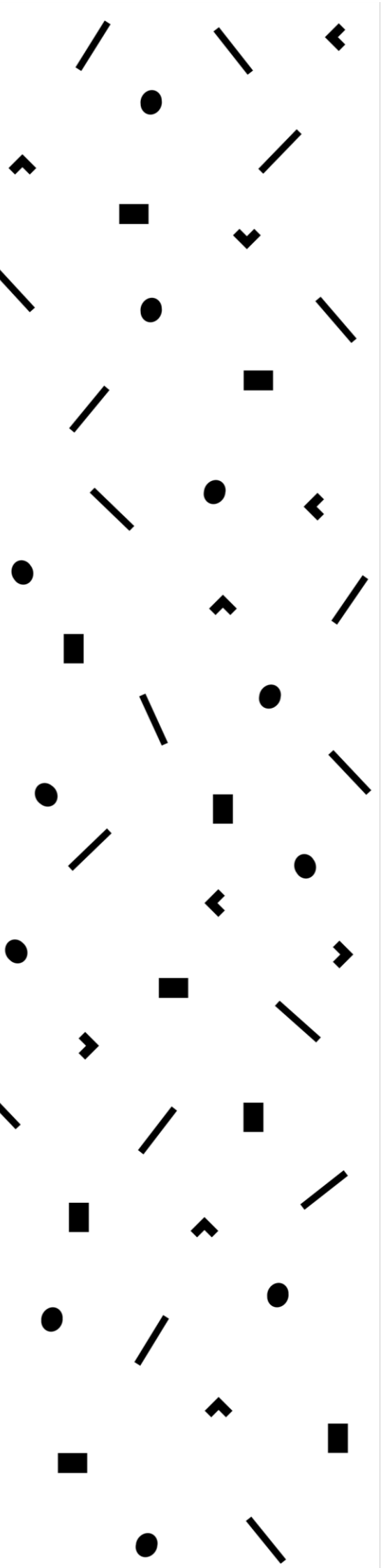


LAMK Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

AUTENTIKOINTI LANGATTOMASSA LÄHIVERKOSSA

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikka
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2015
Tommi Lätti

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

LÄTTI, TOMMI:

Autentikointi langattomassa lähiverkossa

Tietoliikennetekniikan opinnäytetyö, 51 sivua

Kevät 2015

TIIVISTELMÄ

Opinnäytetyön tavoitteena oli suunnitella Päijät-Hämeen sosiaali- ja terveysyhtymälle porttikohtainen autentikointi henkilökunnan uuteen langattomaan verkkoon. Verkon vaatimuksena on, että se on tietoturvallisesti ja käyttäjäystävällisesti toteutettu. Valittu sertifikaatteihin pohjautuva autentikointimenetelmä toteutettiin Lahdessa sijaitsevaan keskussairaalan langattomaan verkkoon.

Ensimmäinen langattomien verkkojen standardi 802.11 julkaistiin vuonna 1997. Alkuperäisen 802.11-standardin mukana tulleet menetelmät käyttäjän autentikointiin ja tiedon salaukseen on saatu murrettua. Tietoturvan korjaamiseksi julkaistiin vuonna 2004 802.11i-standardi. 802.11i mahdollistaa myös autentikoinnin langattomissa verkoissa käyttäen porttikohtaista autentikointia.

Porttikohtainen autentikointi tunnetaan myös nimellä 802.1x ja se laajensi aiemmin kehitetyn EAP-protokollan käytettäväksi langallisissa ja langattomissa verkoissa. EAP itsessään ei ole mikään autentikointi-menetelmä vaan autentikointi tehdään käyttäen jotain monista eri EAP-menetelmistä, jotka voivat perustua käyttäjätunnuksiin ja salasanoihin tai digitaalisiin sertifikaatteihin.

Tietotekniikassa sertifikaatteja voidaan käyttää varmentamaan jonkin laitteen tai käyttäjän identiteetti. Tämä tapahtuu hyödyntämällä luotettavaa tahoa, joka allekirjoittaa kaikki jakamansa sertifikaatit. Sertifikaateilla pystytään myös salaamaan tietoa niin, että vain sertifikaatin haltija voi purkaa sille tarkoitetun tiedon. Tätä menetelmää käytetään usein salausavainten vaihtoon turvallisesti salaamattomien yhteyksien yli.

Tulevaisuudessa langattomista verkoista tulee yhä tärkeämpi osa yritysten muuta tietoverkkoa ja niistä halutaan käyttöön samat resurssit kuin langallisesta verkosta. Jo nykyään ja tulevaisuudessa lähes kaikilla on laitteita, joilla pystytään liittymään langattomiin verkkoihin. Yritysten verkkoon ei haluta mitä tahansa laitteita, jolloin laitteiden tietoturvallisen autentikoinnin merkitys tulee kasvamaan.

Asiasanat: 802.1x, RADIUS, EAP, PEAP, WLAN

Lahti University of Applied Sciences
Degree Programme in Information Technology

LÄTTI, TOMMI: Authentication in wireless networks

Bachelor's Thesis in telecommunications, 51 pages

Spring 2015

ABSTRACT

The goal of this thesis was to design port-based authentication for the new wireless network of the staff of the Päijät-Häme Social- and Health Care Group. Implementation of this network must be secure and user friendly. The chosen certificate based authentication method was implemented in the wireless network located at the Päijät-Häme Central Hospital in Lahti.

The first wireless network standard 802.11 was released in the year 1997. Original methods for user authentication and data encryption that came with 802.11 have been broken. To improve the security, the 802.11i standard was released in the year 2004. This standard also enables the use of port-based authentication in wireless networks.

Port-based authentication is also known by the name of 802.1x. It expanded the previously developed EAP protocol to be used in wired and wireless networks. EAP in itself is not an authentication method. Instead, authentication is done by one of many available EAP-methods that can be based on username and passwords or on digital certificates.

In computer science certificates can be used to verify the identity of some device or user. This is achieved by using trusted a entity, who signs all the certificates it deploys. Certificates can also be used to encrypt information so that only the certificate holder can decrypt the information intended for it. This method is often used to exchange encryption keys safely via unencrypted connections.

In the future, wireless networks will be an even more important part of the information network of organizations and often users want the same access from them to the internal resources as with wired networks. In the future almost everyone will have devices to connect to wireless networks. Corporations do not want any devices in their networks, which increases the importance of secure authentication of devices.

Key words: 802.1x, RADIUS, EAP, PEAP, WLAN

SISÄLLYS

1 JOHDANTO

Opinnäytetyön tarkoituksena on toteuttaa henkilökunnan käyttöön tarkoitetun langattoman verkon turvallinen autentikointi Päijät-hämeen sosiaali- ja terveysyhtymälle.

Yhä useampi työntekijä valitsee nykyään kannettavan tietokoneen pöytäkoneen sijasta, varsinkin jos työpäivän aikana tarvitsee tehdä töitä eri puolilta yhtymää. Kannettaville tietokoneille ei kuitenkaan ole Päijät-Hämeen keskussairaalassa siihen tarkoitettua langatonta verkkoa käytettävissä, jolloin verkkoyhteys on rajoitettu vain omiin työpisteisiin.

Päijät-Hämeen keskussairaala haluaa ottaa käyttöön uuden langattoman verkon olemassa olevaan infrastruktuuriin, jolla se voi tarjota henkilökunnalle mahdollisuuden työskennellä tarvittaessa eri alueilla keskussairaalan sisällä. Vaatimuksena verkolle on, että se toteutetaan tietoturvallisesti ja käyttäjäystävällisesti.

Työn teoriaosuudessa käydään läpi langattoman verkon standardit ja se, mitä alkuperäinen versio tarjosi tietoturvan osalta ja miten sitä on saatu parannettua 802.11i-standardin myötä. Lisäksi esitellään eri protokollat, jotka porttikohtainen autentikointi vaatii käytettäväksi. Lopuksi on vielä yleistä tietoa sertifikaateista, koska ne ovat keskeisessä osassa käyttäjän tunnistamisessa ja tunnistuspalvelimen luotettavuuden varmistamisessa.

2 WLAN

WLAN (Wireless Local Area Network), eli langaton lähiverkko, sai alkunsa kun 80-luvun puolivälissä Motorola esitteli ensimmäisen WLAN-tuotteensa. Tämä ja muut ensimmäiset langattomat lähiverkkoratkaisut sitoivat käyttäjänsä yhteen toimittajaan, jonka tuotteiden tulevaisuudesta ei ollut varmuutta. (Puska 2005, 15.)

IEEE (Institute of Electrical and Electronics Engineering) alkoi kehittämään ensimmäistä langattoman verkon standardia vuonna 1990. Langattoman verkon standardit päätettiin koota 802.11-tunnuksen alle ja ensimmäinen niistä julkaistiin 7 vuotta myöhemmin. Ensimmäisen version nopeudet olivat alhaiset, ja ongelmia aiheuttivat myös yhteensopivuus ja taajuuskaistojen käyttöluvat. 802.11 tarjosi kuitenkin hyvän rungon, josta kehitystä voitiin jatkaa eteenpäin. (Puska 2005, 15.)

Langattomilla verkoilla on nykyään useita eri käyttökohteita toiminnan tehokkuuden ja joustavuuden parantamiseksi. Useammissa sairaaloissa langattomat verkot on otettu käyttöön helpottamaan hoitotyötä. Verkot keskittyvät alueille, joilla on paljon potilaita, kuten vuodeosastot ja odotusaulat. Hoitohenkilökunta liikkuu työssään paljon, jolloin langattoman verkon tarjoamat mahdollisuudet päivittää ja tarkastella potilaiden tietoja paikasta riippumatta parantavat terveydenhuollon nopeutta ja tarkkuutta. (Geier 2005, 17.)

Langattomia verkkoja voidaan hyödyntää erilaisissa paikkatietopalve-luissa. Liikkuvien kohteiden paikannus mahdollistaa monia eri sovelluksia. Sairaaloissa paikkatietopalveluita voisi hyödyntää lääkärien ja hoitajien seuraamiseen. Hätätilanteissa osattaisiin kutsua oikeat henkilöt auttamaan. (Geier 2005, 23.)

Langattomien verkkojen ylläpidossa on omat haasteensa. Verkko hyödyntää yhteisiä taajuusalueita, joissa on käytössä muitakin sovelluksia. Vikatilanteiden, kuten häiriölähteiden, paikantamiseen tarvitaan monesti erikoistyökaluja ja erikoisosaamista. Vanhemmissa langattoman verkon

standardeissa nopeus oli heikko. Tukiaseman alueella käyttäjät joutuvat jakamaan yhteisen siirtotien, jolloin se voi ruuhkautua. (Puska 2005, 15.)

Langattoman verkon suunnittelussa täytyy huomioida monta seikkaa, kuten esteiden vaikutukset signaaliin. Ennen langattoman verkon käyttöönottoa kannattaa yleensä tehdä kuuluvuusmittaus. Kuuluvuusmittauksella saadaan suunnitteluhetkellä kuva ympäristön esteistä ja vaimennuksista. Radioaaltojen etenemisestä johtuvien ilmiöiden takia muutokset ympäristössä voivat vaikuttaa verkon toimintaan. Edellä mainitusta syystä WLAN-verkko voi jollain ajanhetkellä toimia luotettavammin kuin toisella. (Puska 2005, 21 - 22.)

2.1 Standardit

Kaikki 802.11-standardit toimivat ISM (Industrial Scientific Medical) -taajuusalueilla, jotka ovat 2,400 - 2,485 GHz ja 5,150 - 5,825 GHz. Näitä taajuusalueita saa käyttää vapaasti maakohtaisten rajoitusten ja laajennusten puitteissa. Osa näillä taajuusalueilla toimivista laitteista voi häiritä langattoman verkon toimintaa. (Granlund 2007, 293 - 294.)

Ensimmäinen langattoman lähiverkon standardi 802.11 käyttää 2.4 GHz:n taajuusaluetta. Se sisältää taajuushyppelyspektrin FHSS (Frequency-hopping spread spectrum) ja suorasekvenssihajaspektrin DSSS (Direct-sequence spread spectrum) fyysiset kerrokset. 802.11:n maksiminopeus on vain 2 Mbps molemmilla fyysisen kerroksen modulaatiolla. (Geier 2005.)

Vuonna 1999 IEEE julkaisi 802.11a- ja 802.11b-standardit. 802.11a on ensimmäinen standardi 5 GHz:n taajuusalueella, ja se on huomattavasti nopeampi kuin 802.11 ja 802.11b. 54 Mbps enimmäisnopeuden mahdollistaa monikantoaaltomodulointi OFDM (Orthogonal frequency-division multiplexing). (Geier 2005, 124.)

802.11b-standardi toimii 2,4 GHz:n taajuusalueella, ja siinä voidaan käyttää 14:ää eri kanavaa 20 MHz:n kaistanleveydellä. 802.11b on

yhteensopiva alkuperäisen 802.11-standardin kanssa fyysisen kerroksen DSSS:n käytön takia. 802.11b maksiminopeus on vain 11 Mbps, mikä rajoittaa sen käyttökohteita. Sen etuna 802.11a:han verrattuna on parempi kantama. (Geier 2005, 126.)

802.11g julkaistiin 2003, ja se toimii 802.11:n ja 802.11b:n tavoin 2,4 GHz:n taajuusalueella. Yhteistä sillä on 802.11a:n kanssa OFDM-modulaatio, joka nostaa 802.11g:n siirtonopeuden 54 Mbps asti. Merkittävä etu on yhteensopivuus 802.11b-standardin kanssa samanaikaisesti. 802.11b-päätelaite 802.11g-verkossa aiheuttaa sen, että muutkin uudemmat 802.11g-laitteet toimivat silloin hitaamman 802.11b-laitteen nopeudella. (Geier 2005, 127.)

Vuoden 2004 alussa perustettiin työryhmä kehittämään uutta nopeampaa langattoman lähiverkon standardia nimeltä 802.11n. Nopeuden kasvu perustuu MIMO-antennitekniikkaan (Multiple Input Multiple Output). Lähettimessä ja vastaanottimessa on käytössä useampia antenneja. (Granlund 2007, 305.)

802.11n käyttää myös OFDM-modulaatiota ja se on yhteensopiva 802.11g:n ja 802.11a:n kanssa, eli se voi toimia 2,4 GHz:n ja 5 GHz:n taajuusalueilla. Samalla tavalla kaikkien laitteiden linkin nopeus putoaa kuitenkin hitaimman laitteen tasolle, jos verkon alueella on niitä. 802.11n mahdollistaa tuplasti leveämmän kaistanleveyden käytön verrattuna aikaisempiin standardeihin. 802.11n toi mukanaan sanomien yhdistämisen. Lähetettävien pakettien otsikkotietoa saadaan vähennettyä yhdistämällä useamman kehyksen sisältö saman otsikkotiedon alle. 802.11n maksiminopeus on 600 Mbps. (National Instruments 2013.)

802.11n:n on mahdollista käyttää 40 MHz leveätä taajuuskaistaa. Tämä lisää verkon suorituskykyä mutta vähentää rinnakkaisten kanavien määrää. 2,4GHz:n taajuusalueelle mahtuu vain yksi 40 MHz:n kanava ilman päällekkäisyyttä. 40 MHz:n kaistanleveyttä onkin suositeltavaa käyttää vain 5 GHz:n taajuuskaistalla, jossa on enemmän tilaa. (National Instruments 2013.)

802.11ac on viimeisin valmis langattoman verkon standardi. 802.11a:n tapaan se toimii ainoastaan 5 GHz:n alueella. 802.11ac nostaa langattoman verkon nopeutta käyttämällä 256 QAM modulaatiota. Kaistanleveyttä on mahdollista kasvattaa aina 160 MHz:iin asti. Ensimmäiset 802.11ac-standardiin perustuvat laitteet pystyvät 433 - 1300 Mbps siirtonopeuksiin. (Cisco 2014.)

Langattomissa verkoissa on hyvä huomioida, ettei linkin nopeus vastaa todellista siirtonopeutta. Erilaiset aikaviiveet kehysten välillä ja eri verkkokerroksilla olevat otsikkotiedot vähentävät hyötykuorman määrää jokaisessa paketissa. Yleisesti langattoman verkon todellinen nopeus on noin puolet linkin nopeudesta (Puska 2005, 103 - 104.)

2.2 Tietoturva

Langaton verkko käyttää radiotaajuuksia siirtotienään. Tästä syystä verkkoja ei voida rajata tietyille alueille, kuten rakennusten sisälle. Tämä mahdollistaa verkon kuuntelun ja häiritsemisen ulkopuolelta. 802.11:n yhteydessä esitelty WEP (Wired Equivalent Privacy) yrittää tarjota mekanismit tiedon luottamuksellisuutta, eheyttä ja päätelaitteen autentikointia varten. (Puska 2005, 65.)

Jo 802.11:n suunnitteluvaiheessa WEP:n käyttämästä RC4 algoritmista julkaistiin tutkimus, jonka perusteella siinä oli haavoittuvuus. Tästä huolimatta 802.11 julkaistiin käyttäen RC4-salausta. WLAN-verkkojen yleistyessä huoli tietoturvasta kasvoi ja vuonna 2000 julkaistiin muutamia tutkimuksia siihen liittyvistä ongelmista. Vuosi 2001 oli WEP:n luotettavuuden loppu, kun se saatiin murettua kokonaan. 2004 tuli ensimmäiset vapaasti saatavilla olevat työkalut WEP-salausta käyttävien verkkojen murtamiseen. (Lehembre 2005.)

2001 julkaistiin 802.1x-standardi, joka mahdollistaa porttikohtaisen tunnistuksen. Eri laitevalmistajat yrittivät sen avulla paikata WEP-ongelmia. 802.1x oli suunniteltu käytettäväksi langallisten verkkojen kanssa, mikä aiheutti ongelmia sen käytössä langattomissa verkoissa.

Kaikkien näiden ongelmien ratkaisuun kehitettiin 802.11i-standardi, joka pohjautuu 802.1x:ään ja lisää siihen langattomissa verkoissa tarvittavia ominaisuuksia. Tärkein näistä on dynaaminen avaintenhallinta, jolla korvataan WEP käyttämät staattiset avaimet. 802.11i korjaa myös WEP-salaukseen liittyvät ongelmat. (Gast 2002.)

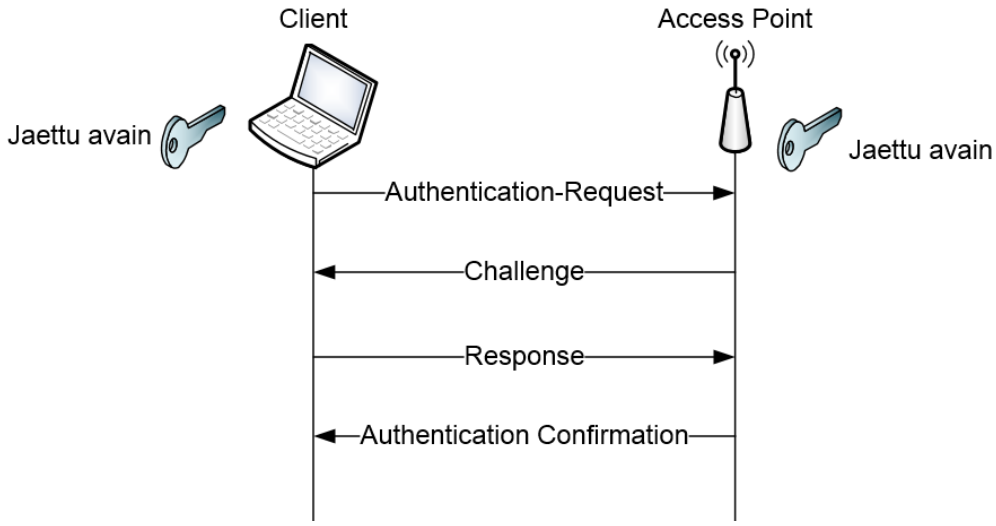
2.3 WEP

WEP käytti alun perin 40-bittistä avainta, jota käytetään tiedon salauksessa ja autentikoinnissa. Myöhemmin avaimen pituus kasvatettiin 104 bittiin. WEP:n käyttämässä RC4-jonosalauksessa salausavaimen ja salattavan tiedon pituus on sama. Jokainen WEP:llä salattu viesti sisältää satunnaisen 24 bitin alustusvektorin. Tämä alustusvektori lähetetään selväkielisenä jokaisessa kehyksessä. (Puska 2005, 80.)

RC4 salausalgoritimilla luodaan kiinteän mittaisesta 40- tai 104-bittisestä salausavaimesta ja 24-bittisestä alustusvektorista jokaista salattavaa kehystä varten salattavan tiedon mittainen merkkijono. Tälle merkkijonolle ja salattavalle tiedolle tehdään XOR-operaatio, jonka lopputulos on salattu data. Salauksen purkua varten tarvitaan tieto alustusvektorista, joka alun perin liitettiin salausavaimeen RC4 vaiheessa. Tämä alustusvektori liitetään salatun kehyksen alkuun. (Puska 2005, 81.)

WEP:n heikkouksina on liian pieni osoiteavaruus alustusvektorissa. Eri vaihtoehtoja on vain 16 777 216 kappaletta. Osa näistä on heikompia kuin muut, ja niitä voidaan käyttää murrettaessa salausavainta. Salakuuntelemalla liikennettä voidaan saada kaapattua näitä heikkoja alustusvektoreita. Samat avaimet joudutaan määrittelemään kaikkiin käytettäviin laitteisiin, ja ne ovat luettavissa selväkielisinä. Avaimen paljastuessa on mahdotonta vaihtaa uusi avain samanaikaisesti kaikkiin laitteisiin ilman käyttökatkoa. Kaikkien verkossa olevien laitteiden liikenne on salattu samalla avaimella. Salausavaimet ovat liian lyhyitä tarjotakseen riittävän hyvän tietoturvan. (Puska 2005, 81.)

Tätä samaa avainta käytetään päätelaitteen tunnistuksessa. Kuviossa 1 on kuvattu WEP-autentikointi. Autentikointi perustuu haaste – vastaus-menetelmään, jossa tukiasema lähettää päätelaitteelle salattavan merkkijonon. Päätelaite salaa merkkijonon siihen määritellyllä avaimella ja lähettää salatun merkkijonon tukiasemalle. Tukiasema purkaa viestin ja vertaa, vastaako sen sisältö alkuperäistä viestiä. Jos viesti on sama, tiedetään, että päätelaitteella on käytössä sama avain. (Puska 2005, 75.)



KUVIO 1. WEP-autentikointi (muokattu lähteestä Puska 2005, 75)

Eri valmistajat yrittivät korjata WEP-tietoturvaa 802.1x:n avulla. 802.1x-standardissa päätelaite autentikoidaan käyttämällä erillistä tunnistuspalvelinta ja siihen tarkoitettuja protokollia. Autentikoinnin yhteydessä pystytään luomaan joka kerralla eri WEP-salausavain. WEP-salausavainta voidaan myös vaihtaa määräajoin, jolloin sen paljastumiselta vältytään. 802.1x ei kuitenkaan korjaa muita WEP:n ongelmia. (Puska 2005, 75.)

2.4 WPA

WEP tietoturvaongelmien takia IEEE aloitti kehittämään uutta 802.11i standardia. Wi-Fi Alliance otti sen hetkisen version 802.11i-standardista ja nimesi sen WPA:ksi (Wi-Fi Protected Access). 802.11i-standardi pohjautuu 802.1x-standardiin, joka määrittelee EAP-protokollan käytön

lähiverkoissa. EAP-protokolla sopi hyvin käytettäväksi autentikointiviestien välitykseen. 802.11i sisälsi myös TKIP:n (Temporal Key Integrity Protocol) ja Michael algoritmin parantamaan tietoturvaa. Wi-Fi alliancen vaatimus WPA:lle oli yhteensopivuus jo markkinoilla olevien laitteiden kanssa ohjelmistopäivitysten kautta. Näin ollen alkuperäinen RC4-salaus jäi käyttöön, jonka ympärille rakennettiin tietoturvaparannukset. (Geier 2005.)

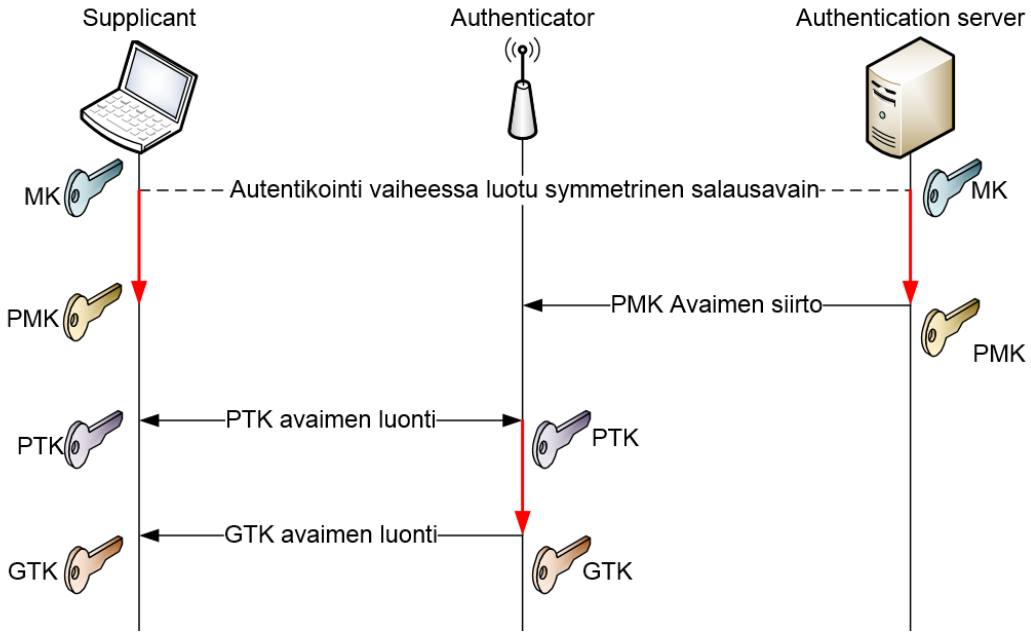
Varsinkin kotikäyttäjillä ei monesti ole käytettävissä erillistä tunnistuspalvelinta, joten WPA:sta luotiin 2 eri versiota: WPA-Personal ja WPA-Enterprise. WPA-Personal hyödyntää autentikointiin esijaettua avainta, joka määritellään kaikissa verkon laitteissa, kun taas WPA-Enterprise käyttää 802.1x:n määrittämiä komponentteja. (Geier 2005, 131.)

WPA:n käyttämä TKIP mahdollistaa jokaisen kehyksen salaamisen eri 128-bittisellä avaimella. Heikkojen alustusvektoreiden ongelmien poistamiseksi alustusvektorin pituus on TKIP:ssa kasvatettu 48 bittiin. Sanoman eheyden tarkistukseen käytetään MIC (Message Integrity Check) -kenttää. TKIP:ssa käytettävä kehyskohtainen salausavain muodostetaan käyttäen päätelaitteen MAC-osoitetta, joten se on yksilöllinen verkossa. TKIP:ssa perusavain vaihdetaan 10 000 paketin välein. TKIP lisää myös jokaiseen pakettiin järjestysnumeron estämään toistohyökkäyksiä. (Puska 2005, 82.)

802.11i-standardin avaintenhallinta perustuu avainpareihin. Tukiasema ja päätelaite salaavat liikenteen parittaisella lähetysavaimella PTK (Pairwise Transient Key), joka on istuntokohtainen. WPA-Enterprise-autentikoinnissa pääavain MK (Master Key) luodaan autentikointiprosessin aikana tunnistuspalvelimen ja päätelaitteen välille. Sekin on päätelaitekohtainen. Pääavaimesta luodaan kaikki muut salaukseen ja tiedon eheyteen tarvittavat avaimet. (Puska 2005, 84.)

Kuviossa 2 on esitetty avaimien luomisen vaiheet. Päätelaitteen autentikoinnin jälkeen pääavaimesta luodaan parittainen yleisavain PMK (Pairwise Master Key). Päätelaite ja tunnistuspalvelin luovat avaimet

autentikoinnin aikana. Käytetty EAP-menetelmä määrittelee miten avain luodaan. Avain lähetetään tukiasemalle liikenteen salausta varten. Parittaisesta yleisavaimesta luodaan parittainen tilapäisavain nelivaiheisen kättelyn tuloksena. PTK pilkotaan osiin, josta saadaan avaintenvaihdon vahvistus avain KCK (Key Confirmation Key), avaintenvaihdon salausavain KEK (Key Encryption Key) ja tilapäisavain TK (Temporal Key). TK-avain on PTK-avaimen bitit 256 – 383, ja sitä käytetään varsinaisen lähetettävän tiedon salaamisessa. Viimeisenä tukiasema luo ryhmälähetysavaimen GTK (Groupwise Transmit Key) ja lähettää sen päätelaitteelle salattuna KEK avaimella. (Puska 2005, 84.)



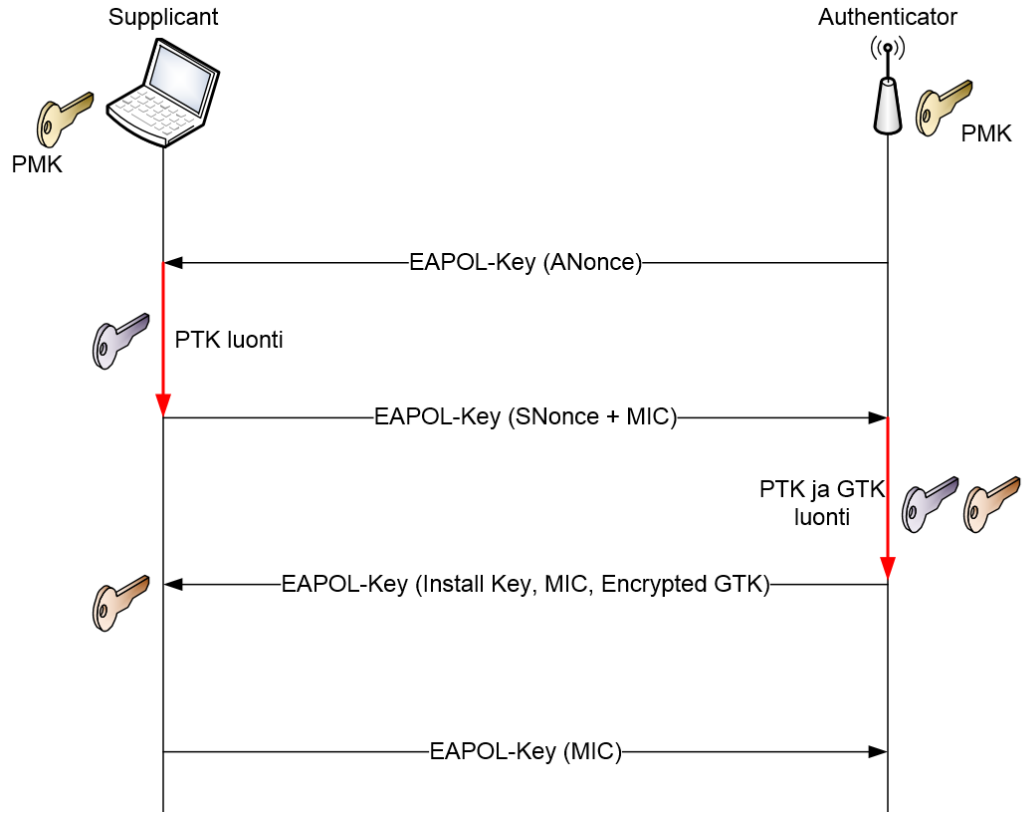
KUVIO 2. Avaimien siirto ja luonti (muokattu lähteestä Strand 2004)

WPA-Personal on suunniteltu käytettäväksi ilman tunnistuspalvelinta. Se tunnistaa päätelaitteen ennalta jaetun avaimen perusteella. Avaimen tulee olla vähintään 8 merkkiä pitkä ja maksimissaan 63 merkkiä. Aiemmin esitetyn PTK-luonnin yhteydessä pystytään varmentamaan, tietääkö päätelaite oikean jaetun avaimen. (IEEE 802.11i 2004.)

Tunnistuspalvelimen puuttumisen vuoksi pääavainta ei voida luoda autentikoinnin yhteydessä vaan se pitää tehdä muulla tavoin. Tähän käytetään samaa salasanaa, jolla autentikoidutaan verkkoon. 256-bittinen

PMK muodostetaan 8 - 63 merkkisestä salasanasta PBKDF2:n (Password-Based Key Derivation Function 2) avulla. (IEEE 802.11i 2004.)

WPA käyttää PBDKF2:ta niin, että siihen syötetään salasana, verkon nimi ja sen pituus. Lopputuloksena on 256-bittinen merkkijono. Avainten murtamisen vaikeuttamiseksi PBDKF2 sisältää arvon, jolla määritellään, montako kierrosta sen käyttämää tiivistefunktiota suoritetaan. 802.11i-standardissa on määritelty, että prosessi toistetaan 4096 kertaa. Tällä saadaan aikaan laskennallista kuormaa avaimen luontiin. Käyttäjä ei huomaa viivettä, jos PMK-laskennassa operaatio suoritetaan 4096 kertaa, mutta salasanaa arvattaessa täytyy jokaista yritystä varten laskenta suorittaa. (IEEE 802.11i 2004.)



KUVIO 3. 4-vaiheinen dynaamisten avainten luonti (muokattu lähteestä 802.11i 2004)

Kuviossa 3 on esitetty, miten PTK-avain luodaan ja miten sillä tunnistetaan käyttäjä. Tukiasema lähettää ensin ANoncen. ANonce on satunnainen merkkijono, jonka tukiasema luo istuntokohtaisesti. ANonce lähetetään

EAPOL-Key-viestissä päätelaitteelle. Seuraavaksi päätelaite luo oman satunnaisen merkkijonon SNoncen. PTK luodaan ANoncen, SNoncen, tukiaseman MAC-osoitteen ja päätelaitteen MAC-osoitteen perusteella. Näin ollen siitä tulee yksilöllinen salausavain kyseiselle istunnolle. Päätelaite luo oman PTK:n ja lähettää SNoncen tukiasemalle. Samalla se laskee koko EAPOL-paketille MIC arvon, joka on liitetty myös viestiin. Tukiasema ottaa SNoncen ja luo samalla tavalla PTK:n ja muut avaimet. Sen jälkeen se laskee vastaanotetulle EAPOL-paketille tarkistussumman KCK-avaimen avulla. Jos tarkistussummat täsmäävät päätelaitteelta saadun arvon kanssa, tukiasema tietää, että käytössä on sama alkuperäinen salasana. Muussa tapauksessa yhteys katkaistaan. Seuraavaksi se luo ryhmälähetysavaimen ja salaa sen käyttäen yhteistä PTK-avainparia. Lopuksi päätelaite kuittaa, että se on ottanut avaimet käyttöönsä ja liikennöinti verkossa voi alkaa. (IEEE 802.11i 2004.)

WPA-Personalin ongelmana on yhteinen salausavain. Kaikkien verkon käyttäjien tulee tietää avain, ja se on myös päätelaitteiden muistista luettavissa. Kaappaamalla EAPOL-Key-viestit, joissa on ANonce ja SNonce, voi kyseisen laitteen ja tukiaseman välisen liikenteen salauksen purkaa. Tästä syystä se ei oikein sovellu käytettäväksi isoissa yrityksissä. (Lehembre 2005.)

2.5 WPA2

Vuonna 2004 julkaistu 802.11i määrittelee aikaisemmin WPA:n yhteydessä esiteltyjen avaintenhallinnan ja TKIP-protokollan lisäksi AES (Advanced Encryption Standard) -salauksen käytön yhdessä CCMP:n kanssa (Counter Mode Encryption with CBC-MAC Data Origin Authenticity Protocol). AES-salaus on huomattavasti raskaampaa kuin RC4, ja se vaatii tuen päätelaitteissa. Näin ollen vanhemmat WEP ja WPA tukevat laitteet eivät toimi WPA2:n kanssa edes ohjelmistopäivityksillä. (Granlund 2007, 321.)

WPA2-salaus käyttää WEP:n ja WPA:n tavoin myös alustusvektoreita, kuitenkin niin, että se vaihtuu jokaisella sanomalla. Kertaalleen käytettyä alustusvektoria ei käytetä uudestaan. WPA2:ssa käytetty AES-salaus tuottaa 128-bittisiä lohkoja, joita käytetään jonosalauksen tavoin ottamalla salattavasta tiedosta kerralla joukko, joka salataan AES:lla. Salattujen lohkojen eheyden varmistamiseen käytetään CCMP:aa. Sen lisäksi, että kaikkia lohkoja käytetään viestin tarkistussumman laskemiseen, niitä myös ketjutetaan ja luodaan riippuvuuksia. (Granlund 2007, 322.)

WPA2:ssa voidaan käyttää samalla tavalla tunnistuspalvelinta tai ennalta jaettua avainta, kuten WPA:ssa. WPA2:n ja AES:n käyttö on pakollista, jos halutaan hyödyntää 802.11n-verkkoa maksiminopeudella. Tukiasema voi tukea WPA:a ja WPA2:a samanaikaisesti, mutta jos alueelle tulee yksikin ainoastaan WPA:n tukema asiakas, nopeus pudotetaan 802.11a:n tai 802.11g:n tasolle riippuen käytössä olevasta taajuusalueesta. (Juniper 2013.)

3 PORTTIKOHTAINEN AUTENTIKOINTI

Porttikohtaisella autentikoinnilla estetään liikennöinti verkossa ennen autentikointia. Yrityksissä tietoverkkoihin halutaan yleensä estää pääsy muilta kuin omilta tai muilta hyväksytyiltä laitteilta varsinkin langattomissa verkoissa. Porttikohtainen autentikointi tehdään yleensä käyttäen salasanoja tai sertifikaatteja. (Taylor & Francis Group 2006.)

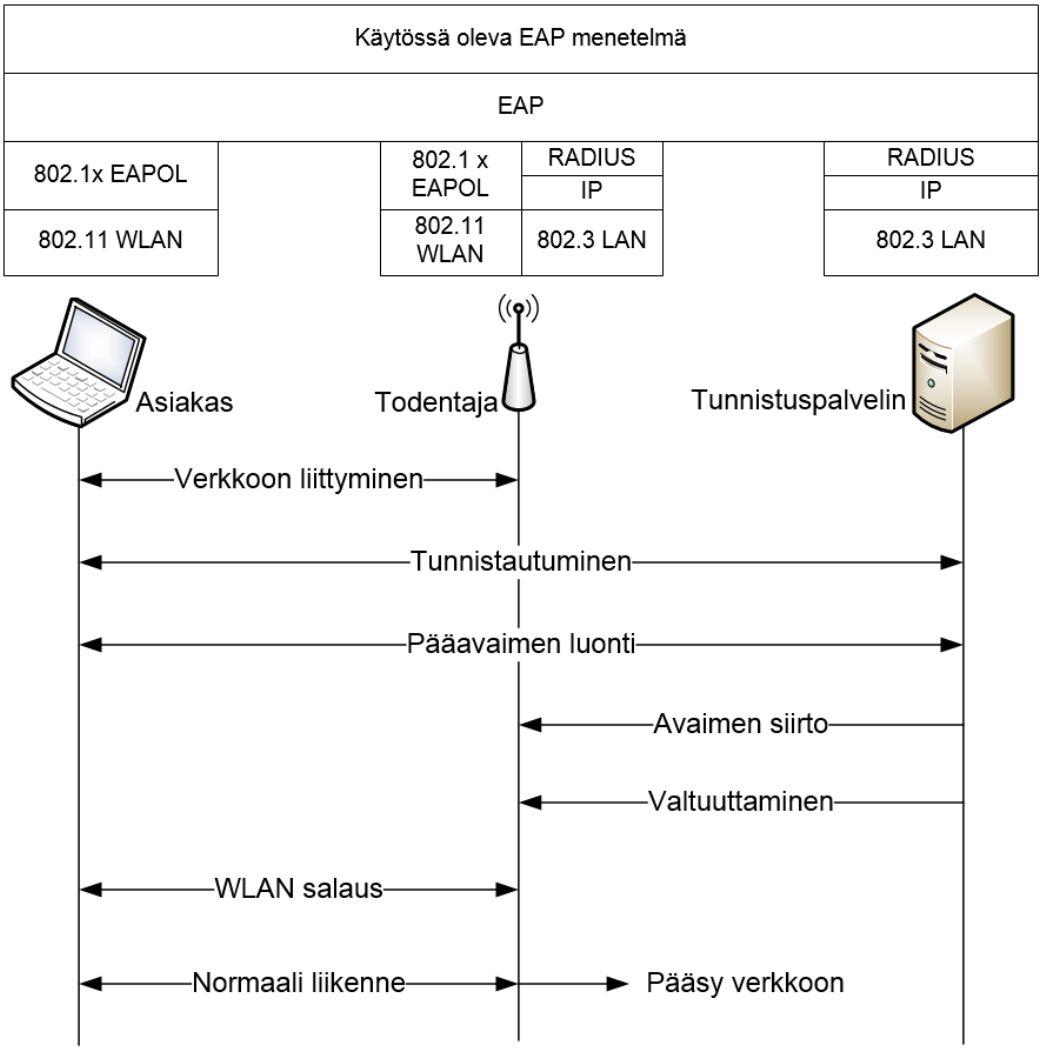
Porttikohtainen autentikointi tunnetaan myös nimellä 802.1x. Siihen liittyy kuitenkin muitakin protokollia. Porttikohtaiseen autentikointiin liittyy kolme komponenttia, jotka ovat 802.1x, joka mahdollistaa päätelaitteen ja tukiaseman keskustelun, itse menetelmät varsinaiseen autentikointiin ja viimeiseksi tunnistuspalvelimen, joka valtuuttaa tai estää käyttäjän pääsyn verkkoon. (Taylor & Francis Group 2006.)

3.1 802.1x

802.1x on IEEE 802 -protokollan laajennus, ja se toimii OSI-mallin siirtoyhteyskerroksella. Tämä mahdollistaa sen käytön langallisissa ja langattomissa lähiverkoissa. 802.1x laajentaa EAP (Extensible Authentication Protocol) -protokollan käytön näihin verkkoihin. Tästä käytetään yleisesti nimitystä EAPOL (Extensible Authentication Protocol over LAN). EAPOL on hyvin yksinkertainen protokolla, joka on käytössä pelkästään porttikohtaisessa autentikoinnissa. Tiedonsiirto tapahtuu kahdella erityyppisellä viestillä, joita ovat pyynnöt ja vastaukset. Näitä välitetään asiakkaan ja todentajan välillä. Riippuen tunnistuksen onnistumisesta käytetään Success- ja Failure-viestejä kertomaan se asiakkaalle. Lisäksi on olemassa muutama muu viestityyppi kuten, EAPOL-Key, jota käytetään salausavainten yhteydessä. (Taylor & Francis Group 2006.)

802.1x määrittää seuraavat komponentit, joita käytetään autentikoinnissa. Nämä ovat asiakas, jolla tarkoitetaan päätelaitteen sisältämää ohjelmistoa verkkoon liittymiseksi, todentaja, joka kontrolloi pääsyä verkkoon estämällä muun kuin EAP-liikenteen ennen autentikointia. Viimeisenä on

tunnistuspalvelin, joka varmistaa, onko asiakkaalle oikeutta käyttää verkkoa. (Puska 2005, 75.)



KUVIO 4. 802.1x:n toimintaperiaate langattomassa verkossa (muokattu lähteestä Microsoft 2004)

Kuviossa 4 on esitetty, miten 802.1x toimii langattomassa verkossa. Ensin asiakas liittyy verkkoon ilman salausta. Todentaja estää muun kuin EAP-liikenteen, jota se välittää asiakkaan ja tunnistuspalvelimen välillä. Autentikointi suoritetaan käyttäen jotain monista eri EAP-menetelmistä. Autentikoinnin yhteydessä luodaan salausavain. Salausavain täytyy välittää todentajalle, koska monesti se luodaan salatussa tunnelissa, jonka sisältöä todentaja ei näe. Tunnistuspalvelin valtuuttaa todentajan päästämään asiakkaan verkkoon. Asiakas ja todentaja neuvottelevat

istuntokohtaiset WLAN-salausavaimet, minkä jälkeen normaali liikennöinti verkossa alkaa. Kuvioon on piirretty lisäksi yleisimmin käytetyt protokollat porttikohtaisen autentikoinnin kanssa. (Microsoft 2004.)

3.2 RADIUS

RADIUS (Remote Authentication Dial In User Service) mahdollistaa keskitetyn käyttäjän autentikoinnin, valtuutuksen ja tilastoinnin. Alun perin se on ollut käytössä sisäänsoittoyhteyksissä. Myöhemmin RADIUS:n käyttö on laajentunut VPN-yhteyksiin, palvelimiin, langattomiin verkkoihin, lähiverkon aktiivilaitteisiin ja muualle. RADIUS toimii UDP-protokollalla ja käyttää porttia 1812 autentikointiin sekä porttia 1813 tilastointiin. (Microsoft 2002.)

Autentikointi RADIUS:a hyödyntäen vaatii todentajan lisäämisen etukäteen RADIUS-palvelimelle asiakkaaksi käyttäen yhteistä avainta ja todentajan IP-osoitetta. Tämä avain ja RADIUS-palvelimen IP-osoite tulee määrittää myös todentajan asetuksissa. Avainta ei koskaan lähetetä verkossa. Samalla avaimella salataan RADIUS-palvelimelle mahdollisesti lähetettävät käyttäjien salasanat. Avainta voidaan käyttää myös RADIUS-viestien sisällön muuttumattomuuden varmistamiseen. (Microsoft 2002.)

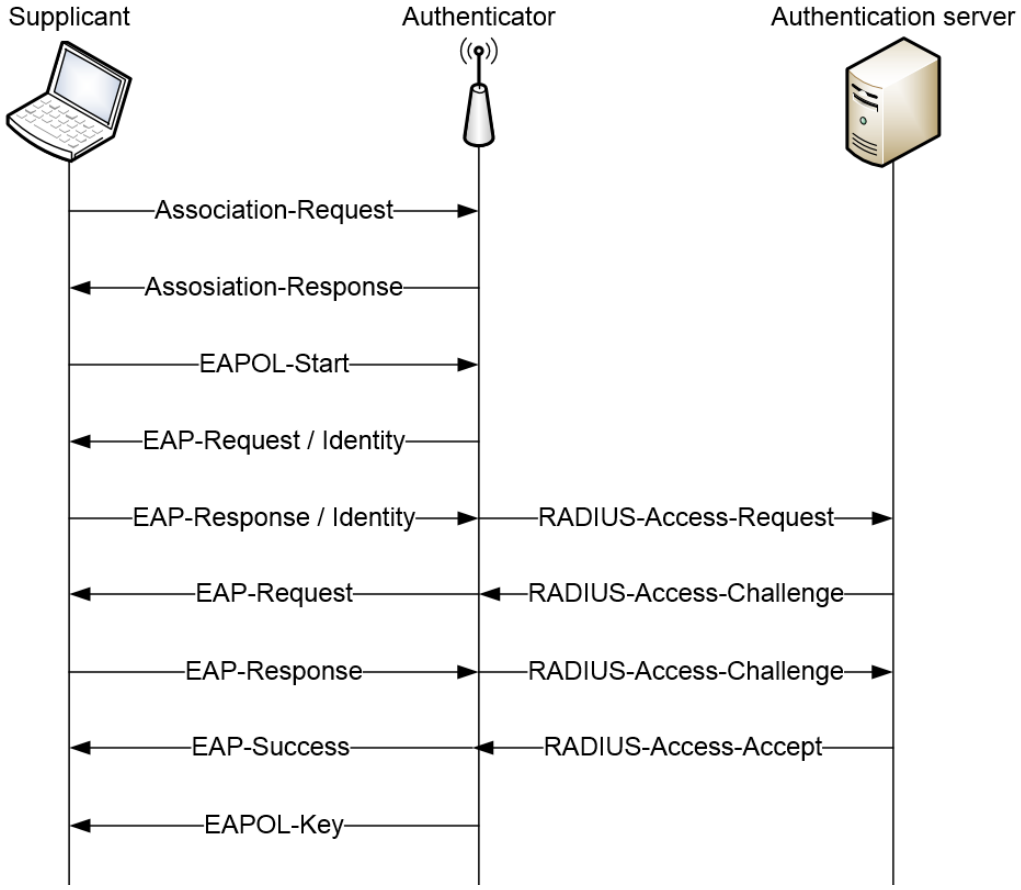
RADIUS-autentikoinnissa on kolme osapuolta: asiakas, todentaja ja itse RADIUS-palvelin. Asiakas on jokin laite, joka haluaa pääsyn verkkoon. Todentaja vastaa asiakkaan viestien uudelleen paketoimisesta RADIUS-viestityyppien sisään. Todentaja paketoi RADIUS-palvelimen vastausviestit vastaavasti takaisin asiakkaan ja todentajan välissä käytettävään protokollaan. RADIUS-palvelin varmistaa, onko kyseisellä laitteella lupa käyttää verkkoa vai ei ja sen perusteella valtuuttaa tai estää käytön. (Cisco 2006.)

3.3 EAP

EAP (Extensible Authentication Protocol) kehitettiin alun perin PPP:n (Point-To-Point Protocol) kanssa käytettäväksi. EAP-protokolla ei vaadi mitään tiettyä siirtoyhteysprotokollan käyttöä vaan riittää, että yhteys täyttää point to point -yhteyksien topologian. Yksittäiset yhteydet lähiverkoissa tietokoneen ja kytkimen portin välillä tai langattoman päätelaitteen ja tukiaseman loogisen portin ovat hyvin paljon point to point -yhteyksien kaltaisia. 802.1x-standardi laajentaa EAP:n käytön 802-lähiverkkoihin. (Taylor & Francis Group 2006.)

EAP ei itsessään ole mikään tunnistusmenetelmä vaan määrittelee protokollassa käytettävät viestityypit ja paketin rakenteen EAP-menetelmien käytettäväksi. Sertifikaatteihin tai salasanoihin perustuvaan käyttäjien tunnistukseen on kehitetty eri EAP-menetelmiä. EAP-menetelmiä on myös tunneleiden luomiseksi näiden tietojen välittämiseen turvallisesti. Kaikki nämä toimivat samojen EAP:n määrittelemien viestien sisällä. (Taylor & Francis Group 2006.)

Vaikka minkä tahansa EAP-menetelmän käyttö on teoriassa mahdollista, täytyy huomioida, että kaikki niistä eivät sovellu käytettäväksi langattomien verkkojen kanssa. Käytetyn EAP-menetelmän täytyy sopeutua käytettäväksi ilman salattua siirtotietä autentikointivaiheessa ja pystyttävä luomaan sen aikana salausavain myöhemmän yhteyden suojaamiseksi. Yleisimmät langattomien verkkojen kanssa käytettäväksi soveltuvat EAP-menetelmät ovat EAP-TLS, PEAP, EAP-TTLS ja LEAP. Näistä Microsoft tukee PEAP- ja EAP-TLS-menetelmiä. (Microsoft 2004.)



KUVIO 5. EAP-liikenne (muokattu lähteestä Puska 2005, 76)

Kuviossa 5 on esitetty, miten EAP-liikenne toimii langattomissa verkoissa (Puska 2005, 76).

1. Päätelaite liittyy tukiasemaan käyttäen langattoman verkon avointa autentikointia. Tukiasema ei välitä muuta kuin EAP-liikennettä ennen päätelaitteen autentikoinnin onnistumista.
2. Päätelaite aloittaa EAP-keskustelun lähettämällä EAPOL-Start-sanoman. Tukiasema kysyy päätelaitteelta sen käyttäjätietoja, johon käyttäjä vastaa oman käyttäjätunnuksen ja salasanan. Varsinaista salasanaa ei lähetetä vaan siitä laskettu tiiviste. Tukiasema tarkistaa, pitääkö kyseinen käyttäjä tunnistaa.
3. Tukiasema muuttaa EAP-viestin RADIUS-pyynnöksi ja lähettää EAP-sanoman RADIUS-viestin sisällä.
4. Tunnistuspalvelin vastaa RADIUS-Access-Challenge-viestillä, joka sisältää satunnaisen merkkijonon.
5. Merkkijono välitetään päätelaitteelle EAP-viestin sisällä.

6. Päätelaite salakirjoittaa merkkijonon ja lähettää sen EAP-vastausviestinä, jonka tukiasema muuntaa jälleen RADIUS-viestiksi.
7. RADIUS salaa aiemmin lähettämänsä merkkijonon sen tietämällä käyttäjän salasanalla ja vertaa sitä äsken saamaansa merkkijonoon. Mikäli merkkijonot täsmäävät, lähettää RADIUS-palvelin Access-Accept-viestin, jonka tukiasema muuntaa EAP-Success-viestiksi ja lähettää sen edelleen päätelaitteelle. RADIUS-palvelimen lähettämä viesti sisältää myös verkossa käytettävän salausavaimen.
8. Tukiasema alkaa välittää muutakin langattoman verkon liikennettä eteenpäin.

3.3.1 EAP-TLS

802.1x kehitettiin alun perin langallisiin lähiverkkoihin, jolloin tietojen salaaminen autentikoinnissa ei ollut välttämätöntä vaikeamman salakuuntelun takia. Langattomissa verkoissa tarvitaan kuitenkin menetelmät tiedon salaamiseen. Verkkoon liittyvien laitteiden on pystyttävä varmistamaan tunnistuspalvelimen luotettavuus, ettei käyttäjän tietoja tai liikennettä yritetä kaapata käyttämällä luvattomia tukiasemia. Nämä vaatimukset pystytään täyttämään IETF:n (Internet Engineering Task Force) kehittämällä TLS (Transport Layer Security) -protokollalla. (Gast 2002.)

EAP-TLS mahdollistaa kaksisuuntaisen autentikoinnin asiakkaan ja tunnistuspalvelimen välillä käyttämällä sertifikaatteja. Tunnistus alkaa palvelimen lähettäessä ensin asiakkaalle oman sertifikaattinsa. Asiakas lähettää oman sertifikaattinsa palvelimelle vasta kun se on ensin varmistanut palvelimen sertifikaatin. Palvelin tunnistaa asiakkaan sertifikaatin sisältämien tietojen perusteella. (Gast 2002.)

Langattomissa verkoissa sertifikaattien vaihto suoritetaan selväkielisenä, jolloin liikennettä seuraamalla pystytään saamaan tietoja asiakkaasta.

EAP-TLS on työläs ottaa käyttöön, koska se vaatii sertifikaatit asiakkaille. Menetelmän käyttö vaatii sertifikaattipalvelimen, josta sertifikaatteja jaetaan käsin tai automaattisesti. (Gast 2002.)

3.3.2 EAP-TTLS ja PEAP

TTLS- (Tunneled Transport Layer Security) ja PEAP (Protected EAP) EAP-menetelmät kehitettiin helpottamaan porttikohtaisen autentikoinnin käyttöönottoa ympäristöissä, joissa ei ole välttämättä sertifikaattipalvelinta. Käyttäjän tunnistukseen riittää monesti yksinkertaisemmat menetelmät, kuten käyttäjätunnus ja sitä vastaava salasana. Salasanoihin perustuvien EAP-menetelmien käyttö langattomissa verkossa ei ole turvallista ilman vahvaa salausta. (Gast 2002.)

Molemmat EAP-menetelmät toimivat kaksivaiheisesti. Ensimmäinen vaihe on molemmissa sama. Siinä luodaan suojattu tunneli asiakkaan ja tunnistuspalvelimen välille. Palvelimen sertifikaatilla asiakas pystyy jälleen varmentamaan verkon luotettavuuden. Toisessa vaiheessa PEAP:n tapauksessa asiakkaan autentikointitiedot välitetään tunnelissa palvelimelle käyttäen jotain muuta EAP-menetelmää, kuten EAP-TLS:a. EAP-TTLS:n kanssa on mahdollista käyttää muitakin kuin EAP-menetelmiä. EAP-TTLS:n käyttö ei ole suoraan tuettuna Microsoft Windows-käyttöjärjestelmillä. (Microsoft 2004.)

Tunneloitujen EAP-menetelmien kanssa käytettäväksi Microsoft on kehittänyt MSCHAPv2 (Microsoft Challenge-Handshake Authentication Protocol version 2) -protokollastaan EAP:n kanssa toimivan version. Protokolla mahdollistaa asiakkaan autentikoinnin käyttäjätunnuksella ja salasanalla. MSCHAPv2 toimii haaste-vastaus-menetelmällä, ja autentikoinnin aikana myös asiakas varmistaa, että tunnistuspalvelin tietää sen salasanan. (Microsoft 2005.)

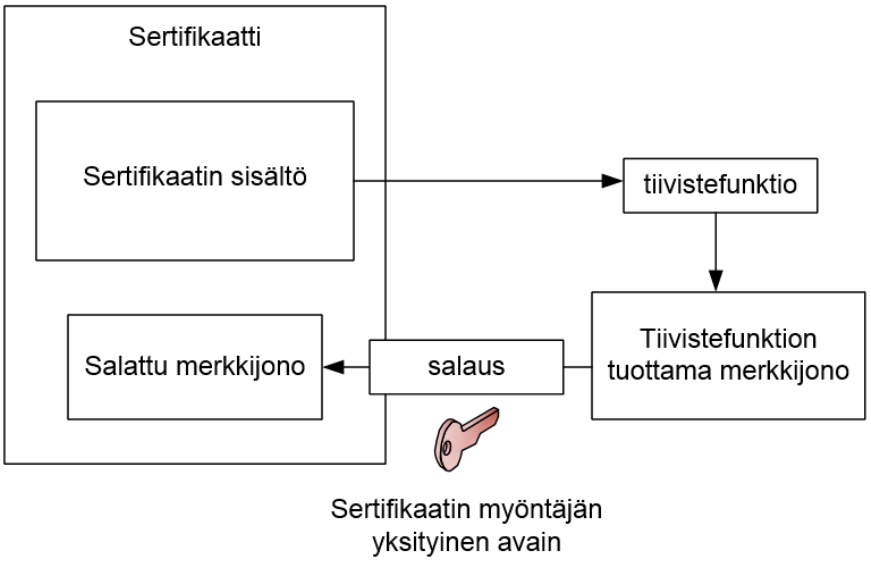
Toinen mahdollisuus on käyttää EAP-TLS-autentikointia tunneloitujen EAP-menetelmien toisessa vaiheessa. Asiakkaan sertifikaatti pysyy salassa, koska se lähetetään salatussa tunnelissa. EAP-TLS-menetelmän

käyttö vaatii kuitenkin edelleen asiakkaille sertifikaatit. PEAP-EAP-TLS-menetelmän käyttö on mahdollista vain Microsoft Windows-käyttöjärjestelmillä. (Cudbard-Bell 2012.)

3.4 Sertifikaatit

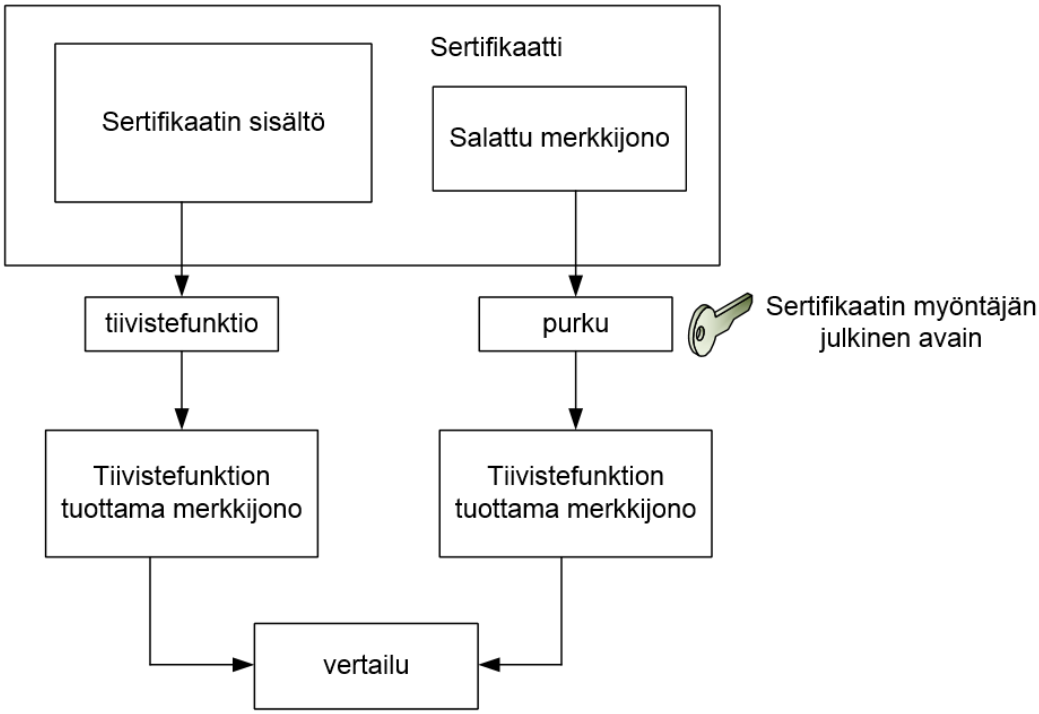
Digitaalinen sertifikaatti on standardoitu tiedostorakenne, mikä ei itsessään tuo lisää tietoturvaa. Sertifikaattien sisältämien tietojen varmistaminen mahdollistavat niiden käytön tietoturvan parantamiseen. Kuka tahansa voi luoda sertifikaatteja, jolloin tarvitaan luotettavat tahot jakamaan niitä. Sertifikaatin sisältämien tietojen avulla voidaan varmistaa, että se on luotettavasta lähteestä. Tämä luotettava taho on esimerkiksi yrityksen sertifikaattipalvelin. Palvelin allekirjoittaa kaikki sen myöntämät sertifikaatit sen omalla sertifikaatilla. (Centero 2012.)

Kuviossa 6 on esitetty, miten sertifikaattiin lisätään sen myöntäjän allekirjoitus. Ensin sertifikaatin tiedoista lasketaan tiiviste. Seuraavaksi sertifikaatin sisältö allekirjoitetaan salaamalla saatu tiiviste sertifikaatin myöntäjän omalla yksityisellä avaimella ja se liitetään jaettavan sertifikaatin tietoihin. (Microsoft 2003a.)



KUVIO 6. Sertifikaatin myöntäjän allekirjoitus (muokattu lähteestä Microsoft 2003a)

Kuviossa 7 on esitetty, miten sertifikaatin allekirjoitus tarkistetaan. Kun sertifikaatti halutaan varmentaa, lasketaan sen sisällöstä samalla tavalla ensin tiivistesumma. Seuraavaksi sertifikaatissa oleva tiiviste puretaan käyttäen myöntäjän julkista avainta ja verrataan, täsmäävätkö summat. Jos merkkijonot täsmäävät, voidaan olla varmoja että, sertifikaatti on luotettavasta lähteestä. (Microsoft 2003a.)

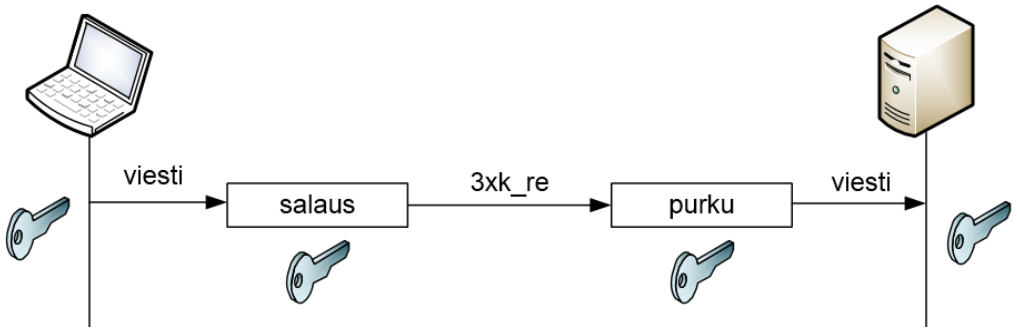


KUVIO 7. Sertifikaatin allekirjoituksen tarkistus (muokattu lähteestä Microsoft 2003a)

Sertifikaattien avulla voidaan muodostaa suojattuja yhteyksiä päätelaitteiden ja palvelimen välille. Suojatussa yhteydessä on turvallista välittää esimerkiksi luottokorttien numeroita tai käyttäjätunnuksia ja salasanoja. Tähän käytetään sertifikaattien sisältämiä avainpareja. (Digicert 2015.)

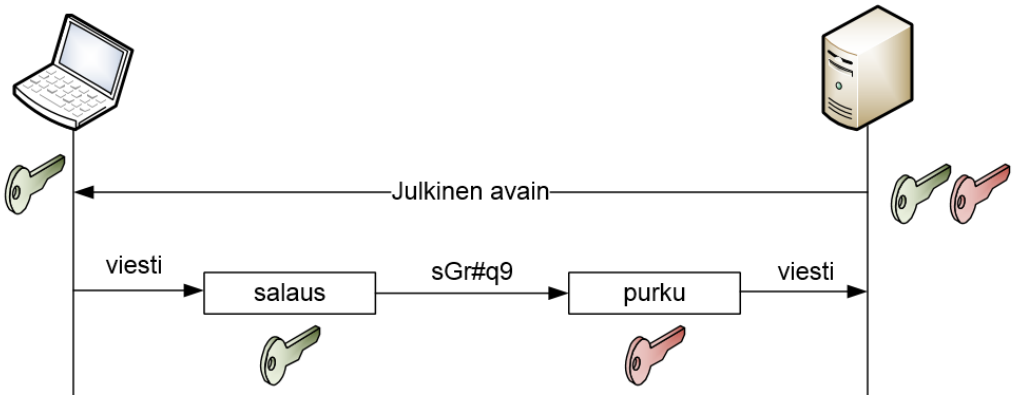
Suojatuissa yhteyksissä siirrettävien tietojen salaus ei ole tehokasta epäsymmetrisen salauksen vaatimilla pitkillä avaimilla. Epäsymmetrisiä avaimia voidaan käyttää turvalliseen symmetristen avainten siirtoon verkossa. (Microsoft 2003b.)

Symmetrisessä salauksessa käytetään samaa avainta tiedon salaamiseen ja purkamiseen. Salausavain täytyy olla molempien osapuolien tiedossa. Symmetriset salausavaimet ovat normaalisti 128- tai 256-bittisiä. Kuviossa 8 on esitetty symmetrisen salauksen periaate. (Digicert 2015.)



KUVIO 8. Symmetrinen salaus (muokattu lähteestä Digicert 2015)

Epäsymmetrisessä salauksessa tiedon salaamiseen käytetään eri avainta kuin purkamiseen. Toinen näistä avaimista on julkinen ja toinen pidetään yksityisenä. Salaus toimii molempiin suuntiin, niin että julkisella avaimella salattu tieto voidaan purkaa yksityisellä avaimella ja toisinpäin. Kuviossa 9 on esitetty epäsymmetrisen salauksen periaate. (Digicert 2015.)

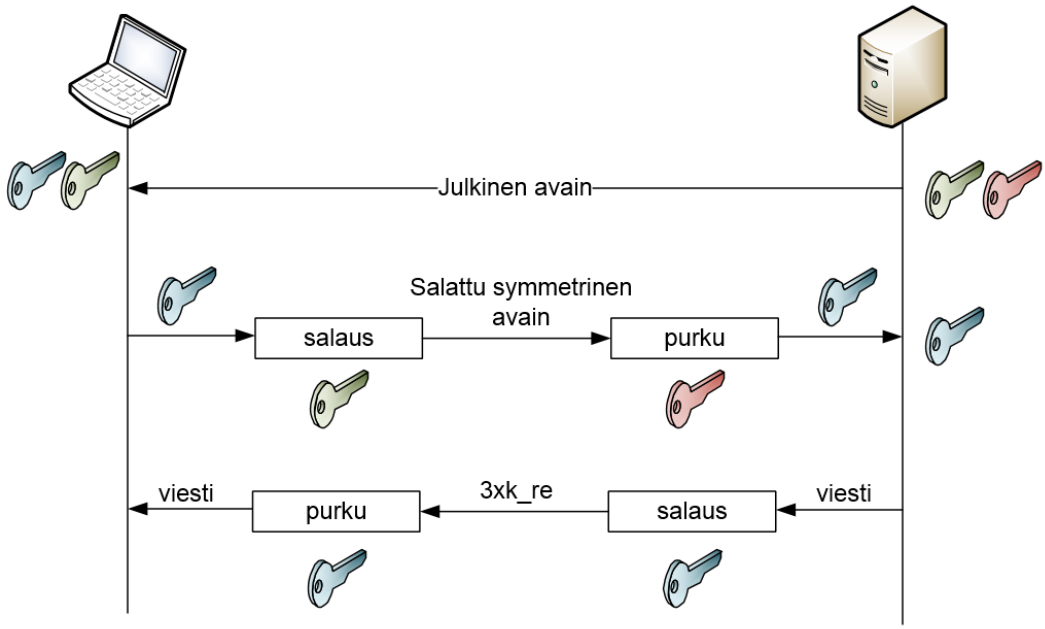


KUVIO 9. Epäsymmetrinen salaus (muokattu lähteestä Digicert 2015)

Epäsymmetrisessä salauksessa joudutaan käyttämään huomattavasti pitempiä avaimia kuin symmetrisessä salauksessa. Avainparit perustuvat kahden alkuluvun tuloon. Niiden lähtöarvot täytyy olla riittävän suuret, jotta avaimen selvittäminen vaikeutuu. Epäsymmetrisessä salauksessa täytyy siis käyttää todella suuria lukuja, koska kaikki mahdolliset numerot eivät

ole alkulukuja. Tyypillisesti avaimien koot ovat 1024 – 4096 bittiä. (Graham-Cumming 2013.)

Kuviossa 10 on esitetty, miten symmetrinen salausavain voidaan siirtää käyttäen epäsymmetristä salausta turvallisesti. TLS lähettää samalla periaatteella autentikoinnin yhteydessä luodun istuntokohtaisen salausavaimen verkon yli. (Microsoft 2003b.)



KUVIO 10. Symmetrisen avaimen siirto ja käyttö (muokattu lähteestä Digicert 2015)

4 802.1X:N KÄYTTÖÖNOTTO PÄIJÄT-HÄMEEN KESKUSSAIRAALAN LANGATTOMASSA VERKOSSA

Toteutettavaa langattoman verkon autentikointia varten täytyi miettiä, mikä vaihtoehto olisi paras tietoturvan kannalta. Autentikointi haluttiin tehdä niin, ettei käyttäjän tarvitse erikseen kirjoittaa tunnuksiaan mihinkään tai itse liittyä verkkoon.

Yhtymässä oli valmiina sertifikaattiympäristö, mikä mahdollisti EAP-TLS-menetelmän käytön. Muussa tapauksessa olisi ollut järkevämpää käyttää tunneloitujen EAP-menetelmien kanssa jotain muuta tunnistusmenetelmää, esimerkiksi EAP-MSCHAPV2:ta. EAP-TLS:n käyttö yksinään olisi ollut riittävää, mutta sen käyttäminen tunneloidun EAP-menetelmän kanssa parantaa tietoturvaa entisestään, koska käyttäjän sertifikaatti ei ole luettavissa verkkoa kuuntelemalla.

Päätelaitteiden ja palvelimien Windows-käyttöjärjestelmien takia vaihtoehdoksi oli helppo valita PEAP, koska se on suoraan tuettuna molemmissa. EAP-TTLS:n käyttö olisi tarjonnut yhtä hyvän tietoturvan, mutta se vaatisi erillisen ohjelman korvaamaan Windowsin asiakasohjelmiston ja sen asentamisen jokaiselle koneelle sekä tunnistuspalvelimelle. Taulukossa 1 on vielä esitetty vertailu eri menetelmistä.

PEAP-EAP-TLS:n kanssa valittiin käytettäväksi konekohtaiset sertifikaatit, joilla saadaan aikaan automaattinen liittyminen verkkoon sen kuuluvuusalueella. Koneet pysyvät verkossa, vaikkei niille olisi kirjautuneena, mikä mahdollistaa esimerkiksi Windows-päivitysten jakelun öisin, jos koneet ovat vain päällä verkon alueella.

TAULUKKO 1. EAP-menetelmät

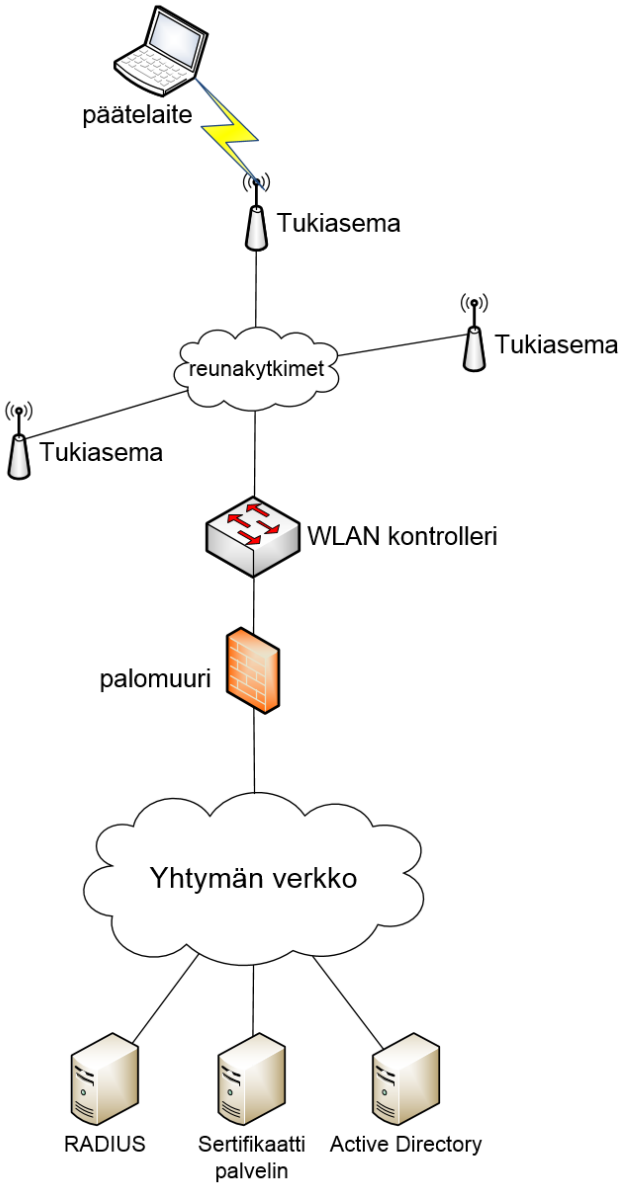
	Autentikointi	Windows tuki	Suojaa päätelaitten autentikointitiedot
EAP-TLS	Sertifikaatti	on	ei
PEAP	Riippuu käytettävästä toisen vaiheen EAP-menetelmästä	on	kyllä
EAP-TTLS	Riippuu käytettävästä toisen vaiheen autentikoinnista	vaatii erillisen sovelluksen	kyllä
EAP-MSCHAPV2	Käyttäjätunnus ja salasana	on	ei

4.1 Päijät-Hämeen sosiaali- ja terveysyhtymä

Työ tehtiin Päijät-hämeen sosiaali- ja terveysyhtymälle Lahdessa sijaitsevaan keskussairaalan verkkoon. Keskussairaala hyödyntää langattomia verkkoja jo ennestään monissa eri sovelluksissa. Yksi esimerkki on kuljetusrobotit, jotka suunnistavat antureiden ja tutkan avulla pitkin käytäviä. Ne tarvitsevat langatonta verkkoa ovien avaamiseen, hissien ohjaukseen ja paikkatiedon ilmoittamiseen. Osastoilla on käytössä lääkärikierroilla langaton verkko helpottamaan potilaiden tietojen katselua ja hoidon varaamista.

4.2 Testiympäristö

Kuviossa 11 on esitetty testiympäristö. Kokonaan oman testiympäristön rakentaminen olisi ollut työlästä, eikä siihen ollut aikaa tai muita resursseja keskussairaalan puolesta, joten testiympäristö päädyttiin tekemään osittain tuotantoympäristöön, kuitenkin niin, että siitä ei ole haittaa jokapäiväiselle toiminnalle. Testiympäristössä käytetty verkko oli eristetty palomuurilla muusta yhtymän verkosta.



KUVIO 11. Testiympäristö

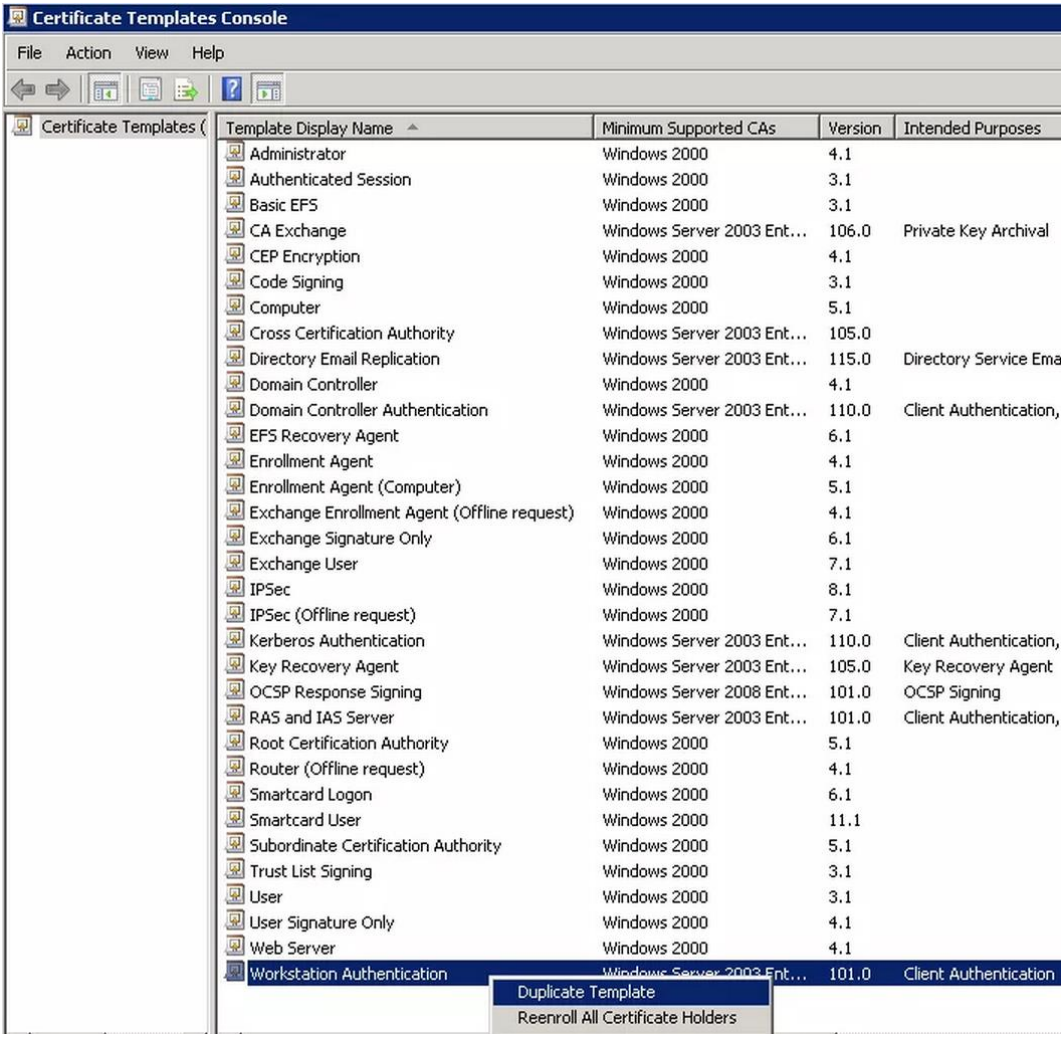
Testiympäristöä varten oli käytössä kaksi kannettavaa eri Windows-versioilla. Active Directoryn ja sertifikaattipalvelimen asetukset tehtiin tuotantoympäristössä. AD:n ja CA:n rakentaminen testiympäristöön ei ollut siksi järkevää, koska kontrollereille asti ei ollut valmiina mitään testiverkkoja. Liikenne testipalvelimille olisi joka tapauksessa mennyt tuotantoverkossa. Uusien langallisten testiverkkojen tekemiseen ei ollut työn tekohetkellä mahdollisuuksia. RADIUS-palvelin kuitenkin päätettiin asentaa erikseen tätä testiympäristöä varten.

Keskussairaalassa oli varattu valmiiksi henkilökunnan käyttöön tarkoitetun verkon IP-osoiteavaruus ja käytettävä VLAN, joten sitä ei työssä tarvinnut suunnitella. Langattoman verkon kontrollereihin täytyi luoda uusi verkko ja muut tarvittavat asetukset autentikointia varten. Myöhemmin esitetyt IP-osoitteet ovat vain esimerkkejä ja osittain sensuroituja.

4.3 Sertifikaattimallien luonti

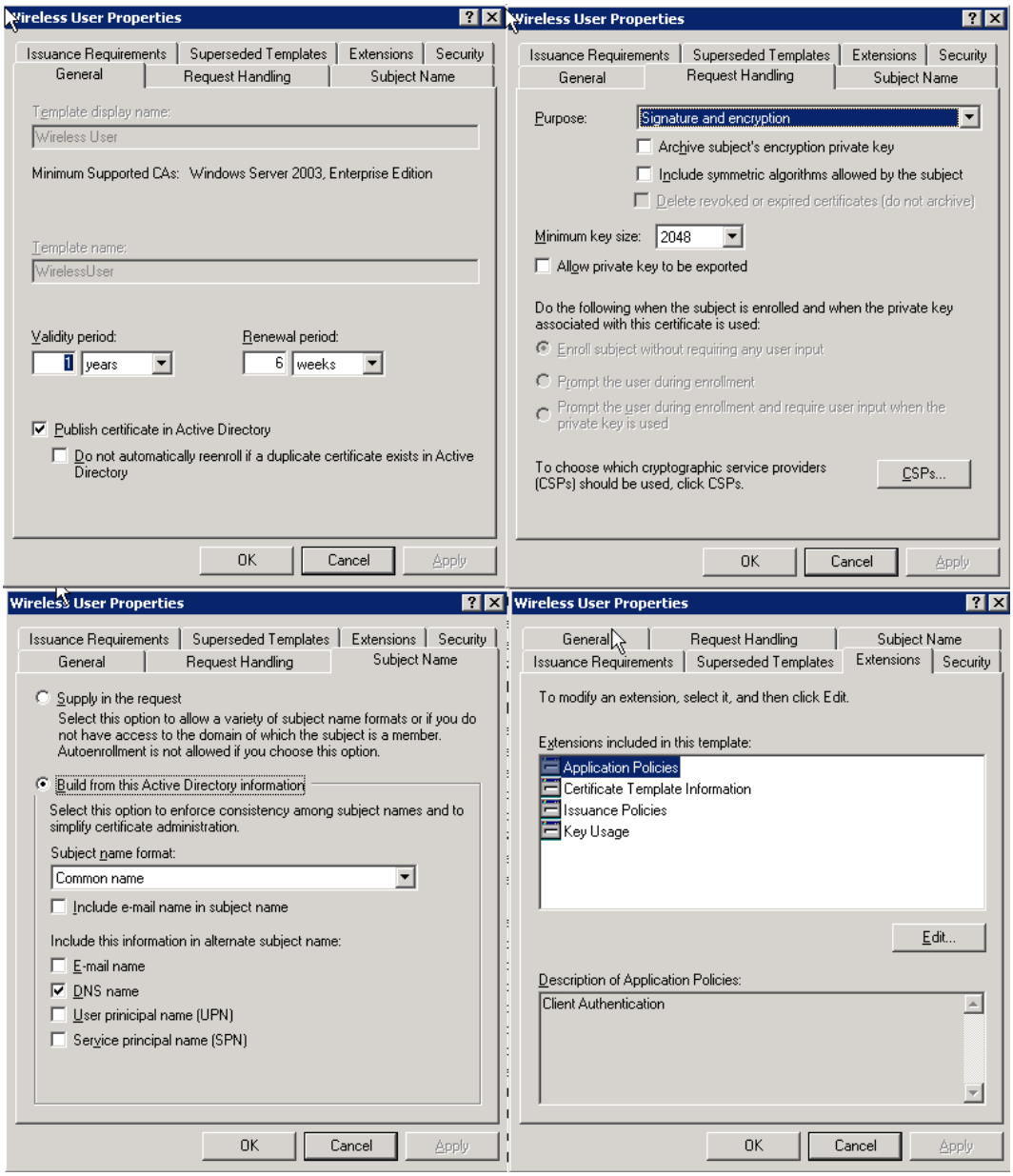
Testiympäristön käyttöönotto alkoi luomalla tarvittavat sertifikaattimallit CA-palvelimelle. Valmis sertifikaattiympäristö oli asennettu Windows 2003 Server -käyttöjärjestelmälle. PEAP-EAP-TLS-autentikointia varten sinne täytyi luoda 2 uutta sertifikaattimallia. Sertifikaattimallissa määritetään sertifikaattikohtaiset asetukset, kuten voimassaoloaika, käyttötarkoitus ja avaimen pituus.

Sertifikaattipalvelimella on olemassa valmiiksi sertifikaattimalleja, jotka on esitetty kuviossa 13. Uuden sertifikaattimallin luominen tapahtuu monistamalla haluttu malli ja tekemällä siihen tarvittavat muutokset. Päätelaitteiden sertifikaatteja varten valittiin Workstation Authentication -malli.



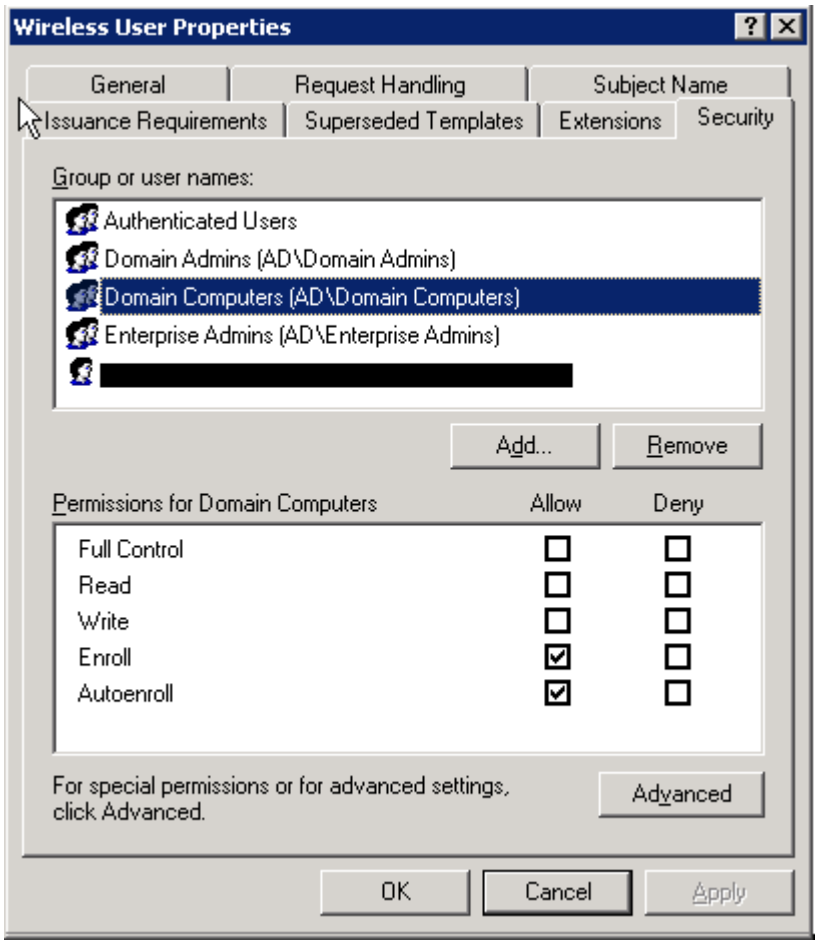
KUVIO 12. Sertifikaattimallin monistus

Kuviossa 12 on esitetty, miten sertifikaattimalli monistetaan. Monistuksen jälkeen täytyy uuden mallin asetukset muuttaa käyttötarkoituksen mukaan.



KUVIO 13. Päätelaitteen sertifikaattimallin asetukset

Kuviossa 13 on esitetty sertifikaattimallin asetukset päätelaitteille jaettavista sertifikaateista. Sertifikaatin avaimen pituus kasvatettiin 1024 bitin oletusarvosta 2048 bittiin. Extensions -välilehdeltä varmistettiin että sertifikaatti soveltuu asiakkaan autentikointiin. Sertifikaatin subject name -kohdassa määriteltiin, että sertifikaattiin tulee tietokoneen nimi. Sertifikaattimallille pitää vielä määritellä tarvittavat oikeudet, jotka on esitetty kuviossa 14.

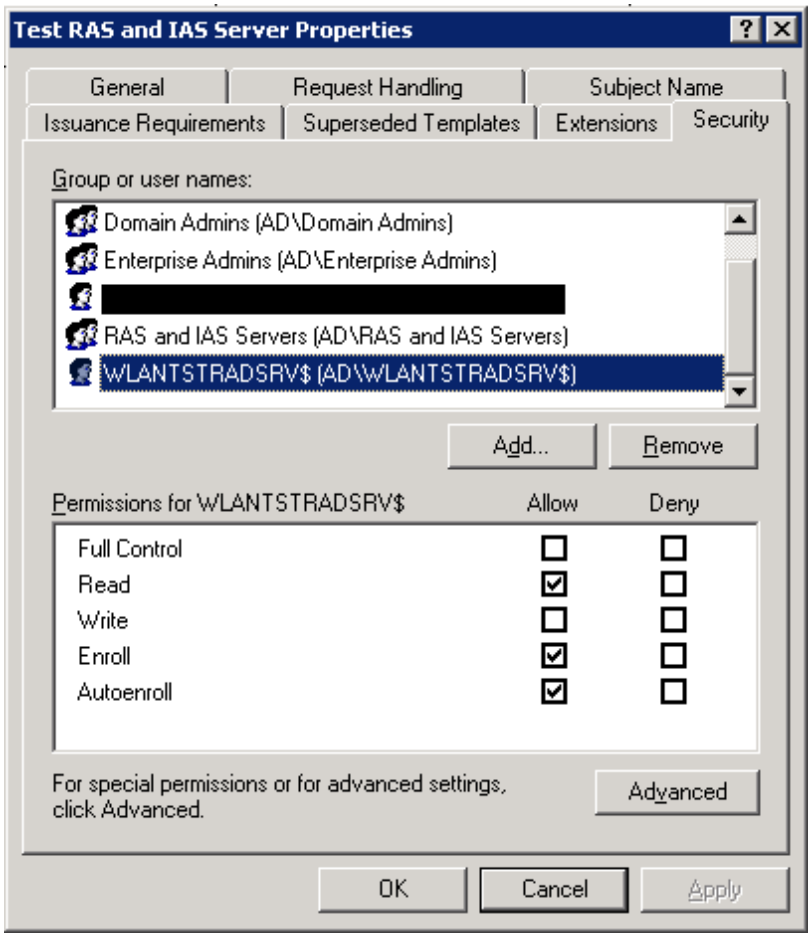


KUVIO 14. Päätelaitteen sertifikaatin oikeudet

Toimialueella oleville koneille annettiin oikeudet hakea tätä sertifikaattia. Toimialueella ei ollut muita käytäntöjä, jotka mahdollistaisivat sertifikaattien haun koneille automaattisesti. Testiä varten olisi kuitenkin ollut järkevää antaa oikeudet vain testikoneille ja ottaa muilta toimialueen koneilta pois. Tämä olisi estänyt sen, ettei vahingossakaan ylimääräisiä sertifikaatteja jaeta palvelimelta.

RADIUS-palvelinta varten tarvitaan myös sertifikaatti, jolla palvelin varmentaa itsensä asiakkaalle. Palvelinta varten monistettiin RAS and IAS Server -sertifikaattimalli. Asetukset poikkesivat asiakkaan sertifikaatista niin, että sertifikaattimallille annettiin pidempi voimassaoloaika ja oikeus varmentaa käyttäjälle palvelin. Sertifikaatteja oli mahdollista hakea vain testipalvelimella.

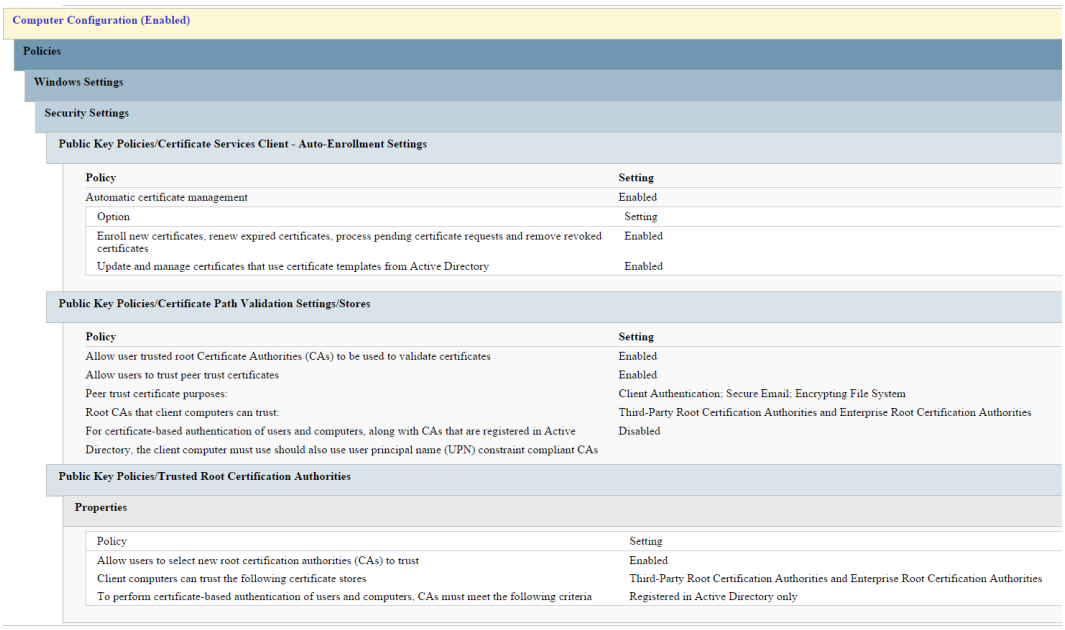
Kuviossa 15 on esitetty, miten sertifikaattien oikeudet oli lisätty sertifikaattimalliin.



KUVIO 15. NPS-palvelimen sertifikaattimallin oikeudet

4.4 AD-ryhmäkäytännöt

Seuraavaksi tehtiin tarvittavat ryhmäkäytännöt Active Directoryyn. Ryhmäkäytäntöjen avulla voidaan tehdä toimenpiteitä toimialueen koneille tai käyttäjille. Tarkoituksena oli automatisoida sertifikaattien ja langattoman verkon asetusten haku. Kuviossa 16 on esitetty päätelaitteiden sertifikaattien automaattisen haun mahdollistava käytäntö. Kuviossa 17 on vastaavasti palvelimelle asetukset sertifikaatin hakuun ja uusimiseen.



Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Public Key Policies/Certificate Services Client - Auto-Enrollment Settings

Policy	Setting
Automatic certificate management	Enabled

Option	Setting
Enroll new certificates, renew expired certificates, process pending certificate requests and remove revoked certificates	Enabled
Update and manage certificates that use certificate templates from Active Directory	Enabled

Public Key Policies/Certificate Path Validation Settings/Stores

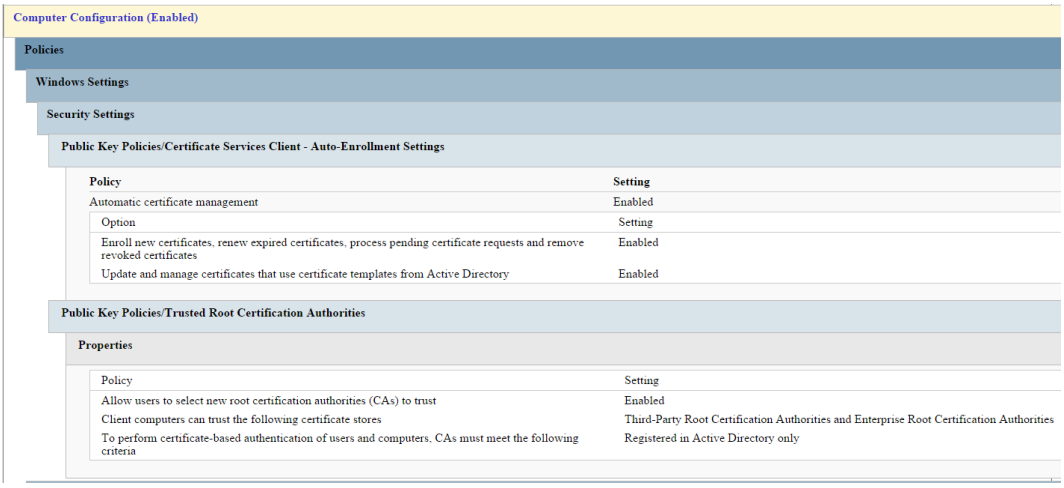
Policy	Setting
Allow user trusted root Certificate Authorities (CAs) to be used to validate certificates	Enabled
Allow users to trust peer trust certificates	Enabled
Peer trust certificate purposes:	Client Authentication; Secure Email; Encrypting File System
Root CAs that client computers can trust:	Third-Party Root Certification Authorities and Enterprise Root Certification Authorities
For certificate-based authentication of users and computers, along with CAs that are registered in Active Directory, the client computer must use should also use user principal name (UPN) constraint compliant CAs	Disabled

Public Key Policies/Trusted Root Certification Authorities

Properties

Policy	Setting
Allow users to select new root certification authorities (CAs) to trust	Enabled
Client computers can trust the following certificate stores	Third-Party Root Certification Authorities and Enterprise Root Certification Authorities
To perform certificate-based authentication of users and computers, CAs must meet the following criteria	Registered in Active Directory only

KUVIO 16. Ryhmäkäytäntö päätelaitteen automaattiseen sertifikaattien hakuun



Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Public Key Policies/Certificate Services Client - Auto-Enrollment Settings

Policy	Setting
Automatic certificate management	Enabled

Option	Setting
Enroll new certificates, renew expired certificates, process pending certificate requests and remove revoked certificates	Enabled
Update and manage certificates that use certificate templates from Active Directory	Enabled

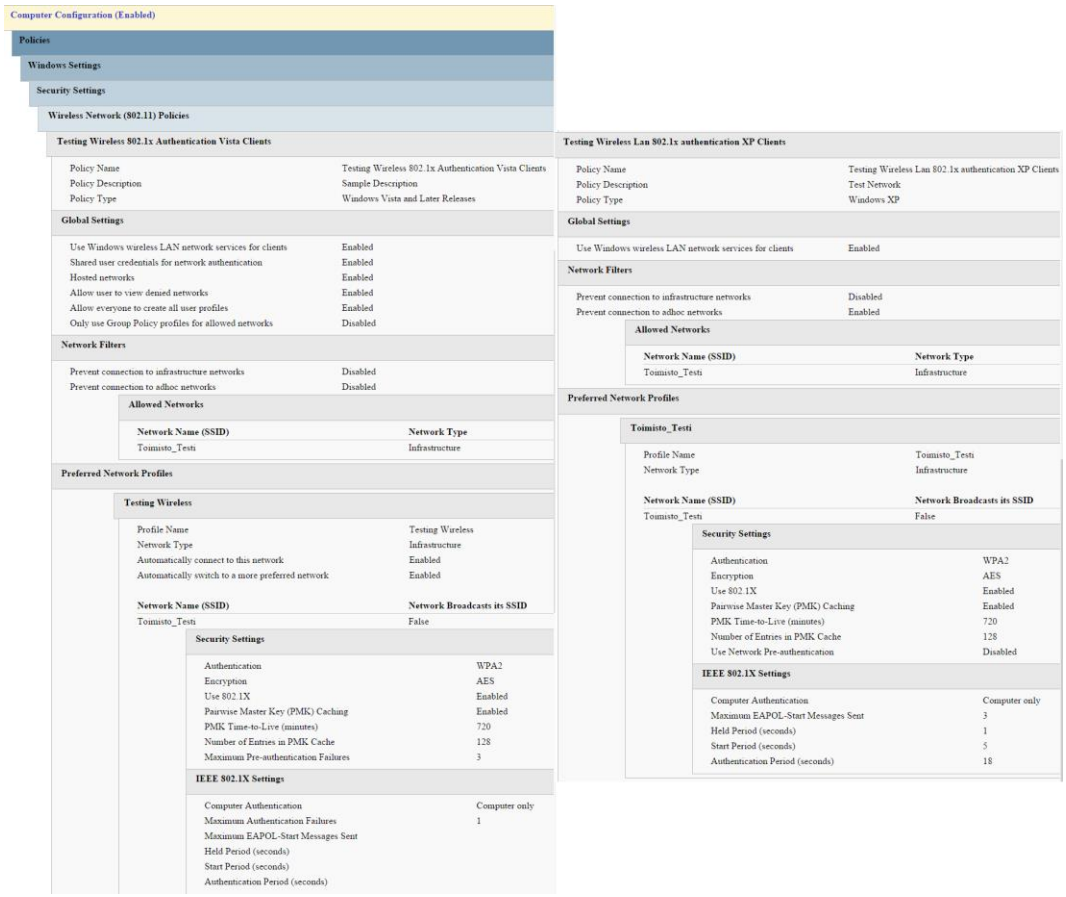
Public Key Policies/Trusted Root Certification Authorities

Properties

Policy	Setting
Allow users to select new root certification authorities (CAs) to trust	Enabled
Client computers can trust the following certificate stores	Third-Party Root Certification Authorities and Enterprise Root Certification Authorities
To perform certificate-based authentication of users and computers, CAs must meet the following criteria	Registered in Active Directory only

KUVIO 17. NPS-palvelimen ryhmäkäytäntö sertifikaattien hakuun

Päätelaitteille täytyy automatisoida vielä langattoman verkon asetusten levitys. Kuviossa 18 on esitetty, mitä nämä ryhmäkäytännöt pitävät sisällään. Windows XP:lle ja Windows 7 molemmille pitää luoda oma käytäntö asetusten hakuun. Asetukset ovat samat molemmissa, ne vain määritellään eri tavoin. Asetuksissa määriteltiin, mihin verkkoon kone liittyy ja mitä salausasetuksia siinä käytetään. 802.1x-asetuksista määritettiin kone tunnistamaan tietokonetilillä.



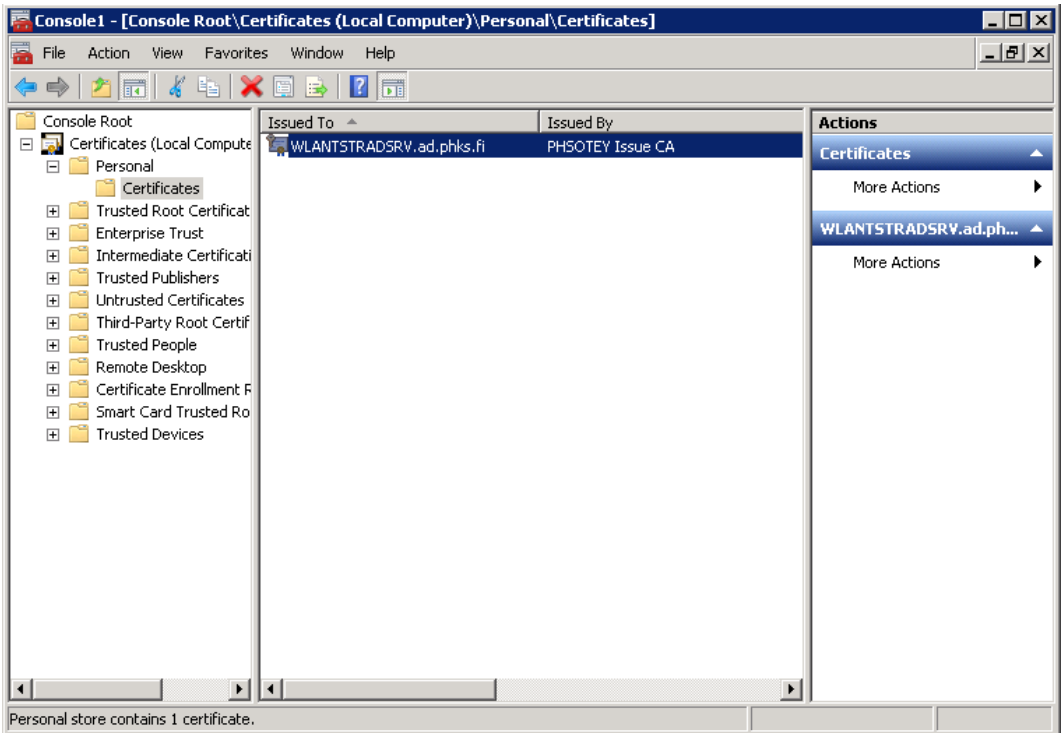
KUVIO 18. Ryhmäkäytännön asetukset WLAN asetusten jakamiselle

Käytännöt täytyy vielä linkittää johonkin OU:hun (Organizational unit), että ne alkavat toimia. OU on toimialueessa oleva alue, jonka alle voidaan lisätä tietokoneita ja käyttäjiä. OU:n perusteella voidaan suorittaa näille esimerkiksi ryhmäkäytäntöjä. Testiä varten luotiin uusi Wlan_Testi OU, johon testikoneet siirrettiin. RADIUS-palvelin oli myös tässä testi OU:ssa. Samalla AD:hen lisättiin ryhmä, johon tietokoneiden täytyy kuulua myöhempää RADIUS-autentikointia varten.

4.5 RADIUS-palvelin

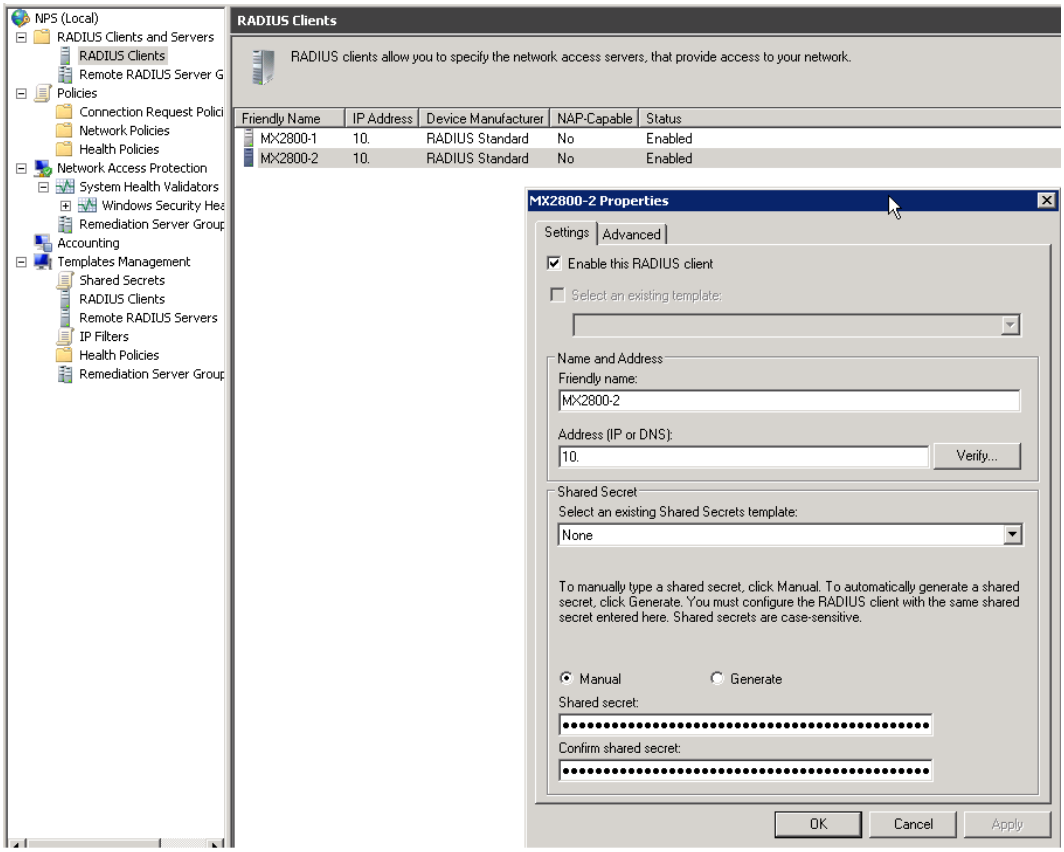
Windows-palvelimissa RADIUS-autentikoinnin käytön mahdollistaa NPS (Network Policy Server). Langattoman verkon testiympäristöön oli saatu yksi palvelin, jolle otettiin käyttöön NPS-rooli. NPS-roolin käyttöönoton jälkeen palvelimelle haettiin aikaisemmin luodun sertifikaattimallin

mukainen uusi sertifikaatti. Kuviossa 19 on nähtävissä kyseinen sertifikaatti.



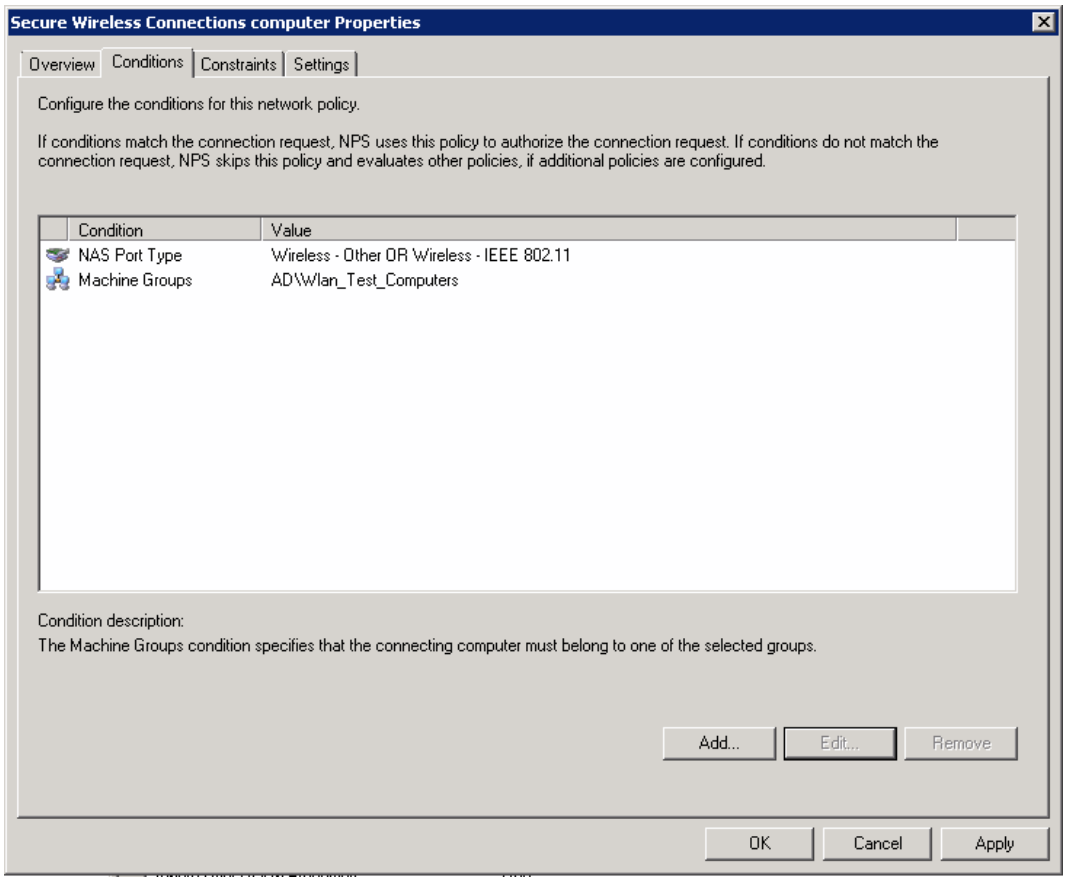
KUVIO 19. NPS-palvelimen sertifikaatti

Seuraavaksi langattoman verkon kontrollerit lisättiin RADIUS-asiakkaiksi. Nämä kontrollerit ovat ne, jotka välittävät kaikki tarvittavat viestit asiakkaan ja RADIUS-palvelimen välillä. Kuviossa 20 on esitetty kontrollerien lisäys RADIUS-asiakkaiksi IP-osoitteen ja yhteisen salasanan avulla. NPS-palvelimella on mahdollista generoida hyvin pitkä satunnainen merkkijono yhteiseksi salasanaksi. Vastaavasti RADIUS-palvelimella luotu pitkä salasana täytyy määritellä kontrollereihin.



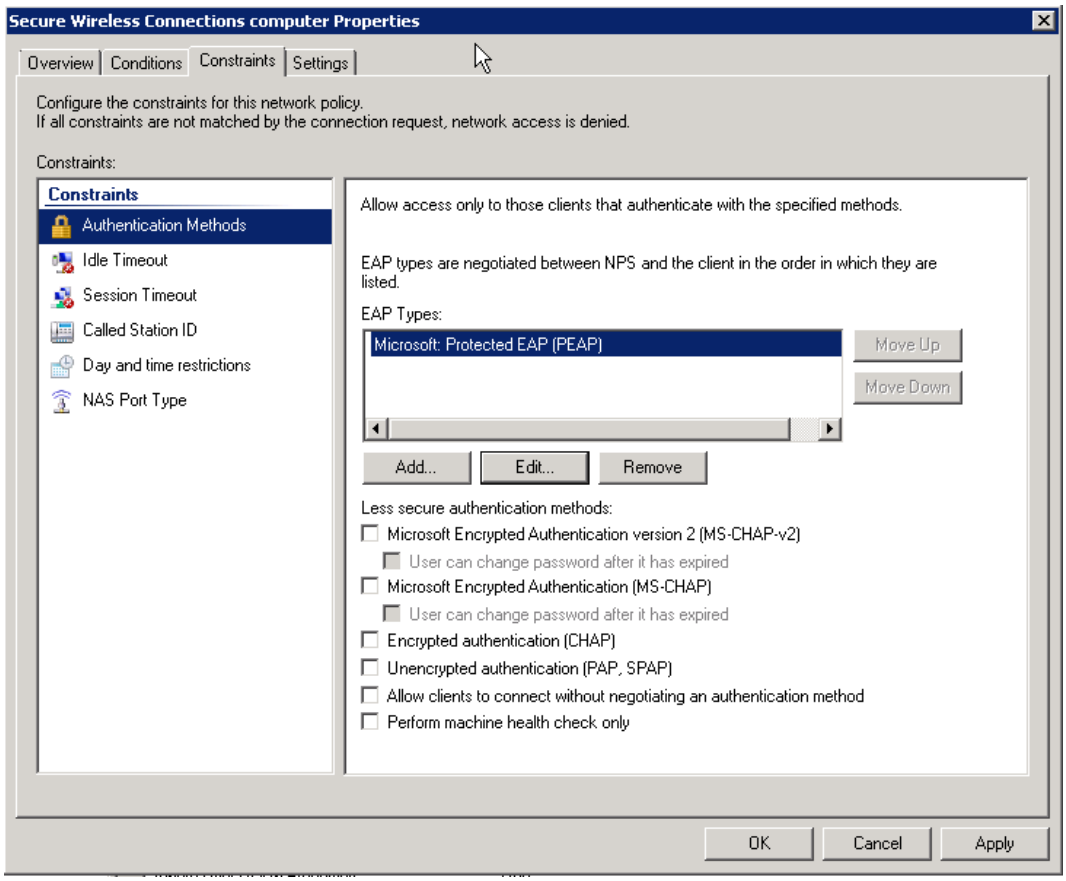
KUVIO 20. kontrollerit RADIUS-asiakkaina

Palvelimelle luotiin seuraavaksi uusi käytäntö, jossa määriteltiin käytettävät autentikointimenetelmät ja vaatimukset verkkoon pääsylle. Kuviossa 21 on esitetty käytännön ehdot. Vaatimuksena verkkoon pääsylle on, että kone kuuluu Wlan_Test_Computers -ryhmään. NAS port type -kohtaan määritettiin, että todentaja on langattoman verkon laite. WLAN-kontrollerilta tulevissa viesteissä on käytössä tämä porttityyppi, jolla varmistutaan, että kyse on langattoman verkon laitteista, jotka haluavat pääsyn verkkoon.



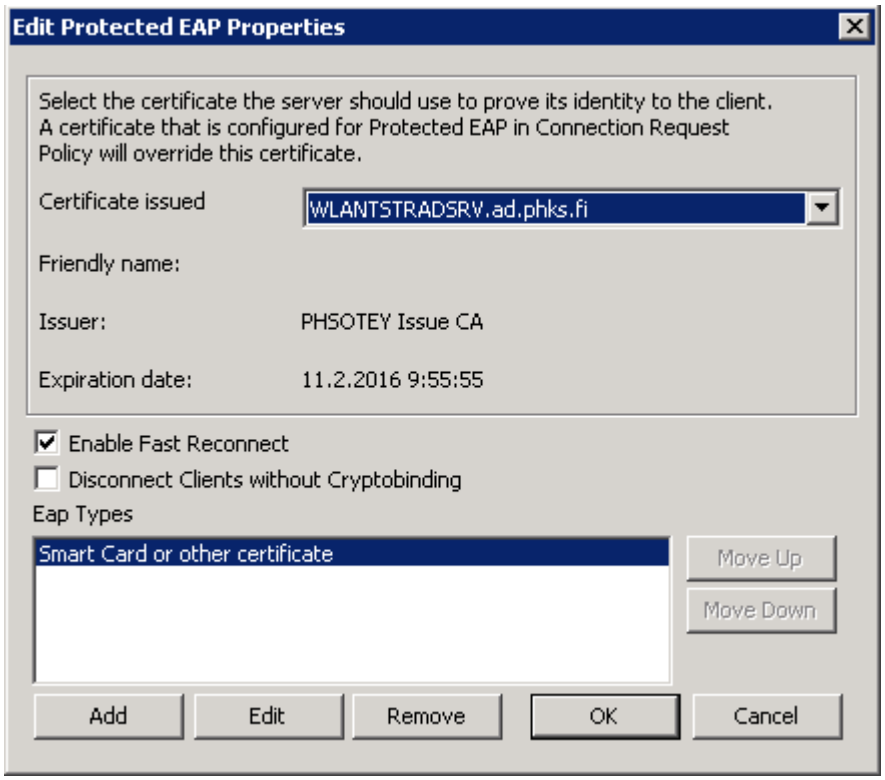
KUVIO 21. Network Policyn ehdot

Constraints-välilehdeltä pystytään valitsemaan käytettävät autentikointimenetelmät. Kuviossa 22 on esitetty valittu PEAP-menetelmä.



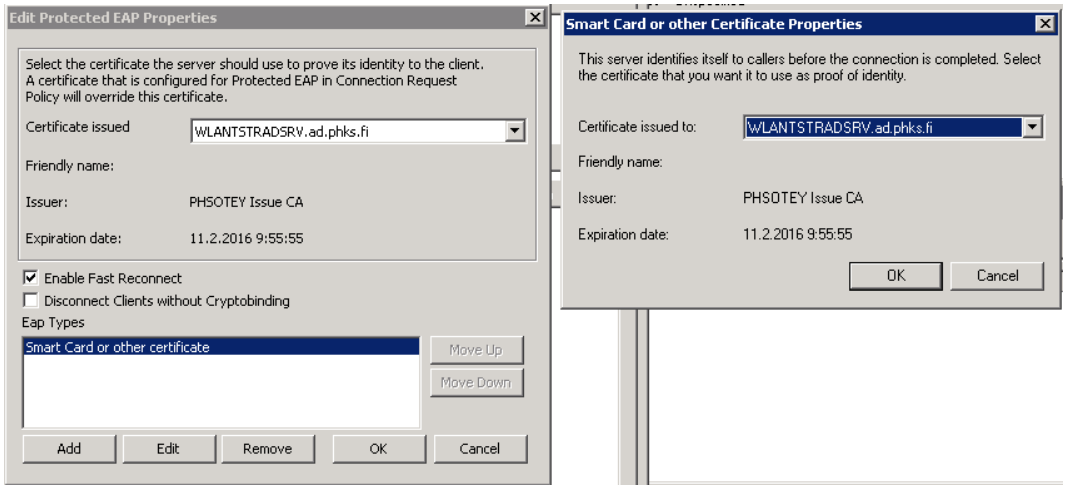
KUVIO 22. autentikointiasetukset

PEAP-asetuksista valittiin sertifikaatti, jota halutaan käyttää palvelimen tunnistuksessa. Samalla otettiin käyttöön fast reconnect, joka mahdollistaa päätelaitteen liikkumisen tukiasemasta toiseen ilman jatkuvaa autentikointia. PEAP-asetuksista valitaan myös toisen vaiheen autentikointimenetelmä. Tässä kohtaa voisi käyttää esimerkiksi MS-CHAPv2:ta jolloin autentikointi tapahtuisi käyttäjän AD-tunnuksella ja salasanalla. EAP-TLS-autentikointia varten valittiin Smart Card or other certificate. Kuviossa 23 on esitetty käytetyt asetukset.



KUVIO 23. PEAP-asetukset

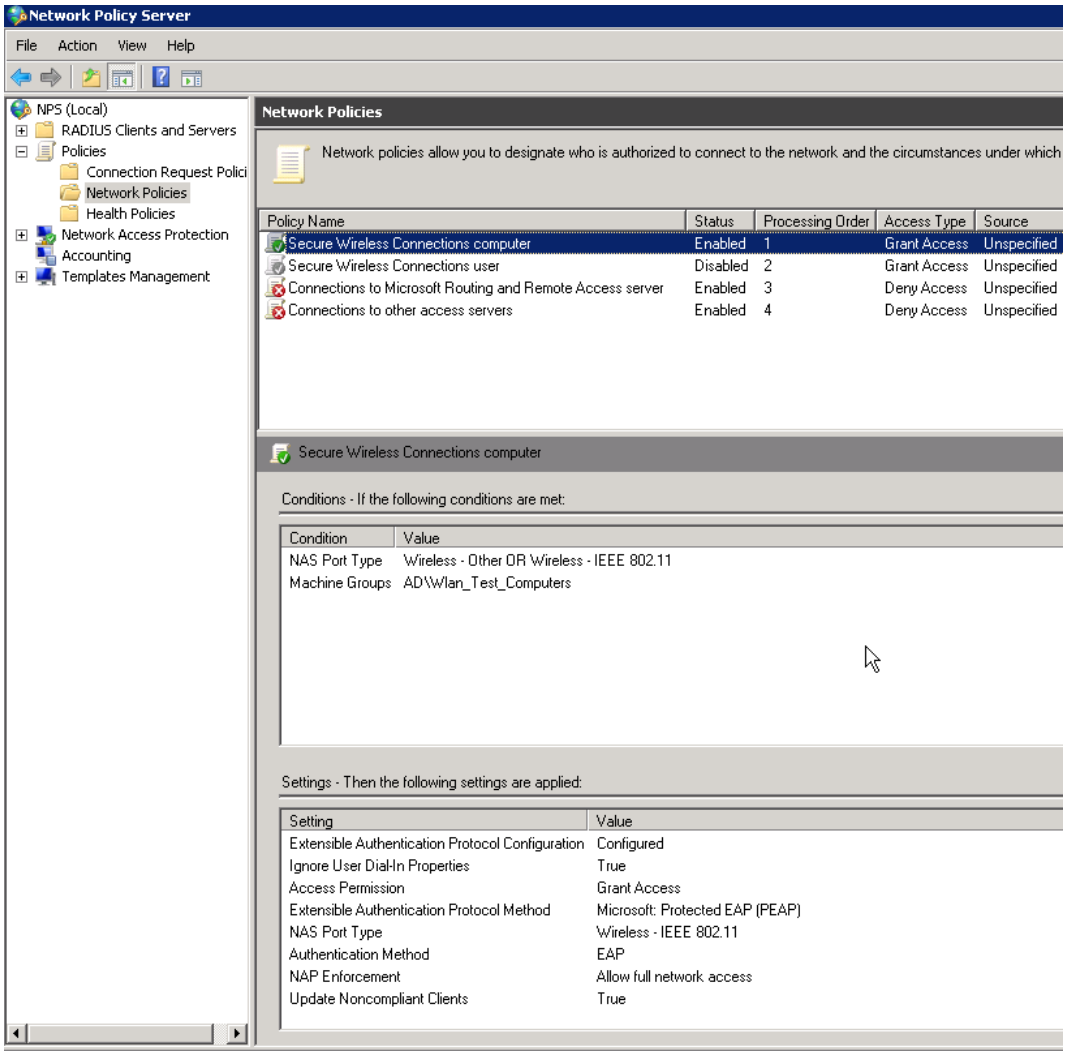
Toisen vaiheen EAP-TLS käyttää myös autentikointiin sertifikaatteja, joten käytettävä sertifikaatti pitää valita asetuksista. Kuviossa 24 on esitetty, miltä valintaikkuna näyttää. Tässä voidaan käyttää samaa sertifikaattia kuin PEAP-tunnelin luomiseen.



KUVIO 24. Sertifikaatin valinta

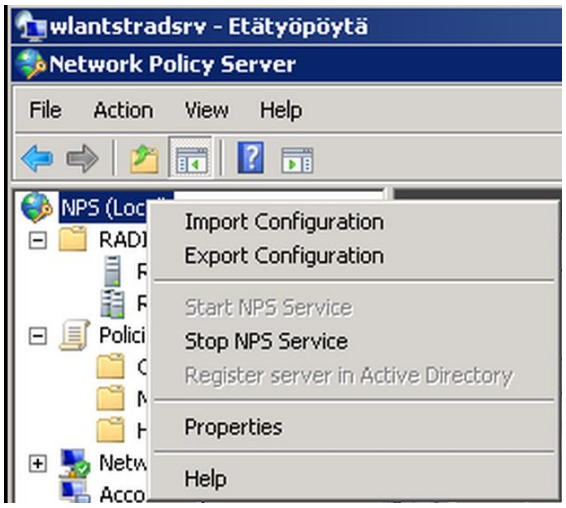
Kuviossa 25 on esitetty yhteenvetona vielä aikaisemmin määritellyt asetukset. RADIUS-palvelimelle voidaan luoda monia eri käytäntöjä,

joiden järjestys määritellään Processing Order -kentän perusteella. Esimerkiksi jollekin muulle päätelaitteelle, joka ei tue PEAP-käyttöä, voisi olla jokin oma EAP-menetelmä määriteltynä. Näille laitteille voisi olla jokin oma ryhmä AD:ssa, jolloin se ei täyttäisi ensimmäisenä olevan Secure Wireless Connection computer policyn vaatimia ehtoja. Viimeisenä on käytäntö, joka estää verkkoon pääsyn, jos laite ei osu minkään muun käytännön ehtoihin.



KUVIO 25. Network policyn asetukset

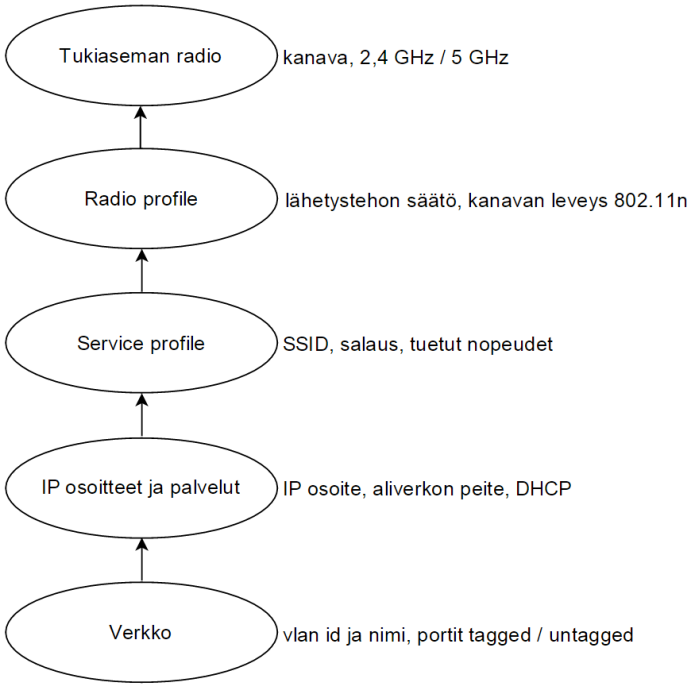
Lopuksi RADIUS-palvelin pitää rekisteröidä AD:hen valitsemalla Register server in Active Directory. Kuviossa 26 on esitetty rekisteröinti, joka on harmaana, koska se on jo tehty.



KUVIO 26. RADIUS.palvelimen rekisteröinti

4.6 WLAN-verkon asetusten määrittely

Työ tehtiin Trapezen MX2800-sarjan WLAN-kontrollereilla, joissa oli käytössä 7.5.3.2-ohjelmistoversio. Kuviossa 27 on esitetty hierarkkisesti, miten verkko määritellään Trapezen kontrollerissa. Kuviossa on annettu esimerkkinä muutama kohta, jota tietyillä tasoilla voi muuttaa. Kuvion tarkoitus on helpottaa hahmottamaan, miten eri komponentit liittyvät toisiinsa. Määrittelyt tehdään myös kuvion esittämässä järjestyksessä.



KUVIO 27. Kontrollerin komponentit

Alimmalla tasolla on verkko, jolla on nimi ja ID. Verkko täytyy myös liittää johonkin porttiin. Ensin luotiin uusi vlan nimeltä toimisto antamalla kontrollerissa komento

set vlan 10 name toimisto

Verkon luonnin jälkeen se täytyi liittää johonkin porttiin antamalla komento

set vlan 10 port 1 tag 10

Vastaavasti verkko täytyy luoda myös toisessa päässä oleviin aktiivilaitteisiin. Seuraavaksi määriteltiin verkolle IP-osoitteet ja tarvittavat palvelut. Testiympäristössä kontrollerilla otettiin käyttöön DHCP, joka jakaa laitteille yksilölliset IP-osoitteet. Verkolle annettiin IP-osoite komennolla

set interface 10 ip 10.0.0.11 255.255.255.0

DHCP-palvelulla jaetaan osoitteet verkosta osoitteet .20 - .250, nimipalvelimien IP:t on komennosta sensuroitu. Komentoon tarvitsee määritellä myös verkon yhdyskäytävä. DHCP saatiin päälle antamalla komento

set interface 10 ip dhcp-server enable start 10.0.0.20 stop 10.0.0.250 primary-dns 10.x.x.x secondary-dns 10.x.x.x default-router 10.0.0.1

Service profiilissa määritellään langattoman verkon asetukset. Service profiili, jonka nimi on toimisto-testi ja SSID Toimisto_Testi luotiin komennolla

set service-profile toimisto-testi ssid-name Toimisto_Testi

Samalle profiilille määriteltiin käytettäväksi WPA2 komennolla

set service-profile toimisto-testi rsn-ie enable

AES-salaus saatiin käyttöön antamalla komento

set service-profile toimisto-testi rsn-ie cipher-ccmp enable

Service profiili täytyy liittää johonkin olemassa olevaan verkkoon. Profiili saatiin liitettyä toimisto-nimiseen vlan:iin antamalla komento

set service-profile toimisto-testi attr vlan-name toimisto

Service-profiilit liitetään erillisiin radioprofiileihin. Testiä varten tehtiin oma radioprofiili yhtä tukiasemaa varten. Testiympäristöä varten riitti hyvin, että verkko näkyi alkuun vain yhdessä tukiasemassa. Radioprofiili nimeltä testi_radio luotiin ja liitettiin service-profiilin komennolla

set radio-profile testi_radio service-profile toimisto-testi

Radio-profiilissa voi olla useita eri service-profiileita, radio profiilien kautta käytännössä määritetään, missä tukiasemissa mitkäkin verkot näkyvät. Radio-profiili testi_radio liitettiin tukiaseman 2,4 GHz:n radioon kanavalle 11 lähetysteholla 13 dBm antamalla komento

set ap 1 radio 1 radio-profile testi_radio channel 11 tx-power 13 mode enable

5 GHz:n radio liitettiin testi_radio-profiiliin 18 dBm-lähetysteholla ja automaattisella kanavanvalinnalla antamalla komento

set ap 1 radio 2 radio-profile testi_radio tx-power 18 mode enable

Yksittäisiä radioita ei pysty lisäämään service-profiileihin, vaan ne pitää aina liittää radioprofiilien kautta. Tukiaseman radio voi kuulua vain yhteen radioprofiilin. Radioprofiilit kannattaakin suunnitella tarkkaan esimerkiksi alueittain, jolloin on helppo määritellä, millä alueella on mitkäkin verkot service-profiilien kautta.

Verkon määrittelyjen lisäksi kontrollerille täytyy laittaa RADIUS-palvelimen IP-osoite ja yhteinen salasana. RADIUS-palvelin nimettiin radius_win2008:ksi, jonka osoite on sensuroitu ja jaettu salasana on salasana. RADIUS-palvelin lisättiin antamalla komento

set radius server radius_win2008 address 10.x.x.x timeout 5 retransmit 3 deadtime 5 key salasana

Komento sisältää myös oletuksena käytetyt ajat viestien uudelleenlähetykselle, vastausten odottamiselle ja yritysten määrälle, jos viesteihin ei saada vastausta. RADIUS-palvelimelle täytyy luoda oma ryhmä radius_group ja lisätä se lisättiin siihen jäseneksi antamalla komento

set server group radius_group members radius_win2008

Toimisto_Testi verkolle piti vielä määritellä, mitä RADIUS-ryhmää se käyttää 802.1x-autentikoinnissa. Kaikille Toimisto_Testi-nimisessä verkossa oleville käyttäjille tehtiin autentikointi käyttäen radius_group:a antamalla komento

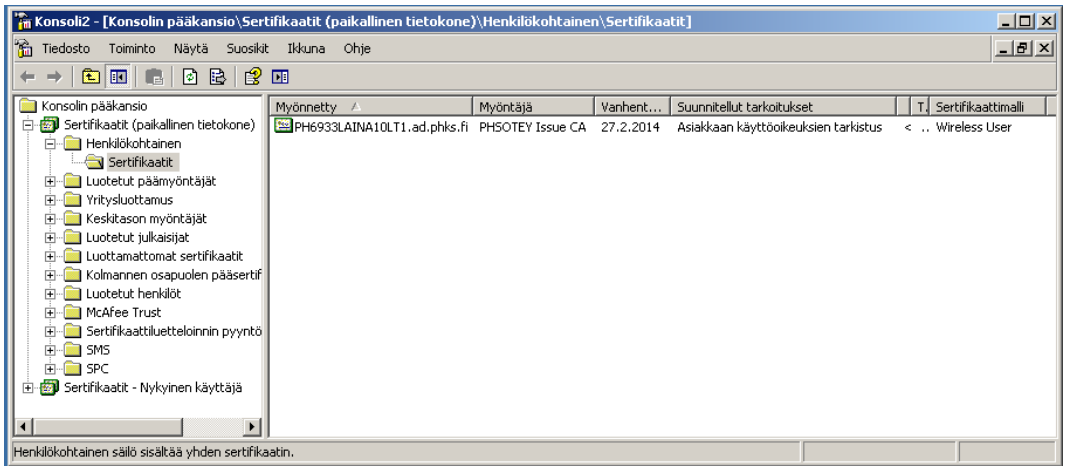
set authentication dot1x ssid Toimisto_Testi ** pass-through radius_group

Lopuksi palomuuriin täytyi tehdä tarvittavat säännöt vielä, jotta kontrolleri pystyy keskustelemaan RADIUS-palvelimen kanssa. WLAN-kontrollerilla täytyy olla yhteys RADIUS-palvelimen 1812 ja 1813 UDP portteihin autentikointia varten.

5 TESTAUS

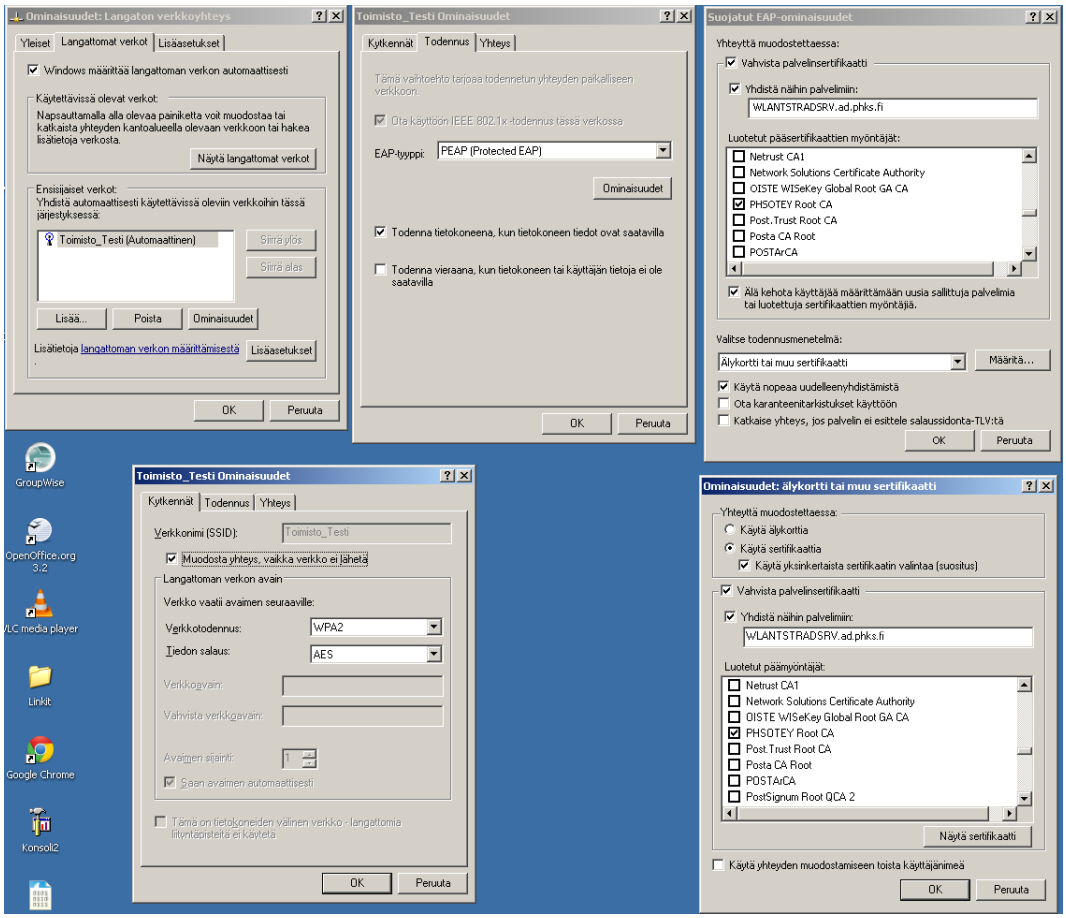
Testaus aloitettiin liittämällä kannettava tietokone langalliseen verkkoon, jotta sillä oli mahdollisuus hakea sertifikaatti ja langattoman verkon asetukset.

Helpoin tapa saada konetili päivittymään on käynnistää kone uudestaan kytkettynä langalliseen verkkoon, jolloin haetaan konekohtaiset ryhmäkäytännöt AD:sta. MMC-työkalulla varmistettiin, että kone oli saanut sertifikaatin. Kuviossa 28 on esitetty MMC-työkalun näkymä ja konekohtainen sertifikaatti. MMC-työkaluun lisätään sertifikaattilaajennus konetilien sertifikaateilla, jolloin päästään näkemään koneen omat sertifikaatit.



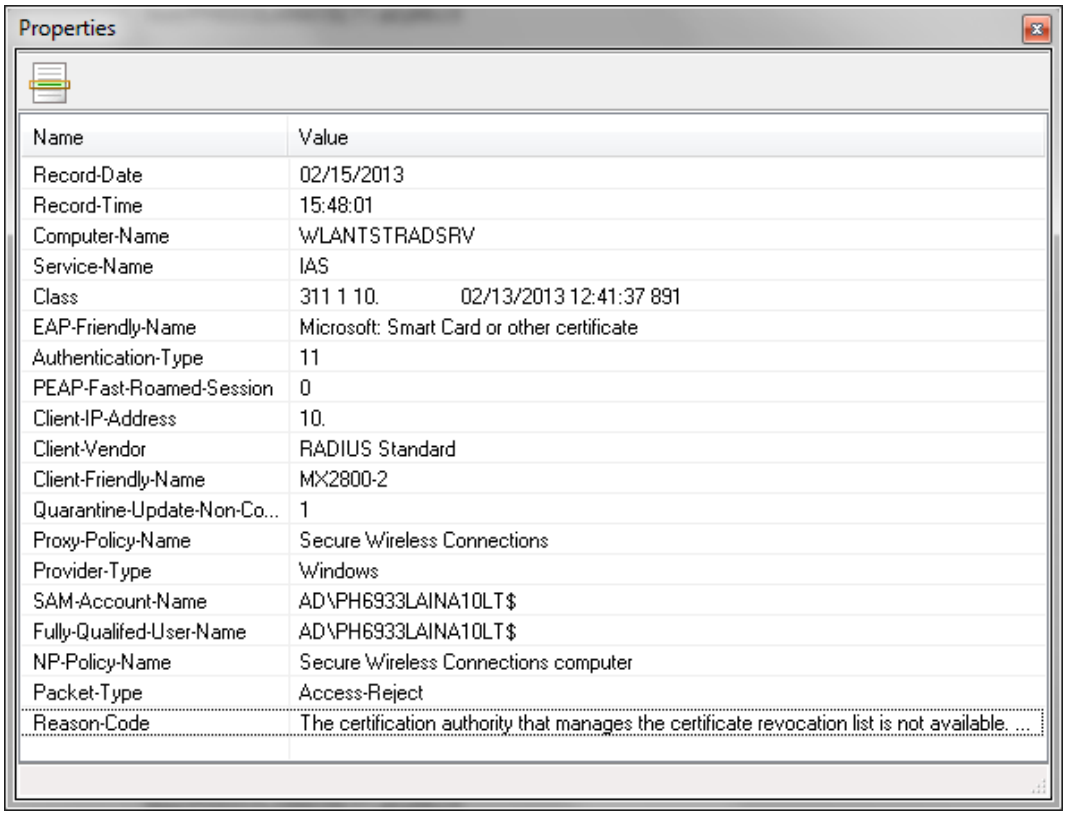
KUVIO 28. Sertifikaatti testikannettavassa

Koneen ryhmäkäytännöt voi päivittää myös antamalla komentorivillä komento gpupdate /force, mutta testien aikana huomasin, ettei se aina riittänyt päivittämään kaikkia tietokonetilin muutoksia. Koneelta tarkistettiin samalla, että se oli saanut langattoman verkon asetukset. Kuviossa 29 on esitetty yhteenveto asetuksista Windows XP-käyttöjärjestelmällä. Kuviossa on nähtävillä myös lisäys, joka tehtiin aikaisempaan ryhmäkäytäntöön. Kone yhdistää vain tietyn nimiseen palvelimeen, ja sen sertifikaatin täytyy olla PHSOTEY Root CA:n allekirjoittama. Tämä vahvistus tehdään autentikoinnin molemmissa vaiheissa.



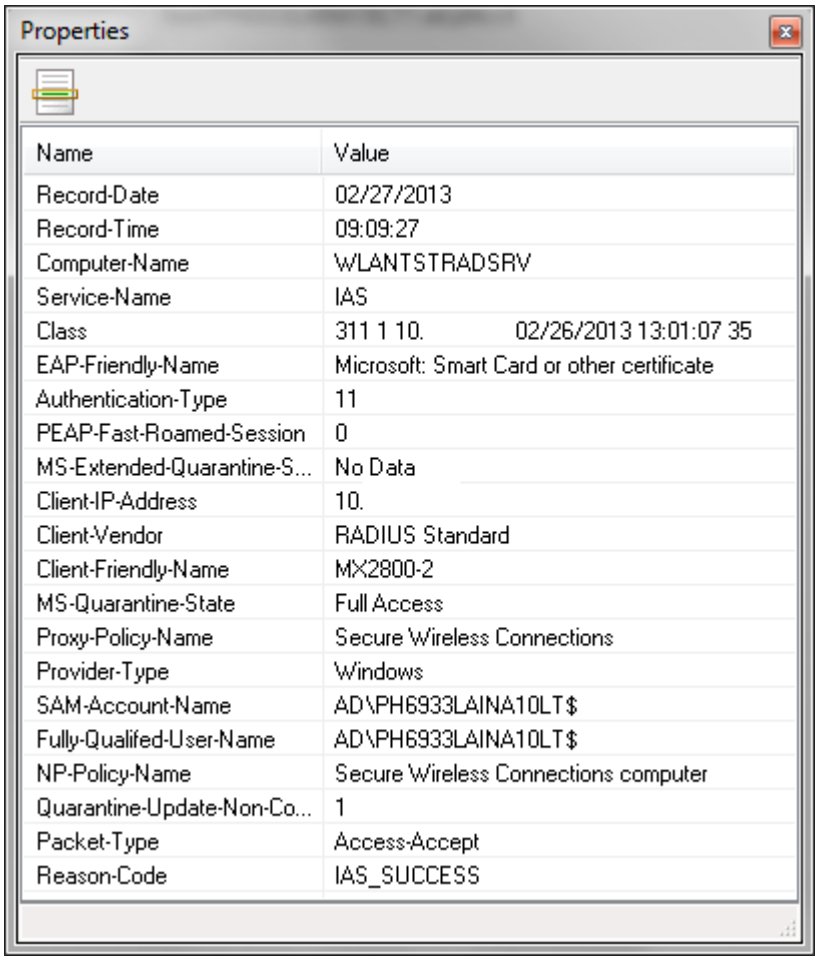
KUVIO 29. Windows XP -koneen langattoman verkon asetukset

Kone ei kuitenkaan onnistunut liitymään verkkoon heti ensimmäisellä yrityksellä. RADIUS-palvelin tallentaa kaikki autentikointiyritykset, paitsi hylätyt access-request-viestit, joten sieltä pystyi helposti tarkistamaan, mihin asti tunnistuksessa oli päästy. Kuviossa 30 on esitetty RADIUS-palvelimen log-tiedostosta otettu kohta, jossa näkyy syy autentikoinnin epäonnistumiselle. RADIUS-palvelin ei pystynyt tarkistamaan juurisertifikaatin sulkulistaa yhteysongelman takia, jolloin myöskään konetta ei voitu päästää verkkoon. Packet-Type -kohdassa näkyy Access-Reject ja sen jälkeen syy. Sulkulista pitää sisällään mitätöidyt sertifikaatit.



KUVIO 30. epäonnistunut autentikointi

Yhteysongelmien korjaamiseen jälkeen kone liittyi ongelmitta verkkoon. Kuviossa 31 on kuvattu vastaavasti, miltä onnistunut autentikointi näyttää RADIUS-palvelimen logeissa.



KUVIO 33. onnistunut autentikointi

Logitiedot ovat hyvä työkalu lähteä selvittämään, jos kone ei pääse verkkoon. Seuraavaksi varmistettiin, että koneelta häviää oikeus verkkoon, jos sen sertifikaatti mitätöidään. Viimeisenä haluttiin tarkistaa, miltä autentikointi näyttää verkossa, ja mitä tietoja sen kautta voitiin nähdä. Kuviossa 34 on esitetty liikennekaappaus Wireshark-työkalulla.

Ensimmäiset 1 - 13 pakettia sisältävät PEAP-tunnelin luonnin. Ensin verkkoon liittyvä laite lähettää identiteettinsä tukiasemalle, josta se menee edelleen RADIUS-palvelimelle asti. RADIUS palvelin kertoo liittyjälle, että käytössä on PEAP. Asiakas vastaa Client Hello -viestillä, joka sisältää sen tukemat salaustavat ja muuta, jota käytetään yhteisen avaimen luomisessa myöhemmin. RADIUS-palvelin lähettää sertifikaattinsa asiakkaalle. Palvelin päättää käytetyn symmetrisen salaustavan tunnelissa ja kertoo sen asiakkaalle.

14 - 35 on tunnelin sisällä menevää autentikointitietoa, jota Wireshark ei pysty purkamaan, koska sillä ei ole tiedossa salausavainta, jonka päätelaite ja RADIUS-palvelin neuvottelivat.

36 on EAP success-viesti, joka kertoo autentikoinnin onnistumisesta.

37 - 40 viesteissä tapahtuu nelivaiheinen kättely istuntokohtaisten avaimien luomiseksi. Loput viestit ovat verkossa tapahtuvat DHCP- ja ARP- kyselyt, jonka jälkeen liikennöinti verkossa on mahdollista.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00	IntelCor_0e:f0:c5	TrapezeN_6e:86:42	EAPOL	19	Start
2	0.00	TrapezeN_6e:86:42	IntelCor_0e:f0:c5	EAP	73	Request, Identity
3	0.00	IntelCor_0e:f0:c5	TrapezeN_6e:86:42	EAP	55	Response, Identity
4	0.02	TrapezeN_6e:86:42	IntelCor_0e:f0:c5	EAP	64	Request, Protected EAP (EAP-PEAP)
5	0.02	IntelCor_0e:f0:c5	TrapezeN_6e:86:42	TLSv1	105	Client Hello
6	0.03	TrapezeN_6e:86:42	IntelCor_0e:f0:c5	TLSv1	1514	Server Hello, Certificate, Certificate Request, Server Hello Done
7	0.05	IntelCor_0e:f0:c5	TrapezeN_6e:86:42	EAP	24	Response, Protected EAP (EAP-PEAP)
8	0.06	TrapezeN_6e:86:42	IntelCor_0e:f0:c5	TLSv1	1514	Server Hello, Certificate, Certificate Request, Server Hello Done
9	0.06	IntelCor_0e:f0:c5	TrapezeN_6e:86:42	EAP	24	Response, Protected EAP (EAP-PEAP)
10	0.07	TrapezeN_6e:86:42	IntelCor_0e:f0:c5	TLSv1	1492	Server Hello, Certificate, Certificate Request, Server Hello Done
11	0.15	IntelCor_0e:f0:c5	TrapezeN_6e:86:42	TLSv1	221	Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
12	0.15	TrapezeN_6e:86:42	IntelCor_0e:f0:c5	TLSv1	75	Change Cipher Spec, Encrypted Handshake Message
13	0.26	IntelCor_0e:f0:c5	TrapezeN_6e:86:42	EAP	24	Response, Protected EAP (EAP-PEAP)
14	0.27	TrapezeN_6e:86:42	IntelCor_0e:f0:c5	TLSv1	64	Application Data
15	0.27	IntelCor_0e:f0:c5	TrapezeN_6e:86:42	TLSv1	82	Application Data
16	0.27	TrapezeN_6e:86:42	IntelCor_0e:f0:c5	TLSv1	65	Application Data
17	0.27	IntelCor_0e:f0:c5	TrapezeN_6e:86:42	TLSv1	51	Application Data
18	0.40	TrapezeN_6e:86:42	IntelCor_0e:f0:c5	TLSv1	64	Application Data
19	0.47	IntelCor_0e:f0:c5	TrapezeN_6e:86:42	TLSv1	132	Application Data
20	0.48	TrapezeN_6e:86:42	IntelCor_0e:f0:c5	TLSv1	1341	Application Data
21	0.52	IntelCor_0e:f0:c5	TrapezeN_6e:86:42	TLSv1	51	Application Data
22	0.53	TrapezeN_6e:86:42	IntelCor_0e:f0:c5	TLSv1	1341	Application Data
23	0.55	IntelCor_0e:f0:c5	TrapezeN_6e:86:42	TLSv1	51	Application Data
24	0.56	TrapezeN_6e:86:42	IntelCor_0e:f0:c5	TLSv1	1341	Application Data
25	0.56	IntelCor_0e:f0:c5	TrapezeN_6e:86:42	TLSv1	51	Application Data
26	0.57	TrapezeN_6e:86:42	IntelCor_0e:f0:c5	TLSv1	629	Application Data
27	0.60	IntelCor_0e:f0:c5	TrapezeN_6e:86:42	TLSv1	1335	Application Data
28	0.65	TrapezeN_6e:86:42	IntelCor_0e:f0:c5	TLSv1	64	Application Data
29	0.67	IntelCor_0e:f0:c5	TrapezeN_6e:86:42	TLSv1	1335	Application Data
30	0.68	TrapezeN_6e:86:42	IntelCor_0e:f0:c5	TLSv1	64	Application Data
31	0.68	IntelCor_0e:f0:c5	TrapezeN_6e:86:42	TLSv1	1031	Application Data
32	0.70	TrapezeN_6e:86:42	IntelCor_0e:f0:c5	TLSv1	102	Application Data
33	0.70	IntelCor_0e:f0:c5	TrapezeN_6e:86:42	TLSv1	51	Application Data
34	0.70	TrapezeN_6e:86:42	IntelCor_0e:f0:c5	TLSv1	120	Application Data
35	0.70	IntelCor_0e:f0:c5	TrapezeN_6e:86:42	TLSv1	120	Application Data
36	0.71	TrapezeN_6e:86:42	IntelCor_0e:f0:c5	EAP	64	Success
37	0.71	TrapezeN_6e:86:42	IntelCor_0e:f0:c5	EAPOL	135	Key (Message 1 of 4)
38	0.72	IntelCor_0e:f0:c5	TrapezeN_6e:86:42	EAPOL	137	Key (Message 2 of 4)
39	0.72	TrapezeN_6e:86:42	IntelCor_0e:f0:c5	EAPOL	169	Key (Message 3 of 4)
40	0.74	IntelCor_0e:f0:c5	TrapezeN_6e:86:42	EAPOL	113	Key (Message 4 of 4)
42	2.75	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0x58c675bf
43	2.86	TrapezeN_7a:c8:12	Broadcast	ARP	60	who has X.X.X.125? Tell X.X.X.11
45	4.75	X.X.X.11	X.X.X.125	DHCP	334	DHCP Offer - Transaction ID 0x58c675bf
46	4.75	0.0.0.0	255.255.255.255	DHCP	385	DHCP Request - Transaction ID 0x58c675bf
47	4.76	X.X.X.11	X.X.X.125	DHCP	334	DHCP ACK - Transaction ID 0x58c675bf
54	7.52	IntelCor_0e:f0:c5	Broadcast	ARP	42	who has X.X.X.1? Tell X.X.X.125
55	7.52	Fortinet_09:02:04	IntelCor_0e:f0:c5	ARP	60	X.X.X.1 is at 00:09:0f:09:02:04

KUVIO 34. Packet capture kannettavan koneen liittymisestä verkkoon

Yksi mahdolliselle hyökkääjälle hyödyllinen tieto on liikenteen kaappauksessa kolmannessa paketissa lähetetty Identity Response, joka sisältää verkkoon liittyvän koneen nimen. Hyökkääjä voisi luoda sertifikaatin itse tällä samalla nimellä, mutta se ei riitä verkkoon pääsylle. Itse luodusta sertifikaatista puuttuu toimialueeseen liitetyn sertifikaattipalvelimen sertifikaatin allekirjoitus.

6 YHTEENVETO

Työssä saavutettiin haluttu lopputulos, kun suunnitellun 802.1x-ratkaisun toteutus ja testaus onnistuivat. Testiympäristöstä on helppo siirtyä pienellä vaivalla tuotantoympäristöön tekemällä tarvittavat käytännöt tuotantoympäristön RADIUS-palvelimelle. Suositeltavaa on myös tehdä monet työssä esitetyt kohdat uudestaan vastamaan yhtymän muuta nimeämiskäytäntöä. DHCP-palvelin voidaan siirtää kontrollerilta pois käyttämällä DHCP-Relay-toimintoa palomuurissa, joka välittää langattoman verkon DHCP-viestit yhtymän sisäverkon DHCP-palvelimille.

Tärkeää olisi tehdä käyttäjille ohjeistus verkosta ja tilanteista, missä kone esimerkiksi katoaa. Vaikka koneelle vaaditaan aina AD-käyttäjätunnus ja salasana sen avaamiseksi, on se silti verkossa, vaikka siihen ei olisi kirjauduttu. Sertifikaattien sulkulistojen avulla koneen sertifikaatti voidaan mitätöidä ennen sen vanhenemista, jolloin koneelta pääsy verkkoon on estetty.

PEAP-käyttö EAP-TLS-kanssa mahdollisti erittäin hyvän toteutuksen tietoturvallisesti ja sen käyttö oli mahdollista, koska työ tehtiin Windows-käyttöjärjestelmille. On hyvä huomioida, jos joskus tulevaisuudessa verkkoon halutaan liittää muita kuin Windows-käyttöjärjestelmällä varustettuja laitteita, että niille täytyy luoda oma verkkokäytäntö RADIUS-palvelimelle. Monesti myös näille laitteille joudutaan verkon asetukset ja mahdolliset sertifikaatit jakamaan muuta kautta.

Tulevaisuudessa langattomista verkoista tulee yhä tärkeämpi osa yritysten muuta tietoverkkoa ja niistä halutaan käyttöön monesti samat resurssit kuin langallisesta verkosta. Jo nykyään lähes kaikilla on laitteita, joilla pystytään liittymään langattomiin verkkoihin. Yritysten verkkoon ei haluta mitä tahansa laitteita, jolloin laitteiden tietoturvallisen autentikoinnin merkitys tulee kasvamaan.

LÄHTEET

Centero Oy. 2012. PKI for Dummies :) [viitattu 26.5.2015]. Saatavissa: http://www.centero.fi/blogi/pki-for-dummies/

Cudbard-Bell, A. 2012. Freeradius wiki EAP-PEAP [viitattu 25.5.2015]. Saatavissa: http://wiki.freeradius.org/protocol/EAP-PEAP

Cisco. 2006. How Does RADIUS Work? [viitattu 26.5.2015]. Saatavissa: http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html

Cisco. 2014. 802.11ac: The Fifth Generation of Wi-Fi [viitattu 22.5.2015]. Saatavissa: http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-3600-series/white_paper_c11-713103.pdf

Digicert. 2015. Behind the Scenes of SSL Cryptography [viitattu 26.5.2015]. Saatavissa: https://www.digicert.com/ssl-cryptography.htm

Geier, J. 2005. Langattomat verkot. Helsinki: Edita Prima Oy.

Gast, M. 2002. A Technical Comparison of TTLS and PEAP [viitattu 25.5.2015]. Saatavissa: http://archive.oreilly.com/pub/a/wireless/2002/10/17/peap.html

Graham-Cumming, J. 2013. Why some cryptographic keys are much smaller than others [viitattu 26.5.2015]. Saatavissa: https://blog.cloudflare.com/why-are-some-keys-small

Granlund, K. 2007. Tietoliikenne. Jyväskylä: WSOYpro.

IEEE 802.11i. 2004. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications [viitattu 23.5.2015]. Saatavissa: http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

Juniper. 2013. Understanding Wireless Encryption and Ciphers [viitattu 23.5.2015]. Saatavissa:

http://www.juniper.net/documentation/en_US/network-director1.5/topics/concept/wireless-encryption-and-ciphers.html

Lehembre, G. 2005. Wi-Fi security – WEP, WPA and WPA2 [viitattu 22.5.2015]. Saatavissa: http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_EN.pdf

Microsoft. 2002. RADIUS Protocol Security and Best Practices [viitattu 25.5.2015]. Saatavissa: https://msdn.microsoft.com/en-us/library/bb742489.aspx

Microsoft. 2003a. How Certificates Work [viitattu 26.5.2015]. Saatavissa: https://technet.microsoft.com/en-us/library/cc776447(v=ws.10).aspx

Microsoft. 2003b. Overview of SSL/TLS Encryption [viitattu 26.5.2015]. Saatavissa: https://technet.microsoft.com/en-us/library/cc781476%28v=ws.10%29.aspx

Microsoft. 2004. Choosing a Strategy for Wireless LAN Security [viitattu 24.5.2015]. Saatavissa: https://www.microsoft.com/en-us/download/details.aspx?id=9904

Microsoft. 2005. MS-CHAP version 2 [viitattu 25.5.2015]. Saatavaissa: https://technet.microsoft.com/en-us/library/cc739678(v=ws.10).aspx

National Instruments. 2013. WLAN - 802.11 a,b,g and n [viitattu 22.5.2015]. Saatavissa: http://www.ni.com/tutorial/7131/en/

Puska, M. 2005. Langattomat lähiverkot. Jyväskylä: Gummerus.

Strand, L. 2004. 802.1X Port-Based Authentication HOWTO [viitattu 22.5.2015]. Saatavissa: http://www.tldp.org/HOWTO/html_single/8021X-HOWTO/

Taylor & Francis Group. 2006. 802.1X Port-Based Authentication [viitattu 25.5.2015]. Saatavissa. http://www.infosectoday.com/Articles/AU4464_C001.pdf