Opinnäytetyö

Kiintolevyjen kryptografinen salaus SafeGuard Enterprise -ohjelmistoperheellä ja AES-256-standardilla

Petri Saarenmaa
Tampereen ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Työn ohjaaja: Yliopettaja Mauri Inha

Tekijä: Petri Saarenmaa
Työn nimi: Kiintolevyjen kryptografinen salaus SafeGuard Enterprise -ohjelmistoperheellä ja AES-256-standardilla
Sivumäärä: 32
Valmistumisaika: 12/2010
Työn ohjaaja: Yliopettaja Mauri Inha
Työn tilaaja: Insta DefSec Oy, ohjaaja Janne Reinola

TIIVISTELMÄ

Työn tavoitteena oli tutkia keinoja kannettavien tietokoneiden kiintolevyjen softapohjaiseen salaukseen ja testata niitä laboratorioympäristössä. Salaus on tyyppiä Full Disk Encryption (FDE), jossa kryptataan koko kiintolevyn sisältö vahvalla salauksella. Koneen katoaminen tai varastaminen ei saa – eikä edes pelkän kiintolevyn irrottaminen alkuperäisestä tietokoneesta saa - mahdollistaa tietojen joutumista vääriin käsiin.

Ensisijaisesti tässä työssä käsitellään SafeGuard Enterprise -ohjelmistoa, jonka on suunnitellut tietoturvayritys Sophos, ja merkittävä osa työstä perustuu Sophosin tietokantoihin sekä manuaaleihin omien kokemusten lisäksi.

Avainsanat: opinnäytetyö, virtuaalisointi, Sophos, Safeguard, AES-256, FDE, salaus, kryptografia, kiintolevy

TAMK University of Applied Sciences
Information Technology
Telecommunications and Information Networks
Thesis: The cryptographic encryption of hard disks using SafeGuard Enterprise and AES-256-standard
Pages: 32
Graduation time: 12/2010
Thesis supervisor: Senior Lecturer Mauri Inha
Co-operating Company: Insta DefSec Oy

ABSTRACT

The objective of the thesis was to explore means of encrypting hard disk drives of portable computers via software and to test this in laboratory settings. Using full disk encryption (FDE), the whole content of the hard disk is encrypted. In other words, the disappearance or theft of the hard drive or computer, can and will not compromise the encrypted data.

Primarily this thesis comprehends the use of SafeGuard Enterprise, which is designed by information security company Sophos. A significant part of the thesis is based on Sophos' knowledge bases and manuals in addition to own experiences.

Keywords: thesis, virtualization, Sophos, Safeguard, AES-256, FDE, encryption, cryptography, hard disk

Esipuhe

Työskentelen tamperelaisen Insta Group Oy -konsernin alaisen Insta DefSec Oy:n ITIL-prosessikehyksen mukaisesti työskentelevissä ICT-palveluissa, jotka ovat ISO/IEC 27001-sertifioitu. Osallistuin osana opinnäytetyötäni kehitysprojektiin, jolla tutkittiin mahdollisuuksia uusia yrityksen kiintolevysalaus-ohjelmistoja.

Insta DefSec Oy on puolustus- ja turvallisuusteknologian yritys, ja yrityksen tietoturva-politiikka vaatii, että varsinkin kannettavien tietokoneiden kiintolevyt ovat kryptattuja. Näin alennetaan tietokonevarkauden aiheuttaman tietomurron riskiä.

Työn tarkoitus oli perehtyä jo käytössä olevan salausohjelmiston uudistettuun versioon ja sitä kautta modernisoida työasemien tietoturvaa sekä mahdollistaa niiden tehokkaampi ylläpito ja hallinta. Lopullisena päämääränä oli ohjelmiston tuotantokäyttö.

Haluaisin kiittää tuesta ja kannustuksesta Janne Reinolaa, Ville Kuumolaa sekä muita kollegoitani. Lisäksi kiitos Ari Rantalalle ja Mauri Inhalle avusta. Kiitokset myös avovaimolleni Marille tärkeimmästä tuesta ja jaksamisesta, sekä Ninjalle & Darwinille kehräämisestä ja näppäimistön päällä kävelystä.

Tampereella joulukuussa 2010

Petri Saarenmaa

Termit ja lyhenteet

AD	Active Directory, Microsoftin hakemistopalvelu Windows-toimialueille (domain).
.cer / .p12	Sertifikaattitiedostoformaatteja
DE	Data Exchange, SafeGuard-tuoteperheen osa.
DHCP	Dynamic Host Configuration Protocol, tietoliikenneprotokolla, jota käytetään IP-verkossa jakamaan IP-osoitteet automaattisesti verkkoon liitetyille laitteille.
DNS	Domain Name System, nimipalvelujärjestelmä, jonka perusteella verkkotunnus- tai nimi muutetaan IP-osoitteeksi.
eSATA/SATA	Kiintolevyjen väylästandardeja, eSATA on ulkoisille levyille tarkoitettu ja pelkkä SATA viittaa sisäiseen väylään. Nykyisin useimmiten käytössä SATA II, jonka tiedonsiirtokapasiteetti on maksimissaan 3 gigabittiä sekunnissa.
FDE	Full Data Encryption tai Full Disk Encryption, tässä työssä tarkoitetaan FDE:llä tietokoneen koko kiintolevyn salausta.
FIPS	Federal Information Processing Standard, Yhdysvaltain liittovaltion tietotekniikkastandardijärjestelmä.
IDE	IDE eli Parallel ATA eli rinnakkais-ATA-väylä on vanhempi kiintolevyohjainten väylästandardi.
LDAP	Lightweight Directory Access Protocol, hakemistopalveluiden (kuten Active Directory) käyttämä protokolla.
MBR	Master Boot Record, kiintolevyllä sijaitseva 512-tavuinen boottisektori, joka sisältää mm. osiointitaulun.
NAT	Network Address Translation, osoitteenmuunnos IP-verkossa.
OU	Organizational Unit, Active Directoryssä käytettävä termi toimialueen yksiköstä.
POA	Power-on-Authentication, tietokoneen boottausvaiheessa vaadittava autentikointi, ennen käyttöjärjestelmän latau-

	tumista.
RAM	Random Access Memory, esimerkiksi tietokoneen keskusmuisti.
Rollout	Käyttöönotto; tätä termiä käytetään tässä opinnäytetyössä yritykseen saapuneiden uusien koneiden käyttöönotosta.
S-box	Substition box, eräs symmetristen avainalgoritmien peruskomponentti.
SCSI	Small Computer System Interface, yleinen fyysisten PC-liitäntöjen (mm. kiintolevyt) standardi.
SG	SafeGuard.
SGE	SafeGuard Easy.
SGMC	SafeGuard Management Center.
SGN	SafeGuard Enterprise.
SQL	Structured Query Language, yksi merkittävimmistä tietokantakielistä.
UAC	User Account Control, Windowsin (alkaen versiosta Vista) turvallisuusinfrastruktuurin osa.
VPN	Virtual Private Network, virtuaalinen ja salattu (näennäinen) lähiverkko.
XML	Extensible Markup Language, merkintäkielistandardi.

Sisällysluettelo

1 Yrityksen tietoturva

Lähtökohtana SafeGuard-salausohjelman tutkimukselle ovat yrityksen tarpeet, joiden pohjana ovat sen omien asiakkaiden vaatimukset tietoturvan tasosta. Eritoten puolustus- ja turvallisuusteknologian parissa on tärkeää, ettei yrityssalaisuuksia tai muuta salassapidettävää tietoa kuljeteta selkokielisenä. Tämä ilmenee esimerkiksi VPN-yhteyksien tarpeena, salattuina sähköpostiviesteinä ja tiedostojen salauksena.

1.1 Kiintolevyjen salaus

Yksittäisten tiedostojen salaamisesta seuraava askel kattavampaan tietoturvaan on koko kiintolevyn salaus, josta käytetään nimitystä *full data* (tai *disk*) *encryption* (FDE). Tällöin koko kiintolevyn sisältö käsitellään kryptografisella salaimella, poislukien boottisektori, koska sitä on tietokoneen pystyttävä lukemaan, jotta levyltä voidaan käynnistää käyttöjärjestelmä. Boottisektorille kirjoitetaan pieni ohjelmisto, jonka avulla kiintolevyn salaus voidaan avata.

Olisi toivottavaa, että mahdollisen koneen (tai pelkän kiintolevyn) katoamisen sattuessa voitaisiin varmistaa, että katoamishetkellä kiintolevy oli kryptattu vahvalla salauksella. Vahvaksi salaukseksi on hyväksytty AES-256-standardi. Sitä käyttävät salausohjelmistot soveltuvat tähän, sillä 256-bittistä AES-salausta ei ole vielä pystytty tiedettävästi murtamaan.

Keskitetty ja auditoinnin mahdollistavalla hallintaympäristöllä voidaan todentaa salaus, mikäli kiintolevy häviää. Myös järjestelmäpäivitykset, kuten käyttöjärjestelmän vaihtuminen uudempaan, on yksinkertaisempia suorittaa, kun salausjärjestelmä on keskitetty. Molemmat näistä vaatimuksista edellyttävät modernia kiintolevyn kryptausratkaisua.

1.2 Riskit FDE-salauksessa

Lähes kaikki koko kiintolevyn salaukseen perustuvat tietoturvaratkaisut ovat mahdollisesti murrettavissa ns. kylmäkäynnistys-hyökkäyksen avulla. Hyökkäys perustuu RAM-muistin säilyvyyteen, toisin sanoen siihen, että data säilyy luettavana muistissa vähintään sekunteja ja jopa minuutteja koneen sammuttamisen jälkeen. Kylmäkäynnistys-

hyökkäyksessä kone sammutetaan ja käynnistetään heti uudelleen erilliseltä boottaavalta asemalta, jossa on pieni käyttöjärjestelmä, jonka ainoa toiminta on siirtää keskusmuistin sisältö talteen. Tällaisella hyökkäyksellä voi olla mahdollista saada salausavaimet selville ja purkaa salaus sitä kautta.

Tämä hyökkäys ei niinkään ole tarkoitettu salauksen murtamiseen vaan salauksen kiertämiseen hyväksikäyttäen järjestelmän fyysisiä rajoitteita. Kuten sanottu, käytännössä kaikki FDE-salausjärjestelmät ovat potentiaalisesti murrettavissa näillä keinoin.

2 Advanced Encryption Standard (AES) -salausstandardi

Lyhenne AES tulee sanoista Advanced Encryption Standard, eli ”edistynyt salausstandardi”. AES on lohkosalausmenetelmä, joka on mm. Yhdysvaltojen NSA:n (kansallinen turvallisuuspalvelu, *National Security Agency*) hyväksymä standardi. Standardi on kansainvälisesti hyväksytty ja se on FIPS-hyväksytty. (Validated FIPS 140-1 and…, 2010).

Yleensä eri salaustasot eritellään niiden bittilohkojen koon perusteella, ts. AES-128, AES-192 ja AES-256. Lyhenteen perässä oleva numero kertoo siis bittilohkon koon (128 bittiä, 192 bittiä jne.). (Wikipedia: AES, 2010)

SafeGuard-tuotteet käyttävät AES-standardin mukaista salausta, ja yrityksen käyttöön tulee AES-256, joka on AES-salauksista vahvin ja murtamaton, kuten muutkin AES-salaukset. (Administrator’s Manual…, 2008, 101)

Liitteessä 1 kuvataan salauksen purkaminen pseudokoodi-esimerkillä. AES pohjautuu Rijndael-algoritmiin.

2.1 Rijndael-algoritmin kierrokset

Rijndael-algoritmi perustuu toistuvaan vaiheittaisten muutosten ketjuun. Näitä muutoksia kutsutaan kierroksiksi.

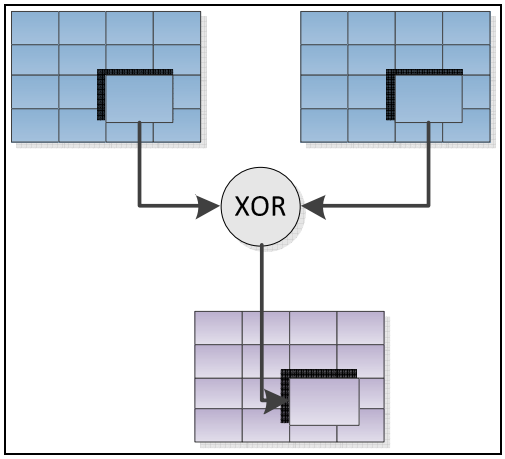
2.1.1 KeyExpansion-vaihe

Ensimmäiseksi kierrosavaimet saadaan Rijndaelin avaintaulusta, jolla laajennetaan lyhyt avain sarjaksi erillisiä kierrosavaimia. Laajennus luo yhteensä Nb (Nr + 1) kappaletta sanoja, algoritmin vaatiessa aluksi Nb kappaletta sanoja ja jokainen Nr -kierros vaatii Nb kappaletta sanoja avaindataa. Lopullinen kierrosavainten sarja sisältää lineaarisen taulukon 4-tavuisia sanoja. (FIPS Publication 197…, 2001, 14, 19)

KeyExpansionin jälkeen siirrytään varsinaisiin kierroksiin, joita AES-256:ssa on 14 kappaletta. AES-128:ssa on 10 kierrosta ja AES-192:ssa 12 kierrosta. (FIPS Publication 197…, 2001, 14)

2.1.2 Ensimmäinen kierros

Ensimmäisellä kierroksella ajetaan vain AddRoundKey-funktio, jossa jokainen tavu yhdistetään kierrosavaimeen XOR-funktiolla (exclusive or, poissulkeva tai). Funktio on esitetty graafisesti kuvassa 1. (FIPS Publication 197…, 2001, 18)



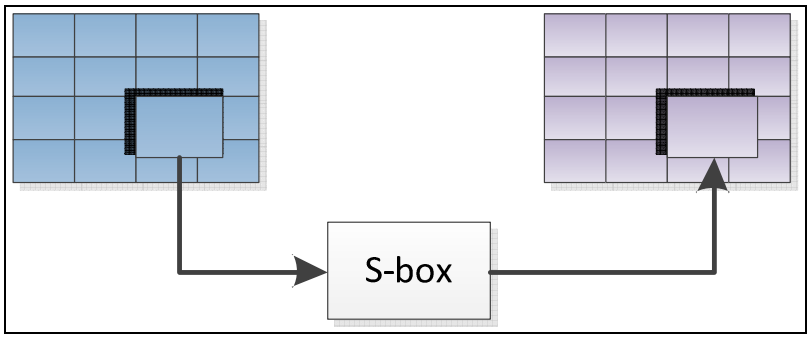
Kuva 1. AddRoundKey.

2.1.3 Varsinaiset kierrokset

Varsinaiset kierrokset koostuvat neljästä eri vaiheesta, jotka ovat

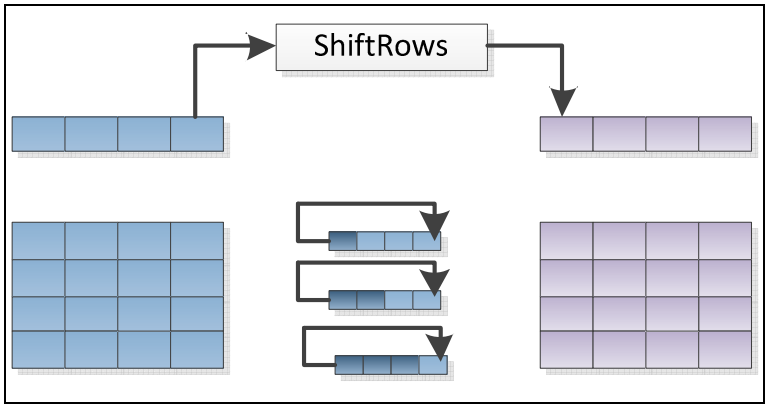
1. SubBytes
2. ShiftRows
3. MixColumns ja
4. AddRoundKey.

Näistä ensimmäisessä, SubBytes-vaiheessa, jokainen taulukon tavu päivitetään pysyvän 8-bittisen korvauslokeron (Rijndael S-box) avulla, joka näkyy kuvassa 2. Tällä *lookup table*en perustuvalla operaatiolla pystytään muodostamaan epälineaarinen salaus. (FIPS Publication 197…, 2001, 15)



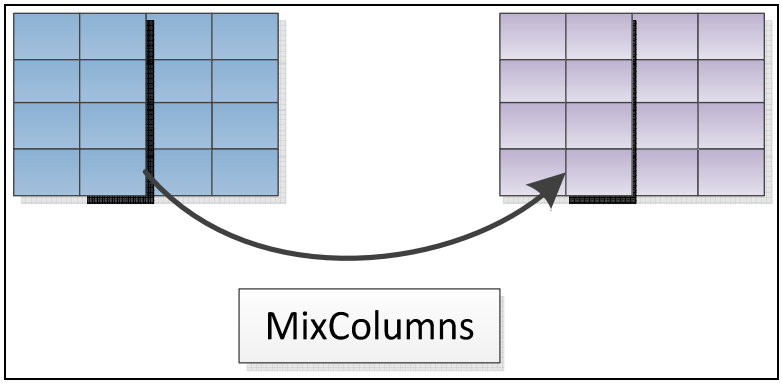
Kuva 2. SubBytes

ShiftRows-vaiheessa tilan rivit siirretään standardissa määritellyllä offset-arvolla. Ensimmäistä riviä ei siirretä, toisen rivin tavuja siirretään kertaalleen (yhden tavun) vasemmalle, kolmatta kaksi kertaa vasemmalle ja niin edelleen. Tämä on esitetty kuvassa 3. 256-bittisessä salauksessa ensimmäinen rivi pysyy muuttumattomana, toinen siirtyy yhden tavun, sen sijaan kolmas kolme tavua sekä neljäs neljä tavua. (FIPS Publication 197…, 2001, 17)



Kuva 3. ShiftRows.

MixColumns-vaiheessa jokaisen tilan neljä tavua, jotka ovat pystysarakkeissa, yhdistetään käännettävän lineaarimuunnoksen kautta. Tässä ei lähemmin tarkastella muunnoksen tarkkaa matemaattista muotoa. Kuvassa 4 näkyy periaate, jolla lohkojen pystysarakkeet sekoitetaan. (FIPS Publication 197…, 2001, 17–18)



Kuva 4. MixColumns.

Lopuksi kierros päättyy AddRoundKey-vaiheeseen, joka käsiteltiin ensimmäisen kierroksen kohdalla.

2.1.4 Viimeinen kierros

Viimeinen (AES-256-salauksessa neljästoista) kierros vastaa edeltäviä kierroksia, mutta MixColumns-vaiheen lineaarimuunnos jää väliin. (FIPS Publication 197…, 2001, 25)

3 Testausympäristö

Testaus- tai laboratorioympäristö koostui pääpiirteittäin yhdestä työasemasta (Core 2 Duo E8500, 3,16GHz; 3,25 GB RAM), eSATA-väyläisestä ulkoisesta kiintolevystä sekä VMWare Workstation 7 -virtuaalisointiohjelmistosta. Näin pystyttiin tekemään edistynyttä testailua hyvinkin edullisilla työkaluilla.

3.1 Virtuaalisointi

Tässä työssä virtuaalisoinnilla viitataan tekniikkaan, jolla isäntäkoneessa (host machine) ajetaan ohjelmistoa, joka pystyy ajamaan useita virtuaalikoneita (virtual machine). Nykyaikaiset moniydinprosessorit ovat mahdollistaneet sen, että pystytään simuloimaan useita koneita samalla isäntäkoneella ja virtuaalisointiohjelmistot mahdollistat näiden välille muodostetut virtuaaliset verkot.

Virtuaalisoinnilla voidaan säästää huomattavia kustannuksia varsinkin laboratorioympäristöä perustettaessa, sillä erillisiä laitehankintoja ei tarvitse tehdä. Yksi tehokas työasema riittää usean palvelimen ja asiakaskoneen simulointiin yhdenaikaisesti. Jos verrataan useiden tuhansien eurojen laitehankintoja parin sadan euron virtuaalisointiohjelmistoon, on säästö selvä.

3.2 VMWare Workstation 7 -ohjelmisto

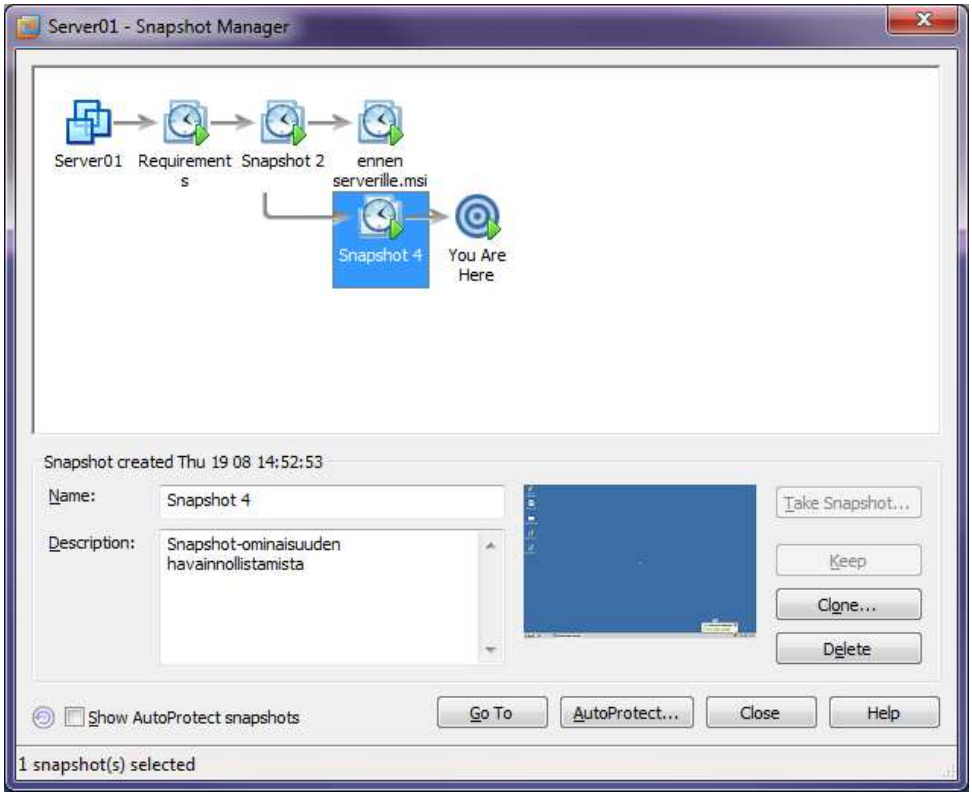
Opinnäytetyössä testattiin SG Enterprise -ohjelmiston toimintaa aluksi täysin virtuaalisesti. Ohjelmistona toimii VMWare Workstation 7, jolla pystyy luomaan ja ajamaan virtuaalikoneita. VMWare tukee virtuaaliverkkoja, jolla voidaan luoda laboratorioverkko isäntäkoneen ”sisään”, jolloin virtuaalikoneet voivat keskustella keskenään. (Workstation User’s Manual…, 2010, 304)

VMWare Workstation tukee isäntäkoneen verkkoresurssien jakamista, jolloin virtuaalikoneiden virtuaaliset verkkokortit saavat VMWaren DHCP:ltä IP-osoitteet isäntäkoneen toimiessa NAT-palvelimena, joka tekee osoitteenmuunnoksen. (Workstation User’s Manual…, 2010, 289)

3.2.1 Snapshot-ominaisuus

VMWaren yksi olennaisista eduista tavalliseen hardwarella tehtyyn testaamiseen on pikakuvien eli snapshottien ottaminen. Pikakuva pystytään ottamaan tavallisesta virtuaalikoneesta nopeimmillaan muutamissa kymmenissä sekunneissa, ja se sisältää kaiken tiedon ko. virtuaalikoneesta kuvan ottamishetkellä. Esimerkiksi voidaan ottaa pikakuva kun virtuaalikoneeseen on asennettu Windows, ja toinen pikakuva kun kaikki olennaiset apuohjelmat on asennettu ja asetukset ovat kohdillaan. Kolmas pikakuva voidaan ottaa levynkryptauksen asennuksen jälkeen ja niin edelleen.

Otettuihin pikakuviin voidaan palata jälkeenpäin, ja kuvassa 5 esitetään, miten VMWare näyttää Snapshot Managerissa niiden kronologisen järjestyksen toisiinsa nähden.



Kuva 5. VMWare Snapshot Manager.

Pikakuvaa tallentaessa sille voidaan antaa nimi (Name) ja kuvaus (Description), jotka helpottavat myöhempää dokumentointia ja testaamista. Kuvassa näkyy miten Snapshot 2 -pikakuvasta on tehty kaksi erillistä testauspolkua (”ennen serverille.msi” ja ”Snapshot 4”). ”You are here”-kohta kertoo missä ajankohdassa virtuaalikone tällä hetkellä on.

3.2.2 Virtuaalikoneet

Vähintään kaksi virtuaalipalvelinta tarvittiin testiympäristön perustamiseen, kuten myöhemmin selviää. Lisäksi tarvittiin yksi virtuaalityöasema, jolta ajetaan hallintaohjelmistoa sekä muutamia, joihin asennetaan client-ohjelmistot. Yksi palvelin asennettiin toimimaan virtuaalisen toimialueen Active Directory -palvelimena, jotta voidaan testata tietokannan siirtoa. Taulukoon 1 on kuvattu testauksessa käytetty tekninen ympäristö.

Virtuaalikoneen nimi	Käyttötarkoitus
Server01	Active Directory
Server02	SQL-palvelin
Server03	SafeGuard Enterprise ja Management Center
Client01	IT-ylläpidon kone, jolle on asennettuna Management Center. Niin sanottu admin-kone.
Client 02 … Client 06	Loppukäyttäjien koneet

Taulukko 1. Virtuaalikoneet.

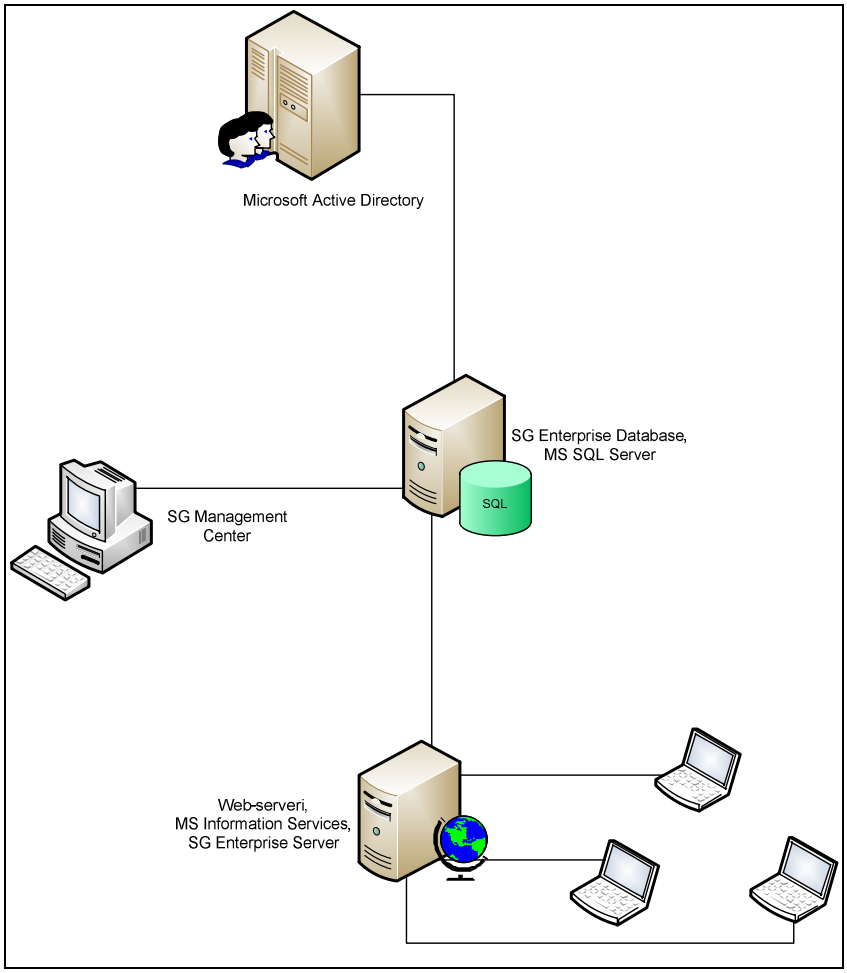
3.3 Käyttökokemukset virtuaalisoinnista

Virtuaalisointi mahdollisti helpomman, tehokkaamman ja nopeamman tavan testata SGN-ohjelmistoa kun vertaa tavallisilla työasemilla ja palvelimilla vastaavan testauksen tekemiseen. VMWaren snapshot-ominaisuudella pystyi palauttamaan jopa katastrofaalisten ongelmien jälkeen testiympäristön oletustilaansa. Muun muassa tietokannan korruptoitumisen testaaminen olisi perinteisellä menetelmällä vaatinut koko tietokannan varmuuskopioinnin konfigurointia, nyt testauksen jälkeen riitti yksi klikkaus.

Virtuaalisointi ei toki ole täysin ongelmaton. Ensinnäkin saadut kokemukset eivät ole suoraan vietävissä reaalimaailmaan, jossa konekonfiguraatiot ja ohjelmistokokoonpanot vaihtelevat merkittävästi. Toiseksi, koska testataan koneen fyysisen komponentin (kiintolevyn) toimintaa, jota virtuaalikoneessa edustaa isäntäkoneen kiintolevyllä oleva tiedosto, joudutaan ottamaan tiettyjä asioita huomioon. Muun muassa yksi ongelmatilanne liittyi SCSI-kiintolevyn emulointiin, kun tämä levyjärjestelmä ei ollut testatun tuotteen tukema.

4 SafeGuard Enterprise -tuoteperhe

Työssä käytetty ja tutkittu ohjelmisto, SafeGuard Enterprise (SGN), on ohjelmistoperhe, johon kuuluu useita komponentteja isäntäpuolelle (palvelimet), hallintaan (*admin*-työasemat) sekä asiakaskoneisiin (*client*). Eri komponentit saattavat sijaita erillisillä fyysisillä laitteilla tai virtuaalikoneilla tai sitten samalla koneella saattaa olla useita komponentteja asennettuna. Kuvassa 6 näkyy komponenttien suhde toisiinsa.



Kuva 6. SG Enterprise -ohjelmistoperheen komponentit

4.1 Komponentit

Seuraavassa käydään läpi SGN-tuoteperheen eri komponentit.

4.1.1 Tietokanta: SGN Database

SafeGuard Enterprise vaatii tuekseen tietokannan, jonne varastoidaan käyttäjätiedot, koneiden sertifikaatit ja turvapolitiikat. Käyttäjätietokanta voidaan tuoda Microsoft Active Directory -toimialueen tietokannasta. Näin jo kertaalleen luotu käyttäjähierarkia replikoituu SGN:n tietokantaan, eikä jouduta luomaan jokaista käyttäjää erikseen. (Installation Manual…, 2008, 16)

Tietokannan teknisiin vaatimuksiin kuuluu Microsoft SQL Server, jonka on sijaittava omalla fyysisellä tai virtuaalisella koneella (valmistajan suositus). Virtuaalilaboratoriossa käytettiin MS SQL Express -asennusta, joka riittää demotarkoituksiin, mutta on varsinaista SQL-palvelinta kevyempi käyttää ja hallinnoida. (Installation Manual…, 2008, 17)

4.1.2 Hallinta: SG Management Center

Management Center (SGMC tai MC) on ohjelmisto, joka voidaan asentaa jollekin hallintapalvelimelle tai tavalliselle työasemalle, joka on SafeGuardin hallintakäyttäjän tai -käyttäjien käytössä. Management Centerille ei ole erikoisia vaatimuksia, mutta edellä mainittu SQL-palvelin on asennettava ensin. (Installation Manual…, 2008, 35)

Hallintaohjelmistolla hoidetaan keskitetysti työasemien hallintaa Enterprise Databasen kautta, luomalla sinne esim. tietoturvapolitiikoita (*policies*). Management Center kommunikoi tietokannan kanssa, kun taas asiakaskoneet Enterprise Serverin kanssa. (Installation Manual…, 2008, 18)

4.1.3 SGN Server -palvelin

Omalla palvelinkoneellaan sijaitsee SG Enterprise Server, joka toimii käyttäjien ja SG-tietokannan rajapintana. Esimerkiksi käyttäjän kirjautuessa koneelle, asiakaskoneen aloittaman pyynnön jälkeen, SG Enterprise Server lähettää politiikan asiakaskoneelle. Palvelin pyörii sovelluksena Microsoft Internet Information Services (IIS) -pohjaisella webpalvelimella. (Installation Manual…, 2008, 25–26)

Vaatimuksena SG Enterprise Serverillä on siis IIS, joka on Microsoftin webpalvelin, ja suosituksena on, että se pyörii omalla palvelinkoneellaan.

4.2 Asiakaskoneet

Lähtökohtaisesti SG Enterprise -ympäristössä asiakaskoneet asennetaan keskitetysti ja ne ovat keskitetyn hallinnan piirissä. Tällöin koneisiin asennetaan MSI-paketoidun asennuspaketin avulla SafeGuard Enterprise Device Encryption.

Device Encryption -ohjelmisto salaa koneen kiintolevyn määritellyn tietoturvapolitiikan mukaisesti, pois lukien kiintolevyn boot- eli käynnistyssektori (*master boot record*, MBR), jonne kirjoitetaan pieni ohjelmisto, joka kysyy käyttäjänimen ja salasanan. Ohjelmistoa kutsutaan POA:ksi, *Power-on Authentication*, joka käynnistyy ilman mitään käyttöjärjestelmää. (Administrator's Manual…, 2008, 263)

Oikean käyttäjänimi/salasana-yhdistelmän syötettyään kone alkaa ladata käyttöjärjestelmää. Käyttäjänimi ja salasana voidaan synkronoida AD-toimialueen kanssa, jolloin käyttäjä samalla kirjautuu Windows-käyttöjärjestelmäänsä POA:iin syöttämillään tunnuksilla. Näin käyttäjän tarvitsee muistaa vain yksi salasana. (User Manual…, 2008, 28)

4.2.1 Online-asiakaskoneet

Device Encryption -ohjelmisto toimii aina aloittajana yhteyksissä sen ja palvelimen välillä. Käyttäjän kirjautuessa koneelleen, ohjelmisto kyselee esim. muuttuneet turvapolitiikat palvelimelta. Lisäksi voidaan asettaa esim. 90 minuutin aikaväli, jolloin aina kysellään palvelimelta ohjeistusta. Tämä tietysti toteutuu vain, jos palvelimeen on tietoliikenneyhteys. (Administrator's Manual…, 2008, 82)

SG Enterprise on suunniteltu siten, että palvelinyhteys ei ole tärkeä varsinaisen FDE-salauksen kannalta, ellei tarkoitus ole jatkuvasti muuttaa tietoturvapolitiikkaa. Jos tarkoituksena on salata käytännössä kaikki kannettavien tietokoneiden kiintolevyt ja jo käyttöönotossa vahvistaa politiikat pysyviksi, ei yhteyttä tarvita muulloin kuin salasanaa vaihdettaessa.

4.2.2 Offline-asiakaskoneet

Yrityksessä, jossa koneita on satoja, on aina poikkeustapauksia, joiden tietoturva joudutaan räätälöimään erityistarpeiden mukaisesti. Silloin voidaan asentaa Device Encryption -ohjelmisto offline-tilassa. Tällaisessa tapauksessa asennus tehdään Standalone-asennuspaketilla. (Installation Manual…, 2008, 62)

Standalone-asennus vaatii tuekseen SG Policy Editorilla tehdyn tietoturvapolitiikan, joka ajetaan asennuksen yhteydessä. Politiikka voi olla sama kuin keskushallinnan piirissä olevilla, mutta Standalone-asiakasohjelma ei kysele päivityksiä palvelimelta. Salasana voi silti olla synkronoitu Windows-kirjautumisen kanssa. Tällainen Standalone-asennus on helppo migraation kautta tuoda myöhemmin keskushallinnan piiriin. (Installation Manual…, 2008, 56)

Vielä harvinaisempia erikoistapauksia varten on olemassa kokonaan offline-käyttöön tarkoitettu asiakasohjelma, nimeltään SafeGuard Easy. Sen ominaisuudet ovat joltain osin rajoitetummat kuin SGN-ohjelmiston.

4.3 Muut SGN-tuotteet

SGN-ohjelmistoperheeseen kuuluu muutamia lisämoduuleita, jotka ovat maksullisia lisätuotteita. Niiden tutkiminen ja käyttöönotto eivät kuulu kuitenkaan tämän opinnäytetyön piiriin, mutta seuraavassa ne esitellään pinnallisesti.

4.3.1 Configuration protection -moduuli

Ohjelmistoon sisältyy myös mm. SG Configuration Protection -moduuli, jolla voidaan vaatia esim. USB-muistien salausta tai estää muistitikkujen käyttö koneissa kokonaan. (Installation Manual…, 2008, 62, 64)

Mikäli käytössä on *hardware*-tason kryptattuja muistitikkuja, ja Configuration Protection mahdollistaisi esim. näiden sallimisen (*whitelist*), ja kieltää tavallisten (salaamattomien) muistitikkujen käyttö.

4.3.2 Data exchange -moduuli

SG Data Exchange (DE) on tarkoitettu muistitikkujen, CD/DVD-levyjen ja vastaavien medioiden salaukseen. DE tukee sähköpostiviestien salaamista SafeGuard PrivateCrypto -ohjelmiston avulla ja se mahdollistaa esim. projekti- tai ryhmäkohtaiset salausavaimet, joten samassa projektissa työskentelevät voisivat läpinäkyvästi salata liikuteltavat

mediat ja kaikki projektin työntekijät voisivat myös läpinäkyvästi tarkastella niiden sisältöä.

4.3.3 Partner connect -moduuli

SG Partner Connect -moduuli tarjoaa mahdollisuuden integroida Windows Vista ja Windows 7 -käyttöjärjestelmien BitLocker-salausohjelmiston SG-tuotteisiin, sekä keskitetyn hallinnon tälle.

4.4 Liittyvät Windows-tuotteet

Koska kyseessä on Windows-ympäristö, on olennaista esitellä tässä työssä mainitut eri tuotteet, joita vaaditaan taustalle toimimaan, jotta voidaan implementoida SGN-ympäristö niiden päälle. Asiakaspuolella tuettuja käyttöjärjestelmiä ovat Windows XP (vähintään Service Pack 2), Windows Vista sekä Windows 7 (myös 64-bittinen versio). Palvelinpuolella tuettuja ovat Windows Server 2003 sekä 2008, molemmista myös 64-bittiset versiot käyvät.

Nämä tiedot pitävät paikkansa, kun käytetään vähintään SGN-versiota 5.50.

4.4.1 Microsoft SQL Server -palvelin

Microsoftin tietokantapalvelin SQL Server toimii SGN:n tietokannan taustalla. Tämä on Microsoftin suunnittelema relaatiotietokantapalvelin, joka käyttää SQL-kyselykieltä. Testiympäristössä käytettiin SQL Server Express -tuotetta, joka on ilmainen mutta rajoitettu versio Microsoftin kaupallisesta palvelimesta. Se soveltuu hyvin testaukseen.

SQL-tietokantaa hallinnoitiin SQL Server Management Studio -ohjelmistolla.

4.4.2 Internet Information Services -palvelu

Useiden Windows-käyttöjärjestelmien mukana tuleva Internet Information Services (IIS) on Microsoftin oma webpalvelinohjelmisto. Sitä vaaditaan SGN Serverin toimintaan, ja sen pitää olla asennettu sekä otettu käyttöön SGN Serverillä.

4.4.3 Active Directory -toimialue

Windows-ympäristössä domain- eli toimialuekirjautumiseen ja -ympäristöön tarvitaan Active Directory (AD), joka sisältää tiedon mm. toimialueen tietokoneista ja käyttäjistä. AD tarjoaa Windows-toimialueelle mm. LDAP-protokollapalveluita ja DNS-nimipalveluita.

SGN tukee käyttäjä- ja konetietojen tuomista AD:sta SGN:n omaan tietokantaan. Näin vältytään manuaaliselta konekannan luomiselta, mikäli yrityksellä on käytössä jo AD.

4.4.4 Microsoft Windows XP ja Windows 7 -käyttöjärjestelmät

Testatut loppukäyttäjien käyttöjärjestelmät olivat Windows XP sekä Windows 7. SGN tukee myös mm. Windows Vistaa, mutta sen testausta ei pidetty tärkeänä, koska loppukäyttäjillä ei sitä ole käytössä.

5 Asennus

Tässä luvussa käsitellään palvelinpuolen asennus käyttökuntoon sekä asiakaskoneiden alustava konfigurointi ja asennus.

5.1 Asennuksen vaatimukset

Tarvetta on vähintään yhdelle Windows Server 2003 tai 2008 -koneelle, josta tehdään SGN Server ja toiselle palvelimelle, joka on Microsoft SQL Server. SQL-tietokantapalvelimelle on oltava luotuna tietokanta. Asiakaskoneissa on oltava jokin tuettu käyttöjärjestelmä asennettuna.

5.1.1 Active Directory -integraatio

AD-toimialue ei ole pakollinen SGN-ympäristön pystyttämisessä, mutta mikäli yrityksen käyttäjähallinta tapahtuu sen kautta, voidaan käyttäjä- ja konetiedot tuoda siitä suoraan SGN-ympäristöön ja näin säästetään manuaalista työtä.

5.2 Hallinta

Hallintakomponenteilla tässä tarkoitetaan SafeGuard Enterprise -tietokantaa sekä SafeGuard Enterprise Server -palvelinta, jolla voi sijaita myös SafeGuard Management Center. SGMC voi sijaita myös asiakaskoneella, esimerkiksi ylläpidon tai helpdeskin koneilla.

5.2.1 Tietokannan asennus ja valmistelu

Ensimmäiseksi SGN-komponentiksi asennetaan SafeGuard Enterprise -tietokanta. Se voidaan luoda joko skriptillä tai SG Management Centerin asennuksen yhteydessä aktivoituvaa konfigurointi-velhoa.

Asennuksen aluksi pitää luoda SQL-tietokannalle käyttäjä. Tämä onnistuu SQL Server Management Studiolla.

Luodaan uusi *Login*, johon syötetään *Login name* -kohtaan käyttäjän nimi ja valitaan Windows-autentikointi (käytetään siis Windows-salasanaa). *Server roles* -sivulta (valitaan vasemmalta) asetetaan käyttäjälle *dbcreator*-rooli. Asennuksen jälkeen roolin voi pudottaa *dbowner*-rooliksi.

5.2.2 Hallintaohjelmistot

Näiden esivalmistelujen jälkeen käynnistetään SG Management Centerin (SGMC) asennusvelho (SGNManagementCenter.msi). Tervetuloa-ikkunasta valitaan Next, sitten hyväksytään lisenssiehdot, valitaan asennuspolku ja asennustyyppi *Typical*.

Asennuksen jälkeen käynnistyy SGMC:n konfiguraatiovelho, johon syötetään tietokannan sijainti ja kirjautumistiedot.

Koska tietokantaa ei ole vielä luotu, valitaan *Create a new database named:* ja annetaan sille nimi. Tämän jälkeen luodaan pääkäyttäjä, *Master Security Officer* (MSO). Tälle annetaan nimi ja määritellään, tarvitseeko kirjautuessa käyttää toimikorttia. MSO:lle pitää luoda sertifikaatti painamalla *Create…*

Sertifikaattivarastolle annetaan salasana, jonka jälkeen asennus haluaa viedä sertifikaatin tiedostoon ja ko. tiedosto salataan uudella salasanalla. Tämän jälkeen pitää vielä luoda yritykselle oma Company-sertifikaatti. Varsinainen asennus on sen jälkeen valmis.

Seuraavaksi avautuu SGMC:n hallintaikkuna, ja tässä vaiheessa olisi suositeltavaa ottaa varmuuskopiot luoduista sertifikaateista. Avataan *Tools / Options / Certificates / Export…* ja syötetään sertifikaattitiedoston salasana. Jos asennus jostain syystä vikaantuu, näitä varmuuskopioituja sertifikaatteja voidaan käyttää sen pelastamiseksi.

5.2.3 SGN Server -palvelinasennus

Seuraavaksi käynnistetään SGE Serverin asennusvelho (SGNServer.msi). Vaatimuksena on, että koneeseen on asennettu Microsoft Internet Information Services (IIS), .NET Framework 3.0 SP1 sekä ASP.NET 2.0 asennettuna ja aktivoituna. Asennusvelho tarkistaa täyttyvätkö edellä mainitut vaatimukset.

Itse velhossa ei tehdä mitään valintoja vaan hyväksytään lisenssisopimus ja painetaan kaikkiin *Next*.

Seuraavaksi palataan SGMC:n hallintaikkunaan, josta valitaan *Tools / Configuration Package Tool…* Mikäli SGMC on samalla koneella kuin SGN Server, valitaan *Make this computer an SGN Server*, muussa tapauksessa tehdään erillinen konfiguraatiopaketti palvelimelle. Konfiguraatiopaketti ajetaan, painetaan *Next* ja *Finish*.

Tämän jälkeen konfiguroidaan IIS, josta valitaan *Web Sites / SGNSRV / Properties*. Avautuvasta ikkunasta valitaan *Directory Security*, jonne sallitaan *Enable anonymous access* ja otetaan rasti pois *Integrated Windows authentication* -kohdasta.

Tässä vaiheessa SQL-tietokannasta pitää tarkistaa, että tietokantaan pääsee kirjautumaan *Login* nimeltään *NT AUTHORITY\NETWORK SERVICE*. Tälle virtuaalikäyttäjälle annetaan *Server Roles* -kohdasta *public*- ja *sysadmin*-roolit.

5.2.4 Toimialueen tuonti SGN-ympäristöön

Tämän jälkeen ollaan valmiit tuomaan Active Directorysta käyttäjä- ja konetiedot. SGMC:n hallintaikkunasta valitaan ensin *Root [Filter is active]* ja mennään valikkoon *Tools / Options / Directory* ja syötetään AD:n LDAP-tiedot.

Painetaan OK ja sen jälkeen *Synchronize*-kohdasta *Synchronize*-nappia. Avautuvasta ikkunasta näkee synkronointitiedot. Tämän jälkeen SGE-ympäristö on hallintapuolelta asennettu. Sen jälkeen vuorossa on joko politiikkojen (policy) tekeminen tai tuonti, jos ne on jo ennalta laadittu.

5.3 Asiakaskoneet

Keskitetyn hallinnan piiriin tuotaviin koneisiin on tehtävä ns. managed-asennus, joka vaatii kolmen erillisen MSI-asennuspaketin ajamista. Näistä ensimmäinen sisältää erilaisia kryptografisia kirjastoja yms., joita SGE vaatii toimiakseen. Asennus ei onnistu jos näitä ei ole ensin asennettu. Tämä voidaan ennalta asentaa vaikka kaikkiin koneisiin, mikäli yrityksellä on käytössä jonkinlainen etäasennusmahdollisuus.

Toinen paketti on varsinainen SGE-asennus, jonka jälkeen asennetaan välittömästi salauspolitiikan sisältävä kolmas paketti. Tämä viimeinen MSI-tiedosto on konfiguraatiopaketti, joka on luotu SG Management Centerillä, joka on asennettu hallintapalvelimelle.

Konfiguraatiopaketin luodaan SGMC:ssä valitsemalla *Tools / Configuration Package Tool / Create Configuration Package (managed).* Jos halutaan tehdä kokonaan uusi paketti, painetaan ensin *Add Configuration Package*. Voidaan myös editoida nykyisiä paketteja.

Configuration Package Toolista annetaan nimi konfiguraatiopaketille ja valitaan mitä politiikkaryhmää se käyttää (*Policy Group*).

5.3.1 Managed-asennus

Suositeltava toimintatapa on käyttää ns. *rollout*-käyttäjiä, joita kutsutaan POA-käyttäjiksi. Power-on-Authentication (POA) ei aktivoidu ennen kuin koneelle kirjaudutaan jollain muulla käyttäjätunnuksella kuin politiikassa määritellyllä POA/rollout-käyttäjällä.

Windows 7:ssä UAC oli asetettu pois päältä, joten tässä ei oteta kantaa sen kysymiin varmistuksiin. Windows XP:ssä asennus ajettiin administrator-oikeuksin. Ensimmäiseksi asennetaan esiasennuspaketti, jonka jälkeen käynnistetään kone uudelleen.

Tämän jälkeen ajetaan varsinainen asennuspaketti, josta valitaan *Device Encryption* ja *Volume Based Encryption.* Heti perään ajetaan konfiguraatiopaketti, jonka jälkeen kone käynnistyy uudelleen. Ensimmäisellä käynnistyksellä POA-ruutu ohitetaan kokonaan.

Tämän jälkeen voidaan kirjautua Windowsiin uudelleen, suositeltavaa olisi kirjautua POA-tunnuksella, jolloin POA ei aktivoidu. Mikäli on tarvetta kirjautua muulla tunnuksella, POA aktivoituu. Windowsiin kirjautumisen jälkeen alapalkissa näkyy ponnahdusikkuna, joka antaa mm. tietoja SGN-palvelinyhteydestä.

Salaus alkaa välittömästi. Koneen uudelleenkäynnistys ei vaikuta salaukseen millään tavalla. Salausohjelma käyttää koneen vapaita resursseja, ja salaus hidastuu, mikäli koneella halutaan tehdä jotain.

Mikäli koneeseen ei ole kirjauduttu muulla kuin rollout/POA-tunnuksella, POA ei ole vielä aktiivinen. Tällöin loppukäyttäjä kirjautuu koneeseen omilla Windows-tunnuksillaan koneen uudelleenkäynnistyksen jälkeen.

Tämän jälkeen POA aktivoituu, joten seuraavalla käynnistyskerralla avautuu SafeGuardin kirjautumisruutu, johon syötetään Windows-tunnukset normaalisti ja valitaan oikea domain-toimialue.

POA-ruudussa Options-nappia painamalla avautuu lisäasetuksia. Oletusarvoisesti Pass through logon to Windows on aktiivisena, joten Windowsiin ei tarvitse enää kirjautua

samoilla tunnuksilla uudelleen. POA:n aktivoiduttua, ensimmäinen siihen kirjautunut käyttäjä on sen ainoa varsinainen käyttäjä (*owner*).

Kun kone toimitetaan loppukäyttäjälle, kirjautumistietoihin syötetään ne domain-tunnukset, joilla koneeseen on jo kertaalleen kirjauduttu. Myös salasana syötetään, mutta ei painetakaan *OK* vaan *Options*, josta otetaan rasti pois *Pass through logon to Windows* -kohdasta. Sen jälkeen painetaan *OK* ja odotetaan Windowsin kirjautumisruutua. Windowsiin voi nyt kirjautua millä tahansa käyttäjällä, jolla on oikeus kyseiseen työasemaan kirjautua. Loppukäyttäjä kirjautuu tässä vaiheessa koneeseen. Seuraavalla käynnistyskerralla POA hyväksyy myös tämän käyttäjätunnus/salasana-parin. Ensimmäisen Windowsiin kirjautumisen tämän jälkeen näkyy SafeGuard-ponnahdusikkuna, jossa kerrotaan: ”Initial user synchronization completed”.

Tällä menettelyllä koneeseen voi lisätä muita käyttäjiä.

5.3.2 Managed-koneet hallintapalvelimella

Kun on tehty uusi managed-tyyppinen asennus, ilmestyy kyseinen kone SGMC:iin. Mikäli konetiliä (*computer account*) ei vielä ole ollut AD:ssa viimeisimmän synkronoinnin yhteydessä, kone ilmestyy ”.Auto registered”-ryhmään. Jos taas AD-synkronoinnissa konetili on tuotu SGMC:n tietokantaan, kone löytyy oikeasta *Organizational Unitista* (OU).

Tämän takia autorekisteröintiryhmässä on syytä olla asetettuna sopiva politiikka, jotta kone saa politiikat rekisteröityessään palvelimelle. Mikäli eri OU:lla halutaan pitää erilaisia politiikkoja, olisi syytä synkronoida SGMC AD:n kanssa usein, jotta koneet siirtyvät oikeaan politiikkaryhmään (kts. 5.2.4).

5.3.2 Standalone-asennus

Koneelle, joka ei ole SGN-hallinnan piirissä, voidaan asentaa ns. standalone-salaus. Olennaisia eroja ei juuri ole asennuksessa, konfiguraatiopaketti luodaan standalone-tyyppiseksi. Palvelinyhteyttä käytetään ainoastaan asennusvaiheessa, jolloin SG lähettää

hallintapalvelimelle varmuuskopion salausavaimesta, jonka avulla voidaan salaus vielä purkaa koneesta myöhemmin tai suorittaa muita ylläpitotehtäviä.

Mikäli standalone-asennettuun koneeseen halutaan tehdä policy-muutoksia, ne pitää jaella erillisellä MSI-paketilla, kun taas managed-asennuksissa palvelin jakaa uudet politiikat aina kirjautumisvaiheessa.

5.4 Politiikan luonti

Politiikka (policy) luodaan SGMC:ssa valitsemalla *Policies*-välilehti. Policies-sivulta löytyy Policy Items -lista, jonka alla ovat määritellyt politiikat. Klikkaamalla *Policy Items* -tekstiä, valitaan *New* ja haluttu politiikkatyyppi.

Kun politiikka on luotu ja tallennettu, luodaan vielä politiikkaryhmä (Policy Group) samalla tavalla. Tämän jälkeen politiikkaryhmään siirretään kaikki halutut politiikat ja tallennetaan. Yksittäisiä politiikkoja ei voi kohdentaa koneille, vaan aina kohdennetaan kokonainen politiikkaryhmä.

5.4.1 Tärkeimmät politiikat

Taulukossa 2 on esitettynä olennaisimmat politiikat kommentoituna.

Policy	**Kommentti**
Logon mode: **User ID/Password**	Koneeseen kirjaudutaan käyttäjänimi-salasana-parilla.
Display unsuccessful logons for this user Display last user logon Disable ’forced logoff’ in workstation lock: **No**	Kaikki kolme kirjautumisesta lisätietoja antavaa politiikkaa on asetettu No-tilaan, jotta ei näytetä turhia tietoja käyttäjälle.
Activate user/domain preselection: **Yes**	POA-kirjautumisruutu muistaa edellisen käyttäjänimen ja domainin

Service Account List: **[listan nimi]**	Rollout-käyttäjät on asetettu valitulle listalle. Tällaisella käyttäjätunnuksella kirjautuessa POA ei aktivoidu.
Pass through to Windows: **Let user choose freely**	Käyttäjä voi valita kirjautuuko automaattisesti Windowsiin samoilla tunnuksilla kuin POA:iin.
Maximum no. of failed logons: **[numero]**	Esim. viiden kirjautumisyrityksen jälkeen kone menee lukkoon. Jokainen epäonnistunut kirjautumisyritys lisäksi aiheuttaa viiveen, ennen kuin salasanan voi yrittää syöttää uudelleen. Viiveen kasvu on lisäksi eksponentiaalinen.
Display ”Logon failed” messages in POA: **Standard/Verbose**	Määrittää miten tarkkaa tietoa epäonnistuneista kirjautumisista annetaan. Standard antaa vähemmän tietoa.
Reaction to failed logons, Lock machine: **Yes**	
Lock screen after X minutes of inactivity: **[numero]**	Voidaan määritellä, että Windows menee lukkoon, kun konetta ei käytetä tiettyyn minuuttimäärään mennessä. Tämä voidaan määritellä myös Windowsin omilla policyillä.
Lock screen after resume: **Yes**	Määrittelee, onko Windows lukittuna, kun se käynnistetään valmiustilasta.
Media encryption mode: **Volume based**	Käytetään koko kiintolevyjen salausta.
Algorithm to be used for encryption: **AES256**	Myös AES-128-salaus olisi valittavana.
Key to be used for encryption: **Defined machine key**	Koneavain luodaan automaattisesti.
User may add or remove keys to or from encrypted volume: **No**	Käyttäjälle ei anneta oikeuksia poistaa avaimia.

Reaction to unencrypted volumes: **Accept all media and encrypt**	SGN salaa kaikki kiintolevyt. Tässä on huomattava, että mikäli käyttäjä kytkee koneeseen esim. USB-kiintolevyn, SGN salaa sen oletusarvoisesti.
User may decrypt volume: **Yes**/**No**	Määrittää, voiko käyttäjä itse poistaa kryptauksen levystä. Normaalipolitiikassa tämä kannattaa pitää kiellettynä, ja tehdä erillispolitiikka, mikäli yksittäisestä kiintolevystä halutaan poistaa kryptaus. Erillisen politiikan voi sitten kohdistaa oikealle koneelle.
Proceed on bad sectors: **Yes**/**No**	Voidaan säädellä, pysähtyykö levynsalaus, mikäli se havaitsee rikkoutuneita kiintolevysektoreita.
Language used on client: **English**	
Activate logon recovery after Windows Local Cache corruption: **Yes/No**	Määrittää, avataanko recovery-dialogi automaattisesti, mikäli Windowsin paikallinen salasanavälimuisti on korruptoitunut.
Enable Local Self Help: **No**	Käyttäjä ei itse voi ohittaa salasanakyselyä.
Enable Logon recovery via Challenge/Response: **Yes**	Sallitaan pelastustoimenpiteet Recovery-valikosta.
Allow automatic logon to Windows: **Yes**	Automaattinen Windowsiin kirjautuminen on sallittu.
Enable POA: **Yes**	POA-ruutu aktiivinen.
Display machine identification: **Workstation name**	Määrittää miten POA-ruudussa esitetään koneen tiedot.
Display legal notice: **Yes/No**	POA-ruutuun voi määritellä infotekstin, esim. ”Vain luvallinen käyttö sallittu, yrityksen ABC omaisuutta!”
Display additional information: **Never**	Lisäksi voidaan määritellä “lisätietoja”.
Enable and show the system tray icon: **Yes/No**	Voidaan piilottaa SGN-ikoni Windowsista.

Show overlay icons in Explorer: **Yes/No**	Tällä viitataan Windowsissa näkyvään ponnahdusikkunaan, joka kertoo SGN-palvelun tietoja.
Virtual keyboard in POA: **Yes**	Mikäli koneen näppäimistö ei toimi, voi POA-ruudussa käyttää virtuaalinäppäimistöä.
Uninstallation allowed: **Yes/No**	Mikäli poistaminen kielletään, asennusta ei voi poistaa muuttamatta politiikkaa.
Enable Sophos tamper protection: **No**	Tämä liittyy Sophoksen erilliseen Endpoint Security and Control –ohjelmistoon.

Taulukko 2. Merkittävimmät politiikat.

Lisäksi policyyn voi asetettaa Recovery-dialogin infoteksti, jonne voidaan lisätä esim. ICT-tuen yhteystiedot. Myös salausruudun taustagrafiikat voidaan määritellä politiikassa.

Logituspolitiikka on määriteltävissä jokaisen virheilmoituksen kohdalta erikseen. Toisin sanoen voidaan hallita, mitä virheilmoituksia logiin kirjoitetaan.

5.5 Salasanan unohtuminen tai vaihtuminen

Mikäli käyttäjä on itse vaihtanut salasanaansa esim. toisella koneella tai ylläpito on vaihtanut sen AD:n kautta, POA-kirjautuminen ei voi vielä tietää uutta salasanaa. Tällöin pitää kirjautua POA:iin kerran vanhalla salasanalla, jonka jälkeen Windowsin kirjautumisruutu herjaa virheellisestä salasanasta. Tämän jälkeen Windowsiin kirjaudutaan normaalisti uudella salasanalla.

Koska SG käyttää samaa käyttäjätunnus/salasana-paria kuin Windows, käyttäjän unohtaessa salasanansa, pitää se nollata myös Active Directorysta. Jotta POA-salasana saadaan vaihdettua salasanan unohtuessa, pitää käyttää Challenge/Response-menettelyä.

5.5.1 Challenge/Response-menettely

Käyttäjän päässä painetaan *Recovery*-nappia POA-kirjautumisruudussa. Käyttäjä lukee Challenge-kohdassa lukevan 30-merkkisen kirjan/numero-jonon. Tukihenkilö avaa SGMC:n, josta mennään valikkoon *Tools/Recovery* ja valitaan oikea kone.

Ensin valitaan *Domain*, jonka jälkeen painetaan …-nappia, josta avautuu hakuikkuna, josta haetaan haluttu kone. Painetaan *Next*, jonka jälkeen valitaan käyttäjä painamalla …-nappia ja käyttämällä hakua. Syötetään käyttäjän luettelema avain ja valitaan haluttu tukitoiminta – tässä tapauksessa *Boot SGN Client without user logon.*

Käyttäjä kirjoittaa tukihenkilön ilmoittaman 60-merkkisen avainjonon. Tämän jälkeen kirjaudutaan Windowsiin uudella salasanalla, jonka ylläpito on vaihtanut AD:ssa. Sophos SafeGuard kysyy sen jälkeen vanhaa salasanaa, mutta koska se oli unohtunut, painetaan *Cancel*. Tämän jälkeen luodaan uusi sertifikaatti uuden Windows-salasanan pohjalta. Salausavain ei kuitenkaan muodostu uudelleen. Seuraavalla POA-kirjautumisella käytetään jo uutta salasanaa.

6 Testaus

Testaus perustui VMWare Workstation 7 -ohjelmistolla tehdyille virtuaalikoneille. Aluksi virtuaalikoneet luotiin ja niiden asetukset määriteltiin, jonka jälkeen niille asennettiin käyttöjärjestelmät. Ensimmäiseksi asennettiin Windows Server 2003, johon ajettiin tarvittavat päivitykset ja konfiguroitiin palvelut sen palvelut tarkoituksenmukaiselle tasolle.

Tämän jälkeen virtuaalikone kopioitiin, jolloin saatiin samalla asennettua kolme identtistä palvelinta. Toimintaperiaate oli siis sama kuin levykuvan ottaminen fyysisestä koneesta ja sen kopiointi toiselle identtiselle laitteelle, mutta virtuaalisessa ympäristössä.

Samoin tehtiin Windows XP -virtuaalikoneiden kanssa. Ennen varsinaisen testauksen alkua yritin asentaa virtuaalikoneelle standalone-versiota levynkryptauksesta, joka johti virtuaalikoneen kaatumiseen ja korruptoitumiseen. Dokumentteja tarkemmin tutkiessa

selvisi, ettei SafeGuard-ohjelmisto tue SCSI-kiintolevyjä, ja VMWare emuloi virtuaalikiintolevyillään SCSI-väylää.

Windows XP-koneet piti tämän jälkeen exportoida siten, että SCSI-kiintolevyt muutettiin virtuaalisiksi IDE-kiintolevyiksi. Palvelinten kiintolevyjen annettiin olla SCSI-muodossa, koska niitä ei kryptattu.

6.1 Testatut käyttötapaukset

Seuraavassa esitetään kronologinen järjestys eri testausskenaariolle, joita toteutettiin työn edistyessä.

6.1.1 Asentaminen

Myös asentaminen piti testata, joten käyttöjärjestelmien asennuksen jälkeen testattiin eri SGN-komponettien asentamista. Asennus tehtiin asennusmanuaalin ohjeiden mukaisesti, eikä ongelmia esiintynyt missään vaiheessa.

6.1.2 Virtuaaliverkon toiminta

Koska SGN-ympäristö on tarkoitettu toimivaksi verkotetussa ympäristössä, piti varmistaa, että eri komponentit pystyvät kommunikoimaan keskenään. Pääasiallisena työkaluna tässä toimi Windowsin omat *netstat*- sekä *ping*-komennot. SGN-ympäristössä on joitain testaamista helpottavia työkaluja tähän. (Installation Manual, 54)

SGN Serveriltä käynnistetiin IIS Manager, jonka hakemistosta haettiin SGNSRV-palvelu. Kun palvelu oli konfiguroitu, sitä pystyi selaamaan Browse-komennolla, jonka jälkeen avautui http-protokollaa käyttävä www-sivu, jolta pystyi ajamaan CheckConnection-ohjelman. Tämä palautti XML-tiedoston, josta löytyi tiedot:

`<WebService>OK</WebService>` ja
`<DBAuth>OK</DBAuth>`.

6.1.3 Salasanan unohtumisskenaariot

IT-tuen näkökulmasta tärkeä tutkittava asia oli selviytyminen salasanan unohtumisesta. Näitä skenaarioita on käytännössä kahdenlaisia:

- salasana unohtunut täysin
- salasana vaihdettu toisella koneella.

Mikäli käyttäjä unohtaa salasanansa kokonaan, pitää aloittaa Challenge/Response, joka on kuvattu kohdassa 5.5.1. Tämän testaamisessa ei ollut ongelmia ja se onnistui oikein jokaisella kerralla. Väärinkirjoitettu challenge tai response näkyi väärinkirjoitettuna, ja pelastustyökalu osasi 10 merkin tarkkuudella näyttää, missä virhe oli.

SGN:n reaktiota testattiin, kun vastaa sen tarjoamaan kyselyyn vanhasta salasanasta väärin (pitäisi painaa Cancel). Tämän jälkeen SGN tarjosi vielä mahdollisuutta syöttää vanha salasana, kuten pitäisikin.

Mikäli salasana on vaihdettu toisella koneella, käyttäjä voi tällä uudella salasanalla kirjautua POA-ruudulla ainoastaan, mikäli salasana on vaihdettu kun a) kone on ollut yhteydessä domain-ohjaimeen ja b) salasana on synkronoitunut esim. uudelleenkirjautumisen myötä (Windows-tasolla). Tämä todettiin testien kautta. Muussa tapauksessa käyttäjän pitää kirjautua kertaalleen vanhalla salasanalla.

6.1.4 Tietokannan korruptoituminen

Hallintapuolella tehtiin testejä, joista tärkein oli SafeGuard-tietokannan korruptoituminen ja siitä selviäminen. Tietokanta korruptoitiin avaamalla se tekstieditorilla ja pyyhkimällä sieltä sattumanvaraisesti dataa pois.

Testin perusteella SGMC osasi heti kertoa tietokannan korruptiosta, ja se yritti sitä palauttaa, tosin onnistumatta. Oletettavasti pienistä muutoksista se olisi voinut selviytyä. Normaalitilanteessa tietokannasta olisi vain palautettu viimeisin varmuuskopio ja sitäkin testattiin, mutta tärkeämpi kiinnostuksen kohde oli SGN-ympäristön selviäminen tietokannan varmuuskopion hajoamisesta.

Koska asennusvaiheessa sertifikaattitiedostot (cer- ja p12-tiedostot) sekä politiikkatiedostot (XML-muodossa) olivat varmuuskopioitu, niiden avulla pystyttiin tietokanta

luomaan uudelleen. Myös uudelleenasennus onnistui niiden avulla siten, että ainoa näkyvä muutos asiakaskoneille oli yhteyden katkeaminen palvelimeen uudelleenasennuksen ajaksi.

Toisin sanoen hyvinkin katastrofaalisesta ongelmasta pystytään selviämään, mikäli alkuperäiset sertifikaatit ovat tallessa. Muuten asiakaskoneille on ajettava vähintään konfiguraatiotiedosto uudelleen. Tätä ei testattu.

6.2 Käyttökokemuksia ja ajatuksia

Virtuaalisoinnista jääneet kokemukset olivat pääosin positiivisia. Virtuaalisoinnin käyttämistä voi suositella niin testaus- ja tutkimustarkoituksiin, samoin kuin tuotantokäyttöön.

Virtuaalisointiin liittyvät ongelmat olivat melko pieniä ja lähinnä liittyivät käytettävän työaseman rajallisiin resursseihin. Esimerkiksi viiden virtuaalikoneen yhdenaikainen ajaminen vaatii erittäin paljon keskusmuistia. Jos näistä koneista yksi on palvelin 512 megatavun keskusmuistilla, ja neljä työasemia 256 megatavun muistilla, yhteensä vaaditaan 2,5 gigatavua keskusmuistia pelkästään virtuaalikoneisiin. Tämän lisäksi isäntäkoneella ajettavat muut ohjelmat vaativat muistia.

Myös kiintolevytilaa vaaditaan paljon, varsinkin levykryptausta testattaessa, sillä jokaisen virtuaalikiintolevyn koko sisältö on salattua ja siten ne vievät isäntäkoneelta koko kapasiteettinsa verran tilaa.

Kokonaisuudessaan arvioidaan virtuaalisoinnin säästäneen rahaa ja aikaa. Virtuaalisointitekniikan käyttö testauksessa on selvästi kustannustehokkaampaa kuin erillislaitteilla suoritettu testaus ja todennus. Sitä voidaan hyödyntää varsinkin, jos testaukseen käytettävä aika on rajallinen.

7 Muita kommentteja

Aikaisempi pitkä ylläpitohistoria testattujen tuotteiden parissa sekä valmiit sopimukset toimittajan kanssa helpottivat hankintaa ja tuotteeseen tutustumista. Asiakasvaatimusten täyttyminen oli tieto, joka oli erittäin tärkeä. Seuraavassa luon pikaisen katsauksen kilpaileviin tuotteisiin, joita markkinoilta löytyy.

7.1 Kilpailevia tuotteita lyhyesti

Symantec Endpoint Encryption on suora kilpailija Sophoksen SafeGuard-ratkaisulle. Molemmat yritykset, Sophos sekä Symantec, ovat laaja-alaisia tietoturvallisuuskonserneja, joilta löytyy niin salaus- kuin virustorjuntaohjelmistoja. Molemmat pyrkivät tarjoamaan ratkaisuja samoihin ongelmiin ja tarpeisiin, mutta luonnollisesti hieman erilaisessa ympäristössä.

Symantecin Endpoint Encryption tarjoaa ennen käyttöjärjestelmän käynnistystä (preboot) ilmestyvää kirjautumista, kuten Sophoksen POA. Tuettuna salaustyyppinä on mm. AES-256 ja hallintatyökalut löytyvät hieman samaan tapaan kuin SGN-ympäristössä. (Endpoint Encryption, 2010)

Jotain mahdollisia synergiaetuja saattaisi tulla, mikäli yrityksessä käytettäisi eksklusiivisesti Sophoksen tai Symantecin tuotteita aina virustorjunnasta sekä työasemien palomuureista kiintolevysalaukseen ja työasemahallintaan.

Trusted Computing Group –kollaboraation (jäseniä mm. AMD, Fujitsu, IBM, Intel, Wave Systems) kehittämä Opal-standardi edustaa hardware-pohjaista salausratkaisua. Ratkaisua tutkittiin lyhyesti Wave Systemsin kehittämällä ohjelmistolla ja Seagaten kiintolevyllä, jotka pystyi ostamaan Dellin tiettyihin konemalleihin lisäpalveluna. Hardware-pohjaisen salauksen etuna olisi käyttöjärjestelmäriippumattomuus, mutta haittapuolena mm. tämänhetkinen salaustyyppi (AES-128). Ensikosketus standardin ratkaisuun jätti kuvan hieman keskeneräisestä tuotteesta, mutta potentiaalia ratkaisulla olisi, mikäli lastentaudeista päästään eroon.
(Opal Security…, 2009; Disk-drive encryption…2009)

Hardware-salaus toimisi kiintolevyohjaimen tasolla, jossa kaikki levylle kirjoitettu data salataan automaattisesti, ja käyttöjärjestelmälle levy näkyy tavallisena SATA-kiintolevynä. Tämä näkyisi myös suorituskyvyssä, koska salaus ei kuormittaisi koneen suoritinta.

Avoimen lähdekoodin TrueCrypt-ohjelmisto edustaa ilmaista ratkaisua. TrueCrypt on saatavissa myös muille kuin Windows-käyttöjärjestelmille, mutta vain Windows-versiosta löytyy *pre-boot*-autentikointi. Ohjelmistosta ei löydy keskitettyä hallintaa eikä se varauksitta sovellu yritysten - eritoten turvallisuusteknologiayritysten - käyttöön, sillä ohjelmiston kehittäjät pyrkivät esiintymään anonyymeinä eikä ohjelmistolle ole saatavissa muun muassa virallista kaupallista tukea.
(TrueCrypt Documentation, 2010)

TrueCrypt-ohjelmisto soveltuu parhaiten kuluttajatason käyttöön, mahdollisesti pienille yrityksille, mutta kirjoittajan mielestä ei laaja-alaiseen yritysjakeluun.

8 Loppusanat

Työ sujui kohtuullisen hyvin aikataulussa ja sen tekemiseen oli tarpeeksi resursseja. Tätä kirjoittaessa ensimmäiset käyttöönottovaiheet on toteutettu tuotantoympäristössä ja lisätutkimusta on aloitettu. Muun muassa toimikortilla kirjautumisen integrointi SGN-järjestelmään ja sen testaaminen ovat käynnissä.

9 Lähteet

Administrator’s Manual, SafeGuard Enterprise version 5.50 [pdf]. 2008.

FIPS Publication 197, Specification for the Advanced Encryption Standard (AES) [pdf] [viitattu 14.03.2010]. 2001. Federal Information Processing Standards.

Endpoint Encryption-datalehti, Symantec [pdf] [viitattu: 12.10.2010]. 2010. Saatavissa; http://www.symantec.com/business/endpoint-encryption

Installation Manual, SafeGuard Enterprise version 5.50 [pdf]. 2008.

Opal Security Subsystem Class Specification FAQ, Trusted Computing Group Storage Work Group [pdf] [viitattu: 12.10.2010]. 2009. Saatavissa: http://www.trustedcomputinggroup.org/files/static_page_files/B1105605-1D09-3519-AD6FD7F6056B2309/Opal_SSC_FAQ_final_Jan_27_4_.pdf

Disk-drive encryption gets boost from Opal standards effort, Network World [verkkojulkaisu] [viitattu 12.10.2010]. Saatavissa: http://www.networkworld.com/news/2009/012909-opal.html

TrueCrypt Documentation [viitattu 12.10.2010] 2010. Saatavissa: http://www.truecrypt.org/docs/

User Manual, SafeGuard Enterprise version 5.50 [pdf]. 2008.

Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules [viitattu 14.03.2010]. 2010. Saatavissa: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Wikipedia: AES [viitattu 14.03.2010]. 2010. Saatavissa: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Workstation’s User Manual, VMWare Workstation 7.0 [pdf] [viitattu 1.10.2010]. 2010. Saatavissa: http://www.vmware.com/pdf/ws7_manual.pdf

Liitteet

Liite 1: Pseudokielinen koodi AES-salauksen purkamiseen

Pseudo Code for the Equivalent Inverse Cipher

```
EqInvCipher(byte in[4*Nb], byte out[4*Nb], word dw[Nb*(Nr+1)])
begin
      byte state[4,Nb]

      state = in

      AddRoundKey(state, dw[Nr*Nb, (Nr+1)*Nb-1])

      for round = Nr-1 step -1 downto 1
            InvSubBytes(state)
            InvShiftRows(state)
            InvMixColumns(state)
            AddRoundKey(state, dw[round*Nb, (round+1)*Nb-1])
      end for

      InvSubBytes(state)
      InvShiftRows(state)
      AddRoundKey(state, dw[0, Nb-1])
      out = state
end
```

For the Equivalent Inverse Cipher, the following pseudo code is added at the end of the Key Expansion routine (Sec. 5.2):

```
      for i = 0 step 1 to (Nr+1)*Nb-1
            dw[i] = w[i]
      end for

      for round = 1 step 1 to Nr-1
            InvMixColumns(dw[round*Nb, (round+1)*Nb-1]) //note change
      of type
      end for
```

Note that, since InvMixColumns operates on a two-dimensional array of bytes while the Round Keys are held in an array of words, the call to InvMixColumns in this code sequence involves a change of type (i.e. the input to InvMixColumns() is normally the State array, which is considered to be a two-dimensional array of bytes, whereas the input here is a Round Key computed as a one-dimensional array of words).

Lähde: FIPS Publication 197, Specification for the Advanced Encryption Standard (AES) [pdf]. 2001. Federal Information Processing Standards.

Saatavilla: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf