sisältää tutkimusstrategian kuten laboratorio- ja kenttäkokeet sekä simuloinnin (Nunamaker ym. 1991). Kokeita ohjaavat olemassa oleva teoriatieto ja ne johtavat järjestelmän kehittämisvaiheeseen. Järjestelmän kehittämiseen kuuluu tutkimustyössä viisi tasoa: konseptin suunnittelu, arkkitehtuurin rakentaminen, prototyypin rakentaminen, tuotekehitys sekä tuotantoon siirtäminen (Nunamaker ym. 1991). Nunamakerin (2010) mukaan suurimmat haasteet tulevat tietojärjestelmien kehittämisessä usein viimeisellä ”tutkimusmaililla”. Tässä tutkimuksessa kului merkittävästi aikaa kehitetyn konseptin testaamiseen ja toimivuuden todentamiseen ennen tuotantokäyttöön siirtämistä.

Prototyypin tuotantokäyttöön siirron jälkeen havaitaan usein, kuinka kehiteltyä tuotetta tai ratkaisua voitaisiin edelleen kehittää (Nunamaker ym. 1991). Loppukäyttäjän tekemillä havainnoilla voidaan usein parantaa esimerkiksi tuotteen tai ratkaisun käytettävyyttä. Esimerkiksi tässä tutkimuksessa loppukäyttäjiltä saadun palautteen avulla eroteltiin eri palveluympäristöjen kirjautumissivut selkeämmin toisistaan. Lisäksi päätelaitteen käynnistymisprosessia selkeytettiin loppukäyttäjän näkökulmasta pidentämällä aikaa, jolloin eri ympäristöjen käynnistysvalikko on näkyvissä päätelaitteen virtojen kytkemisen jälkeen. Näillä toimenpiteillä ehkäistiin merkittävästi loppukäyttäjän riskiä väärään palveluympäristöön kirjautumiseen. Loppukäyttäjiltä saatava palaute on tärkeää, jotta ratkaisu vastaa työntekijän tarpeita työtehtävien tehokkaaseen hoitamiseen. Lisäksi riittävällä perehdyttämisellä päätelaitteen käyttöön ehkäistään käyttäjien vastarintaa uuden päätelaiteratkaisun käyttöönottoon.

Tässä tutkimuksessa tavoitteena oli kehittää tekninen ratkaisu eri tietoturvaluokan palveluympäristöjen käyttöön samalla päätelaitteella. Tutkimuksessa hankitun teoriatiedon, omien kokemusten ja testaamisen perusteella rakennettiin prototuote, jota testattiin ensin laboratorioympäristössä. Mikäli protomalli ei toiminut testien perusteella, pyrittiin selvittämään mahdollista ongelmakohtaa teoria-aineiston, havainnoinnin sekä asiantuntijaverkoston kautta. Prototuotteen läpäistyä testit kriteerien mukaisesti, toistettiin testejä useasti toimivuuden systemaattisesti todentamiseksi. Prototuotteen toimivuuden lisäksi sen tietoturvallisuus oli todennettava auditoinnilla. Turvallisuusauditoinnista saadulla palautteella päätelaiteratkaisua kehitettiin entistä tietoturvallisemmaksi. Tämän vaiheen jälkeen kehitetty tuote siirrettiin tuotantoympäristöön laajemman validiuden osoittamiseksi. Loppukäyttäjien päätelaitteen käyttökokemuksien perusteella ratkaisun käytettävyyttä lisättiin vielä tuotantokäyttövaiheessa. Tutkimuksessa käytetyllä tutkimusmenetelmällä sulautetaan teoriatiedon hankkiminen, järjestelmän kehittäminen, käytännön testaaminen ja observointi yhdeksi prosessiksi.

2.1.1 Grounded teoria

Järvisen ja Järvisen (2004) mukaan ” Grounded on induktiivisesti tutkittavasta ilmiöstä johdettu teoria”. Tutkittavan ilmiön teoriaa kehitetään ja analysoidaan. Tutkimuksessa kehitettävää ilmiötä todennetaan tietoja keräämällä ja analysoimalla (Järvinen & Järvinen 2004, 71). Grounded teoria on menetelmällinen lähestymistapa, jonka avulla pyritään muodostamaan uutta teoriaa tutkittavan ilmiön olemassa olevasta teoria-aineistosta. (Yhteiskuntatieteellinen tietoarkisto 2012).

Grounded teorian keskeisimmät kriteerit ovat teorian suhteessa tutkittavaan ilmiöön: yhteensopivuus, ymmärtäminen, yleisyys ja kontrolli (Strauss & Corbin 1990, Järvisen ym. 2004, 71 mukaan). Aineistoa kerätään tutkittavasta ilmiöstä, kunnes se ei enää tarjoa uutta ainesta kehiteltävään teoriaan. Tässä tutkimuksessa aineistoa kerättiin olemassa olevasta kirjallisuudesta ja julkaisuista. Olemassa olevien ratkaisuiden ja aiheeseen liittyvän teoriatiedon hankkimiseen käytettiin runsaasti aikaa. Painetun teoriatiedon lisäksi kartoitettiin käytännön kokemuksia alan asiantuntijoilta. Tutkimuksessa tutkittavaan ilmiöön haettiin yhteensopivuutta kaikkiin Windows käyttöjärjestelmiin, jolloin ratkaisun yleistämisen näkökulma täyttyy. Lisäksi kehitettävän ratkaisun oli täytettävä laajassa käytössä olevan kansallisen turvallisuusauditointikriteeristö KATAKRI:n vaatimukset. Kontrolli testaamiseen ja hankitun teoriatiedon havainnointiin saavutettiin vakioidulla testiympäristöllä sekä testitapausten dokumentoimisella. Lisäksi tutkimuksessa kehitettävä ratkaisu auditoitiin ulkopuolisen asiantuntijaorganisaation toimesta.

2.1.2 Triangulaatio

Tutkimuksessa käytetty tutkimusote perustuu triangulaatioon. Anttilan (2011) mukaan triangulaatiolla tarkoitetaan lähestymistä tutkittavaan ilmiöön monimenetelmällisesti usealta eri suunnalta. Triangulaation avulla osoitetaan, että tutkimustulos ei ole sattumanvarainen. Sama lopputulos on saavutettava usealla eri lähestymistavalla. Triangulaation avulla tutkimuksen validiutta saadaan parannettua. Luotettavuutta lisää, kun tutkimuksessa esitetyt hypoteesit saadaan osoitettua systemaattisesti toteen. (Anttila 2011.)

Tutkimusongelmaa lähestyttiin olemassa olevan teoriatiedon ja käytännön testaamisen kautta. Omille havainnoille haettiin luotettavuutta kontrolloiduilla kokeilla, asiantuntijahaastattelujen sekä valmiin loppuratkaisun ulkopuolisen turvallisuusviranomaisen auditoinnin avulla. Omien hypoteesien, olemassa olevan teoriatiedon ja asiantuntijahaastattelujen kautta syntynyttä prototyyppiä testattiin systemaattisesti. Tuotteen läpäistyä testit prototyyppi tuotteistettiin ja syntynyttä teknistä ratkaisua asennettiin useita satoja kertoja tuotantokäyttöön. Näin omat hypoteesit saatiin osoitettua systemaattisesti toteen.

Tutkittavaa ilmiötä oli lähestyttävä useasta eri kulmasta, sillä olemassa olevaa ratkaisua ei ollut olemassa. Lisäksi olemassa olevaa teoriaa oli kehitettävä ja sovellettava, jotta toimivaan ja vaatimukset täyttävään lopputulokseen päästäisiin. Triangulaatio oli keskeinen tekijä tutkimuksen validiteetin osoittamisessa. Sen käyttö oli tarkoituksenmukaista juuri sen vuoksi, ettei tutkittavasta ilmiöstä ollut paljoa tietoa. Lähestyttäessä tutkimusongelmaa monimenetelmällisesti saatiin virheet ja ristiriitaisuudet karsittua kattavasti. Tutkimuksessa käytetty tutkimusote oli mielestäni työläs, mutta loppujen lopuksi ainoa vaihtoehto konkreettisen ja luotettavan lopputuloksen saavuttamiseksi.

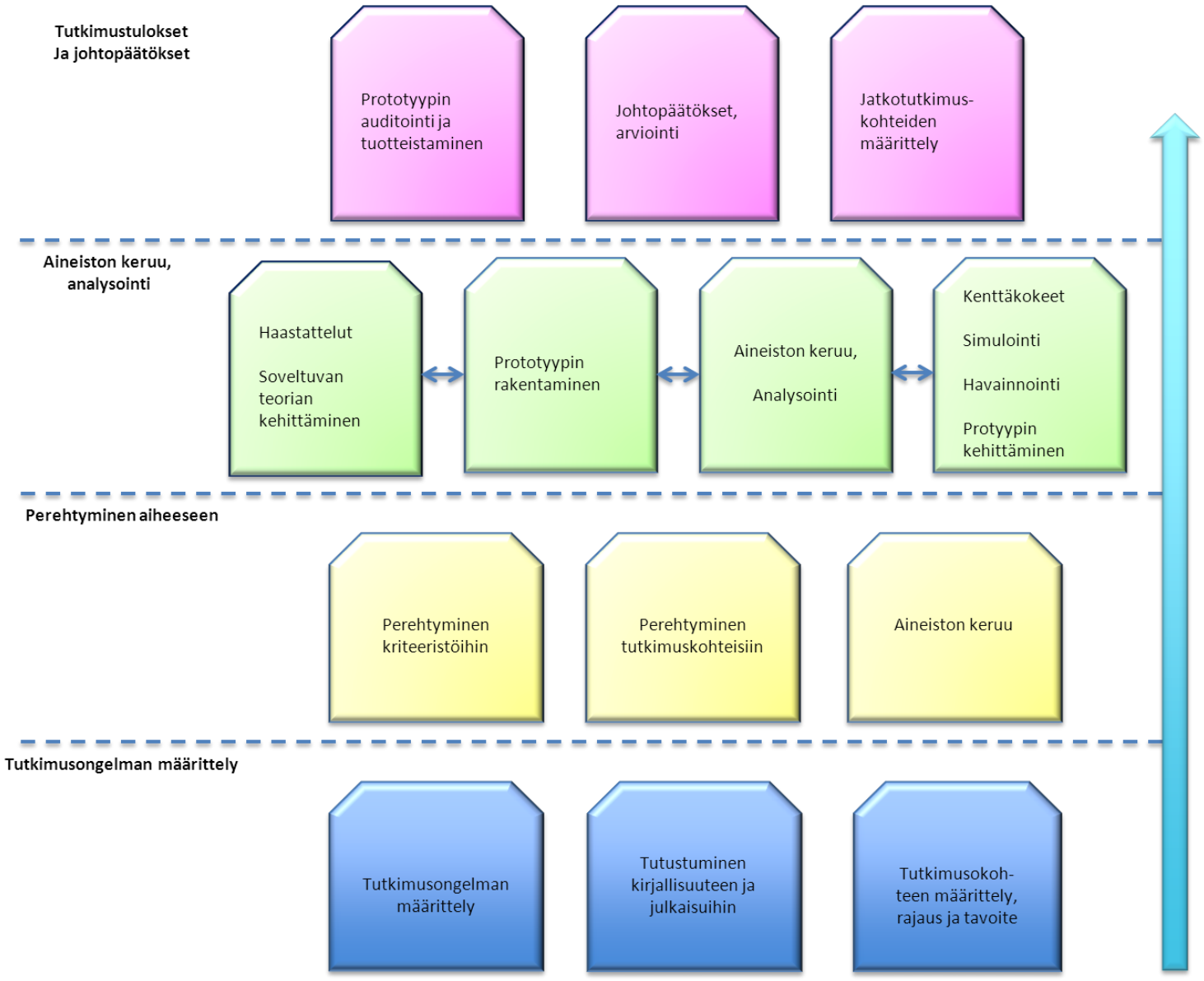
2.2 Tutkimusprosessin eteneminen

Tutkimusprosessin aluksi määriteltiin selkeä tavoite, joka tässä tutkimuksessa oli tekninen ratkaisu usean eri palveluympäristön käytölle samalla päätelaitteella. Tämän jälkeen haettiin keinoja tavoitellun päätelaiteratkaisun toteuttamiseksi. Aiheeseen liittyviin julkaisuihin ja kirjallisuuteen tutustuttiin mahdollisten olemassa olevien ratkaisuiden löytämiseksi. Lisäksi hyödynnettiin omia kokemuksia tietoturvallisuudesta, työasema-asennuksista sekä Windows-käyttöjärjestelmistä. Riittävän aiheeseen perehtymisen jälkeen tehtiin päätelaitteen vaatimusmäärittely. Tämän jälkeen korostui käytännön testaaminen. Ensimmäiseksi ratkaisumalliksi löydettiin toisen kiintolevyn manuaalinen käytöstä poistaminen Windowsin laitehallinnan kautta. Käytöstä poistaminen oli tehtävä ennen kiintolevyn salaamista. Käyttöjärjestelmä ei pystynyt käynnistymään, mikäli muiden ympäristöjen käytöstä poistamista ei tehty ennen kiintolevynsalausprosessia. Ratkaisun löydyttyä tutkittiin, kuinka ratkaisun saisi automatisoitua.

Tehdyn taustatutkimuksen ja omien kokemusten perusteella päädyin esiteltyyn ratkaisumalliin, jossa yhteys toisiin ympäristöihin estetään automaattisesti devcon-ohjelmiston avulla koneen käynnistyessä. Ratkaisua vahvistaakseni haastattelin alan asiantuntijoita ja selvitin, olisiko muita ratkaisuja olemassa. Toisin sanoen hain ratkaisulleni referenssejä muilta alan ammattilaisilta. Käytännön testejä toistettiin useita kymmeniä kertoja, jotta ratkaisun toimivuus saatiin varmennettua ennen turvallisuusauditointia ja tuotantokäyttöön siirtämistä.

Tutkimusprosessin aikana työn ohjauksessa hyödynnettiin Maanpuolustuskorkeakoulun tietoturvapäällikkö Jyri-Petteri Aron tietoturvallisuusosaamista. Teknisestä ratkaisusta - kirjallisuuden lisäksi - haastateltiin Viestikoulun tutkimus- ja kehittämisosaston tutkimusinsinööri Vesa Roihaa, Anvia Hostingin Ludvig Liljequistia, tietoturvayritys Xcure Oy:n toimitusjohtaja Peik Åströmiä, Maanpuolustuskorkeakoulun tietoturvapäällikkö Jyri-Petteri Aroa, Maanpuolustuskorkeakoulun tietohallintopäällikkö Mikael Puskaa sekä tietoturvayhtiö Nixun asiantuntijaa. Asiantuntijahaastatteluilla pyrittiin saamaan palautetta kehitettyyn ratkaisuun

sekä kartoittaa mahdollisia muita ratkaisuja esitettyyn tutkimusongelmaan. Haastattelut ja keskustelut vahvistivat näkemystäni, että esitetty ratkaisu on käyttökelpoinen, helposti implementoitava sekä riittävän yksinkertainen. Haastattelut toteutettiin teemahaastatteluina. Haastattelut olivat luonteeltaan keskusteluja, jonka rakenteen olin valmistellut etukäteen. Valitsin teemahaastattelun strukturoidun haastattelun sijaan, jotta minun olisi mahdollisuus saada mahdollisimman paljon aineistoa, joka perustuu aidosti haastateltavan henkilön kokemuksiin. Valittu malli sopi hyvin tutkimusongelman luonteeseen. Vaatimukset täyttävän ja toimivan protomallin löydyttyä suoritettiin päätelaiteratkaisun turvallisuustason todentava auditointi. Kuviossa 2 on kuvattu vaiheittain tutkimusprosessin eteneminen.



Kuvio 2. Tutkimusprosessin eteneminen

2.3 Datan kuvaus ja datan kerääminen

Tutkimukseen kerättiin tietoa kirjallisuuden lisäksi EBSCO:n, IEEE:n sekä ACM:n tietokannoista. Kirjallisen materiaalin lisäksi tutkimusdataa kerättiin asiantuntijahaastatteluiden avulla. Tutkimuksessa haastateltiin Maanpuolustuskorkeakoulun tietoturvapäällikkö Jyri-Petteri Aroa, tietohallintopäällikkö Mikael Puskaa, Puolustusvoimien tutkimusinsinööri Vesa Roihaa, Anvia Hosting Oy:n Ludvig Liljequistia, Xcure Oy:n toimitusjohtaja Peik Åströmiä sekä tietoturvallisuuteen erikoistuneen yhtiön NIXU:n asiantuntijaa. Asiantuntijoiden ammattitaitoa hyödynnettiin etenkin esitetyn ratkaisun käyttökelpoisuudesta. Asiantuntijalausunnoilla pyrittiin myös hankkimaan tukea ja eri näkökulmaa laboratoriotesteissä tehdyille havainnoille. Haastatteluilla ja kirjallisuuden avulla kartoitettiin virtualisoidun päätelaiteratkaisun tutkimustuloksia sekä päätelaitteen käyttötapauksia pilvipalveluna. Windows-käyttöjärjestelmän tietoturvallisuuden tiukentamisessa tietoa hankittiin KATAKRI:n lisäksi NIST:in (National Institute of Standards and Technology) julkaisutietokannasta, Microsoftin, BSI:n sekä NSA:n Windows-ympäristöille luoduista tietoturvallisuuden tarkistuslistoista.

Teknisen loppuratkaisun vaatimusmäärittely muodostettiin Kansallisen turvallisuusauditointikriteeristön perusteella. NIST:in, Microsoftin, BSI:n sekä NSA:n tietokannoista hankituilla tiedoilla tiukennettiin Windows-päätelaitteiden turvallisuutta KATAKRI:n ohella. KATAKRI:in tutustuttiin perusteellisesti, jotta tutkimuksessa kehitetty ratkaisu täyttää todellisuudessa kaikki kriteeristön vaatimukset. Tutkimusprosessin aikana turvallisuusauditointikriteeristön tulkitsemisessa konsultoitiin Maanpuolustuskorkeakoulun tietoturvapäällikköä Jyri-Petteri Aroa. Hänellä on KATAKRI pääauditoijan koulutus ja usean vuoden kokemus eri yritysten turvallisuusauditoinneista.

Tutkimusongelmaan ei löytynyt olemassa olevaa ratkaisua, joten merkittäväksi menetelmäksi muodostui havainnointi sekä testaaminen hankitun teoriatiedon pohjalta. Testien avulla havainnoitiin ja osoitettiin muodostettuja hypoteeseja toteen. Tietojärjestelmän kehittämisprosessissa korostuu käytännön testaaminen ja uuden teorian luominen olemassa olevan pohjalta uutta ongelmaa ratkaistaessa.

2.4 Testiympäristön kuvaaminen

Tutkimuksessa käytännön testaukset suoritettiin Hewlett-Packardin Elitebook 8560P – kannettavalla. Sata-kiintolevyt asennettiin koneen rungon lisäksi optisen aseman paikalle. Kolmatta ympäristöä testattiin ulkoisella kiintolevyllä sekä eSATA- että USB-liitännän kautta. Testeissä käytettiin 128 GB SSD-, 500GB eSATA- sekä Lacien 500 GB USB-kiintolevyjä. Testit suoritettiin Windows XP- ja Windows 7- käyttöjärjestelmillä. Kiintolevyjen salaamiseen käytettiin Utimacon Safeguard Easy - levynsalausohjelmistoa. Windows 7-käyttöjärjestelmän kanssa käytettiin

Sophoksen Safeguard Easy - levynsalausohjelmistoa. Tuote on pääpiirteittään sama, sillä tuotteen nimen vaihtumisen taustalla on yrityskauppa, jossa Sophos osti Utimacon. Laboratoriotesteissä käytetty laitekokoonpano on esitetty kuviossa 3.

Käytännön testaamiseen kului tutkimuksessa runsaasti aikaa. Käyttöjärjestelmäasennuksen jälkeen kiintolevyihin asennettiin salausohjelmisto. Kiintolevyn kapasiteetista riippuen salausprosessi kesti kahdesta tunnista kahdeksaan tuntia. Esimerkiksi epäonnistuneen skriptin tai asetuksen jälkeen asennukset jouduttiin usein aloittamaan alusta. Käyttöjärjestelmäasennukset suoritettiin Symantecin Altiris-työasemienhallintajärjestelmän avulla. Altiriksen Deployment Solution-järjestelmästä oli tutkimuksessa käytössä versio 6.9 SP 5. Asennusympäristöön valmisteltiin eri suojaustasojen levykuvat. Epäonnistuneen testin jälkeen työasemaa ei tarvinnut asentaa alusta asti uudelleen, vaan valmiin levykuvan avulla säästettiin asennuksiin kuluvaa aikaa. Muiden palveluympäristöjen kiintolevyt irrotettiin testien alussa päätelaitteesta asennuksen ajaksi. Testien edetessä asennusympäristöä saatiin kehitettyä siten, että päätelaitteesta ei tarvinnut enää irrottaa kiintolevyjä. Asennusjärjestelmään määriteltiin erillinen komento, jolla pystyttiin määrittelemään kiintolevy, johon image-asennuksen oli tarkoitus kohdistua. Tämä nopeutti ja helpotti merkittävästi ratkaisun avulla toteutettuja usean sadan päätelaitteen massa-asennuksia.

Kuvio 3. Laboratoriotesteissä käytetty laitekokoonpano

Testaamisen tarkoituksena oli osoittaa ideoiden toimivuus käytännössä. Toistamalla testejä useaan otteeseen tavoiteltiin luotettavaa loppuratkaisua. Ympäristöjen asennukset toistettiin

useita kymmeniä kertoja ennen kuin käytön estävät ongelmat oli saatu ratkaistua. Testiolosuhteet pyrittiin pitämään samanlaisina koko tutkimusprosessin aikana. Masonin (1988) mukaan kontrollin tuominen kokeeseen on tärkeää, koska kokeen tarkoitus on tuoda varmistettua käytännön tietoa. Toimivan ratkaisun löydyttyä testit toistettiin useita kymmeniä kertoja tuotteen laadun varmistamiseksi ennen tuotantoon siirtämistä sekä ratkaisun turvallisuustason todentavaa auditointia. Teknisen ratkaisun toimivuus ja käytettävyys todennettiin lopulta laajassa tuotantokäytössä.

3 KATAKRI – kansallinen turvallisuusauditointikriteeristö

Tutkimuksessa kehitettävän päätelaiteratkaisun vaatimusmäärittelyn perustana toimi kansallinen turvallisuusauditointikriteeristö. Tässä luvussa esitellään yleisesti KATAKRI:n piirteitä ja sen asettamia vaatimuksia usean eri tietoturvaluokan päätelaitteelle. Tutkimuksessa kehitetty ratkaisu auditoidaan KATAKRI:n vaatimusten perusteella turvallisuusviranomaisen toimesta.

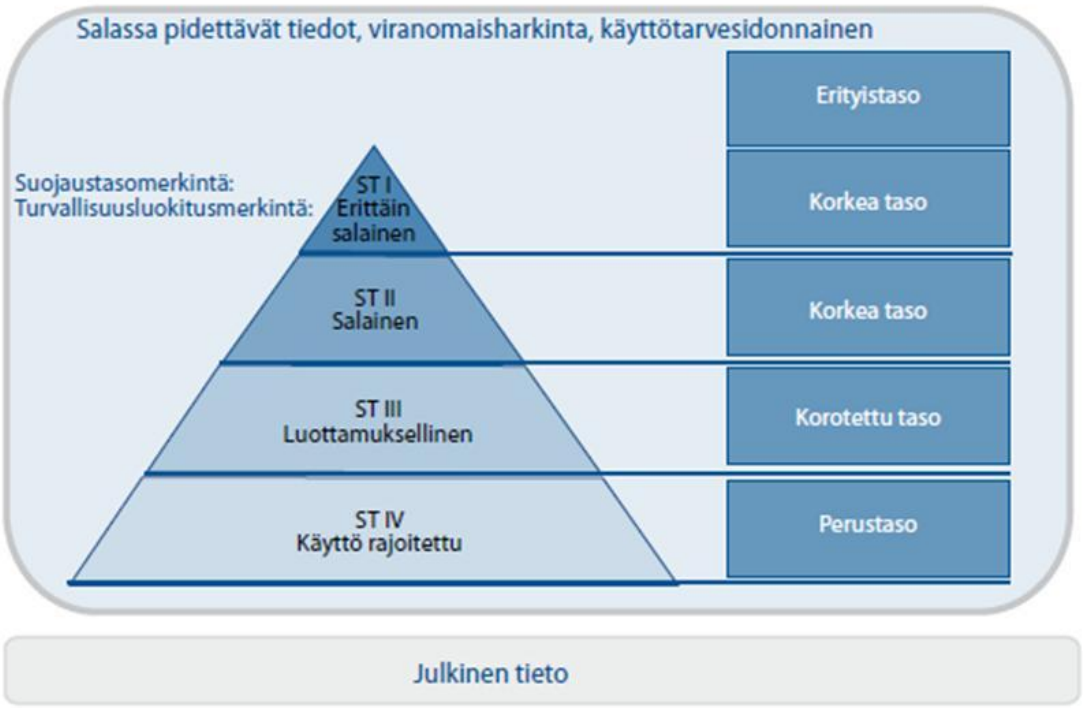
”Kansallisen turvallisuusauditointikriteeristön ensimmäisenä päätavoitteena on yhtenäistää viranomaistoimintoja silloin, kun viranomainen toteuttaa yrityksessä tai muussa yhteisössä kohteen turvallisuustason todentavan tarkastuksen, auditoinnin” (Puolustusministeriö 2011). KATAKRI on siis tarkoitettu työkaluksi viranomaisille tai turvallisuuden todentaville auditoijille, joille on annettu valtuus todentaa kohteen turvallisuuden taso KATAKRI:n kriteerien perusteella (Vahti-ohje 2011).

Turvallisuusauditointikriteeristön toisena tavoitteena on auttaa yrityksiä ja muita yhteisöjä omassa sisäisessä turvallisuustyössä. Kriteeristö jakautuu neljään pääosioon: hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus ja tietoturvallisuus. Osioille on laadittu kolmiportainen vaatimusluokittelu: perustaso, korotettu taso ja korkea taso (Puolustusministeriö 2011).

Tässä tutkimuksessa kehiteltävän teknisen ratkaisun vaatimuksissa huomioidaan tietojärjestelmäturvallisuuden osa-alueen asettamat vaatimukset eri suojaustasojen (IV-II) ympäristöjen työasemille tai kannettaville. ”Turvallisuusauditointikriteeristön tietoturvaosio kuvaa tietoturvallisuuden vähittäisvaatimukset sellaisille tiedoille, joiden luottamuksellisuutta, eheyttä ja käytettävyyttä tulee suojata.” Tietoturvakriteeristötyössä on otettu huomioon valtionhallinnon tietoturvallisuusasetuksen ja tätä täydentävien ohjeiden yksityiskohtaiset linjaukset.” (Puolustusminiteriö 2011, 73.)

Osa-alueiden vaatimukset on jaettu kolmeen tasoon: perustason vaatimukset (IV), korotetun tason vaatimukset (III) ja korkean tason vaatimukset (II). Erittäin salaisen ympäristön vaatimuksia (suojaustaso I) ei KATAKRI:ssa määritellä. Vaatimuksia tulkittaessa on huomioitava,

että alemman tason asettamat vaatimukset on täytyttävä ylemmällä tasolla sen erillisvaatimusten lisäksi. (Puolustusministeriö 2011, 73.) Kuviossa 4 on esitetty eri tietoturvaluokat ja turvallisuusluokitukset.



Kuvio 4. Eri suojaustasot (Vahti-ohje 2012)

Kansainvälistä turvallisuusluokittelussa KATAKRI:a vastaavat turvallisuusmerkinnät ovat: Restricted (Käyttö Rajoitettu), Confidential (Luottamuksellinen) ja Secret (Salainen) (Puolustusministeriö 2011). Tutkimuksessa käytettiin uusinta saatavilla olevaa KATAKRI:n vuonna 2011 päivitettyä versiota 2. Seuraava KATAKRI:n versio 3 julkaistaan vuoden 2013 kuluessa. Uuden KATAKRI:n suunnittelussa ovat korostuneet edellistä versiota parempi skaalautuvuus, riskiperusteinen tarkastelu sekä käytettävyys organisaation turvallisuustyökaluna. (Evwaraye 2012.)

3.1 KATAKRI:n tietoturvallisuuden osa-alueet

Kansallinen turvallisuusauditointikriteeristön tietoturvallisuuden osa-alue koostuu neljästä osa-alueesta:

- Tietoliikenneturvallisuus, osa-alue I400
- Tietojärjestelmäturvallisuus, osa-alue I500
- Tietoaineistoturvallisuus, osa-alue I600
- Käyttöturvallisuus, osa-alue, I700

Tämän tutkimuksen teknisen päätelaitetoteutuksen kannalta merkittävin tietoturvallisuuden osa-alue on tietojärjestelmäturvallisuus. Tietoliikenneturvallisuuden osa-alue asettaa vaatimuksia päätelaitetoteutukseen lähinnä langattomaan tiedonsiirtoon tarkoitettujen laitteiden osalta, kuten 3G, Bluetooth sekä WLAN. Tietoaineistoturvallisuuden osa-alue esitellään tässä luvussa lyhyesti, sillä tiedonluokittelumenettely vaikuttaa tietoaineiston käsittelyyn eri tietoturvaluokan ympäristöissä. Käyttäjän tulee tuntea luokittelumenettely, jotta ymmärtää käsitellä eri suojaustason aineistoja sille tarkoitetussa ympäristössä. Käyttöturvallisuuden osa-alue asettaa puolestaan vaatimuksia, jotka tulee huomioida tutkimuksessa kehitettyä ratkaisua tuotteistettaessa. Käyttöturvallisuuden osa-alue asettaa vaatimuksia esimerkiksi päätelaitetoteutuksen dokumentointiin ja asennusmenettelyihin liittyen.

3.1.1 Tietoliikenneturvallisuuden osa-alue I400

Kansallisen turvallisuusauditointikriteeristön tietoliikenneturvallisuuden osa-alue asettaa vaatimuksia liittyen tietoliikenneverkkoon, verkonvalvontaan, liikenteen suodatukseen sekä langattomien verkkojen käyttöön. Tietoliikenneturvallisuuden osa-alueen vaatimuksista tämän tutkimuksen päätelaiteratkaisuun koskevat vaateet ohjelmistopalomuurin käytöstä sekä eri suojaustasojen rajoitteet langattomien verkkojen käytölle. Lisäksi tietoturvaluokitellun palveluympäristön päätelaitteesta tulee poistaa IPv6 käytöstä työasemista, mikäli sen käytölle ei ole perusteita (Puolustusministeriö 2011).

3.1.2 Tietojärjestelmäturvallisuuden osa-alue I500

Tietojärjestelmäturvallisuus on yksi neljästä KATAKRI:n vuonna 2011 julkaistun version tietoturvallisuuden osa-alueista. Tietojärjestelmäturvallisuuden I500 osa-alue sisältää yksityiskohtaisia kriteereitä liittyen tunnistautumiseen, järjestelmien asennukseen sekä lokien keräämiseen ja säilyttämiseen (Puolustusministeriö 2011). Tässä tutkimuksessa päätelaiteratkaisun vaatimusmäärittely perustui merkittävästi tietojärjestelmäturvallisuuden osa-alueen asettamiin vaatimuksiin.

Tietojärjestelmäturvallisuuden todentavalla auditoinnilla tarkoitetaan teknisen tietoturvallisuusratkaisun hyväksyntää järjestelmässä käsiteltävän tiedon turvallisuusluokitusta vastaavalle tasolle. Tietoturvallisuusauditointi on prosessi, jossa toimivaltainen viranomainen yhdessä tietojärjestelmän omistajan kanssa määrittää järjestelmään kohdistuvan riskitason ja hyväksyy sen mukaiset suojaustoimet. (Turvallisuusviranomaisten käsikirja yrityksille 2011.) KATAKRI:n asettamat vaatimukset tietojärjestelmäturvallisuuden osa-alueella I500 ovat tämän tutkimuksen liitteenä 2. Tässä tutkimuksessa esitetty tekninen ratkaisu auditoitiin tutkimuksen yhteydessä KATAKRI:n tietoturvallisuuden osa-alueita peilaten.

3.1.3 Tietoaineistoturvallisuuden osa-alue I600

Tietoaineistoturvallisuuden tavoitteena on säilyttää asiakirjojen ja tiedostojen luottamuksellisuus. Tietoaineistoturvallisuudella pyritään varmistamaan myös tiedon eheys, käytettävyys, asianmukainen säilyttäminen sekä hävittäminen. Tietosisällöltään suojattavat dokumentit tulee merkitä suojaustasoa vastaavalla merkinnällä. Perusajatuksena on, että dokumentit luokitellaan sisällöltään korkeimman luokituksen mukaisesti. Dokumenttiin tulee myös merkitä, jos asiakirjan ja sen liitteiden luokitustaso ei ole sama. Tiedot luokitellaan niiden merkittävyyden sekä lakisääteisten vaatimusten perusteella. Tietojen luokittelua ohjaavat laki viranomaisten toiminnan julkisuudesta (621/1999) sekä kyseisen lain pohjalta annettu asetus (1030/1999). Myös tiedon salassapitoajat on määrätty lainsäädännössä. (Vahti-ohje 2011.) Tiedon omistaja määrittää viimekädessä aineiston tietoturvaluokituksen. Tilasta poistuttaessa korotetun suojaustason materiaali tulee siirtää vaatimukset täyttävään kassakaappiin. Suojattavien sähköisten aineistojen hävittäminen tulee toteuttaa luotettavasti. Esimerkiksi suojattavaa tietoa sisältävän kiintolevyn ylikirjoituksessa on käytettävä luotettavaa menetelmää tai kiintolevy on tuhottava mekaanisesti. (Puolustusministeriö 2011.)

3.1.4 Käyttöturvallisuuden osa-alue I700

Käyttöturvallisuudesta päätelaiteratkaisuun liittyy vaatimus dokumentoinnista. Kehitettävän päätelaiteratkaisun toteutus tulee dokumentoida kattavasti, jotta asennukset voidaan toteuttaa järjestelmällisesti. Dokumentaation avulla mahdollistetaan myös vikatilanteesta toipuminen ja mahdollisten asennusvirheiden korjaaminen. Ainoastaan valtuutettu taho saa asentaa järjestelmät ja ohjelmistot. Tutkimuksessa esitetyn ratkaisun näkökulmasta on tärkeää, että loppukäyttäjällä ei ole järjestelmänvalvojatason oikeuksia. Tällöin loppukäyttäjä ei pääse muokkaamaan tai muuttamaan ympäristöjen teknistä erottelua. Toisin sanoen asennus- ja asetustenmuokkausoikeus tulee sallia vain ylläpitäjille (Puolustusministeriö 2011, 109). Ympäristöön kytkettävien laitteiden tulee olla käyttöympäristöön hyväksyttyjä. Käyttöjärjestelmien oletustilit tulee myös poistaa käytöstä. Testaus- ja kehitysympäristöjen on oltava erilliset.

3.2 KATAKRI:n eri suojaustasot ja vaatimukset työaseman laitekokoonpanoon

Tässä luvussa käsitellään kansallisen turvallisuusauditointikriteeristön vaatimuksia eri suojaustason ympäristöjen päätelaitteiden laitekokoonpanoihin sekä konfiguraatioille. Luvussa esitetään työaseman tietoturvallisuuden vaatimukset perustason, korotetun suojaustason sekä korkean suojaustason osalta. Lisäksi eri suojaustasojen vaatimuksia tutkittaessa huomioidaan,

mitä eri suojaustason ympäristöjä samalla päätelaitteella on mahdollista käyttää. Kansallisen turvallisuusauditointikriteeristön tietojärjestelmäturvallisuuden vaatimustaulukko on tutkimuksen liitteenä 3. Kansallinen turvallisuusauditointikriteeristö ei ota kantaa suojaustason I (erittäin salainen) tiedon suojausmenettelyyn. Suojaustason I tietojen turvaaminen tarkastellaan aina erikseen (Puolustusministeriö 2011). Tämän vuoksi tässä luvussa ei käsitellä suojaustason I vaatimuksia päätelaitteelle.

3.2.1 Perustason ympäristön (STIV) vaatimukset päätelaitteelle

Tässä luvussa kuvataan perustason asettamat vaatimukset päätelaitteelle. Perustason (STIV) käsittely-ympäristö on mahdollista kytkeä internetiin, jos suojaustason muut edellytykset täyttyvät (Puolustusministeriö 2011, 121). Työasemien tietoturvallisesti kovennettu asennus tulee toteuttaa järjestelmällisesti. Korkeamman suojaustason ympäristön päätelaitteen on täytettävä myös perustason asettamat vaatimukset.

Päätelaitteen käyttöjärjestelmään ja ohjelmistoihin on asennettava tarpeelliset turvapäivitykset. Lisäksi käyttöjärjestelmän alustassa tulee olla käytössä ainoastaan järjestelmän tarvitsemia ohjelmistokomponentteja. (Puolustusministeriö 2011, 122.) Käyttöjärjestelmän oletustilit, kuten järjestelmänvalvoja- ja vierailijatilit tulee poistaa käytöstä. Työasemien on lukkiuduttava automaattisesti 10 minuutin käyttämättömyyden jälkeen. Ohjelmistot, kuten Web-selain, PDF-lukijat ja toimisto-ohjelmat, tulee olla turvallisesti konfiguroituja. Tietojärjestelmien käytön yhteydessä syntyvät suojattavaa tietoa sisältävät väliaikaistiedostot on hävitettävä säännöllisesti (Puolustusministeriö 2011, 89).

Päätelaitteissa on käytettävä henkilökohtaisia käyttäjätunnisteita ja sisäänkirjautuminen käyttöjärjestelmään on toteutettava turvallisella ja tunnetulla tekniikalla. Myös järjestelmien ja sovellusten ylläpitotunnuksien tulee olla henkilökohtaisia. Salasanalle on asetettava turvallisuuden vähimmäisvaatimukset ja salasanan vaihto tulee pakottaa määräajoin. (Puolustusministeriö 2011, 85.) Perustason ympäristön suositusvaatimuksena pakotetulle salasanan vaihdolle on vähintään 180 päivän määräajoin. Tunnuksen tulee lukkiutua liian usean epäonnistuneen tunnistautumisyrityksen seurauksena. Autentikaatiodataa - kuten salasanoja - ei saa säilyttää tietojärjestelmissä selkokielisinä, vaan ne tulee suojata tunnetulla ja luotettavana pidetyllä menetelmällä (Puolustusministeriö 2011).

Suojaustaso IV-ympäristön päätelaitteen kiintolevy tulee olla luotettavasti suojattu. Käytettävät salausratkaisut sekä tuotteet tulee olla hyväksytty suojaustasolle tietoturvaviranomaisen toimesta. (Puolustusministeriö 2011.) Perustason työasemissa on oltava haittaohjelmantorjuntaohjelmisto sekä palomuuri. Palomuurisäännöstöt estävät oletuksena kaiken liikenteen (default-deny) ja vain toiminnalle välttämätön verkkoliikenne sallitaan. Lisäksi torjuntaohjelmis-

to tulee päivittää säännöllisesti sekä sen tulee tuottaa lokitietoja havaintojen seuraamiseksi. Perustasolla teknisten palveluiden tuottamista lokitiedoista tulee kyetä todentamaan tietomurrot. Lokitiedostoja tulee säilyttää oletusarvoisesti 6 kuukautta, ellei erillistä sopimusta säilyttämisestä ole määritelty. Suojattavaa tietoa sisältävien lokitiedostojen pääsynvalvonta, käsittely ja poisto tulee toteuttaa asianmukaisesti (Puolustusministeriö 2011). Teknisten menetelmien lisäksi ympäristön loppukäyttäjiä tulee ohjeistaa haittaohjelmauhista sekä organisaation tietoturvaperiaatteista.

Perustason työasemaa käytöstä poistettaessa on huomioitava, että suojattavaa tietoa sisältävät laitteet, kuten kiintolevyt, muistikortit ja muistit on tyhjennettävä luotettavasti. Mikäli käytössä ei ole luotettavasti muistin tyhjentävää ohjelmistoa, tulee muistit tuhota mekaanisesti. Kolmannen osapuolen suorittamat päätelaitteen huollot on valvottava tai suojattavaa tietoa sisältävät komponentit irrotettava ennen huoltotoimenpiteitä. (Puolustusministeriö 2011, 91.)

Perustason työasemista ja sen ohjelmistoista on pidettävä rekisteriä, josta tulee ilmetä myös käytöstä poistetut laitteet. Työasemien hankinnat ja asennukset tulee toteuttaa ainoastaan luotettavista ja luvallisista lähteistä. (Puolustusministeriö 2011, 92.)

3.2.2 Korotetun suojaustason ympäristön (STIII) vaatimukset päätelaitteelle

Korotetun suojaustason ympäristöt ovat lähtökohtaisesti fyysisesti erillään ei - luotetuista verkoista. Tapauskohtaisesti suojaustason III käsittely-ympäristön voi yhdistää fyysisesti eri verkkoon, mikäli sen turvallisuus on tarkastettu ja hyväksytty auditoinnissa. Tässä luvussa esitettyjen vaatimusten lisäksi korotetun suojaustason päätelaitteen on täytettävä perustason (STIV) vaatimukset.

Korotetun suojaustason työasemassa tarjottavat palvelut tulee olla minimoituna vain välttämättömiin. Verkkojaot on poistettava käytöstä. Käyttöjärjestelmien ja ohjelmistojen konfiguroinnit määritellään siten, että päivitykset tapahtuvat ainoastaan tähän tarpeeseen tarkoitetuista lähteistä. Näin parannetaan luvattoman verkkoliikenteen havainnointia verkonvalvonnassa. Kaikki tarpeeton verkkoliikennöinti tulee olla poistettuna käytössä, kuten esimerkiksi Bluetooth ja WLAN. (Puolustusministeriö 2011, 82.) Suojattavaa tietoa sisältäviä tallenteita ja lokitiedostoja säilytetään 24 kuukautta, ellei erillisellä sopimuksella ole toisin määrätty. Lokitiedostoja on seurattava vähintään viikoittain poikkeavien tapahtumien ja käyttöjärjestelmien luvattomien käyttöyritysten havaitsemiseksi. Lisäksi lokit tulee varmuuskopioida säännöllisesti ja niiden eheyden varmistamiseksi tulee olla käytössä menetelmä. (Puolustusministeriö 2011, 88.)

BIOS-asetukset tulee olla suojattuna salasanalla ja vain valtuutetulla taholla tulee olla pääsy BIOS-määrityksiin. Lisäksi tarpeettomat portit ja palvelut tulee poistaa käytöstä BIOS:sta. Tapauskohtaisesti päätelaitteesta poistetaan käytöstä tarpeettomat liitännät. Mikäli liitäntöjen, kuten USB-porttien, käytölle on olemassa perusteet, tulee arvioida tapauskohtaisesti millaisia laitteita järjestelmään voidaan kytkeä. (Puolustusministeriö 2011, 87.) Työasemien ja kannettavien tietoaineistoturvallisuuden turvaamiseksi on tärkeää, että kiintolevyjen tiedot eivät ole selkokielisenä. Yksittäisten tiedostojen salausten ohella esimerkiksi yrityssalaisuuksien turvaamiseksi käytetään koko kiintolevyn salausta (FDE) (Saarenmaa 2010). Kiintolevyn sisältö käsitellään kryptograafisella salaimella, lukuun ottamatta käynnistyssektoria. Käyttöjärjestelmän on kyettävä lukemaan käynnistyssektoria käynnistyäkseen, jonka vuoksi sen on oltava salaamaton (Saarenmaa 2010). Kiintolevyn vahva salaus on tärkeää, jotta voidaan varmistaa, ettei tieto joudu väärin käsiin laitteen tai kiintolevyn kadotessa. Korotetun suojaustason ympäristön kiintolevyissä tulee käyttää AES 256-bittistä salausalgoritmia (Puolustusministeriö 2011). Saarenmaan (2010) mukaan AES-salausta ei ole tiettävästi pystytty murtamaan.

Korotetun suojaustason palveluympäristön ohjelmistojen ja päivitysten eheys tulee tarkastaa. Lisäksi esimerkiksi ohjelmistotoimittajilta vaaditaan selvitys tietoturvallisuuden huomioimisesta tuotekehityksessä. (Puolustusministeriö 2011, 97.)

3.2.3 Korkean suojaustason ympäristön (STII) vaatimukset päätelaitteelle

Päätelaitteen ohjelmistojen palomuurien tulee sallia vain erikseen määriteltyjen protokollien liikennöinti, joita organisaatiossa tarvitaan. Langattomia verkkoja ei saa käyttää korkean suojaustason ympäristöissä. Päätelaitteesta tulee poistaa käytöstä 3G, Bluetooth sekä langattoman lähiverkon verkkokortti. (Puolustusministeriö 2011, 82.)

Tapauskohtaisesti päätelaitteesta poistetaan käytöstä tarpeettomat liitännät. Päätelaitteesta tulee poistaa käytöstä esimerkiksi USB-portit, mikäli USB-muistien käyttö ei ole ympäristössä välttämätöntä. Korkean suojaustaso tietoa sisältävissä työasemissa ja kannettavissa kiintolevyt tulee olla salakirjoitettu. Korkean suojaustason tietojärjestelmän eheys tulee tarkastaa viikoittain. Lisäksi suojattavien tietojen käsittelystä tulee tallentaa käsittelytietojen lokimerkinnät (Puolustusministeriö 2011, 88). Lokitietojen pidemmän säilytysajan (24 kuukautta) ja kerättävän lokimäärän vuoksi lokien keräämiseen on varattava riittävästi tallennus- ja säilytyskapasiteettia.

Päätelaitteiden hankintaan kansallinen turvallisuusauditointikriteeristö määrittelee, että laitteen on mahdollistettava muistin salakirjoitus. Lisäksi on varmistettava, että laitevalmistaja tarjoaa riittävää tukea esimerkiksi turvapäivityksiin ja takuu- sekä lisenssiehtohin. Korkean suojaustason päätelaitteen tulee olla toisin sanoen muokattavissa turvallisuustason vaatimuk-

sia vastaaviksi (Puolustusministeriö 2011, 98). Korkean suojaustason palveluympäristössä käytettäviltä sovelluksilta edellytetään viranomaisen hyväksyntää. Lisäksi järjestelmän turvallisuuteen vaikuttavan koodin turvallisuus on oltava julkisesti tarkasteltavista. Esimerkiksi kiintolevynsalausohjelmiston hyväksyntä suojaustasolle edellyttää tälläistä toimintatapaa.

Järjestelmällisesti toteutettavan kovennetun asennuksen lisäksi korkean suojaustason ympäristössä tulee olla käytössä mekanismi, jolla järjestelmään tehdyt muutokset tallentuvat ja ne voidaan jälkikäteen havaita (Puolustusministeriö 2011, 86). Laitteet tulee myös suojata luvattomien laitteiden, kuten key-loggerien liittämistä vastaan.

3.2.4 Yhteenveto eri suojaustasojen asettamista vaatimuksista päätelaitteelle

Tässä luvussa esitetään yhteenveto KATAKRI:n asettamista vaatimuksista päätelaitteelle eri suojaustasoilla. Eri suojaustasojen vaatimusten havainnollistamiseksi vaatimukset on määritelty taulukkoon. Vaatimukset on jaettu kolmeen päätelaitteeseen vaikuttavaan osa-alueeseen. Jaottelussa vaatimukset jaettiin seuraaviin kokonaisuuksiin:

- Vaatimukset tietoliikenteelle
- Vaatimukset käyttöjärjestelmälle ja ohjelmistoille
- Vaatimukset päätelaitteelle ja BIOS:iin

Taulukoista on mahdollista tarkastaa, mitä asioita tulee huomioida konkreettisesti päätelaiteasennuksessa, jotta päätelaite täyttää suojaustason asettamat vaatimukset. Toteutussarakkeessa on esitetty käytännön toimenpide, jolla vaatimus saadaan täytettyä. Vaatimukset on koottu KATAKRI:n tietoliikenneturvallisuuden-, tietojärjestelmäturvallisuuden, käyttöturvallisuuden ja tietoaineistoturvallisuuden osa-alueista.

ID	Vaatimus päätelaite asennukseen liittyen	Perustaso (IV)	Korotettu taso (III)	Korkea taso (II)	Toteutus
Tietoliikenne					
	Organisaatiopalomuurin lisäksi työasemiin on asennettava turvallisesti konfiguroitu palomuuri	Kyllä	Kyllä	Kyllä	Säännöstöt estävät oletuksena kaiken liikenteen, mitä ei ole erikseen sallittu (default-deny). 2) Määrittelemätön liikennöinti on estetty molempiin suuntiin.
	Langattomat verkot ovat lähtökohtaisesti kielletty		Kyllä	Kyllä	Poistetaan käytöstä STIII-ympäristön päätelaitteesta 3G,WLAN,Bluetooth.
	IPv6 poistetaan käytöstä, mikäli sen käytölle ei ole perusteita	Kyllä	Kyllä	Kyllä	IPv6 poistetaan käytöstä, mikäli sen käytölle ei ole perustetta

Taulukko 1. Tietoliikenneturvallisuuden asettamat vaatimukset päätelaitekonfigurointeihin

Vaatimus päätelaite asennukseen liittyen	Perustaso (IV)	Korotettu taso (III)	Korkea taso (II)	Toteutus
Käyttöjärjestelmä ja ohjelmistot				
Käytössä on menettelytapa, jolla uudet päätelaitteet asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus	Kyllä	Kyllä	Kyllä	Käytössä on menettelytapa, jolla uudet työasemat asennetaan järjestelmällisesti. Kovennuksista esimerkiksi osoitteesa www.nsa.gov/ia/security_configuration guides
Ohjelmistot tulee konfiguroida turvallisiksi	Kyllä	Kyllä	Kyllä	Erityisesti web-selaimet, PDF-lukijat,toimisto-ohjelmat ja sähköpostiohjelmat
Oletussalasanat tulee olla vaihdettu sekä automaattisesti luodut tilit poistaa käytöstä. Lisäksi käyttöoikeudet on asetettu vähimpien oikeuksien periaatteella.	Kyllä	Kyllä	Kyllä	Poistetaan käytöstä työaseman administrator/järjestelmänvalvoja ja guest/vieras-tilit. Loppukäyttäjälle myönnetään ainoastaan tarvittavat oikeudet.
Laitteista tulee kerätä keskeiset lokitiedot ja käsitellä niitä asianmukaisesti	Kyllä	Kyllä	Kyllä	STIV keskeisiä tallenteita säilytetään 6kk, suojaus asianmukaisesti.STIII tallenteiden säilytys 24kk lisäksi käytössä menettely hyökkäyksen/väärinkäyttöyrityksen havaitsemiseen, käsittelyyn ja torjuntaa Huomioitava lokimenettelyt päätelaitteiden konfiguroinneissa.
Tarvitaanko kiintolevyn tai massamuistien salaus tietojen suojaamiseksi	Kyllä *	Kyllä	Kyllä	STIV tasolla määritellään "kiintolevyjen suojaus riittävällä tasolla". Salakirjoitetaan NCSA-FI hyväksymällä tuotteella. Salaiset avaimet ainoastaan valtuutettujen käyttäjien hallussa
Päätelaitteissa saa olla ainoastaan luvallisia ohjelmistoja	Kyllä	Kyllä	Kyllä	Ohjelmistoista pidetään rekisteriä, johon kirjataan käytössä olevat ohjelmistot ja lisenssit. Loppukäyttäjille ei anneta admin-oikeuksia, vaan ohjelmisto asennukset ainoastaan valtuutetun tahon toimesta.
Istunnonhallinnassa tulee käyttää tunnettua ja luotettavana pidettyä tekniikkaa	Kyllä	Kyllä	Kyllä	Istunnonhallinnassa käytetään tunnettua ja luotettavana pidettyä tekniikkaa
Autentikaatiodataa ei säilytetä tietojärjestelmissä selväkielisinä	Kyllä	Kyllä	Kyllä	Autentikaatiodataa (kuten salasanoja, sormenjälkiä, jne.) ei säilytetä tietojärjestelmissä selväkielisinä.
Ajettavan koodin turvallisuudesta on oltava varmistus	Kyllä	Kyllä	Kyllä	Ohjelmistoja hankitaan ja asennetaan vain luotettavista ja luvallisista lähteistä.
Päätelaitteen dokumentaation tulee mahdollistaa vikatilanteesta toipuminen.	Kyllä	Kyllä	Kyllä	Esimerkiksi päätelaitteen tekninen dokumentaatio (asennusohje) tulee olla dokumentoitu.
Oltava selkeät suunnitelmat ketkä saavat asentaa ohjelmistoja, tietoliikenneyhteyksiä ja oheislaitteita	Kyllä	Kyllä	Kyllä	Käytössä on selkeät periaatteet ja toimintatavat siitä, ketkä saavat asentaa ohjelmistoja, tietoliikenneyhteyksiä ja oheislaitteita. Rajoitetaan asennus- ja asetusten muokkausoikeus vain ylläpitäjille).
Asennettavista ohjelmistoista ja palveluissa tulee huomioida CERT-toimijoiden tietoturvatiedotteet	Kyllä	Kyllä	Kyllä	Viranomaisten (esim. CERT-toimijat), laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan ja tarpeelliset turvapäivitykset asennetaan hallitusti.
Päätelaitteenn automaattinen lukkiutuminen tulee määrittää, jotta työskentelytauoilla tai työskentelyn jälkeen laitteet eivät jää ilman riittävää suojaa	Kyllä	Kyllä	Kyllä	Asetetaan päätelaitteeseen automaattinen lukitus. STIV tasolla koneen lukkiuduttava 10 minuutin käyttämättömyyden jälkeen.

Taulukko 2. KATAKRI:n asettamat vaatimukset käyttöjärjestelmä- ja ohjelmistoasennuksiin

Vaatimus päätelaite asennukseen liittyen	Perustaso (IV)	Korotettu taso (III)	Korkea taso (II)	Toteutus
Laitteisto				
BIOS on suojattava salasanalla		Kyllä	Kyllä	Suojataan BIOS-salasanalla, jos päätelaitteeseen kytketään STIII tai STII palveluympäristö
Arvioidaan tapauskohtaisesti käytössä tarvittavat liitännät (esimerkiksi USB)		Kyllä	Kyllä	Mikäli liityntöjen käytölle on todelliset perusteet, arvioidaan tapauskohtaisesti edellytykset ja ehdot, minkä mukaisia laitteistoja ja välineitä käytetään. Jos tarvetta ei ole poistetaan liitännät käytöstä asennusvaiheessa.
Tietoturva-asiat tulee huomioida laitehankinnoissa. Esimerkiksi päätelaitteeen tulee olla konfiguroitavissa suojaustason vaatimusten mukaisesti	Kyllä	Kyllä	Kyllä	Laitteet hankitaan keskitetysti tietoturva-asiat huomioiden.

Taulukko 3. KATAKRI:n asettamat vaatimukset laitteistolle

Edellä kuvatuissa taulukoissa on otettu huomioon ainoastaan päätelaiteasennuksissa huomioitavat asiat. Esimerkiksi ympäristön palvelimeen konfiguroitaviin tekijöihin ei oteta kantaa. Taulukoissa on mainittu tietojen luotettavasta suojauksesta. Ympäristössä käytettävä salausratkaisu tulee aina hyväksyttää salaustuotekohtaisesti CAA (Crypto Approval Authority) – viranomaisella. Suomessa kansallisena salaustuotteiden hyväksyjänä toimii Viestintäviraston NCSA-FI (Puolustusministeriö 2011, 122). Peruskäytäntönä on, että ohjelmistopohjaiset salausratkaisut hyväksytään perustasolle (STIV) ja reunaehdoin korotetulle tasolle (STIII). Pääsäänöisesti korotetun tason ja korkean tason ympäristöissä tietoturvakovennukset toteutetaan alustan luotettavuuden kautta. (Puolustusministeriö 2011.)

4 Usean palveluympäristön käyttö samalla päätelaitteella

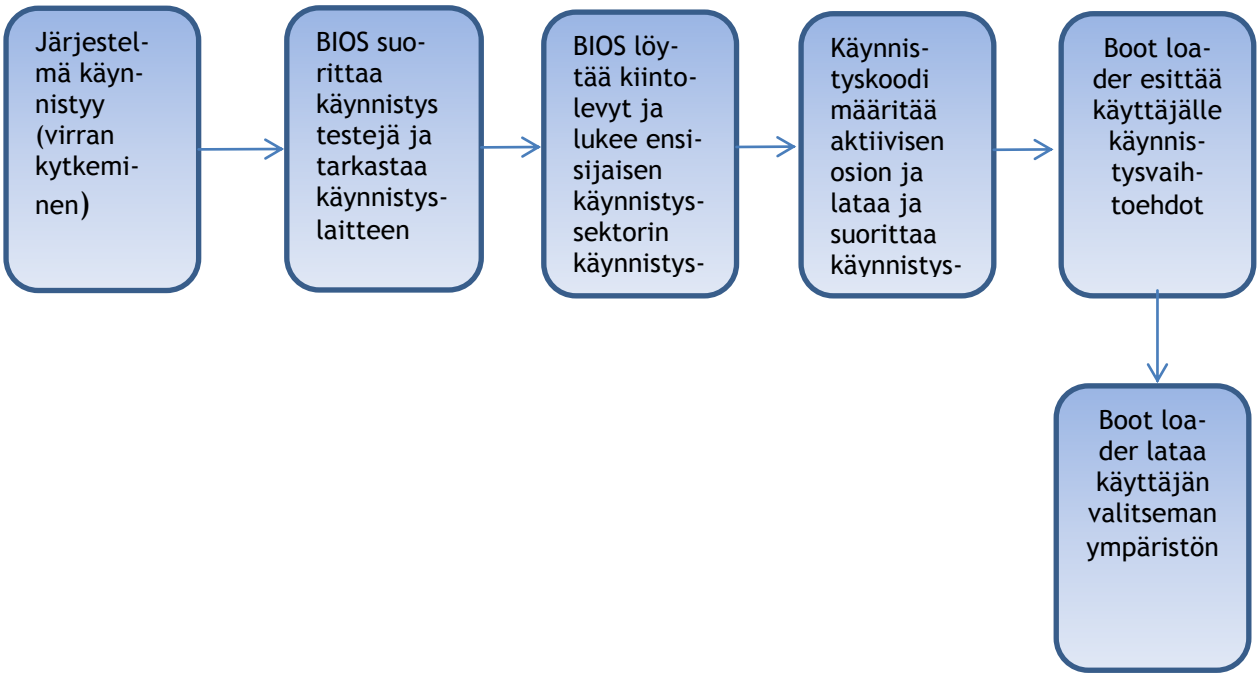
Tässä luvussa käsitellään päätelaitteen tekniseen toteutukseen vaikuttavia tekijöitä. Luvussa esitellään lyhyesti eri osatekijöiden vaikutusta ja omaisuuksia usean eri tietoturvaluokan päätelaiteratkaisua kehiteltäessä. Luvussa esiteltävät tekijät osoittautuivat tutkimusprosessin aikana merkittäviksi päätelaiteratkaisua kehiteltäessä.

4.1 Usean käyttöjärjestelmän käynnistymisprosessi

Mikäli samassa päätelaitteessa on useita eri käyttöjärjestelmiä, kone suorittaa multibootin. Käyttöjärjestelmät voivat sijaita samalla kiintolevyllä omassa osiossa eli partitiossa tai jokainen fyysisesti omalla kiintolevyllään. (Clyman 2004.) Tässä tutkimuksessa toteutetussa mallissa jokainen eri käyttöjärjestelmä sijaitsee omalla fyysisellä levyllään, sillä ne ovat eri tieto-

turvaluokan ympäristöjä. Eri tietoturvaluokan verkkoympäristöillä on erilaiset vaatimukset esimerkiksi laitehallinnalle, jonka vuoksi niitä ei voi käyttää samalla kiintolevyllä eri partitioissa. Jokaisessa kiintolevyssä ensimmäisen sektorin muodostaa Master Boot Record (MBR). Master Boot Record sisältää fyysisen kiintolevyn loogisen osiointitaulun (Clyman 2004).

Tietokoneen käynnistyessä BIOS etsii Master Boot Recordista käyttöjärjestelmän latauskoodin. Latauskoodin löydyttyä BIOS suorittaa koodin, joka tutkii aktiivisen osion ja lataa käyttöjärjestelmän käynnistymisen vaatiman tiedon. Boot loader esittää käyttäjälle käynnistysvaihtoehdot. Käyttäjän valitsee käynnistettävän palveluympäristön kiintolevyn, jonka jälkeen Windows-käyttöjärjestelmä latautuu. Windows-käyttöjärjestelmän lataamiseen käytettävä tiedosto on nimeltään NTLDR. (Clyman 2004, 80-81.) Kuviossa 5 on esitetty tietokoneen käynnistysprosessi kaaviona.



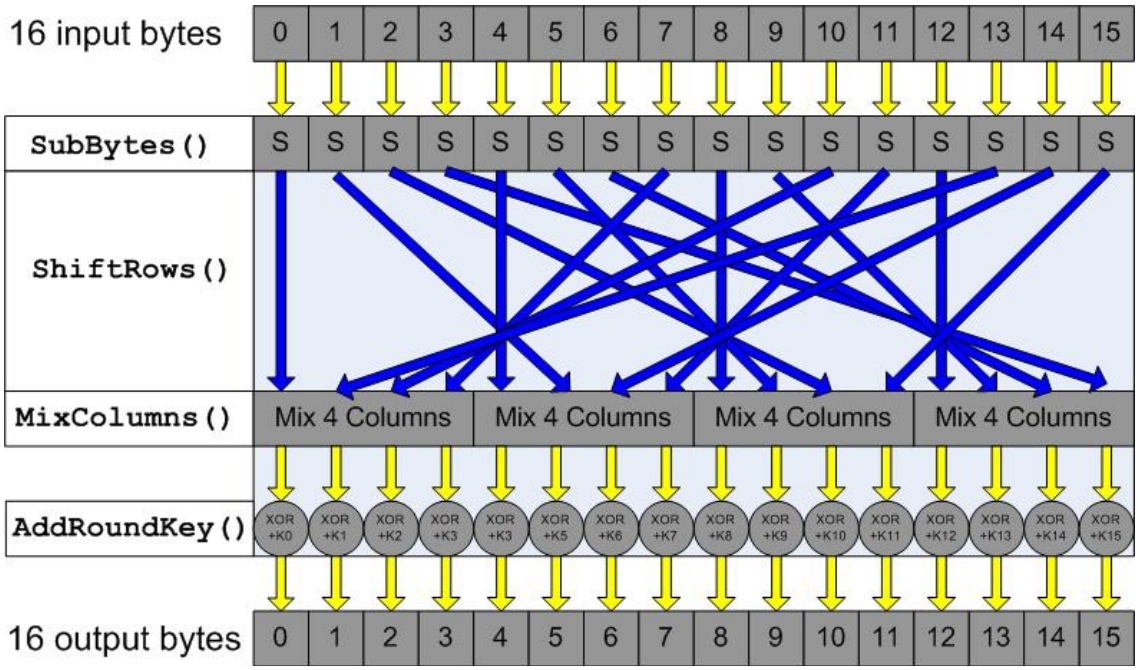
Kuvio 5. Tietokoneen käynnistymisprosessi (Clyman 2004, 80-81)

4.2 Kiintolevyn salaus

Nykyään entistä enemmän organisaatiolle kriittistä tietoa tallennetaan kannettavien päätelaitteiden kiintolevyille. Sen vuoksi on noussut tärkeäksi tekijäksi suojata kiintolevyillä oleva tieto mahdollisten tietovuotojen välttämiseksi. (Zhang, Chen, Tang, Xu, Li & Li 2009.) Yksittäisten tiedostojen salausten ohella esimerkiksi yrityssalaisuuksien turvaamiseksi käytetään koko kiintolevyn salausta (FDE) (Saarenmaa 2010). Kiintolevyn sisältö käsitellään kryptograafisella salaimella, lukuun ottamatta käynnistyssektoria – Master Boot Recordia, jota käyttöjärjestelmän on kyettävä lukemaan käynnistyäkseen (Saarenmaa 2010). Kiintolevyn vahva salaus

on tärkeää, jotta voidaan pienentää riskiä, ettei tieto joudu väärin käsiin laitteen tai kiintolevyn kadotessa.

AES (Advanced Encryption Standard) standardin kehittäminen DES:in (Data Encryption Standard) korvaajaksi aloitettiin tammikuussa vuonna 1997 yhdysvaltalaisen standardointivirasto NIST:in toimesta. Avoimen kilpailun voittajaksi ja uudeksi AES-algoritmiksi valittiin viiden kandidaatin joukosta Rijndaelin kehittämä algoritmi joulukuussa vuonna 2001. (Järvinen, 2008, 12.) AES on lohkosalausmenetelmä, jossa lohkon koko on 128 bittiä. Avaimissa on käytettävissä kolmea eri pituutta: 128-, 192- ja 256-bittiä. AES on iteratiivinen algoritmi ja käytettävien kierrosten määrä riippuu avaimen pituudesta. AES-128 sisältää 10 kierrosta, AES-192 12- ja AES 256 puolestaan 14 kierrosta. (Järvinen, 2008, 47.) Tässä tutkimuksessa käytetyn kiintolevynsalaustuotteen salausalgoritminä oli 256-bittinen AES, joka on algoritminä hyväksytty viestintäviraston toimesta korkeaan suojaustasoon saakka. Kuviossa 6 on kuvattu AES-salausalgoritmin tekninen toimintaperiaate.



Kuvio 6. AES-salausalgoritmin kierrosfunktion kuvaus (Conrad 2012)

AES - salausalgoritmi on lohkosalausmenetelmä, joka käyttää salauksessa kolmekerroksisesta muunnosta (Gustafsson 2012). Kierrosfunktio toteutetaan salausavaimen pituudesta riippuen 10, 12 tai 14 kertaa. Kierrosfunktio sisältää neljä erillistä tilaa muokkaavaa funktiota. Kuviossa 3 on kuvattu AES:in toimintaa yhdessä kierrosfunktiossa. Neljä tilaa muokkaavaa funktiota ovat kuviossa esitetyt SubBytes, ShiftRows, MixColums ja AddRounKey. AddRoundkey-funktio lisää kierrosavaimen XOR-operaatiolla. XOR-operaatio tarkoittaa poissulkevaa tai- operaatiota. SubBytes-funktio etsii S-Boksista tavuja vastaavat arvot. Kaikki tavut korvataan vuorol-

laan. Tavun neljä ensimmäistä bittiä määräävät tarkasteltavan rivin ja loput sarakkeen. Korvaava arvo muodostuu näiden risteyskohdasta. S-Box on kuvattu tutkimuksen liitteessä 6. (Havukainen & Kansanen 2004.) ShiftRows-funktio siirtää tavuja vasemmalle, ensimmäistä riviä lukuun ottamatta. AES-lohkosalausta käytetään tällä hetkellä laajasti niin valtionhallinnossa kuin yritysmaailmassakin. AES-salausalgoritmi on hyväksytty FIPS:in toimesta vuonna 2001 (FIPS 2011). Saarenmaan (2010) mukaan 256-bittistä AES-salausta ei ole tiettävästi kyetty murtamaan.

Tutkimuksessa käytettiin pääsääntöisesti Safeguard Easy - kiintolevynsalausohjelmistoa, joka löytyy Naton hyväksyttyjen salaustuotteiden listalta. Päätelaiteratkaisun auditoinnit suoritettiin päätelaitteeseen Safeguard Easy-ohjelmistolla salattuihin kiintolevyihin. Salausalgoritmeinä ohjelmistossa ovat käytettävissä AES-128 sekä AES-256. Lisäksi ohjelmisto täyttää Valtionhallinnon salauskäytäntöjen tietoturvaohjeen (2010) suositusten mukaisesti FIPS (Federal Information Processing Standard)- standardin asetukset.

4.3 DEVCON-työkalu

Devcon on Microsoftin kehittämä Windows-käyttöjärjestelmien laitehallintaan kehitetty komentoriviapuohjelma. Sen avulla voidaan laitteita ottaa käyttöön, poistaa käytöstä, käynnistää uudelleen tai päivittää laiteajureja. Työkalun avulla voidaan laitteille tai laiteryhmille tehdä myös kyselyjä. Se sisältää pääpiirteittään samat toiminnot kuin Windows-käyttöjärjestelmän graafinen laitehallintaliittymä. Devcon-työkalu toimii Windows 2000- ja sitä uudemmissa 32- ja 64-bittisissä Windows-käyttöjärjestelmissä. Työkalua voidaan käyttää skriptien eli komentojen avulla esimerkiksi poistamaan laitteita käytöstä automaattisesti. Devconin käyttö on mahdollista ainoastaan järjestelmänvalvoja-tasoisella käyttäjätunnuksella. (Microsoft 2012.) Windows 7-käyttöjärjestelmä vaatii vuonna 2010 päivitetyn version Devcon – työkalusta, jotta kaikki ominaisuudet toimivat oikein. Windows 7 - yhteensopiva versio Devconista on sisällytetty Windowsin Driver Kit 7.1.0 – päivityspakettiin.

Tässä tutkimuksessa Devcon-työkalua hyödynnetään toisen palveluympäristön kiintolevyn käytöstä poistamiseen. Tutkimuksessa tuotettua ratkaisua käyttöönotettaessa päätelaitteen levykuvaan tulee asentaa Devcon-työkalu. Koneen paikallisiin ryhmäkäytäntöjen käynnistyskomentoihin lisätään toisen ympäristön kiintolevyn käytöstä poistava komento: ”C:\\Windows\system32\i386\devcon.exe disable ”@IDE*0.0.0*”. Tällä toiminnolla varmistetaan, että eri suojaustason kiintolevyt eivät ole yhteydessä keskenään. Devcon-työkalun käyttö mahdollistaa Windows-käyttöjärjestelmän käynnistymisen salakirjoitettujen kiintolevyjen ollessa päätelaitteessa kiinni samanaikaisesti. Windows-käyttöjärjestelmä ei käynnisty, mikäli se käynnistyessään yrittää lukea toisen kiintolevyn salattua levynpintaa. Mikäli järjestelmänvalvoja tasoisella käyttäjätilillä otetaan toisen ympäristön kiintolevy käyttöön, ei Windows

käynnisty enää uudelleen. Tällöin skriptin ”hakkeroinnilla” saadaan aikaan ainoastaan toimimaton päätelaite. Kiintolevyn salaus suojaa toisen ympäristön tiedostoja siinä tapauksessa, että toisen kiintolevyn näkyvyys palautetaan käyttöjärjestelmän jo käynnistyttyä. Myös tämä toimenpide edellyttää järjestelmänvalvojan oikeuksia, joita turvaluokitelluissa ympäristöissä on ainoastaan valtuutetuilla käyttäjillä. Järjestelmänvalvoja tasoisella käyttäjätilillä toisen ympäristön kiintolevy on mahdollista formatoida. Devcon-työkalun asentaminen ja esimerkkejä käyttötapauksista on kuvattu tutkimuksen liitteessä 1.

4.4 Levykuva ja työasemien vakiointi

Levykuva (image) on tiedosto, johon on tallennettu koko sisältö ja rakenne massamuistista kuten kiintolevyltä. Levykuvan avulla voidaan toteuttaa työasemien vakiointi. Työasemien vakioinnilla voidaan saavuttaa merkittäviä säästöjä työasemien ylläpitoon kuluvissa henkilöstöresursseissa. Työasema-asennuksista suoriudutaan huomattavasti nopeammin, kun käyttöjärjestelmiä ja yksittäisiä ohjelmistoja ei tarvitse asentaa käsin jokaiselle työasemalle erikseen. Myös vian etsiminen vakioidusta työasemasta on huomattavasti helpompaa (Hurme 2011, 14).

Päätelaitteen tietoturvallisesti kovennettu asennus tehdään ympäristön suojaustason asettamien vaatimusten mukaisesti. Mallikoneeseen määritellään myös edellisessä luvussa kuvattu devcon-työkalua suorittava komento. Mallikoneesta otetaan levykuva, jota voidaan hyödyntää vastaavan laitemallin päätelaiteasennuksissa. Levykuvaa hyödyntämällä työasemien vakioinnissa jokaiselle päätelaitteelle ei tarvitse tehdä erikseen esimerkiksi tietoturvakovennuksia tai ohjelmistoasennuksia. Levykuvan asentamiseen käytetään laajoissa tietoteknisissä ympäristöissä usein erillistä ohjelmistoa. Tässä tutkimuksessa päätelaitteen levykuva asennettiin Symantecin Altiris Deployment Server-järjestelmällä. Järjestelmästä oli käytössä laboratoriotesteissä versio 6.9. KATAKRI edellyttää systemaattisesti toteutettua tietoturvallisesti kovennettua asennusta (Puolustusministeriö 2011). Levykuvan käyttö on tärkeä työkalu systemaattisen asennuksen osoittamiseksi ja toteuttamiseksi. Lisäksi levykuvan käyttö nopeuttaa päätelaite asennuksia merkittävästi. Tutkimuksessa päätelaiteauditointi suoritettiin työasemien vakioinnissa käytetyn levykuvalla asennetulla päätelaitekokoonpanolla. Mallikoneen läpäistyä auditoinnin levykuvaa voitiin hyödyntää ympäristön työasemien vakioinnissa tuotantoympäristössä.

4.5 Käyttöjärjestelmän suorittaminen ulkoiselta muistilta

Käyttöjärjestelmän suorittaminen ulkoiselta muistilta on mahdollista. Tässä tutkimuksessa kehitetyn teknisen ratkaisun soveltuvuutta tutkittiin myös käyttöjärjestelmää ulkoiselta muistilta suoritettaessa. Käytössä olleiden resurssien vuoksi laboratoriotestit jäivät vähäisiksi USB-

käynnistyksen osalta. Tehtyjen tutkimusten ja laboratoriotestien perusteella voidaan kuitenkin todeta, että esitetty ratkaisu tukee myös USB-muistilta käynnistämistä. Tulevaisuudessa päätelaitteet pienentyvät entisestään ja samaan laitteeseen ei välttämättä mahdu kahta kiinteää, fyysistä kiintolevyä. Tämän vuoksi on tärkeää, että tekninen ratkaisu soveltuu esimerkiksi ulkoiselta USB-muistilta suoritettavaan palveluympäristöön.

Laboratoriotesteissä Windows XP- ja Windows 7-käyttöjärjestelmiä käytettäessä USB-muistilta esiintyi lähinnä laiteajuriongelmia. Devcon- komentoa voidaan kuitenkin hyödyntää eri kiintolevyjen käytöstä poistamiseen koneen käynnistyksen yhteydessä, riippumatta muistin liitännästä. Windows 8-käyttöjärjestelmän myötä Microsoft tarjoaa käyttöjärjestelmälle paremman tuen USB-muistilta käynnistämiseen Windows To Go- toiminnon myötä.

5 Usean eri tietoturvaluokitellun ympäristön päätelaite

Tässä tutkimuksessa merkittävimmäksi haasteeksi osoittautui eri ympäristöjen kiintolevyjen yhteyden ja näkyvyyden estäminen toisille levyille. Tämän integroiminen valmiiksi levykuvaan ei ollut mahdollista muutoin kuin erillisen suoritettavan komennon avulla. Hankitun teoriatiedon soveltamisen ja käytännön testausten jälkeen päädyttiin Microsoftin kehittämän Devcon-työkalun käyttöön. Käyttöjärjestelmän käynnistyskomentoihin on lisättävä toisen ympäristön kiintolevyn käytöstä poistava komento. Esimerkiksi IDE-levyn käytöstä poistaminen tapahtuu seuraavalla komennolla: ”C:\\Windows\system32\i386\devcon.exe disable ”@IDE*0.0.0*”. Devcon-työkalu on asennettu esimerkissä Windowsin i386-kansoon, josta sitä suoritetaan komennolla. Komennon avulla loppukäyttäjän valitseman palveluympäristön käynnistyessä estetään muiden ympäristöjen näkyvyys ja käyttö automaattisesti.

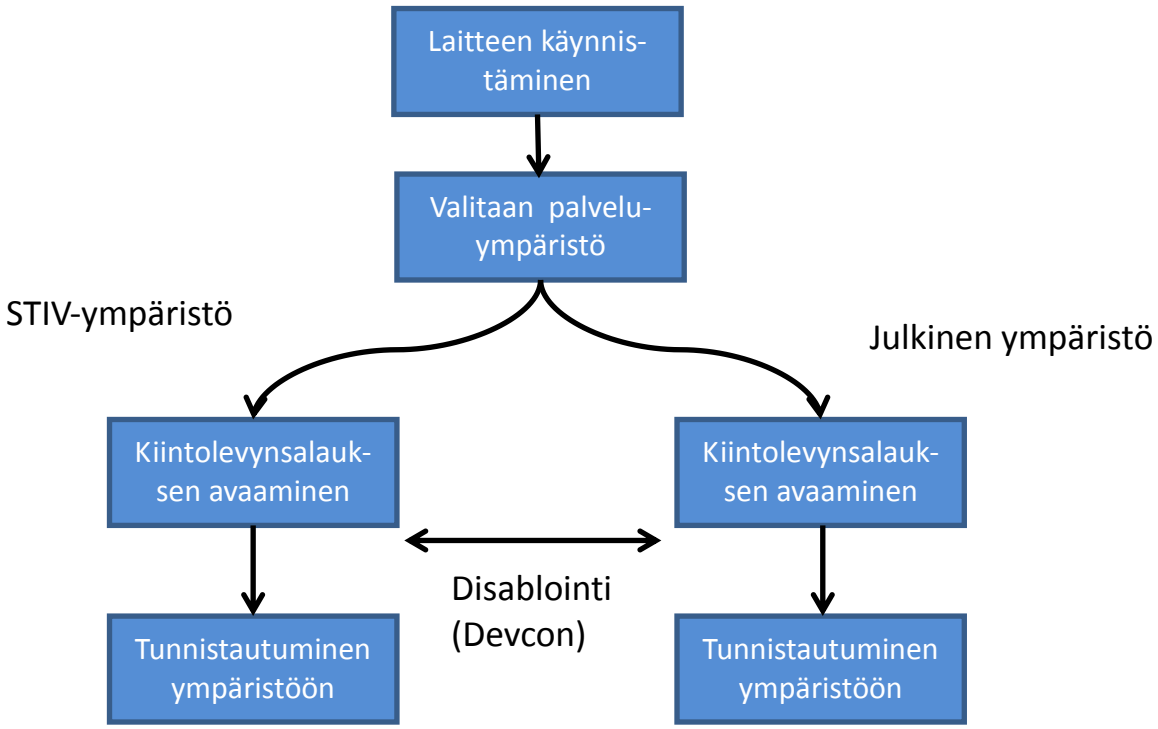
Toisena vaihtoehtona on kiintolevyjen manuaalinen käytöstä poistaminen Windowsin laitehallinnan kautta. Se ei kuitenkaan ole hyvä ratkaisu, sillä disabloinnit on tehtävä jokaiselle ympäristölle erikseen ennen kiintolevynsalauksen asennusta. Lisäksi skriptillä toteutettu ratkaisu estää automaattisesti seuraavan käynnistyskerran yhteydessä palveluympäristöjen keskinäisen näkyvyyden. Manuaalisesti toteutetussa mallissa toisen kiintolevyn käyttöönottaminen järjestelmänvalvoja-tasoisilla oikeuksilla tekee päätelaitteesta toimimattoman seuraavalla käynnistyskerralla. Toisen ympäristön kiintolevyn käytöstä poistaminen ei enää onnistu, mikäli kiintolevy on salakirjoitettu. Devcon-komento voidaan suorittaa myös Windowsin Active Directory-ympäristössä ryhmäkäytäntöjen avulla. Ryhmäkäytännöt on määritettävä tällöin koneeseen ennen kovalevyn salaamista. Laajoissa Active Directory- ympäristöissä, joissa päätelaitteet eivät ole vakioituja, voi ilmetä ongelmia, jos politiikkaa jaetaan laajasti. Komento voi johtaa tällöin tarpeellisten kiintolevyjen käytöstä poistamisiin. Tämä asettaa haasteita ympäristön ryhmäkäytäntöjen hallinnointiin ja rakenteeseen. Tämän vuoksi tutkimuksessa toisen kiintolevyn käytöstä poistava komento määritettiin ympäristön levykuvaan.

Eri tietoturvaluokan asettamat vaatimukset laitteen kokoonpanoasetuksiin vaihtelevat, kuten esimerkiksi verkkoasetukset, 3G, Bluetooth- asetukset. Laitteiden kokoonpanolle asetetut vaatimukset on otettava huomioon levykuvassa, jolloin tietoturvakovennukset tulevat päätelaitteeseen asennuksen yhteydessä. Päätelaitteen BIOS-asetukset on määritettävä korkeimman suojaustason ympäristön mukaisesti ja suojattava salasanalla. Ympäristöjen käynnistysjärjestys määritellään koneen BIOS-asetuksissa. Koneen virtoihin kytkeytymisen jälkeen loppukäyttäjä valitsee käynnistysvalikosta, minkä palveluympäristön käynnistää.

5.1 Päätelaitteen toimintaperiaate

Tässä luvussa esitetään toimintaperiaate usean eri ympäristön käytöstä samalla päätelaitteella. Esitetyssä toimintatapamallissa käydään läpi loppukäyttäjälle näkyvät toimenpiteet. Loppukäyttäjä kytkee päätelaitteeseen virran. Tämän jälkeen käyttäjälle näkyy laitteessa olevat ympäristöt, joista hän valitsee käynnistettävän ympäristön. Valikko on määritelty BIOS-asetuksissa näkymään 30 sekunnin ajan, mikäli käynnistettävää ympäristöä ei määritetä, käynnistyy oletusympäristöksi määritelty kiintolevy.

Kiintolevyn käyttöönottaminen edellyttää kiintolevyn levynsalauksen salasanan syöttämistä. Tämän jälkeen ympäristön käynnistyskomentoihin määritelty komento estää muiden ympäristöjen käytön ja käyttöjärjestelmä alkaa latautua. Käyttöjärjestelmän käynnistyttyä loppukäyttäjä tunnistautuu ympäristöön. Käytettävän palveluympäristön vaihto tapahtuu käynnistämällä kone uudelleen. Uudelleenkäynnistyksen yhteydessä valitaan käytettävä ympäristö ja suoritetaan edellä kuvatut toimenpiteet uudelleen. Päätelaitteen käyttö ja käynnistymisprosessi on esitetty kaaviona kuviossa 7. Kaaviossa esitetyssä esimerkissä kuvataan käyttötapaus, jossa päätelaitteessa on julkisen palveluympäristön ja perustason (STIV) palveluympäristön kiintolevyt.



Kuvio 7. Usean eri tietoturvaluokan palveluympäristön päätelaitteen toimintaperiaate

5.2 Päätelaiteratkaisun riskit

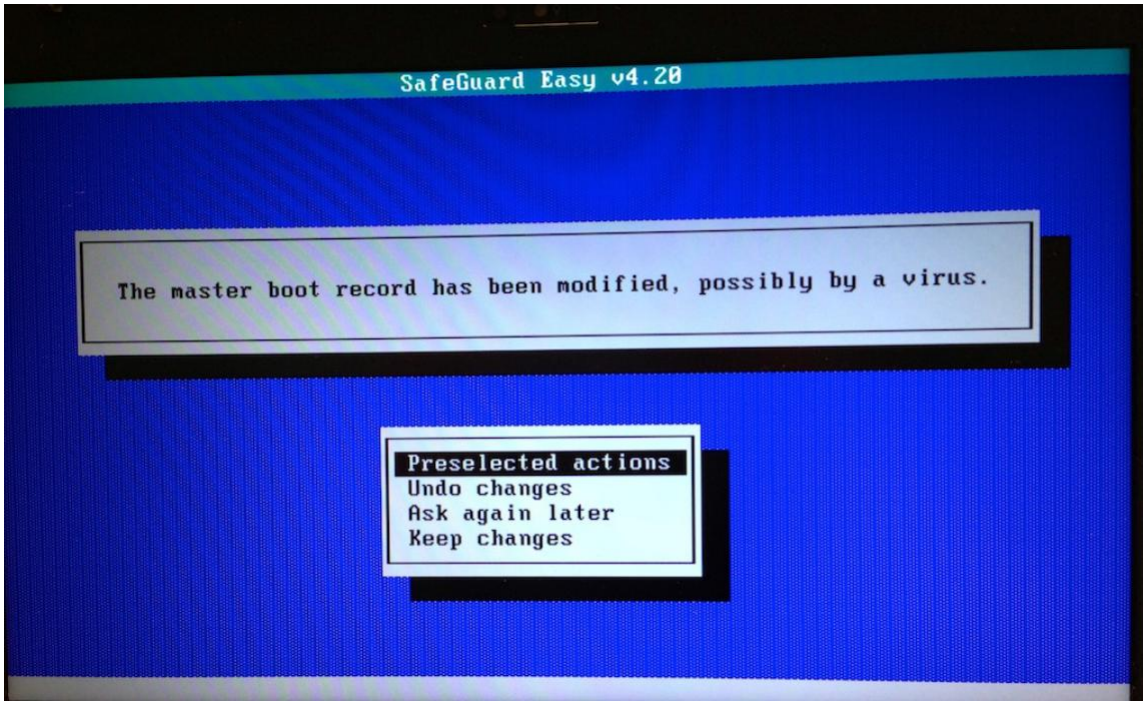
Tässä luvussa käsitellään tutkimuksessa kehitettyyn päätelaiteratkaisuun liittyviä riskejä. Luvussa esitetään riskien lisäksi niin teknisiä toimenpiteitä kuin toimintatapamalleja riskitasojen laskemiseksi. Luvun viimeisessä kappaleessa mahdollisia uhkia verrataan eri laitekoonpanoskenaarioiden välillä.

Päätelaiteratkaisun auditoinneissa ei löydetty merkittäviä tietoturvapoikkeamia. Matalan riskitason poikkeamiksi nähtiin Master Boot Record-osion saastuminen ja sen kautta haittaohjelman siirtyminen palveluympäristöstä toiseen. BIOS-järjestelmä sisältää kirjoittavan muistialueen, jonka kautta haittaohjelma voi mahdollisesti pesiytyä. Lisäksi päätelaitteeseen voi tarttua haittaohjelma ulkoisen USB-muistin tai muun siirrettävän median kautta. Merkittävimmäksi riskiksi nähtiin loppukäyttäjän kytkeytyminen väärään palveluympäristöön.

5.2.1 Master Boot Record-osion saastuminen

Kiintolevyn Master Boot Record- osio on kirjoitettavissa ja se tarjoaa teoriassa tartuntapinnan haittaohjelmille. MBR-osion on oltava salaamaton, jotta käyttöjärjestelmä pystyy käynnistymään. Tutkimuksessa levynsalaukseen käytetty Utimacon SafeGuard Easy -

kiintolevynsalausohjelmisto tarkistaa jokaisessa käynnistyksessä Master Boot Record-osion eheyden, joka tuo järjestelmälle lisäsuojan MBR-osioon tarttuvia viruksia vastaan. Teoriassa on mahdollista, että saastuneen MBR-osion kautta haittaohjelma voi siirtyä ympäristöstä toiseen, kun kiintolevyt ovat fyysisesti kytkettynä yhtä aikaa samaan päätelaitteeseen. Kiintolevynsalausohjelmiston tekemä Master Boot Record-osion eheystarkastus vähentää tätä riskiä huomattavasti. (Clarified Networks 2012.) Tutkimuksessa testattiin auditoinnin yhteydessä, että kiintolevyn salausohjelmisto todella varoittaa MBR-osion muokkaamisesta. Kiintolevynsalausohjelmiston konfiguroinneissa on mahdollista myös määrittää, että käyttöjärjestelmä ei käynnisty, mikäli MBR-osioon tehdään muutoksia. Kuviossa 8 on laboratoriotesteissä käytetyn Safeguard Easy - kiintolevynsalausohjelmiston varoitusilmoitus MBR-osion muuttumisesta.

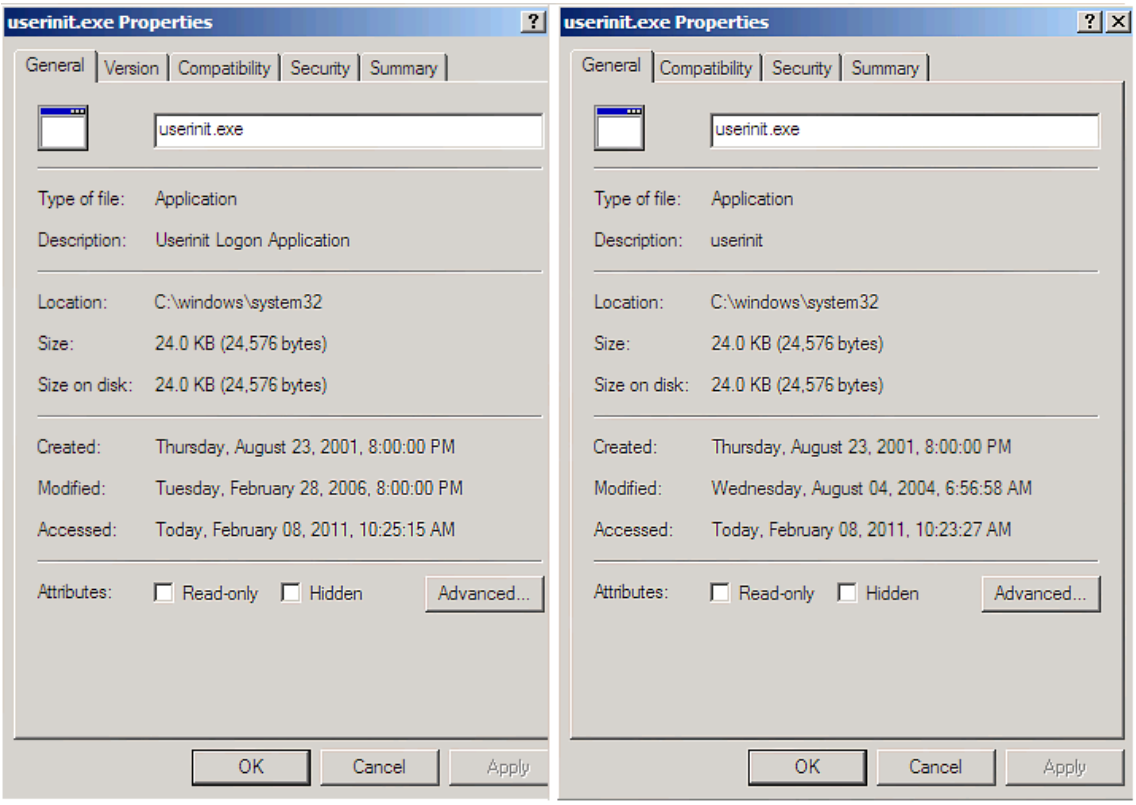


Kuvio 8. SafeGuard Easy-levynsalausohjelmiston virheilmoitus MBR-sektorin muuttumisesta

MBR-virus voi tyypillisesti tarttua ulkoisen median tai internet-rajapinnan kautta.
MBR-virus korvaa MBR-osion koodin viallisella koodilla. MBR-osion saastuminen on koneelle erittäin haitallista, sillä kone suorittaa MBR-osion käynnistyskoodin jokaisen käynnistymiskerran aikana. (Cheston, Dayan, & Springfield 2005.) Tällä hetkellä Master Boot Recordin kautta leviävät virukset eivät ole kovin yleisiä, mutta kuitenkin mahdollisia (F-Secure 2012). Niiden kehitys ei tällä hetkellä ole aktiivista, sillä muiden haittaohjelmien avulla saavutettavat taloudelliset hyödyt ovat tällä hetkellä ”hakkereita” houkuttelevampia. MBR-virukset olivat erittäin yleisiä DOS-aikoina 1990-luvulla. Master Boot Record-viruksia kuitenkin havainnoidaan maailmalla ja tämän voi todeta myös F-Securen virustietokannasta. (F-Secure 2012.) Master Boot Recordin saastuminen on kuitenkin mahdollista ja sen kautta virus voi teoriassa levitä ympäristöstä toiseen. MBR-virusten ehkäisemiseksi kiintolevynsalauksen MBR-osion tarkasta-

minen ja automaattinen palautuminen ovat erityisen tärkeitä toiminnallisuuksia. Tämä tulisi huomioida vaatimusmäärittelyssä kiintolevynsalaustuotetta hankittaessa. Nykyään myös tietoturvayritykset ovat varautuneet virustorjuntatuotteillaan MBR-viruksiin. Esimerkiksi Symantecilla on NBRT (Norton Bootable Recovery Tool), joka palauttaa saastuneen MBR-osion alkuperäiseksi (Symantec 2013). On kuitenkin mahdollista, että virustorjuntatuote ei tunnista MBR-virusta. MBR-virus aiheuttaa kuitenkin epäilyttävää verkkoliikennettä. Tällöin MBR-virusta kantava kone on havaittavissa tunkeutumisenhavaitsemis (IPS) -järjestelmän avulla. (Symantec 2013.)

Saastuneen Master Boot Recordin puhdistaminen voidaan toteuttaa myös korvaamalla saastunut MBR-osio Microsoftin työkaluilla. Päätelaite on tällöin käynnistettävä palautuskonsoliin. Windows XP- käyttöjärjestelmässä tulee suorittaa fixmbr-komento. Windows 7 - käyttöjärjestelmässä saman toimenpiteen voi suorittaa Bootrec-komennolla. Kansallinen turvallisuusauditointikriteeristö ei ota kantaa Master Boot Record - viruksen aiheuttamaan uhkaan tai sen vaikuttavuuteen eri suojaustasoilla. Tässä tutkimuksessa MBR-viruksen riskitason arviointi perustui ulkopuolisen asiantuntijan arvioon turvallisuusauditoinnin yhteydessä. Lisäksi MBR-viruksen yleisyyttä ja todennäköisyyttä kartoitettiin alan asiantuntijoilta sekä F-Securen virustietokannasta. Kuviossa 9 on esitetty F-Securen julkaisema esimerkki MBR-viruksen saastuttamasta userinit.exe-tiedostosta. Kuviossa 9 on esitetty alkuperäinen sekä MBR-viruksen saastuttama userinit.exe-tiedosto.



Kuvio 9. Alkuperäinen ja MBR-viruksen saastuttama Userinit.exe (F-Secure 2008)

5.2.2 Devcon-ohjelmistoa suorittavan skriptin korruptoituminen

Laboratoriotesteissä käyttämättömän ympäristön kiintolevyä yritettiin ottaa käyttöön järjestelmänvalvojatasoisella käyttäjätunnuksella. Toisen kiintolevyn tietoja ei päässyt selaamaan kiintolevyjen salauksesta johtuen. Mikäli toisen kiintolevyn disabloiva komento poistettiin käytöstä järjestelmänvalvoja tasoisella tunnuksella, ei käyttöjärjestelmä pystynyt enää käynnistymään. Testien perusteella uskon sen johtuvan siitä, että käyttöjärjestelmän käynnistyessä se pyrkii lukemaan salakirjoitettua kiintolevyn pintaa. Lopputuloksena oli ”bluescreen” ja koneen käynnistyminen uudelleen. Tietoturvan kannalta tämä on hyvä, sillä esimerkiksi virheellisen asennuksen jälkeen ei ole mahdollista, että loppukäyttäjä pystyy käyttämään päätelaitetta siten, että eri tietoturvaluokan ympäristöt ovat yhteydessä keskenään.

Tämän tutkimuksen laboratoriotesteissä ei ollut käytettävissä Windows 8 - käyttöjärjestelmää. Windows 8 – käyttöjärjestelmässä on sisäänrakennettuna Master Boot Recordin saastumista ehkäisevä Trusted Boot- ominaisuus. Ominaisuus tarkkailee käynnistysprosesseihin kätkeytyviä haittaohjelmia ja siten ehkäisee niiden leviämistä ympäristöltä toiselle Master Boot Recordin kautta (Tamminen 2012). Tässä tutkimuksessa ei ratkaisua testattu Windows 8-käyttöjärjestelmällä.

5.2.3 Kirjautuminen väärään palveluympäristöön

Auditoinnissa merkittävimmäksi riskiksi arvioitiin, että loppukäyttäjä ei tiedä, minkä ympäristön kiintolevyä käynnistetään. Tätä riskiä voidaan pienentää huomattavasti, kun käynnistettävän ympäristön kiintolevynsalausohjelmiston kirjautumissivulle nimetään selkeästi ympäristö. Lisäksi auditoinnissa todettiin, että eri turvaluokan levyjen salaukseen tulisi käyttää eri salasanoja virheiden välttämiseksi. Tämä olisi hyvä varmistaa myös teknisesti. (Clarified Networks 2012.)

Tutkimuksen edetessä auditoinnin perusteella havaittiin, että eri ympäristöt on eroteltava toisistaan selkeästi loppukäyttäjälle. BIOS-asetuksissa tulee määrittää käynnistysvalikko näkymään riittävän pitkäksi aikaa, jotta käyttäjä ehtii valitsemaan tarvitsemansa ympäristön. Kiintolevynsalaussovelluksen kirjautumisnäkymään lisättiin myös merkintä käynnistettävästä ympäristöstä, jotta käyttäjä voi olla varma, että on kirjautumassa oikeaan ympäristöön. Mikäli mahdollista tulisi myös kiintolevynsalausohjelmiston konfiguroinnit toteuttaa niin, että salasanaksi ei voi määrittää samaa salasanaa eri ympäristöihin. Tällä toimenpiteellä ehkäistään riskiä kirjautua väärään ympäristöön.

Teknisten ratkaisuiden lisäksi on tärkeää, että loppukäyttäjiä ohjeistetaan riittävästi laitteen käytössä. Esimerkiksi ympäristöä vaihdettaessa tulee huomioida, että on kytkeytynyt oikean verkon liityntäpisteeseen. Tämän vuoksi myös eri palveluympäristöjen verkon liityntäpisteissä tulee olla selkeä merkintä.

5.2.4 Yleisesti tunnetut riskit päätelaitteelle

Moderneissa tietokoneissa on useampia kirjoitettavia muistialueita, joihin haittaohjelma voi mahdollisesti tarttua ja sitä kautta siirtyä koneella käytettävien ympäristöjen välillä. Esimerkiksi BIOS ja näytönohjaimen firmware ovat tällaisia. Tämä riski on sama, riippumatta siitä ovatko levyt yhtä aikaa fyysisesti kytkettynä koneeseen vai irrotetaanko käyttämätön levy välillä. (Clarified Networks 2012.)

Käyttäjä saattaa vahingossa tai tarkoituksella kytkeä koneeseen saastuneen USB-muistin. USB-muistin kautta koneelle voi tarttua haittaohjelma. Tämä riski on myös sama, riippumatta siitä ovatko levyt yhtä aikaa fyysisesti kytkettynä koneeseen vai irrotetaanko käyttämätön levy. (Clarified Networks 2012.)

5.2.5 Yhteenveto päätelaiteratkaisun riskeistä

Päätelaitteiden kehittämisessä tulee teknisten toimenpiteiden ohella keskittyä siihen, että päätelaitteiden loppukäyttäjiä ohjataan luonnolliseen, turvalliseen käyttöön. Tietoturva-alan asiantuntijoiden haastatteluissa ilmeni, että todellisuudessa merkittävimmäksi riskiksi muodostuu todennäköisesti loppukäyttäjä. Tällöin korostuu ohjeistus- ja päätelaitteen riittävä koulutus, jotta päätelaitetta osataan käyttää oikein. Loppukäyttäjän on päätelaitteen toimintaperiaatteen omaksumiseksi harjoiteltava riittävästi.

Taulukossa 4 esitetään tässä aikaisemmin tässä luvussa esitetyt mahdolliset uhkakuvat päätelaitteelle. Uhkakuvat on arvioitu eri laitekokoonpanoskenaarioissa. Ensimmäiseksi arvioitiin tunnistettuja uhkia tutkimuksessa esitetyn teknisen ratkaisun mukaisesti, jolloin päätelaitteessa on sama runko ja levyt eriytetty toisistaan teknisesti. Toisessa skenaariossa uhkat arvioitiin päätelaitteessa, jossa koneen runko on sama, mutta kiintolevy vaihdetaan koneeseen fyysisesti toiseen palveluympäristöön siirryttäessä. Viimeisessä skenaariossa uhkat arvioitiin vaihtoehtoa, jossa eri tietoturvaluokan palveluympäristöjä käytetään fyysisesti eri päätelaitteilla.

UHKA	Sama päätelaitteen runko, levyt eriytetty teknisesti	Sama päätelaitteen runko, vaihdettava kiintolevy	Erilliset päätelaitteet
USB-muisti tai muu siirrettävä media	X	X	X
Koneen kytkeminen väärään verkkoon	X	X	X
BIOS:n tai muun ohjaimen ohjelmiston saastuminen	X	X	
Haittaohjelman leviäminen saastuneen MBR-osion kautta	X		

Taulukko 4. Mahdolliset uhat eri laitteistokokoonpanoille (Clarified Networks 2012)

Päätelaiteratkaisun tekniseen toteutukseen liittyvät riskit eivät ole niin merkittäviä, että ne estäisivät ratkaisun tuotantokäytön. Tutkimuksen aikana toteutetuissa auditoinneissa ei havaittu esteitä teknisen toteutuksen käytölle korotetun suojaustason (STIII) ympäristölle saakka. Tutkimuksessa ratkaisua ei auditoitu suojaustasoa II vasten.

Tutkimuksessa toteutettu ratkaisumalli on implementoinnin jälkeen asennettu tuotantoympäristössä noin 700:ään päätelaitteeseen. Tällöin ratkaisun toimivuudesta on olemassa melko kattavasti näyttöä. Tekninen ratkaisu on hyväksytty tuotantokäyttöön Puolustusvoimissa turvallisuusauditoinnin seurauksena. Tekninen ratkaisu vaikuttaa toimivalta eikä teknisiä ongelmia ole tuotantokäytössä ilmennyt. Aiheeseen liittyviä julkaisuja oli saatavilla vähän. Tämän vuoksi ei voida taata, ettei ongelmaan löytyisi toista ratkaisua. Nyt käytetty malli vaikuttaa hyvältä, sillä komennon avulla suoritettava työkalu on käyttöjärjestelmän toimittajan, Microsoftin ohjelmisto. Tämän vuoksi on todennäköistä, että työkalu on yhteensopiva myös tulevaisuudessa julkaistavien Microsoftin käyttöjärjestelmäversioiden kanssa. Esimerkiksi tutkimusta tehtäessä uusin Microsoftin Windows 8-käyttöjärjestelmä tukee Devcon-työkalun käyttöä.

Tutkimuksen luotettavuuden parantamiseksi teknistä ratkaisua esiteltiin alan asiantuntijoille. Heidän kanssaan käydyt keskustelut ja haastattelut vahvistivat näkemystä ratkaisun käytettävyydestä. Negatiivista palautetta ei haastatteluiden yhteydessä saatu. Asiantuntijahaastattelut vahvistivat myös näkemystä haasteista virtualisoidun ratkaisun löytämiseksi usean eri turvaluokan päätelaitteelle. Tutkimuksessa käytettävissä olleiden resurssien näkökulmasta voidaan jälkeenpäin todeta, että oli oikea ratkaisu lähestyä tutkimusongelmaa usean eri fyysisen kiintolevyn ratkaisulla. Kehitetty ratkaisu on yksinkertainen toteuttaa ja se on sen vuoksi helppo implementoida eri ympäristöissä. Lisäksi tutkimuksessa esitetty ratkaisu skaalautuu hyvin ympäristöihin, joissa eri palveluympäristöjä hallinnoi ja ylläpitää eri organisaatiot.

Tutkimuksessa olisi ehkä voinut myös kartoittaa kattavammin kansainvälisesti, onko olemassa vastaavanlaisia ratkaisuja muualla käytössä. Ongelmaksi olisi saattanut muodostua työn julkisuus. Tällöin esimerkiksi eri maiden puolustushallinnon materiaalia ei opinnäytetyössäni olisi voitu hyödyntää. Tutkimuksessa käytössä olleiden resurssien vuoksi tutkimuksessa käytettyjä päätelaitemalleja ei ollut käytössä kuin yksi, joten laajaa näyttöä toimivuudesta eri laitemalleissa ei ole olemassa. Tutkimuksessa kehitetty ratkaisu ei ole riippuvainen laitemallista, mutta testeillä tätä havaintoa ei ole todennettu. Tekninen ratkaisu perustuu Windows käyttöjärjestelmän ominaisuuksiin ja toiminnallisuuksiin, jonka vuoksi päätelaitemallilla ei ole merkitystä teknisen toteutuksen näkökulmasta.

Päätelaitteen turvallisuusauditoinneissa ei tullut esille merkittäviä tietoturvapoikkeamia. Kiintolevynsalausohjelmiston Master Boot Record-osion tarkastuksella voidaan pienentää MBR-virusten teoreettista uhkaa leviämisestä eri ympäristöjen välillä merkittävästi. MBR-virukset eivät vaikuta tällä hetkellä olevan kovin yleisiä, mutta tulevaisuudessa tämä riski tulee ottaa huomioon salaustuotetta käyttöönotettaessa. Lisäksi käyttäjien ohjeistukseen ja kouluttamiseen on kiinnitettävä huomioita. Eri palveluympäristöt tulee erottaa toisistaan mahdollisimman selkeästi, jotta virheellisiltä kirjautumisilta vältyttäisiin. Esimerkiksi kiintolevynsalausohjelmiston kirjautumissivulle tulee merkitä selkeästi käynnistettävä ympäristö, jotta loppukäyttäjä tietää mitä ympäristöä ollaan ottamassa käyttöön. Lisäksi käynnistysvalikkoon olisi hyvä kuvata käytettävä palveluympäristö. Merkittävimpänä riskinä todettiinkin loppukäyttäjän kirjautuminen väärään palveluympäristöön.

Loppukäyttäjän tulee myös muuttaa mahdollisesti aiempia työskentelytapojaan, sillä hänen on mahdollista käyttää yhtä palveluympäristöä kerrallaan. Näkemykseni mukaan organisaation johdon tulee tukea yhden koneen politiikan käyttöönottoa, jotta ratkaisu saadaan laajamittaiseen käyttöön organisaatiossa. Mikäli organisaatio ei sitoudu siihen, niin ratkaisulla saavutettavia kustannussäästöjä ei saada täysimääräisinä. Esimerkiksi lisenssejä tai päätelaitteiden leasing-sopimuksia ei voida päättää tai irtisanoa systemaattisesti, mikäli loppukäyttäjä ei luovu vanhoista erillisistä päätelaitteista.

Tutkimukselle asetetut vaatimukset ja tavoitteet täyttyivät hyvin. Tutkimuksessa kehitettiin ratkaisu todellisessa ympäristössä olevaan ongelmaan. Kehitetty ratkaisu täytti tietoturvallisuusauditointikriteeristön vaatimukset ja sen turvallisuus todennettiin turvallisuusviranomaisen toteuttamalla auditoinnilla. Teknisen ratkaisun avulla toteutetulle päätelaiteratkaisulle on myönnetty tuotantokäyttölupa ja ratkaisun toimivuus on osoitettu laajassa tuotantokäytössä.

Kansallisessa turvallisuusauditointikriteeristön liitteessä on maininta, että korotetun suojaustason (STIII) työaseman tai kannettavan BIOS-asetuksissa tulisi olla sallittuna ainoastaan ensisijaiselta kiintolevyltä käynnistys. Päätelaiteratkaisun auditoinneissa tätä ei koettu riskiksi. Muilla teknisillä toimenpiteillä päätelaitteesta saadaan turvallinen. (Puolustusministeriö 2011, 120.) Esimerkiksi BIOS-asetuksissa käytöstä poistetaan kaikki tarpeettomat palvelut. Lisäksi SafeGuard Easy - kiintolevynsalausohjelmiston konfiguroinneissa on mahdollista estää muilta medioilta käynnistäminen käyttöjärjestelmän käynnistymisprosessissa. Tällä ominaisuudella ehkäistään esimerkiksi ulkoiselta ei- sallitulta USB-medialta käynnistys, kun kiintolevynsalausohjelmiston salasana on syötetty ja käyttöjärjestelmä lähtee käynnistymään. Tämä toiminnallisuus testattiin myös laboratoriotesteissä ja auditoinnissa. Kansallisessa turvallisuusauditointikriteeristössä on maininta, että ”KATAKRI koulutuksen erityistavoitteena on luoda auditoijille kyky korvaavien keinojen hyödyntämiseen tapauksissa, joissa yksittäisen vaatimuksen täyttäminen ja toteuttaminen on vaikeaa taikka mahdotonta.” (Puolustusministeriö 2011, 3.)

6 Yhteenveto ja johtopäätökset

Tutkimuksessa kehitettiin tekninen ratkaisu, joka täyttää kansallisen turvallisuusauditointikriteeristön vaatimukset. Kriteeristö on laajasti käytössä niin valtionhallinnossa kuin yritysmaailmassa. Ratkaisua voidaan hyödyntää vapaasti ja sen myötä on mahdollista saavuttaa merkittäviä kustannussäästöjä niin laite- kuin lisenssikustannuksissa organisaatioissa, joissa on käytössä useita eri tietoturvaluokan palveluympäristöjä.

Tutkimuksessa esitetyn ratkaisun käyttöönoton myötä on mahdollista saavuttaa merkittäviä kustannussäästöjä. Laitekustannusten lisäksi säästöjä saadaan lisensseistä. Useissa lisensseissä on mahdollista yhden lisenssin käyttö, mikäli yhdeltä päätelaitteelta käytetään yhtä ympäristöä kerrallaan. Esimerkiksi työntekijällä, jolla on aiemmin ollut eri tietoturvaluokan ympäristöihin oma päätelaite, vaaditaan jokaiseen laitteeseen oma lisenssi. Saavutettavia kustannussäästöjä laite- ja lisenssikustannusten osalta on esitetty esimerkin avulla liitteessä 3.

Tutkimustuloksia voidaan hyödyntää laajasti. Eri tietoturvaluokan ympäristöjä on tällä hetkellä monessa organisaatiossa ja tulevaisuudessa tietoturvallisuuteen ja kustannustehokkuuteen tullaan kiinnittämään entistä enemmän huomiota. Tutkimuksessa kehitetty ratkaisu on käyttökelpoinen tapauksissa, joissa eri ympäristöjä ei tarvitse käyttää samanaikaisesti. Tutkimuksessa käytetty turvallisuusauditointikriteeristö on käytössä Suomessa laajasti. KATAKRI:n turvallisuusvaatimusten perusteella rakennetaan ja kehitetään esimerkiksi valtionhallinnon organisaatioiden sekä suurten yritysten tietotekniikka-arkkitehtuuria. Teknistä ratkaisua voidaan hyödyntää etenkin valtionhallinnossa. Valtionhallinnon lisäksi ratkaisu voisi soveltua esimerkiksi pankkialalle, verohallintoon sekä tilitoimistoihin (L.Liljequist, henkilökohtainen tiedonanto 9.4.2013). Usein myös puhelinmyynnissä myydään kilpailevien organisaatioiden palvelui-

ta ja tuotteita (esimerkiksi lehtimyynnissä ALMA, Sanoma), jolloin on tärkeää, että eri organisaatioiden tiedot ovat eroteltu selkeästi toisistaan. Lisäksi eri organisaatioiden tutkimusryhmillä on usein tarve työskennellä tietoturvaluokitellun aineiston parissa, jolloin tutkimuksessa esitettyä ratkaisua voitaisiin hyödyntää (P.Åström, henkilökohtainen tiedonanto 18.4.2013).

Tutkimuksessa esitetyn teknisen ratkaisun riskit eivät vaikuta korkeilta. Esimerkiksi MBR-osion saastuminen toisen palveluympäristön kautta ei vaikuta kovin todennäköiseltä. MBR-viruksia esiintyi vielä 2000-luvun alussa, etenkin DOS-aikoina. Nykyään kuitenkaan MBR-virukset eivät ole kovin yleisiä. Osaltaan tähän vaikuttaa se, että MBR-viruksia houkuttelevampia kohteita on ”hakkereille” tarjolla, joista voi saavuttaa taloudellista hyötyä MBR-saastuttamista enemmän. Riski on kuitenkin olemassa ja kiintolevynsalaussovelluksen MBR-osion tarkastuksella tätä riskiä voidaan merkittävästi pienentää. Teknisiä riskejä merkittävämmäksi nähtiin loppukäyttäjän toimet, kuten kirjautuminen väärään palveluympäristöön. Päätelaitteen ohjeistukseen ja koulutukseen on kiinnitettävä huomiota. Eri ympäristöt on eroteltava mahdollisimman selkeästi toisistaan niin käynnistysvalikossa kuin kiintolevynsalausohjelmiston kirjautumissivulla. Käytettävyyden näkökulmasta loppukäyttäjän tulee opetella työskentelytapa, jossa yhtä palveluympäristöä käytetään kerrallaan. Palveluympäristön vaihto tapahtuu uudelleen käynnistyksen yhteydessä.

Tutkimusmenetelmäksi valitsemani Nunamakerin monimenetelmällinen tietojärjestelmän kehittämistutkimuksen malli soveltui tutkimukseen hyvin. Jälkeenpäin voidaan todeta, että se sopi erinomaisesti tutkimukseen, jossa rakennettiin tekninen ratkaisumalli aikaisemmin ratkaisemattomaan ongelmaan. Tutkimusprosessissa testaamisen ja teoriatiedon yhdistäminen käytännön tuotekehitystyöhön palvelivat tutkimukselle asetettuja tavoitteita parhaiten.

Toteutin tutkimuksen ja siinä esitetyn ratkaisun itsenäisesti. Hyödynsin tutkimuksessa kolmea oman organisaationi edustajaa, joilta hain palautetta esittämälleni ratkaisulle. Lisäksi Maanpuolustuskorkeakoulun tietoturvapäällikön asiantuntemusta hyödynnettiin KATAKRI:n tulkitsemisessa. Tutkimuksessa esitetty ratkaisu on auditoitu Puolustusvoimissa Maanpuolustuskorkeakoulun ympäristössä tutkimusprosessin aikana vuosina 2012 ja 2013. Tekniselle ratkaisulle on myönnetty tuotantokäyttölupa. Teknistä ratkaisua käytettäessä tulee huomioida, että ratkaisun avulla käytetyt palveluympäristöt tulee myös olla auditoitu. Korkean suojaustason (STII) ympäristön mukaista ulkopuolisen suorittamaa auditointia tekniselle ratkaisulle tämän tutkimuksen yhteydessä ei toteutettu.

Tutkimuksessa esitettyä teknistä ratkaisua on hyödynnetty Maanpuolustuskorkeakoulun ympäristössä vuoden 2013 huhtikuun loppuun mennessä noin 700:ssä päätelaitteessa. Ratkaisu on toiminut hyvin, eikä teknisiä ongelmia ole ilmennyt. Kustannussäästöjä on saavutettu noin 200 000 euroa vuodessa. Säästetyt lisenssikustannukset ovat noin 60 000 euroa ja 140 000 eu-

ron säästö on syntynyt vähentyneiden päätelaitteiden vuokrista. Kustannussäästöjä on mahdollista saavuttaa enemmän vanhojen päätelaitteiden vuokra-ajan umpeutuessa. Saavutettavia kustannussäästöjä on esitetty yksityiskohtaisemmin opinnäytetyön liitteessä 4.

6.1 Jatkotutkimusaiheet

Tutkimusta tehtäessä tietoturvavaatimukset täyttävää ja auditoitua päätelaiteratkaisua eri tietoturvaluokan palveluympäristöjen käyttämiseksi ei ollut olemassa. Tietoturvavaatimukset vaikeuttavat virtualisoidun ratkaisun kehittämistä. Lisäksi virtualisoidun päätelaiteratkaisun haasteena ovat käytettävyys sekä suorituskyky (P.Åström, henkilökohtainen tiedonanto 18.4.2013). Esimerkiksi omassa työympäristössä eri palveluympäristöt ovat usein eri organisaation ylläpitämiä, joka myös vaikeuttaa virtualisoidun päätelaiteratkaisun kehittämistä. Lisäksi mahdollinen virtualisoitu ratkaisu voi olla haastava sellaiselle loppukäyttäjälle, joka ei ole teknisesti valveutunut. Tässä tutkimuksessa virtualisoidun päätelaiteratkaisun kehittäminen rajattiin pois, sillä tarkoituksena oli kehittää tutkimusprosessin aikana konkreettinen tuotantokäyttöön soveltuva ratkaisu.

Teoriassa on mahdollista, että eri palveluympäristöjä voisi ajaa myös samalta, osioidulta kiintolevyltä. Tällöin päätelaitteessa ei tarvitsisi välttämättä useaa kiintolevyä (P.Åström, henkilökohtainen tiedonanto 18.4.2013). Esimerkiksi tutkimuksessa käytetty kiintolevynsalaustuote tukee osioidun kiintolevyn käyttöä. Ratkaisu asettaa kuitenkin käytännön haasteita esimerkiksi ylläpidolle. Käyttöjärjestelmän image on haastavaa asentaa tietylle kiintolevyn osiolle siten, että mahdollisesti kiintolevyn toisella osiolla olevan palveluympäristön asennus säilyy samalla levyllä. Haasteita aiheuttaa myös levynsalauksen hallinnointi, mikäli eri ympäristöistä vastaa eri organisaatiot. Kiintolevyn rikkoutuessa loppukäyttäjä ei kykenisi työskentelemään päätelaitteella lainkaan. Tämän vuoksi fyysisesti eri kiintolevyjen käyttö takaa loppukäyttäjälle paremman käytettävyyden. Tutkimuksessa esitetty ratkaisu skaalautuu laajemmin eri ympäristöihin. Esimerkiksi omaan työympäristööni ei osioidun kiintolevyn käyttö soveltuisi. Osittain tämän vuoksi tässä tutkimuksessa ei testattu syvällisemmin eri palveluympäristöjen käyttöä eri kiintolevyn osioilta. Se voisi soveltua joihinkin ympäristöihin. Teknisessä ratkaisussa voisi hyödyntää devcon-työkalua eri osioiden erotteluun. Ratkaisua tulisi kuitenkin testata runsaasti ja suorittaa tietoturva-auditointi, jotta ratkaisun tuomat mahdolliset lisäriskit saadaan kartoitettua.

Tutkimuksessa käyttöjärjestelmän käynnistäminen ulkoiselta muistilta jäi vähälle resursseista johtuen. Päätelaitteiden pienentyessä on ehdottoman tärkeää, että ympäristöjen käyttö onnistuu myös ulkoiselta muistilta, sillä päätelaitteeseen ei enää välttämättä mahdu useaa kiinteää kiintolevyä. Tutkimuksessa esitettyä ratkaisua voidaan soveltaa myös ulkoiselta muistilta käyttöjärjestelmän suorittamiseen. Lähinnä ajurihaasteet tulee ratkaista tuossa kontekstissa.

Windows 8-käyttöjärjestelmä tarjoaa Windows To Go – toiminnallisuuden, jonka avulla käyttöjärjestelmän suorittaminen USB-muistilta helpottuu. Laboratoriotesteissä suoritettujen testien ja havaintojen osalta voidaan todeta, että tekninen ratkaisu soveltuu myös ulkoiselta muistilta ajettavaan käyttöjärjestelmään. Tässä tutkimuksessa Windows 8 – käyttöjärjestelmää ei laboratoriotesteissä käytetty ja se rajattiin tutkimuksen ulkopuolelle. Tekninen ratkaisu on kuitenkin yhteensopiva Windows 8-käyttöjärjestelmän ja todennäköisesti myös tulevaisuudessa julkaistavien Microsoftin Windows-käyttöjärjestelmäversioiden kanssa.

Tutkimuksessa kehiteltiin tuote Windows-käyttöjärjestelmäympäristöihin. Jatkossa tulee tutkia myös käyttöjärjestelmäriippumatonta ratkaisua, jolloin myös MAC – ja Linux- päätelaiteympäristöissä voidaan siirtyä yhden koneen politiikkaan. Tulevaisuudessa voisi myös tutkia, voidaanko eri tietoturvaluokan palveluympäristöjä käyttää niin sanotulla ”tyhmällä” päätelaitteella, jolloin itse päätelaitteelle ei tallenneta mitään ja käytettävien palveluiden käyttö toteutetaan tietoturvaluokan vaatimusten mukaisella tunnistautumismenetelmällä sekä tietoliikenteen salausalgoritmillä.

Lähteet

AES Crypt. 2013. AES information. http://www.aescrypt.com/aes_information.html. Viitattu 10.8.2012

Alomari, M. A., Samsudin, K. & Ramli, A. R. 2009. A Study on Encryption Algorithms and Modes for Disk Encryption. International Conference on Signal Processing Systems, 793–797.

Anttila, P. Triangulaatio. Ylemmän AMK-tutkinnon metodifoorumi. Virtuaaliammattikorkeakoulu. Viitattu 20.5.2012. http://www.amk.fi/opintojaksot/0709019/1193463890749/1193464114103/1194104842149/1194105145587.html

Aro, J.P. 2012. Henkilökohtainen tiedonanto. 10.9.2012. Maanpuolustuskorkeakoulu, Helsinki.

Auditointi raportti. 12/2012. Clarified Networks. Helsinki.

Cheston, W, Dayan, R.,Springfield, R. 2005. Method and system for master boot record recovery.US Patent 6862681. Yhdysvallat.

Clyman, J. 2004. Manage Multiple Operating Systems.PC Magazine. Volume 23, Issue 22, 80-82.

Conrad, E. Advanced Encryption Standard. http://www.giac.org/cissp-papers/42.pdf. Viitattu 15.10.2012.

Ecrypt. 2011. II Yearly Report on Algorithms and Keysizes (2010-2011). Revision 1.0. Tulostettu 25.10.2012. http://www.ecrypt.eu.org/documents/D.SPA.17.pdf D.SPA.17.pdf.

Evwaraye, A. 2012. Kansallinen turvallisuusauditointikriteeristö KATAKRI kohti versiota III. CIP-Seminaari 28.10.2012. Sisäasiainministeriö. Viitattu 20.2.2013. www.cert.fi/attachments/cipseminaarit/cip_2012/6BsghQGIx/Evwaraye.pdf.

FIPS. Publication 197. Announcing the Advanced Encryption Standard (AES).2001. Tulostettu 12.2.2013. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

F-Secure. 2013. Boot Virus. Viitattu 25.2.2013. www.f-secure.com/v-descs/boovirus.shtml

F-Secure. 2013. Analysis of MBR File System Infector. Viitattu 25.3.2013 www.f-secure.com/weblog/archives/00002101.html

Gustafsson, J.2012.Käyttöjärjestelmäosion ja kiintolevyn salaus. Turun Ammattikorkeakoulu.Tietoliikenne.Ohjelmistotuotanto.

Havukainen ja Kansanen. 2004. Advanced Encryption Standard. Lappeenrannan teknillinen yliopisto. Viitattu 13.2.2013. http://www2.it.lut.fi/kurssit/03-04/010628000/Seminars/AES.pdf.

Hevner, A., March, S., Park, J. & Ram, S. 2004. Design Science in Information Systems Research.MIS Quarterly. Volume. 28 Issue.1.

Hurme, J. 2011.Laitteistoriippumaton työasemien vakiointi. Opinnäytetyö. Tietotekniikan koulutusohjelma. Tampereen ammattikorkeakoulu.

Jianwen, Z., Xiaochao, L. & Donghui G. 2008. A novel multiboot framework for embedded system. 344-347.

Järvinen, K.2008. Studies on High-Speed Hardware Implementation of cryptographic algorithms. Aticle dissertation.TKK, Department of Signal Processing and Acoustic. Espoo.

Järvinen, P. & Järvinen, A. 2004. Tutkimustyön metodeista. Opinpajan Kirja. Tampere.

Kansallinen turvallisuusauditointikriteeristö. 2011. Puolustusministeriö. Helsinki. Tulostettu 1.9.2012.

Karjalainen, T.2012. Henkilökohtainen tiedonanto 7.5.2012. Nixu Oy, Helsinki.

Kesäläinen, M. 2013. KATAKRI kehittyy. Miten se on muuttunut? Viitattu 21.2.2013. www.logisec.fi/files/KATAKRI.pdf

Liljequist, L. 2013. Haastattelu. Maanpuolustuskorkeakoulu.2.4.2013.Helsinki

Mason, R. O. 1988. Experimentation and knowledge – A pragdamic perspective, Knowledge:Creation, Diffusion, Utilization 10, No 1, 145-155.

Masrom, M. & Ismail, Z. 2008. Computer security and computer ethics awareness: A component of management information system Information Technology. Volume 3, 1-7.

Microsoft. 2012. Devcon-työkalun asentaminen ja käyttö. Tulostettu 10.4.2012. http://www.microsoft.com/en-us/download/details.aspx?id=11800.

Microsoft. 2012. How to obtain the current version of Device Console Utility (DenCon.exe). Tulostettu 12.4.2012. http://social.technet.microsoft.com/wiki/contents/articles/182.how-to-obtain-the-current-version-of-device-console-utility-devcon-exe.aspx

Nunamaker, J., Minder, C. & Purdin, T.1991. Systems Development in Information Systems Research..

Nunamaker, J.2010. Interview with Jay F. Nunamaker, Jr. on “Toward a Broader Vision of IS Research”. Business & Information Systems Engineering. Edition 5.

Oikawa, S., Ishikawa, H., Iwasaki, M. & Nakajima, T. 2005. Constructing secure operating environments by co-locating multiple embedded operating systems. Consumer Communications and Networking Conference, 43 – 48

Puska, M. 2012. Henkilökohtainen tiedonanto.15.11.2012. Maanpuolustuskorkeakoulu, Helsinki.

Roiha, V. 2012. Henkilökohtainen tiedonanto 26.5.2012.Viestikoulu, Riihimäki.

Saarenmaa,P.2010. Kiintolevyjen kryptografinen salaus SafeGuard Enterprise -ohjelmistoperheellä ja AES-256-standardilla. Tampereen ammattikorkeakoulu. Tietotekniikankoulutusohjelma. Viitattu 1.9.2012. http://theseus17kk.lib.helsinki.fi/bitstream/handle/10024/23929/Petri_Saarenmaa.pdf?sequence=1

Spanbauer, S. 2008. Run Multiple OSs Harmoniously on One PC (or Mac). PC World. Volume 26, Issue 4, 122-122.

Steers, K., Lasky, M. & O'Reilly, D. 2002. Multiboot Your PC to Avoid UnXPected Problems. PC World. Volume 20, 152.

Stone, M. 2003. BIOS Boot Trick. PC Magazine. Volume 22, 76.

Symantec. 2011.MBR Confusion. Viitattu 3.4.2013.
http://www.symantec.com/connect/blogs/mbr-confusion

Turvallisuusviranomaisten käsikirja yrityksille. 1.12.2011. Ulkoasianministeriö. Tulostettu 10.8.2012. formin.finland.fi/public/download.aspx?ID=89013&GUID.pdf.

Valtiovarainministeriö. 2010. Ohje tietoturvallisuudesta valtionhallinnossa. Tulostettu 14.10.2012.http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101028Ohjeti/02_Ohje_tietotuvallisuudesta_valtionhallinnossa.pdf

Valtiovarainministeriö. Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI ohjeisto. https://www.vahtiohje.fi Viitattu 21.2.2013

Zhang, W.,Chann, W., Tang, J., Xu, P., Li, Y. & Li,S.2009. The Development of a Portable Hard Disk Encryption/Decpryption System with a MEMS Coded Lock. ISSN 1424-8220. Sensors 2009.

Åström, P. 2012. Henkilökohtainen haastattelu.18.4.2013. Helsinki. Maanpuolustuskorkeakoulu.

Päätelaitteiden tietoturva kovennuksissa käytetyt lähteet:

Federal Office for Information Security. IT Security Guidelines. Luettu 18.7.2012
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf

Information Assurance Support Environment. The Security Technical Implementation Guide. Luettu 16.7.2012. http://iase.disa.mil/stigs/checklist/index.html

Microsoft.2012. Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP. Luettu 21.9.2012. http://technet.microsoft.com/library/dd162275

Microsoft. 2012. Microsoft Security Comliance Manager: Security Settings Simplified. TechNet Magazine 11/2011. Luettu 15.9.2012. http://technet.microsoft.com/en-us/magazine/hh489604.aspx

National Institute of Standards and Technology. 2012. Federal Desktop Core Configuration. Luettu 16.7.2012. http://nvd.nist.gov/fdcc/index.cfm

National Institute of Standards and Technology. 2012. National Checklist Program Repository. Luettu 15.7.2012. http://web.nvd.nist.gov/view/ncp/repository

National Institute of Standards and Technology. 2013. The United States Government Configuration Baseline. Luettu 15.7.2012. http://usgcb.nist.gov/

National Institute of Standards and Technology. 2012. Special Publications (800 Series). Luettu 16.7.2012. http://csrc.nist.gov/publications/PubsSPs.html

Thompson, K. The Best Guides for Information Security Management. Luettu 18.9.2012. http://www.crypt.gen.nz/papers/infosec_guides.html

California Institute of Technology. Rebuilding and hardening for Windows XP Professional. Luettu 13.9.2013. http://www.its.caltech.edu/win/xpharden.pdf

Kuviot

Taulukot

Liitteet

Liite 1 Devcon - työkalun asentaminen ja käyttö

1. Lataa DevCon-työkalu Microsoftin sivustolta. Windows 7-käyttöjärjestelmälle on toteutettu päivitetty versio Devcon-työkalusta. Windows Driver Kit 7.1.0-päivityspaketti pitää sisällään setuptools-työkalut, joista löytyy oikea Devcon versio. Työasemavakioinnissa on huomioitava, että 32- ja 64-bittisille käyttöjärjestelmäversiolle on oma asennustiedostonsa. Esimerkiksi Windows XP-käyttöjärjestelmään yhteensopiva Devcon-versio ei toimi kaikilta toiminnoillaan Windows 7-käyttöjärjestelmässä. Saat ladattua Devcon-työkalun seuraavasta linkistä: http://www.microsoft.com/en-us/download/details.aspx?id=11800
2. Pura ISO-tiedosto.
3. Saadaksesi Devconin käyttöön sinun tulee suorittaa seuraavat komennot:
    - "%SystemRoot%\System32\msiexec.exe" /a "C:\WDK\setuptools_x64fre.msi" targetdir="%temp%"
    - Yllä olevassa esimerkissä asennetaan Devcon-työkalun 64-bittinen versio työaseman temp-hakemistoon. Lisäksi esimerkissä on oletettu, että ISO-tiedosto on purettu polkuun C:\WDK\.

Seuraavassa on esimerkkejä Devcon-työkalun käytöstä:

`devcon hwids *` - komennolla saadaan selville kaikkien laitteiden ID:t ja kuvaukset. Tätä hyödynnettiin tutkimuksessa kovalevyjen ID:eiden tiedon saamiseksi.

Devconilla voi poistaa käytöstä myös esimerkiksi USB-portit ja verkkokortit ym. laitteet. Laitteen tai liitännän poistaminen käytöstä tapahtuu **disable**-komenolla. **Remove**-komennolla voi poistaa laitteen.

Tässä tutkimuksessa Devcon työkalu asennettiin system32-kansioon. Sitä suoritettiin käyttöjärjestelmän käynnistyssektoriin määritellyllä komennolla: C:\\Windows\system32\i386\devcon.exe disable ”tähän-esimerkiksi-IDE-levyn-määrittely”.

Seuraavalla sivulla on esitetty Microsoftin esimerkkejä Devcon-komennoista.

classfilter	Allows modification of class filters.
classes	List all device setup classes.
disable	Disable devices that match the specific hardware or instance ID.
driverfiles	List driver files installed for devices.
drivernodes	Lists all the driver nodes of devices.
enable	Enable devices that match the specific hardware or instance ID.
find	Find devices that match the specific hardware or instance ID.
findall	Find devices including those that are not present.
help	Display this information.
hwids	Lists hardware ID's of devices.
install	Manually install a device.
listclass	List all devices for a setup class.
reboot	Reboot local machine.
remove	Remove devices that match the specific hardware or instance ID.
rescan	Scan for new hardware.
resources	Lists hardware resources of devices.
restart	Restart devices that match the specific hardware or instance ID.
stack	Lists expected driver stack of devices.
status	List running status of devices.
update	Manually update a device.
UpdateNI	Manually update a device without user prompt
SetHwID	Adds, deletes, and changes the order of hardware IDs of root enumerated devices.

Esimerkkejä Devcon-komennoista (Microsoft 2013)

Liite 2 Tietojärjestelmäturvallisuuden osa-alueen asettamat vaatimukset päätelaitteelle

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomais-vaatimus: Korkea taso (II)	Elinkeino-elämän suositukset	Lähde/lisätietoa	HUOM!	Audi-tointi-tulos: OK/ poik-
I 501.0 Tunnistetaanko ja todennetaanko käyttäjät ennen pääsyn sallimista organisaation tietoverkkoon ja -järjestelmiin? *Lisäkysymys:* *Miten tämä on käytännössä järjestetty?*	Käyttäjät tunnistetaan ja todennetaan ennen pääsyn sallimista organisaation tietoverkkoon ja -järjestelmiin: 1) Käytössä yksilölliset henkilökohtaiset käyttäjätunnisteet. 2) Kaikki käyttäjät tunnistetaan ja todennetaan. 3) Pääsyä käyttöjärjestelmään valvotaan turvallisen sisäänkirjausmenettelyn avulla. 4) Tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestetty luotettavasti. 5) Todennus tehdään vähintään salasanaa käyttäen. Mikäli käytetään salasanatodennusta, a) käyttäjiä on ohjeistettu hyvästä turvallisuuskäytännöstä salasanan valinnassa ja käytössä, b) käyttöä valvova ohjelmisto asettaa salasanalle tietyt turvallisuuden vähimmäisvaatimukset ja pakottaa salasanan vaihdon sopivin määräajoin. 6) Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin aiheuttaa tunnuksen lukittumisen. 7) Järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia. Mikäli tämä ei kaikissa järjestelmissä/ sovelluksissa ole teknisesti mahdollista, vaaditaan sovitut ja dokumentoidut salasanojen hallintakäytännöt yhteiskäyttöisille tunnuksille.	Perustason vaatimusten 1-4, 6, 7 lisäksi: Käyttäjän tunnistamiseen käytetään vahvaa käyttäjäntunnistusta, mikäli samalla tietojärjestelmällä hallinnoidaan useampia kuin yhtä ko. suojaustason hanketta tai projektia.	Perustason vaatimusten 1-4, 6, 7 lisäksi: Käyttäjän tunnistamiseen käytetään aina vahvaa käyttäjäntunnistamista. Ks. kohdennetut vaatimukset: liitteen 1 huomautukset (I 502.0 / IV ja III).	Käyttäjät tunnistetaan ja todennetaan ennen pääsyn sallimista organisaation tietoverkkoon ja -järjestelmiin.	ISO/IEC 27002 11.3.1, ISO/IEC 27002 11.4, ISO/IEC 27002 11.5.1, ISO/IEC 27002 11.5.2, PCI DSS 8.1, PCI DSS 8.5, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf, VAHTI 8/2006, VAHTI 2/2010:n liite 5 (TTT), VAHTI 3/2010	Tunnistamisen ja todentamisen luotettavaan järjestämiseen kuuluu huolehtiminen ainakin siitä, että i) todennusmenetelmä on suojattu välimieshyökkäyksiltä (man-in-the-middle), ii) sisäänkirjautuessa, ennen todennusta, ei paljasteta mitään tarpeetonta tietoa, iii) todennuskredentiaalit ovat aina salatussa muodossa jos ne lähetetään verkon yli, iv) todennusmenetelmä on suojattu uudelleenlähetyshyökkäyksiä vastaan, v) todennusmenetelmä on suojattu brute force –hyökkäyksiä vastaan. Suojaustasojen III ja II vaatimukset vahvasta käyttäjätunnistuksesta voidaan joissain tapauksissa täyttää siten, että tietojärjestelmään on mahdollista päästä vain tiukasti rajatusta fyysisestä tilasta, jonka pääsynvalvonnassa käytetään vahvaa, kahteen tekijään perustuvaa tunnistamista. Tällöin käyttäjän tunnistaminen tietojärjestelmässä voidaan järjestää käyttäjätunnus-salasana -parilla.	

I 502.0 Onko organisaatiossa menettelytapa, jolla uudet järjestelmät (työasemat, kan- nettavat tietokoneet, palvelimet, verkkolaitteet, verkkotulostimet ja vastaavat) asennetaan järjestelmälli- sesti siten, että lopputuloksena on kovennettu asennus? Katso lisätietoja liitteestä 1 (I 502.0)	Käytössä on menettelytapa, jolla uudet järjestelmät (työasemat, kannettavat tietokoneet, palvelimet, verkkolaitteet, ja vastaavat) asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus. Katso kohdennetut vaatimukset: liite 1 huomautukset (I 502 / IV).	Käytössä on menettelytapa, jolla uudet järjestelmät (työasemat, kannettavat tietokoneet, palvelimet, verkkolaitteet, ja vastaavat) asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus. Ks. kohdennetut vaatimukset: liite 1 huomautukset (I 502.0 / IV ja III).	Korotetun tason vaati- musten lisäksi: On käytössä mekanismi, menetelmä tai menettelytapa, jolla tietojärjes- telmään tehtävät muutokset tallentuvat ja tehdyt muutokset voidaan jälkikäteen havaita (vrt. I 504.0). Ks. kohdennetut vaatimukset: liite 1 huomautukset (I 502.0 / II).	Käytössä on menettelytapa, jolla uudet järjestelmät (työasemat, kannettavat tietokoneet, palvelimet, verkkolaitteet, ja vastaavat) asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus.	PCI DSS 2.1, PCI DSS 2.2, ISO/IEC 11.2.3, VAHTI 8/2006, VAHTI 2/2010:n liite 5 (TTT), VAHTI 3/2010 Lähteitä järjestelmien/laitteiden kovennukseen ja turvalliseen konfiguraatioon: http://www.nsa.gov/ia/guidance/security_configuration_guides/, http://nvd.nist.gov/fdcc/index.cfm, http://web.nvd.nist.gov/view/ncp/repository, http://usgcb.nist.gov/, http://www.ia.nato.int/ > IA Guidance > Best Practices > Security Checklist, http://iase.disa.mil/stigs/stig/index.html, http://iase.disa.mil/stigs/checklist/index.html, http://technet.microsoft.com/en-us/library/cc163140.aspx, http://technet.microsoft.com/en-us/library/cc757698.aspx, http://httpd.apache.org/docs/1.3/misc/security_tips.html, http://csrc.nist.gov/publications/PubsSPs.html, http://www.cisco.com/en/US/tech/tk648/tk361/ technologies_tech_note-09186a0080120f48.shtml, http://www.hp.com/rnd/pdfs/Hardening_ProCurve_Switches_White_Paper.pdf, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf http://kb2.adobe.com/cps/837/cpsid_83709/attachments/ Acrobat_Enterprise_Administration.pdf, http://www.sans.org/critical-security-controls/control.php?id=3, http://www.sans.org/critical-security-controls/control.php?id=4	Järjestelmäkovennuksissa edellytetään suojaustasolla III FDCC:tä tai vastaavaa tasoa. Osalle kansainvälisistä aineistoista edellytetään FDCC:tä vastaavaa tasoa jo suojaustasolla IV. Katso kohdennetut vaatimukset liitteen 1 huomautuksista (I 502.0) Suojaustason II vaatimus voidaan toteuttaa esimerkiksi tiedostojärjestelmän eheyttä tarkkailevalla ohjelmistolla. Lisätietoa löytyy esimerkiksi osoitteesta http://nsrc.org/security/#integrity. Vrt. sähköpostisuojaukset vaatimuksesta I 605.0.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomais-vaatimus: Korkea taso (II)	Elinkeino-elämän suositukset	Lähde/lisätietoa	HUOM!	Audi-tointi-tulos: OK/ poik-keama
I 503.0 Miten on pienennetty haittaohjelmien aiheuttamia riskejä? *Tarkentavia ohjeita liitteessä 1 (I 503).*	1) Haittaohjelmantorjunta- ohjelmistot on asennettu kaikkiin sellaisiin järjestelmiin, jotka ovat yleisesti alttiita haittaohjelmatartunnoille (erityisesti työasemat, kannettavat tietokoneet ja palvelimet). 2) Torjuntaohjelmistot ovat toimintakykyisiä ja käynnissä. 3) Torjuntaohjelmistot tuottavat havainnoistaan lokitietoja. 4) Haittaohjelmatunnisteet päivittyvät säännöllisesti. 5) Käyttäjiä on ohjeistettu haittaohjelmauhista ja organisaation tietoturvaperiaatteiden mukaisesta toiminnasta (vrt. A 806.0). 6) Haittaohjelmahavaintoja seurataan (vrt. A 408.0).	Perustason vaatimusten lisäksi: Tapauskohtaisesti arvioidaan tarve järjestelmien USB-porttien ja vastaavien liityntöjen käytölle. Mikäli liityntöjen käytölle ei ole todellista perustetta, ne poistetaan käytöstä. Mikäli liityntöjen käytölle on todelliset perusteet, arvioidaan tapauskohtaisesti edellytykset ja ehdot, minkä mukaisia laitteistoja ja välineitä (esim. USB-muisteja) järjestelmään voidaan kytkeä.	Perustason vaatimusten lisäksi: Tapauskohtaisesti arvioidaan tarve järjestelmien USB-porttien ja vastaavien liityntöjen käytölle. Mikäli liityntöjen käytölle ei ole todellista perustetta, ne poistetaan käytöstä. Mikäli liityntöjen käytölle on todelliset perusteet, arvioidaan tapauskohtaisesti edellytykset ja ehdot, minkä mukaisia laitteistoja ja välineitä (esim. USB-muisteja) järjestelmään voidaan kytkeä.	Haittaohjelmien havaitsemis- ja estotoimet sekä niistä toipumismekanismit ja asiaankuuluvat käyttäjien valppautta lisäävät ohjeet on otettu käyttöön.	ISO/IEC 27002 10.4.1, PCI DSS 5.1, PCI DSS 5.2, http://www.sans.org/critical-security-controls/control.php?id=12, VAHTI 2/2010:n liite 5 (TTT), VAHTI 3/2010, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/ guidelines/guidelines_pdf.pdf		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomais-vaatimus: Korkea taso (II)	Elinkeino-elämän suositukset	Lähde/lisätietoa	HUOM!	Audi-tointi-tulos: OK/ poik-keama
I 504.0 Pääkysymys: Ovatko organi-saation teknis-ten laitteiden ja palveluiden lokimenettelyt kunnossa? *Lisäkysymys:* *Kerätäänkö ver-koista, laitteista ja järjestelmistä kes-keiset lokitiedot ja käsitelläänkö niitä asianmukaisesti?* Katso lisämää-reet liitteestä 1 (I 504).	1) Tallenteiden kattavuus on riittävä tietomurtojen tai niiden yritysten jälkikäteiseen todenta-miseen. 2) Keskeisiä tallenteita säilytetään 6 kk tai erillisessä sopimuksessa määrätty aika. 3) Suojattavaa tie-toa sisältävät lokitiedot on suojattu asianmukaisesti (pääsynvalvonta, käsittely, poisto).	Perustason vaatimusten 1 ja 3 lisäksi: 1) Keskeisiä tallenteita säilytetään 24 kk tai erillisessä sopimuksessa määrätty aika. 2) On käytössä menettely hyök-käyksen/väärinkäyttöyrityksen ha-vaitsemiseen, käsittelyyn ja torjun-taan. Menettelyn on sisäl- lettävä vähintään kerran viikossa tapahtu-va lokitietojen tarkkailu normaali-tilaan nähden poikkeavi- en tapah-tumien havaitsemiseksi. Erityisesti tietojärjestelmän luvaton käyttöyri-tys on kyettävä havaitse- maan (vrt. I 408.0 ja A 410.0). 3) Samassa organisaatiossa tai tur-vallisuusalueella olevien olen-naisten tietojenkäsittelyjärjestelmi-en kellot on synkronoitu sovitun tarkan ajanlähteen kanssa. 4) Lokitiedot ja niiden kirjauspal-velut ovat suojattuja väärentämi-seltä ja luvattomalta pääsyltä. On käytössä jokin menetelmä lokien eheyden (muuttumattomuuden) varmistamiseen. 5) Keskeiset lokitiedot varmuusko-pioidaan säännöllisesti. 6) Syntyneiden lokitietojen käy-töstä ja käsittelystä muodostuu merkintä. 7) Kriittisistä ylläpitotoimista tal-lennetaan kirjausketju (audit trail).	Korotetun tason vaatimusten li-säksi: 1) Tietojärjes-telmän eheydes-tä varmistutaan vähintään kerran viikossa (vrt. I 502.0). 2) Suojaustason II tietojen käsit-telystä tallenne-taan käsittely-tiedon sisältävät lokimerkinnät (vrt. I 607.0).	1) Tallenteiden kattavuus on riittävä tietomurtojen tai niiden yri-tysten jälkikä-teiseen toden-tami- seen. 2) Keskeisiä tallenteita säilytetään riskienar-vioinnissa määritetty aika.	ISO/IEC 27002 10.6.1, ISO/IEC 27002 10.10.1, ISO/IEC 27002 10.10.2, ISO/IEC 27002 10.10.3, ISO/IEC 27002 10.10.6, PCI DSS 10.1, PCI DSS 10.2, PCI DSS 10.3, PCI DSS 10.4, PCI DSS 10.5, VAHTI 8/2006, VAHTI 3/2009, VAHTI 2/2010:n liite 5 (TTT), VAHTI 3/2010 http://www.sans.org/critical-security-controls/control.php?id=6, http://technet.microsoft.com/en-us/library/bb742610.aspx, http://technet.microsoft.com/en-us/ library/dd408940%28WS.10%29.aspx, http://www.team-cymru.org/ReadingRoom/Templates/secure-ntp-template.html		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomais-vaatimus: Korkea taso (II)	Elinkeino-elämän suositukset	Lähde/lisätietoa	HUOM!	Audi-tointi-tulos: OK/ poik-keama
I 505.0 Miten suojattavat tiedot säilytetään tietojärjestelmissä? **Katso lisätietoja liitteestä 1 (I505)**	1) Tietojärjestelmissä suojattavat tiedot on eritelty käyttöoikeus-määrittelyillä ja järjestelmän käsittelysäännöillä tai jollain vastaavalla menettelyllä. 2) Tietojärjestelmien käytön yhteydessä syntyvät suojattavaa tietoa sisältävät väliaikaistiedostot hävitetään säännöllisesti (ks. I 603.0). 3) Suojaustason IV tietoa sisältävät kannettavien tietokoneiden kiintolevyt ovat riittävällä tasolla suojattuja (vrt. I 506).	Perustason vaatimusten 1 ja 2 lisäksi: 1) Palvelimissa, työasemissa, kannettavissa tietokoneissa, ja muissa tallennusvälineissä suojaustason III tiedot säilytetään aina luotettavasti salakirjoitettuna (ks. I 509.0). 2) Mikäli samalla palvelimella/ palvelimilla säilytetään useamman kuin yhden ko. turvatason hankkeen/projektin/ toiminnon tietoja, palvelimella olevat tiedot säilytetään luotettavasti salakirjoitettuna käyttöoikeusrajoitteisissa hakemistoissa tai alueilla. 3) Suojaustason III tieto pidetään erillään julkisesta ja muiden suojaustasojen tiedoista.	1) Palvelimissa, työasemissa, kannettavissa tietokoneissa, ja muissa tallennusvälineissä suojaustason II tiedot säily- tetään aina luotettavasti salakirjoitettuna (ks. I 509.0). 2) Suojaustason II tieto pidetään erillään julkisesta ja muiden suojaustasojen tiedoista.	Tietojärjestelmissä suojattavat tiedot on eritelty käyttöoikeus-määrittelyillä ja järjestelmän käsittelysäännöillä tai jollain vastaavalla menettelyllä.	VAHTI 8/2006, VAHTI 2/2010, VAHTI 3/2010 http://www.nsa.gov/ia/guidance/ security_configuration_guides/ database_servers.shtml, http://www. oracle.com/technetwork/articles/ idm/tde-089026.html, http://www. oracle.com/technetwork/database/ security/twp-transparent-data- encryption-bes-130696.pdf, http:// www.ibm.com/developerworks/data/ library/techarticle/dm-0907encryptionexpert/, http://publib.boulder. ibm.com/epubs/pdf/eetuga13.pdf, http://technet.microsoft.com/en-us/ library/cc278098%28SQL.100%29. aspx, http://technet.microsoft.com/ en-us/library/cc875821.aspx, http:// support.microsoft.com/kb/223316, http://publib.boulder.ibm.com/infocenter/lnxinfo/v3r0m0/topic/liaai/ secure/ liaaisecuresles.htm, http:// www.linuxtopia.org/online_books/ suse_linux_guides/SLES10/ suse_enterprise_linux_server_installation_admin/cha_cryptofs.html, http:// www.postgresql.org/docs/manuals/, http://www.sans.org/critical-security-controls/control.php?id=15		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poik-
I 506.0 Kuinka varmistutaan siitä, että suojattavaa tietoa sisältävät liikuteltavat kiintolevyt, muistit, mediat, älypuhelimet, mobiilipäätteet ja vastaavat ovat aina suojattuja luvatonta pääsyä vastaan?	1) Suojattavaa tietoa sisältävät kannettavien tietokoneiden kiin- tolevyt, USB-muistit, tallennusmediat ja vastaavat ovat luotettavasti suojattuja. 2) Turvaluokiteltua tietoa sisältävät älypuhelimet: a) Pääsy puhelimen ja muistikortin tietoihin suojataan salasanalla. b) Käytössä puhelimen/ SIM-kortin/muistikortin automaattinen lukittuminen. c) Etätyhjennysmahdollisuus käytössä. d) Puhelimen ja muistikortin muisti suojataan. e) Verkko- ja haittaohjelmauhat huomioidaan riskienarvioinnin mukaisesti. f) Bluetooth- ja WLAN-yhteydet ovat oletusarvoisesti kytketyt pois päältä ja ne aktivoidaan vain käytön ajaksi. Bluetooth- asetuksissa puhelimen näkyvyys on oletuksena asetettu piilotetuksi.	Perustason vaatimuksen 1 lisäksi: Suojaustason III aineistoa ei lähtökohtaisesti käsitellä älypuhelimilla. Toimivaltainen viranomainen voi kuitenkin tapauskohtaisesti erillishyväksyä tietyt toteutukset, joissa älypuhelin ja kaikki sen kautta kulkeva liikenne suojataan luotettavasti.	Perustason vaatimuksen 1 lisäksi: Suojaustason II aineistoa ei lähtökohtaisesti käsitellä älypuhelimilla. Toimivaltainen viranomainen voi kuitenkin tapauskohtaisesti erillishyväksyä tietyt toteutukset, joissa älypuhelin ja kaikki sen kautta kulkeva liikenne suojataan luotettavasti.	Suojattavaa tietoa sisältävät kannettavien tietokoneiden kiintolevyt, USB-muistit, tallennusmediat ja vastaavat ovat luotettavasti suojattuja. Suojattavaa tietoa sisältävät älypu- helimet suojataan riskienarvioinnin mukaisesti (lukitus, salakirjoitus, etähallinta, jne.).	ISO/IEC 27002 10.8.3, ISO/IEC 27002 9.2.5, VAHTI 8/2006, VAHTI 2/2010, VAHTI 3/2010, EU:n turvallisuussäännöstö 6952/2/11 REV2 /1.4.2011 9. artikla, http://www.sans.org/score/handheld-schecklist.php	Useimmat nykyiset käyttöjärjestelmät tarjoavat jo asennuksen yhteydessä mahdollisuuden kiintolevyn salaa- miseen. Vaihtoehtoisesti voidaan käyttää erillistä ohjelmistoratkaisua. USB-muistien ja muiden tallennusme- dioitten salaamiseen on olemassa sekä ohjelmisto- että laitetason ratkaisuja. Vrt. I 509.0.	

Kysymys	Viranomaisvaatimus Perustaso (IV)	Viranomaisvaatimus Korotettu taso (III)	Viranomaisvaatimus Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 507.0 Kuinka varmistutaan siitä, etteivät suojattavat tiedot joudu kolmansille osapuolille huoltotoimenpiteiden tai käytöstä poiston yhteydessä?	1) Kaikki suojattavaa tietoa sisältävät laitteistojen osat (kiintolevyt, muistit, muistikortit, jne.) tyhjennetään luotettavasti käytöstä poiston tai huoltoon lähetyksen yhteydessä (vrt. I 603.0). Mikäli luotettava tyhjennys ei ole mahdollista, suojattavaa tietoa sisältävä osa on tuhottava mekaanisesti. 2) Kolmannen osapuolen suorittamia huoltotoimenpiteitä valvotaan (esim. monitoimilaite), jos laitteen muistia tai vastaavaa ei voida luotettavasti tyhjentää ennen huoltotoimenpiteitä.	1) Kaikki suojattavaa tietoa sisältävät laitteistojen osat (kiintolevyt, muistit, muistikortit, jne.) tyhjennetään luotettavasti käytöstä poiston tai huoltoon lähetyksen yhteydessä (vrt. I 603.0). Mikäli luotettava tyhjennys ei ole mahdollista, suojattavaa tietoa sisältävä osa on tuhottava mekaanisesti. 2) Kolmannen osapuolen suorittamia huoltotoimenpiteitä valvotaan (esim. monitoimilaite), jos laitteen muistia tai vastaavaa ei voida luotettavasti tyhjentää ennen huoltotoimenpiteitä.	1) Kaikki suojattavaa tietoa sisältävät laitteistojen osat (kiintolevyt, muistit, muistikortit, jne.) tyhjennetään luotettavasti käytöstä poiston tai huoltoon lähetyksen yhteydessä (vrt. I 603.0). Mikäli luotettava tyhjennys ei ole mahdollista, suojattavaa tietoa sisältävä osa on tuhottava mekaanisesti. 2) Kolmannen osapuolen suorittamia huoltotoimenpiteitä valvotaan (esim. monitoimilaite), jos laitteen muistia tai vastaavaa ei voida luotettavasti tyhjentää ennen huoltotoimenpiteitä.	1) Kaikki suojattavaa tietoa sisältävät laitteistojen osat (kiintolevyt, muistit, muistikortit, jne.) tyhjennetään luotettavasti käytöstä poiston tai huoltoon lähetyksen yhteydessä (vrt. I 603.0). Mikäli luotettava tyhjennys ei ole mahdollista, suojattavaa tietoa sisältävä osa on tuhottava mekaanisesti. 2) Kolmannen osapuolen suorittamia huoltotoimenpiteitä valvotaan (esim. monitoimilaite), jos laitteen muistia tai vastaavaa ei voida luotettavasti tyhjentää ennen huoltotoimenpiteitä.	ISO/IEC 27002 9.2, ISO/IEC 27002 9.2.6, VAHTI 8/2006, VAHTI 2/2010	Luotettavalla tyhjennyksellä tarkoitetaan tässä yhteydessä tiedon ylikirjoittamista. Vaatimus kattaa kaikki laitteistot, joihin on joskus tallennettu suojattavaa tietoa, esim. kannettavat, työasemat, palvelimet, puhelimet, tulostimet, verkkolaitteet, jne. Vrt. I 603.0. Mikäli luotettava tyhjennys ei ole mahdollista, laitteisto tai sen osa on tuhottava mekaanisesti.	

	Perustaso (IV)	Korotettu taso (III)	Korkea taso (II)	suositukset			titulos: OK/ poik-keama
I 509.0 Miten on var-mistuttu siitä, että käytetyt salausratkaisut ovat riittävän turvallisia?	Salausratkaisujen (ja -tuotteiden) tietoturval-lisuus on tarkastettu ja hyväksytty ko. suojaus-tasolle a) kansainvälisen tieto-turvaviranomaisen toimesta, b) kansallisen tieto-turvaviranomaisen toimesta, tai c) erillisessä ratkaisulle suoritetussa tarkastuk-sessa.	Salausratkaisujen (ja -tuotteiden) tietoturval-lisuus on tarkastettu ja hyväksytty ko. suojaus-tasolle a) kansainvälisen tietotur-vaviranomaisen toimesta, b) kansallisen tietoturva-viranomaisen toimesta, tai c) erillisessä ratkaisulle suoritetussa tarkastuk-sessa.	Salausratkaisujen (ja -tuot-teiden) tietoturvallisuus on tarkastettu ja hyväksyt-ty ko. suojaustasolle a) kansainvälisen tietotur-vaviranomaisen toimesta, b) kansallisen tietoturvavi-ranomaisen toimesta, tai c) erillisessä ratkaisulle suoritetussa tarkastuk-sessa.	Käytetään tunnet-tuja ja yleisesti luo-tettavina pidettyjä salausratkaisuja, tai ratkaisun luo-tettavuudesta on varmistuttu jollain muulla luotettaval-la menetelmällä.	EU:n turvallisuus-säännöstö 6952/2/11 REV2 /1.4.2011 10. artikla, http://www. consilium.europa. eu/information- assu-rance, http:// www.ia.nato.int/ niapc, Kansallisen salaustuotteiden hy-väksyntäviran- omai-sen hyväksytty- jen salausratkaisujen lis-ta, Kansallisen turval-lisuusviran- omaisen “Kansainvä- lisen turvallisuusluo- kitel-lun tietoaineiston kä-sittelyohje”	Erityisesti kansainvälisen turvaluoki-tellun tiedon salaamisessa edellytetään käytettävän käytännössä vain tiedon omistajan (esim. EU) hyväksymiä sa-lausratkaisuja. Kansallisella salaus-tuotteiden hyväksyntäviranomaisella (CAA, Crypto Approval Authority, Suomessa NCSA-FI) on tietyin rajauk-sin mahdollisuus hyväksyä myös mui-ta tuotteita/ratkaisuja kansainvälisen turvaluokitellun tiedon suojaamiseen. Usean kansainvälisen turvallisuus-viranomaisen salaustuotehyväksynnät edellyttävät tuotteelta erinäisiä sertifi-kaatteja (erityisesti Common Criteria, toisinaan myös esim. FIPS 140), ja li-säksi tiettyjen erityisvaatimusten (esim. lähdekoodin luovutus ja tarkas-tus, hajasäteilysuojaukset) täyttämistä.	

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poik-
I 510.0 Salausavainten hallinta. Pääkysymys: Ovatko salaiset avaimet vain valtuutettujen käyttäjien ja prosessien käytössä? Lisäkysymys: Ovatko salausavainten hallinnan prosessit ja käytännöt dokumentoituja? Miten käytän- nön toteutus on järjestetty? Katso lisätiedot liitteestä 1 (I 510.0).	1) Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä. 2) Salausavaintenhallinnan prosessit ja käytännöt ovat dokumentoituja ja asianmukaisesti toteutettuja. Prosessit edellyttävät a) kryptografisesti vahvoja avaimia, b) turvallista avaintenjakelua, c) turvallista avainten säilytystä, d) säännöllisiä avaintenvaihtoja, e) vanhojen tai paljastuneiden avainten vaihdon, f) valtuuttamattomien avaintenvaihtojen estämisen.	1) Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä. 2) Salausavaintenhallinnan prosessit ja käytännöt ovat dokumentoituja ja asianmukaisesti toteutettuja. Prosessit edellyttävät a) kryptografisesti vahvoja avaimia, b) turvallista avaintenjakelua, c) turvallista avainten säilytystä, d) säännöllisiä avaintenvaihtoja, e) vanhojen tai paljastuneiden avainten vaihdon, f) valtuuttamattomien avaintenvaihtojen estämisen.	1) Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä. 2) Salausavaintenhallinnan prosessit ja käytännöt ovat dokumentoituja ja asianmukaisesti toteutettuja. Prosessit edellyttävät a) kryptografisesti vahvoja avaimia, b) turvallista avaintenjakelua, c) turvallista avainten säilytystä, d) säännöllisiä avaintenvaihtoja, e) vanhojen tai paljastuneiden avainten vaihdon, f) valtuuttamattomien avaintenvaihtojen estämisen.	Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä.	ISO/IEC 27002 12.3.2, PCI DSS 3.6, VAHTI 8/2006, VAHTI 2/2010		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 511.0 Käytetäänkö istunnonhallinnassa tunnettua ja luotettavana pidettyä tekniikkaa?	Istunnonhallinnassa käytetään tunnettua ja luotettavana pidettyä tekniikkaa tai istunnon kaappaus ja kloonaus on muuten tehty huomattavan vaikeaksi. Mikäli ei käytetä tunnettua tekniikkaa, huolehdittava kuntoon ainakin 1) suljettujen istuntojen uudelleenaktivoinnin esto, 2) istuntoavainten eriytys niiden lähettämisessä käytetyistä avaimista, 3) istunnon sulkeminen mikäli ei käyttäjäaktiviteetteja tiettyyn aikaan, 4) istuntojen pituuksien rajoitukset.	Istunnonhallinnassa käytetään tunnettua ja luotettavana pidettyä tekniikkaa tai istunnon kaappaus ja kloonaus on muuten tehty huomattavan vaikeaksi. Mikäli ei käytetä tunnettua tekniikkaa, huolehdittava kuntoon ainakin 1) suljettujen istuntojen uudelleenaktivoinnin esto, 2) istuntoavainten eriytys niiden lähettämisessä käytetyistä avaimista, 3) istunnon sulkeminen mikäli ei käyttäjäaktiviteetteja tiettyyn aikaan, 4) istuntojen pituuksien rajoitukset.	Istunnonhallinnassa käytetään tunnettua ja luotettavana pidettyä tekniikkaa tai istunnon kaappaus ja kloonaus on muuten tehty huomattavan vaikeaksi. Mikäli ei käytetä tunnettua tekniikkaa, huolehdittava kuntoon ainakin 1) suljettujen istuntojen uudelleenaktivoinnin esto, 2) istuntoavainten eriytys niiden lähettämisessä käytetyistä avaimista, 3) istunnon sulkeminen mikäli ei käyttäjäaktiviteetteja tiettyyn aikaan, 4) istuntojen pituuksien rajoitukset.	Istunnonhallinnassa käytetään tunnettua ja luotettavana pidettyä tekniikkaa tai istunnon kaappaus ja kloonaus on muuten tehty huomattavan vaikeaksi. Mikäli ei käytetä tunnettua tekniikkaa, huolehdittava kuntoon ainakin 1) suljettujen istuntojen uudelleenaktivoinnin esto, 2) istuntoavainten eriytys niiden lähettämisessä käytetyistä avaimista, 3) istunnon sulkeminen mikäli ei käyttäjäaktiviteetteja tiettyyn aikaan, 4) istuntojen pituuksien rajoitukset.	ISO/IEC 27002 11.5, VAHTI 3/2001		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditoin-titulos: OK/ poik-
I 511.0 Käytetäänkö istunnonhallinnassa tunnettua ja luotettavana pidettyä tekniikkaa?	Istunnonhallinnassa käytetään tunnettua ja luotettavana pidettyä tekniikkaa tai istunnon kaappaus ja kloonaus on muuten tehty huomattavan vaikeaksi. Mikäli ei käytetä tunnettua tekniikkaa, huolehdittava kuntoon ainakin 1) suljettujen istuntojen uudelleenaktivoinnin esto, 2) istuntoavainten eriytys niiden lähettämisessä käytetyistä avaimista, 3) istunnon sulkeminen mikäli ei käyttäjäaktiviteetteja tiettyyn aikaan, 4) istuntojen pituuksien rajoitukset.	Istunnonhallinnassa käytetään tunnettua ja luotettavana pidettyä tekniikkaa tai istunnon kaappaus ja kloonaus on muuten tehty huomattavan vaikeaksi. Mikäli ei käytetä tunnettua tekniikkaa, huolehdittava kuntoon ainakin 1) suljettujen istuntojen uudelleenaktivoinnin esto, 2) istuntoavainten eriytys niiden lähettämisessä käytetyistä avaimista, 3) istunnon sulkeminen mikäli ei käyttäjäaktiviteetteja tiettyyn aikaan, 4) istuntojen pituuksien rajoitukset.	Istunnonhallinnassa käytetään tunnettua ja luotettavana pidettyä tekniikkaa tai istunnon kaappaus ja kloonaus on muuten tehty huomattavan vaikeaksi. Mikäli ei käytetä tunnettua tekniikkaa, huolehdittava kuntoon ainakin 1) suljettujen istuntojen uudelleenaktivoinnin esto, 2) istuntoavainten eriytys niiden lähettämisessä käytetyistä avaimista, 3) istunnon sulkeminen mikäli ei käyttäjäaktiviteetteja tiettyyn aikaan, 4) istuntojen pituuksien rajoitukset.	Istunnonhallinnassa käytetään tunnettua ja luotettavana pidettyä tekniikkaa tai istunnon kaappaus ja kloonaus on muuten tehty huo- mattavan vaikeak- si. Mikäli ei käytetä tunnettua tekniikkaa, huolehdittava kuntoon ainakin 1) suljettujen istuntojen uudelleenaktivoinnin esto, 2) istuntoavainten eriytys niiden lähettämisessä käytetyistä avaimista, 3) istunnon sulkeminen mikäli ei käyttäjäaktiviteetteja tiettyyn aikaan, 4) istuntojen pituuksien rajoitukset.	ISO/IEC 27002 11.5, VAHTI 3/2001		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poik-
I 512.0 Onko huolehdittu, että autentikaatiodataa ei säilytetä tietojärjestelmissä selväkielisinä?	Autentikaatiodataa (kuten salasanoja, sormenjälkiä, jne.) ei säilytetä tietojärjestelmissä selväkielisinä. Tietojärjestelmissä voidaan säilyttää vain yksisuuntaisella tiivistefunktiolla, tai vastaavalla luotettavana pidetyllä menetelmällä autentikaatiodatasta saatuja tiivisteitä.	Autentikaatiodataa (kuten salasanoja, sormenjälkiä, jne.) ei säilytetä tietojärjestelmissä selväkielisinä. Tietojärjestelmissä voidaan säilyttää vain yksisuuntaisella tiivistefunktiolla, tai vastaavalla luotettavana pidetyllä menetelmällä autentikaatiodatasta saatuja tiivisteitä.	Autentikaatiodataa (kuten salasanoja, sormenjälkiä, jne.) ei säilytetä tietojärjestelmissä selväkielisinä. Tietojärjestelmissä voidaan säilyttää vain yksisuuntaisella tiivistefunktiolla, tai vastaavalla luotettavana pidetyllä menetelmällä autentikaatiodatasta saatuja tiivisteitä.	Autentikaatiodataa (kuten salasanoja, sormenjälkiä, jne.) ei säilytetä tietojärjestelmissä selväkielisinä. Tietojärjestelmissä voidaan säilyttää vain yksisuuntaisella tiivistefunktiolla, tai vastaavalla luotettavana pidetyllä menetelmällä autentikaatiodatasta saatuja tiivisteitä.	PCI DSS 3.2, PCI DSS 8.4, ISO/IEC 27002 11.5.3		

Kysymys	Viranomaisvaatimus: Perustaso (IV)	Viranomaisvaatimus: Korotettu taso (III)	Viranomaisvaatimus: Korkea taso (II)	Elinkeinoelämän suositukset	Lähde/lisätietoa	HUOM!	Auditointitulos: OK/ poikkeama
I 513.0 Miten on varmistettu ajettavan koodin turvallisuudesta? * Katso lisätiedot liitteestä 1 (I 513.0).	Ohjelmistoja hankitaan ja asennetaan vain luotettavista ja luvallisista lähteistä.	Perustason vaatimuksen lisäksi: 1) Asennettavien ohjelmistojen ja päivitysten eheys tarkistetaan (tarkistussummat, haittaohjelmatarkistus). 2) Hankittavilta/toteutettavilta sovelluksilta vaaditaan turvallisen ohjelmoinnin periaat- teiden, esim. Open Web Application Security Pro- ject Guide, toteuttamista. Toimittajilta vaaditaan selvitys, miten tietoturval- lisuus on otettu huomioon tuotekehityksessa.	Perustason vaatimuksen lisäksi: Vaihtoehdot: 1) Käytetään vain viranomaisen ko. toimintaympäristöön hyväksymiä järjestelmiä/ohjelmistoja. 2) Hankittavilta/toteutettavilta sovelluksilta vaaditaan turvallisen ohjelmoinnin periaat- teiden, esim. Open Web Application Security Pro- ject Guide, toteuttamista. Toimittajilta vaaditaan selvitys, miten tietoturval- lisuus on otettu huomioon tuotekehityksessä. Lisäksi kaikki ko. järjestelmän turvallisuuteen oleellisesti vaikuttava koodi on avoimesti tarkastettavissa (esim. takaportit, turvattomat toteutukset, jne.) tai sopimuksessa on varattu oikeus lähdekoodin tarkastukseen. Vaihtoehdossa 2 on näytettävä todiste koodin luotettavaksi toteamisesta (esim. kuvaukset toimittajan prosesseista ja ulkopuolisen tekemä katselmointiraportti).	Ohjelmistoja hankitaan ja asennetaan vain luotettavista ja luvallisista lähteistä.	ISO/IEC 27002 12.2.1, ISO/IEC 27002 12.4.1, ISO/IEC 27002 15.1.2, PCI DSS 6.5, VAHTI 8/2006, http://www.bsi-mm.com/, http://www.opensamm.org/, http://www.owasp.org/index.php/Category:OWASP_Guide_Project, http://www.owasp.org/index.php/ Category:OWASP_Top_Ten_Project, http://www.cpni.gov.uk/Docs/Vendor_security_questions.pdf, http://www.sans.org/critical-security-controls/control.php?id=7	Ohjelmistotoimittajalta voidaan vaatia esim. seuraavia: 1) Ohjelmistokehittäjien riittävä tietoturvatietous on varmistettu. 2) Ohjelmistokehityksen aikana on suoritettu tietoturvauhka-analyysi ja havaitut riskit on joko kontrolloitu tai nimenomaisesti hyväksytty. 3) Rajapinnat (ainakin ulkoiset) on testattu viallisilla syötteillä sekä suurilla syötemäärillä. 4) Riippuen ohjelmointiympäristöstä, helposti ongelmia aiheuttavien funktioiden ja rajapintojen käyttöön on määritelty politiikka ja sitä valvotaan (esim. Microsoftilla on listat kielletyistä funktioista). 5) Arkkitehtuuri ja lähdekoodi on katselmoitu. 6) Ohjelmakoodi on tarkastettu automatisoidulla staattisella analyysillä. 7) Ohjelmakoodin versionhallinnan ja kehitystyökalujen eheys on varmistettu. Hankittavista ohjelmistoista on saatava myös dokumentaatio, josta selviää lisäksi ainakin sovelluksen käyttämät verkkoportit. Suotavaa on myös edellyttää, että a) sovellukset käyttävät pientä määrää määriteltyjä portteja, b) dynaamisia portteja käyt- tävät sovellukset käyttävät vain pientä porttiavaruutta, ja c) ohjelmistot eivät vaadi laajoja käyttöoikeuksia toimiak- seen (ts. ohjelmistojen on toimittava “peruskäyttäjän” oikeuksilla).	

Liite 3 Esimerkki saavutettavista kustannussäästöistä

Alla olevassa taulukossa on laskettu teoreettiset päätelaitekustannukset Maanpuolustuskorkeakoululla tapauksessa, jossa hankitaan jokaiseen palveluympäristöön oma päätelaite loppukäyttäjälle. Kustannuslaskelmassa on laskettu vuosittaiset kustannukset 3-vuoden leasing-sopimuksella olevilla päätelaitteilla.

Päätelaitteet	Lukumäärä	Kustannus vuodessa
Hallinnollinen ympäristö	1050	330
Yliopistoverkko	1050	330
Maavoimien taktinen harjoitusverkko	250	330
Merivoimien tietojärjestelmän harjoitusverkko	60	330
Erillinen tutkimustyöasema	30	330

Kustannukset yhteensä vuodessa **805200**

Alla olevassa taulukossa on laskettu optimistinen tulevaisuuden tila päätelaitekustannuksille, jossa eri ympäristöjä käytetään yhdellä päätelaitteella. Arvioinnissa on huomioitu, että kymmenellä prosentilla henkilökunnasta on tarve työskennellä eri ympäristöissä samanaikaisesti työtehtävien luonteesta johtuen.

Päätelaitteet	Lukumäärä	Kustannus vuodessa (€)
Hallinnollinen ympäristö	1050	330
Yliopistoverkko	35	330
Maavoimien taktinen harjoitusverkko	35	330
Merivoimien tietojärjestelmän harjoitusverkko	35	330
Erillinen tutkimustyöasema	35	330

Kustannukset yhteensä vuodessa **392700**

Seuraavassa taulukossa on esitetty realistinen arvio päätelaitekustannuksista tapauksessa, jossa yhden koneen politiikka on ollut tuotantokäytössä organisaatiossa vuoden ajan. Tällöin 3-vuoden leasing-sopimuksella olevista päätelaitteista on palautunut leasing-yhtiölle yksi kone-erä. Kustannusarviossa on otettu huomioon henkilöstön kymmenen prosentin osuus, joille jää usea päätelaite työtehtävien luonteesta johtuen.

Päätelaitteet	**Lukumäärä**	**Kustannus vuodessa (€)**
Hallinnollinen ympäristö	1050	330
Yliopistoverkko	700	330
Maavoimien taktinen harjoitusverkko	35	330
Merivoimien tietojärjestelmän harjoitusverkko	35	330
Erillinen tutkimustyöasema	35	330

Kustannukset yhteensä vuodessa	**612150**

Päätelaitekustannuksien lisäksi säästöjä saavutetaan lisenssikustannuksissa. Useat eri ohjelmistot ovat sellaisia, että niihin ei tarvitse hankkia jokaiselle koneelle omaa lisenssiä, mikäli yhtä palveluympäristöä käytetään samalla päätelaitteella kerrallaan. Säästöjä saavutetaan esimerkiksi F-Securen, Microsoftin sekä kiintolevynsalausohjelmiston lisenssikustannuksissa. Yllä esitetyn konekannan osalta kustannussäästöt ovat vuositasolla noin 60 000 euroa. Mikäli eri ympäristöjä hallinnoidaan eri organisaatioiden toimesta, tulee lisenssien hankinnassa ja hallinnoimisessa tehdä tiivistä yhteistyötä, ettei ylimääräisiä lisenssejä hankita. Lisäksi lisenssien hankinnassa tulee huomioida organisaatioiden luonne. Esimerkiksi yliopisto-organisaatiolle lisenssit ovat usein edullisempia kuin ”normaalille” yritykselle. Lisenssit kannattaa tällöin hankkia edullisemman vaihtoehdon mukaan.

Liite 4 S-Box

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Liite 5 Teemahaastatteluiden rakenne

Tutkimuksessa haastattelut käytiin teemahaastattelun periaatteella. Haastatteluiden rakenne oli seuraava:

Onko teillä tietoa tutkimusongelmaan liittyvistä ratkaisuista tai parhaillaan meneillään olevista projekteista?

Onko teillä tietoa virtualisoidun päätelaiteratkaisun kehittämisestä eri tietoturvaluokan palveluympäristöjen käyttöön samalla päätelaitteella? Mitkä ovat olleet merkittävimmät käyttöä estävät puutteet?

Miltä tutkimuksessa kehitelty ratkaisu vaikuttaa?

Kuinka käyttökelpoisena sitä pidätte? Millaisissa organisaatioissa ratkaisua voisi hyödyntää näkemyksesi mukaan ja kuinka laajasti ? Mitkä näette teknisen ratkaisun merkittävimpinä riskeinä?

Millaisina riskeinä koette tutkimuksessa esitetyt riskit esimerkiksi MBR-viruksen leviämisestä palveluympäristöltä toiselle?

Millaisilla toimenpiteillä riskejä voisi pienentää?

Mihin suuntaan ratkaisua kannattaisi kehittää?

Miten näette ratkaisun käytettävyyden tulevaisuudessa?

Muita huomioita tai vinkkejä?

Vapaata keskustelua ja palautetta käytännön demon jälkeen