TEKNIIKKA JA LIIKENNE

Tietotekniikka

Tietoliikennetekniikka

INSINÖÖRITYÖ

WAP JA LANGATON TIETOTURVA

Työn tekijä: Juha Uotinen
Työn ohjaajat: Janne Salonen

Työ hyväksytty: ___. ___. 2009

Janne Salonen
lehtori

ALKULAUSE

Tämä insinöörityö tehtiin kirjallisuustutkimuksena Metropolia Ammatikorkeakoululle. Kiitän lehtori Janne Salosta työn ohjaamisesta, sekä vaimoni Virvan ja tyttäreni Vilhelmiinan kärsivällisyydesta työtä tehdessä.

Helsingissä 29.5.2009

Juha Uotinen

Metropolia

TIIVISTELMÄ

Työn tekijä: Juha Uotinen

Työn nimi: WAP ja langaton tietoturva

Päivämäärä: 29.5.2009	**Sivumäärä:** 25 s.
Koulutusohjelma:	**Suuntautumisvaihtoehto:**
Tietotekniikka	Tietoliikennetekniikka

Työn ohjaaja: lehtori Janne Salonen

Työn ohjaaja:

Työ on tehty kirjallisuustutkimuksena WAPista ja siihen liittyvästä langattoman yhteyden tietoturvasta. Työssä käsitellään WAPin kehitystä ensimmäisestä versiosta nykyiseen versioon.

Ensimmäisenä työssä käsitellään WAP-arkkitehtuuria ja protokollia ja niiden vaikutuksia eri versioiden välillä.

Seuraavaksi työssä käsitellään WAP-sivujen sisällön muodostamista WAP 1.x- ja WAP 2.0-versioiden mukaisesti.

Viimeiseksi työssä tarkastellaan turvallisuutta ja sitä miten langattoman yhteyden turvallisuus on hoidettu WAP-ympäristössä.

Avainsanat: WAP 1.x, WAP 2.0, WTLS, WPKI

Metropolia

ABSTRACT

Name: Juha Uotinen

Title: WAP and wireless security

Date: 29.5.2009 **Number of pages:** 25 pages

Department: Information Technology

Study Programme: Telecommunications

Instructor: Janne Salonen

Supervisor:

This final project was made for Helsinki Metropolia University of Applied Sciences. This project are focused to WAP technology and wireless security.

First part of this project was focused on WAP architecture and protocols to different versions.

Second part are focused on making WAP pages on different WAP 1.x and WAP 2.0 version.

Final part are focused on security and how it is made in wireless evironment.

Keywords: WAP 1.x, WAP 2.0, WTLS, WPKI

SISÄLLYS

LYHENTEET

HTML	Hypertext Markup Language, sivunkuvauskieli
HTTP	Hypertext Transfer Protokol, hypertekstin siirtoprotokolla
IP	Internet Protocol, internetprotokolla
PKI	Public Key Infrastructure, julkisen avaimen järjestelmä
SSL	Secure Sockets Leyer, salausprotokolla
TCP	Transmission Control Protocol, tietoliikenneprotokolla
URL	Uniform Resource Locator, osoite
WAE	Wireless Application Evironment, sovellusympäristö
WAP	Wireless Application Protocol, langattoman sovelluksen protokolla
WCSS	Wireless Cascading Style Sheets, langaton tyylitiedosto
WDP	Wireless Datagram Protocol, langaton tiedossiirtoprotokolla
WML	Wireless Markup Language, sivunkuvauskieli
WPKI	Wireless Public Key Infrastructure, langaton julkisen avaimen järjestelmä
WSP	Wireless Session Protocol, langaton istuntoprotokolla
WTA	Wireless Telephone Application, langaton puhelinsovellus
WTLS	Wireless Transport Layer Security, langaton siirtokerroksenprotokolla
WTP	Wireless Transaction Protocol, langaton tapahtuma protokolla
WWW	World Wide Web, maailman laajuinen verkko
XHTML MP	Extensible Hypertext Markup Language Mobile Profile, sivunkuvauskieli matkapuhelimille

XHTML	Extensible Hypertext Markup Language, sivunkuvauskieli
XML	Extensible Markup Language, merkkaus kieli

1 JOHDANTO

Internet on yleistynyt tiedonlähteenä. Valtaosa ihmisistä käyttää palveluita kotoa tai työpaikalta päivittäin. Normaalisti internetin käyttäminen vaatii tietokoneen ja yhteyden internetpalvelimeen. Tämän heikkoutena on kuitenkin rajoitettu liikkuvuus johtuen päätelaitteen koosta, kuten kannettavasta tietokoneesta.

WAP (Wireless Application Protocol) on WAP-Forumin kehittämä menetelmä, joka mahdollistaa internetin palveluiden selaamiseen kannettavalla päätelaitteella, kuten matkapuhelimella ilman erillisiä lisälaitteita. Matkapuhelimen näytön fyysinen koko kuitenkin rajoittaa sisällön paljon kevyemmäksi kuin internetissä on totuttu näkemään.

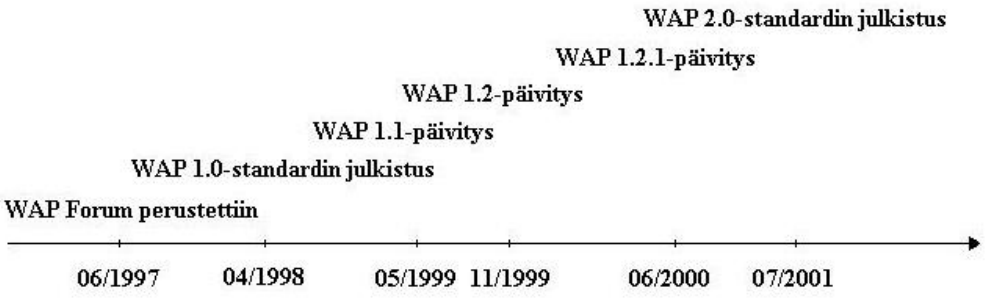
WAP-tekniikkaa ei siis voida pitää WWW:n (World Wide Web) korvaajana, mutta sillä voidaan tarjota lisää vaihtoehtoja julkaista palveluita.

2 WAP

Suuret matkapuhelinvalmistajat Ericsson, Motorola, Nokia ja Unwired Planet perustivat kesäkuussa 1997 WAP Forumin, joka nykyään on nimeltään OMA (Open Mobile Alliance). Tämän yhteistyön tuloksena julkaistiin huhtikuussa 1998 ensimmäinen WAP-standardi, joka sai nimekseen WAP 1.0.

Toukokuussa 1999 seurasi päivitys WAP 1.1 ja jo marraskuussa 1999 julkaistiin seuraava päivitys WAP 1.2. Kesäkuussa 2000 julkaistiin päivitys WAP 1.2.1. Tämä versio on ollut käytössä useimmissa nykyisissä WAP-palveluita tukevissa matkapuhelimissa.

Uusin WAP 2.0 -versio julkaistiin heinäkuussa 2001 ja ensimmäinen tätä versiota tukeva matkapuhelin julkaistiin vuoden 2002 lopulla.

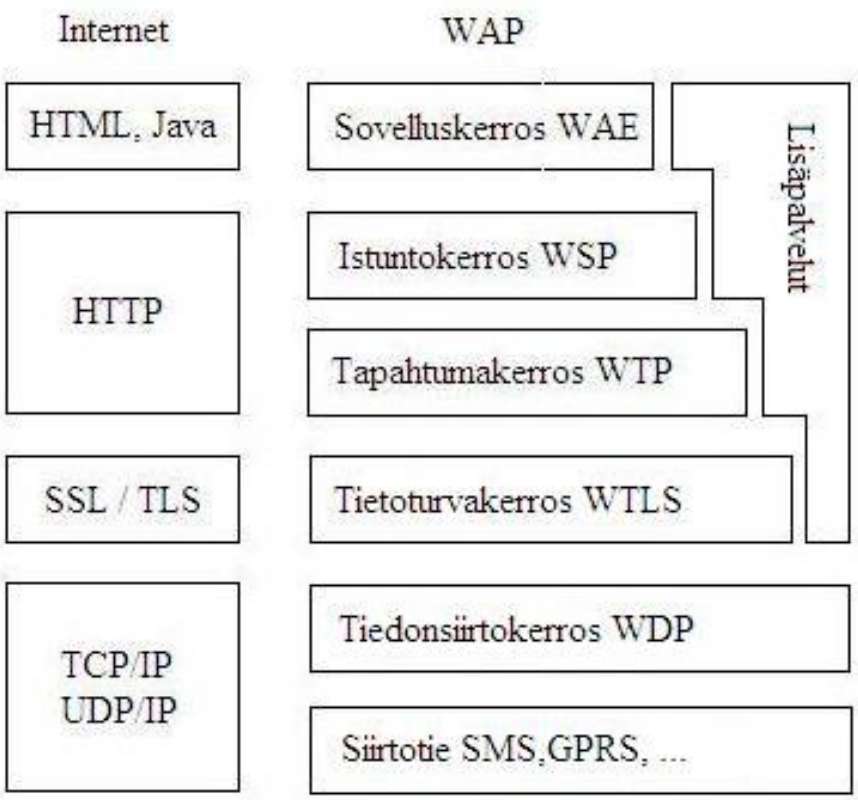


Kuva 1. WAP:n kehitys

2.1 WAP-protokollat

WAP-protokollat voidaan jakaa kolmeen osaan. Niitä ovat WAE (Wireless Application Evironment), varsinainen WAP-protokollapino sekä siirtotieprotokollat. WAE:llä tarkoitetaan käyttäjälle näkyvää WAP-sovellusympäristöä. Tätä vastaa WWW:ssä käytettävä HTML ja JavaScript. WAP-protokollapino muodostuu neljästä kerroksesta: WSP:stä (Wireless Session Protocol), WTP:stä (Wireless Transaction Protocol), WTLS:stä (Wireless Transport Layer Security) ja WDP:stä (Wireless Datagram Protocol). Nämä vastaavat WWW:ssä HTTP:tä ja TLS:ää. Siirtotieprotokollilla tarkoitetaan yhteyskäytäntöjä, joiden avulla voidaan välittää WAP-liikennettä esimerkiksi matkapuhelinverkossa.

WAP 1.x protokollat verrattuna internetprotokolliin on esitetty kuvassa 2.



Kuva 2. WAP 1.x protokollat

Wireless Application Evinroment

WAE on yleinen langattoman WAP-tekniikan ja olemassa olevan WWW-tekniikan yhdistävä langaton sovellusympäristö. WAE-kerrokseen kuuluu muun muassa WAP-selainympäristö. Langattoman maailman WAE vastaa näkyviltä osiltaan WWW-tekniikassa HTML-kielen ja JavaScript-sovellusten muodostamaa palvelukokonaisuutta, jota voidaan tarvittaessa täydentää esimerkiksi CGI-rajapinnan tai PHP-kielen avulla. WAE:n sisältö toteutetaan pääosin WML- (Wireless Markup Language) ja WMLScript-kielillä. WAE:hen kuuluu myös edellä mainittujen sisältötyyppien lisäksi muun muassa WTA (Wireless Telephone Application), WAP-tekniikkaan pohjautuva puhelinrajapinta.

Wireless Session Protocol

WSP tarjoaa sovellusrajapinnan sisältäen kaksi yhteystyyppiä: yhteydellisen ja yhteydettömän muodon. WDP:n päällä toimivaa yhteydetöntä muotoa voidaan käyttää, mikäli sovelluksen ei tarvitse varmistaa tiedon perillemenoa. Hyvä esimerkki tällaisesta sovelluksesta on WWW, jossa kyselyn perillemenoa ei valvota. WTP:n päällä toimivan yhteydellisen muodon tapauksessa

WSP huolehtii yhteyden muodostamisesta ja esimerkiksi sisältötyyppien tunnistuksesta.

Wireless Transaction Protocol

WTP on erityisesti pienitehoisille päätelaitteille suunniteltu kyselyprotokolla. WTP-kyselyt voivat olla joko luotettavia yksi- tai kaksisuuntaisia kyselyitä tai epäluotettavia yksisuuntaisia kyselyitä. Jälkimmäisessä tapauksessa kyselyyn ei edellytetä vastausta. WTP sallii myös asynkroniset kyselyt.

Wireless Transport Layer Security

WTLS on WAP-protokollapinon tietoturvakerros. Läheisesti WWW-tekniikan TLS-tietoturvaominaisuuksia (Transport Layer Security) muistuttavan WTLS:n tarkoituksena on varmistaa tiedon kryptaus salakirjoitus käytettävissä olevalla salausmenetelmällä. WTLS ei ole tiedonsiirron kannalta pakollinen protokollakerros, mutta jokin WAE:n sovellus saattaa edellyttää sen olemassaoloa.

Wireless Datagram Protocol

WDP sijaitsee WAP-protokollista alimpana ja hoitaa varsinaisen tiedonsiirron. WDP sopeutuu tarjolla olevaan siirtotiehen ja muodostaa yhteyden siirtotien ja ylemmän tason protokollien välille. Juuri WDP:n kyky sopeutua useisiin siirtoteihin mahdollistaa WAP:n salliman laajan päätelaitevalikoiman.

Siirtotieprotokollat

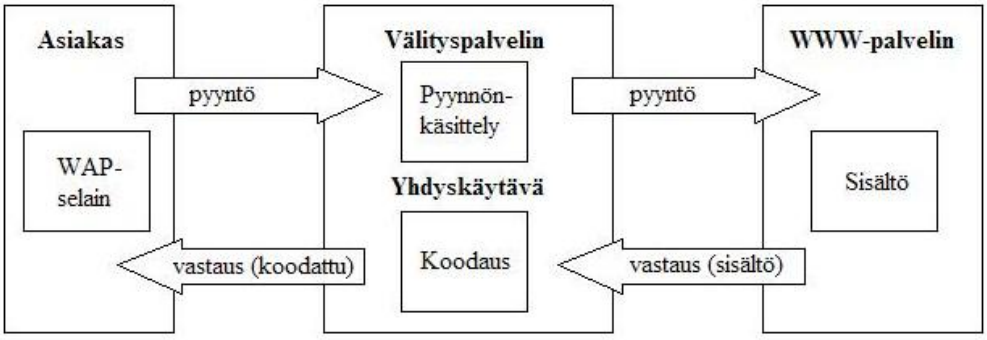
Siirtotieprotokollat tarjoavat nimensä mukaisesti mahdollisuuden tiedonsiirtoon fyysisen väylän, jossa WAP-dataa voidaan kuljettaa. WAP on suunniteltu sopeutumaan useisiin erilaisiin päätelaitteisiin, mikä edellyttää useiden eri siirtoteiden tukea. WAP-siirtotienä voidaan käyttää esimerkiksi SMS-lyhytviestejä tai joko paketti- tai piirikytkentäistä GSM-datayhteyttä. Koska WDP tarjoaa tiedonsiirtokerroksena rajapinnan siirtotieprotokollan ja muun WAP-pinon välillä, määrittelee WDP käytettävissä olevat siirtotieprotokollat ja -tavat, miten tietoa kullakin siirtotiellä siirretään.

2.2 WAP 1.x -arkkitehtuuri

WAP:n ohjelmointimalli pohjautuu WWW:n ohjelmointimalliin, joten WWW-standardin mukaiset URL-osoitteet ovat käytössä myös WAP-arkkitehtuurissa. WAP-arkkitehtuuri määrittelee kuitenkin yhdyskäytävän, jo-

ta käytetään langattoman päätelaitteen ja internetissä sijaitsevan sisältöpalvelimen välillä. WAP-välityspalvelin toteuttaa yhdyskäytävän, joka muuntaa pääteläitteen pyynnöt WAP-protokollasta WWW:ssä käytettäviksi HTTP-, SSL- ja TCP/IP-protokolliksi.

Matkapuhelimessa olevan WAP-selaimen lähettäessä pyynnön se ohjautuu ensin operaattorin, Internet-palveluntarjoajan tai yksittäisen yrityksen omaan WAP-yhdyskäytävään. WAP-yhdyskäytävä tulkitsee WAP-protokollan mukaisen palvelupyynnön ja etsii URL-osoitteessa määritellyn palvelinkoneen ja luo HTTP-yhteyden kyseiseen koneeseen. WAP-yhdyskäytävä esittää pyynnön URL-osoitteen määrittelemästä sisällöstä. HTTP-palvelinkone käsittelee pyynnön ja palauttaa vastauksen. WAP-yhdyskäytävä vastaanottaa sisällön, koodaa sen ja lähettää sen eteenpäin asiakkaalle, jossa WAP-selain tulkitsee sen ja näyttää käyttäjälle (kuva 3).



Kuva 3. WAP-ohjelmoinnin malli

WAP-arkkitehtuurissa WAP-puhelin ei siis voi muodostaa suoraan yhteyttä olemassa olevaan WWW-palvelimeen, vaan välissä on tarvitaan protokollamuunnoksen tekevä WAP-yhdyskäytävä.

2.3 WAP-välityspalvelin

WAP yhteys edellyttää välityspalvelimen käyttöä. Matkapuhelin käyttää seuraavia TCP/IP-portteja muodostaessaan yhteyksiä välityspalvelimen kanssa:

- 9200 yhteydetön
- 9201 yhteydellinen
- 9202 salattu yhteydetön
- 9203 salattu yhteydellinen.

3 WAP-SIVUT

WAP-sisältöpalvelut tuotetaan WML-kielellä, joka on määritelty XML-dokumenttityyppinä ja joka muistuttaa HTML-kieltä. Erona on, että se on kevennetty versio kielestä ja sovitettu pienille päätelaitteille. WAP-selaimella katseltava WML-dokumentti on nimeltään pakka, joka koostuu yhdestä tai useammasta kortista. Pakka vastaa HTML-sivua, ja se tunnistetaan yksilöllisellä URL-osoitteella.

3.1 Wireless Markup Language WML

WML on erityisesti kannettavia päätelaitteita varten suunniteltu sivunkuvauskieli. WML:ää suuniteltaessa on otettu huomioon eritysesti päätelaitteen näytön pienuus, siirtotien kapea kaista sekä rajalliset muisti- ja prosessorikapasiteetit. WML-kielessä on pyritty myös ottamaan huomioon syöttölaitteiden rajoitteet.

XML-standardiin pohjautuva WML käsittää mahdollisuudet tekstiä ja kuvaa sisältävien WAP-dokumenttien esittämiseen. WML-standardi sisältää määritykset tekstin korostamiseen ja muotoiluun. Dokumentteihin on mahdollista sisällyttä erilaisia ohjausrakenteita, kuten valintaikkunoita ja tekstinsyöttöeditoreja.

WML vaikuttaa HTML:n kevennetyltä varsiolta sovitettuna matkapuhelimen tai PDA:n näytölle sopivaan muotoon. Vaikka kieltä on kevennetty HTML:n verrattuna, niin siihen on lisätty toimintoja, joita HTML ei tue, kuten muuttujamäärittelyt.

WML ei määritä HTML:n tavoin sivulle tarkkaa ulkoasua, vaan lopullinen ulkoasun muotoilu jää käyttäjän selainohjelman päätettäväksi. WML-dokumentit ovat rakenteellisia ja pyrkivät vain toimittamaan sisältönsä mahdollisimman laajalle lukijakunnalle. Dokumenteilla ei siis pyritä tavoittelemaan yhtenäistä ulkoasua päätelaitteesta riippumatta.

WML-kielen yksittäiset sivut eli kortit muodostavat laajemman kokonaisuuden, jota kutsutaan pakaksi. Päätelaitteesta ja näytön resoluutiosta riippuen käyttäjä näkee ruudullaan yhden tai useamman kortin. Näytön koosta riipumatta käyttäjän on mahdollista liikkua pakan sisältämien korttien välillä käyttämällä hyperlinkkejä. WML-pakka on URL-osoitteeltaan yhtäläinen HTML-

sivun kanssa. WML-korttien käyttöä WAP-tekniikassa voisi verrata HTML:n <anchor>-tagiin, jolla voidaan määrittää siirtyminen tiettyyn kohtaan dokumentin sisällä.

WAP-sivujen välille voi HTML:n tapaan luoda hyperlinkkejä. Linkit voivat osoittaa joko johonkin korttiin samassa pakassa tai toisessa pakassa olevaan korttin. Hyperlinkkien tehokkaalla käytöllä mahdollisestaan laajojenkin sisältökokonaisuuksien julkaiseminen kannettavissa päätelaitteissa.

3.2 WML-dokumentti

Koska WML-koodi periytyy XML-kielestä, niin sen täytyy sisältää XML-spesifikaation mukainen dokumentin tyypin määrittely heti koodin alussa. Esimerkin 1 mukainen määrittely tulee olla jokaisen WML-dokumentin ensimäisillä riveillä.

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
"http//www.wapforum.org/DTD/wml_1.1.xml">
```

Esimerkki 1. WML-dokumentin määrittely

Dokumentin pakka määritellään <wml>-komennolla, ja se vaatii myös lopetuksen </wml>. Tämä komento vastaa HTML-kielessä <html>-komentoa. Dokumentin sisältö tulee <card>-komennon jälkeen, jota HTML-kielessä vastaa <body>-komento. Esimerkissä 2 on kuvattu yksinkertainen WML-dokumentti, joka tulostaa päätelaitteen näytölle tekstin ”Hei vaan kaikille”. Esimerkissä 3 on vertauksena sama tehtynä HTML-dokumenttina.

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
"http://www.wapforum.org/DTD/wml_1.1.xml">

<wml>
<card id="kortti" title="Esimerkki">

<p>
Hei vaan kaikille
</p>

</card>
</wml>
```

Esimerkki 2. WML-dokumentti

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
http://www.w3c.org/TR/html4/DTD/loose.dtd">

<html>
<head>
<title>Esimerkki</title>
</head>
<body>

<p>
Hei vaan kaikille
</p>

</body>
</html>
```

Esimerkki 3. HTML-dokumentti

3.3 WML-komennot

Seuraavissa taulukoissa 1-4 on lueteltuina WML-dokumentin muodostamiseen käytettäviä komentoja niiden käyttötarkoituksen mukaan ryhmiteltynä. Pakan ja kortin määrittelyihin käytetyistä komennoista pakollisia komentoja dokumentissa ovat <card> ja <wml>.

<card>…</card>-komennon väliin sijoitetaan kortin sisältöön kuuluvat määritteet. Tämä komento esiintyy vaikka pakassa olisikin vain yksi kortti.

Toinen pakollinen komento WML-dokumentissa on <wml>…</wml>-komento, jonka sisälle tulevat pakan ja korttien määrittelyt.

Taulukko 1. Pakan ja kortin määrittelyn komennot

Komento	Käyttötarkoitus
<access>	Määrittelee näkyvyyden kokonaiselle pakalle
<card>	Määrittelee kortin
<head>	Tämän sisällä määritellään <access> ja <meta> komennot
<meta>	Määrittelee metatiedon
<template>	Määritellään pakan korteille yhtenevä malli
<wml>	Määrittelee pakan

Taulukko 2. Tekstin määrittelyn komennot

Komento	Käyttötarkoitus
 	Sivunvaihto
<p>	Tekstielementti
<table>	Määrittelee taulukon
<td>	Määrittelee taulukon solun
<tr>	Määrittelee taulukon rivin

Taulukko 3. Tekstin muotoilun komennot

Komento	Käyttötarkoitus
<b>	Tekstin lihavointi
<big>	Fontin suurennus
	Teksti korostus
<i>	Tekstin kursivointi
<small>	Fontin pienennys
	Tekstin korostus
<u>	Tekstin alleviivaus

Taulukko 4. Kuvien ja linkkien määrittelyn komennot

Komento	Käyttötarkoitus
<a>	Määritellään linkki
<anchor>	Määritellään linkki dokumentin sisällä
<img>	Määritellään kuva

Tekstin ja kuvien määrittelemiseen ja muotoiluun käytetyt komennot ovat siis samankaltaisia kuin HTML-sivuissa käytettävät. WAP-sivuja tehtäessä täytyy muistaa, että WML-dokumentin komennot pitää olla pienellä. Tämä ei ole pakollista HTML-dokumentissa, mutta on nykyisen määrityksen mukaan suositeltavaa.

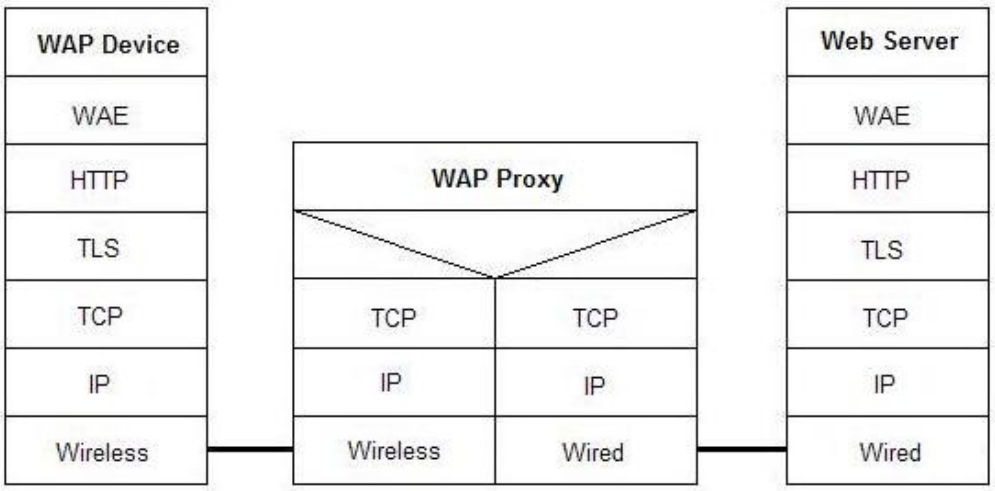
4 WAP 2.0

Vuonna 2001 julkistettiin uusi versio WAP 2.0. Tämän julkistuksen myötä WAP lähestyi internetiä, kun mukaan tuli tuki internetistä tutuille protokollille IP, TCP ja HTTP. Tuen näille mahdollisti aiempaa nopemmat langattomat yhteydet, kuten 3G.

Uuden version myötä tietoturvaan saatin parannusta, kun halutessaan voidaan toteuttaa päästä-päähän-suojaus protokollien päätepisteiden välillä.

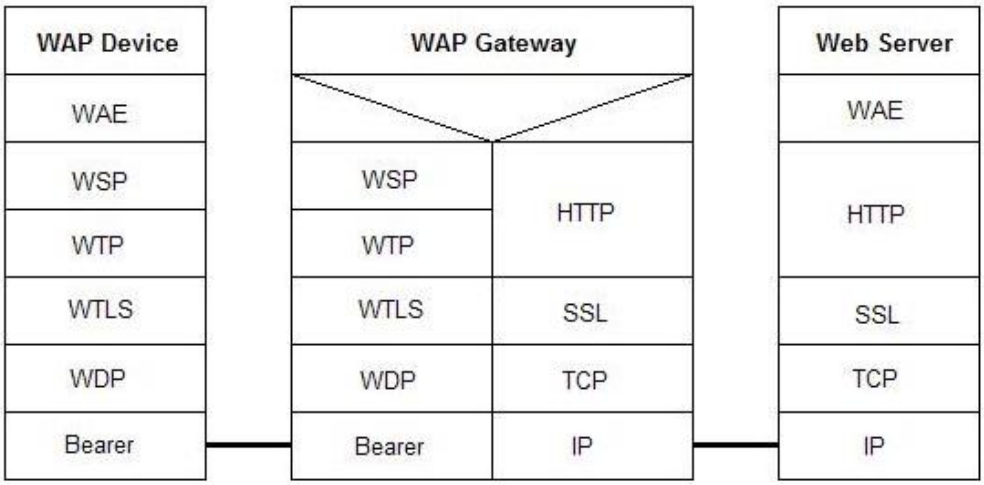
4.1 WAP 2.0 -yhteyden muodostus palvelimeen

WAP 2.0:ssa voidaan yhteys muodostaa suoraan web-palvelimeen, joten siinä ei tarvita välissä WML-muunnosta tekevää WAP Gatewaytä, kuten vanhemmissa WAP-versioissa (kuva 4).



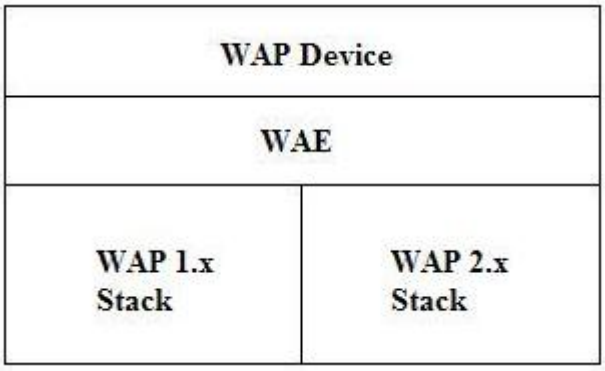
Kuva 4. WAP 2.0 proxy

Vanhemmissa WAP 1.x -versioissa yhteyden muodostamiseen web-palvelimeen tarvittiin väliin WAP Gateway. Tämä teki muunnoksen WML-dokumentista binäärimuotoiseksi päätelaitteelle (kuva 5).



Kuva 5. WAP 1.x gateway

WAP 2.0 tukee molempia pinoja, joten ne toimivat itsenäisesti omina pinoinaan (kuva 6). Yhteyttä muodostettaessa käytetään sille vaadittavaa protokollapinoa. WAP 2.0 -yhteydessä käytetään sille määriteltyä protokollapinoa. Vanhemman version mukaiseen yhteyteen käytetään sille tarkotettua WAP 1.x -protokollapinoa.



Kuva 6. Kahden pinon tuki

4.2 WAP 2.0 -sisältö

WAP 2.0 -selaimesta käytetään nimitystä XHTML-selain. Sivut on toteutettu XHTML-kielellä, joka on yhdistelmä HTML:stä ja XML:stä. WAP 2.0:ssa käytetään oikeastaan erikseen mobiililaitteille kehitettyä versiota XHTML MP, johon on lisätty tuki WCSS-tyylitiedoille.

XHTML MP on hieman kevyempi versio WWW:ssä käytetystä XHTML:stä, koska siinä ei ole mm. tukea kehyksille. WAP 2.0 -päätelaitteella pystyy selaamaan WWW:ssä olevia sivuja, mutta ne eivät kuitenkaan välttämättä toimi kovinkaan hyvin sivujen koosta ja näytön resoluutiosta johtuen. Jo olemassa olevat sivut on helppo muuttaa kuitenkin pieniin päätelaitteisiin sopivaan muotoon, kun toteutus tapahtuu käytännössä samalla kielellä. Tärkeintä asiassa on muistaa kuitenkin pitää sivujen koko pienenä, jotta sivujen latausajat pysyvät lyhyinä.

WAP 2.0 päätelaite tukee myös WAP:in vanhempia versioita, joten sillä pystyy selaamaan myös WML-kielellä toteutettuja dokumentteja. Tämä johtuu siitä, että kehitettäessä WAP 2.0 spesifikaatiota haluttiin säilyttää tuki vanhalle tekniikalle.

WAP 2.0:ssa sisältö välitetään suoraan palvelimelta päätelaitteelle, joten erillistä käännöstä ei tarvitse välissä tehdä, vaan päätelaitteen selain muokkaa sille sopivan ulkoasun.

4.3 XHTMP MP

Jokaisen XHTML MP -dokumentin alussa tulee olla esimerkin 4 mukainen dokumenttityypin määrittely.

```
<?xml version="1.0"?>
<!DOCTYPE html PUBLIC"-//WAPFORUM//DTD XHTML Mobile 1.0//EN"
"http://www.wapforum.org/DTD/xhtml-mobile10.dtd">
```

Esimerkki 4. XHTML MP -dokumentin määrittely

XHTML MP -dokumentin rakenne on samanlainen kuin HTML-dokumentin rakenne, joten dokumenttien laatiminen on usealle totutun mukainen. XHTML-dokumentti on hieman kurinalaisempaa, jolloin lähdekoodista tulle myös siistimpää. Lähdekoodilta vaaditaan seuraavia ulkoasullisia vaatimuksia.

- Tagit tulee olla kirjoitettuna pienaakkosin.
- Tagit tulee olla päätetty asianmukaisesti.
- Atribuuttien arvot tulee olla sijoitettu lainausmerkkien sisälle.
- Atribuuttien lyhentäminen ei ole sallittua.
- Tagien tulee olla suljettu oikeassa järjestyksessä.

Näiden säännösten takia lähdekoodi on selkeämpää ja siistimpää. Esimerkissä 5 on kuvattuna edellisten esimerkkien kanssa saman kaltainen XHTML MP -dokumentti määrittelyineen. Matkapuhelimen selaimelle tulee näkyviin teksti ”Hei vaan kaikille”.

```
<?xml version="1.0"?>
<!DOCTYPE html PUBLIC"-//WAPFORUM//DTD XHTML Mobile 1.0//EN"
"http://www.wapforum.org/DTD/xhtml-mobile10.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>Esimerkki</title>
</head>
<body>

<p>
Hei vaan kaikille
</p>

</body>
</html>
```

Esimerkki 5. XHTML MP -dokumentti

Pienten päätelaitteiden tarpeisiin suunniteltuja sivuja ei ulkoasullisesti määritellä yhtä tarkasti, kuten normaalisti nettisivuja tehtäessä. Tämä johtuu yksinkertaisesti siitä, että esim. matkapuhelimien näytöt ovat eri kokoisia, joten on mahdotonta määritellä sivuja jotka näyttäisivät kaikissa pääteläitteissa samanlaisilta. Ulkoasun määrittely jätetään siis selaimen tehtäväksi. Tästä

johtuen myös sivulla olevien kuvien tulisi olla kooltaan melko pieniä, jotta sivun ulkoasu olisi mahdollisimman selkeä ja helposti selattavissa.

XHTML MP -dokumentti tukee WCSS-tyylitietoja, joten kehitettävien sivujen tyylitiedot kannattaa tehdä erilliseen CSS-tiedostoon. Tämän menettelyn ansiosta sama tyyli on helppo lisätä kaikille tehtäville sivuille, eikä niitä tarvitse kirjoittaa erikseen jokaiselle sivulle.

CSS-tyylitiedot voidaan sijoittaa sivulle sisäisenä- tai ulkoisenalinkkinä. Tämän tyylitiedoston tarkoituksena on antaa sivuille yhtenäisen tyylin. Tyylitiedostoon voidaan tehdä muun muassa seuraavat määritteet:

- tausta, määritetään sivuille tausta (väri tai kuva)
- teksti, määritellään tekstin väri ja fontin koko
- tekstin asemointi, määritellään tekstin sisennykset
- linkit, määritellään miten linkit näytetään.
- kuvat, määritellään kuvien sijoitukset.

5 TURVALLISUUS

WAP-palveluiden turvallisuutta on kehitetty ensimmäisen version jälkeen, jossa oli selvästi heikko tietoturvataso. Tietoturvan heikkous johtui erityisesti päätelaitteen pienestä prosessoritehosta ja pienestä muistista. Lisäksi turvallisuutta heikensi yhteyden välissä oleva WAP-gateway, joka tallensi käyttäjän tietoja palvelimeen.

WAP 2.0 -julkistuksen mukana tuli tietoturvaan merkittävää parannusta, kun mahdollistettiin päästä päähän turvallisuus kahden päätelaitteen välillä.

Turvallisuutta tarvitaan tiedon oikeellisuuden varmistamiseen, sekä haluttaessa välittää tieto vain ennalta tarkoitetulle taholle, siten ettei muut pysty sen sisältöä lukemaan ja muuttamaan. Yhteyden turvallisuutta tarvitsevia palveluita ovat mm. pankki- ja verkkokauppapalvelut.

Hyvältä tietoturvalta yleisesti vaadittavia asiota ovat

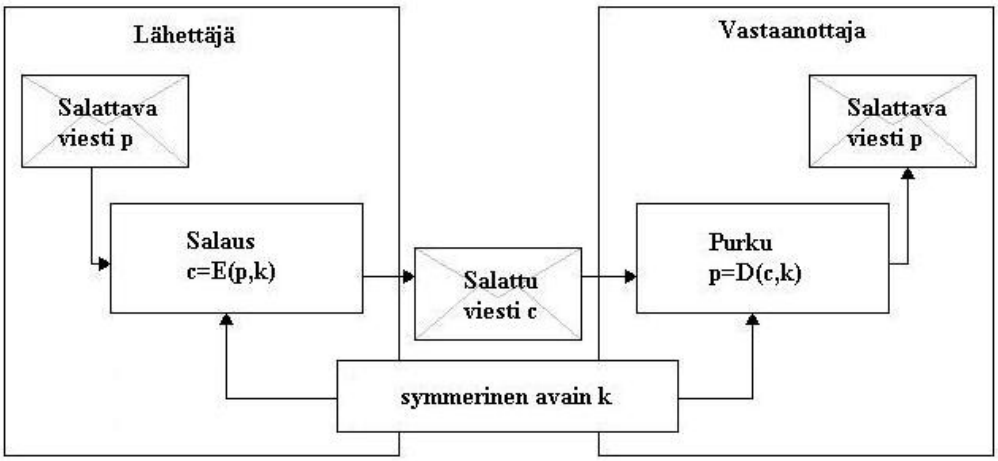
- yksityisyys, eli halutaan ettei kukaan pääse välissä tarkastelemaan sisältöä.
- eheys, eli varmistutaan ettei paketti ole muuttunut lähetyksen aikana.
- todennettavuus, eli varmistetaan että molemmat osapuolet ovat niitä joita sanovat olevansa.
- kiistättömyys, eli kumpikaan osapuoli ei pysty kiistämään tapahtumaa.

5.1 Symmetrinen salaus

Lähetettäessä suojaamatonta kanavaa pitkin viestiä, jota ei haluta muiden kuin vastaanottajan pystyvän lukemaan, tarvitaan salausta. Salaus voidaan suorittaa erilaisilla menetelmillä. Yksi käytettävä tapa on salata viesti symmetrisesti, eli salausmetodi on yleinen, mutta salausavain on vain kummankin osapuolen tiedossa.

Tämä menetelmä on helposti purettavissa niin sanotulla väsytysmenetelmällä, jossa ajetaan eri avaimia läpi, kunnes oikea osuu kohdalle. Tätä menetelmää vastaan voidaan suojautua valitsemalla salausavain riittävän pitkäksi, jolloin mahdollisen salausavaimen löytäminen kestää nykyisillä laskentatehoilla liian kauan ratkaistavaksi.

Symmetrisessä menetelmässä käytetään siis samaa salausavainta viestin salaamiseen ja purkamiseen, joten salausavain on pidettävä siten ettei ulkopuoliset pääse siihen käsiksi. Kuvassa 7 on esitetty symmetrisen salauksen periaate. Salattava viesti p ja symmetrinen avain k syötetään salausalgoritmille E, jonka tuloksena on salattu viesti c. Tämä viesti välitetään avoimessa verkossa vastaanottajalle, joka purkaa salauksen purkualgoritmilla D ja symmetrisellä avaimella k. Tämän tuloksena vastaanottaja saa alkuperäisen viestin p.



Kuva 7. Symmetrinen salaus

Salausmenetelmän ydin on salausalgoritmi. Erilaisia symmetrisiä salausalgoritmeja on useita ja vanhimmat ovat melko helposti purettavissa yksinkertaisillakin välineillä. Nykyään käytössä olevia salausalgoritmeja ei pystytä oleellisesti purkamaan kuin väsytysmenetelmällä. Yksi tunnetuimmista salausalgoritmeista on DES (Data Encryption Standard).

Salausalgoritmista riippumatta symmetrinen salaus johtaa ongelmaan, jossa salattujen viestien vaihtaminen edellyttää sovittua salausavainta, joka ei ole muiden kuin lähettäjän ja vastaanottajan tiedossa.

Koska keskenään kommunikoivien osapuolten määrä avoimessa verkossa on todella suuri, niin ei voida olettaa, että jokaisen osapuolen kanssa olisi ennalta sovittuna salausavain. Siispä käytännön ratkaisuissa osapuolet sopivat symmetrisestä avaimesta silloin, kun haluavat aloittaa salattujen viestien lähettämisen toisilleen. Tämän jälkeen osapuolten viestit salataan ns. istuntoavaimella, kunnes asia on saatu toimitetuksi ja suojattu yhteys voidaan purkaa.

5.2 Epäsymmetrinen salaus

Symmetristen salausmenetelmien rinnalle kehitettiin epäsymmetrinen salausmenetelmä 1970-luvulla. Epäsymmetrinen eroaa siten, että salausmenetelmässä käytetään yhden avaimen sijasta kahta eri avainparia, joka koostuu kahdesta avaimesta: julkisesta avaimesta ja yksityisestä avaimesta. Avainten välillä on matemaattinen yhteys, mutta yksityistä avainta on mahdoton päätellä, mikäli vain julkinen avain tunnetaan. Julkinen avain voidaan siis

huoletta julkistaa. Epäsymmetrinen salausmenetelmä tunnetaan myös julkisen avaimen salausmenetelmänä.

Sovellettaessa epäsymmetristä salausmenetelmää jokaisella kommunikoivalla osapuolella on ainakin yksi avainpari. Kukin osapuoli asettaa julkisen avaimensa muiden kommunikoivien osapuolien saataville. Avain voidaan tallettaa esimerkiksi julkiseen avainhakemistoon, josta halukkaat voivat sen noutaa. Sen sijaan yksityinen avain pidetään tarkasti vain omassa hallussa eikä sitä saa missään tapauksessa päästää muiden tietoon.

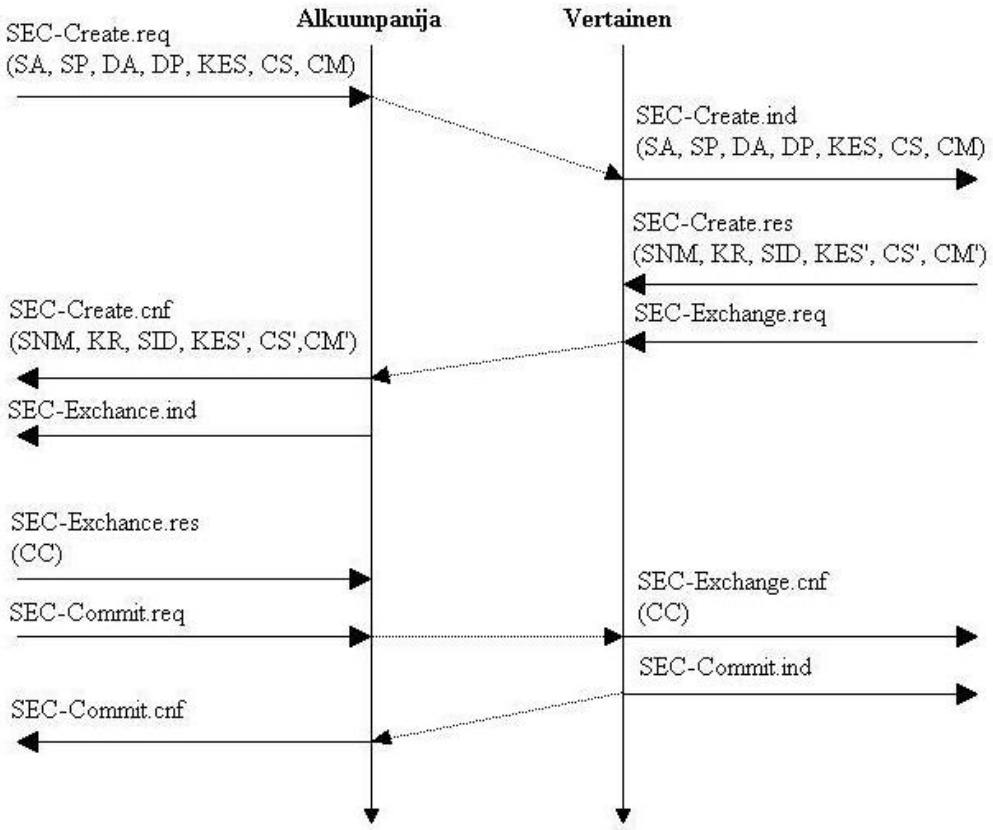
Epäsymmetrisiä salausalgoritmeja tunnetaan useita. Osa algoritmeista on yleiskäyttöisiä ja toiset taas soveltuvat johonkin eritystarkoitukseen, kuten avaimen sopimiseen tai digitaaliseen allekirjoitukseen. Yleisin yleiskäyttöön tarkoitettu salausalgoritmi on RSA, joka tulee kehittäjien nimistä (Rivest, Shamir, Aldeman).

5.3 WTLS

Wireless Transport Layer Security on vastuussa WAP-yhteydessä käytettävästä turvallisuudesta. WTLS perustuu kuljetuskerroksen turvallisuuteen TLS (Transport Layer Security) tai aikaisemmin käytössä olleeseen SSL:ään (Secure Sockets Layer), joka on tunnettu WWW:stä. WTLS on optimoitu langattomien verkkojen kapeakaistaisten kanavien käyttöön.

Mikäli sovellus pyytää turvallisuuspalvelua, voidaan WTLS integroida WDP:n päälle. WTLS tarjoaa eri tasoista turvallisuutta yksityisyyteen, tiedon eheyteen ja todennukseen.

Ennen kuin tietoa voidaan vaihtaa WTLS:n kautta, pitää sitä ennen muodostaa turvallinen istunto. Istunto voidaan keskeyttää milloin tahansa, jos ehdotetut parametrit eivät ole hyväksyttäviä. Kumpikin osapuoli voi keskeyttää istunnon milloin tahansa. Kuvassa 8 on esitetty turvallisen istunnon muodostus.



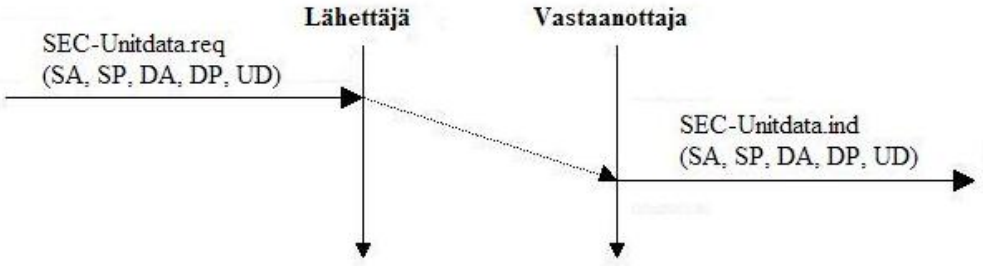
Kuva 8. Turvallisen istunnon muodostus

Ensimmäisessä vaiheessa aloitetaan istunto SEC-Create-primitiivillä. Parametreinä on lähdeosoite SA (Source Address), lähdeportti SP (Source Port), kohdeosoite DA (Destination Address) ja kohdeportti DP (Destination Port). Lisäksi ehdotetaan avainten vaihtoperhettä KES (Key Exchance Suite), salausavainperhettä CS (Cipher Suite) ja pakkausmenetelmää CM (Compression Method). Vertaislaite vastaa parametreihin järjestysnumeromuodolla SNM (Sequence Number Mode), avaimen virkistysjaksolla KR (Key Refresh), istunnon tunnisteella SID (Session Identifier) ja valituilla avaimen vaihtoperhellä KES', salausavainperhellä CS' sekä pakkaus-menetelmällä CM'. Vertaislaite antaa myös SEC-Exchance-primitiivin, joka ilmaisee sen, että vertaislaite haluaa suorittaa julkisen avaimen todennuksen asiakkaan kanssa.

Ensimmäisen vaiheen jälkeen muodostettaessa turvallista istuntoa alkuunpanija vastaa sertifikaatipyyntöön ja lähettää asiakassertifikaatin CC (client certificate). Alkuunpanija lähettää samalla myös SEC-Commit.req-primitiivin, joka ilmaisee vertaiselle, että kättely on päättynyt alkuunpanijan puolella ja haluaa nyt kytkeytyä neuvoteltuun yhteystilaan. Vertaislaitteen WTLS-kerros

lähettää takaisin vahvistuksen alkuunpanijalle. Tämä päättää turvallisen istunnon muodostamisen kättelyn.

Sen jälkeen, kun turvallinen yhteys on muodostettu kahden vertaislaitteen välille, niin käyttäjädataa voidaan välittää. Käyttäjädataa välitetään SEC-Unitdata-primitiivillä lähettäjän ja vastaanottajan välillä. Tämä tiedonsiirto on epäluotettavaa, mutta nyt turvallista (kuva 9).



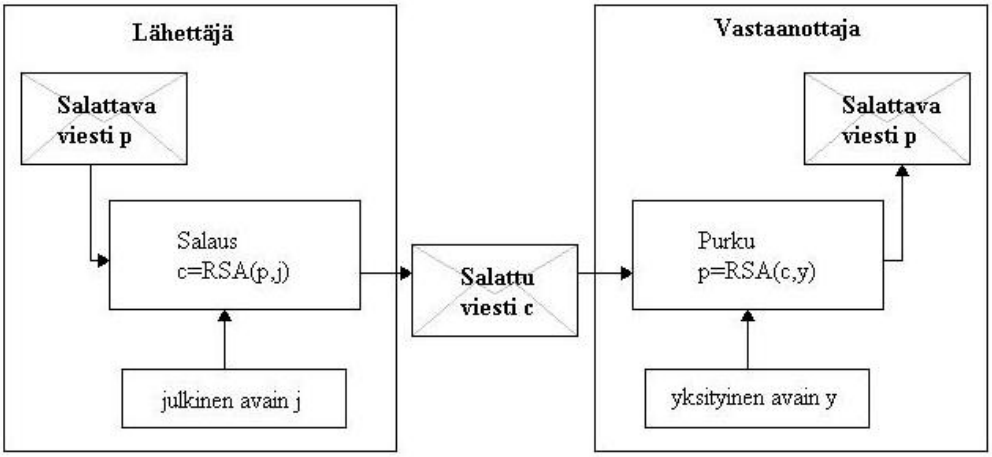
Kuva 9. WTLS-tiedonsiirto

5.4 Public Key Infrastructure PKI

PKI on julkisen avaimen järjestelmä. Tällä tarkoitetaan järjestelyä, jolla tieto suojataan avoimissa tietoverkoissa epäsymmetrisellä salauksella. Järjestelmän salaukseen kuuluu avainparit julkinen ja salainen avain. Avainparit varmennetaan digitaalisella allekirjoituksella.

Julkisen avaimen järjestelmässä lähettäjä salaa viestin vastaanottajan julkisella avaimella. Salaus voidaan purkaa vain vastaanottajan salaisella avaimella, eli lähettäjä ei pysty itsekään enää purkamaan viestiä tämän jälkeen. Digitaalinen allekirjoitus suoritetaan omalla salaisella avaimella, jolloin vastaanottaja voi varmistaa allekirjoituksen lähettäjän julkisella avaimella. Tällaista salausta ja varmennusta tarvitaan yleisesti mm. pankki- ja verkkokauppapalveluissa.

Julkisen avaimen järjestelmässä käytetään epäsymmetristä salausmenetelmää. Kuvassa 10 on esitetty julkisen avaimen järjestelmän viestin salaus käyttäen RSA-algoritmia. Salattava viesti p salataan RSA-algoritmilla käyttäen vastaanottajan julkista avainta j. Tuloksena tästä saadaan salattu viesti c, joka välitetään vastaanottajalle avoimessa verkossa. Vastaanottaja purkaa salatun viestin RSA-algoritmilla ja omalla yksityisellä avaimellaan, jonka tuloksena saadaan alkuperäinen salaamaton viesti p.



Kuva 10. Viestin salaaminen RSA-algoritmilla

Julkisen avaimen järjestemässä yleisimmin kätössä oleva salausalgoritmi on RSA, joka tulee sen kehittäjien nimistä Ron Rivest, Adi Shamir ja Len Adleman. Menetelmä on julkistettu jo vuonna 1978.

5.5 WPKI

WAP-ympäristössä on käytössä WPKI (Wireless Public Key Infrastructure), joka on langattoman verkon käyttöön suunniteltu julkisen avaimen järjestelmä. Järjestelmässä voidaan käyttää X.509-varmenteiden lisäksi WTLS-varmenteita.

WTLS-varmenteet ovat WAP-forumin määrittelemiä langattomaan ympäristöön tarkoitettuja varmenteita. WTLS-varmenteet pohjautuvat X.509-varmenteisiin, mutta ovat kooltaan pienempiä ja soveltuvat täten paremmin langattomaan ympäristöön.

X.509- ja WTLS-varmenteita käyttämällä mahdollistetaan WPKI:n liittäminen jo olemassa oleviin PKI-ympäristöihin. Samalla vähennetään verkon liikennettä ja säästetään päätelaitteiden suoritustehoa sekä tallennuskapasiteettiä. WPKI perustuu seuraaviin määrityksiin:

- Päätelaitteilla säilytettävät WTLS-palvelimien ja varmentajien varmenteet ovat WTLS-varmenteita.
- Palvelimilla säilytettävät WTLS-palvelimien ja varmentajien varmenteet ovat X.509-varmenteita.
- Langattoman tietoyhteyden yli lähetettävät tai päätelaitteessa säilytettävät asiakkaiden tai juurivarmentajien varmenteet ovat X.509-varmenteita.

- Päätelaitteella suositellaan säilyttämään URL:ia varmennepalvelimella sijaitsevalle varmenteelle, mikäli muulloin pitäisi lähettää X.509-varmenteita langattoman tietoyhteyden yli.
- X.509-varmenteita säilytetään päätelaitteissa ainoastaan tilapäisesti.

5.6 Varmenteet

Julkisen avaimen järjestelmässä kiistämättömyys varmistetaan sertifikaattien eli varmenteiden avulla. Varmenne on tavallisesti luotettavan kolmannen osapuolen tarjoama todistus varmennettavan identiteetistä. Luotettavaa tahoa, joka tarjoaa tällaista palvelua, kutsutaan varmentajaksi CA (Certification Authority).

Varmentajat toimivat hierarkisesti siten, että juurivarmentaja RCA (Root Certification Authority) varmentaa alemman tason varmentajia, jotka toimivat yksityisten tahojen varmentajina. Tällaisia julkisia varmennuksia tarjoaa Suomessa muun muassa väestörekisterikeskus.

Varmenteen avulla voidaan käyttäjän identiteetin lisäksi osoittaa käyttäjän hallinnoima julkinen avain. Varmenteen loppuun on liitetty varmentajan salaisella avaimella digitaalisesti allekirjoitettu tiiviste. Mikäli kommunikoivat osapuolet eivät tunnista toistensa varmentajia allekirjoituksia tarkastettaessaan, voivat he tarkastaa varmentajien varmennusketjun, kunnes vastaan tulee tunnettu varmentaja tai juurivarmentaja.

X.509 -varmenne

Varmenteeseen sisältyviä tietoja kutsutaan kentiksi ja niitä on X.509 tapauksessa määritelty lähes kolmekymmentä. Osa kentistä on pakollisia ja osa vapaaehtoisia. Kuvassa 11 on esitetty X.509-varmenteen rakenne.

Kuva 11. X.509-varmenteen rakenne

Versio-kenttä ilmaisee, mistä varmenteen versiosta on kyse. Käytössä tällä hetkellä on yleisesti versio v3, joka sallii laajennuskenttien määrittelyn varmenteisiin. Sarjanumero on varmentajan antama juokseva numero varmenteelle. Jokaisella varmentajan antamalla varmenteella tulee olla eri sarjanumero.

Allekirjoitusalgoritmi määrittelee algoritmin, jota varmentaja on käyttänyt muodostaessaan digitaalisen allekirjoituksen varmenteesta. Myöntäjän nimi on varmenteen myöntäjän X.500-muotoinen nimitunniste.

Voimassaoloaika kuvastaa varmenteen alkamis- ja päättymisajankohdan. Haltijan nimi kenttä kertoo varmenteen haltijan X.500-muotoisen nimitunnisteen.

Julkisen avaimen tiedot sisältää varmenteen haltijan julkisen avaimen. Tietokenttä sisältää myös tunnisteen, johon salausalgoritmiin kyseinen avain

sopii. Varmentajan tunniste ja varmenteen haltijan tunniste kenttiä käytetään myöntäjän ja haltijan yksilöiviin tunnisteisiin.

Laajennusosa kentässä voidaan esittää jotain muuta käyttäjäkohtaista tietoa, kuten mistä sulkulistat voidaan hakea. Allekirjoituskentässä on koko varmenteesta muodostettu digitaalinen allekirjoitus.

WTLS-varmenne

WTLS-varmenne perustuu X.509-varmenteeseen, mutta ne ovat kooltaan pienempiä. Kuvassa 12 on esitetty varmenteen rakenne.

Kuva 12. WTLS-varmenteen rakenne

Versio-kenttä kuvaa varmenteen versionumeron, joka on nykyisen määrityksen mukaan 1. Allekirjoitusalgoritmi on WTLS-määritelmässä tuettu allekirjoitusalgoritmi, jota on käytetty varmenteen allekirjoitukseen.

Myöntäjä ilmaisee varmenteen allekirjoittajan. Voimassaoloaika määrittelee varmenteen voimassaolon alkamis- ja päätymisajankohdan. Haltija-kenttä kuvastaa varmenteen omistajan tiedot.

Julkisen avaimen tiedot-kenttä sisältää julkisen avaimen algoritmin, jonka syötteenä avainta voidaan käyttää. Julkista avainta ei esitetä varmenteessa, vaan ainoastaan palvelimen osoite, josta varmenne ja julkinen avain on noudettavissa. Allekirjoitus on varmenteesta muodostettu digitaalinen allekirjoitus.

6 TUTKIMUKSET

WAP-tekniikan vanhentuessa tutkimustyötä tekniikan parissa ei ole varsinaisesti ollut vähään aikaan. Kehitys on lähinnä keskittynyt matkapuhelinten osalta langattomien lähiverkkojen mahdollistamiseen matkapuhelimeen ja päätelaitteen selaimen kehittämiseen.

Kehitystyö selaimin parissa on keskittynyt niin sanottuun täyteen salailuun, eli selaimella tulisi pystyä selaamaan sekä web-sivuja että eri WAP-versioiden sivuja.

Vuosia erillään olleet WAP-ja WWW-ympäristö on tullut HSDPA ja WLAN yhteyksien vuoksi siihen pisteeseen, että nykyään vaatimuksena matkapuhelinten osalta edellytetään molempien tekniikoiden käsittely kykyä. Monet selainohjelmia kehittävät tahot ovat julkaisseet omat versionsa selaimesta, jotka pystyvät käsittelemään molempia WAP- ja WWW-sivuja.

Matkapuhelinten prosessorin suorituskyky ja muistikapasiteetti on merkittävästi kasvanut vuosien saatossa, sekä matkapuhelinten näyttöjen koko on merkittävästi suurentunut. Lisäksi matkapuhelinten tiedonsiirtonopeudet ovat merkittävästi parantuneet. Näiden vuoksi WWW-sovellusten käyttäminen matkapuhelimella on mahdollista.

7 YHTEENVETO

WAP on ollut jo vuosia käytössä, mutta ihmisten kiinnostus palveluihin on ollut melko vähäistä johtuen suurelta osin alku aikojen sisällön vähäiseen tarjontaan. Ensimmäisten versioiden aikaan operaattorit rajoittivat WAP-yhteyksiä ja ne olivat melko kalliita käyttää. Ongelmana olivat myös silloin käytössä olleet hitaat yhteydet. Näistä seikoista johtuen ihmisten kiinnostus kyseisiin palveluihin katosi, kun sisältökään ei vastannut sitä, mihin oltiin WWW-sovelluksissa totuttu.

Kun uudistuksen myötä mukaan tuli myös nopeammat yhteydet ja mahdollisuus näyttävämpiin sivuihin, oli ihmisten kiinnostus jo asiaa kohtaan kadonnut. WAP ei ole siis oikein koskaan lyönyt itseään läpi.

Tänä päivänä langaton verkko WLAN on monin paikoin saatavilla käyttöön kaupungilla ja esimerkiksi kahviloissa. Lisäksi 3G-verkkoa hyväksi käyttävät modeemit ja niiden palvelut ovat tulleet edullisiksi. Näiden lisäksi markkinoille on tullut pieniä nettikäyttöön tarkoitettuja kannettavia tietokoneita, joita kaupataan kyseisten palveluiden yhteydessä. Nämä yhdessä ovat aiheuttaneet entisestään WAP-palveluiden ja siihen kiinnostuksen hiipumisen.

VIITELUETTELO

[1] Mobile Communications 2nd edition, Jochen Schiller, Addiso-Wesley 2003 [s. 392 - 439].

[2] Inside WAP, Pekka Niskanen, IT Press 2000 [s. 9 - 25].

[3] Mikael Linden, Julkisen avaimen järjestelmä, toimikortit ja niiden soveltaminen organisaatiosssa, Lisensiaattityö Tampereen teknillinen yliopisto 2003.

[4] WAP 2.0 Technical White Paper [verkkodokumentti], WAP forum, [viitattu 15.4.2009], www.wapforum.org/what/WAPWhite_Paper1.pdf.

[5] WAP White Paper [verkkodokumnetti], WAP forum, [viitattu 15.4.2009], www.wapforum.org/what/WAP_white_pages.pdf.

[6] Tuomo Repo, Henkilökohtaisen päätelaitteen käyttö lähimaksujärjestelmässä, Diplomityö Lappeenrannan Teknillinen yliopisto 2004.

[7] Wireless Transport Layer Security [verkkodokumentti], Open mobile alliance, [viitattu 13.5.2009], www.openmobilealliance.org/tech/affiliates/wap/wap-261-wtls-20010406-a.pdf.

[8] WPKI [verkkodokumentti], Open mobile alliance, [viitattu 13.5.2009], www.openmobilealliance.org/tech/affiliates/wap/wap-217-wpki-20010424-a.pdf.

[9] MiniWap: Navigatin WAP with Minimo [verkkodokumentti], IEEE, [viitattu 31.5.2009]http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4291103&isnumber=4291085.