KYMENLAAKSON AMMATTIKORKEAKOULU
Elektroniikan koulutusohjelma / tietoliikennetekniikka

Juhamatti Pienmunne
Jari Paulow

KERTAKÄYTTÖISET SALASANAT TIETOVERKOISSA

Opinnäytetyö 2009

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU
Elektroniikan koulutusohjelma

PIENMUNNE, JUHAMATTI
PAULOW, JARI

Kertakäyttöiset salasanat tietoverkoissa

Insinöörityö 38 sivua + 7 liitesivua
Työn ohjaaja Yliopettaja Martti Kettunen
Toimeksiantaja Optimiratkaisut Oy
Joulukuu 2009
Avainsanat one time password, tietoturva, salaus, todennus

Opinnäytetyössä tarkastellaan ja tutkitaan RSA SecurID -tuoteperhettä ja kertakäyttösalasanajärjestelmän toimintaa tietoliikennelaboratorio-olosuhteissa.

RSA SecurID on julkiseen avaimeen perustuva salausjärjestelmä, jossa RSA SecurID -tokenien ja RSA SecurID -ohjelmiston välille luodaan turvattu yhteys. Toimeksiantajan pyynnöstä opinnäytetyössä keskityttiin järjestelmän asennukseen ja testaamiseen, jotta RSA SecurID:n toiminnasta saadaan riittävästi käytännön tietoa ja kokemusta.

Opinnäytetyössä luotiin toimiva testiverkko Kymenlaakson ammattikorkeakoulun tietoliikennelaboratorioon. Testiverkko sisälsi Windows Server 2003 -palvelimen johon oli asennettu RSA Authentication Manager 7.1, Ciscon 2800-sarjan reitittimen sekä testikäyttäjien Windows XP -koneita. Yhteys palvelimen ja testikäyttäjien välille luotiin käyttämällä VPN-yhteyttä.

Opinnäytetyössä onnistuttiin tarkastelemaan RSA SecurID:n toimivuutta ja luomaan toimiva ja turvallinen todennettu yhteys. Toimiva RSA SecurID -todennuspalvelin luotiin ja palvelimen tiedot saatiin vain niiden käyttäjien käyttöön, joilla on oikeudet tarkastella palvelimen tietoja.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU
University of Applied Sciences

Electronics

PIENMUNNE, JUHAMATTI	One-Time Passwords in Networking
PAULOW, JARI	
Bachelor's Thesis	38 pages + 7 pages of appendices
Supervisor	Martti Kettunen, Principal Lecturer
Commissioned by	Optimiratkaisut Oy
December 2009	
Keywords	one-time password, otp, encryption

This paper examines the RSA SecurID product family and the performance of a disposable password in a data communications laboratory environment.

RSA SecurID is a public-key-based encryption system that creates a secure connection between RSA SecurID tokens and RSA SecurID software. By the request of Optimiratkaisut Oy, the paper focuses on the installation and testing of the system with the purpose of gathering sufficient practical information and experience.

A functional test network was created at the data communications laboratory of Kymenlaakso University of Applied Sciences. The test network consisted of a Windows Server 2003 with RSA Authentication Manager 7.1 installed, a Cisco 2800 series router, and several test user computers with Windows XP. The server and the test users were connected by a VPN.

An authenticated and secure connection between the test users and the server was established and the performance of the RSA SecurID was documented. A working RSA SecurID authentication server was created, enabling only users with proper permission to access information on the server.

SISÄLLYS

TIIVISTELMÄ

ABSTRACT

TERMIT JA LYHENTEET

1 JOHDANTO 8

2 TIETOTURVA TIETOLIIKENTEESSÄ 9

2.1 Tietoturva 9

2.2 Salasanojen vahvuudesta 9

2.3 Tietoturvapolitiikka 10

2.4 Tietoturvallisuuden määritelmät 11

2.5 Todentaminen 13

2.6 Salausprotokollat 13

2.6.1 SSH-protokolla 14

2.6.2 SSL/TLS-protokolla 15

2.6.3 IPSec 16

2.6.4 RSA:han pohjautuvia salaustekniikoita 17

2.7 Sertifikaatit 17

2.8 Allekirjoitus 19

3 TODENTAMISKOKONAISUUDEN LUOMINEN 19

3.1 Todentamisympäristö 20

3.2 RSA Authentication Managerin asentaminen 21

3.3 Cisco VPN Clientin asennus 23

3.4 Kytkentä ja reitittimen konfigurointi 25

4 RSA AUTHENTICATION MANAGER 27

4.1 RSA Security -konsoli 27

4.2 RSA AM -palvelimen hallinnointi 27

5 TODENNUSTAPOJA 33

5.1 Laitteisto-tokenit 33

5.2 Ohjelmisto-tokenit 33

5.3 Hybriditodennus 34

5.4 On-demand-todennus 35

5.5 OTP token -työkalurivi, RSA SecurID Toolbar 35

6 YHTEENVETO 36

LÄHTEET 37

LIITTEET

Liite 1. Laitteisto-tokenit

Liite 2. Ohjelmisto-tokenit

Liite 3. Hybridi-tokenit

Liite 4. On-demand-todennus

Liite 5. Näytöllinen kortti

TERMIT JA LYHENTEET

CISCO IOS	Internetwork Operating System, komentorivipohjainen käyttöjärjestelmä Ciscon kytkimille ja reitittimille.
CISCO VPN CLIENT	Mahdollistaa VPN-tunnelin luomisen päätekoneelta.
FQDN	Fully Qualified Domain Name
IP	Internet Protocol
IPsec	Internet Protocol Security, protokolla käsittää salauksen, osapuolten todennuksen ja tiedon eheyden varmistamisen IP-verkoissa.
IPv4	IP-protokollan 4. versio.
IPv6	IP-protokollan 6. versio.
OTP	One-Time Password, kertakäyttösalasana.
KEYLOGGER	Salasanoihin kohdistuva hyökkäys.
PIN	Personal Identification Number.
RADIUS	Remote Authentication Dial-In User Service, todennusprotokolla.
RSA	Julkisen avaimen salausalgoritmi.
RSA AM	RSA Authentication Manager, todennuksenhallintaohjelmisto.
RSAES-OAEP	RSA Encryption Scheme - Optimal Asymmetric Encrytion Padding, salaustekniikka.
RSASSA-PSS	RSA Signature Scheme with Appendix – Probabi- listic Signature Scheme, salaustekniikka.
SSH	Secure Shell, salausprotokolla.

SSL	Secure Sockets Layer, salausprotokolla.
TLS	Transport Layer Security, salausprotokolla.
TOKEN	Laitevarmistusavain.
TWO-FACTOR AUTHENTICATION	Kahden tekijän todennustapa, vahva todennus.
VPN	Virtual Private Network, mahdollistaa etäyhteyden kahden verkon tai käyttäjän välille.

1 JOHDANTO

Optimiratkaisut Oy antoi tehtäväksi tutkia RSA SecurID -tuoteperhettä ja luoda todennuspalvelimen tietoliikennelaboratorio-olosuhteissa. Tehtävä kuulosti mielenkiintoiselta, ajankohtaiselta sekä riittävän haastavalta.

Tavoiteltu toiminnallisuus oli muodostaa yhteys Ciscon IPsec Clientillä Ciscon VPN Gatewaylle, joka konfiguroitiin Ciscon IOS-versiolle 12.4(13r)T. Käyttäjätunnustodennus oli tarkoitus hoitaa RADIUS-protokollalla RSA-palvelimen ja Cisco IOS:n välillä. Opinnäytetyössä pyrittiin hyödyntämään RSA:n omaa RADIUS-komponettia ja käyttäjätietokantaa.

Tietoturva on nykymaailmassa erittäin tärkeä elementti ja tietoturvan merkitys korostuu ihmisten mobiililaitteiden määrän kasvaessa. Ihmisten tulee päästä käsiksi suojattuihin tietoihinsa missä vain ja mihin kellonaikaan tahansa. Tietoturva koostuu useasta eri osa-alueesta, mutta tässä opinnäytetyössä on keskitytty todennukseen eli käyttäjän tunnistamiseen.

Tämän opinnäytetyön käytännön osiossa on tarkoitus luoda toimiva todennuspalvelu, johon otetaan yhteys VPN:n välityksellä. Todennus suoritetaan käyttämällä RSA SecurID -tuoteperhettä.

2 TIETOTURVA TIETOLIIKENTEESSÄ

2.1 Tietoturva

Nykymaailmassa tärkeät tiedot tulisi suojata hyvin. Suojattuihin tietoihin päästään käsiksi tietoturvallisella VPN-etäyhteydellä, jota voidaan käyttää lähes millä tahansa mobiililaitteella, älypuhelimesta kannettavaan tietokoneeseen.

Todennus on iso osa nykypäivän tietoturvaa. Todennuksella tarkoitetaan käyttäjän tunnistamista, ja se määrittelee sen, oletko se henkilö, kuka väität olevasi. Todennus on yleisesti yhdistetty kirjautumiseen salasanalla ja salasanan tietäminen on vakuus henkilön todentamisesta. (Authentication. Searchsecurity.com, 2007.)

2.2 Salasanojen vahvuudesta

Salasanan olisi hyvä olla parinkymmenen merkin pituinen ja sen tulisi koostua satunnaisista merkeistä, eli pelkkiä selkokielisiä sanoja tulisi välttää. Lisäksi samaa salasanaa ei tulisi käyttää useammassa kuin yhdessä paikassa ja se olisi hyvä vaihtaa säännöllisesti, jopa kerran kuukaudessa. Salasana ei saisi olla mitään, mikä liittyy henkilökohtaiseen elämään, sillä ne ovat helposti johdettavissa. Lapsen, kumppanin tai lemmikin nimet tai syntymäajat ovat kaikkein yleisimpiä salasanoja tai tunnuksia. Tämän tapaisia salasanoja myös kokeillaan ensimmäisenä. (Suoranta 2009, 76; Järvinen 2002, 340-342.)

Tietoturvan näkökulmasta edelliset neuvot ovat varsin hyviä ja toimivia, mutta harvat niitä noudattavat. Useimmat eivät halua opetella ulkoa useita, jopa kymmeniä, salasanoja vuosittain, eikä se ole tarkoituskaan. (Suoranta 2009, 76.)

Salasanan on oltava mahdollisimman monimutkainen, jotta se olisi turvassa erilaisilta hyökkäyksiltä. Hyökkäyksiä on monenlaisia ja kuten tietokoneviruksetkin, toiset niistä ovat haitallisempia kuin toiset. Keylogger-hyökkäys on yksi vaarallisimmista salasanoihin kohdistuvista riskitekijöistä. Keylogger-hyökkäykset ovat huomaamattomia tietokoneohjelmia, jotka tallentavat kaikki

näppäinpainallukset ja lähettävät ne eteenpäin. Hyökkääjä ei tarvitse montakaan minuuttia tällaisen ohjelman asentamiseen, joten kaikki julkiset Internetin käytön tarjoavat paikat, kuten kirjastot ja nettikahvilat, ovat erittäin alttiita Keylogger-hyökkäyksille. Tästä syystä on oltava varma käytetyn päätteen tietoturvatasosta. Päätteissä, joihin kirjaudutaan omilla tunnuksilla sisään, tämä uhka on minimoitu. Esimerkiksi korkeakoulujen päätteet ovat hyvä esimerkki tällaisista, sillä näiden koneiden ylläpitäjällä on niistä tarkempi kontrolli. (Suoranta 2009, 77.)

Myös tuntemattomien wlan-verkkojen käytössä on oltava varuillaan, sillä joku saattaa yrittää siepata web-palvelujen salasanoja. Tällaista ongelmaa ei ole, jos sivusto on suojattu ssl-salauksella. (Suoranta 2009, 77; Järvinen 2002, 342.)

Vaikka useasti kielletään omien salasanojen tallennus tai listaus muualle kuin omaan muistiin, on sekin mahdollista, jos sen tekee oikein. Ihan normaali tekstitiedosto on käypä vaihtoehto, jos sen tallentaa salausohjelmiston luomalle virtuaaliasemalle. Tällaisten tiedostojen käsittelyssä tulee olla varovainen, sillä monet ohjelmat luovat tilapäistiedostoja tietokoneen muistiin ja ne unohtuvat sinne helposti. (Suoranta 2009, 77.)

Salasanojen tallentamista web-selaimeen kannattaa välttää, vaikka se kuinka helpottaisi ja nopeuttaisi omia toimia. Osaavalta kaverilta salasanojen löytäminen vie aikaa muutaman napin painalluksen verran. Oma tietokone on asia erikseen, mutta julkisilla päätteillä tätä tulisi välttää. (Suoranta 2009, 77.)

Kertakäyttöiset salasanat ovat erittäin tietoturvallisia, eikä käyttäjän tarvitse niitä erikseen muistella. Tässä opinnäytetyössä laitevarmistusavain, token, generoi kertakäyttöisen salasanan ja oikeastaan ainut asia, joka käyttäjän tarvitsee muistaa, on kantaa tokenia mukanaan.

2.3 Tietoturvapolitiikka

Suunniteltaessa yrityksen tai organisaation tietoturva-asioita on tavoitteena luoda toimiva tietoturvapolitiikka. Organisaation ylin johto on päättämässä, mil-

lainen tietoturvataso nähdään tarpeelliseksi ja halutaan saavuttaa. Tietoturvapolitiikan on tarkoitus kuvata yleisesti organisaation liiketoimintaprosessien tarvitsemia turvaamisasteita. Tietoturvapolitiikkaan kuuluvat tietoturvallisuuteen liittyvät hallinnolliset kysymykset ja menetelmät, jotka selvittävät, miten haluttuun tietoturvatasoon voidaan pyrkiä. (Hakala, Vainio & Vuorinen 2006, 7.)

Tietoturvapolitiikka laaditaan kirjallisesti ja sen tarkoitus on toimia noin 5 tai noin 10 vuotta eli keskipitkän tai pitkän aikavälin mukaisesti. Se toimii ohjeena tietojärjestelmistä vastaaville henkilöille ja eri liiketoimintaprosessien esimiehille. Pitkästä aikavälistä johtuen tekniset tietoturvaan liittyvät yksityiskohdat on jätetty pois. Tietoturvapolitiikka tarkistetaan vuosittain, jotta se vastaisi yrityksen tai organisaation sen hetkistä toimintaa. (Hakala, Vainio & Vuorinen 2006, 7.)

Jokaiselle organisaation liiketoimintaprosessille voidaan määritellä oma tietoturvaluokitus, käytäntö. Käytännössä se tarkoittaa esim. sitä, että eri liiketoimintaprosesseilta voidaan evätä pääsy muihin paitsi omaan liiketoiminnan osa-alueeseen. (Hakala, Vainio & Vuorinen 2006, 7.)

2.4 Tietoturvallisuuden määritelmät

Klassisesti tietoturvallisuus koostuu kolmesta osatekijästä, jotka ovat luottamuksellisuus, käytettävyys ja eheys. Luottamuksellisuus kertoo tietojärjestelmän tietojen olevan vain luotettujen ja oikeutettujen henkilöiden käytettävissä. Tämän ylläpitoon auttaa henkilöiden omat käyttäjätunnukset sekä salasanat. Näin arvokas ja arkaluonteinen materiaali saadaan helposti suojattua. (Hakala, Vainio & Vuorinen 2006, 4.)

Käytettävyys kertoo tietokannan olevan oikeassa muodossa sekä helposti ja nopeasti käytettävissä. Käytettävyys saadaan hyväksi oikeanlaisilla tieto- ja tietoliikennejärjestelmien laitevalinnoilla. Myös laitteiden ohjelmistojen on oltava riittävät tarvittavan tiedon käsittelyyn. (Hakala, Vainio & Vuorinen 2006, 4.)

Eheydellä tarkoitetaan tietokannan virheettömyyttä. Tietokannan materiaalin on oltava luotettavaa ja tietojen on pidettävä paikkansa. Tietojen sisällössä ei saa olla tahallisia tai tahattomia virheitä. Eheyttä pyritään ylläpitämään suurimmaksi osaksi ohjelmoinnin avulla. Useimmat salakirjoitusmenetelmät soveltuvat myös ylläpitoon. Tietoliikenneratkaisuiden protokollissa ja laitteissa käytetään virheen tunnistus- ja korjausmenetelmiä. (Hakala, Vainio & Vuorinen 2006, 4-5.)

Klassisen tietoturvallisuuden määritelmää pidetään nykyisin riittämättömänä, sillä tiedon tuottajan ja tiedon omistajan henkilöllisyys jää taka-alalle. Huomiotta jää myös laitteiston ja tietoliikennejärjestelmien arvo. Laajennettu tietoturvallisuuden määritelmä sisältää viisi osatekijää, joista kolme ensimmäistä ovat tutut klassisesta määritelmästä. Kaksi jäljelle jäävää ovat kiistämättömyys ja pääsynvalvonta. (Hakala, Vainio & Vuorinen 2006, 5.)

Tietojärjestelmän kykyä tunnistaa ja tallentaa järjestelmää käyttävän henkilön tiedot kuvataan kiistämättömyydellä. Kiistämättömyydellä varmistetaan tiedon alkuperä ja estetään tietokannassa olevien tietojen luvaton käyttö. Biometriset tunnisteet tai salausmenetelmiin liittyvät tunnistusmekanismit ovat hyviä työkaluja kiistämättömyyden ylläpitoon. Älykortit ja muut pienet mukana kuljetettavat laitteet ovat yleisimpiä salaustekniikoita hyödyntäviä käyttäjätunnistukseen tarkoitettuja laitteita. Näihin laitteisiin on tallennettu käyttäjän henkilötiedot ja yleensä vain määrätyn ajan voimassa oleva käyttölupa, sertifikaatti. (Hakala, Vainio & Vuorinen 2006, 5.)

Pääsynvalvonnalla rajoitetaan tieto- ja tietoliikennejärjestelmien käyttöä. Organisaatio haluaa usein rajoittaa tai kokonaan estää laitteiden tai tietoliikenneyhteyksien luvattoman käytön. Luvaton käyttö kuormittaa laitteistoa ja yhteyksiä turhaan, mikä heikentää tietokannan käytettävyyttä. Tätä kautta myös erilaiset haittaohjelmat voivat päätyä ja levitä koko organisaation verkkoon. Tämä johtaa taas ongelmiin muissa tietoturvallisuuden osatekijöissä. (Hakala, Vainio & Vuorinen 2006, 5-6.)

2.5 Todentaminen

Todennuksessa tarkastetaan, että tietokantaan kirjautuva on se, kuka väittää olevansa. Kirjautuvan ei tarvitse olla ihminen, vaan se voi yhtä hyvin olla myös laite, nettipalvelu tai esimerkiksi tiedon alkuperä. Kirjautuminen suoritetaan yleisesti ottaen tunnuksella ja salasanalla, mutta näiden lisäksi voi olla älykortti tai biometrinen tunnistus. (Hakala, Vainio & Vuorinen 2006, 124; Järvinen 2002, 25.)

Todennus on hyvin arkipäiväinen ilmiö, vaikka se teknisesti onkin melko hankala. Todennamme tuttavamme ulkonäön perusteella tai puhelun tullessa todennamme hänet äänen perusteella. Sähköpostiviesteissä todennamme henkilöt sähköpostiosoitteen perusteella. Tämä on kylläkin melko turvatonta, sillä osoitteiden väärentäminen on helppoa. Myös pankkiautomaateilla piilee omat riskinsä, mutta silti me lähes päivittäin työnnämme pankkikortin automaattiin olettaen sen olevan aito. Pankkiautomaatteihin on voitu kuitenkin asentaa ylimääräinen kortinlukija, joka kopio tunnusluvun lisäksi kortin magneettiraidan. (Järvinen 2002, 25.)

Todennuksen lähtökohtana on se, että tietokantaan annetun tiedon oikeellisuus tarkistetaan. Tietoturvan näkökulmasta, tarkistus olisi tehtävä siten, ettei tieto paljastu. Tieto voi olla esimerkiksi henkilön itse määrittämät tunnus ja salasana tai hänelle luovutetut tunnukset. Lähtökohtaisesti salasanan tietäminen riittää henkilön todentamiseen. Salasanojen varastaminen tai unohtaminen on tällaisten järjestelmien heikkous. (Authentication, SearchSecurity.com 2009; Järvinen 2002, 27.)

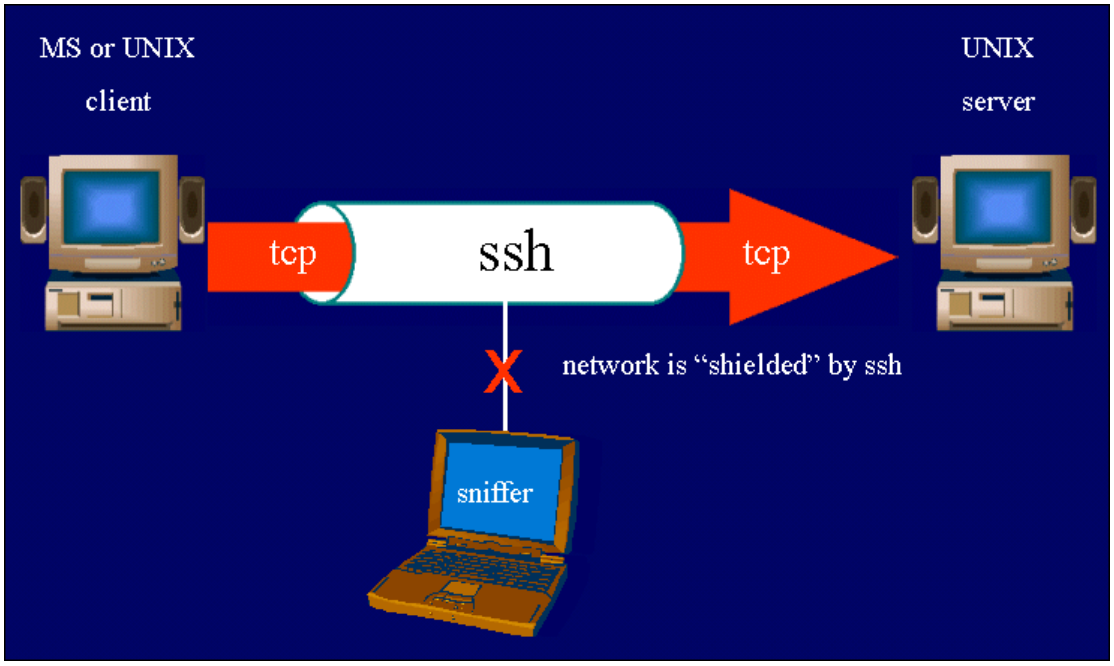
2.6 Salausprotokollat

Salausprotokollat salaavat lähetetyn viestin ja niitä voidaan hyödyntää salatuissa yhteyksissä. Niiden tehtävä on varmistaa, ettei lähetetty viesti muutu matkalla lähettäjältä vastaanottajalle. Lisäksi salausprotokollat salakirjoittavat lähetettyjen viestien sisällöt ja ne käyttävät usein tunnistus-, avaimensopimis- ja/tai avaintenjakoprotokollia. (Hakala, Vainio & Vuorinen 2006, 388.)

Oli viestin sisältö arkaluonteista tai ei, on salausprotokollaa hyvä käyttää, sillä se salaa myös käytetyn salasanan. Näin murtautujankin on vaikea erottaa arkaluonteinen materiaali normaalista ihmisten kanssakäymisestä. Salausprotokollaa on molempien osapuolien osattava käyttää tai siitä ei ole mitään hyötyä. Se voi toimia itsenäisesti omana läpinäkyvänä kerroksenaan, eli piilossa ohjelmilta, tai käyttöön voidaan vaatia omia ohjelmia. (Hakala, Vainio & Vuorinen 2006, 388.)

2.6.1 SSH-protokolla

SSH eli Secure Shell -järjestelmää käytetään turvalliseen tiedonsiirtoon. SSH:lla luodaan yleensä etäyhteys SSH-asiakasohjelman ja SSH-palvelimen välille, mikä luo mahdollisuuden käyttää toista konetta merkkipohjaisen konsolin kautta. SSH:n avulla voidaan tunneloida myös mikä tahansa muu yhteys, kuten HTTP- ja FTP-liikenne. SSH:ta suositellaan käytettäväksi, jos yhteyden suojaustaso on matalalla. SSH-protokolla toimii TCP-protokollan päällä sovelluskerroksessa, ja sen toiminta jakautuu kolmeen eri kerrokseen: siirto-, käyttäjäntunnistus- ja yhteyskerrokseen. (Hakala, Vainio & Vuorinen 2006, 388-389.)



Kuva 1. SSH-tunnelointiesimerkki. (University Of Washington 2009.)

Suojatussa liikenteessä on tärkeää, että mahdollisimman monia erityyppisiä algoritmeja käytetään mahdollisimman monissa paikoissa. Tämän tyyppinen ratkaisu turvaa muut yhteydet, sillä jos yksi saadaan murrettua, samaa keinoa ei voi käyttää muiden yhteyksien murtamiseen. (Hakala, Vainio & Vuorinen 2006, 388.)

2.6.2 SSL/TLS-protokolla

SSL-salausprotokolla toimii muuten lähes samalla tavalla kuin SSH-protokolla, mutta SSL toimii läpinäkyvänä kerroksena, kun SSH toimii sovelluskerroksessa. SSL käyttää yhteyden turvaamiseen luottamuksellisuutta, eheyttä ja osapuolten todennusta. Osapuolten todennusta voidaan käyttää sekä palvelimen aitouden varmistamiseen että käyttäjän todennukseen. (Hakala, Vainio & Vuorinen 2006, 390; Järvinen 2002, 376.)

SSL:n toiminta on jaettu kahteen eri protokollaan: Handshake ja Record Layer. Handshake-protokollalla työasemalta lähetetään palvelimelle viesti, joka kertoo työaseman osaamat salakirjoitusmenetelmät. Näistä palvelin valitsee käytettävän menetelmän ja lähettää siitä tiedon työasemalle. Lopuksi sovitaan käytettävästä istuntoavaimesta aikaisemmin sovitulla salakirjoitusmenetelmällä. Tästä eteenpäin kaikki viestit ovat salattuja, eikä sovittuja menetelmiä voida enää yhteyden aikana muuttaa. (Hakala, Vainio & Vuorinen 2006, 390-391.)

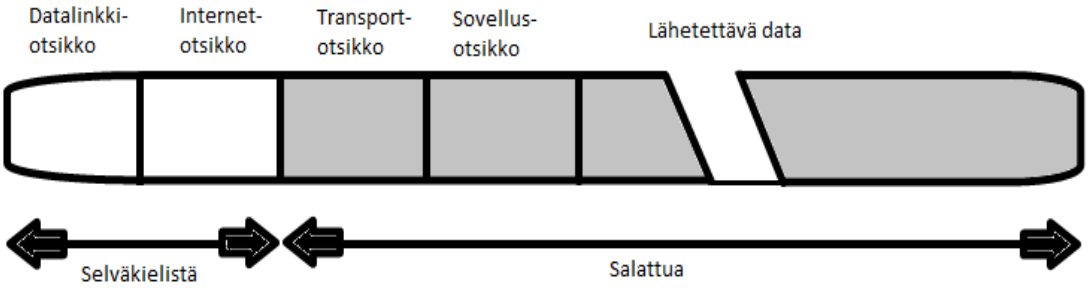
Viestit osioidaan, pakataan, salakirjoitetaan ja eheys varmistetaan Record Layer -protokollalla, joka toimii TCP-protokollan päällä. Salakirjoituksessa käytetään salaisen avaimen menetelmiä ja viestien eheys varmistetaan tiivistefunktioiden avulla. SSL käyttää hälytysviestejä toiminnassaan, jos yhteydessä tapahtuu jotakin odottamatonta. Odottamatonta voi olla esimerkiksi vanhentunut sertifikaatti tai viestin muuttuminen matkalla. Yhteyden kohtalo riippuu virheen luonteesta, ja radikaalein ratkaisu on yhteyden katkaisu. (Hakala, Vainio & Vuorinen 2006, 391.)

TLS on SSL:n korvaaja ja se pohjautuu hyvin pitkälti SSL-salausprotokollaan. Näiden kahden protokollan erot ovat lähes olemattomat, mutta ne ovat silti eri

standardit. TLS käyttää vahvempia salausalgoritmeja kuin SSL, ja sitä on mahdollista käyttää eri porteissa. Hyvin usein käytetyt ohjelmat tukevat molempia protokollia. (Knowledge Base, Indiana University 2009; Transport Layer Security, Wikipedia-artikkeli 2009.)

2.6.3 IPSec

IP Security mahdollistaa viestien eheyden ja lähettäjän varmistamisen, viestien toistamisen estämisen ja viestien salakirjoittamisen. IPSec:lla pystytään turvaamaan mikä tahansa IP-protokollan päällä toimiva protokolla. Se sisältyy IPv6-protokollaan, mutta se voidaan huomioida myös IPv4-protokollassa. IPSec:lla on kaksi eri toimintatapaa: kuljetusmoodi ja tunnelimoodi. (Hakala, Vainio & Vuorinen 2006, 393; Kerttula 1999, 221.)



Kuva 2. IPSec-salauksen paketin perusformaatti (Kerttula 1999, 220.)

Kuljetusmoodissa kahden osapuolen välinen yhteys turvataan sekä siinä suojataan lähetettävä viesti. Lähetetyn viestin eheys myös tarkistetaan ja varmistetaan, ettei viesti ole muuttunut matkalla. Kuljetusmoodia käytettäessä IP-otsikkoa ei voida salakirjoittaa. (Hakala, Vainio & Vuorinen 2006, 393.)

Tunnelimoodissa luodaan kahden osapuolen välille suojattu tunneli, millä saadaan suojattua muiden yhteyksien viestejä. Kaikki yhteydellä lähetettävät viestit kootaan yhdeksi uudeksi viestiksi ja sen sisältö suojataan asetuksiin määrätyllä tavalla. Saatu uusi viesti lähetetään toiselle osapuolelle tai se voidaan myös välittää eteenpäin. Uudesta viestistä lopullinen vastaanottaja osaa purkaa alkuperäisen viestin. Tunnelimoodissa koko viesti voidaan salakirjoittaa, joten kaapatusta viestistä paljastuu vain IP-otsikkotiedot ja viestin lähde- ja kohdeosoitteet pysyvät salattuina. (Hakala, Vainio & Vuorinen 2006, 393.)

IPSec-yhteyden osapuolina voivat toimia tietokoneet, reitittimet tai palomuurit. Reitittimet ja palomuurit toimivat yhdyskäytävinä, jotka käyttävät aina tunnelimoodia viestien välittämiseen. Tietokoneissa voi käyttää molempia toimintatapoja. Myös turvallisuuden taso voidaan merkitä viestiin IPSec:n avulla. Turvallisuuden on pysyttävä vähintään merkityllä tasolla, jotta viestiä voidaan verkossa siirtää.(Hakala, Vainio & Vuorinen 2006, 393-394.)

2.6.4 RSA:han pohjautuvia salaustekniikoita

On olemassa useita erilaisia RSA:han perustuvia salaustekniikoita ja protokollia. RSA Laboratoriot suosittelevat RSAES-OAEP-salausta ja RSASSA-PSS-allekirjoitusta uusiin sovelluksiin. (RSA Laboratories. RSA Algorithm, RSA.com 2009)

RSAES on julkiseen avaimeen perustuva salausjärjestelmä, jossa OAEP-metodi yhdistetään RSA-algoritmiin. OAEP:n kehittivät Mihir Bellare ja Phillip Rogaway Don B. Johnsonin ja Stephen M. Mátyásin avustuksella. (RSA Laboratories. RSA Algorithm, RSA.com 2009)

RSASSA-PSS on epäsymmetrinen allekirjoitusjärjestelmä, joka saadaan yhdistämällä RSA-algoritmi PPS-koodausmenetelmään. PPS-koodausmenetelmän keksivät Mihir Bellare ja Phillip Rogaway. (RSA Laboratories. RSA Algorithm, RSA.com 2009)

2.7 Sertifikaatit

Sertifikaatit ovat digitaalisia todistuksia, jotka sitovat julkisen avaimen, tiettyyn yksilöön tai yhteisöön. Sertifikaattien avulla voidaan tarkistaa, että tietty julkinen avain varmasti kuuluu tietylle henkilölle. Sertifikaatit auttavat estämään tapauksia, joissa henkilö esittää olevansa joku muu kuin todella on. Joissain tapauksissa voi olla tarpeellista luoda ketju sertifikaatteja, joista jokainen todistaa edellisen sertifikaatin. Sertifikaattiketjua jatketaan, kunnes osapuolet luottavat toistensa henkilöllisyyksiin. (RSA Laboratories. What are certificates?, RSA.com 2009)

Yksinkertaisimmassa muodossa sertifikaatit sisältävät julkisen avaimen ja nimen. Usein sertifikaatti sisältää myös viimeisen voimassaolopäivän, sertifikaatin myöntäneen viranomaisen nimen, sarjanumeron ja mahdollisesti muita tietoja. Mikä tärkeintä, sertifikaatti sisältää sertifikaatin myöntäjän digitaalisen allekirjoituksen. Laajimmin hyväksytty sertifikaattien muoto on määritelty kansainvälisessä ITU-T X.509 -standardissa. Kyseiset sertifikaatit ovat luettavissa ja kirjoitettavissa millä tahansa ohjelmalla, joka noudattaa X.509-standardia. (RSA Laboratories. What are certificates?, RSA.com 2009)

SSL-salauskäytännön mukaisia suojattuja internet-yhteyksiä käytettäessä on kaikilla palvelimilla oma sertifikaattinsa. Sertifikaatista ilmenee palvelimen nimi ja muita tietoja. Sertifikaatin avulla varmistetaan, että palvelin on se, mikä väittää olevansa. SSL-sertifikaatissa sekä asiakas- että maksutiedot salataan 128-bittisellä tai 256-bittisellä salauksella verkkomaksun turvaamiseksi. SSL-palvelimen suojatun yhteyden huomaa, kun internet-osoitteen alku ”http://” korvautuu aluksi ”https:// ”. (Tietotekniikkaosasto, Helsingin yliopisto 2009.)

Digitaalisen sertifikaatin muita nimityksiä ovat julkisen avaimen sertifikaatti ja identiteettisertifikaatti. Identiteettisertifikaatilla varmistetaan julkisten avainten salaustekniikassa, että julkisen avaimen omistaja on sama kuin se, joka lähettää avaimen mukana salattuja tai digitaalisesti allekirjoitettuja tietoja. (Symantec, Sanasto 2009; Symantec, Tietoturvainfo 2009.)

Digitaalinen sertifikaatti on sähköinen asiakirja, jolla varmistetaan henkilöllisyys käyttäen hyvin suojattuja salaustunnuksia. Digitaalista sertifikaattia käytetään esimerkiksi suojatuissa verkkokauppaostoksissa. Käyttäjän halutessa maksaa ostoksensa vaihtavat käyttäjän ja kaupan tietokoneet digitaalisia sertifikaatteja keskenään. (Symantec, Sanasto 2009; Symantec, Tietoturvainfo 2009.)

Sertifikaatti sisältää julkisen avaimen ja digitaalisen allekirjoituksen. Niiden avulla varmistetaan sertifikaatin aitous ja että lähettäjä on avaimen oikea omistaja. Vaihtamalla sertifikaatteja on mahdollista muodostaa suojattu Internet-yhteys ostajan ja kaupan välille. Sertifiointiyritykset, kuten VeriSign, hank-

kii yksityiskohtaisia tietoja verkkokaupan liiketoiminnasta ja voi myöntää kaupalle sertifikaatin. (Symantec, Sanasto 2009; Symantec, Tietoturvainfo 2009.)

2.8 Allekirjoitus

RSA:n algoritmia käytetään myös allekirjoittamiseen. Allekirjoituksessa viestistä lasketaan tiiviste tiivistefunktion avulla. Laskettu tiiviste salataan yksityisellä allekirjoitusavaimella. Tarkistettaessa allekirjoitus puretaan ensin tiivisteen salaus ja sen jälkeen lasketaan viestistä uusi tiiviste. Jos uusi tiiviste ja alkuperäinen tiiviste ovat samoja, ei viesti ole muuttunut matkalla ja viestin lähettäjä on oikea. (RSA, Wikipedia-artikkeli 2009.)

Digitaalisen allekirjoituksen periaate on sama kuin tavallisen käsin kirjoitetun allekirjoituksen, eli vahvistaa henkilön henkilöllisyys. Dokumentin digitaalinen allekirjoitus perustuu sekä dokumentin tietoihin että lähettäjän henkilökohtaiseen avaimeen. (RSA Laboratories, What is a digital signature and what is authentication? 2009.)

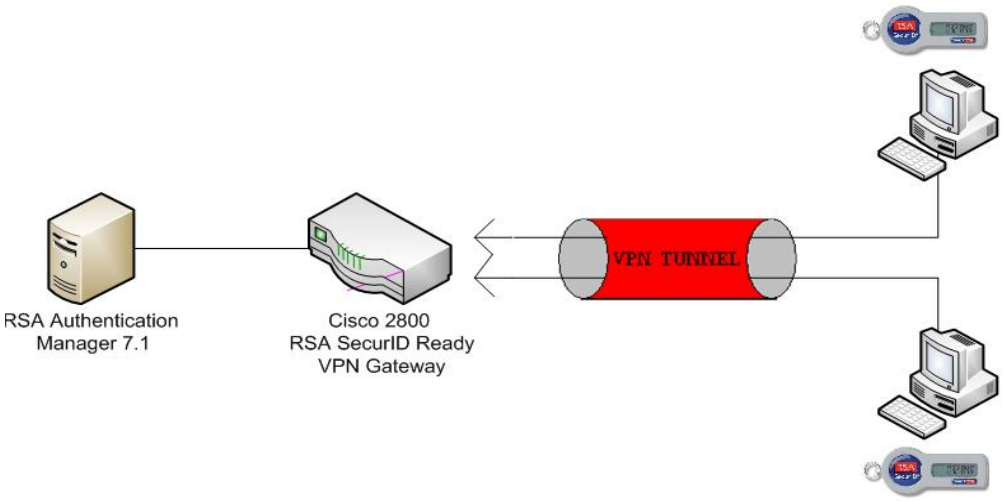
Sekä digitaalinen allekirjoitus että käsin kirjoitettu allekirjoitus luottavat siihen, että on hyvin epätodennäköistä, että kahdella ihmisellä on täysin samanlainen allekirjoitus. Julkisen avaimen salausta käytetään digitaalisen allekirjoituksen luomiseen liittämällä jotakin ainutlaatuista jokaiselle henkilölle, kuten esimerkiksi salasana tai PIN-koodi. Kun julkisen avaimen salausta käytetään viestin salaamiseen, viestin lähettäjä salaa viestin vastaanottajan julkisella avaimella. Kun julkisen avaimen salausta käytetään digitaalisen allekirjoituksen laskemiseen, lähettäjä salaa dokumentin digitaalisen sormenjäljen omalla yksityisellä avaimellaan. Jokainen, jolla on pääsy allekirjoittajan julkiseen avaimeen, voi vahvistaa allekirjoituksen. (RSA Laboratories, What is a digital signature and what is authentication? 2009.)

3 TODENTAMISKOKONAISUUDEN LUOMINEN

Tässä luvussa esitellään todentamiskokonaisuutta ja siihen kuuluvia osa-alueita, kuten tärkeimpien ohjelmistojen asentamista sekä laitteiston kytkemistä ja konfigurointia.

3.1 Todentamisympäristö

Tämän opinnäytetyön käytännön osuuden tärkein osa-alue oli saattaa koulun tietoliikennelaboratorion laitteistolla yksinkertainen todennuspalvelin toimintaan. Palvelin koostuu Windows Server 2003 -käyttöjärjestelmästä, RSA Authentication Manager 7.1 -todennuksenhallintaohjelmistosta, Ciscon 2800-sarjan reitittimestä sekä testikäyttäjistä (Kuva 3).



Kuva 3. Todennusympäristö

Oletus oli, että RSA Authentication Manager -ohjelmiston asennus olisi yhtä yksinkertaista kuin minkä tahansa Windows-ohjelmiston. Näin asia ei kuitenkaan ollut, vaan ensimmäiset ongelmat tulivat jo asennusvaiheessa. RSA AM -ohjelmiston asennuksen kannalta kriittisin virhe tapahtui jo Windows-palvelimen asetusvaiheessa.

RSA AM on tarkka palvelimen DNS-asetusten osalta, ja niiden piti olla täysin oikein. Lisäksi Windows ei saa toimia Domain Controller -tilassa, sillä tässä tilassa se tuottaa virheen RSA AM:n asennusvaiheessa, eikä ohjelmisto tästä syystä toimi oikein. Kun nämä kaksi asiaa sekä laitteiston minimivaatimukset täyttyvät, ei pitäisi tulla ongelmia asennukssa.

Tarkoituksena oli luoda todennuspalvelin alusta loppuun asti, joten eteneminen alkoi palvelimen käyttöjärjestelmän asennuksesta.

3.2 RSA Authentication Managerin asentaminen

Kun Windows oli asennettu ja sen asetukset oikein määritetty, oli turvallista aloittaa RSA AM:n asennus. Palvelin tulee toimimaan pääpalvelimena, joten käytettävä tietokanta tulee samalle palvelimelle. Ohjelmisto tarjoaa myös mahdollisuuden ottaa käyttöön toiselle palvelimelle asennetun tietokannan, mutta tässä tapauksessa luodaan oma tietokanta sekä otetaan käyttöön RSA AM-ohjelmiston tarjoama RADIUS-komponentti. Myös RADIUS-komponetti on haluttaessa mahdollista asentaa toiselle palvelimelle, mutta annettujen lähtökohtien mukaisesti se asennettiin samalle palvelimelle.

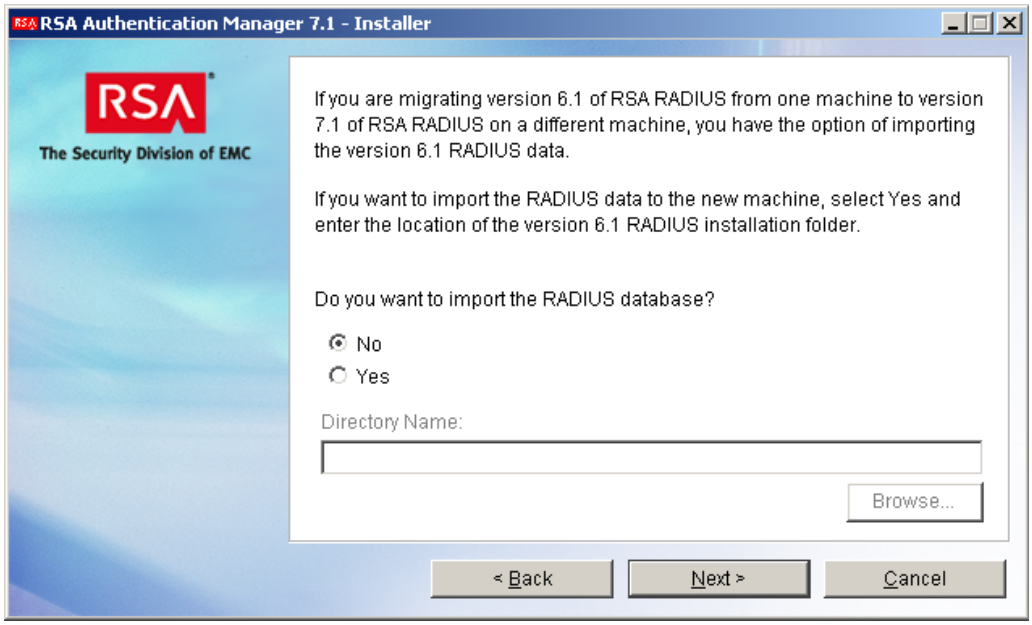
Järjestelmän ylläpito on huomattavasti vaivattomampaa, kun tärkeimmät komponentit ovat samalla palvelimella. Haittapuolena on taas se, että palvelimen kaatuessa koko järjestelmä lakkaa toimimasta, eikä käyttäjiä voida todentaa. Tästä syystä on hyvä ottaa huomioon järjestelmän redundanttisuus, ja järjestelmän toimivuuden kannalta kriittisimmät komponentit tulisi kahdentaa. Tässä opinnäytetyössä kahdentaminen jätettiin taka-alalle ja keskityttiin muihin osa-alueisiin.

Ennen asennuksen aloittamista on syytä ottaa erilliseltä CD-levyltä talteen lisenssitiedosto, palvelinavain ja sertifikaatti, jotta ei itse asennuksessa tule ongelmia. Asennuksen tärkein vaihe on nimen ja IP-osoitteen antaminen palvelimelle. Jos Windows Server 2003 -palvelimen DNS-palvelu on otettu käyttöön ja se on oikein asetettu, RSA AM:n asennusvaiheessa palvelimen FQDN ja IP-osoite tulevat näkyviin, kuten kuvasta 4 näkyy.

Kuva 4. Palvelimen nimi ja IP-osoite.

Seuraavaksi oli vuorossa lisenssitiedoston, palvelinavaimen ja sertifikaatin lataaminen aikaisemmin valitusta kohteesta. Käyttäjänimen ja salasanan luomisen jälkeen oli päätettävä, asennetaanko palvelimelle ensisijainen RADIUS-komponentti vai mahdollisesti aikaisemmin luodun RADIUS-komponentin replika, jäljennös.

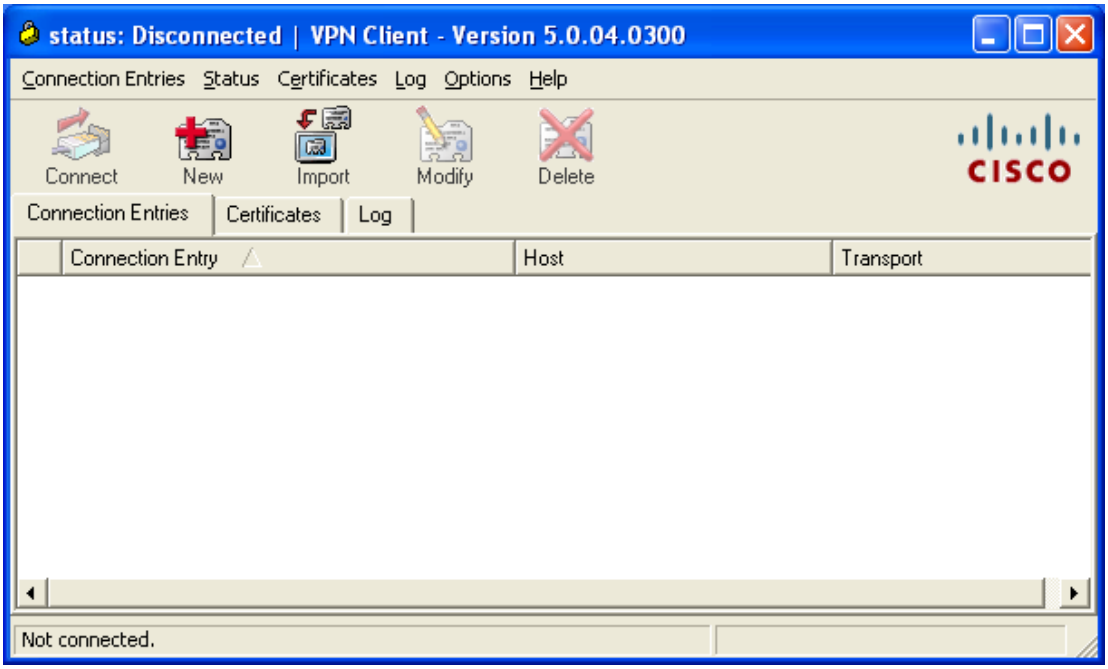
Asennuksen seuraavassa vaiheessa kysyttiin halukkuutta importoida aikaisemmin luotu RADIUS-tietokanta, mutta koska sellaista ei ollut saatavilla, asennettiin uusi tietokanta (kuva 5).



Kuva 5. Tietokannan asennus.

3.3 Cisco VPN Clientin asennus

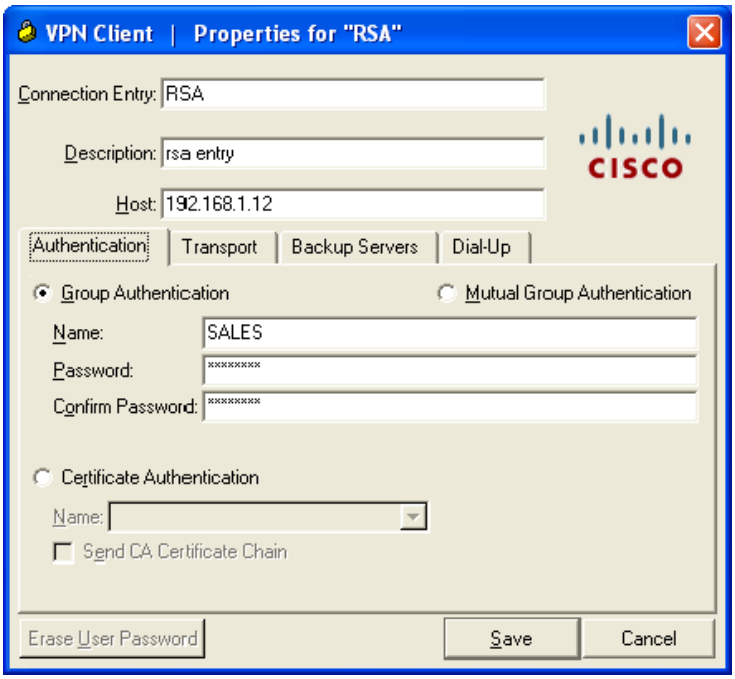
Virtuaalikoneiden alustana toimi VMware Workstation, johon asennettiin Cisco VPN Client -ohjelma. VMware-koneiden käyttöjärjestelmänä oli Windows XP. Ohjelman asennuksen jälkeen oli virtuaalikone käynnistettävä uudestaan. Uudelleenkäynnistyksen jälkeen VPN Client käynnistettiin ja kuvan 6 mukaisesti painettiin ”New”.



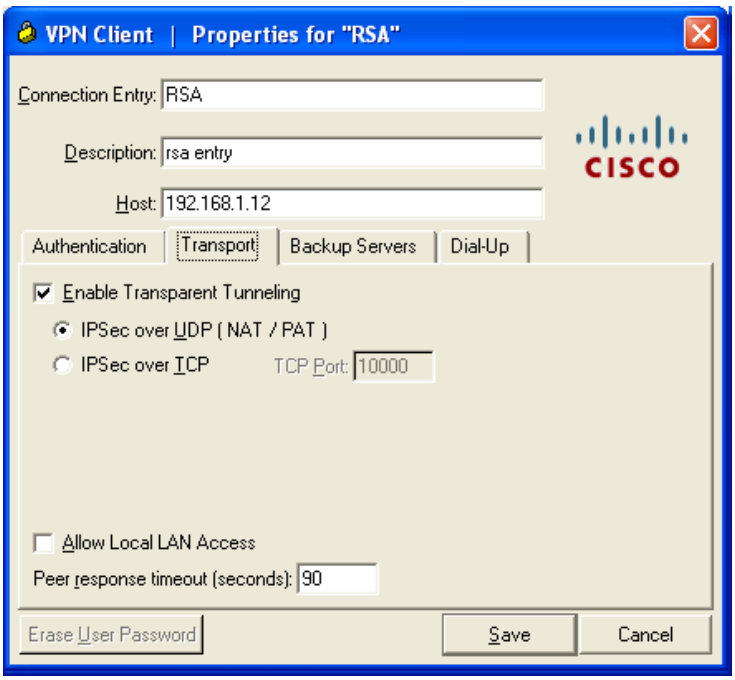
Kuva 6. Cisco VPN Client -ohjelman käyttöönotto.

Seuraavana annettiin käytettävälle yhteydelle nimi RSA ja IP-osoitteeksi asetettiin yhdyskäytävän osoite 192.168.1.12. ”Authentication”-välilehdestä valittiin ”Group Authentication” ja nimeksi oli annettava reitittimeen konfiguroitua vastaava nimi eli tässä tapauksessa ”SALES” ja nimeä vastaava salasana (kuva 7).

”Transport”-välilehdeltä valittiin kuvan 8 mukaisesti ”Enable Transparent Tunneling” ja ”IPSec over UDP (NAT/PAT)”, minkä jälkeen valinnat tallennettiin.



Kuva 7. Yhteysasetuksien määrittäminen.



Kuva 8. Kuljetustavan valitseminen.

Näin VPN Client oli asetettu toimintavalmiiksi ja VPN-yhteys oli yhdistämistä vaille valmiina.

3.4 Kytkentä ja reitittimen konfigurointi

Kytkentä koostui Cisco 2800 sarjan reitittimestä, palvelinkoneesta sekä kahdesta virtuaalikoneesta, jotka kuvasivat tässä kytkennässä käyttäjiä. Käyttäjillä oli RSA:n tarjoamat tokenit, jotka generoivat todennukseen vaadittavan luvun.

Koko järjestelmän tietoturva perustuu johonkin, mitä käyttäjä tietää, ja johonkin mitä käyttäjä omistaa. Tapahtumaa voi etäisesti verrata tapahtumaan pankkiautomaatilla, eli käyttäjä omistaa pankkikortin ja tietää siihen kuuluvan PIN-koodin. Jotta käyttäjä pääsee tilitietoihinsa käsiksi, pitää hänellä olla sekä pankkikortti että PIN-koodi.

Tässä järjestelmässä pankkikorttia vastaa RSA SecurID -token, joka generoi uuden OTP:n joka 60. sekunti, ja PIN-koodi on käyttäjän itse määrittelemä. Todennus onnistuisi myös pelkän tokenin generoiman luvun avulla, mutta koska tietoturvan haluttiin olevan mahdollisimman vahva, päädyttiin ns. two-factor-todennukseen.

Konfigurointi tehtiin Cisco 2800 -sarjan reitittimen IOS-versioon 12.4(13r)T. Reititin toimi VPN-yhteyden yhdyskäytävänä VPN-tunnelin ja RSA AM:n välillä. Seuraavassa on käytetty Cisco-reitittimen konfiguraatio:

```
hostname RSA
boot-start-marker
boot-end-marker
aaa new-model
aaa authentication login VPNAUTHEN group radius local
aaa authorization network VPNAUTHOR local
aaa session-id common
resource policy
ip cef
username vpnrsa password 0 cisco
crypto isakmp policy 3
 hash md5
 authentication pre-share
 group 2
crypto isakmp client configuration group SALES
 key cisco123
 domain cisco.com
 pool IPPOOL
crypto ipsec transform-set MYSET esp-des esp-md5-hmac
```

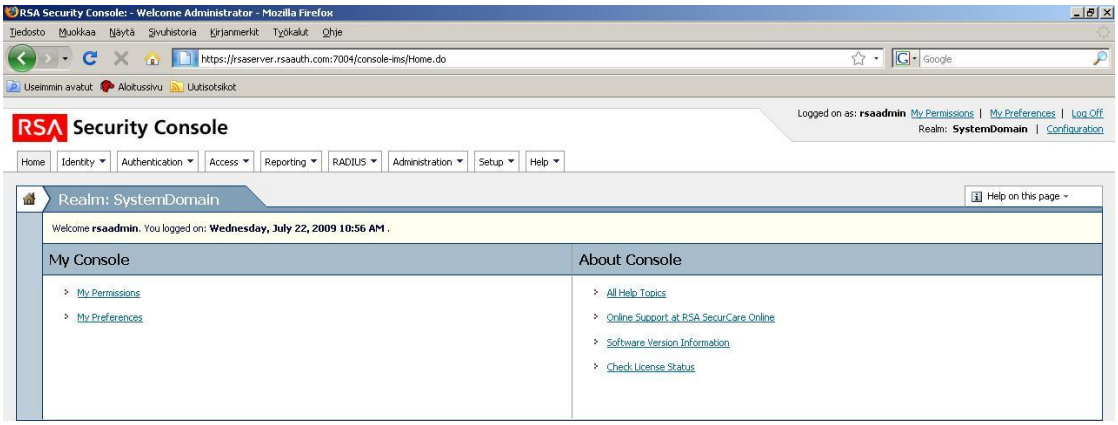
```
crypto dynamic-map DYNMAP 10
 set transform-set MYSET
 reverse-route
crypto map CLIENTMAP client authentication list VPNAUTHEN
crypto map CLIENTMAP isakmp authorization list VPNAUTHOR
crypto map CLIENTMAP client configuration address respond
crypto map CLIENTMAP 10 ipsec-isakmp dynamic DYNMAP
interface FastEthernet0/0
 ip address 193.167.58.193 255.255.255.192
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 192.168.1.12 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
 crypto map CLIENTMAP
router eigrp 1
 redistribute static
 network 172.26.0.0
 network 192.168.1.0
 no auto-summary
ip local pool IPPOOL 11.0.1.20 11.0.1.30
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
ip http server
no ip http secure-server
ip nat inside source list 5 interface FastEthernet0/0 overload
access-list 5 permit any
radius-server host 193.167.58.199 auth-port 1645 acct-port 1646
radius-server timeout 120
radius-server key rsasecret
control-plane
line con 0
line aux 0
line vty 0 4
scheduler allocate 20000 1000
end
```

4 RSA AUTHENTICATION MANAGER

Tässä osiossa käsitellään RSA Authentication Managerin hallinnointia RSA Security -konsolilla sekä ohjeistetaan RSA Security -konsolin käyttöä. Myös järjestelmän toiminnan kannalta tärkeimmät toiminnot on käsitelty osiossa.

4.1 RSA Security -konsoli

RSA Authentication Manager on selainpohjainen käyttöliittymä, joka käyttää Java-ohjelmistoalustaa. RSA Security -konsolin avulla ylläpitäjä hallinnoi, ohjaa ja seuraa käyttäjien, tokeneiden ja serverien toimintaa. Kuvassa 9 on esitetty RSA Security -konsolin etusivu. RSA Security -konsoliin kirjaudutaan asennusvaiheessa luoduilla järjestelmänvalvojan tunnuksilla.



Kuva 9. RSA Security -konsolin etusivu.

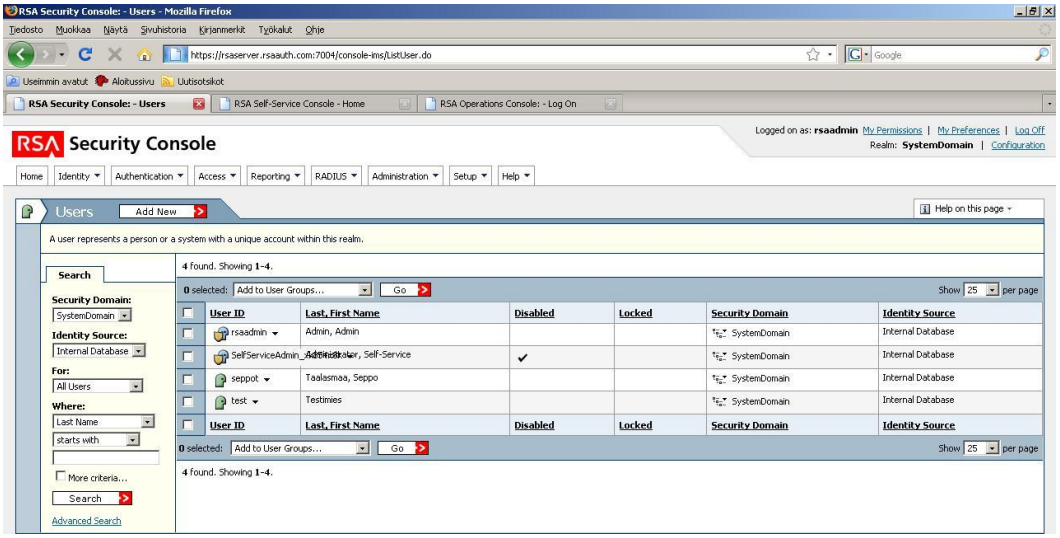
4.2 RSA AM -palvelimen hallinnointi

Konsolista käsin voidaan hallinnoida lähes kaikkea, mikä liittyy käyttäjien todennukseen ja todennusserveriin. Käyttäjät ja tokenit määritellään konsolista, ja niiden tietoja ja asetuksia voidaan muuttaa vain konsolista käsin. Käyttäjä pystyy vain määrittämään PIN-koodin ja senkin vain, jos konsolin ylläpitäjä on asettanut sen pakolliseksi.

Security-konsolin avulla tilien hallinnointi on helppoa ja yksinkertaista, eikä tokenien käyttäjien tarvitse kuin kirjoittaa PIN-koodi oikein kirjautuessaan. Kokemattomampikin ylläpitäjä oppii nopeasti löytämään tärkeimmät sivut ja laittamaan asetukset toimiviksi. Etusivulla näkyvästä ”Help”-välilehtilinkistä löytyy

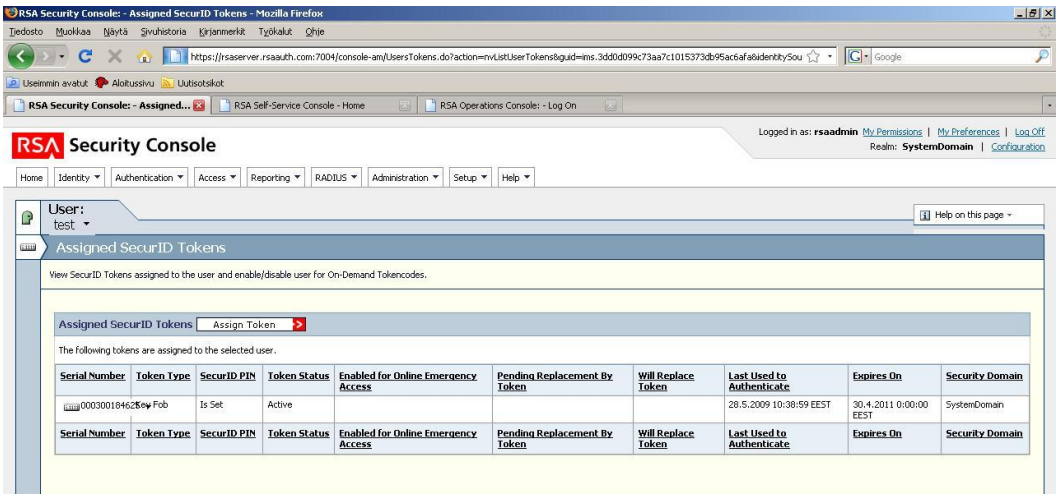
apu lähes kaikkiin ongelmiin, joita Security-konsolin kanssa voi ilmetä. ”Reporting” -välilehtilinkistä pääsee tarkastelemaan serverin tapahtumia, joista ylläpitäjä voi tarkastella raportit kirjautumisista, virheilmoituksista sekä muista serverin tapahtumista.

Konsolin Users (käyttäjät) -sivulta (Kuva 10) näkyvät kaikki RSA Tokenien rekisteröidyt käyttäjät ja käyttäjien tietoja hallinnoidaan täältä. Users-sivulta näkyy myös se, mihin hallinta-alueeseen ja tietokantaan käyttäjät kuuluvat. Users-sivulta selviää myös, onko käyttäjän tili lukittu tai poistettu.

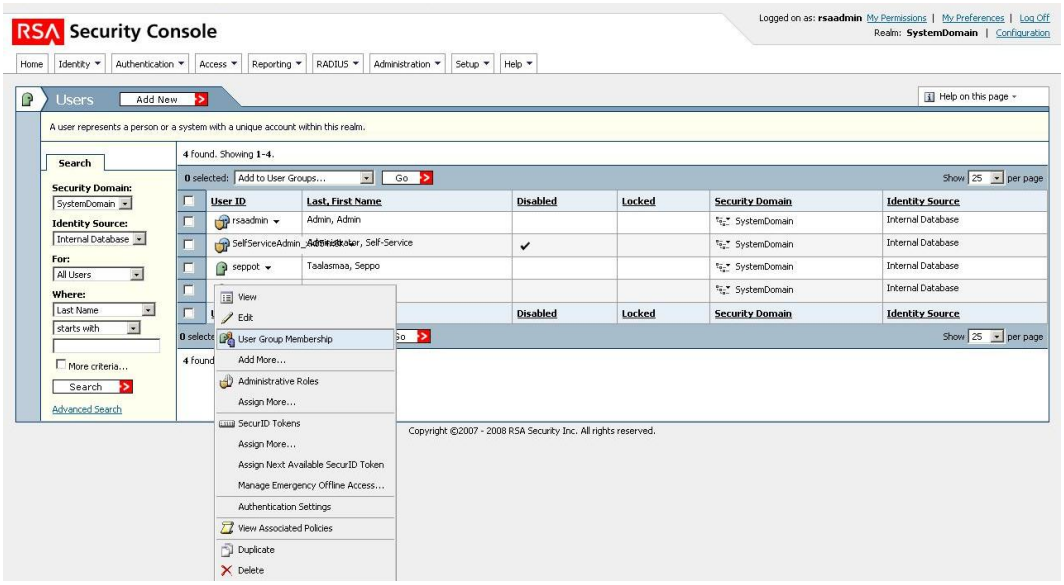


Kuva 10. Users-sivu.

Users-sivulta päästään tarkastelemaan käyttäjien käytössä olevien tokenien tietoja (Kuva 11) painamalla hiiren oikeanpuoleista nappia käyttäjän nimen kohdalla ja valitsemalla valikosta linkin ”SecurID Tokens”, kuten kuvassa 12.



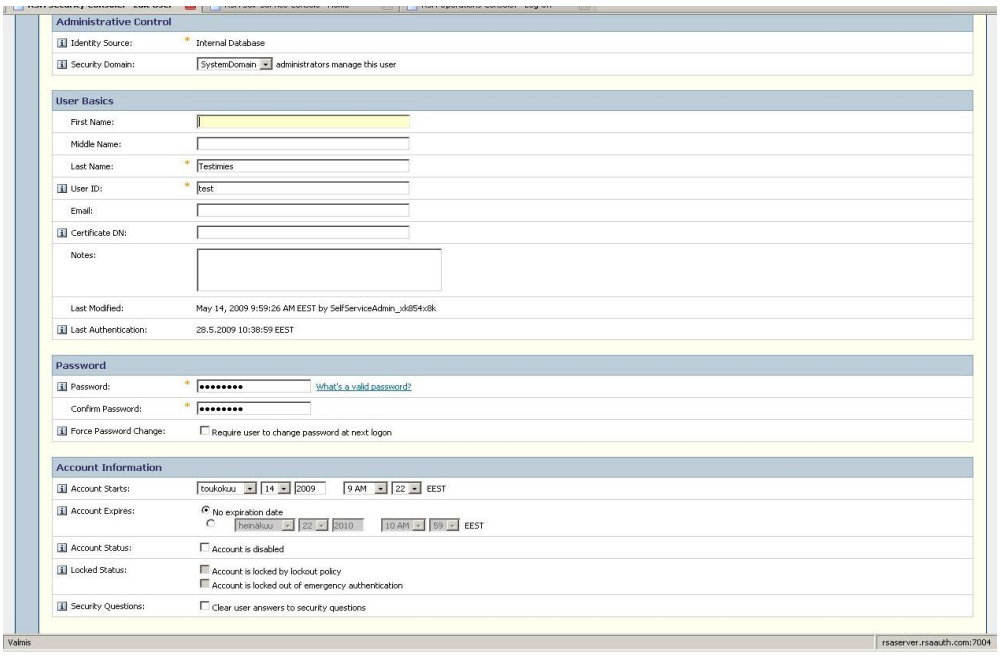
Kuva 11. Käyttäjän "test" käytössä olevan tokenin tiedot.



Kuva 12. Linkin käyttäminen Users-sivulta, SecurID Tokens -sivulle.

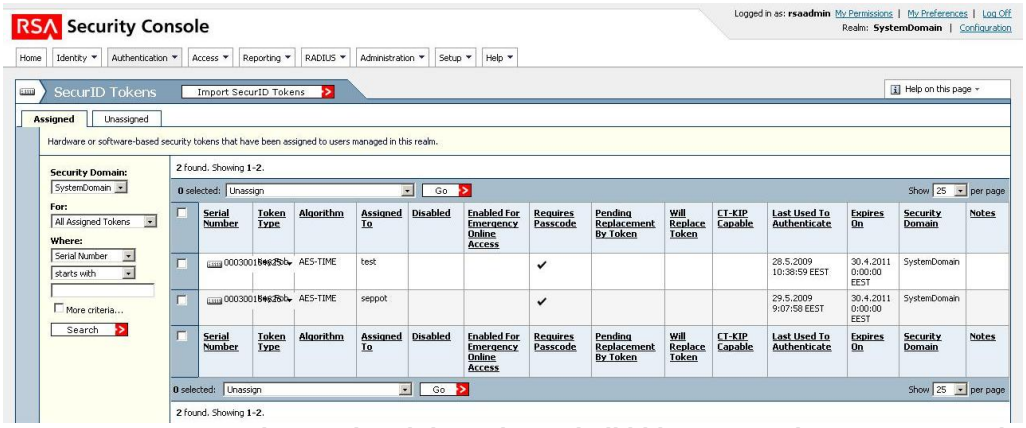
Tokenin tiedot -sivulta (Kuva 11) selviää myös SecurID PIN -koodin ja tokenin tilat ja se, milloin viimeinen todennus on suoritettu, tokenin vanhentumisaika sekä mihin toimialueeseen kyseinen token kuuluu.

Käyttäjien tilejä voidaan hallinnoida ja muokata Edit Users -sivulta (Kuva 13). Tileille voidaan määritellä tilin avautumis- ja sulkeutumisaika sekä tilit voidaan lukita tai poistaa käytöstä tältä sivulta. Käyttäjän perustiedot, kuten nimi ja käyttäjätunnus, voidaan määrittää tai niitä voi muokata Edit Users -sivun kautta.



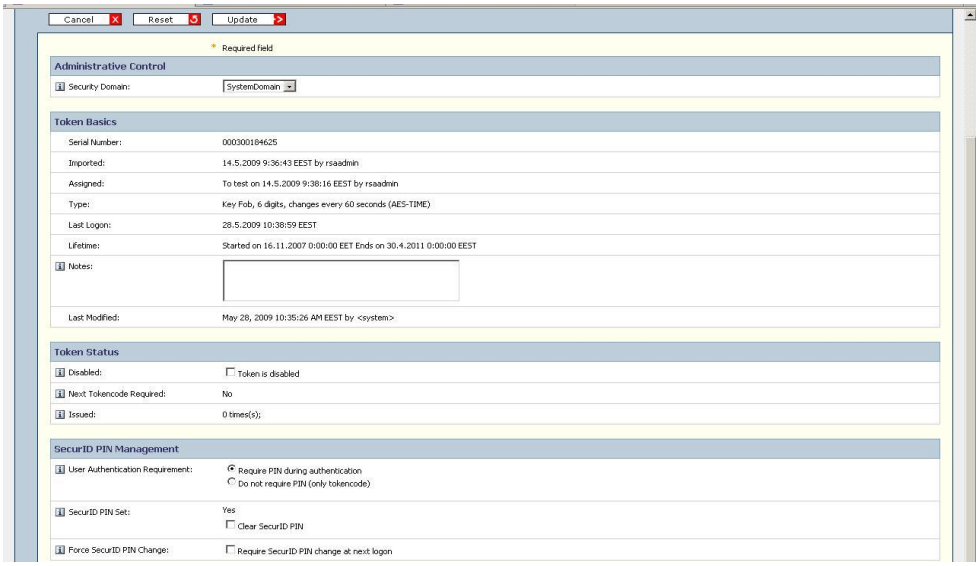
Kuva 13. Edit Users -sivu.

SecurID Token -sivulta (Kuva 14) voidaan muokata sekä tarkastella tokeneiden tietoja ja kirjautumissääntöjä. Sivulta selviävät kaikkien käytössä olevien SecurID-tokenien sarjanumerot, tyypit, käytössä oleva algoritmit, tokenien käyttäjät sekä se, milloin edellinen kirjautuminen milläkin tokenilla on tapahtunut.



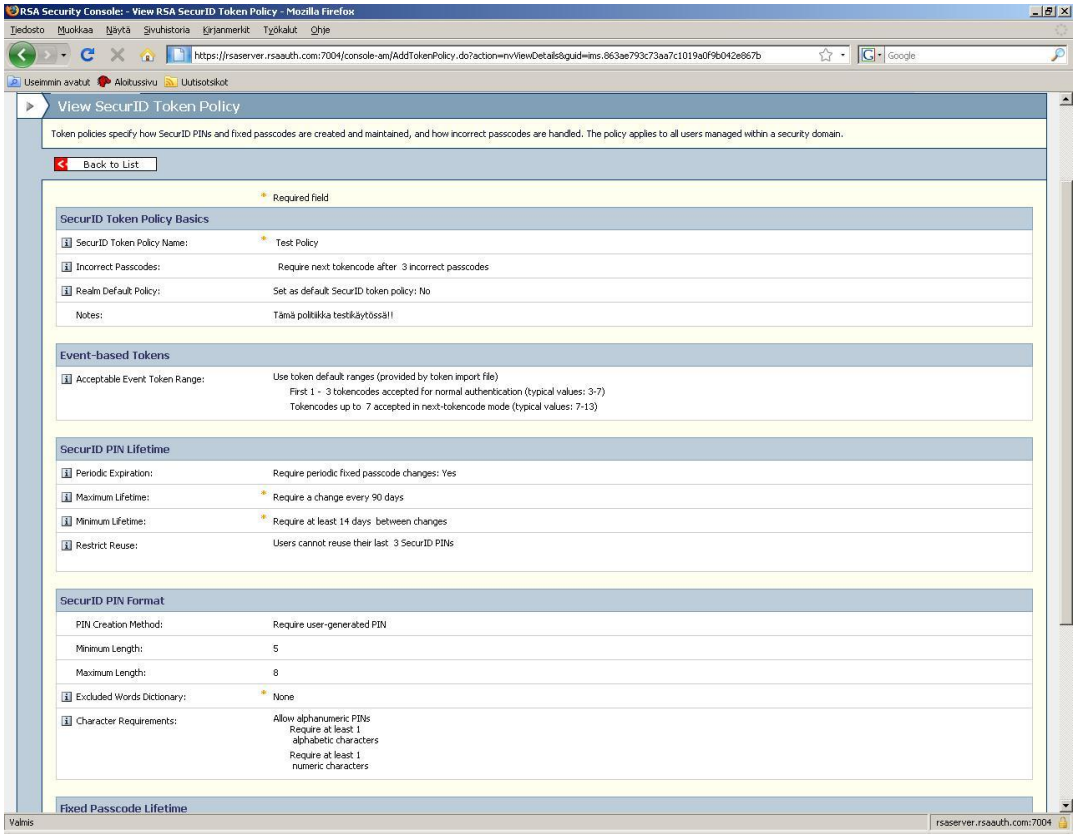
Kuva 14. SecurID Tokens -sivu, jolta näkyvät kaikki käytössä olevat SecurID-tokenit.

Edit SecurID Tokens -sivulta (Kuva 15) voidaan määrittää yhteyden todentamistapa. Yhteys voidaan todeta joko pelkällä tokenin luomalla koodilla tai yhteisesti tokenin luomalla koodilla ja PIN-koodilla. Normaalisti kirjautuminen tapahtuu tokenin luoman koodin sekä käyttäjän itse määrittelemän PIN-koodin avulla. Edit SecurID Token -sivulta voidaan token kytkeä pois päältä tai pakottaa käyttäjää vaihtamaan PIN-koodi seuraavan kirjautumisen yhteydessä.



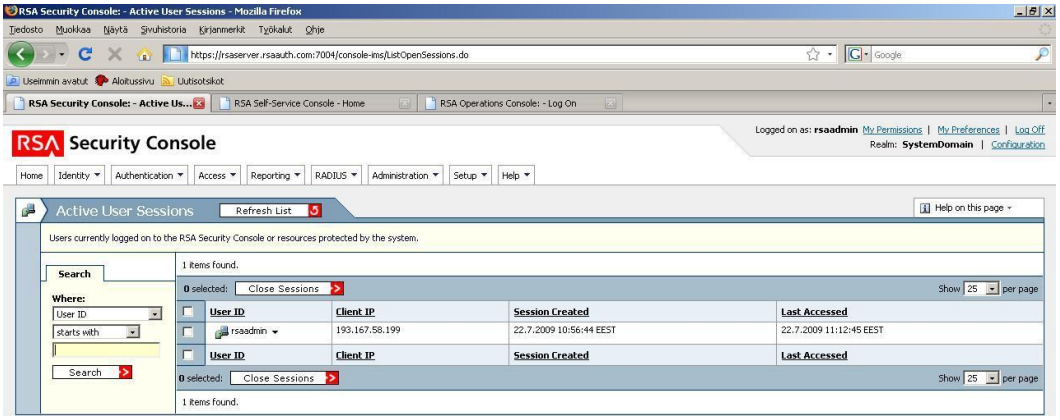
Kuva 15. Edit SecurID Token -sivu.

SecurID Token Policy -sivulta (Kuva 16) selviää, mitä määrityksiä PIN-koodille on tehty. PIN-koodille voidaan asettaa erilaisia määrityksiä, kuten minimi- ja maksimipituus sekä numeroiden ja aakkosten minimimäärät.



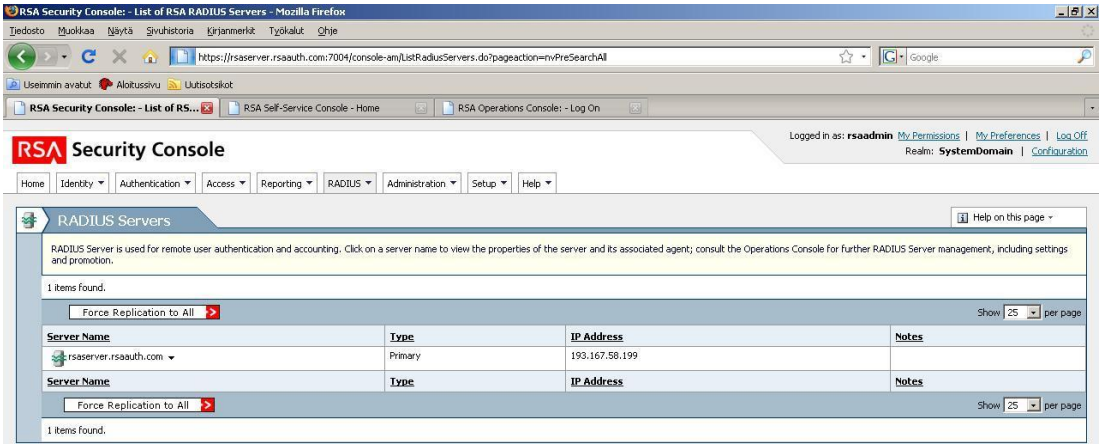
Kuva 16. SecurID Token Policy -sivu.

Active User Sessions -sivulta (Kuva 17) näkee aktiivisena olevat käyttäjätilit. Sivulta selviää käyttäjän IP-osoite sekä milloin viimeinen yhteysjakso on avattu ja milloin viimeinen vierailu on tehty.



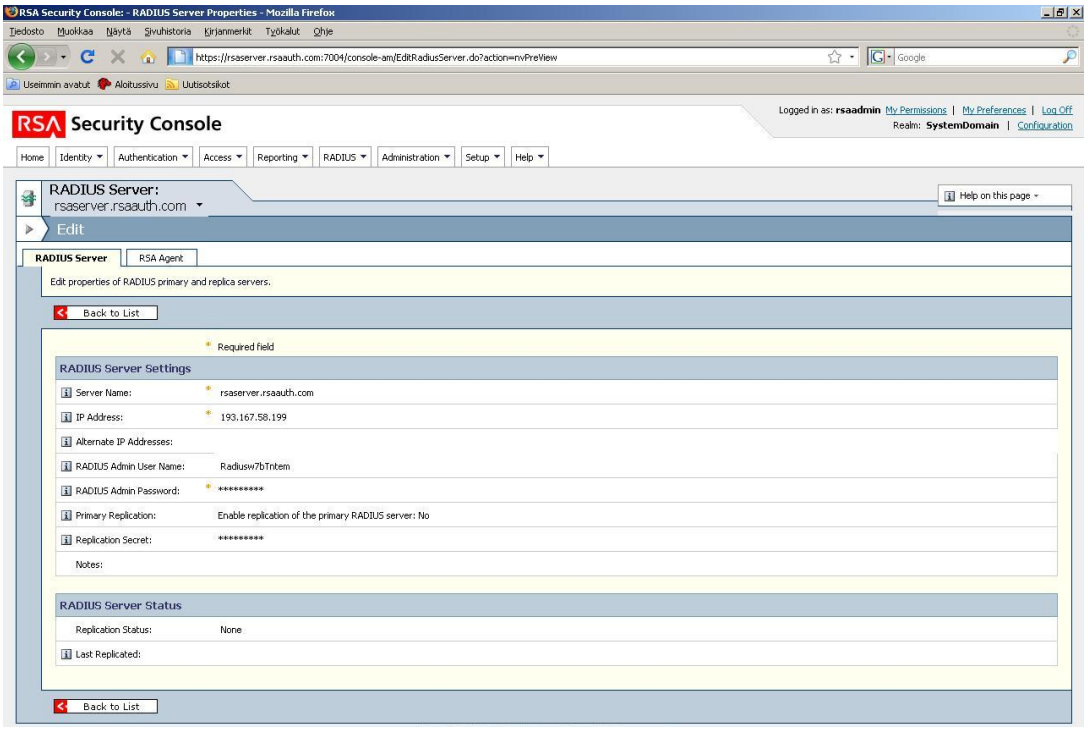
Kuva 17. Active User Sessions -sivu, jolta näkyvät aktiiviset käyttäjät.

RADIUS Servers -sivulta (Kuva 18) selviää palvelimen tai palvelimien nimet, tyyppi sekä palvelimien IP-osoitteet. RADIUS-palvelimet toimivat joko ensisijaisena tai toissijaisena palvelimena. Jos RADIUS-palvelimia on vain yksi, on se silloin automaattisesti ensisijainen palvelin.



Kuva 18. RADIUS Servers -sivu.

RADIUS-palvelimen tarkemmat tiedot saadaan näkyviin painamalla halutun palvelimen kohdalla hiiren oikeata näppäintä ja valitsemalla valikosta Edit. RADIUS Server Edit -sivulta (Kuva 19) selviää serverin tarkemmat tiedot.



Kuva 19. RADIUS Server Edit –sivu

5 TODENNUSTAPOJA

5.1 Laitteisto-tokenit

Laitteisto-tokenit (LIITE 1) tarjoavat hakkerikestävän kahden tekijän todennuksen, mistä seuraa, että todennus on helppokäyttöinen ja käyttäjän tunnistus tehokasta. Laitteisto-tokenit perustuvat RSA:n patentoimaan ajan synkronisointiteknologiaan, jossa matemaattinen 128-bittinen AES-algoritmi tuottaa 60 sekunnin välein kertakäyttöisen todennuskoodin, OTP:n. Tässä opinnäytetyössä käytössä on token mallia RSA SecurID 700. (Hardware Authenticators, RSA.com 2009; Technical Specifications, RSA.com 2009.)

Päästäkseen käsiksi SecurID:n turvaamaan järjestelmään käyttäjä yhdistää kirjautuessaan oman PIN-koodinsa tokenin generoimaan todennuskoodiin. Nämä kaksi numerosarjaa ovat yhdessä uniikki kertakäyttösalasana, jota käytetään käyttäjän tunnistamiseen tai todennukseen. Jos SecurID-järjestelmä vahvistaa kertakäyttösalasanan (One-Time Password, OTP), pääsee käyttäjä käsiksi suojattuun materiaaliin, mutta jos käyttäjää ei voida tunnistaa, evätään häneltä pääsy järjestelmään. Tätä menetelmää voidaan verrata toimintaan pankkiautomaatilla, eli käyttäjä omistaa pankkikortin ja tietää siihen kuuluvan PIN-koodin, joiden avulla hän pääsee omiin tilitietoihinsa käsiksi. (Hardware Authenticators, RSA.com 2009.)

Käytettäessä Hardware todennusta ei vuorovaikutusta tietokoneen kanssa tarvita. Käyttäjän ei siis tarvitse asentaa tai ylläpitää mitään ohjelmistoa. Myöskään käyttäjän saama token ei vaadi häneltä mitään toimenpiteitä. Se on heti käyttövalmis laatikosta ulos otettuna, eli se ei vaadi käyttäjältä mitään koodaustaitoa. RSA SecurID Hardware Tokenit ovat täysin umpinaisia ja niiden sisältämä paristo kestää eliniän, eli käyttäjän ei tarvitse huoltaa tai vaihtaa paristoja. (Hardware Authenticators, RSA.com 2009.)

5.2 Ohjelmisto-tokenit

RSA SecurID:n kahden tekijän todennus toimii monenlaisten henkilökohtaisten laitteiden avulla, mikä helpottaa IT-järjestelmänvalvojan vahvan todennuk-

sen suorittamista kätevänä osana liiketoimintaa. RSA SecurID Software -todentaja (LIITE 2) vähentää niiden laitteiden määrää, joita käyttäjän täytyy hallita. Toisin sanoen ohjelmiston asennuksen voi suorittaa esimerkiksi käyttäjän omaan matkapuhelimeen tai kannettavaan tietokoneeseen, minkä seurauksena erillistä tokenia ei tarvitse kantaa mukana. (Software Authenticators, RSA.com 2009; Partner Authenticators, RSA.com 2009.)

Ohjelmisto-tokenit tarjoavat vahvan kahden tekijän todennuksen erittäin turvallisessa ohjelmistototeutuksessa. Ohjelmisto-tokenit yhdistetään käyttäjän henkilökohtaiseen laitteeseen, mikä poistaa tarpeen kuljettaa toista laitetta mukana. Yhteen henkilökohtaiseen laitteeseen voidaan yhdistää jopa kymmenen ohjelmisto-tokenia ja ne tukevat monenlaisia tietojärjestelmiä ja laitteita. Näin ne tarjoavat myös joustavuutta todennuksen malleissa ja valvonnassa. (Software Authenticators, RSA.com 2009.)

RSA SecurID -ohjelmisto-tokenit tukevat samoja algoritmeja kuin alan johtavat RSA SecurID laitteisto-tokenit. Sen sijaan että symmetrinen avain olisi tallennettu RSA SecurID laitteisto-tokenille, on se turvassa käyttäjän tietokoneessa, PDA:ssa tai matkapuhelimessa. RSA SecurID:n symmetriset avaimet voidaan tallentaa myös älykorttiin tai USB-laitteeseen ja käyttää yhdessä RSA SecurID -ohjelmisto-tokenin kanssa käyttäjän tietokoneella. (Software Authenticators, RSA.com 2009.)

5.3 Hybriditodennus

Hybriditodennus (LIITE 3) koostuu tokenista, joka sisältää standardien mukaisen digitaalisen sertifikaatin ja sitä varten USB-liitännän. Sertifikaatti tukee mm. levyjen ja tiedostojen salausta, digitaalista allekirjoitusta ja muita sovelluksia, jotka vahvistavat yksinkertaista salasanaa. Tämä token voi sisältää useamman käyttäjäprofiilin ja salasanan kirjautumista varten. Tätä tokenia käytettäessä tunnistautuminen tapahtuu ohjelmistopohjaisesti eikä käyttäjän tarvitse itse painella numerokoodia palveluun. (RSA Hybrid Authenticators, RSA.com 2009.)

Hybriditodennusta tukevat RSA SecurID 800 ja 900. RSA SecurID 900 on pankkikortin näköinen ja kokoinen sekä se sisältää allekirjoitusfunktion. Tämä funktio suojaa vahvasti yrityksen transaktioita. Kun käyttäjä kirjautuu taloudellisille sivuille ja hänen suorittaessaan rahansiirron, kysyy sivu vahvistusnumeron. Käyttäjä syöttää tämän vahvistusnumeron tokeniinsa ja vastineeksi token generoi vastineen vahvistusnumerolle. Jos tokenin generoima vastine ja sivun antama vahvistusnumero täsmäävät, voidaan rahansiirto suorittaa. (RSA Hybrid Authenticators, RSA.com 2009.)

5.4 On-demand-todennus

Nimensä mukaisesti tämä todennustapa toimittaa uniikin OTP:n vaadittaessa. OTP voidaan toimittaa käyttäjän palveluun rekisteröimän sähköpostin välityksellä tai tekstiviestinä suoraan matkapuhelimeen. Tietoturvasyistä myös matkapuhelimesta tai kannettavasta laitteesta on oltava maininta todennuspalvelussa. Kuten Hardware tokenit, myös on-demand-todennus (LIITE 4) toimii two-factor-periaatteella, eli käyttäjä syöttää kirjautumispalveluun saamansa OTP:n ja tietämänsä PIN-koodin. (On-demand Authenticators, RSA.com 2009)

On-demand-todennus mahdollistaa myös väliaikaisen käyttöoikeuden luotettuihin materiaaleihin. Tämä on tarpeellista, jos yritykseen palkataan esimerkiksi ulkopuolinen urakoitsija. Kun urakoitsija saa työnsä tehtyä tai hänen palveluitaan ei jatkossa tarvita, voidaan hänen käyttöoikeutensa kuolettaa. (On-demand Authenticators, RSA.com 2009)

5.5 OTP token -työkalurivi, RSA SecurID Toolbar

OTP token -työkalurivi (LIITE 5) yhdistää verkkosovellusten auto-fill-ominaisuuden tietojen kalastuksen (anti-phishing) estävään mekanismiin. Ulkoasultaan se muistuttaa muita internet-selaimeen saatavia työkalurivejä sekä sen asennus on yhtä vaivatonta. Jotta petosyrityksiltä vältyttäisiin, OTP lähetetään vain luotetuille sivustoille. RSA SecurID Toolbar tukee kahtakymmentä eri tokenia, joten kaikki käyttäjät eivät tarvitse omaa sovellusta.

6 YHTEENVETO

Kun opinnäytetyön käytännön osuuden ongelmat oli ohitettu, oli työn saattaminen loppuun melko vaivatonta. Koulun laboratorion aiheuttamat omat ongelmat, kuten laitteiden riittävyys ja laitteiden muiden opiskelijoiden kanssa jakaminen, hidastivat myös hieman tehtävän etenemistä.

Todentamiskokonaisuuden toimintaan saattaminen oli kaiken kaikkiaan haastava mutta monipuolinen tehtävä. Kokonaisuutta olisi voitu jalostaa vielä useampaankin eri suuntaan, mutta riittämättömien laitteiden ja vähäisen ajan vuoksi keskityimme työn ydinkohtiin. Esimerkiksi olisi ollut hyvä ottaa huomioon redundanttisuus, eli järjestelmän toimivuuden kannalta oleellisten laitteiden kahdentaminen.

Opinnäytetyön ehdottomasti tärkein osa-alue oli saada todentamiskokonaisuus toimimaan koulun laboratorio-olosuhteissa. Tämä tavoite saavutettiin alun ongelmien jälkeen. Kokonaisuus toimi, niin kuin sen oli tarkoituskin, ja sen käyttäminen oli melko yksinkertaista.

RSA Authentication Manager -todennuksenhallintajärjestelmän käyttäminen ja muokkaaminen omien tarpeiden mukaiseksi oli helppoa heti, kun hallintajärjestelmän käyttöliittymään oli tottunut.

Tälle opinnäytetyölle asetut tavoitteet tulivat täytetyksi ja tulevaisuus näyttää, yleistyykö tämän todennusjärjestelmän tapainen kokoonpano pienemmissäkin yrityksissä.

LÄHTEET

Authentication. Searchsecurity.com, 2007. Saatavissa: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211621,00.html [viitattu 21.10.2009].

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. 1. painos. Porvoo: WS Bookwell.

Hardware Authenticators 2009. Saatavissa: https://www.rsa.com/node.aspx?id=1158 [viitattu 11.10.2009].

Järvinen, P. 2002. Tietoturva & Yksityisyys. 1. painos. Porvoo: WS Bookwell.

Kerttula, E. 1999. Tietoverkkojen tietoturva. 2. uudistettu painos. Helsinki: Oy Edita Ab.

Knowledge Base. Indiana University 2009. Saatavissa: http://kb.iu.edu/data/anjv.html [viitattu 23.9.2009]

On-demand Authenticators. 2009. Saatavissa: https://www.rsa.com/node.aspx?id=3481 [viitattu 7.10.2009].

Partner Authenticators. 2009. Saatavissa: https://www.rsa.com/node.aspx?id=3217 [viitattu 16.8.2009].

RSA, Wikipedia-artikkeli 2009. Saatavissa: http://fi.wikipedia.org/wiki/RSA [viitattu 19.10.2009].

RSA Hybrid Authenticators 2009. Saatavissa: https://www.rsa.com/node.aspx?id=1215 [viitattu 13.8.2009]

RSA Laboratories. RSA Algorithm, 2009. Saatavissa: http://www.rsa.com/rsalabs/node.asp?id=2146 [viitattu 16.9.2009].

RSA Laboratories. What are certificates?, 2009. Saatavissa: http://www.rsa.com/rsalabs/node.asp?id=2277 [viitattu 20.8.2009].

RSA Laboratories, What is a digital signature and what is authentication? 2009. Saatavissa: http://www.rsa.com/rsalabs/node.asp?id=2182 [viitattu 20.8.2009]

SearchSecurity.com. Authentication. Saatavissa: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211621,00.html [viitattu 21.10.2009].

Software Authenticators 2009. Saatavissa: https://www.rsa.com/node.aspx?id=1313 [viitattu 21.7.2009].

Suoranta, L. 2009. Valitse parempia salasanoja. Tietokone 1/2009.

Symantec, Sanasto 2009. Saatavissa: http://www.symantec.com/fi/fi/norton/clubsymantec/glossary/index.jsp [viitattu 20.10.2009].

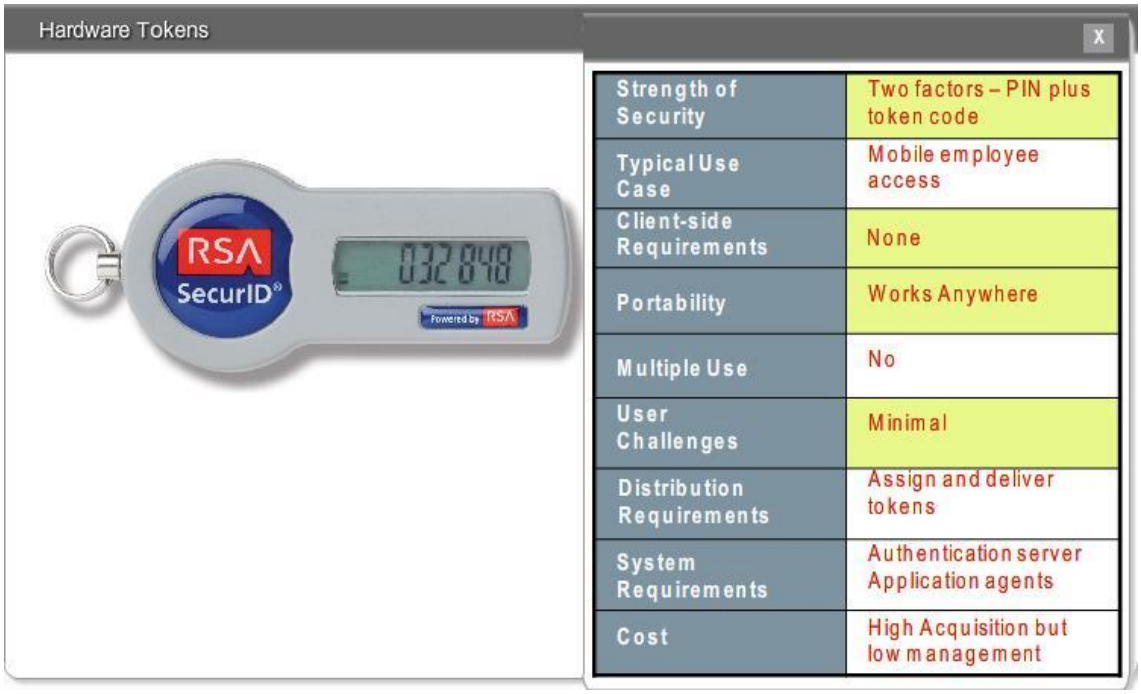
Symantec, Tietoturvainfo 2009. Saatavissa: http://www.symantec.com/region/fi/corporate/glossary.html [viitattu 20.10.2009].

Technical Specifications 2009. Saatavissa: https://www.rsa.com/node.aspx?id=1311 [viitattu 13.9.2009].

Tietotekniikkaosasto, Helsingin yliopisto 2009. Saatavissa: www.helsinki.fi/atk/www/ca/ [viitattu 19.10.2009].

Transport Layer Security. Wikipedia-artikkeli 2009. Saatavissa: http://en.wikipedia.org/wiki/Transport_Layer_Security [viitattu 8.9.2009]

University Of Washington 2009. Saatavissa: http://gis.washington.edu/phurvitz/professional/ssh_ESRI_2000/p19715.gif [viitattu 11.8.2009].



Etuja:

- Erittäin tietoturvallinen
- Voidaan käyttää missä vain ja milloin vain
- Toimii ”all access” -metodeilla
- Ei vaadi ohjelmiston hallintaa (zero footprint)

Haittoja:

- Käyttöönoton monimutkaisuus
- Korkea hinta

RSA:n tarjoamat ratkaisut:

- RSA Authentication Manager
- RSA SecurID -tokenit

Software Token on USB Device

Strength of Security	Two factors – PIN plus token code
Typical Use Case	Mobile employee access
Client-side Requirements	None
Portability	Works Anywhere
Multiple Use	No
User Challenges	Minimal
Distribution Requirements	Assign and deliver tokens
System Requirements	Authentication server Application agents
Cost	High Acquisition but low management

Etuja:

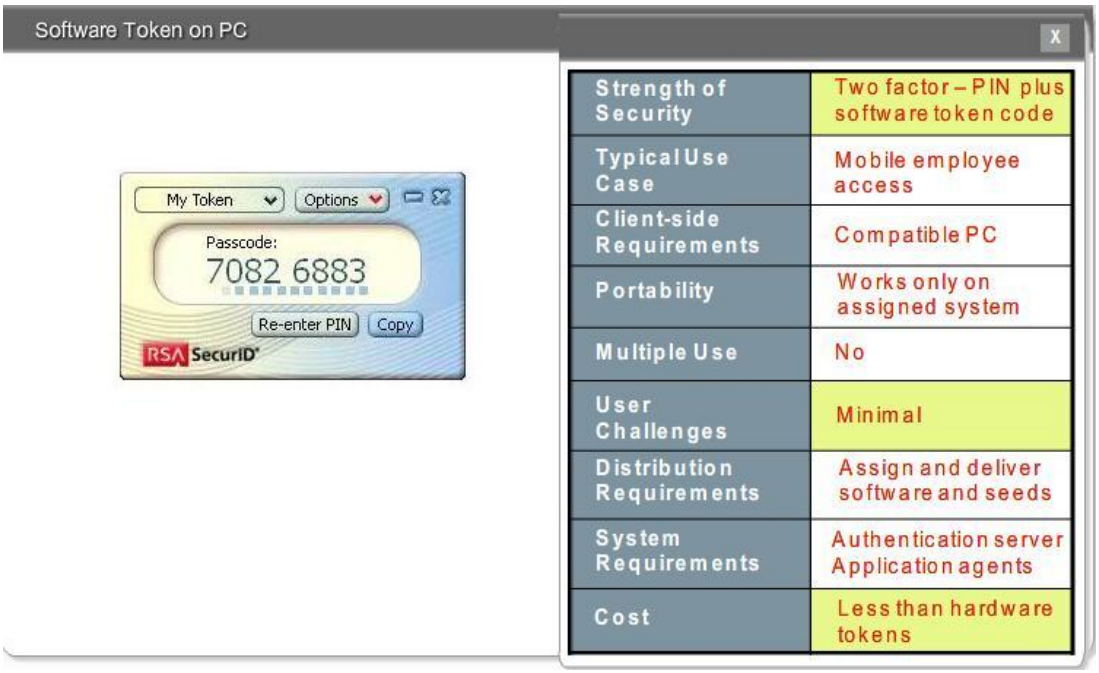
- Pääsy missä ja milloin tahansa
- Vahva tietoturva
- Monitoimisuus
- Tiedostojen ja datan tallennus

Haittoja:

- Korkea hinta (ohjelmisto-token + laite)
- Tarvitsee USB-portin

RSA:n tarjoamat ratkaisut:

- RSA Authentication Manager
- RSA SecurID software token
- 3rd Party devices: SanDisk, MXI Security, IronKey, RedCannon, UPEK



Etuja:

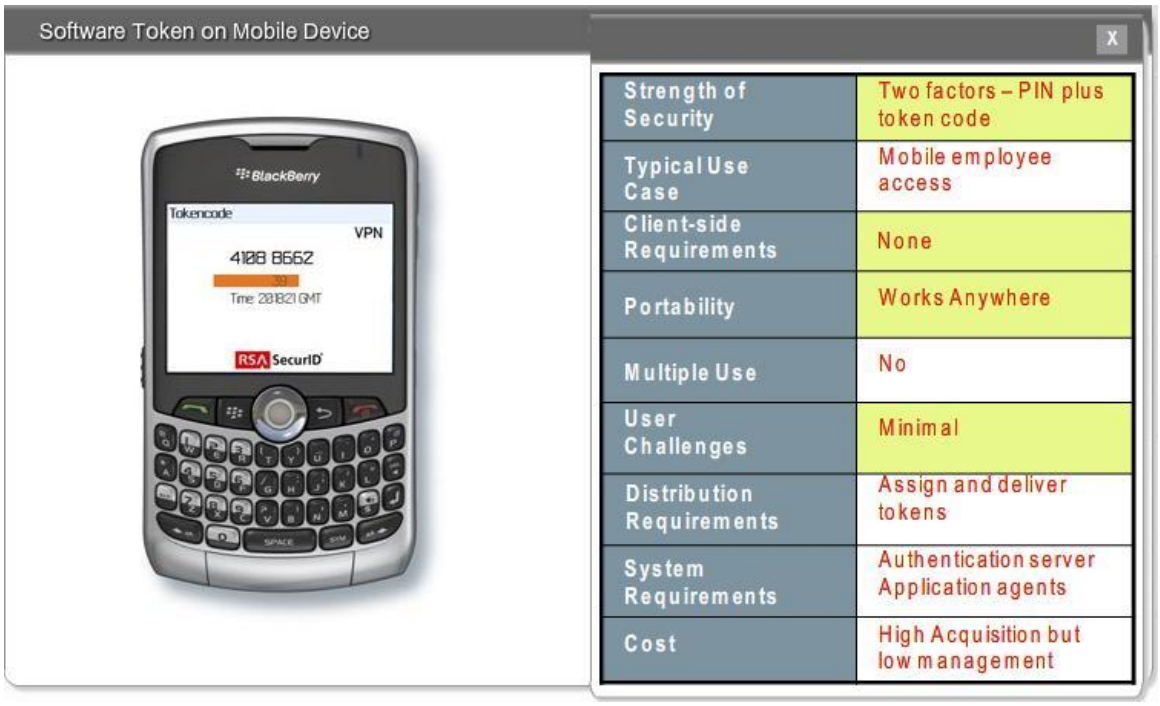
- Turvallinen
- Toimii kaikilla kirjautumismetodeilla
- Toimii tietokoneella
- Matalammat hankintakustannukset
- Windows- ja Mac OS-alustatuki

Haittoja:

- Käyttöönoton monimutkaisuus
- Rajoitettu siirrettävyys

RSA:n tarjoamat ratkaisut:

- RSA Authentication Manager
- RSA SecurID Software token
- RSA Toolbar token



Etuja:

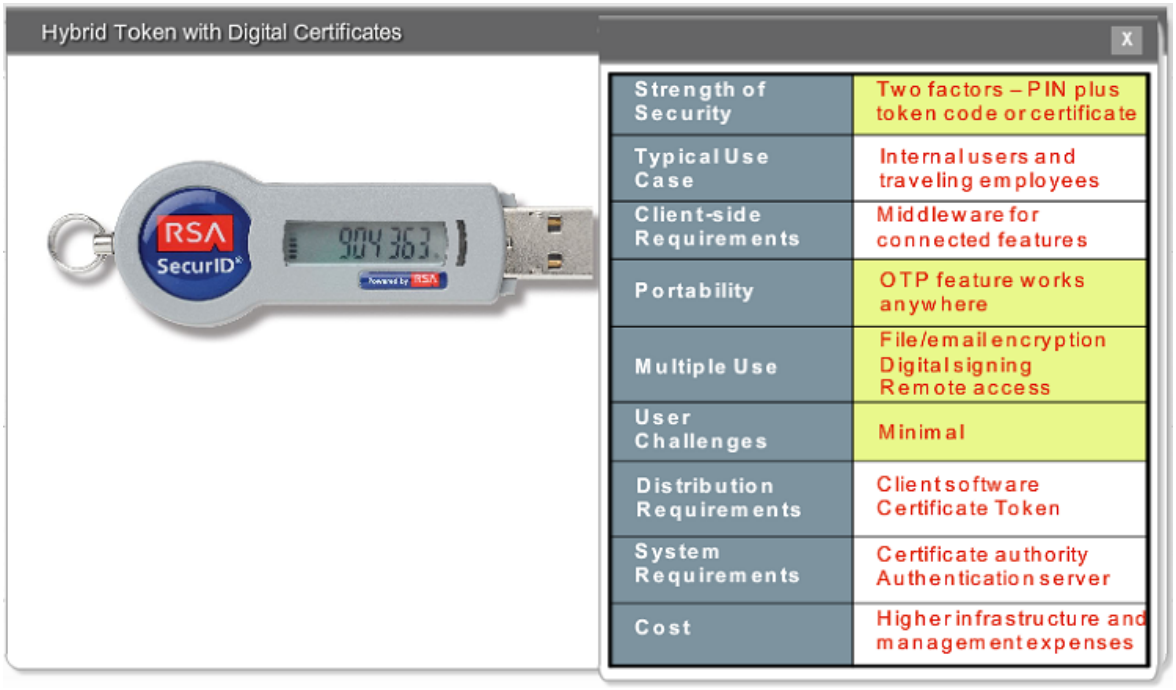
- Turvallinen
- Toimii missä vain ja milloin vain
- Toimii kaikilla kirjautumismetodeilla
- Toimii monikäyttöisillä laitteilla (esim. älypuhelimet)
- Matalammat hankintakustannukset

Haittoja:

- Käyttöönoton monimutkaisuus

RSA:n tarjoamat ratkaisut:

- RSA Authentication Manager
- RSA SecurID software tokenit



Etuja:

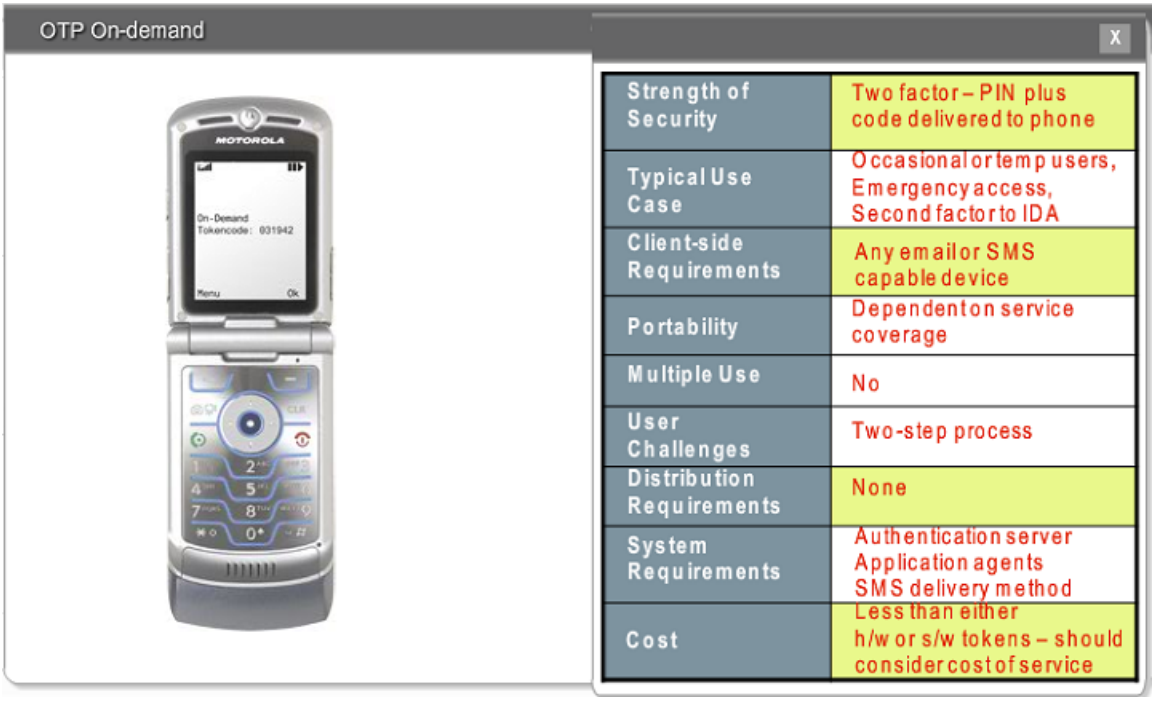
- Yhdistää OTP:n älysirukykyyn
- Voi käyttää tiedosto- tai sähköpostisalausta
- Mahdollistaa etäyhteyden missä ja milloin vain
- Voi tallentaa jopa 7 x.509 sertifikaattia ja 3 Windows kirjautumisparia (userid and password)

Haittoja:

- Vaatii ylläpitoa
- Sertifikaattivaltuudet
- Vahvistusvaltuudet
- Vaatii työpöytäväliohjelmiston
- Korkea hinta

RSA:n tarjoamat ratkaisut:

- RSA SID800
- RSA Authentication Client



Etuja:

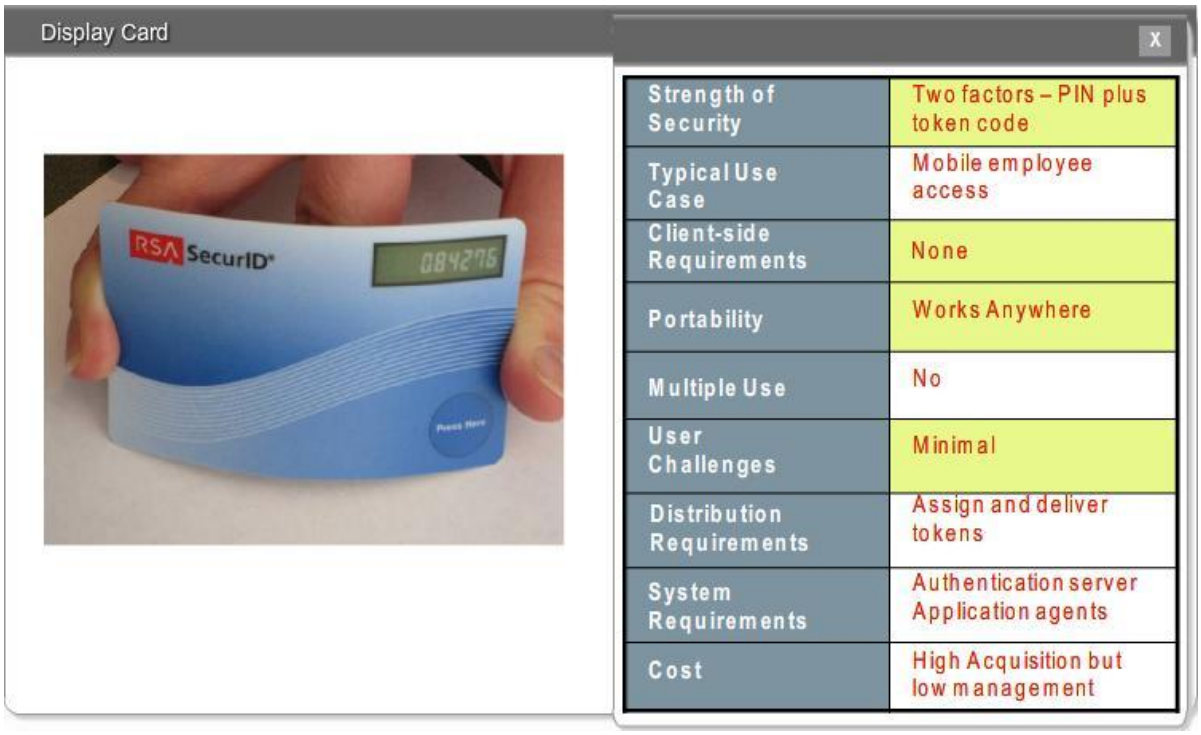
- Turvallisuus
- Toimii kaikilla pääsymetodeilla
- Toimii monikäyttöisillä laitteilla
- Ei käyttöönottoa

Haittoja:

- Rajoitettu toimivuus -> verkon kuuluvuusalueelle
- Kahden askeleen prosessi

RSA:n tarjoamat ratkaisut:

- RSA Authentication Manager
- RSA SecurID On-Demand



Etuja:

- Mahtuu lompakkoon
- Kortti voidaan kustomoida asiakkaan haluamalla kuvamateriaalilla esim. firman logolla
- Magneettiraita kortin takaosassa
- Mahdollistaa kirjautumisen missä vain ja milloin vain
- Yhteensopiva kaikkien RSA SecurID Ready -tuotteiden kanssa

Haittoja:

- Korkea hinta
- Käyttöönoton monimutkaisuus
- Tällä hetkellä saatavuus on rajoitettu suuriin tilauksiin

RSA:n tarjoamat ratkaisut:

- RSA SecurID1100 Display Card
- RSA Authentication Manager
- RSA Secure Authentication Engine