NTNU
Norwegian University of
Science and Technology

User Friendly Access Solutions for Mobile WiMAX

Brage Rønning Tukkensæter

Master of Science in Communication Technology
Submission date: June 2009
Supervisor: Yuming Jiang, ITEM
Co-supervisor: Thomas Jelle, Trådløse Trondheim
Lene Maria Myhre, Trådløse Trondheim

Norwegian University of Science and Technology
Department of Telematics

Problem Description

The objective of this project is to investigate possible user friendly access solutions for Mobile WiMAX. The study includes both a theoretical and a practical part.

The theoretical part should investigate the IEEE 802.16e and WiMAX Forum standards for user access. Security should be discussed, and a brief comparison with Wi-Fi and GSM/UMTS access solutions should be given.

The practical part should design and implement a proof-of concept access solution for Mobile WiMAX, including organizational RADIUS authentication and paying users. The access solution should give users secure and user friendly access to the Mobile WiMAX network.

Assignment given: 21. January 2009
Supervisor: Yuming Jiang, ITEM

Abstract

Today, WiMAX networks are deployed several places worldwide. To get access to these networks, users have to buy equipment specialized for one operator with a subscription. User equipment has earlier been stationary or mounted, but with the Mobile WiMAX amendment, smaller receivers are made possible. Mobile WiMAX allows users to move between different operators, making user access and roaming a more challenging task.

In this thesis, several Mobile WiMAX access solutions are discussed, emphasizing security and user friendliness. A captive portal solution is developed, and an EAP-TTLS (Extensible Authentication Protocol - Tunneled Transport Layer Security) solution utilizing FreeRADIUS is planned.

Security in WiMAX is compared to Wi-Fi very good. Even in an open WiMAX network traffic can be encrypted, this makes a WiMAX captive portal solution secure for most purposes.

For traveling or visiting users, the EAP-TTLS solution may be complicated to use. Users need an account prior to the connection, or the visited operator needs roaming agreements with the user’s home operator. Roaming agreements are not common today, but is currently promoted by the WiMAX Forum. With the captive portal, users are able to buy access without having an account or subscription in advance.

A captive portal solution is recommended for visiting users, and EAP-TTLS without roaming is recommended for users more permanently located in the operator’s area. EAP-based roaming may be deployed if roaming becomes more common in the future, but is not recommended today.

Preface

This thesis was written as the final part of a master's degree in communication technology during the spring 2009. The thesis was accomplished at the Department of Telematics (ITEM) at the Norwegian University of Science and Technology (NTNU), in cooperation with Wireless Trondheim. The thesis covers 30 ECTS credits (European Credit Transfer System).

My first meeting with Wireless Trondheim was the summer of 2007, when I accomplished a summer internship for them. With Wireless Trondheim I developed a captive portal access solution for their outdoor Wi-Fi network. This work is used as a foundation for some of the work done in this thesis. After my summer internship, I have continued working part-time at Wireless Trondheim as a software developer and architect.

In the autumn of 2008, as part of my master’s degree, I carried out a specialization project in cooperation with Wireless Trondheim. This project had the title “Using Citywide WLAN as primary Internet connection for homes”. In this project, I worked mostly with technical aspects and business opportunities.

There are several reasons for me to write this thesis. First, Wireless Trondheim is a company that I know very well, and I enjoy working with the people there very much. Mobile WiMAX is very interesting wireless technology, and I take a great interest in access solutions and the combination of security and user friendliness. When managing director Thomas Jelle in Wireless Trondheim proposed this thesis for me, I thought it was a great idea, and I have enjoyed working with these topics.

Acknowledgements

Several people that have helped me during the work with this thesis.

First, I would like to thank my two supervisors Thomas Jelle at Wireless Trondheim and Professor Yuming Jiang at Department of Telematics, NTNU. They have both been of great help pointing me in the right directions.

I would thank a number of people that have helped me in different ways. Kristoffer Milligan in NextNet for guiding me while using the Alvarion equipment and providing information on NextNet’s WiMAX network. Jardar Leira at Uninett for setting up the Alvarion BS and providing useful information on how the equipment works. Jonas Lagerquist in Aptilo Networks for providing useful information on CSNs and trends in the WiMAX community.

I would like to thank my wife Åse for believing in me and motivating me this semester. You’re the best.

At last I want to say thanks to you guys at the office: Ørjan Bækkelund, Øyvind Risan and Jens Wiel Monrad-Hansen, I have had a great time with you. If you ever beat my Minesweeper record (152 sec on large), please let me know.

Content

List of Figures

List of Tables

List of Abbreviations

(R)UIM	(Removable) User Identity Module
3DES	Triple Data Encryption Algorithm
3G-SGSN	3G Serving GPRS Support Node
AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
AK	Authorization Key
ASN	Access Service Network
ASP	Access Service Provider
BS	Base Station
BTS	Base Transceiver Station
CA	Certificate Authority
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CLI	Command line interface
CPE	Customer Premises Equipment
CSN	Connectivity Service Network
cURL	
DB	Database
DHCP	Dynamic Host Configuration Protocol
DP	Decision Point
EAP	Extensible Authentication Protocol
EAP-AKA	EAP Method for 3rd Generation Authentication and Key Agreement
EAP-TLS	EAP Transport Layer Security
EAP-TTLS	EAP Tunneled Transport Layer Security
ECTS	European Credit Transfer System
EP	Enforcement Point

ESP	Encapsulating Security Payload
GMSC	Gateway Mobile Switching Centre
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile communications (originally from Groupe Spécial Mobile)
GW	Gateway
HLR	Home Location Register
H-NSP	Home Network Service Provider
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	Internet Protocol Security
ISP	Internet service provider
KEK	Key Encryption Key
LoS	Line-of-Sight
LTE	Long Term Evolution
MAC	Media Access Control
MAN	Metropolitan area network
MIB	Management Information Base
MNE	Mobile network enablers
MNO	Mobile network operator
MS	Mobile Station
MSC	Message Sequence Chart
MSC	Mobile Switching Centre
MVNO	Mobile virtual network operators
NAP	Network Access Provider
NSP	Network Service Provider
NTLM	NT LAN Manager
NTNU	Norwegian University of Science and Technology
NWG	WiMAX Networking Group
OFDMA	Orthogonal frequency-division multiple access
OSI	Open Systems Interconnection
PEAP	Protected EAP
PHP	PHP Hypertext Preprocessor

PHY	Physical Layer
PKI	Public key infrastructure
PKM	WiMAX Privacy Key Management Protocol
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RFC	Request for comment
RNC	Radio Network Controller
RSA	Rivest, Shamir,and Adleman (asymmetric cryptography)
SA	Security Association
SCP	Service Control Point
SIM	Subscriber identity module
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SS	Subscriber Station
TEK	Traffic Encryption Key
TKIP	Temporal Key Integrity Protocol
TLS	Transport Level Security
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
USIM	UMTS Subscriber Identity Module
VLR	Visitor Location Register
VSA	Vendor Specific Attributes
WCM	Alvarion Wireless Connection Manager
WEP	Wired Equivalent Privacy
Wi-Fi	(Brand name, not a abbreviation)
WiMAX	Worldwide Interoperability for Microwave Access
WPA	Wi-Fi Protected Access
WS	Web Services
XML	Extensible Markup Language

1 Introduction

1.1 Motivation

Today there are several WiMAX networks deployed worldwide. Most of these are Fixed WiMAX, but several Mobile WiMAX sites are being deployed, giving users the possibility to gain access directly with their laptops or cellular phones.

With WiMAX, a user is normally connected with a device placed at a fixed location. This makes user friendly user access a simple matter, as the company deploying the WiMAX also is managing the WiMAX user equipment. Users typically connect their computers with an Ethernet cable to the CPE (Customer Premises Equipment). This makes it easy for the users, as the only action required is to plug in the cable.

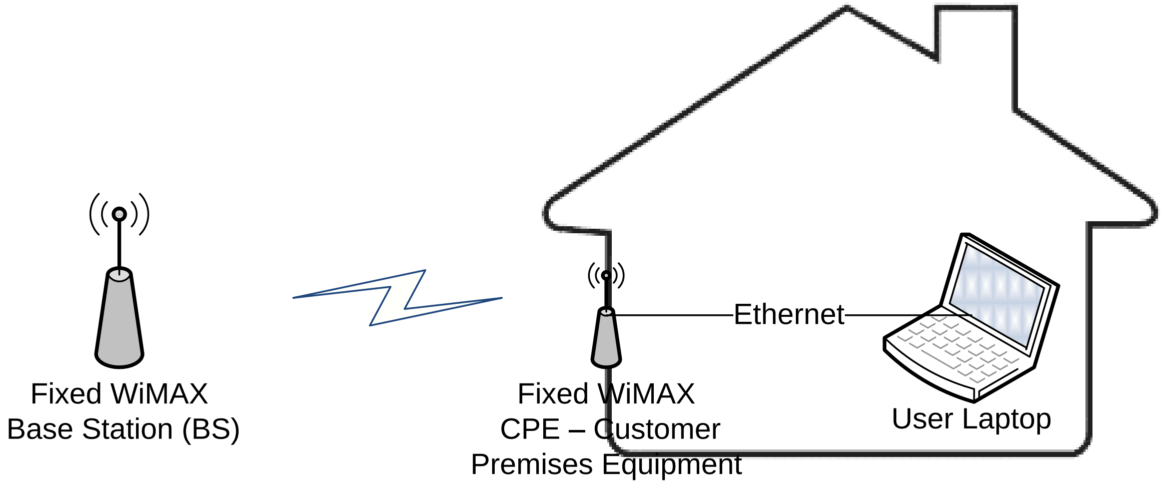


Figure 1 Fixed WiMAX: user is connected to a fixed CPE with Ethernet cable

In the newer Mobile WiMAX, users are connected directly to the Mobile WiMAX network with their smaller and portable devices, making the setup more flexible for the users. This flexible setup may be a challenge for the users and the operators, as the users now must handle the network connection directly. Mobile WiMAX is standard oriented, and there are several vendors of WiMAX Mobile Stations (MS), which all have different software drivers to their devices. This gives several user interfaces, both for the user to set up and network operator to support. A user may also travel between different operators, wanting to use its Mobile WiMAX equipment other places. This introduces challenges regarding roaming between operators and short time access. All this together makes user access a more complex task in Mobile WiMAX than in Fixed WiMAX.

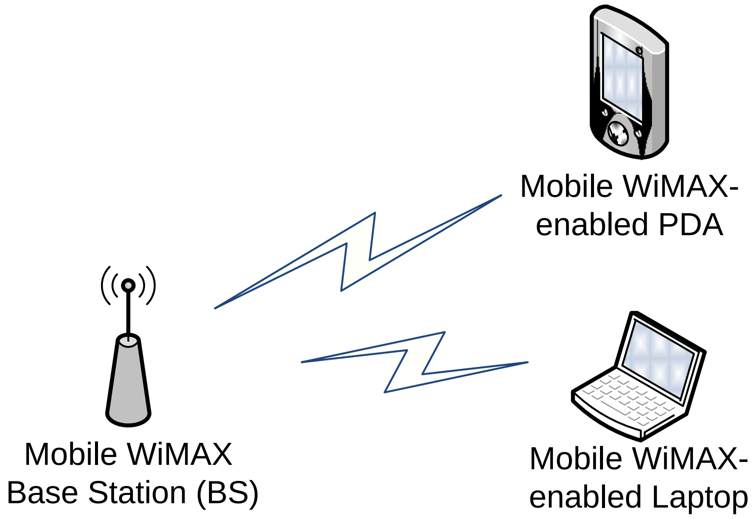


Figure 2 Mobile WiMAX: user is connected directly with Mobile Station

1.2 Methodology

The theoretical technology study is mostly based on reliable sources, where documents from IEEE 802.16 and WiMAX Forum are used as much as possible, as they define the standards. As a second source of information published papers, books and documents from WiMAX equipment vendors are used. As a last source of information, Internet sites and non-published material are used.

For the practical part, an experimental methodology has been used, where the implementations have been tested during the process.

1.3 Scope

A WiMAX network can serve multiple purposes, and seek to reach different market segments. Before the Mobile WiMAX amendment, users connected to the WiMAX network with stationary CPEs (Customer Premises Equipment).The CPE is often bought or leased from the WiMAX operator together with a subscription. With the Mobile amendment smaller customer equipment can be produced, and users can be able to move between different WiMAX hotspots operated by different operators.

This thesis covers Mobile WiMAX access solutions where users are connected directly to the Mobile WiMAX network with a Mobile Station (MS), not where users are connected to a stationary or mounted CPE, or where WiMAX is used as a backhaul for Wi-Fi or other access networks. Visiting users like travelers is a user group that is especially considered. These are users that usually do not have a subscription to the current operator, and they may be demanding with regards on easy access.

User friendliness and security are parameters that are emphasized. Quality of Service profiles and individual throughput limiting[1] are also discussed. Parameters like total throughput utilization and handover are not discussed or tested in this thesis.

1.4 Related work and WiMAX sites

Several WiMAX networks have been deployed worldwide, WiMAX Forum claims that there are over 450 WiMAX networks deployed in over 130 countries [1].

1.4.1 WiMAX Forum

The WiMAX Forum has done some work on user access techniques and roaming, and has published several documents and best practices on the topic. The Network Working Group (NWG) have released the WiMAX Stage 2 and Stage 3 documents, which amongst others describes EAP methods, hotlining and more.

The WiMAX Forum announced 02. June 2009, a couple of days before this thesis was delivered, that they together with several industry partners are going to test global roaming. They have launched a website for this at http://wimaxroaming.org [2].

[1] Individual throughput limiting means that a single user is given a maximum throughput. This is useful if the service is differentiated and sold for different prices, but also to prevent abuse.

1.4.2 NextNet in Norway

NextNet is a company based in Flekkefjord, Norway, which delivers WiMAX Internet connection for homes and companies in Østfold, and plans to deploy a WiMAX network in Gjøvik and Vestre Toten. [3] NextNet deploys a Fixed WiMAX network, where the CPEs (Customer Premises Equipments) are mounted on the customers' houses.

For user access and individual throughput limiting, NextNet uses an open source captive portal[2] solution named NoCat [4]. NextNet uses Alvarion WiMAX equipment, and have done some tests with an Alvarion BreezeMAX base station and FreeRADIUS, but have not succeeded in making this work.

1.4.3 Clearwire

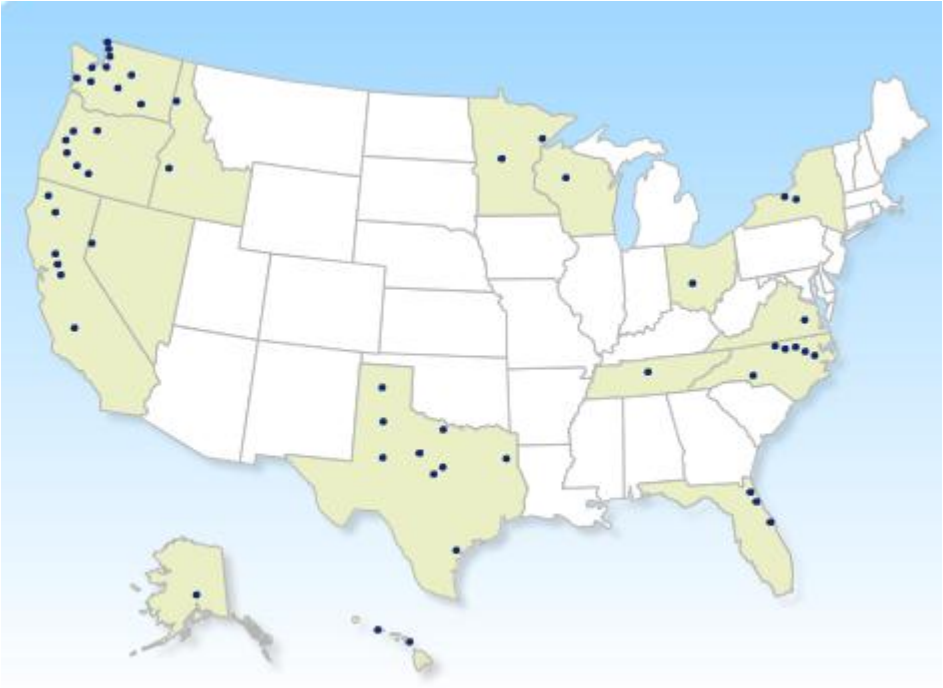


Figure 3 Clearwire deployed WiMAX sites

Clearwire is a company that has deployed several WiMAX hotspots in the United States (US). Clearwire has around 50 WiMAX sites deployed, and are currently upgrading these from Fixed to Mobile WiMAX [5]. Clearwire sells branded WiMAX devices under the brand name

[2] "Captive Portal" is an authentication solution which lies on top of an open network. When users try to access Internet through a web browser they are redirected to a "captive portal" and is given the possible to authenticate with username and password, or buy access with e.g. credit card. Captive portals are often used in Wi-Fi networks in public locations like airports and hotels.

“Clear”, and it they uses EAP-TLS (Extensible Authentication Protocol - Transport Level Security) to authenticate users to their network.

1.4.4 XOHM (Sprint Nextel)

XOHM was the brand name of the Sprint Nextel WiMAX network in Baltimore, US. XOHM does, like Clearwire, sell branded WiMAX equipment with preinstalled EAP-TLS, and do also utilize hotlining[3] to let customers buy access after the first login.

XOHM was acquired by Clearwire in December 2008, and should be re-branded as Clear [6]. This text refers to XOHM before they are merged into Clear.

1.5 Terms and clarifications

In this thesis the terms “WiMAX”, “Mobile WiMAX” and “Fixed WiMAX” is used widely, and to avoid misunderstandings, a clarification may be needed. “WiMAX” is used as a general term for the technology based on IEEE802.16 defined by the WiMAX Forum. “Mobile WiMAX” is used for technology defined by the IEEE802.16e-2005 amendment and WiMAX Forum Mobile system profile. Fixed WiMAX is used as a term for WiMAX technology before Mobile WiMAX. Fixed and Mobile WiMAX are non-overlapping subsets of WiMAX.

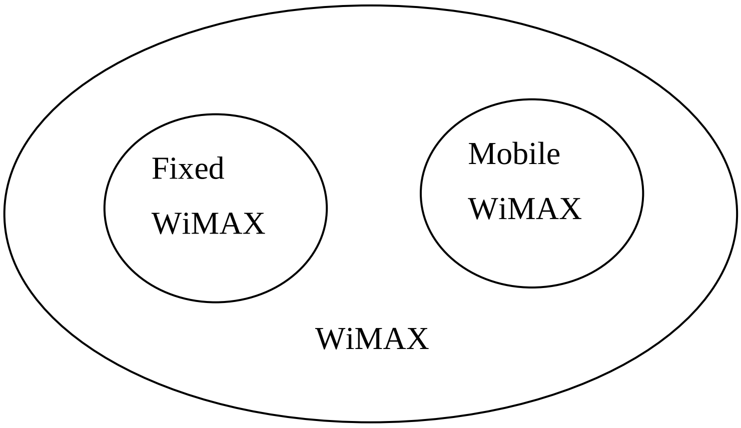


Figure 4 Fixed and Mobile WiMAX as a subset of WiMAX

[3] Hotlining is a technique that redirects the user to a web portal for subscription management after the user is authenticated to the network using EAP. Hotlining is a tecnique that is introduced in WiMAX, and from a user point-of-view it looks like a captive portal.

1.6 Reader’s guide

Chapter 1 includes the introduction with motivation, methodology, scope and related work.

Chapter 2 gives an introduction to WiMAX, with emphasis on system architecture and the Mobile amendment.

Chapter 3 introduces Wireless Trondheim and gives an overview of their Wi-Fi user access solutions and WiMAX testing.

Chapter 4 gives an overview of wireless user access and security. General security requirements and techniques are discussed, and Wi-Fi, UMTS and WiMAX are compared.

Chapter 5 describes several WiMAX user access solutions in detail, and evaluates these solutions.

Chapter 6 gives an overview of the practical work and implementation done.

Chapter 7 gives a discussion of which user access solutions to use in which cases, and gives some recommendations.

Chapter 8 gives conclusion and suggestions for future work.

Appendix A gives a brief overview of protocols for machine to machine communication that are used in this thesis.

Appendix B includes a detailed explanation on how an EAP-TTLS solution can be set up with FreeRADIUS and an Alvarion BreezeMAX 4Motion base station.

Appendix C describes the captive portal implementation in detail, gives details on Nomadix configuration and the system architecture. This appendix is restricted, and is put in a separate document. Contact Wireless Trondheim to get access to this.

Appendix D includes an overview of attached files to this thesis. As Appendix C, Appendix D is together with the attached files restricted.

2 Background on IEEE 802.16 and WiMAX

2.1 WiMAX Introduction

WiMAX (Worldwide Interoperability for Microwave Access) is wireless technology using licensed frequencies. WiMAX is standards-based, and gives wider coverage than Wi-Fi.

According to WiMAX Forum: [1] *“WiMAX is based upon the IEEE 802.16 standard enabling the delivery of wireless broadband services anytime, anywhere. WiMAX products can accommodate fixed and mobile usage models. The IEEE 802.16 standard was developed to deliver non-line-of-sight (LoS) connectivity between a subscriber station and base station with typical cell radius of three to ten kilometers”*

2.2 IEEE 802.16

In 1998, the Institute of Electrical and Electronics Engineers (IEEE) formed a group to develop a standard for what was called “Wireless metropolitan area network”, or just “Wireless MAN” [7]. This working group was named 802.16.

The IEEE 802.16 standards define the structure of the PHY (Physical Layer) and link layer operations that occur between subscriber stations and base stations (BSs). Over-the-air upper layer signaling, network architecture and protocols behind the base stations required for an end to end specification are considered outside the scope of this standard, this cases are handled by WiMAX Forum.

2.3 WiMAX Forum

The WiMAX Forum was founded in 2003 to promote WiMAX as a new wireless access technology based on IEEE 802.16 standards [8]. The WiMAX Forum has released several specifications to complement the IEEE 802.16, this is done by defining minimum requirements. Standardization and interoperability between WiMAX equipment is an important part of WiMAX Forum’s work, and all vendors who want to make “WiMAX Certified” equipment have to let WiMAX Forum test the equipment for interoperability. The WiMAX Forum is for IEEE 802.16 what the Wi-Fi Alliance is for IEEE 802.11.

2.4 Mobile WiMAX

Mobile WiMAX is technology based on the older ”Fixed” WiMAX. Mobile WiMAX is built on the IEEE 802.16e-2005 amendment, and has several enhancements to ordinary Fixed WiMAX; some of them are listed below [9]:

- Mobility support, handover
- More QoS classes
- Updated security layer (PKMv2), support for several types of authentication and encryption
- Power saving mode for mobile stations
- Several updates on the physical layer

2.4.1 Documents

Here is a listing of documents defining Mobile WiMAX, with emphasis of the subject discussed in this thesis.

Table 1 Important documents describing Mobile WiMAX in general and WiMAX access techniques

Document	Description
IEEE 802.16-2004	This is the most recent IEEE 802.16 standard. This standard supersedes the original IEEE 802.16(-2001) with amendments.
IEEE 802.16e-2005	The IEEE 802.16 “e” amendment standard, which is the basis for Mobile WiMAX
IEEE 802.16-2009	This is the “Rev2” revision of 802.16-2004 that is going to be published in late 2009. This standard consolidates several standards, 802.16e is one of them.

WiMAX Forum Mobile System Profile Release 1.0	Approved standard for WiMAX Forum.
WiMAX Forum Mobile System Profile Release 1.5	A newer system profile, not finished yet (June 2009). This standard builds on the not yet released 802.16-2009. See Figure 5
WiMAX NWG Stage 2	Subtitle “Architecture Tenets, Reference Model and Reference Points” This document is important for this thesis as is defines several user access mechanisms. The Network Reference model is defined here.
WiMAX NWG Stage 3	Subtitle “Detailed Protocols and Procedures”.
WiMAX NWG Stage 3 Annex: Prepaid Accounting	Document that in detail describes a way of handling prepaid accounting in WiMAX
WiMAX Forum Roaming Guidelines	Best practices of roaming is described here

2.5 WiMAX Roadmap and Timeline

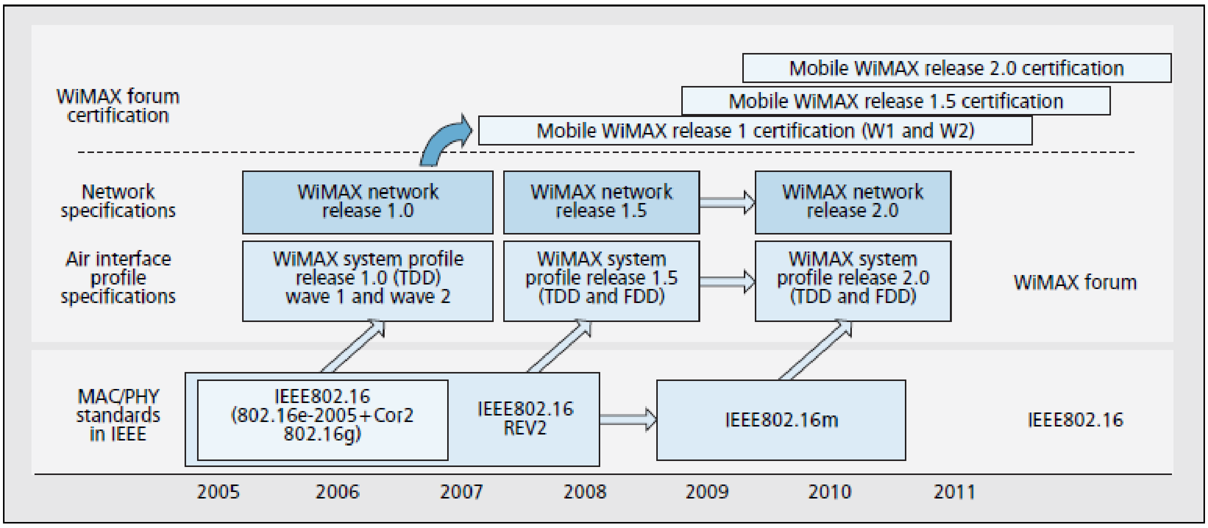

Mobile WiMAX release 2.0 certification
WiMAX forum certification
Mobile WiMAX release 1.5 certification
Mobile WiMAX release 1 certification (W1 and W2)
Network specifications
WiMAX network release 1.0
WiMAX network release 1.5
WiMAX network release 2.0
Air interface profile specifications
WiMAX system profile release 1.0 (TDD) wave 1 and wave 2
WiMAX system profile release 1.5 (TDD and FDD)
WiMAX system profile release 2.0 (TDD and FDD)
WiMAX forum
MAC/PHY standards in IEEE
IEEE802.16 (802.16e-2005+Cor2 802.16g)
IEEE802.16 REV2
IEEE802.16m
IEEE802.16
2005
2006
2007
2008
2009
2010
2011

Figure 5 Mobile WiMAX technology and network evolution roadmap [8].

This roadmap is an important figure to watch in detail to understand the process of making a WiMAX standard. First IEEE defines the physical layers, with an IEEE standard or amendment, after that WiMAX Forum works with finding out what parts of the IEEE standard that has to be fulfilled to a WiMAX certified product. The work of the WiMAX Forum is done to ensure interoperability between.

This makes as illustrated in the figure below, the WiMAX specification a subset of the IEEE 802.16 standard.

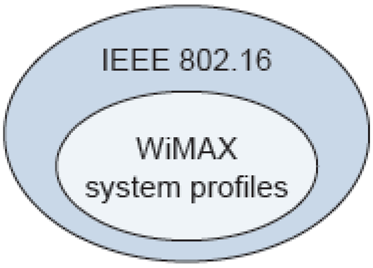


Figure 6 WiMAX system profiles [9]

This timeline shows an overview of important IEE802.16 and WiMAX events.

Table 2 Timeline of important IEEE 802.16 and WiMAX events

Date	Event
1998	IEEE 801.16 group formed
July 1999	First 802.16 working group meeting
June 2001	WiMAX Forum founded
December 2001	IEEE 802.16-2001 standard completed for >11GHz
January 2003	IEEE 802.16a amendment completed, specifying 2-11 GHz [10]
June 2004	IEEE 802.16-2004 standard completed, supersedes the old 802.16 with amendments.
September 2004	Intel starts shipping the first WiMAX chipset
December 2005	IEEE 802.16e-2005 standard completed (Mobile)
January 2006	First Wimax Forum certified product announced
	WiMAX NWG Stage 2 released
February 2006	WiMAX NWG Stage 3 released
	WiMAX Forum Mobile System Profile 1.0 approved
April 2008	First certified Mobile WiMAX products announced
January 2009	WiMAX Forum announces launch of global roaming program
June 2009	WiMAX Forum announces global roaming testing [2]
December 2009	IEEE 802.16-2009, Rev2 standard is to be released

2.6 Mobile WiMAX Reference Model

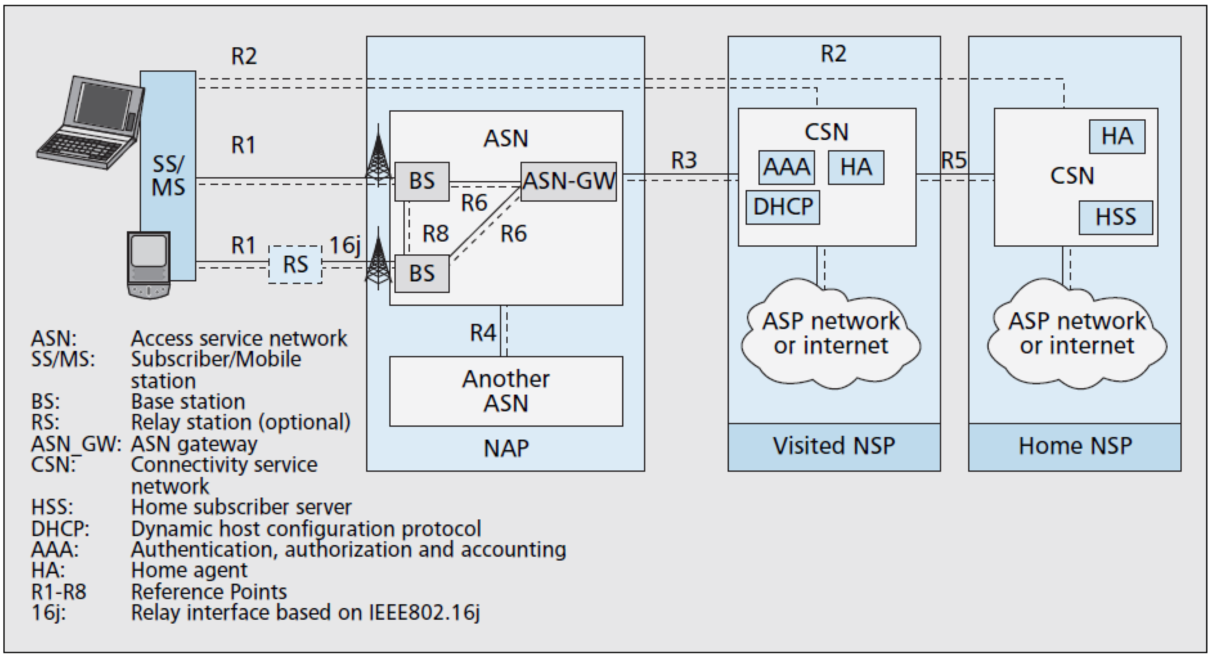

R2
R1
SS/
MS
R1
RS
16j
ASN
BS
ASN-GW
R6
R8
R6
BS
R4
Another
ASN
NAP
R3
R2
CSN
AAA
HA
DHCP
ASP network
or internet
Visited NSP
R5
HA
CSN
HSS
ASP network
or internet
Home NSP
ASN: Access service network
SS/MS: Subscriber/Mobile station
BS: Base station
RS: Relay station (optional)
ASN_GW: ASN gateway
CSN: Connectivity service network
HSS: Home subscriber server
DHCP: Dynamic host configuration protocol
AAA: Authentication, authorization and accounting
HA: Home agent
R1-R8 Reference Points
16j: Relay interface based on IEEE802.16j

Figure 7 Mobile WiMAX network reference model [8].

This is the Mobile WiMAX Reference Model, which is specified by the WiMAX NWG (Network Working Group) in the "Stage 2" document [11]. The solid lines represent the bearer plane and dashed lines represent the control plane.

2.6.1 Mobile Station (MS)

The MS is the device users use to connect to a WiMAX network. In Mobile WiMAX, this can be a USB device, PCMCIA card, Mini-PCI module etc. In Fixed WiMAX, the customer equipment is called CPE (Customer Premises Equipment) or SS (Subscriber Station).

The MS includes a manufacturer-signed X.509 certificate, which includes the MAC address of the MS and public keys to be used in RSA authentication/key exchange [12].

2.6.2 Access Service Network (ASN) Functions

An ASN is defined as a complete set of network functions needed to provide radio access to a WiMAX subscriber [13]. The ASN may include one or more Base Stations (BS), and one or more ASN Gateways (ASN-GW).

ASN is defined in detail in the WiMAX NWG Stage 2 documents [11].

Some of the functions mandatory in ASN are:

- WiMAX Layer 2 connectivity with WiMAX mobile station

- Transfer AAA (Authentication, Authorization and Accounting) messages to the subscriber’s NSP (Network Service Provider)
- Radio resource management
- ASN-CSN tunneling

2.6.2.1 Base Station (BS)

A Base Station is a part of the ASN entity.

The BS implements WiMAX MAC and PHY according to the IEEE 802.16e standard.

A BS must include the following basic functions [13]:

- Extensible Authentication Protocol (EAP) relay. The BS does not process the EAP message, just forward it between MS and ASN-GW
- Scheduler functions for uplink and downlink resources
- Traffic authentication and encryption
- Handover management
- QoS management

2.6.2.2 ASN Gateway (ASN-GW)

The ASN-GW is an entity that functions as a gateway between the ASN and CSN. The ASN-GW has several functions, and they are divided into two groups, the decision point (DP) and enforcement point (EP). Bearer plane functions are included in EP, and DP handles non-bearer functions.

Functionality of ASN-GW EP (bearer):

- Classification of downlink data into generic routing encapsulation (GRE) tunneling
- DHCP functionality
- Handover functionality

Functionality of ASN-GW DP (non-bearer):

- Implementation of EAP Authenticator
- Authentication key generation
- AAA accounting client

2.6.3 Connectivity Service Network (CSN) Functions

CSN is a set of functions that is needed to provide a MS IP connectivity. It may be built up by several network elements such as routers, proxies, AAA servers, Internet gateways etc.

A CSN may include the following functions [13]:

- MS IP address allocation (DHCP)
- Internet access
- AAA server or proxy
- Policy and admission control
- ASN-CSN tunneling

While ASN is specified in detail with reference points by WiMAX Forum NWG, the CSN is not standardized the same way, giving operators and vendors more freedom to choose more what to implement.

2.6.4 Network Access Provider (NAP)

Both NAP and NSP are business entities. A NAP owns one or more ASNs with ASN-GWs and BSs, and provides WiMAX radio access infrastructure to WiMAX network service providers (NSP). A WiMAX NAP can be compared to a UMTS/GSM mobile network operator (MNO) or mobile network enablers (MNE) (Telenor, Netcom and Network Norway in Norway)

2.6.5 Network Service Provider (NSP)

A Network Service Provider is another business entity that does not own its own ASN access network. A NSP is some sort of extension of an internet service provider (ISP), and it can provide Internet access and other services. A NSP must have an agreement with one or more NAPs to provide these services to customers. A private customer will typically have an agreement with a NSP, not a NAP. If a WiMAX NSP should be compared to a UMTS/GSM equivalent, one may compare to the mobile virtual network operators (MVNO), in Norway operators like OneCall, Chess, Tele2 etc. that do not own their own access network.

One actor may operate as both NAP and NSP, providing both ASN and CSN.

2.6.6 WiMAX NWG Reference points

The Mobile WiMAX network reference model consists of several logical reference points. The location of these reference points can be found in the Mobile WiMAX reference model in Figure 7.

Table 3 Mobile WiMAX reference points [14]

R1	Interface between the MS and ASN Functionality: air interface
R2	Interface between the MS and CSN Functionality: AAA, IP host configuration , mobility management
R3	Interface between the ASN and CSN Functionality: AAA, policy enforcement, mobility management
R4	Interface between ASNs Functionality: mobility management
R5	Interface between CSNs Functionality: internetworking, roaming
R6	Interface between BTS and ASN gateway Functionality: IP tunnel management to establish and release MS connection
R8	Interface between Base stations Functionality: handoffs

2.7 Mobile WiMAX Roaming between Operators

WiMAX Forum defines some best practices for roaming between operators in the document “WiMAX Forum Roaming Guidelines”[15]. Roaming does in this context mean the process where a user connects as a visitor to a WiMAX network, using his existing credentials from his Home-NSP (Network Service Provider), and being billed by his Home-NSP.

In the WiMAX roaming guidelines, two different scenarios are described:

- MS connect via HA (Home Agent) located in the visited network (V-CSN)
- MS connect via HA located in the home network (H-CSN)

These two scenarios can be realized with a direct connection NSP to NSP, or NSPs connecting with each other via a 3rd party WiMAX Roaming eXchange Provider (WRX).

The HA is the anchor point of the MS, and this is where traffic is anchored when the MS is moving between different BSs and ASNs. If the HA is located in the home network (H-CSN), bearer traffic has to be routed through H-CSN before it reaches Internet.

Figure 8 shows the scenario where the HA is located in the H-CSN. Note that solid lines represent the bearer plane and dashed lines represent the control plane.

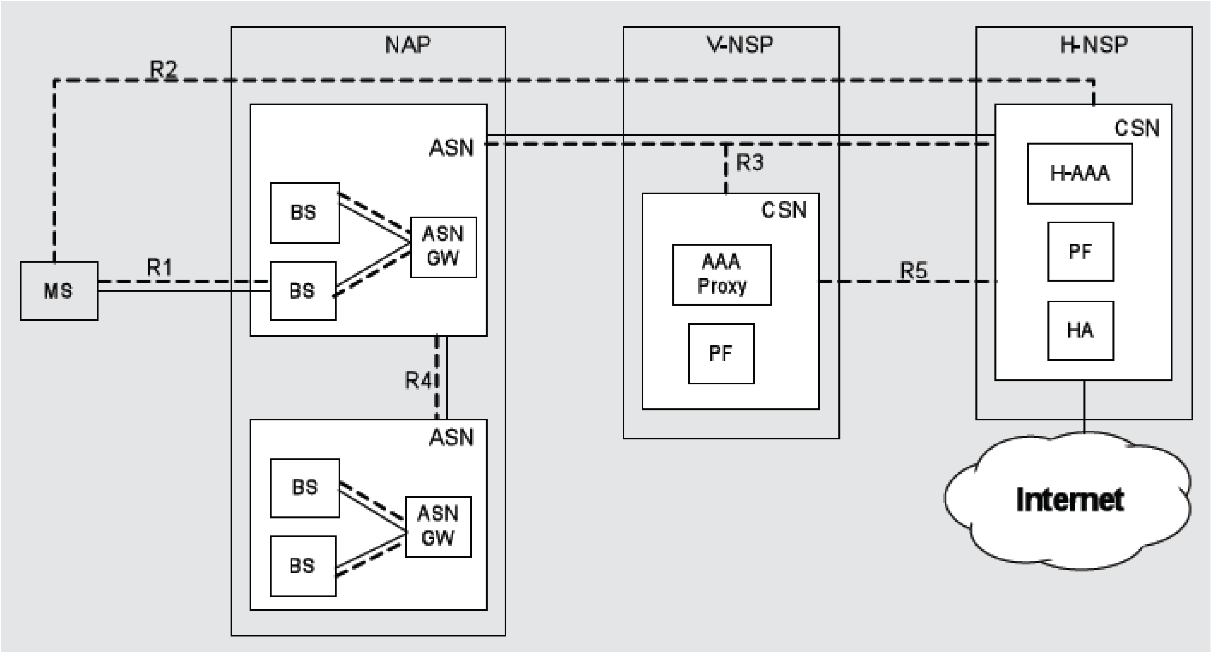


Figure 8 Network Reference Model without WRX with HA Located in the Home NSP [15]

Figure 9 shows a roaming scenario with a WRX. The WRX acts as a proxy for control messages between the V-NSP and the H-NSP, and handle clearing between the two business entities. Which Internet connection to used for the MS is decided by where the HA is located. If there is a HA located in both CSNs, a “HA selection procedure” is defined in [16].

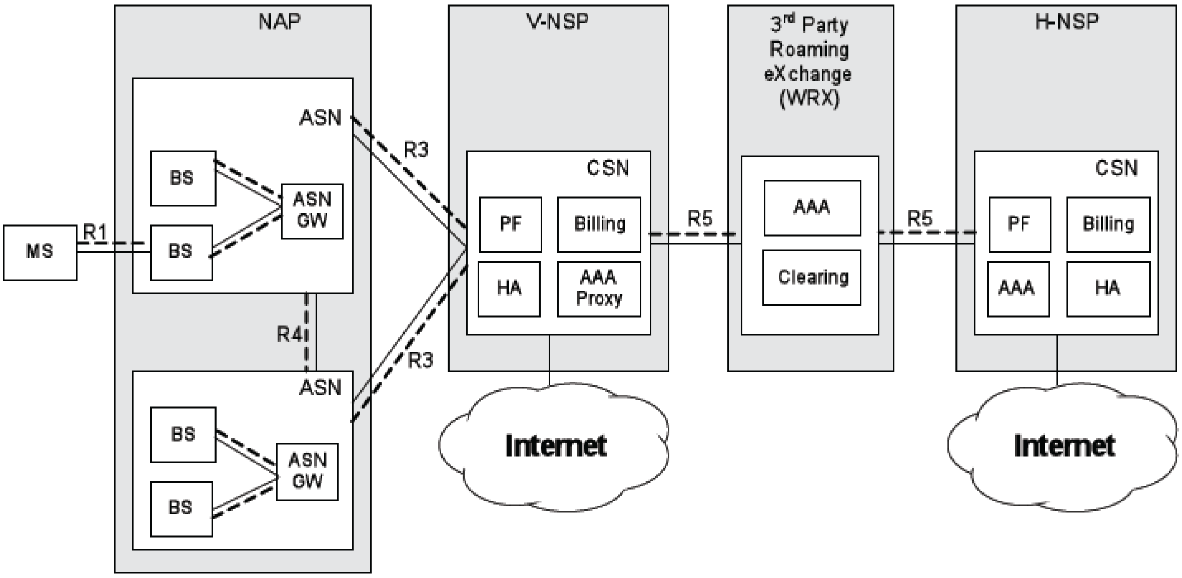


Figure 9 Network Reference Model with WRX [15]

With models lacking WRX exchanges, the number of potential roaming agreements that have to be made may be very large, potentially $\frac{n*(n-1)}{2}$ agreements in total, where each operator may have up to (n-1) agreements. With 100 operators, this number is 4950 agreements, while if all NSP nodes are connected to a central WRX, only 100 agreements are needed. Several WRX’s can also be interconnected, giving many possibilities for roaming.

For many small NSPs, the approach with WRX exchanges would probably be preferred, while larger NSPs may connect directly to each other.

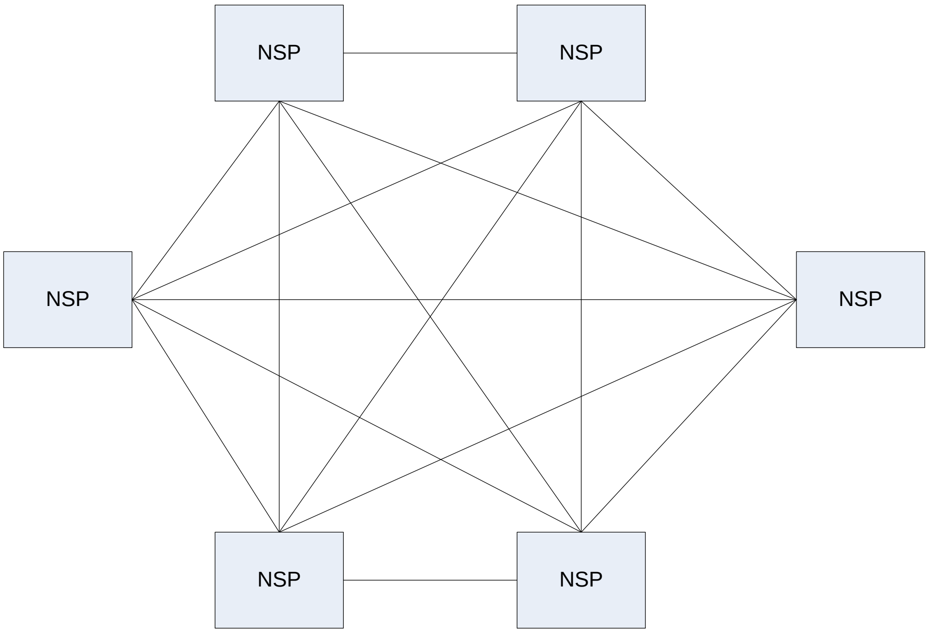


Figure 10 Roaming agreements between NSPs without WRX

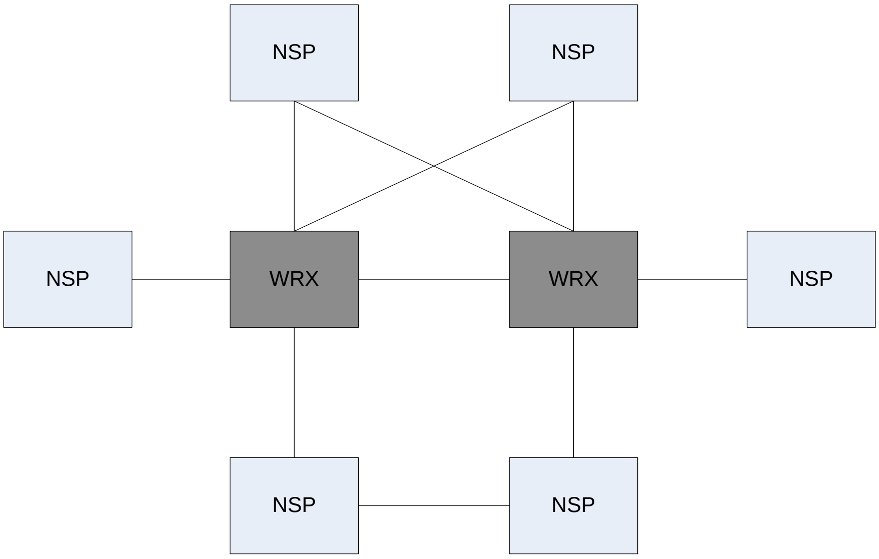


Figure 11 Roaming agreements between NSPs with multiple WRXs

2.7.1 WiMAX Forum Roaming Initiative

The WiMAX Forum has a website dedicated to roaming, http://wimaxroaming.org, which is a portal that describes and discusses roaming in WiMAX. Here several resources can be found, like white papers, templates for roaming agreements, proposed business models and more. Most of the documents on this website are recent; almost all are dated from 2009.

3 Wireless Trondheim

Wireless Trondheim is a company running a wireless network in Trondheim. The network is currently based on Wi-Fi, but they are now testing Mobile WiMAX. Today the network has outdoor Wi-Fi coverage in the inner city of Trondheim, with around 100 access points.

This chapter introduces Wireless Trondheim and gives an overview of technology and access solutions used.

3.1 History

Wireless Trondheim started as a research and development project initiated by the Norwegian University of Science and Technology (NTNU) in 2005 [9]. Covering the city of Trondheim with outdoor wireless networks is one of the objectives of the project, and this is until now achieved in the most central areas with Wi-Fi. In September 2006, the network was opened mainly for students at NTNU, and in September 2007, the network was made accessible for everyone as a paid service.

3.2 Wireless Trondheim access solutions

Wireless Trondheim offers several ways to access their Wi-Fi network, for different customers.

- **Captive portal on an unsecured network.** Users can gain Internet access by paying with SMS, credit card or using credentials from an organization with an agreement with Wireless Trondheim.
- **Eduroam.** Eduroam is a WPA Enterprise PEAP (Protected Extensible Authentication Protocol) based solution for educational institutions. All students and staff at NTNU

have access to this solution, and students from other universities are also allowed to use this network.

- **WPA Enterprise EAP-TLS.** (EAP - Transport Level Security) For Sør-Trøndelag Fylkeskommune Wireless Trondheim offered a highly secure solution based on EAP-TLS. This is not in use anymore; the highly secure solution is exchanged with a more user friendly and insecure captive portal.

These three access solutions are fairly different in both how easy they are to set up for the user, and regarding security.

The most used solution is the captive portal. It is easy to log in, and does not require a lot of technical information for the user. There are several drawbacks with the captive portal: the users must enter their credentials every time they want to use the network, and it is an unsecure solution vulnerable to several security threats.

Eduroam is a more secure solution, which is based on WPA Enterprise and PEAP. Users need to set up their equipment with Eduroam settings the first time the use the network, and after that, they are automatically logged in. To set up Eduroam for the first time the user needs to know some security parameters like protocols, root certificate etc., these are obtained on a webpage at NTNU or other Eduroam institutions.

The last access solution is WPA Enterprise with strong mutual authentication with both client- and server-side security certificates based on EAP-TLS. To connect to this network every user needs an individually signed certificate, and a PKI (Public key infrastructure) is therefore needed to distribute certificates. This will in practice often mean that the people using this need to meet at some office to obtain and install this certificate.

Table 4 Different access solution in Wireless Trondheim Wi-Fi network

Solution	Security	Easy first setup	Easy succeeding setups
Captive Portal	Very Poor	Easy	Easy
Eduroam - PEAP	Good	Medium	Very easy
EAP-TLS	Very good	Difficult	Very easy

3.3 Wireless Trondheim Wi-Fi Coverage

Today, Wireless Trondheim uses about 100 Wi-Fi access points to give the inner city of Trondheim (Midtbyen) coverage.

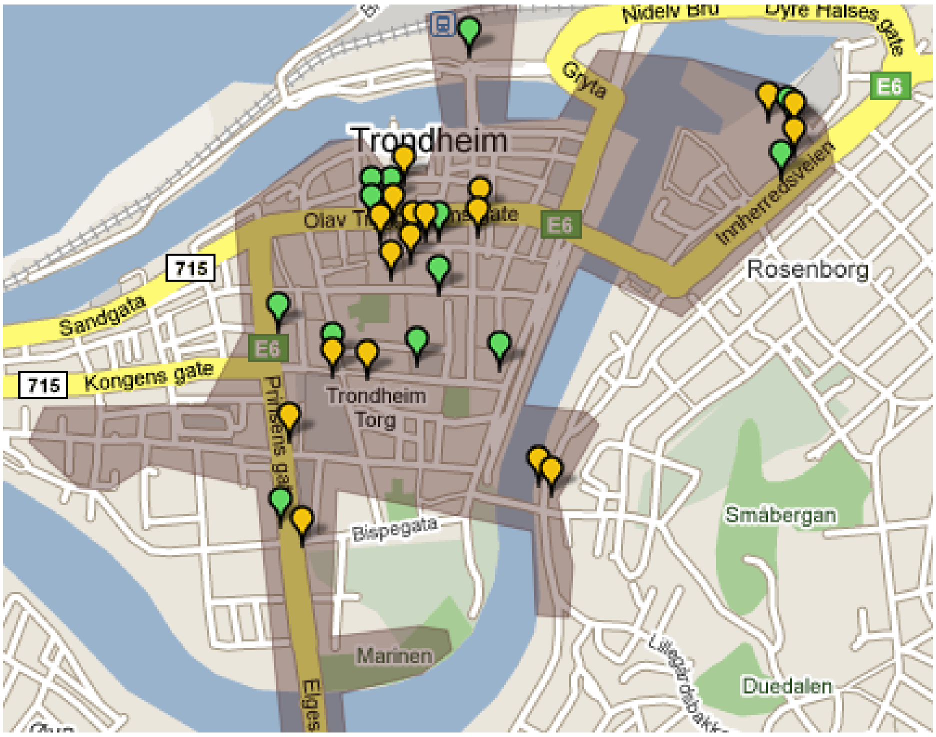


Figure 12 Outdoor Wi-Fi coverage in Wireless Trondheim[17]. The balloons are cafés with indoor coverage.

3.4 WiMAX Testing

Wireless Trondheim is together with Uninett running a project that is testing WiMAX. Uninett is a governmental company, which amongst others is running all core networks for universities and educational institutions in Norway.

Equipment from Alvarion was installed late spring 2008. The base station chosen is an Alvarion BreezeMAX 2500 shelf edition [9]. The BS is certified for Fixed WiMAX, but implements some of the functions from the 802.16e amendment, making it a so-called “Pre-Mobile”.

Certain master theses and project assignments are completed within this WiMAX project, mostly testing the physical part of WiMAX. Some work is done in the area of radio planning and measuring coverage, nothing is done on regarding user access, which is the topic this thesis deals with.

4 Wireless User Access and Security

This chapter will discuss wireless user access and security in general, comparing Wi-Fi, UMTS/3G and WiMAX.

4.1 Introduction to Wireless Security

There are mainly two stakeholders in wireless security, network users and network operators

Table 5 Stakeholders and concerns in wireless networks[14]

Stakeholder	Security Concern	Comment
Network User	Privacy	Protect from eavesdropping
	Date integrity	Protect user data from being tampered in transit
	Access to services	User has the correct credentials
	Correct accounting	Accuracy and efficiency of accounting
Network Operator	User authentication	Is the user who he says he is?
	Device authentication	Is the device the correct device?
	Authorization	Is the user authorized to receive a particular service?
	Access control	Only authorized users have access to services

Table 5 shows different stakeholders with their security concerns that have to be handled. A good solution does not necessary handle all these issues, but it can be used as framework for evaluating security in wireless networks.

4.2 Overview of Important Wireless Access Technologies and Techniques

This sub-chapter will give a brief overview of the following important access technologies and techniques:

- AAA - Authentication, Authorization and Accounting
- RADIUS - Remote Authentication Dial In User Service
- EAP - Extensible Authentication Protocol
- Captive Portal
- Hotlining

4.2.1 AAA - Authentication, Authorization and Accounting

AAA is a model specified by the IETF (Internet Engineering Task Force) to handle the following questions[18]:

- Who are you?
- What services am I allowed to give you?
- What did you do with my services while you were using them?

While these questions may be easy to answer for a single network device with a user database, this can be difficult question for a distributed environment. AAA is an architecture that handles these questions.

4.2.1.1 Authentication

Authentication refers to finding a digital identity for a client. The process is done between the client and another device, by presenting the user/client's credentials to the device. Credentials can be username/password, digital (X.509) certificates, phone numbers and more [19].

4.2.1.2 Authorization

Authorization refers to the process of granting a user different privileges based on their authentication. Authorization can be based on several rules like restrictions, time-of-day, location and more, and different users can often get different types of service.

4.2.1.3 Accounting

Accounting is tracking of resources utilized by users in a network. Accounting can be used for network management and billing, not only financial accounting. Information gained through accounting may be the identity of the user, bandwidth used, start and end of the service, the service type and more.

4.2.2 RADIUS - Remote Authentication Dial In User Service

RADIUS is probably the most used AAA protocol, and is widely supported by different network equipment.

The RADIUS protocol is standardized by IETF (Internet Engineering Task Force), and there are several RFC's describing RADIUS functionality. Authentication and Authorization is defined in RFC2865, Accounting is defined in RFC2866. A complete list of RADIUS RFC's can be found at Wikipedia [20].

There are several security concerns with RADIUS. Many of these are described in the "RADIUS" book published by O'Reilly [18]. There are several ways to compensate for these concerns, EAP, IPsec and long shared secrets are some of the countermeasures, which are commonly used.

RADIUS supports several authentication methods: PAP, CHAP and MS-CHAP and more, all these have different features and security levels. PAP (Password authentication protocol) is held to be the least secure of them, but is the only one that is compatible with all forms of password storage [21]. CHAP (Challenge-handshake authentication protocol) does for instance require the password to be stored in clear-text, while MS-CHAP (Microsoft CHAP) can take clear-text or NTLM (NT LAN Manager) hash.

PAP "encrypts" the password in a combination of MD5 and XOR with the shared secret, this has been shown to be not very secure, and requires very strong passwords and shared secrets.

CHAP and MS-CHAP are challenge-response protocols, where the password is never sent over the network. Here a random challenge is sent, which must be encrypted with the password as a key. The result is sent back, and compared with the expected result.

4.2.3 EAP - Extensible Authentication Protocol

Extensible Authentication Protocol (EAP) is an authentication framework much used in wireless networks. EAP is defined by IETF in RFC3748 (June 2004), and updated in RFC5247 (August 2008).

EAP is a way of securing RADIUS. EAP messages are encapsulated in RADIUS messages. The client and the NAS (Network Access Server) negotiate the use of EAP. The NAS, which acts as a RADIUS client, encapsulates the EAP message as a RADIUS message and sends it to the RADIUS server [18].

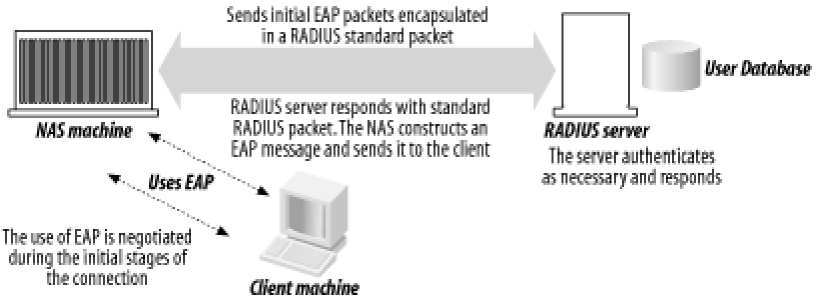

Sends initial EAP packets encapsulated in a RADIUS standard packet
User Database
NAS machine
RADIUS server responds with standard RADIUS packet. The NAS constructs an EAP message and sends it to the client
RADIUS server
The server authenticates as necessary and responds
Uses EAP
The use of EAP is negotiated during the initial stages of the connection
Client machine

Figure 13 EAP and RADIUS working together [18]

EAP is just a framework, and to be used methods are needed. There are several methods, both proprietary and standardized. The ones specified as a parts of the WiMAX standard are listed below.

4.2.3.1 EAP-TLS – EAP Transport Layer Security

This is held to be the most secure authentication protocol [22], giving strong mutual device authentication. The reason for this being the most secure protocol is that a CA (Certificate Authority)-signed X.509 client certificate is required both at the client and authentication server. The problem is that a Public Key Infrastructure (PKI) is needed to distribute the client certificates in a secure way, making the management costs high and the user friendliness low. EAP-TLS provides strong mutual authentication, meaning that both the user can be sure to be connected to the right access point, and the authentication server can be sure which devices are connected. EAP-TLS is often used in cases where the network operator has control of all user equipment; this makes the process of distributing the certificates easier for the operator.

4.2.3.2 EAP-TTLS – EAP Tunneled Transport Layer Security

EAP-TTLS is a protocol where a TLS tunnel is set up between the supplicant (client) and the authentication server. The TLS tunnel is set up with a X.509 digital certificate on the authentication server side. No individual certificate is needed on the client side, making this authentication protocol easier to deploy than EAP-TLS, where a PKI is needed. Users are authenticated by username and password, or other credentials.

4.2.3.3 EAP-AKA – EAP Method for 3rd Generation Authentication and Key Agreement

EAP-AKA is the authentication protocol used in UMTS, based on SIM cards (Subscriber Identity Module). From the RFC4187 [23]: *“...EAP mechanism for authentication and session key distribution that uses the Authentication and Key Agreement (AKA) mechanism. AKA is used in the 3rd generation mobile networks Universal Mobile Telecommunications*

System (UMTS) and CDMA2000. AKA is based on symmetric keys, and typically runs in a Subscriber Identity Module, which is a UMTS Subscriber Identity Module, USIM, or a (Removable) User Identity Module, (R)UIM, similar to a smart card."

4.2.4 Roaming

Roaming refers to the process of extending a wireless connection to another place than the service originated. Roaming is a general term that is widely used in the GSM community for roaming between operators. Roaming allows customers to get access to a network as a visitor outside the geographical coverage area of the customer's home network.

4.2.5 Captive Portal

A captive portal is a way to give users access to a network without needing a subscription in advance.

In a captive portal setup, the user connects to the network and tries to visit some web site. The gateway captures all HTTP (port 80) traffic, and redirects the user to the captive portal web site. Now the user must authenticate, typically by buying access with credit card, SMS etc, or logging in with existing username and password, the latter is often done using RADIUS. When the user has authenticated the user is able to access the Internet.

If the user buys access for a limited time and the time runs out, the user will be redirected to the captive portal web page again to buy more time.

Captive portals use the MAC-address of the user's network card as identifier of the user. This is not a very strong identity, and has in most network equipment been easy to spoof.

Captive portals are common at places where there are many traveling or visiting users like airports, hotels and municipal wireless networks. Captive portals can be used in all sorts of IP-based networks, also wired, but is currently most common in Wi-Fi networks.

4.2.6 Hotlining

Hotlining is a solution for user access that combines EAP and captive portal. In difference to the captive portal, the user has to authenticate using EAP (TTLS, TLS, AKA etc) with an existing identity. After that being redirected to a portal page where the user can buy pre-paid access, start a subscription etc.

Hotlining uses the EAP-identity of the user as identification, not the MAC-address like in the captive portal. The EAP-identity is considered being a more secure identity than the MAC-address.

4.3 Wi-Fi Security and User Access

In traditional 802.11 / Wi-Fi there are several ways for users to get access to the wireless network.

- Unsecured wireless network without authentication
- Unsecured wireless network with captive portal
- WEP
- WPA Personal
- WPA Enterprise

4.3.1 Unsecured Wi-Fi

There are several drawbacks with running a Wi-Fi network without any security. First, everyone will get free access. Second, people with some computer skills will be able to eavesdrop the traffic making the service unsecure for the users. Another problem is that there will be difficulties with Authentication, Authorization and Accounting (AAA). Who does really access the network? According to Table 5, this approach does not cover any of the requirements of a secure network.

4.3.2 Unsecured Wi-Fi with Captive Portal

The solution used in most wireless hotspots in cities, airports etc. is an unsecured Wi-Fi network with captive portal redirection. This approach is fairly user-friendly, but the main drawback is that the network runs without any encryption, and will thus not meet the requirements “privacy” and “data integrity” from Table 5. With a captive portal, AAA can be achieved.

4.3.3 WEP

WEP (Wired Equivalent Privacy) was the first 802.11 security standard, introduced in 1999. WEP is a security protocol based on a shared secret / shared password; this means that the network owner does not have control of who is using its network. WEP is now depreciated, and according to *“Breaking 104 bit WEP in less than 60 seconds WEP is based on a shared secret”*[24] it is easily breakable in less than one minute with the right equipment.

4.3.4 WPA Personal

Like WEP, WPA (Wi-Fi Protected Access) Personal is based on a shared secret. According to recent studies [25], it is possible to break WPA if it uses the most common TKIP (Temporal Key Integrity Protocol) encryption. If the newer CCMP-AES is used, the attack is not applicable. AAA will be difficult, only the “Authorization” part of AAA is met, both Accounting and Authentication must be handled on some other point using WPA Personal.

4.3.5 WPA Enterprise

These protocols utilize that each user has an individual username and password. An advantage with WPA Enterprise is that users are authenticated individually, and because RADIUS is used, AAA is easy to achieve. All security concerns in Table 6 can be met with WPA Enterprise. WPA Enterprise is most often used in corporate environments.

4.3.6 Wi-Fi Summary

Table 6 Wi-Fi Security according to stakeholders

Stakeholder	Security Concern	Unsecured	Captive Portal	WPA Shared sec.	WPA Enterprise
Network User	Privacy			☑*	☑
	Date integrity			☑*	☑
	Access to services		☑	☑	☑
	Correct accounting		☑		☑
Network Operator	User authentication		☑		☑*
	Device authentication				☑*
	Authorization		☑	☑	☑
	Access control		☑		☑

** Partly, dependent on setup*

4.4 UMTS security and user access

4.4.1 UMTS Network Architecture

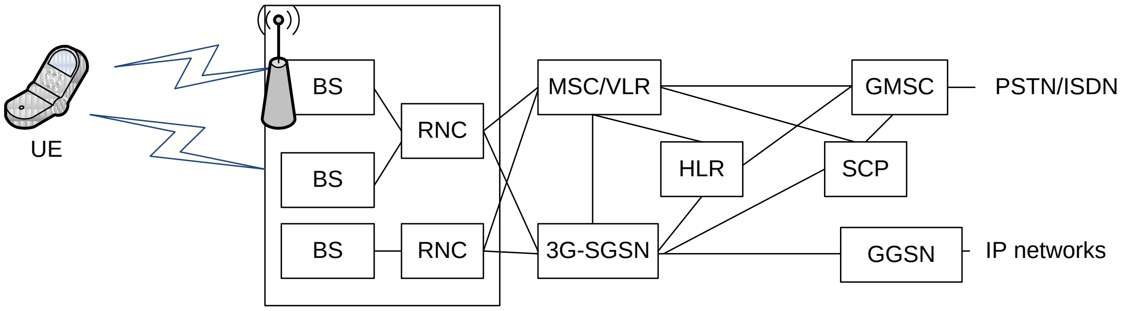


Figure 14 UMTS system architecture. (figure inspired by [26]) For abbreviations please see List of Abbreviations

The UMTS (Universal Mobile Telecommunications System) network architecture can in many ways be compared to the Mobile WiMAX reference model (ref. Figure 7).

The distributed architecture with VLR (Visitor Location Register) and HLR (Home Location Register) is especially interesting, since this makes roaming possible. HLR and VLR is user databases holding the location of a user, the HLR is located in the "home" network of the user while the VLR is placed in the network where the user is currently connected.

The user equipment (UE) includes a USIM card, which is a smart card holding subscriber information, authentication and encryption keys and other information. Parts of the authentication algorithms are also executed on the USIM [27].

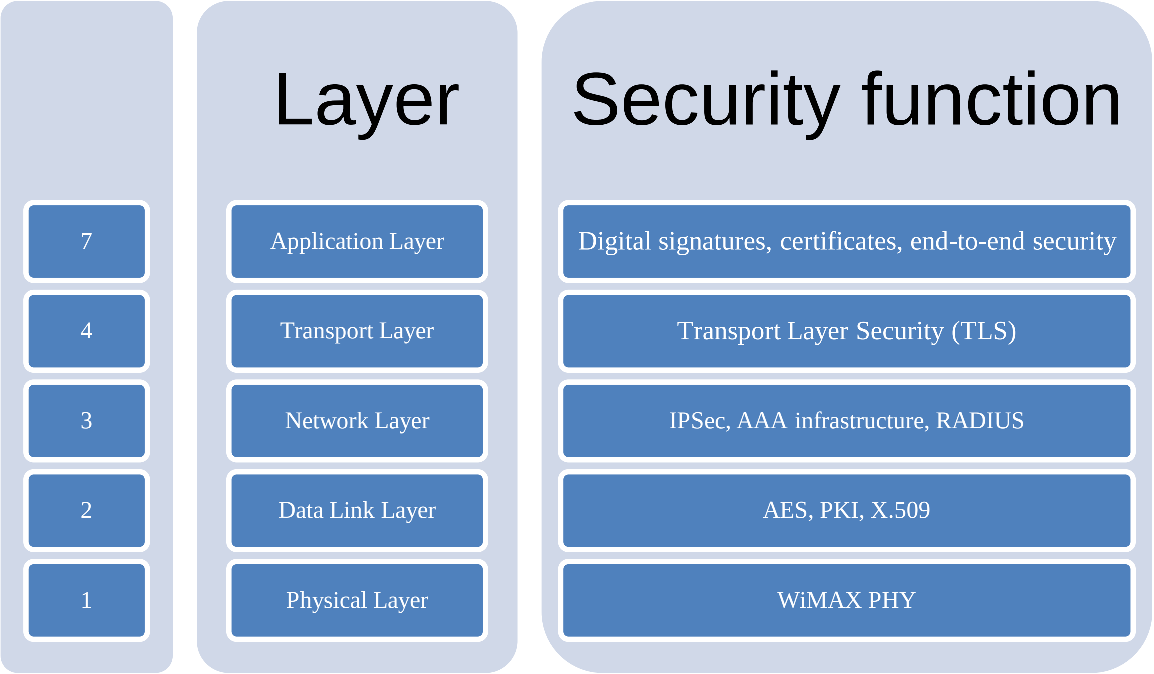
4.4.2 UMTS User Access

Unlike Wi-Fi, the UMTS operators have only one main way to let users connect to an UMTS network.

User access is in UMTS handled with the USIM. All users must have a subscription to an operator, and if the user wishes to use his device in another network, roaming agreements have to be made.

4.5 Mobile WiMAX Security and User Access

In Mobile WiMAX security is handled on different layers in the network. From the OSI-model, security can be mapped to different layers.



	Layer	Security function
7	Application Layer	Digital signatures, certificates, end-to-end security
4	Transport Layer	Transport Layer Security (TLS)
3	Network Layer	IPSec, AAA infrastructure, RADIUS
2	Data Link Layer	AES, PKI, X.509
1	Physical Layer	WiMAX PHY

Figure 15 Mobile WiMAX security functions [14]

In IEEE 802.16e-2005 [12], a security sublayer is specified. This deals with only with Data Link Layer security (layer 2). Link layer authentication and authorization makes the network only accessible for permitted users, while link layer encryption ensures privacy and prevents eavesdropping and tampering of data by unauthorized third parties. An important feature for Mobile WiMAX is that every MS (Mobile Station) must have its own central-signed X.509 digital, which enhances security very much compared to Wi-Fi [28].

Layer 3 security (Network layer) is not specified in IEEE 802.16e-2005 [12], but in the Mobile WiMAX network architecture the use of these techniques is addressed [14].

4.5.1 WiMAX Authentication

Authentication in WiMAX can be done in two ways

- Unilateral (one-way) authentication where the base station authenticates the mobile station or
- Mutual authentication where both the base station authenticates the mobile station and the mobile station authenticates the base station.

4.5.1.1 WiMAX Privacy Key Management (PKM) Protocol

IEEE 802.16e-2005 [12] defines the PKM protocol that gives three options for authentication [14]:

- RSA based authentication with X.509 certificates
- EAP based authentication
- RSA based authentication followed by EAP authentication

An advantage with all these three schemes is that they all give at least good unilateral authentication where the MS is authenticated. This means that if a MS is connected to a BS it is hard for an attacker to spoof the identity of the first MS to gain access to the network.

The problem with the first alternative (RSA based with certificate) is that the BS is not authenticated by the MS. This can give problems with rouge base stations or “Evil Twin”-attacks, which are attacks where the user is mislead to connect to a BS set up by a malicious user. [29]

4.5.2 WiMAX EAP methods

From the “WiMAX Forum Network Architecture Stage 3: Detailed Protocols and Procedures” it is defined which EAP methods WiMAX equipment has to support [16].

The mobile station (MS) has to support EAP-TLS and at least one of EAP-TTLS and EAP-AKA. The Home Network Service Provider (H-NSP) has to support EAPT-TLS, and it is recommended to support both EAP-TTLS and EAP-AKA.

4.5.3 WiMAX Traffic Encryption

WiMAX traffic can be encrypted using AES (Advanced Encryption Standard) or 3DES (Triple Data Encryption Algorithm), which both are secure symmetric encryption standards, approved by NIST (National Institute of Standards and Technology) [30]. Traffic is encrypted using the encryption keys in the built-in X.509 certificates in the MS, making it possible to encrypt the traffic without authenticating the user using EAP.

Together with possible encryption schemes, Mobile WiMAX utilize the OFDMA (Orthogonal frequency-division multiple access) modulation scheme, which also gives protection against eavesdropping[31].

4.5.4 Mobile WiMAX Security Summary

Table 7 gives an overview over the security concerns in WiMAX. An open Mobile WiMAX network with a captive portal is vulnerable for rouge base stations, as it does not provide mutual authentication. More information on this is given in chapter 5.2.3. EAP-TTLS and the captive portal does not provide device authentication as they are only based on username and password, while EAP-TLS provides device authentication with certificates. EAP-TLS may also provide user authentication if hotlining is used.

Table 7 Overview of WiMAX Security

Stakeholder	Security Concern	Captive Portal	EAP-TLS	EAP-TTLS
Network User	Privacy	☑	☑	☑
	Date integrity		☑	☑
	Access to services	☑	☑	☑
	Correct accounting	☑	☑	☑
Network Operator	User authentication	☑	☑*	☑
	Device authentication		☑	
	Authorization	☑	☑	☑
	Access control	☑	☑	☑

4.6 Comparison of Wireless Security and User Access

User access in Wi-Fi, UMTS and Mobile WiMAX are different from each other, as the three wireless technologies serve different purposes.

Wi-Fi has the most flexible user access solutions, allowing a variety of different methods like shared password, EAP-based for enterprises, captive portals for hotspots etc. The application for Wi-Fi is most often indoor coverage, in private homes or offices. Wi-Fi equipment is available in almost every laptop and several cellular phones sold. It is not common to sell Wi-Fi equipment together with subscriptions, users must connect to different Wi-Fi networks with different passwords. Roaming agreements are not very common.

UMTS’s access solution is fairly different from Wi-Fi. With UMTS, every user needs a subscription, and this subscription lies in a physical USIM card, which includes encryption codes and identification. When a UMTS user visits another UMTS network, roaming agreements let the user use the network with his existing subscription without having to sign up a to a new subscription.

Mobile WiMAX lies somewhere between Wi-Fi and UMTS with regards on user access. Like Wi-Fi, Mobile WiMAX is IP-based, and supports a variety of user access solutions, most of them EAP-based. The Mobile WiMAX network architecture is created in a way similar to UMTS to support roaming, and today most WiMAX user equipment is sold together with a subscription to a specific operator, but without roaming agreements.

5 Solutions for Mobile WiMAX User Access

This chapter will present different solutions for achieving user access with the equipment available for the testing for Wireless Trondheimand Uninett. Since WiMAX is a standards-based protocol, solutions suggested in this chapter should work in any WiMAX network.

5.1 Issues to be discussed

There are several issues for the solutions mentioned in this chapter that should be discussed.

1. User friendliness – how easy is it for the user to connect to the network?
2. Subscription handling – is it possible for a user to connect without a subscription, possibilities for roaming?
3. Security – is the solution secure, is the users privacy protected and does the operator know the identity of the users?
4. Cost and complexity – how expensive is the solution, does it include many components and is it difficult to set up?

5.2 Generic captive portal

This is a simple solution for giving users access without interacting with the whole Mobile WiMAX architecture. The scheme can be set up by routing traffic from users in the WiMAX network to a so-called “Access Gateway”, which takes care of user authentication, bandwidth allocation etc. This access gateway will include a captive portal, where HTTP traffic for unauthorized users will be redirected to a captive portal where the user can buy access or login with his/her credentials.

A solution like this is easy to set up in any IP-based network, independent of technology. This is the reason it is called a "generic" captive portal. The same equipment can be used both for WiMAX and Wi-Fi, and the costs of such a solution would probably be lower than deploying specialized WiMAX solutions.

Captive portals can support both pre- and post-paying customers. The captive portal can handle payments with credit cards, PayPal, SMS (Short Message Service) etc, but also authorize pre-paid RADIUS users.

Negative aspects of this solution would be that one may not benefit from WiMAX's built in Quality of Service profiles, and that the architecture may not be as clean as proposed in the WiMAX documents.

The big difference with a captive portal in WiMAX compared to Wi-Fi is that WiMAX traffic can be encrypted without authentication [28]. Every mobile station and base station includes a signed X.509 security certificate, giving traffic encryption, and protection for "MAC-spoofing", which are two of the main vulnerabilities with captive portals on Wi-Fi networks.

5.2.1 Architecture

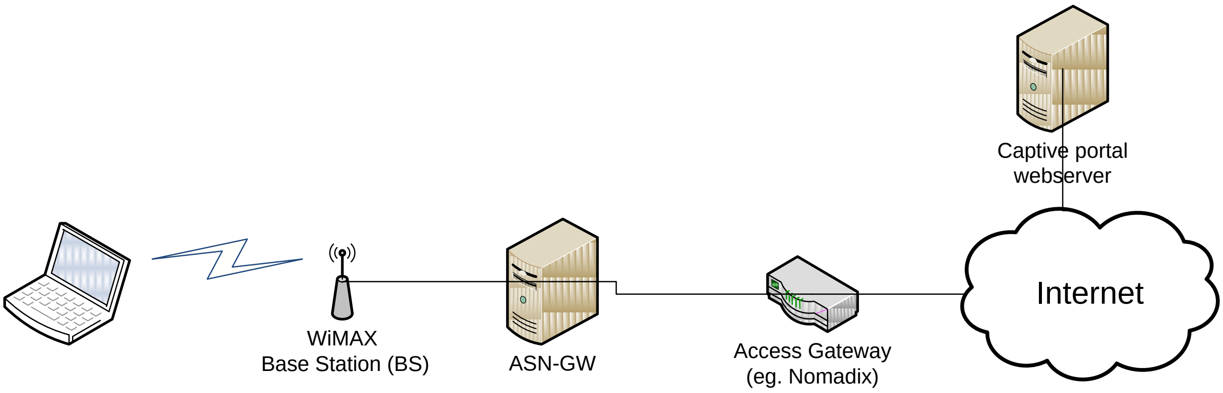


Figure 16 Generic captive portal network overview

5.2.2 Equipment for captive portal

Several ways to set up a captive portal solution exists. There are both embedded commercial solutions like Nomadix, and open source software solutions like NoCatAuth [4]. Wireless Trondheim uses for their Wi-Fi network a solution based on Nomadix, and this solution will be investigated in more detail.

5.2.2.1 ASN Gateway

An ASN gateway is not necessarily needed when making a solution with a captive portal. Traffic can be routed to the generic access gateway (eg. Nomadix) directly from the base station, but an ASN gateway would probably be used to manage the base station, handle handover etc. In the Alvarion BS that Uninett and Wireless Trondheim uses there is an ASN-GW included.

5.2.2.2 Nomadix Access Gateway

The Nomadix access gateway is placed as a gateway between the wireless network and the Internet, and all traffic is routed through this box. The access gateway's main task is to determine whether users should have Internet access or not, and to dynamically add and remove users. Individual throughput limiting may also be handled. To communicate (add user, set max throughput for user etc.) with the access gateway a XML web services interface is included

The Nomadix has an internal user database and also supports external RADIUS users.

Different models of the Nomadix Access gateway are available, AG3100 and AG5500 are the two most common, the difference lies mostly in how many users that can be connected.

5.2.2.3 Web Server for Captive Portal

A web server is needed to host the captive portal. For very simple portals, the internal web server in the Nomadix can be used, but for more advanced solutions an external web server is needed.

5.2.3 Security

Several security issues need to be handled in this setup.

- RADIUS messages from the access gateway (Nomadix) to the Home AAA server is not encapsulated
- Captive portal web site must be secured with HTTPS
- Communication between web server and access gateway must be secured
- Rouge base station (BS)

Most of these issues are relatively easy to handle.

The RADIUS protocol has several security issues [32][18]. Even if the protocol is designed to never send passwords in plaintext, there are several vulnerabilities. To handle this, RADIUS messages can be routed through a secure link, where IPsec [33] with Encapsulating Security Payload (ESP) encrypted with AES would be the preferred alternative [32].

The captive portal web site needs to be secured by HTTPS. Even if WiMAX has mechanisms superior to Wi-Fi in preventing eavesdropping, the packets may travel over the Internet, making them vulnerable for eavesdropping and tampering. HTTPS would protect against this.

Communication between the web server and the access gateway should be protected, this could be done either by running the web service on HTTPS, IPsec or both.

Rouge base stations is the threat that is most difficult to protect against. A rouge base station is a base station set up by a cracker. The user is fooled to connect to this base station, and the cracker can now eavesdrop, tamper data, perform a man-in-the-middle attack and more. One can argue that the attack is mostly theoretical, since WiMAX base stations today are very expensive. However, prices will probably drop, making the required equipment more common and available. Some may claim that HTTPS will protect against rouge base stations since a signed certificate can verify the domain name of the captive portal web site. This assumes that the user who uses the service is able to tell whether he/she is visiting a HTTPS site and the domain name is correct. Most users, even most IT professionals will probably fail doing this.

Especially if the user is using passwords that are valid several places (e.g. corporate networks), rouge base stations may be a threat, giving the cracker the possibility to get the user’s password. The consequences are less severe if one-time passwords are used, this can be achieved by using some sort of SMS-authentication that gives the user a unique code for each session.

5.2.4 Cost

The cost of a captive portal solution can be predicted to be is as follows:

5.2.4.1 Nomadix

Prices from Dataequipment, which is one of Wireless Trondheim’s equipment vendors.

Nomadix AG3100: 15 000 NOK
Nomadix AG5500: 32 000 NOK

5.2.4.2 Web Server

Almost any web server can be used, this will cost about 10 000 NOK, but this equipment is something that the operator probably already own.

5.2.4.3 Implementation, Management and Other Costs

This solution may require some implementation for the operator. Especially the web application can require some implementation effort for the operator. In some cases, a Wi-Fi solution could be reused. Some costs may also accrue with the payment solutions.

5.2.5 User Friendliness

For a user without a subscription this will be a very good solution. The user can connect to the network without a subscription, and pay for access in the Internet browser.

5.2.6 Login Details

Figure 17 shows the HTTP(S) and RADIUS message sequence for a user authenticating through the captive portal. The message flow is simplified, and traffic between the Internet browser and the Nomadix is routed from the MS through the BS and ASN-GW to the Nomadix.

This message sequence chart (MSC) shows a login for a user with a pre-configured username and password.

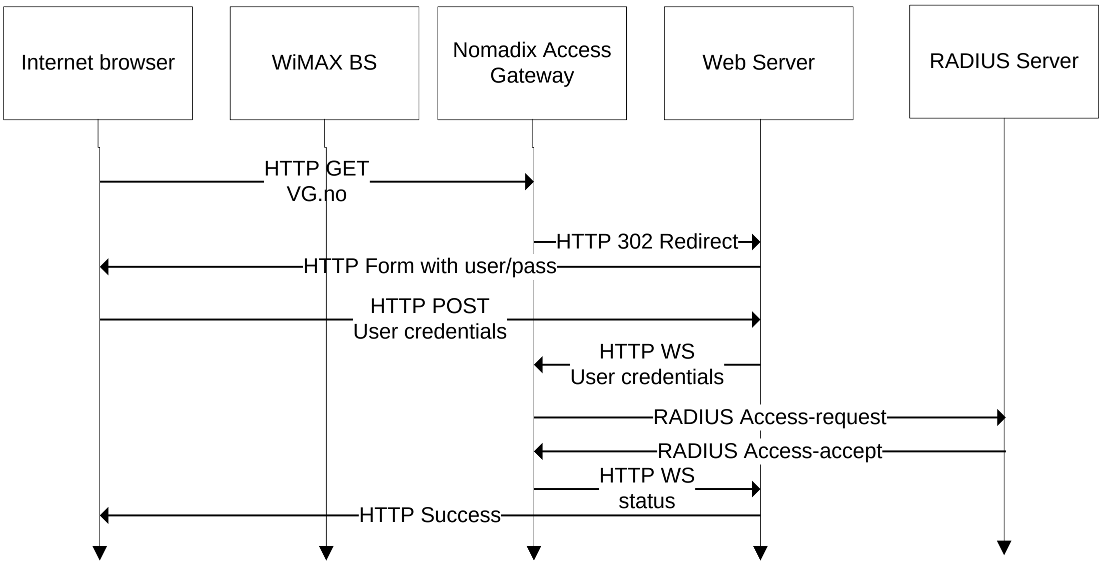


Figure 17 Example of Message Sequence Chart of RADIUS login with access gateway (HTTP and RADIUS messages)

Figure 18 shows a successful SMS authentication for a user without a pre-configured account. The dashed lines are SMS, full lines are HTTP requests/responses

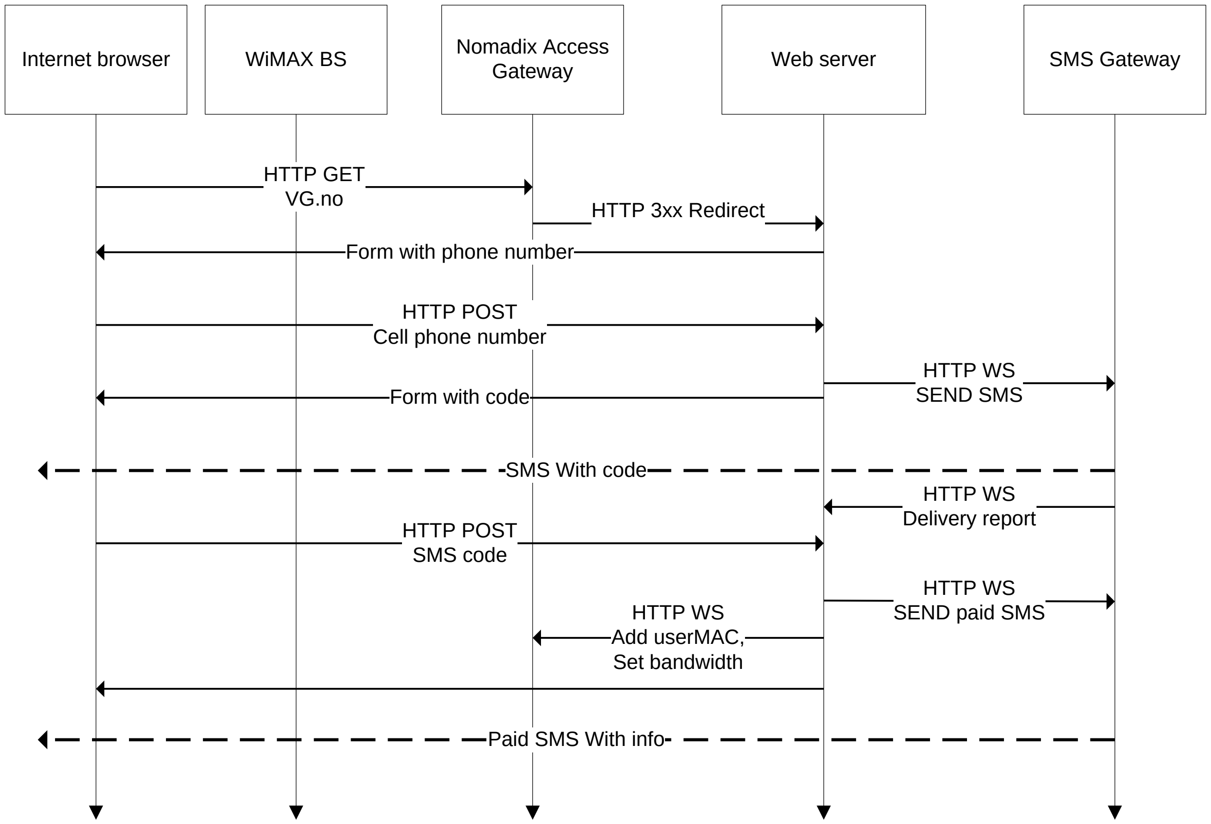


Figure 18 Example of Message Sequence Chart of SMS login with access gateway

5.3 FreeRADIUS and EAP-TTLS/EAP-TLS

In this sub-chapter a solution based on EAP is described. This is a solution where users log on with username and password (EAP-TTLS), or security certificates (EAP-TLS). This approach can be compared to WPA Enterprise in Wi-Fi, which also utilizes RADIUS and EAP.

FreeRADIUS is chosen in this setup from a variety of reasons. Any RADIUS server that supports WiMAX would do. FreeRADIUS is an open-source RADIUS server that supports WiMAX attributes. FreeRADIUS is free to use, and there is a large community around the project, making it easy to get help and support. FreeRADIUS is also the most deployed RADIUS server in the world [34].

FreeRADIUS supports a variety of different EAP-methods, the widely used EAP-TLS and EAP-TTLS would be considered here.

5.3.1 Architecture

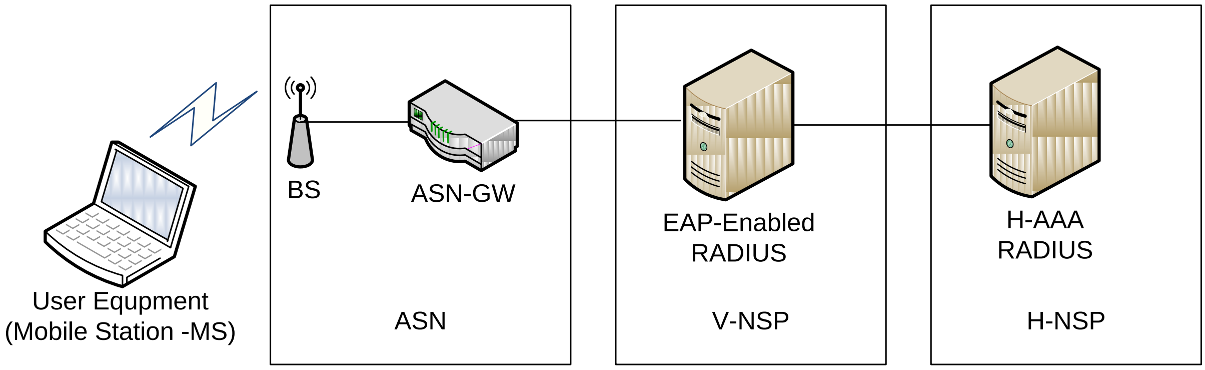


Figure 19 EAP Network architecture

In this setup, there are two RADIUS AAA-servers, one located at the visiting NSP (Network Service Provider), and one at the H-NSP.

5.3.2 Equipment for EAP-based solutions

To set up an EAP-based solution not very much equipment is needed.

5.3.2.1 ASN Gateway

An ASN gateway is needed to forward EAP messages, the ASN Gateway works as the EAP authenticator. Some WiMAX BSs have EAP authenticator functionality, but if the operator of the network should have several BSs a ASN-GW must be in place. In the Alvarion BS that Uninett and Wireless Trondheim uses there is an ASN-GW included.

5.3.2.2 FreeRADIUS Server

A FreeRADIUS server is needed. This can run on almost any hardware that runs Linux.

5.3.3 Security

With an EAP-based solution there are not so many security concerns as with the captive portal. Both EAP-TLS and EAP-TTLS are protocols designed by security in mind.

The rouge BS problem associated with the captive portal is handled with both EAP-TLS and EAP-TTLS as they can give mutual authentication.

5.3.4 Cost

In this case, only a FreeRADIUS server is needed. FreeRADIUS is free software, which runs on almost any Linux distribution. The estimated costs of a simple Linux server may be 10 000 NOK. If the operator has a FreeRADIUS server already, this can of course be re-used.

FreeRADIUS is pretty light-weight, and probably does not need a dedicated server if the traffic is not very intensive.

5.3.5 User Friendliness

The main drawback with all EAP-based solutions is that the users need some sort of subscription in advance. This means that a user without an account cannot access the network at all before the user signs up, making it difficult for new users as they have to register and pay on a computer connected to the Internet. One can minimize this problem by having roaming agreements so users from other operators can connect, but if there are many operators this can be a resource intensive job.

Current operators (like XOHM and Clear) have solved this problem by selling the mobile stations their self, branded with their company name. These devices have preinstalled X.509 certificates for EAP-TLS, and users have to buy the device together with a subscription.

5.3.6 Login Details

Figure 20 shows an example of a successful EAP-TLS or EAP-TTLS login, in a system with both H-CSN and V-CSN. The RADIUS server in the V-CSN (V-AAA) acts as a proxy.

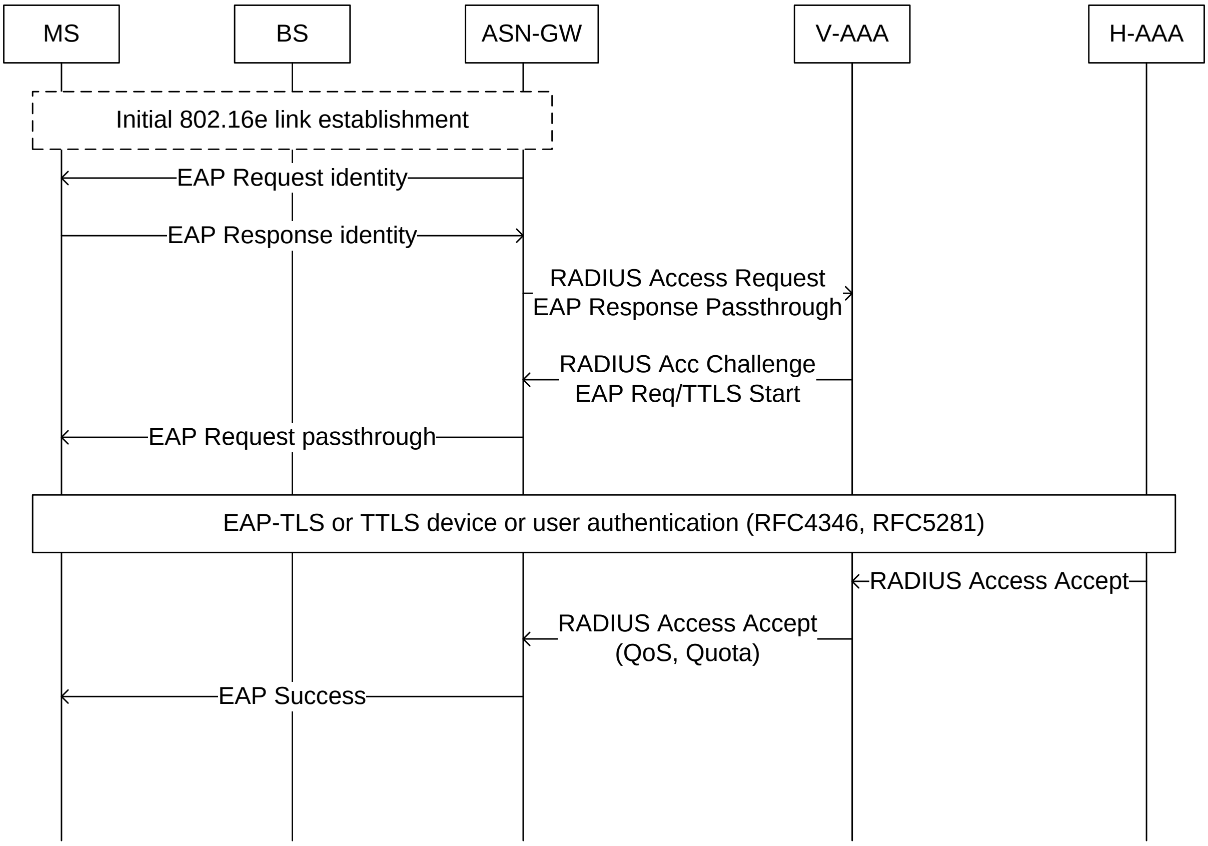


Figure 20 MSC of EAP and RADIUS messages. Successful authentication

5.4 Commercial products – “Aptilo WiMAX AAA+” CSN System

Aptilo is a company based in Sweden that delivers several products for wireless networks. One of their products is the “Aptilo WiMAX AAA+”, which implements several CSN functions from NWG release 1 v1.2 [35]. This product implements several CSN functions [36]:

- AAA server (Which is an extension of FreeRADIUS)
- WiMAX key management
- ASN R3 and R5 interfaces
- QoS and Policy engine with WiMAX and vendor-specific attributes
- Subscriber management

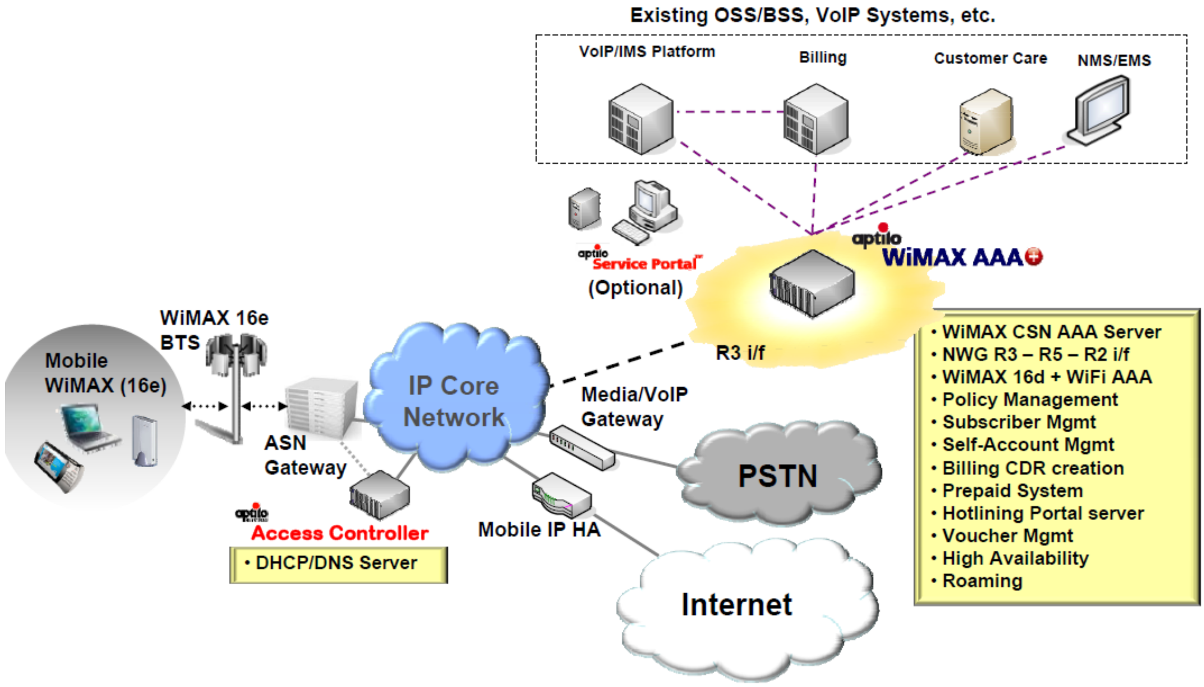


Figure 21 "WiMAX 16e architecture with Aptilo WiMAX AAA+" (From sales brochure) [36]

One feature with the Aptilo product is that it has support hotlining. Hotlining is some sort of captive portal page, but different from ordinary captive portals as hotlining requires the user to be authenticated with EAP first. The hotlining portal page shows only if the user needs credits, or if it is the first time user logs in [37]. One positive feature with hotlining is that WiMAX native QoS parameters can be set during the EAP-negotiation.

The Aptilo product does not support Wi-Fi-like captive portals where the network is open without EAP. This means that users need to have some sort of account before they can be able to connect to the network.

The Aptilio CSN can for an extra cost include a home agent (HA), making roaming between operators possible.

5.4.1 Cost

Compared to the captive portal and FreeRADIUS solution, the Aptilo CSN is an expensive solution, the software for the simplest “Aptilo WiMAX AAA+ Starter Ed” starts at 20 000 USD or around 130 000 NOK. This is just software, and in addition comes hardware, yearly support, maintenance and licenses per user.

Even if Aptilo CSN may seem like an expensive solution, one must remember that it includes more features than the simple EAP solution based on only FreeRADIUS.

6 Practical Work and Implementation

This chapter will describe the implementations done in this project. First, a captive portal was implemented using the Nomadix access gateway, later a test of with FreeRADIUS using EAP-TTLS was planned.

Unfortunately no testing with the WiMAX equipment was done. This is because Wireless Trondheim and Uninett's Alvarion base station was not operable at all during the writing of this thesis. The problems began when Uninett attempted to upgrade the software of the base station, and the problems just continued. There has been a dialogue with both the vendor (Alvarion) and the manufacturer (Upgrade Communication) of the WiMAX equipment, but a solution has not been found.

Especially the FreeRADIUS/EAP solution has suffered without a working base station, it has been impossible to verify the working of this solution. The captive portal has been tested more, but not in the WiMAX network.

6.1 Captive Portal with Nomadix

This section will describe the implementation of a captive portal using a Nomadix access gateway. The implementation is done in PHP5 and MySQL, and is made to support both Wi-Fi and WiMAX (or any other type of IP-based network).

This implementation is an extension of an existing captive portal solution planned and implemented earlier by the author of this thesis. The captive portal is used in Wireless Trondheim's Wi-Fi network, and is used by around 200 users daily. The solution is the property of Wireless Trondheim. Some of the technical details in this part is restricted, and is located in Appendix C.

6.1.1 Requirements

The solution should give users the possibility to buy access, or identify themselves with existing credentials to gain access through a web portal to the Internet. The user should not have to be registered in advance to use the service, and it should be easy to use for novice users.

Users should be able to get access with the following methods:

- Buy access with Cell phone / SMS (Short Message Service)
- Buy access with credit card (PayPal)
- Login with existing organizational user (RADIUS)

6.1.2 Network architecture

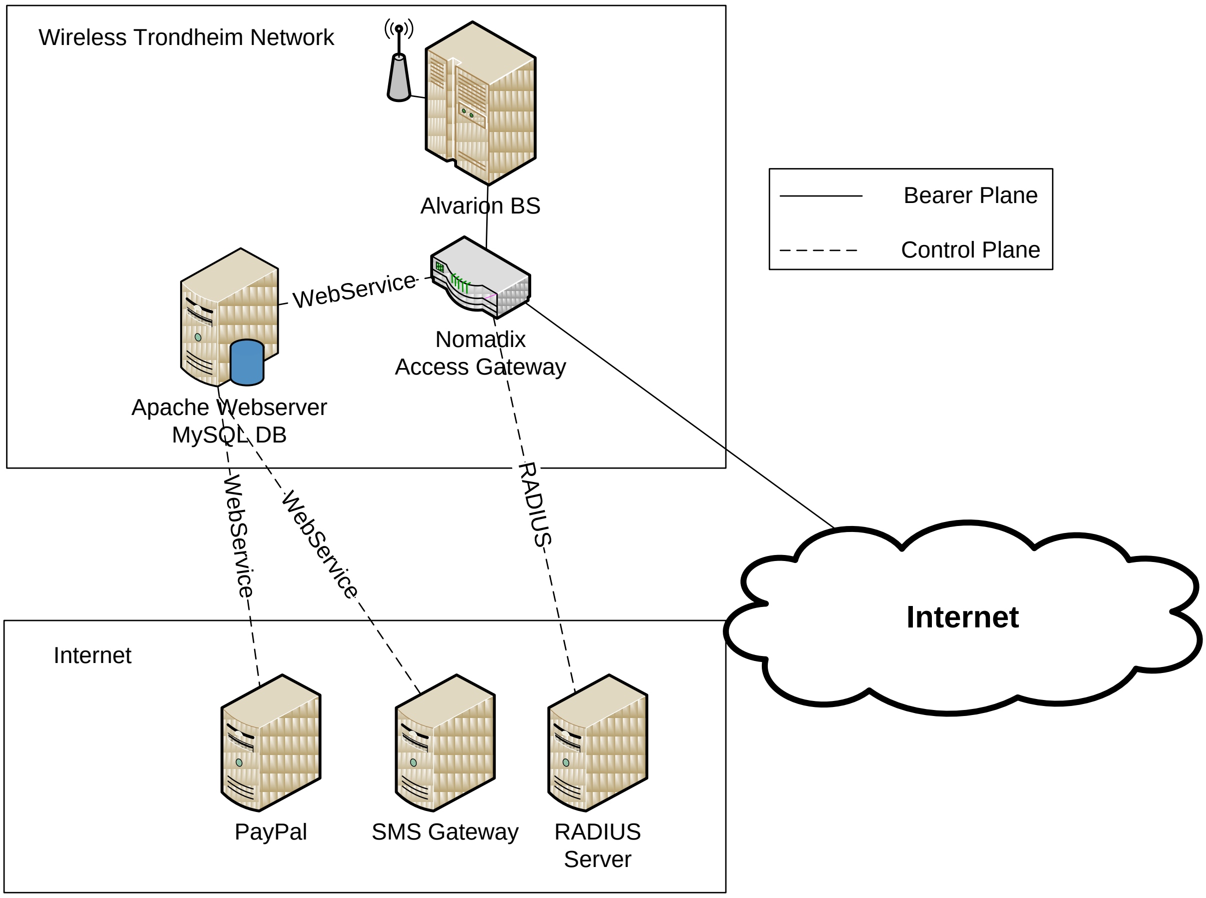


Figure 22 Nomadix Access gateway network architecture

This is a simple overview of how different components in the solution are connected. The main components are the Nomadix access gateway and the Apache web server, which is communicating through a Web service offered by the Nomadix. The Apache server connects to third-party services like PayPal and SMS Gateway through Web services, and RADIUS messages go directly from the Nomadix to the RADIUS server.

All traffic between the servers is routed through Internet, and all traffic between the user and Internet flows through the Nomadix access gateway. Nomadix access gateway can limit the max throughput for each user, preventing one user to use all the capacity.

6.1.3 Login sequence

When an unauthorized user connects to the network, he receives IP address from the Nomadix which acts as a DHCP server. When the user opens a web browser to surf the Internet, the Nomadix check if the user visits a white listed[4] website. If the web site is not white listed, the Nomadix will return “HTTP 302 Moved Temporarily” which redirects the user to the captive portal web page. The URL the user is redirected to is built up as follows:

```
http://tradlosetrondheim.no/?
UI=0192eb&
UURL=http://194.19.111.162:1111/usg/userok.htm&
MA=0013E874E4A7&
OS=http://vg.no/&
SC=7969
```

Here the most interesting parameter is “MA”, which is the MAC-address of the user connected. OS is the website the user tried to connect to in the first place. UI is a unique identification of the Nomadix, and is actually the five last digits of the Nomadix’s MAC-address. This can be useful in a setup with multiple Nomadix devices.

When the user arrives at the captive portal web site, useful variables like the user’s MAC-address are stored.

6.1.3.1 Message Sequence Chart – SMS

Figure 23 shows a successful authentication by SMS. The user receives two SMS messages, the first one includes a code which the user has to verify. The second SMS message is optional, and is sent out if the operator wants to charge the user. It is important that the first SMS is not over-taxed, as the mobile number is not verified yet.

[4] ”White listed website” means that there are some defined IP-addresses or URLs that are not redirected to the captive portal. This can e.g. be from sponsors, payment gateways etc. ”Walled garden” is another term that often is used for white listing of websites.

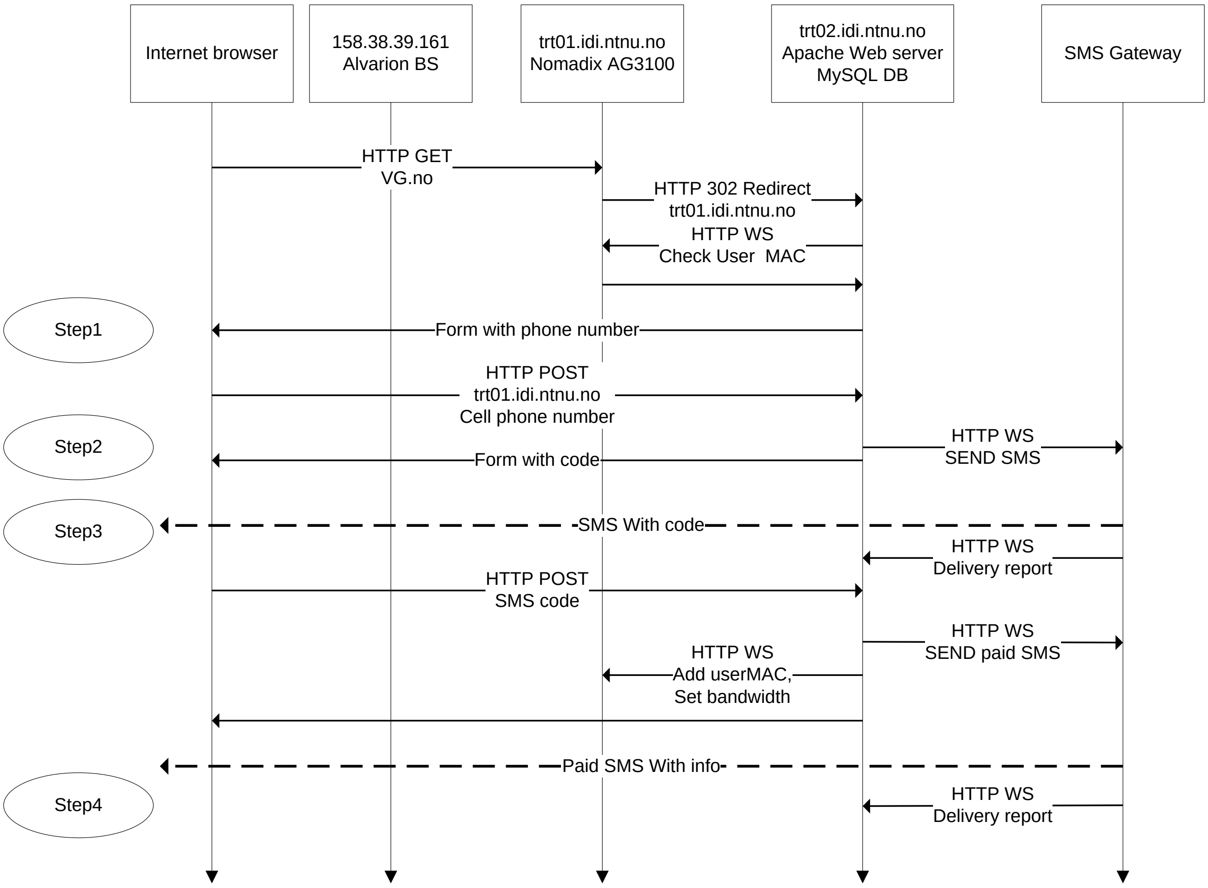
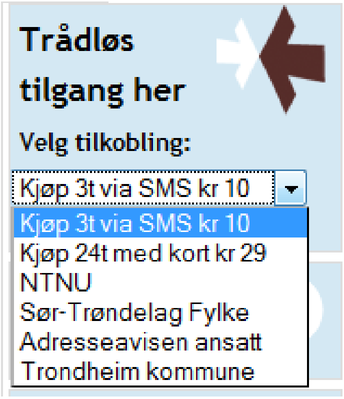


Figure 23 MSC for successful SMS login. Shows HTTP, HTTP Web services (WS) messages and SMS

6.1.3.2 Screenshots - SMS

This series of screenshots shows a successful login sequence for a customer paying with SMS. These screenshots are taken from Wireless Trondheim's captive portal access solution at http://tradlosetrondheim.no. Please refer to the steps in the MSC in Figure 23.

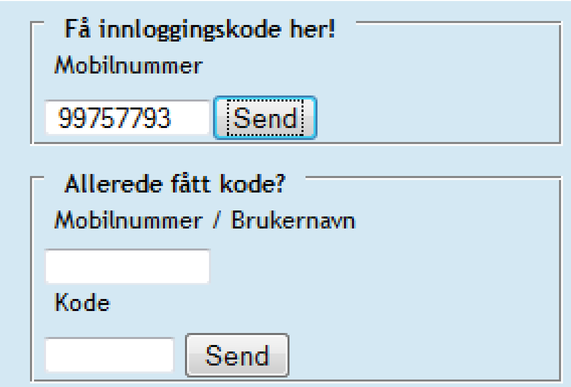

Trådløs tilgang her

Velg tilkobling:

Kjøp 3t via SMS kr 10

- Kjøp 3t via SMS kr 10
- Kjøp 24t med kort kr 29
- NTNU
- Sør-Trøndelag Fylke
- Adresseavisen ansatt
- Trondheim kommune

Figure 24 Different login choices are shown (Step 1 in MSC)



Få innloggingskode her!

Mobilnummer

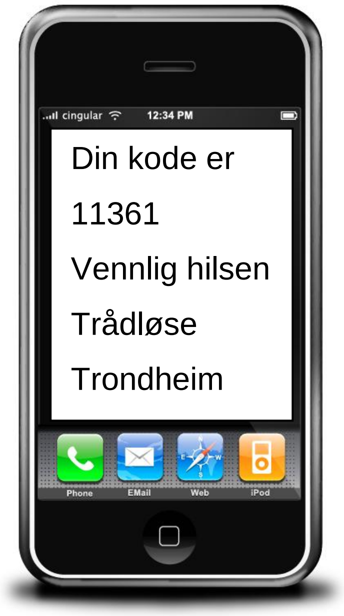
99757793

Allerede fått kode?

Mobilnummer / Brukernavn

Kode

Figure 25 User enters phone number, and clicks "Send"



Din kode er

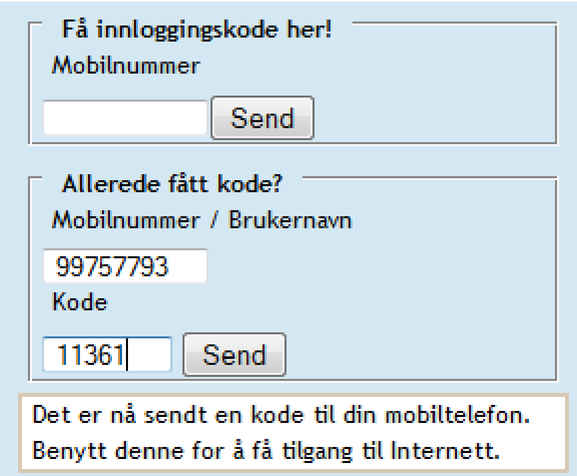
11361

Vennlig hilsen

Trådløse

Trondheim

Figure 26 Code received by SMS (Step 2 in MSC)



Få innloggingskode her!

Mobilnummer

Allerede fått kode?

Mobilnummer / Brukernavn

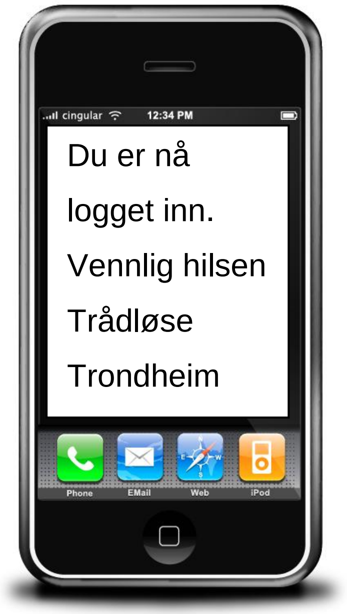
99757793

Kode

11361

Det er nå sendt en kode til din mobiltelefon.
Benytt denne for å få tilgang til Internett.

Figure 27 User enters the code received on SMS (Step 3 in MSC)



Du er nå
logget inn.
Vennlig hilsen
Trådløse
Trondheim

Figure 28 User receive over-taxed SMS. (Step 4 in MSC)

6.1.3.3 Message Sequence Chart – RADIUS

The MSC in Figure 29 shows a successful RADIUS login with the captive portal. The Nomadix does support RADIUS VSAs (Vendor Specific Attributes), which gives the possibility to set attributes like max throughput, expiration time, and more.

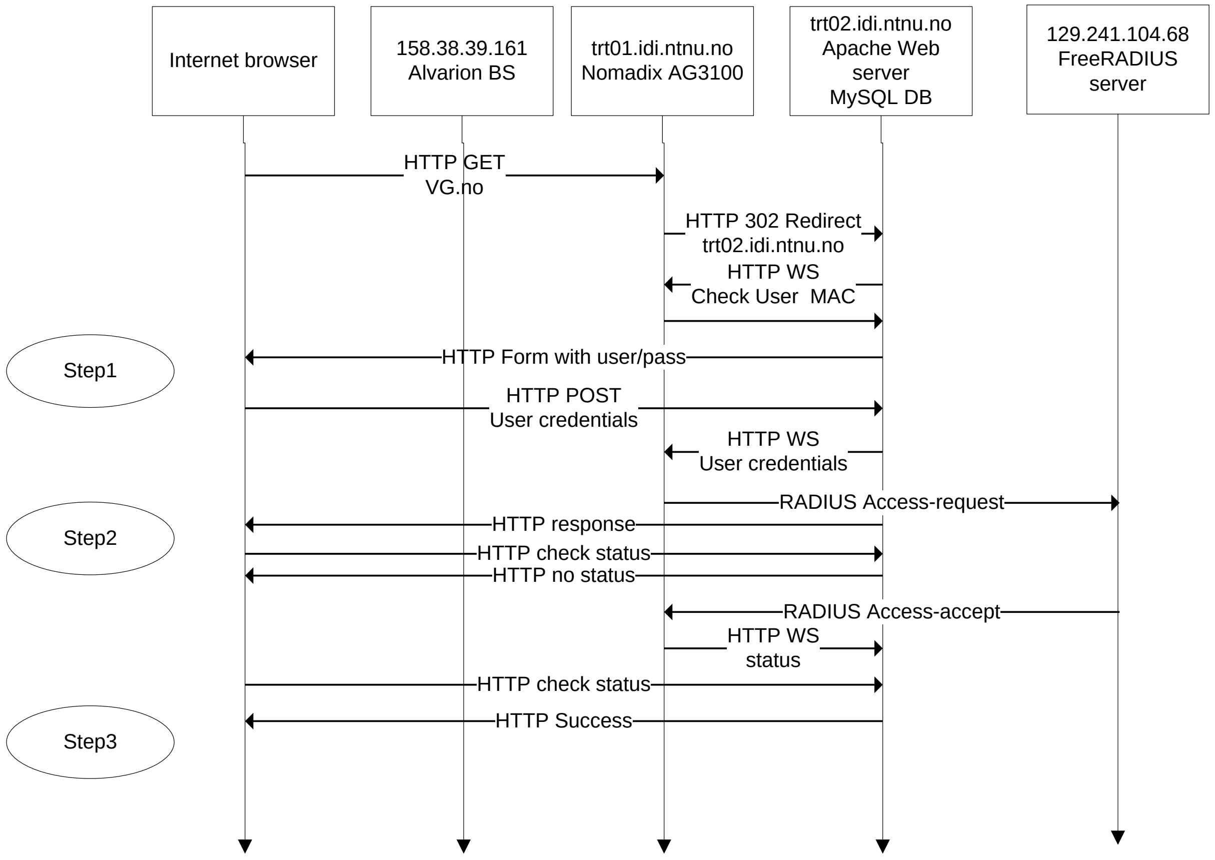


Figure 29 MSC for successful RADIUS login. Shows HTTP, HTTP Web services (WS) messages and RADIUS messages

6.1.3.4 Screenshots – RADIUS

This series of screenshots shows a successful login sequence for a customer paying with SMS. Refer to the steps in the MSC in Figure 29

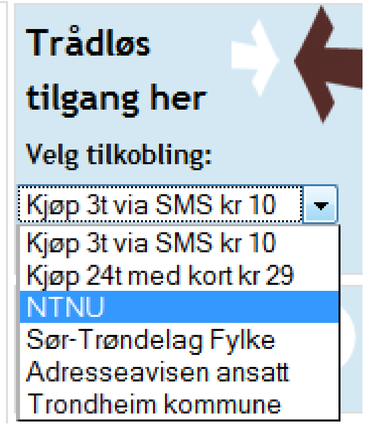
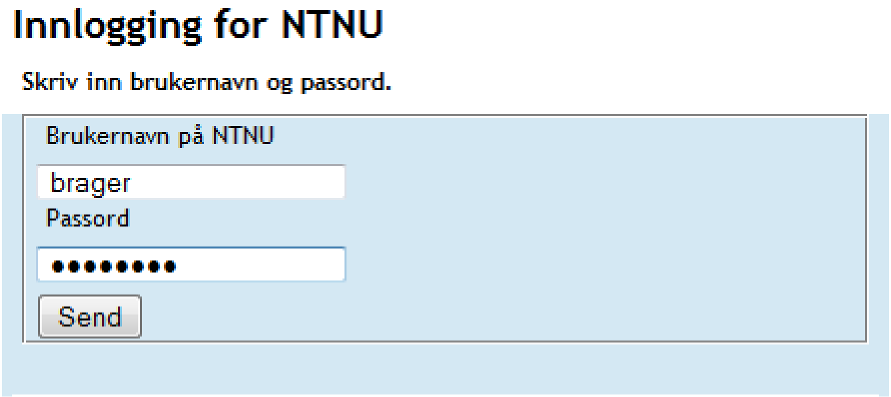


Figure 30 Different login choices are shown (Step 1 in MSC)



Innlogging for NTNU

Skriv inn brukernavn og passord.

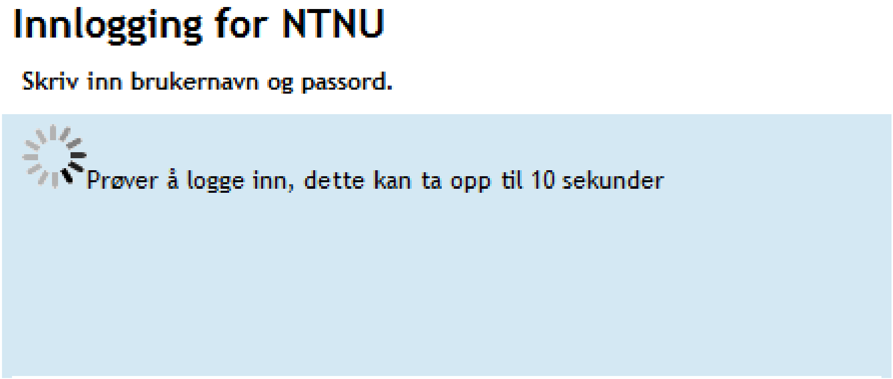
Brukernavn på NTNU

brager

Passord

●●●●●●●●●

Figure 31 User types in predefined username and password

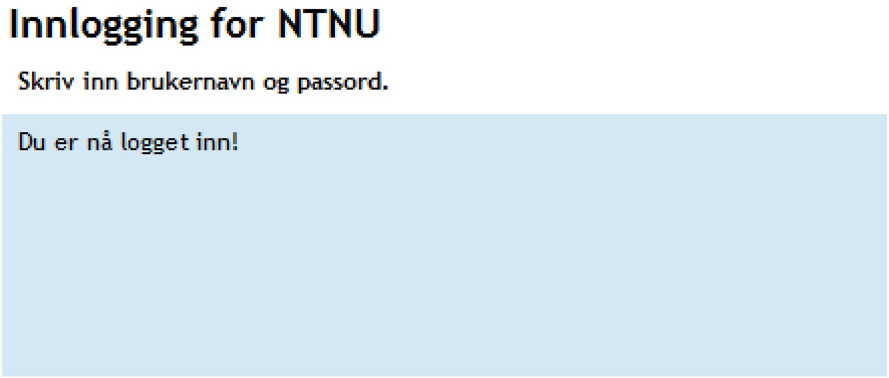


Innlogging for NTNU

Skriv inn brukernavn og passord.

Prøver å logge inn, dette kan ta opp til 10 sekunder

Figure 32 Web browser polls the web server several times to check if RADIUS login is successful (Step 2 in MSC)



Innlogging for NTNU

Skriv inn brukernavn og passord.

Du er nå logget inn!

Figure 33 Login successful (Step 3 in MSC)

6.1.4 WiMAX-specific customizations

This setup is not very WiMAX-specific, and the setup would fit in almost any IP-based network. Especially to set WiMAX QoS settings individually for users is a nice feature, as this allows to give different customers different services. The Nomadix is able to limit the throughput that flows through the Nomadix individually per user, but it would be favorable to do this in the WiMAX network.

Several attempts have been done to assign a client MAC-address to a service profile in the Alvarion BS, but only EAP-authenticated users are allowed in the service profiles. The Alvarion BS does not have a Web Services interface, but supports SNMP (Simple Network Management Protocol). SNMP can be used from PHP, which the system is implemented in. The SNMP MIBs (Management Information Base) tell which attributes that could be changed, but it is not possible to assign user MAC-address to a service profile. Figure 34 shows the proposed setup. Some other BSs may be able to give users different service profiles based on MAC-addresses.

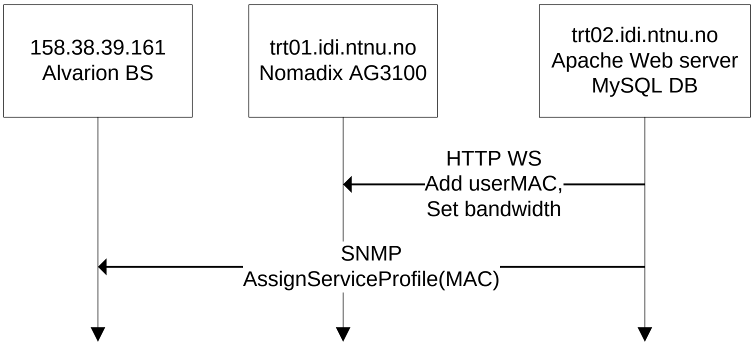


Figure 34 Proposed MSC, but this setup was not achievable

The solution to QoS profiles and individual throughput limiting is to define a default QoS profile in the Alvarion BS for all users, and set max bit rate for the users in the Nomadix. This is not an optimal solution, a user can exploit this setup by sending UDP datagrams in a rate that the Nomadix will not allow, making the Nomadix drop packets. The user will be able to utilize a larger part of the channel between the BS an MS than allowed, and even if the user's throughput is not higher than restricted in the Nomadix, this user can make the service quality poorer for other users.

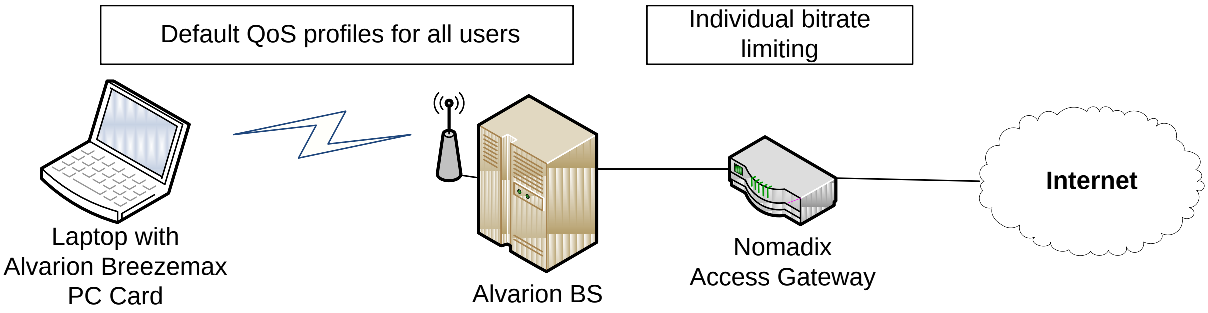

Default QoS profiles for all users
Individual bitrate limiting
Laptop with Alvarion Breezemax PC Card
Alvarion BS
Nomadix Access Gateway
Internet

Figure 35 Captive portal QoS and bitrate limiting. Default WiMAX QoS profiles, individual limiting in Nomadix

6.2 EAP-TTLS with FreeRADIUS

As a part of this project, an EAP-TTLS solution is set up and prepared to be tested. Because of the mentioned trouble with the Alvarion BS, this system has not been tested, so it is not certain that the setup will work as expected.

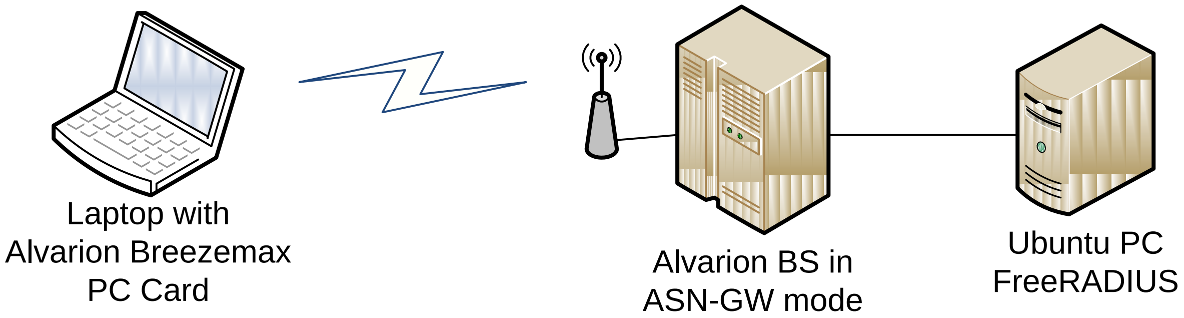
For a detailed guide of how to set up this, with configuration files and commands, please see Appendix B.

6.2.1 Equipment

The solution is set up with the following equipment:

Table 8 Equipment used for EAP-TTLS FreeRADIUS testing

RADIUS Server	Pentium4 3,6GHz 2GB RAM Ubuntu Linux 9.04 FreeRADIUS v2.1.0 built from Ubuntu repository MySQL
Alvarion Base Station	Alvarion BreezeMAX 4Motion 2500
Alvarion BreezeMAX PC card	Model Name: 4M-CPE-PCcard 2.5



6.2.1.1 Ubuntu / FreeRADIUS server

This is the entity where most configuration has to be done. EAP modes is set here, and X.509 certificates are also installed here.

6.2.1.2 Alvarion 4Motion BS

There are not very many settings that have to be set in the BS, mostly pointing out the right RADIUS server and add a shared secret. The Alvarion BS has an included ASN-GW that has to be activated, making it a combined BS and ASN-GW.

Quality of Service (QoS) profiles may be defined in the BS. A detailed explanation of how QoS profiles is set is given in Appendix C.

6.2.1.3 Alvarion BreezeMAX PC card

This card is set up on a laptop, with included software installed. No certificate is needed on the client side, only username and password to authorize the user.

6.2.2 Login Sequence

Figure 36 shows a successful EAP-TTLS authentication between a mobile station (MS), the Alvarion BS and a FreeRADIUS server. Notice the second last message, from the FreeRADIUS server to the BS. This is the message that sets to QoS profile and optional quota (time or quantity), and it is realized with RADIUS VSAs (vendor specific attributes)

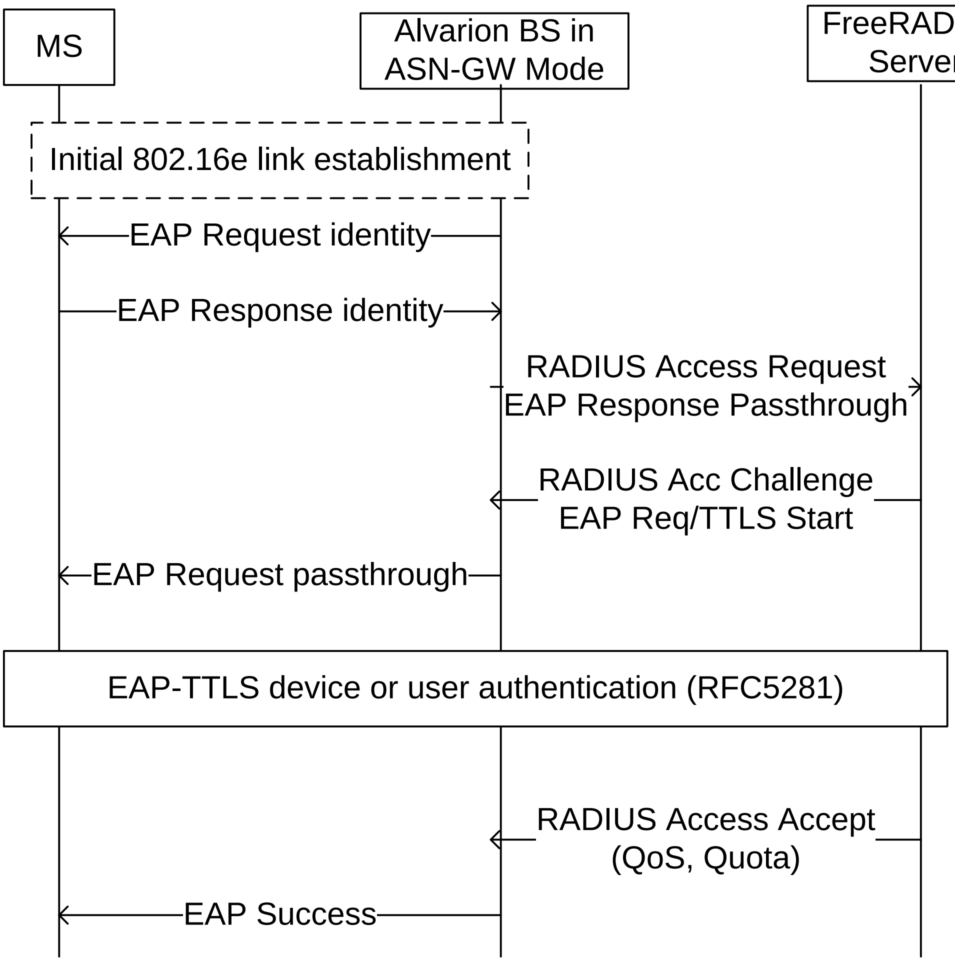


Figure 36 MSC of EAP TTLS solution with FreeRADIUS

6.2.3 Quality of Service

This setup allows interacting with the WiMAX QoS profiles, and here users can be assigned to different service profiles in the BS.

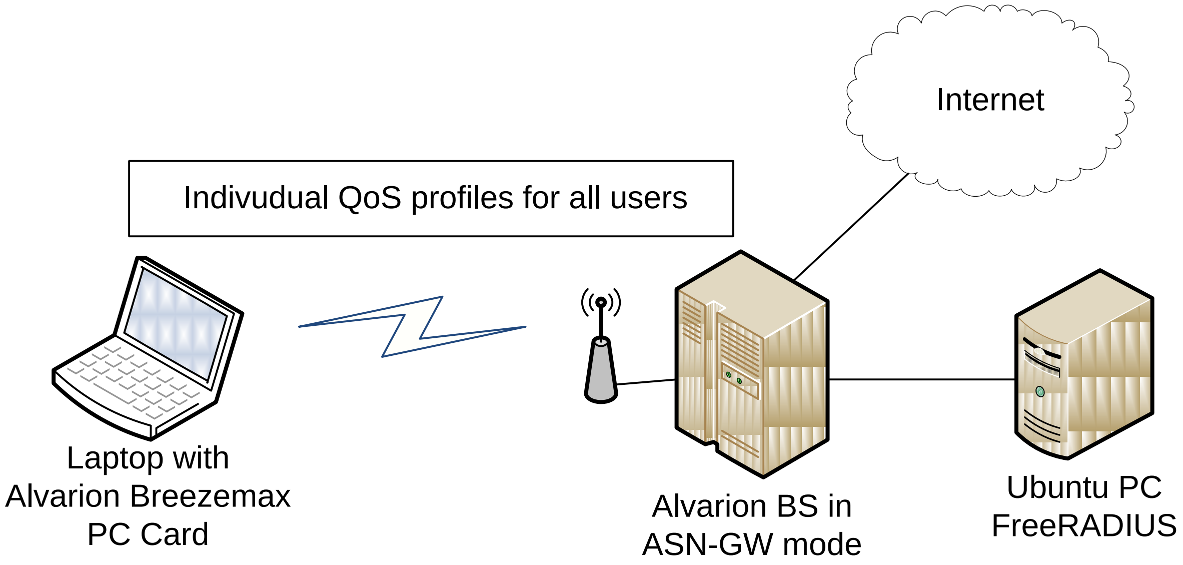


Figure 37 QoS profiles in the EAP solution. QoS is done between MS and BS

7 Discussion and Recommendations

This chapter gives an overview of advantages and disadvantages for the different solutions, and in the end tries to make some recommendations for different cases.

7.1 Comparison of different access solutions

There are several different user access solutions that support different needs. Which business models the operators choose is important for which user access solutions that are to be deployed.

Today it seems like most businesses that own WiMAX networks sell branded WiMAX devices with preinstalled passwords and certificates to their customers, making user access a minor issue for the customers, just plug and play.

The problem with today’s solution is that customers are bound to one operator. If the customers want to use their devices on another operator’s networks, it is difficult to use existing devices, and the customers must also in most cases buy a new subscriptions to the new operator’s network.

For visiting users there will probably be two solutions to choose between:

- Subscription to one operator – EAP with roaming agreements
- Captive portal

Both of these solutions have strengths and weaknesses, and different cases can give different recommendations.

7.1.1 Subscription – EAP-based Solutions

If it becomes common to sell laptops and handheld devices with Mobile WiMAX support, but without bound to a specific operator, an EAP solution may not be very user friendly. With EAP, users need to have some sort of subscription to an operator in advance to connect to a network. EAP-TTLS would probably be the preferred choice, as it only needs username and password on the client side. EAP-TLS require a client certificate, which makes a PKI required to distribute certificates.

The advantage with EAP is that it is a bit more secure than captive portals, and when the user has set up the system with EAP credentials etc. the user will be instantly logged on to the network without extra effort. EAP-based solutions also fit well in the WiMAX reference model, and QoS parameters etc. can be utilized easily.

EAP solutions may support both prepaid and postpaid access, and with hotlining, this can be done in a flexible way.

7.1.2 Subscription – EAP-based Solutions with Roaming

If EAP-based subscription solutions should be a success for traveling users that visits several Mobile WiMAX locations, roaming agreements between operators worldwide must be made. This makes it necessary to have only one subscription, just like on cellular GSM/UMTS phones.

A challenge with roaming agreement is that if there are many NSPs (Network Service Providers), many roaming agreements have to be made. As a solution to this challenge, a business entity WRX (WiMAX Roaming Exchange) is introduced. The WRX is a broker that connects multiple NSPs to simplify roaming, making the number of roaming agreements that NSP have to make smaller. A drawback with using a WRX is that it would make the roaming cost higher, but with many small Mobile WiMAX NSPs, it would be infeasible to achieve roaming without such setup.

The EAP-based solution with Roaming would require some more equipment than a solution without Roaming. Especially is a HA (Home Agent) needed, but business support systems (BSS) must also be more advanced as the complexity rises.

When comparing roaming in Mobile WiMAX with GSM and its successors, it is important to remember that there is one big difference. While Mobile WiMAX's primary task is to give users Internet access, GSM and its successors are phone networks where users connect not just to make outbound calls, but also for others to make incoming calls to the connected user. Unlike in Mobile WiMAX, roaming is essential for the service in GSM, as users expect to be able to receive calls when they are connected to other operators.

When the roaming prices of Telenor, the largest GSM operator in Norway, are investigated, one can see that roaming is very expensive for the customers. Outbound calls in their own network cost around 0,49 NOK/min, and incoming calls are free to receive. However, to make outbound calls and to receive calls when connected to another operator is very expensive. In Europe the rates are between 3,50 and 7 NOK for outbound calls, and between 2 and 4 NOK/min for receiving calls. In the rest of the world, the rates can be up to 25 NOK/min for outbound calls, which is 50 times as much as in their own network [38]. When comparing GPRS roaming data rates these are also very high compared to when the user is connected to the home operator.

These prices can not be transferred directly to Mobile WiMAX prices, but may be an indicator on the costs or having roaming agreements.

7.1.3 Captive Portal-based Solutions

Captive portals are more user friendly for users without a subscription. With captive portals, the user can log on the Mobile WiMAX network, and pay for access in his web browser without having a subscription in advance.

Captive portals are today mostly found at Wi-Fi networks at airports and municipal Wi-Fi networks like Wireless Trondheim. Captive portals works great for tourists and travelers, as the users do not need a subscription in advance.

7.1.4 Cost

Both EAP-based subscriptions with roaming and captive portals give visiting users access to the WiMAX network.

If one compares costs in these solutions, the EAP-based roaming solution would probably be more expensive and more difficult to manage. The equipment may be more expensive, but the large extra cost will come because roaming agreements with other operators must be handled, and money must be transferred between roaming-partners. This will introduce an overhead, both administrative, and to possible third party WRXs.

With a captive portal solution, the operator does not necessarily need to handle roaming agreements. Captive portals do not exclude the possibility to have roaming agreements with other operators, but the main solution for visiting users will probably be to pay in advance for e.g. 3 hours or 24 hours directly with credit card or SMS.

7.2 General recommendations

To make some general recommendations for a Mobile WiMAX, the situation today has to be considered. Mobile WiMAX is not very widely deployed compared to GSM/UMTS, and roaming between operators is not very common.

So far, Mobile WiMAX equipment is almost only sold with a subscription, and the most common is to sell branded Mobile WiMAX equipment together with preinstalled certificates for EAP-TLS and a subscription.

It seems like the WiMAX Forum wants operators to use EAP, and the reference model is well prepared for roaming.

If Mobile WiMAX equipment continues to be sold bundled with subscriptions, the best approach would be, like the WiMAX forum suggests, to have roaming agreements between operators. This would work like in GSM/UMTS, where users have a subscription to one operator and get one single bill. An approach based on roaming will be very easy to use for the customers, they would be automatically connected to any Mobile WiMAX network that their network service provider (H-NSP) has a roaming agreement with.

Before roaming agreements gets common, captive portals is the only way to allow visitors access to the network.

Figure 38 illustrates the problem discussed, Mobile WiMAX lies between the Wi-Fi Captive portal and GSM/UMTS with full roaming. Which direction to choose?

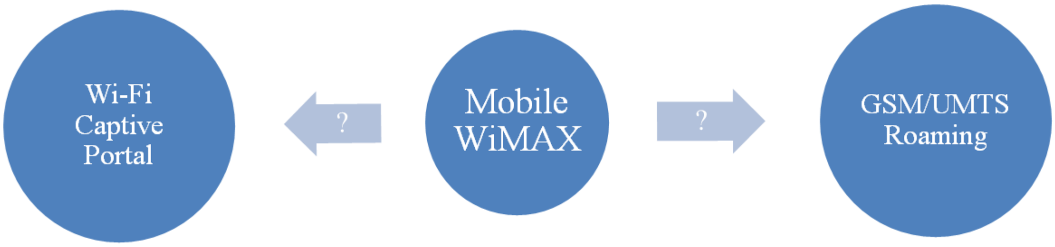


Figure 38 Mobile WiMAX user access. Wi-Fi- like Captive portal or GSM/UMTS-like roaming agreements?

7.3 Recommendations for Wireless Trondheim

For a small actor such as Wireless Trondheim the easiest solution would be to deploy a captive portal. Existing solutions for Wi-Fi networks can be re-used, and this can be done for a small extra cost. A captive portal will probably be the only solution possible for visiting users, as roaming agreements can be troublesome.

EAP-based solutions like EAP-TTLS can be deployed in parallel and be offered to users more permanently located in the area, providing them a slightly more secure solution.

An EAP-based solution with roaming with other operators is not recommended at the moment, as Mobile WiMAX is not widely deployed yet. Roaming agreements are not very common today, and the cost of equipment and effort needed to set up roaming will be too high compared to the value of the extra service this would give to the customers. If roaming agreements get more common later, and roaming becomes a service that customers expect, EAP with roaming agreements can be deployed.

8 Conclusion and Future Work

8.1 Conclusion

There are mainly three main paths when discussing user access in Mobile WiMAX:

- Open network with captive portals
- EAP based solutions without roaming
- EAP based solutions with full GSM/UMTS-like roaming possibilities between Mobile WiMAX operators.

There are positive and negative sides about all solutions. EAP-TLS and EAP-TTLS are great for users living or working in the operator's coverage area. These users can buy subscriptions, and will tolerate some more steps to connect the first time, with the advantage of being connected quickly the next times.

For visiting users there are two possibilities: Captive portal or EAP with roaming. EAP is well integrated with the WiMAX reference model, but with roaming, it is an expensive solution for the operator to deploy. Roaming between operators is not very common in Mobile WiMAX today, but as the WiMAX Forum is promoting it, roaming may be more common later [15]. The EAP solution can utilize the different Quality of Service modes in WiMAX, this is something that is difficult to achieve with the captive portal. The captive portal is easy to deploy and less expensive, and gives visiting users an easy way to connect without an existing account.

Security is one of the issues that are discussed in this thesis, and overall, security in all solutions proposed is reasonably good. No major issues are found in EAP-based solutions. The captive portal only has issues with the "rouge base station problem", as this solution does not provide mutual authentication, but this threat is mostly theoretical and has low consequences. Compared to a Wi-Fi captive portal, a WiMAX captive portal is much more secure, and secure enough for most applications.

The practical work in this thesis has showed that access solutions in Mobile WiMAX can be implemented in an inexpensive and not very complex way. Unfortunately these solutions have not been validated and tested because of failures in the Alvarion WiMAX BS.

8.2 Future work

It may be interesting to look further into several topics related to this thesis.

8.2.1 Practical testing of user access solutions

During this thesis, several user access solutions have been specified and partly implemented. Unfortunately since there has been a lot of trouble with the Alvarion BS. Testing the solutions in a real environment would be useful to see if they work and measure parameters like stability, throughput, user acceptance etc.

Comparing the two user access solutions suggested with regard on throughput would be useful and interesting. The EAP-based solution utilizes QoS-functions integrated in the WiMAX architecture, while the captive portal provides individual throughput limiting near the Internet gateway. Especially with several clients connected, how would these two approaches separate?

8.2.2 The cost of roaming in Mobile WiMAX

As part of the discussion in this thesis, it is stated that roaming agreements between operators may be expensive to handle. Between larger operators it is probably more likely that roaming agreements are applicable, but what about smaller operators with coverage just in smaller cities? Are there threshold-values for how large operators or how widespread Mobile WiMAX needs to be before it is profitable to enter roaming agreements? Are there technical issues with having roaming agreements?

8.2.3 LTE (Long Term Evolution)

LTE is wireless technology that is proposed as the successor of HSDPA and maybe also replace Mobile WiMAX. How do LTE differ from HSDPA and Mobile WiMAX, and will there be place for Mobile WiMAX when LTE is released?

8.2.4 WiMAX Hotlining

Hotlining is an interesting technique that combines EAP with a self-service web portal where users can buy more access time, upgrade service class etc. Hotlining is specified by the WiMAX Forum, and implemented by several commercial CSN products. A thesis proposal could be to investigate hotlining more in detail and implement a working prototype based on FreeRADIUS.

9 Reference

[1] WiMAX Forum. *WiMAX Forum*. http://wimaxforum.org

[2] Reuters. *WiMAX Forum Announces First Commercial Global Roaming Trials at WiMAX Forum Global Congress 2009*. http://www.reuters.com/article/pressRelease/idUS52466+02-Jun-2009+BW20090602

[3] NextNet AS. *NextNet AS.* http://nextnet.no/

[4] NoCat Community. *NoCat*. http://nocat.net

[5] Alleven, M. *Clearwire Launches Mobile WiMAX in Portland*. http://www.wirelessweek.com/Clearwire-Mobile-WiMAX-Portland.aspx

[6] XOHM. *Clearwire Completes Transaction with Sprint Nextel and $3.2 Billion Investment to Launch 4G Mobile Internet Company*. http://www.xohm.com/en_US/about/news-events/press-release/press-release-20081201.html

[7] Andrews, J. G., Ghosh, A., & Muhamed, R. (2007). *Fundamentals of WiMAX, Understanding Broadband Wireless Networking.* Prentice Hall.

[8] Etemad, K. (2008, October). Overview of Mobile WiMAX Technology and Evolution. *IEEE Communications Magazine* , pp. 31-40.

[9] Karlsen, R. S. (2008). *The Wireless Tram. (Master thesis from NTNU)*

[10] IEEE. *IEEE 802.16 Task Group a*. http://wirelessman.org/tga/index.html

[11] WiMAX Forum. (2009). *WiMAX Forum Network Architecture (Stage 2: Architecture Tenets, Reference Model and Reference Points) Release 1.0 Version 4.*

[12] IEEE (2005). *IEEE 802.16-2005 Std.*

[13] Alvarion. (2008). *4Motion System Manual.*

[14] Airspan Networks. (2007). *Mobile WiMAX Security Whitepaper.*

[15] WiMAX Forum. (2008). *WiMAX Forum Roaming Guidelines, Release 1.0 Approved.*

[16] WiMAX Forum. (2009). *WiMAX Forum Network Architecture Stage 3: Detailed Protocols and Procedures Release 1.0 Version 4.*

[17] Wireless Trondheim. *Wireless Trondheim.* http://wirelesstrondheim.no

[18] Hassel, J. (2003). *RADIUS.* O'Reilly.

[19] Wikipedia contributors. *AAA protocol*. http://en.wikipedia.org/w/index.php?title=AAA_protocol&oldid=279750709

[20] Wikipedia contributors. *RADIUS*. http://en.wikipedia.org/w/index.php?title=RADIUS&oldid=287787486

[21] DeKok, A. (2009). *Protocol and Password Compatibility*. http://deployingradius.com/documents/protocols/compatibility.html

[22] Ou, G. (2005). *Understanding the updated WPA and WPA2 standards*. http://blogs.zdnet.com/Ou/index.php?p=67

[23] IETF. (2006). *RFC 4187 Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA).* http://tools.ietf.org/html/rfc4187

[24] Tews, E., Weinmann, R.-P., & Pyshkin, A. *Breaking 104 bit WEP in less than 60 seconds.*

[25] Beck, M., & Tews, E. (2008). *Practical attacks against WEP and WPA.* (Paper from TU Darmstadt, Germany)

[26] Niemi, V., & Nyberg, K. (2003). *UMTS Security.* Wiley.

[27] Wireless Center. *UMTS Architecture Description*. http://www.wireless-center.net/Wireless-Internet-Technologies-and-Applications/1855.html

[28] Sanders, T.. *WiMax.com Premium Five Essential Elements of WiMAX Security*. http://www.wimax.com/commentary/spotlight/wimax-com-premium-five-essential-elements-of-wimax-security

[29] Hartley, J. M. *Wi-Fi and WiMAX Protocols of Security*. http://software.intel.com/en-us/articles/wi-fi-and-wimax-protocols-of-security/

[30] NIST - National Institute of Standards and Technology. *Block Ciphers*. http://csrc.nist.gov/groups/ST/toolkit/block_ciphers.html

[31] Zyablov, V. V., & Osipov, D. S. (91-98). On the optimum choice of a threshold in a frequency hopping OFDMA system. *Problems of Information Transmission*, 2008.

[32] Microsoft. *RADIUS Protocol Security and Best Practices*. http://technet.microsoft.com/en-us/library/bb742489.aspx

[33] Wikipedia contrbutors. *IPsec*. http://en.wikipedia.org/w/index.php?title=IPsec&oldid=283304480

[34] FreeRADIUS Server Project. *FreeRADIUS.* http://freeradius.org/

[35] Aptilo Networks. (2008). *Aptilo WiMAX CSN System (White paper).*

[36] Aptilo Networks. (2009). *Aptilo WiMAX AAA+ Starter Ed (Presentation).*

[37] Aptilo Networks. (2009). *Aptilo Signaling flow: WiMAX Forum NWG Prepaid billing support (White paper).*

[38] Telenor. *Priser Mobilabonnement*. http://www.telenor.no/privat/mobil/priser/

[39] The World Wide Web Consortium (W3C). *Web Services Glossary*. http://www.w3.org/TR/ws-gloss/

[40] Net-SNMP Community. *Net-SNMP*. http://www.net-snmp.org/

[41] The PHP Group. *PHP: SNMP*. http://www.php.net/manual/en/book.snmp.php

[42] Nomadix, Inc. (2005). *AG5000 User Guide 5.4.1.*

[43] Nomadix, Inc. (2007). *Nomadix XML Interface DTD 5.0.15*.

Appendix A Methods for Machine to Machine Communication

This appendix will briefly describe a few protocols/methods for machine to machine communication. These protocols is used in the captive portal solution.

A.1 Web Services

The World Wide Web Consortium (W3C) have defined Web services the following way: *"A Web service is a software system designed to support interoperable machine-to-machine interaction over a network."*[39]

Web services can be implemented in several different ways, using different techniques. Common for all web services is that they are used to transfer data between computers over a network. The computers may run different operating systems, and use different programming languages. There is for instance possible for a PHP script running on a Linux server to access an ASPX web service on a Windows server.

Web services are very flexible, and it is up to the ones who are deploying the web service to tell what the web service should do, which parameters to take in and send out etc.

Most web services runs over HTTP(S), and it is thus easy to use them over the Internet. Another argument for using web services is that most firewalls pass through HTTP and HTTPS traffic.

A.2 Simple Network Management Protocol (SNMP)

SNMP is a protocol for monitoring and configuring network-attached devices. The protocol is simple, and can read and write attributes to the SNMP managed devices.

The protocol is defined by the Internet Engineering Task Force (IETF), and is a part of the Internet protocol suite.

There are several versions of SNMP (SNMP v1, v2 and v3), where version one and two is the most common. The two first versions do not implement encryption, making the protocol vulnerable for eavesdropping and tampering. If SNMP is going to be used on the Internet and not just internally on a local network, it has to be secured using IPsec etc.

SNMP can be used as a supplement or instead to web services where web services are not present or does not suit your needs.

A.2.1 SNMP MIB (Management Information Base)

The SNMP protocol does not define which attributes that the managed system should offer this is done by MIBs. MIBs define the structure of the management information data, and vendors can define their own MIBs, making the protocol very flexible.

A.2.2 Net-SNMP

Net-SNMP is a widely used open source SNMP software suite that can be used from various platforms. [40] There is a PHP interface to Net-SNMP, making it easy to use from PHP. [41]

Appendix B EAP-TTLS with FreeRADIUS detailed configuration

This appendix describes how to set up an EAP-TTLS-based solution with the popular RADIUS server FreeRADIUS.

It is important to note that this setup is not tested, so it not certain that all steps in this appendix will work, and especially the interaction between the components is not proven to work.

B.1 FreeRADIUS

Resources of information on FreeRADIUS is the official FreeRADIUS website, http://FreeRADIUS.org, examples inside the configuration files, and the “FreeRADIUS users” mailing list at freeradius-users@lists.freeradius.org. There is high activity on the mailing list, and it is easy to get help there. The mailing list archives are also a good place to search for info.

B.1.1 FreeRADIUS configuration files

In a standard Ubuntu install, FreeRADIUS configuration files are located in /etc/freeradius/. The configuration files in the Ubuntu package mostly stripped down for comments and examples, but the latest package from FreeRADIUS.org has configuration files that are well documented with comments and examples inside the files.

This subchapter will describe some of the most important configuration files, and show examples of

/etc/freeradius/clients.conf

```

client localhost {
     secret          = superBrageSecret2000
     shortname  = localhost
}
client trt01.idi.ntnu.no {
     secret          = nomadixsuper
     shortname  = trt01
}
client 158.38.39.161 {
     secret          = supersecret123
     shortname  = alvarion
}
```

/etc/freeradius/users

```
Brage            Cleartext-Password := "BragePass"
                 Reply-Message = "Hello, %{User-Name}"
```

/etc/freeradius/eap.conf

```
eap {
     ttls {

                default_eap_type = md5


                copy_request_to_tunnel = no

                use_tunneled_reply = no


                virtual_server = "inner-tunnel"
          }
 }
```

The last line defines which virtual server the inner tunnel points to

/etc/freeradius/sites-enabled/inner-tunnel

This file says something about the inner protocol to be used in EAP-TTLS.

/usr/share/freeradius/

This directory includes dictionary files for WiMAX, Alvarion, Nomadix and many other vendors. These are the vendor specific attributes (VSA)

/usr/share/freeradius/dictionary.wimax

The following code is taken from the dictionary.wimax file, and shows which VSAs that are available as a part of the WiMAX standard. Below is a selected part of the file, the whole dictionary has 133 atributes.

```
# -*- text -*-
####################################################################
##########
#
#    WiMAX Forum
#
#    Updated from NWG_R1_V1.2.1-Stage-3.pdf
#
#    NWG_R1_V1.2-Stage-3.pdf
#    RADIUS discussion is on pp. 432-498
#    WiMAX VSA's are on p. 450 and following.
#

VENDOR          WiMAX                24757 format=1,1,c

BEGIN-VENDOR    WiMAX

ATTRIBUTE  WiMAX-Capability          1     tlv

BEGIN-TLV  WiMAX-Capability
ATTRIBUTE  WiMAX-Release                   1    string
ATTRIBUTE  WiMAX-Accounting-Capabilities        2    byte
ATTRIBUTE  WiMAX-Hotlining-Capabilities         3    byte
ATTRIBUTE  WiMAX-Idle-Mode-Notification-Cap4    byte

# This is really a bitmap
VALUE WiMAX-Accounting-Capabilities  No-Accounting         0
VALUE WiMAX-Accounting-Capabilities  IP-Session-Based1
VALUE WiMAX-Accounting-Capabilities  Flow-Based      2

# This is really a bitmap
VALUE WiMAX-Hotlining-Capabilities   Not-Supported         0
VALUE WiMAX-Hotlining-Capabilities   Hotline-Profile-Id    1
VALUE WiMAX-Hotlining-Capabilities   NAS-Filter-Rule       2
VALUE WiMAX-Hotlining-Capabilities   HTTP-Redirection4
VALUE WiMAX-Hotlining-Capabilities   IP-Redirection        8

END-TLV         WiMAX-Capability

BEGIN-TLV WiMAX-Packet-Flow-Descriptor
ATTRIBUTE  WiMAX-Packet-Data-Flow-Id       1    short
ATTRIBUTE  WiMAX-Service-Data-Flow-Id      2    short
ATTRIBUTE  WiMAX-Service-Profile-Id        3    integer

ATTRIBUTE  WiMAX-Uplink-QOS-Id             7    byte
ATTRIBUTE  WiMAX-Downlink-QOS-Id           8    byte
ATTRIBUTE  WiMAX-Uplink-Classifier              9    string
ATTRIBUTE  WiMAX-Downlink-Classifier       10   string
END-TLV    WiMAX-Packet-Flow-Descriptor
```

```
ATTRIBUTE  WiMAX-QoS-Descriptor            29   tlv

BEGIN-TLV WiMAX-QoS-Descriptor
ATTRIBUTE  WiMAX-QoS-Id                    1    byte
ATTRIBUTE  WiMAX-Global-Service-Class-Name      2    string # 6
octets
ATTRIBUTE  WiMAX-Service-Class-Name        3    string
ATTRIBUTE  WiMAX-Schedule-Type             4    byte
ATTRIBUTE  WiMAX-Traffic-Priority               5    byte
ATTRIBUTE  WiMAX-Maximum-Sustained-Traffic-Rate 6    integer
ATTRIBUTE  WiMAX-Minimum-Reserved-Traffic-Rate  7    integer
ATTRIBUTE  WiMAX-Maximum-Traffic-Burst          8    integer
ATTRIBUTE  WiMAX-Tolerated-Jitter               9    integer
ATTRIBUTE  WiMAX-Maximum-Latency           10   integer
ATTRIBUTE  WiMAX-Reduced-Resources-Code         11   byte
ATTRIBUTE  WiMAX-Media-Flow-Type           12   byte
ATTRIBUTE  WiMAX-Unsolicited-Grant-Interval13   short
ATTRIBUTE  WiMAX-SDU-Size                  14   short
ATTRIBUTE  WiMAX-Unsolicited-Polling-Interval   15   short
ATTRIBUTE  WiMAX-Media-Flow-Description-SDP16   string

VALUE WiMAX-Schedule-Type        Best-Effort          2
VALUE WiMAX-Schedule-Type        nrtPS           3
VALUE WiMAX-Schedule-Type        rtPS            4
VALUE WiMAX-Schedule-Type        Extended-rtPS        5
VALUE WiMAX-Schedule-Type        UGS             6

VALUE WiMAX-Media-Flow-Type      VoIP            1
VALUE WiMAX-Media-Flow-Type      Robust-Browser       2
VALUE WiMAX-Media-Flow-Type      Secure-Browser-VPN   3
VALUE WiMAX-Media-Flow-Type      Streaming-Video      4
VALUE WiMAX-Media-Flow-Type      Streaming-Live-TV    5
VALUE WiMAX-Media-Flow-Type      Music-Photo-Download 6
VALUE WiMAX-Media-Flow-Type      Multi-Player-Gaming  7
VALUE WiMAX-Media-Flow-Type      Location-Based-Services    8
VALUE WiMAX-Media-Flow-Type      Text-Audio-Books9
VALUE WiMAX-Media-Flow-Type      Video-Conversation   10
VALUE WiMAX-Media-Flow-Type      Message              11
VALUE WiMAX-Media-Flow-Type      Control              12
VALUE WiMAX-Media-Flow-Type      Data            13

END-TLV WiMAX-QoS-Descriptor

# 3 octets of NAP Id
# 3 octets of base-station Id
ATTRIBUTE  WiMAX-BS-Id                     46   octets
ATTRIBUTE  WiMAX-Location                  47   octets

ATTRIBUTE  WiMAX-Blu-Coa-IPv6              51   ipv6addr
ATTRIBUTE  WiMAX-DNS-Server           52   combo-ip
ATTRIBUTE  WiMAX-Hotline-Profile-Id        53   string

# Formatted as per IP Filter rule specification.
ATTRIBUTE  WiMAX-HTTP-Redirection-Rule          54   string
```

```

# Formatted as per IP Filter rule specification.
ATTRIBUTE  WiMAX-IP-Redirection-Rule        55    string
ATTRIBUTE  WiMAX-Hotline-Session-Timer            56    integer

# 3 octets
ATTRIBUTE  WiMAX-NSP-Id                     57    octets
ATTRIBUTE  WiMAX-HA-RK-Key-Requested        58    integer

VALUE WiMAX-HA-RK-Key-Requested  No               0
VALUE WiMAX-HA-RK-Key-Requested  Yes              1
-DM-Action-Code            60    integer
```

B.2 X.509 security certificates

To utilize EAP-TTLS a X.509 security certificate must be generated, signed and installed on the FreeRADIUS server. There are sample certificates in the FreeRADIUS install in /etc/freeradius/certs/ which can be used for testing. In a production environment, real certificates have to be generated and signed.

B.3 Testing FreeRADIUS locally

To start the FreeRADIUS server in debug mode, use the following command. The “-X” flag is to print all debug output.

```
brager@brager-ununtu:~$ sudo freeradius -X
```

To test if the server works, the following command may be run:

```
$ radtest Brage BragePass localhost 1812 superBrageSecret2000
```

B.3.1 FreeRADIUS and Alvarion interoperability

There have been some discussions about Alvarion’s RADIUS implementation. The lead developer of the FreeRADIUS project, Alan DeKok, writes on May 18, 2009 on the “FreeRADIUS users” mailing list (freeradius-users@lists.freeradius.org):

“FreeRADIUS works with WiMAX equipment from Nokia, Cisco and Motorola. (That I've seen.) Other vendors known to have problems include Alvarion. They don't seem to care that their equipment doesn't work, and they haven't answered any of my messages about it.

*The only solution is to point out publicly that Alvarion is *not* following the WiMAX specs, and therefore people should buy *real* WiMAX equipment.”*

Kristoffer Milligan in NextNet has also done some testing with FreeRADIUS and Alvarion equipment without succeeding with this.

B.4 Alvarion BreezeMAX 4Motion BS

All these configurations must be done on the CLI (command line interface). There is a NMS (Network Management System) named Alvarion AlvariSTAR that may be smart to use instead of the CLI. The CLI is not always easy to understand, and the manual has to be used extensively to understand which commands to use, and how things relate to each other. AlvariSTAR gives a more intuitive GUI, and does also have other favorable features like fault management and performance monitoring.

The Alvarion BS have to be set up in ASN-GW mode to support several ASN-GW functions like EAP authenticator, RADIUS client, DHCP etc. To set up the BS in ASN-GW mode, the following command must be executed:

```
npu(config)# nextbootmode asngw
```

To check which mode the BS is running, run the command `show bootmode`.

Chapter "4.3.10 Configuring the ASN-GW Functionality" in the 4Motion system manual [13] does describe how to set up the ASN-GW functionality. According to the manual, only one AAA client can be configured in this version of the BS.

B.4.1 RADIUS

To configure the BS as a RADIUS AAA client, the following steps is done. The IP-address set is the IP of our FreeRADIUS server. For more information, see the manual.

```
npu(config)# aaa-client eaptest      #creates an aaa client alias
npu(config-aaa)# config src-intf bearer
npu(config-aaa)# config primary-serveraddr 129.241.104.68
npu(config-aaa)# config rad-sharedsecret supersecret123
npu(config-aaa)# config auth-port 1812
npu(config-aaa)# config acct-port 1813
```

B.4.2 Service Groups

The Alvarion BTS has in ASN-GW-mode support for “Service Groups”, which in short is a classification of a group of mobile stations (MSs). These groups can define several parameters, like DHCP pool/proxy, primary gateway and DNS.

Example of service group configuration (taken from the manual [13]):

```
npu(config)# srvc-grp group-1
npu(config-srvcgrp)# config srvcif-alias eth0 waitdhcp-holdtime 5
dhcp-ownaddr 12345678

npu(config-srvcgrp)# dhcp-server
npu(config-srvcgrp-dhcpserver)# config pool-minaddr 10.10.10.1
pool-maxaddr 10.10.10.100 pool-subnet 255.255.255.0 dflt-gwaddr
10.10.10.200 lease-interval 100 renew-interval 50 rebind-interval
85 dnssrvr-addr 11.11.11.1

npu(config-srvcgrp)# exit
```

B.4.3 Service Profiles

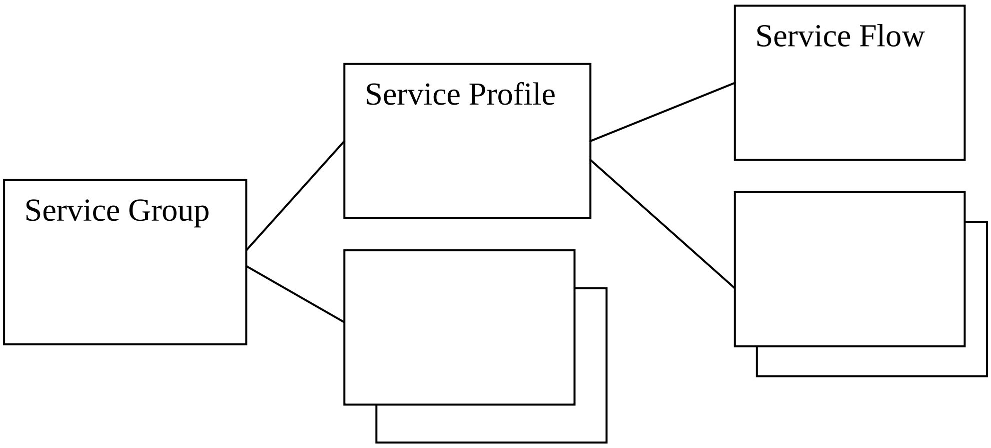


Figure 39 The relationship between Service -Group, -Profile and –Flow

Service profiles and service flows are not necessary to achieve user access, but are needed to classify MSs and users and to avoid the problems with some users using too much capacity.

One service profile is connected to one service group, one service group may have several service profiles.

The Alvarion 4Motion manual [13] describes the relationship between Service profiles and service flows very well:

“The QoS approach is connection-oriented, whereby user traffic is classified into "service flows." A service flow is a unidirectional stream of packets, either in the downlink or uplink direction, associated with a certain set of QoS requirements such as maximum latency. The QoS requirements for service flows are derived from "service profiles" defined by the operator. A service profile is a set of attributes shared by a set of service flows. For instance, an operator might define a service profile called "Internet Gold" that will include QoS and other definitions to be applied to service flows associated with users subscribed to the operator's "Internet Gold" service package.”

A Service Profile does not have many parameters, actually only name and the service group. This configuration creates or modifies the profile with name “prof-1”, and tells that this profile is a part of the “group-1” Service Group.

```
npu(config)# srvc-profile prof-1
npu(config-srvcprfl)# config profile-enable srvc-grp group-1
npu(config-srvcprfl)# exit
```

B.4.3.1 Service Flows

Several QoS parameters may be set, 11 in total. Most of them are optional, and an example of how they can be configured is given below. Here a new flow with id 12 is created, attached to the “prof-1” Service Profile.

```
npu(config)# srvc-profile prof-1

npu(config-srvcprfl)# flow 12

npu(config-srvcprfl-flow)# flow-type bidirectional cs-type 10
media-type voice traffic-pref 6 pag-pref 1 enable-pref
uldatadlvry-type 3 ulqos-maxsustainedrate 5000
ulqos-trafficpriority 6 dlqos-maxsustainedrate 2000

npu(config-srvcprfl-flow)# exit
```

B.4.3.2 Service Flow Authorization (SFA)

The Service Flow Authorization (SFA) handles maintenance of service flows for a MS. SFA maps service profile received from the AAA (RADIUS) server to WiMAX-specific QoS parameters. One service profile may have several service flows.

SFA can also define default values for MSs that does not fit a Service Profile.

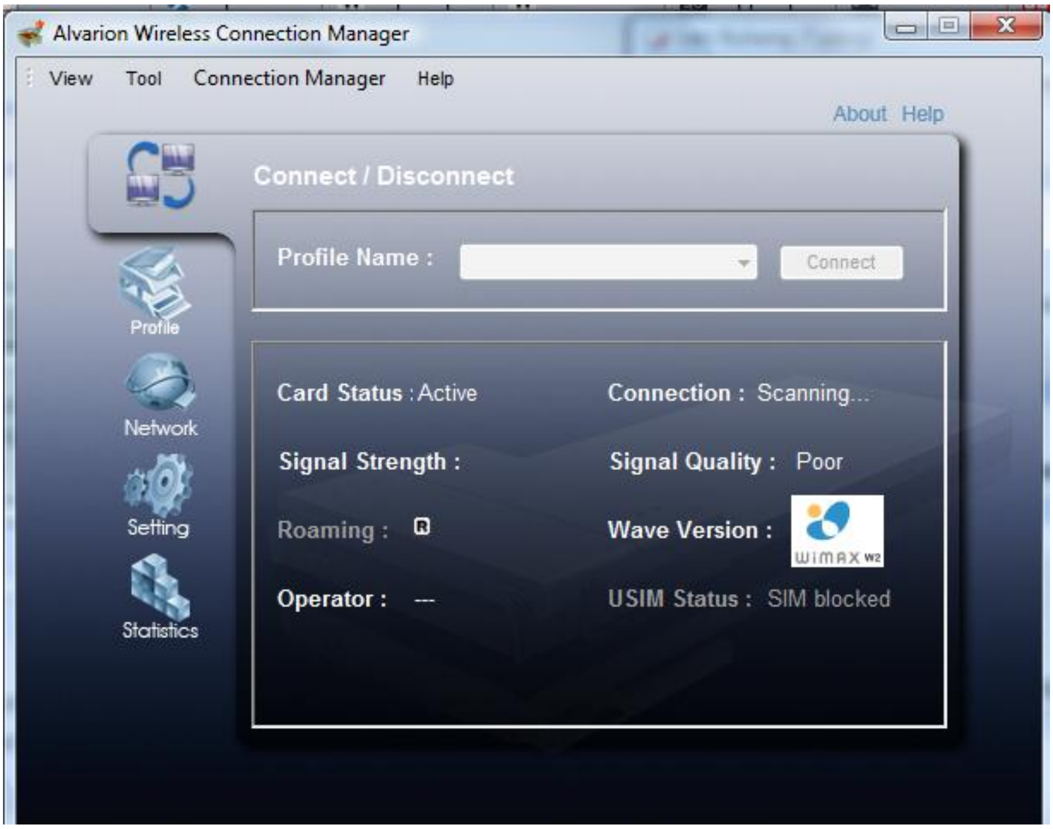
B.5 Alvarion BreezeMAX PC Card

This sub-chapter will investigate the Alvarion BreezeMAX PC Card from an end-user point of view. The software version used in this section is “Alvarion Wireless Connection Manager” version 1.0.0.29, build date 2008/04/30.

How easy is it to set up for a novice user?

The setup of the device may not be very easy for non-technical people. Expressions like Frequency, Bandwidth, EAP etc. is used, not all people know a lot of this.

If an average computer user is told to set up a computer to connect to a WiMAX network he/she must be given detailed instructions on how to set up the device. Today there is too much technical jargon, and the common user will probably fail in connecting. In newer versions, the user interface should be made easier to understand for novice users.



Card Status : Active

Connection : Scanning...

Signal Strength :

Signal Quality : Poor

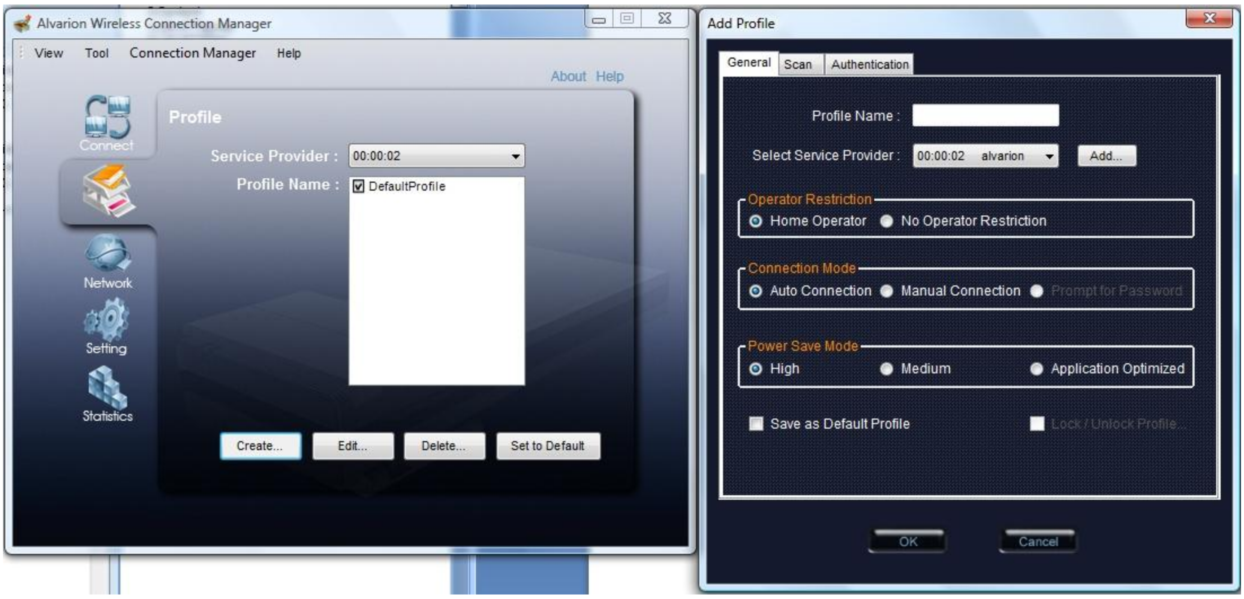
Roaming :

Wave Version :

Operator : ---

USIM Status : SIM blocked

Figure 40 Alvarion WCM main image. If Profiles is set up the user can connect to a profile.



Profile

Service Provider : 00:00:02

Profile Name : ☑ DefaultProfile

Profile Name :

Select Service Provider : 00:00:02 alvarion

Operator Restriction

○ Home Operator ● No Operator Restriction

Connection Mode

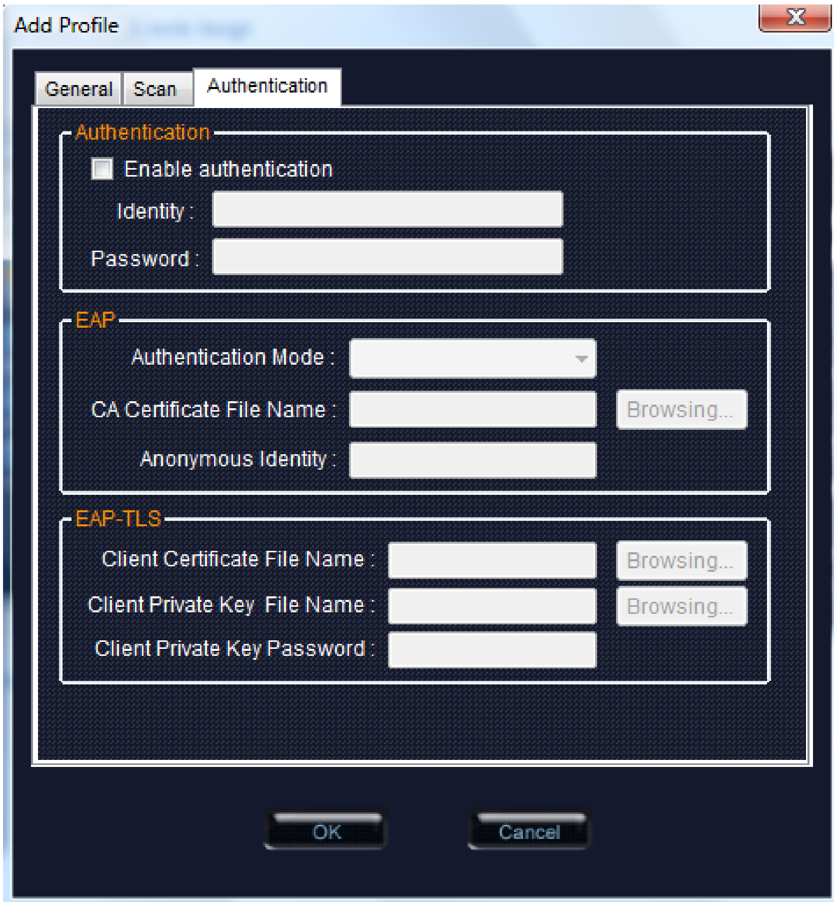
○ Auto Connection ● Manual Connection ● Prompt for Password

Power Save Mode

○ High ● Medium ● Application Optimized

□ Save as Default Profile □ Lock / Unlock Profile...

Figure 41 Alvarion WCM Profile manager and Add Profile. Here there are three tabs with different settings, for instance frequency band and bandwidth.



Authentication

□ Enable authentication

Identity :

Password :

EAP

Authentication Mode :

CA Certificate File Name :

Anonymous Identity :

EAP-TLS

Client Certificate File Name :

Client Private Key File Name :

Client Private Key Password :

Figure 42 Alvarion WCM Authentication tab at Add Profile. Multiple EAP variants supported.