TECHNICAL STANDARD FOR WIRELESS BROADBAND - WiMAX

MTSFB 001 : 2006

CONTENTS

FIGURES

TABLES

ANNEXES

Acknowledgements

Committee representation

The Working Group on Wireless Broadband (WiMAX) under whose authority this MTSFB technical standard was developed, comprises representatives from the following organizations:

Alcatel Network Systems (M) Sdn. Bhd.
Cambridge Broadband
Celcom Berhad
DiGi Telecommunications Sdn. Bhd.
Ericsson (M) Sdn. Bhd.
Huawei Technologies (M) Sdn. Bhd.
Intel Electronics (Malaysia) Sdn. Bhd.
Jaring Bhd.
Malaysian Communications and Multimedia Commission (MCMC)
Marconi (M) Sdn. Bhd.
Maxis Communications Berhad
MiTV Corporation Sdn. Bhd.
Motorola Technology Sdn Bhd
Palette Multimedia Bhd
Rohde & Schwarz Malaysia Sdn. Bhd.
Siemens Malaysia Sdn Bhd
SMART Digital Communications Berhad
Telekom Malaysia Berhad
Telekom Research & Development Sdn Bhd.
TIME dotCom Berhad
Universiti Putra Malaysia
Volans Technology Sdn Bhd
ZTE Corporation Malaysia Sdn Bhd.

FOREWORD

MTSFB (Malaysian Technical Standard Forum Bhd) is a technical standard forum mandated by MCMC (Malaysian Communications and Multimedia Commission) under section 184 of the Communications and Multimedia Act 1998.

This document was developed by the Wireless Broadband working group under the supervision and authority of the MTSFB and is intended to define and serve as a guideline for manufacturers, consulting engineers, licensees, conformance assessment bodies and others who are responsible for designing, installing, operating, certifying or maintaining broadband wireless access network equipment.

This technical standard will be reviewed and revised by the Wireless Broadband working group as necessary to ensure the growth and development of wireless broadband networks and to meet the requirements of end users.

TECHNICAL STANDARD FOR WIRELESS BROADBAND – WiMAX

1 Introduction

Wireless Access Systems (WAS) are radiocommunications systems that connect end-users to core networks. Broadband wireless access (BWA) systems are capable of delivering high data speed to end-users. It is generally used for fast Internet access and can provide businesses and residential users constant, 'always on' Internet access without the need to dial up each time a service is connected.

The technologies used for implementing broadband wireless access include cellular and wireless local area network systems. In addition to Internet access BWA systems can support a wide range of applications including, telephony/voice services, video telephony, video conferencing, computer gaming, telemedicine, distance learning and IPTV.

BWA systems can also be used to provide backhaul links to local area networks (LAN), metropolitan area networks (MAN), wireless local area networks (WLAN) and cellular mobile networks.

2 Wireless local loop (WLL)

Wireless local loop (WLL) refers to wireless technologies employed to connect subscribers to the public-switched telephone network instead of using fixed copper wires. Wireless local loop is a practical solution for extending the reach of existing fixed line networks or for connecting subscribers living in remote areas where it is not economical to operate a wired network. It is a viable alternative to fixed lines in rural areas and in new suburban areas.

The advantages of wireless systems are obvious: there is no need to install cable or rely on existing copper infrastructure that may be inadequate for various reasons.
Wireless access systems are usually owned by a service provider that operates within metropolitan areas. Services include Internet access for businesses, MTUs (multi-tenancy unit), homes, as well as private LAN bridging in metropolitan areas.

3 BWA topologies

There are three basic topologies used in BWA systems.

- Point-to-point (P-P) topology where a station communicates directly with another station;
- Point-to-multipoint (P-MP) topology where each subscriber unit (SU) communicates directly with a base station (BS);
- Multipoint-to-multipoint mesh (MP-MP) topology where SUs communicate with their nearest neighbours and information is relayed through the mesh.

4 Available BWA technologies and standards

In recent years the use of Broadband Wireless Access (BWA) solutions to solve connectivity needs for both commercial and residential applications has surged in popularity. The major advantages of wireless systems are communications to mobile subscribers, the opportunity for reducing infrastructure costs in fixed systems, the ability to rapidly deploy new systems, and the implementation of communications for sparsely populated areas and global users. A broad range of fixed and mobile, terrestrial and satellite systems as well as local area networks are currently being used. Table 4.1 summarizes the BWA technologies and standards currently available worldwide.

4.1 Table 4.1

Standard	Data Rate	Description
IEEE 802.11	Up to 2Mbps in the 2.4GHz band	Use Direct Sequence Spread Spectrum (DSSS) or Frequency Hopping Spread Spectrum (FHSS) as the modulation scheme. This specification has been extended into 802.11b
IEEE 802.11a (Wi-Fi)	Up to 54Mbps in the 5GHz band	Products that adhere to this standard are considered "Wi-Fi Certified". OFDM-based with eight available channels. Less potential for RF interference than 802.11b and 802.11g. Better than 802.11b at supporting multimedia voice, video and large-image applications in densely populated user environments. Relatively shorter range than 802.11b and not interoperable with 802.11b.
IEEE 802.11b/g (Wi-Fi)	802.11b: Up to 11Mbps in the 2.4GHz band 802.11g: Up to 54 Mbps in the 2.4 GHz band	Products that adhere to this standard are considered "Wi-Fi Certified". Use Direct Sequence Spread Spectrum (DSSS) and Complementary Code Keying (CCK) where a set of 64 eight-bit code words used to encode data. Not interoperable with 802.11a. Require fewer access points than 802.11a for coverage of large areas. Offers high speed access to data at up to 300 feet from base station. 14 channels available. The 'g' version was developed to meet demand for increased bandwidth and is backward compatible with 'b'. Current version of 802.11 (a, b and g) do not support quality of service (QoS)
IEEE 802.16	802.16a: Up to 70 Mbps at distances up to 50 km.	802.16 is a family of air interface standards developed for wireless Metropolitan Area Networks (MAN) supporting multimedia services. The original 802.16 standard, published in December of 2001, was specified for point-to-multipoint broadband wireless access (BWA) systems operating in the range 10 GHz to 66 GHz. In January of 2003 an amendment, 802.16a, was approved for systems operating in the range 2 GHz to 11 GHz. More information about the 802.16 family of standards is given in Paragraph 5.
Bluetooth	Up to 2Mbps in the 2.45Ghz band	Use FHSS, no native support for IP, so it does not support TCP/IP and wireless LAN applications well. Best suited for connecting PDAs, cell phones and PCs in short intervals.

HomeRF	Up to 10Mbps in the 2.4GHz band	Intended for use in home. Range is only 100m from base station. Relatively inexpensive to set up and maintain. Voice quality is always good because it continuously reserves a chunk of bandwidth for voice services. Respond well to interference because of frequency-hopping modulation. Note: HomeRF is no longer being supported by any vendors or working groups.
HiperLAN/1 (Europe)	Up to 20Mbps in 5Ghz band	HiperLAN is totally ad-hoc, requiring no configuration and no central controller. Relatively expensive to operate and maintain with no guarantee of bandwidth. Use Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA), that listens to a network in order to avoid collisions, that contributes to network traffic because, before any real data is transmitted, it has to broadcast a signal onto the network in order to listen for collision scenarios and to tell other devices not to broadcast.
HiperLAN/2 (Europe)	Up to 54Mbps in 5GHz band	OFDM based, designed to carry Asynchronous Transfer Mode (ATM) cells, Firewire packets (IEEE 1394) and digital voice from cellular phones. Better quality of service than HiperLAn/1 and guarantees bandwidth.
HiperAccess	Up to 100 Mbps; typical at 25 Mbps	High Performance Radio Access (HiperAccess) is developed by ETSI BRAN to provide high speed broadband systems at high frequency bands, especially the band 40.5 GHz to 43.5 GHz.
HiperMAN		High Performance Radio Metropolitan Area Network (HiperMAN) is developed by ETSI BRAN for broadband fixed wireless access systems operating in the range 2 GHz to 11 GHz. The standard is designed for Fixed Wireless Access and is harmonised with 802.16-2004
OpenAir	Pre802.11 protocol with bit rate of 0.8 and 1.6Mbps	OpenAir is the proprietary protocol from Proxim. All OpenAir products are based on Proxim's module

5 WiMAX 802.16 family of standards and WiMAX

5.1 The organization that is responsible for the 802.16 Family of Standards is IEEE (Institute of Electrical and Electronics Engineers).

The IEEE 802.16 Working Group on Broadband Wireless Access Standards is the Working Group that has been developing the IEEE 802.16 WirelessMAN® Standard for Wireless Metropolitan Area Networks. This Working Group has been active since 1999 until today. Some of (the main) standards that have been produced by the Working Group are as follows:

IEEE Standard	Amendment	Released / Published	Status
802.16-2001	IEEE Standard for Local and metropolitan area networks — Part 16: Air Interface for Fixed Broadband Wireless Access Systems	8 April 2002	Superceded
802.16a-2003	Amendment 2: Medium Access Control Modifications and Additional Physical Layer Specifications for 2-11 GHz	1 April 2003	Superceded
802.16c-2002	Amendment 1: Detailed System Profiles for 10–66 GHz	15 January 2003	Superceded
802.16.2-2001	Coexistence of Fixed Broadband Wireless Access Systems	10 September 2001	Superceded
P802.16d	Amendment 3: Detailed System Profiles for 2-11 GHz	10 August 2003 (Draft 3)	Terminated
802.16-2004	*Revision of 802.16-2001, 802.16c-2002 and 802.16a-2003*	*1 October 2004*	*Active*
802.16e-2005	*Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands*	*28 February 2006*	*Active*
802.16f-2005	Management Information Base	1 December 2005	Active
802.16g	Management Plane Procedures and Services		Draft under development
802.16h	Improved Coexistence Mechanisms for License-Exempt Operation		Pre-draft
802.16i	Mobile Management Information Base		Pre-draft
802.16j	Mobile Multihop Relay (MMR)		Pre-draft
802.16k	Media Access Control (MAC) Bridges - Bridging of 802.16		Draft under development

There are 2 most popular and important IEEE 802.16 standards;

- The IEEE 802.16-2004 standard that is used for Fixed WiMAX implementation.
- The IEEE 802.16e-2005 standard that is used for Mobile WiMAX implementation.

5.2 WiMAX

The Worldwide **I**nteroperability for Microwave Access (WiMAX) forum is an industry-led, non-profit corporation formed in April, 2001 to promote conformance and certify the interoperability of broadband wireless products compliant with the IEEE 802.16 -2004 and ETSI HiperMAN standards. The Forum's goal is to accelerate global deployments of and grow the market for standards-based, interoperable, broadband wireless access (BWA) solutions.

To ensure that equipment conforms to these open standards and is interoperable, the WiMAX Forum has established a certification program to promote the worldwide adoption of the technology.

WiMAX testing requirements are defined by system profiles and certification profiles. There are currently two system profiles, one for fixed WiMAX and one for mobile WiMAX. Fixed WiMAX currently supports five certification profiles, which define classes of products that interoperate with each other on the basis of spectrum band, channelization and duplexing mode. To date, five certification profiles have been defined in the 3.5 GHz band—where both Time Division Duplex (TDD) and Frequency Division Duplex (FDD) can be used—and the 5.8 GHz TDD band. New certification profiles may be added in response to demand from vendors and operators.

As of May 2006, equipment is certified under Release 1, which focuses exclusively on testing for mandatory features. Release 2 will include three optional modules: QoS (Quality of Service) for improved support for real-time applications, AES (Advanced Encryption Standard) for advanced security and ARQ (Automatic Repeat reQuest) for improved link budget.

6 Availability of WiMAX equipment

WiMAX equipment can generally be categorized into two types, namely, those based on the standard 802.16-2004 (Revision D) and the other which are based on 802.16e-2005 (Revision E).

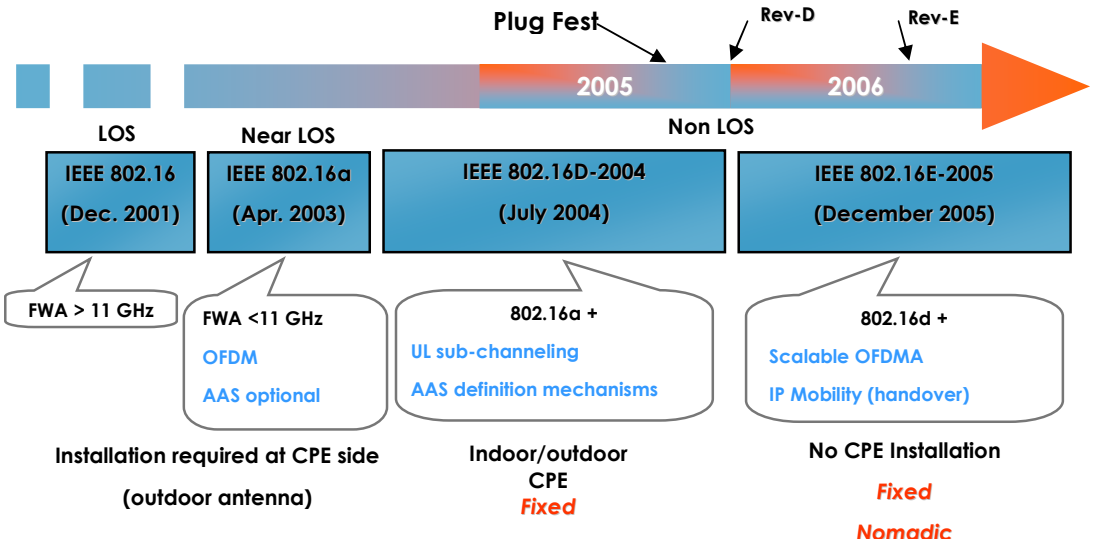
The ratification of the "D" version of WiMAX standards was reached in July 2004 while "E" achieved ratification in December 2005. This provides an indication of the availability of the WiMAX equipment. 802.16-2004 type equipment started appearing in the market as early back as Q3'2004. On the other hand, first available equipment for 802.16e-2005 is starting to appear now (Q3'2006).

However, if we look into specifics, then the actual availability also depends on several other factors, for instance:

- frequency band to be used (2.3GHz, 2.5GHz, 3.3GHz, 3.5GHz, 3.6GHz, etc)
- required type of application – fixed, nomadic or mobile
- channel bandwidth requirements
- etc.

Another aspect to consider with regards to equipment availability would be the contribution of the certification process by the WiMAX Forum. Based on the WiMAX Forum certification program which is handled by the Certification Working Group (CWG), certified 802.16-2004 equipment has been achieved only starting from beginning 2006. For 802.16e-2005, the current expectation is to have first certified equipment coming at the end of 2006 or in Q1'2007.

The diagram below summarizes the milestones of the WiMAX industry:



7 CPE (Subscriber Stations) – For fixed and mobile application

WiMAX will promote the adoption of new devices and applications that take advantage of its high-throughput, low latency and QoS functionality and the support for mobile access. Among the mobile devices expected to have a WiMAX interface are:

- Data centric devices: notebooks, PDAs, Ultra Mobile PCs
- CE devices: games consoles, MP3 players
- Voice and voice/data devices: cellular phones, smartphones
- Vertical applications devices: CCTV cameras, in-vehicle devices.

WiMAX is a broadband wireless technology that supports fixed, nomadic, portable and mobile access. To meet the requirements of different types of access, two versions of WiMAX have been defined. The first is based on IEEE 802.16-2004 and is optimized for fixed and nomadic access. The initial WiMAX Forum CERTIFIED products will be based on this version of WiMAX. The second version is designed to support portability and mobility, and will be based on the IEEE 802.16e-2005 amendment to the standard. Table 1 shows how WiMAX supports different types of access and their requirements.

Table 1. Types of access to a WiMAX network					
Definition	**Devices**	**Locations/ Speed**	**Handoffs**	**802.16-2004**	**802.16e**
Fixed access	Outdoor and indoor CPEs	Single/ Stationary	No	Yes	Yes
Nomadic access	Indoor CPEs, PCMCIA cards	Multiple/ Stationary	No	Yes	Yes
Portability	Laptop PCMCIA or mini cards	Multiple/ Walking speed	Hard handoffs	No	Yes
Simple mobility	Laptop PCMCIA or mini cards, PDAs or smartphones	Multiple/ Low vehicular speed	Hard handoffs	No	Yes
Full mobility	Laptop PCMCIA or mini cards, PDAs or smartphones	Multiple/ High vehicular speed	Soft handoffs	No	Yes

Source: WiMAX Forum

Fixed Application:
Initial WiMAX deployment will be fixed application, based on IEEE802.16-2004 standards, to complement DSL/cable modem to provide last mile for broadband access where broadband infrastructure is non existent or not cost effective to provide wired broadband infrastructure.

Typical configuration will be CPE's having outdoor antenna with the indoor unit, indoor CPE and PCMCIA cards connected to consumer device like PC.

Mobile Application:
The Mobile WiMAX, based on IEEE802.16e-2005 standards, would complement 3G services in providing high speed data centric services. The introduction of mobile devices with embedded WiMAX Systems-On-Chips (SOCs), such as notebooks, the Ultra Mobile PC (UMPC), PDAs, phones, smartphones and other wireless devices are expected to follow in 2008.

8 Conclusion and Recommendations

Current open standards for Metropolitan Area Networks are the IEEE 802.16 and HiperMAN. The two standards are harmonised and can support multimedia services.The open-standards approach and the interoperability fostered by WiMAX certification will lead to more competition in the market and to economies of scale that will lower equipment prices. Operators will also benefit from greater flexibility and sourcing from multiple vendors.
It is recommended that WiMAX certification be included in a technical standard that may be used in the type approval of WiMAX equipment. This technical standard will provide for:

- interoperability of WiMAX equipment ;
- compliance with minimum public safety standards;
- compliance with minimum radio performance levels for broadband wireless access;
- compliance with regulatory requirements in the relevant Standard Radio System Plans

9 Scope of Technical Standard

This technical standard is intended for the type approval of WiMAX equipment and it applies to wireless broadband access (BWA) equipment operating on radio frequencies identified by MCMC for BWA in the frequency bands 2 300 MHz to 2 400 MHz; 2 504 MHz to 2 688 MHz; and 3 400 MHz to 3 600 MHz

The types of equipment covered by this technical standard are as follows:

- base stations
- fixed internal and external subscriber stations
- nomadic, mobile subscriber stations:

The equipment may be used to provide broadband wireless communications in point-to-point or point-to-multipoint radio links

10 Normative references

SRSP 507a, Requirements for Fixed Wireless Access (FWA) systems operating in the frequency band from 3 400 MHz to 3 600 MHz.

SRSP 523, Requirements for Broadband Wireless Access (BWA) systems operating in the frequency band from 2 504 MHz to 2 688 MHz

SRSP 532, Requirements for Broadband Wireless Access (BWA) systems operating in the frequency band from 2 300 MHz to 2 400 MHz

IEC CISPR 22:2003-04 “Information Technology Equipment – Radio disturbance characteristics – Limits and methods of measurement;

IEC 60950-1: 2001-10 “Information Technology Equipment - Safety”

IEEE Std. 802.16- 2004 “IEEE Standard for Local and Metropolitan Networks Part 16: Air Interface for Fixed Broadband Wireless Systems”

IEEE Std. 802.16e-2005 “Air Interface for Fixed and Mobile Broadband Wireless Access Systems”

ETSI EN 301 489-1 V1.6.1 (2005-09) “Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements”

ETSI TS 102 210 V1.2.1 (2005-01) “Broadband Radio Access Networks (BRAN); HIPERMAN; System profiles”

ETSI 302 326-2v1.1.1 “Fixed Radio Systems; Multipoint Equipment and Antennas; Part 2: Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive for Digital Multipoint Radio Equipment”

FCC Part 27, §27.53 Emission Limits (for BRS)

Restriction on the use of certain Hazardous Substances (RoHS):Directive 2002/95/EC

Directive on Waste of Electrical and Electronic Equipment (WEEE):Directive 2002/96/EC

11. Abbreviations

BWA	Broadband Wireless Access
BRS	Broadband Radio Service, the service name used by FCC to rename Multipoint Distribution Service (MDS) / Multichannel Multipoint Distribution Service (MMDS) in the band 2 495 MHz to 2 690 MHz
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FDD	Frequency Division Duplex
HiperMAN	High Performance Radio Metropolitan Area
SRSP	Standard Radio System Plan (SRSP) - Documentation that is part of the Spectrum Plan that provides information on the efficient use of spectrum by radio systems operation in specific frequency bands
TDD	Time Division Duplex

12. Requirements

12.1 Frequency

The BWA equipment shall be tuned to operate within the frequency bands specified by the following SRSP documents:

SRSP 507a : 3 400 MHz to 3 600 MHz
SRSP 523 : 2 504 MHz to 2 688 MHz
SRSP 532 : 2 300 MHz to 2 400 MHz

12.2 Transmitted Power

The transmitted power of BWA equipment shall comply with the maximum output power specified in the SRSP applicable to the corresponding frequency band.

12.3 Emission Limit

The BWA equipment shall, in relations to emission limits, comply with the relevant sub-parts of FCC Rules or the ETSI HiperMAN standards given below:

a) 2 504 MHz to 2 688 MHz; 2 300 MHz to 2 400 MHz

(i) FCC Rule Part 27, § 27.53 Emission limits (for BRS)

The power of any emissions outside the licensee's frequency bands of operation shall be attenuated below the transmitter power (P) measured in watts by not less than 43 + 10 log(P) dB or;

(ii) The relevant PHY profile given in ETSI TS 102 210

The spurious emissions shall not exceed – 57 dBm in the frequency range 30 MHz to 1 GHz (measurement bandwidth: 100 kHz) and – 50 dBm in the frequency range GHz to 26.5 GHz (measurement bandwidth: 1 MHz).

b) 3 400 MHz to 3 600 MHz

(i) ETSI EN 302 326-2 or;

(ii) The relevant PHY profile given in ETSI TS 102 210

The spurious emissions shall not exceed – 57 dBm in the frequency range 30 MHz to 1 GHz (measurement bandwidth: 100 kHz) and – 50 dBm in the frequency range 1 GHz to 26.5 GHz (measurement bandwidth: 1 MHz).

12.4 Electromagnetic Compatibility (EMC)

EMC emission from the BWA equipment shall comply with the following:

a) ETSI EN 301 489-1 or;

b) IEC CISPR 22 : 2003-4

12.5 Electrical Safety

The BWA equipment shall comply with the safety requirements defined in IEC 60950-1 safety standard.

12.6 Environmental Requirement (RoHS Directive, WEEE and ECMA)

The restriction on the use of hazardous substances in BWA equipment shall comply with:

Restriction on the use of certain Hazardous Substances (RoHS):Directive 2002/95/EC

Directive on Waste of Electrical and Electronic Equipment (WEEE):Directive 2002/96/EC

12.7 Interoperability Compliance

The BWA equipment shall be compliant to the 802.16-2004/HiperMAN or 802.16e-2005. Specifications selected by the WiMAX Forum. Proof of compliancy will be in the form of documentary evidence of certification issued by, Centro de Tecnologia de las Comunicaciones S.A., (CETECOM) or any other certification bodies conformance assessment bodies sanctioned by the WiMAX Forum.

ANNEX A
(Informative)

Recommended requirement for BWA equipment

A1. Interfaces for BWA equipment

The Base Station Equipment for the following interfacing purposes should support, but not limited to, the corresponding interface standards:-

Purpose	Input/Output	Connection Type
Network Element Management	IN/OUT	RJ45, Gigabit or 10/100 Base-T Ethernet LAN
Local Area Network	IN/OUT	RJ45, Gigabit or 10/100 Base-T Ethernet LAN
Antenna	IN/OUT	Coaxial antenna connectors
External Devices/ Alarms	IN	Data Network Communication (DCN) based on IP, USB, RS232,RJ45 or 10/100 Base-T Ethernet LAN

A2. CPE Interface

The CPE should support, but not limited to, the following interface standards:

Purpose	Input/Output	Connection Type
Local Area Network	IN/OUT	RJ45 or 10/100 BaseT Ethernet LAN
VOIP	IN/OUT	RJ11, USB, 802.11 b/g
Wireless LAN	IN/OUT	802.11 b/g
External Device/ Alarms	IN	Data Network Communication (DCN) based on IP, USB, RS 232, RJ45 or 10 BaseT Ethernet LAN, 802.11 b/g
PC Connectivity	IN/OUT	Embedded, USB, PCMCIA, USB, 802.11 b/g

A3. Operating Temperature Range and Humidity of Outdoor Base Station Equipment

By means of a convectional cooling the temperature range shall be supported by the outdoor Base Station.

Equipment should be able to operate up to +55 ℃ or higher.

The equipment should be able to operate at relative humidity level of up to 95% or higher.

A4. Acoustic noise and ultrasonic

The emitted sound power level should not exceed 30 dBA without fan and 54 dBA with fan in one-meter distance (sound power measured according to ISO 3743).

A5. Environmental protection for outdoor BWA equipment

The BWA equipment for outdoor installation should meet the environmental protection level IEC 529 IP55 (with cover for connectors and sun protection) as described in IEC 529 "Classification of degrees of protection provided by enclosures".

ANNEX B
(Informative)

Service / Applications

B1. Service

IEEE 802.16-2004 specification (and beyond) supports well-defined robust quality of service.

WiMAX - compliant products shall be vendor interoperable. Different class of scheduling should be provided to support different requirements of user applications. Four classes of scheduling shall be supported as per IEEE 802.16-2004 specification.

Table B1. WiMAX Class of Services

Class	Traffic Type	User Application
Unsolicited Grant Service (UGS)	Real time fixed-size data at periodic intervals.	T1/E1, VoIP without silence suppression
Real-time Polling Service (rtPS)	Real time variable-sized data at periodic intervals	MPEG video
Non real-time Polling Service (nrtPS)	Delay tolerant and variable-sized data	FTP
Best Effort (BE)	Best effort. No minimum service level.	Email

Table B1 show the mapping of class of service and user application. Each type of user application will generate certain type of traffic. Each traffic type should utilize the appropriate class of scheduling to achieve the desired quality of service.

In addition, the class of services allow operator to tailor service levels to meet customer requirements. For example, “Unsolicited Grant Service” can guarantee high bandwidth and low latency to support real-time traffic for enterprise customers.

B2. Applications

The applications offered by the IEEE 801.16-2004 specification include fixed, nomadic and mobile services.

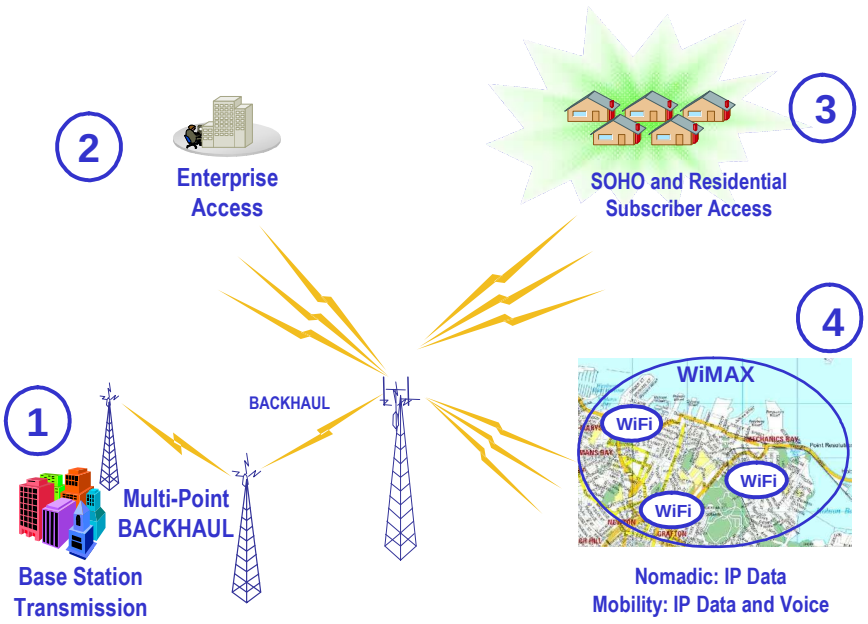


Figure B1. WiMAX Applications

As shown in Figure B1, they are:

1 Backhaul: point-to-point or point-to-multi-points. It may serve as rapidly deployable backhaul solution from base stations to switch facility.

2 A wireless alternative to leased line (T1/E1 equivalent) access for enterprise subscribers.

3 A wireless alternative to DSL or other similar broadband access for SOHO and residential subscribers.

4 Hot Zones: similar to the Hot Spots, but much wider coverage.

The standard of IEEE 801.16-2004 will offer mobility function, which allows subscribers being able to get access anywhere. Subscribers shall be able to roam from one area to another area. For example, a subscriber in a hot zone will be able to move to another hot zone without re-establishing connection session.

ANNEX C
(Informative)

Deployment

C1. Objectives

This document wishes to address WIMAX deployment issues and concerns. The areas under review include the access elements, stages of preparations, options for deployment and concerns arising from said deployment scenarios.

The document also attempts to take into account perspectives from the service operators, the SMEs, the vendors and the end-user themselves.

Note that the deployment scenarios do not touch on integration issues with billing and charging mechanisms and inter-service roaming (WIMAX to WiFi/GSM/WCDMA/etc).

C2. Access Elements

The elements would be differentiated as follows: Customer Premises Equipment (CPE), Radio Access Network (RAN) and IP core network. The diagram shown below highlights the key sections.

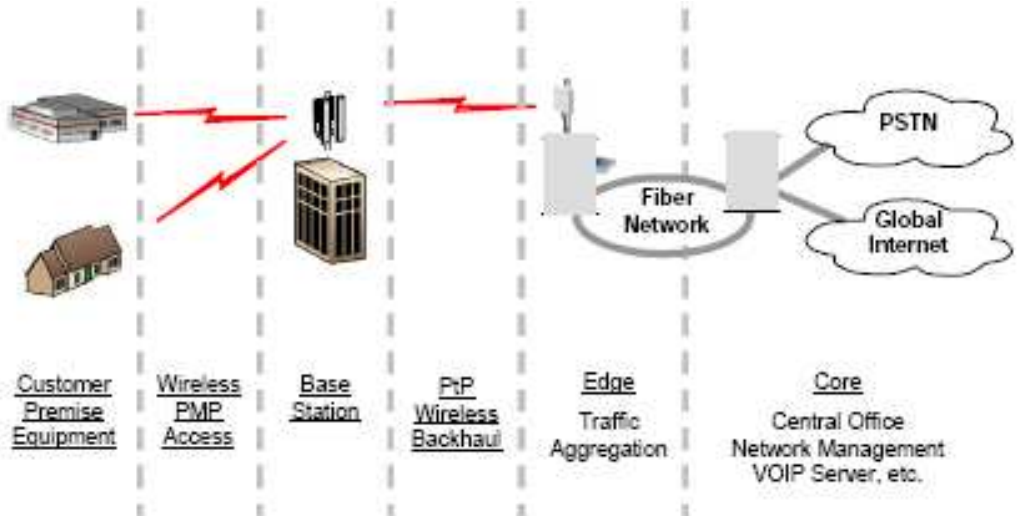


Figure C1. End to end network architecture to support WIMAX
(courtesy WIMAX Forum whitepaper, Oct 10 2004)

The following table shows the variants of possible WiMAX devices, their usage and which standards are relevant.

Definition	Devices	Locations/ Speed	Handoffs	802.16-2004	802.16e
Fixed access	Outdoor and indoor CPEs	Single/ Stationary	No	Yes	Yes
Nomadic access	Indoor CPEs, PCMCIA cards	Multiple/ Stationary	No	Yes	Yes
Portability	Laptop PCMCIA or mini cards	Multiple/ Walking speed	Hard handoffs	No	Yes
Simple mobility	Laptop PCMCIA or mini cards, PDAs or smartphones	Multiple/ Low vehicular speed	Hard handoffs	No	Yes
Full mobility	Laptop PCMCIA or mini cards, PDAs or smartphones	Multiple/ High vehicular speed	Soft handoffs	No	Yes

Table C1: Variants of WiMAX access into the network.
(courtesy: "Fixed, nomadic, portable and mobile applications for 802.16-2004 and 802.16e-2005 WiMAX networks.", Senza Fili Consulting, November 2005)

C3. Customer Premises Equipment (CPE)

The CPE may take on the form of a fixed outdoor transceiver unit connected to an indoor hub, allowing connectivity to the end-user's home computer network. Or it could take on the form of a nomadic indoor on-table transceiver, PCMCIA , Handset or Laptop computer where it is embedded in the form of a chipset.

The initial WIMAX rollout however may likely be based on the 802.16d or 802.16-2004 standards specification, whereby nomadic movement is possible within the cell coverage area. This particular CPE type follows the set-top box concept as provided by satellite broadcasting companies.

Continued development by the chip suppliers and CPE manufacturers should shift the CPE form-factor from a relatively large outdoor/indoor unit to an integrated indoor version. Further evolution would generate integrated WIMAX chipsets directly into laptops and onwards into mobile devices and handsets based on 802.16e-2005 standards with mobility as a key feature. The diagram below highlights the roadmap timelines for each category of devices made available for commercial deployment.

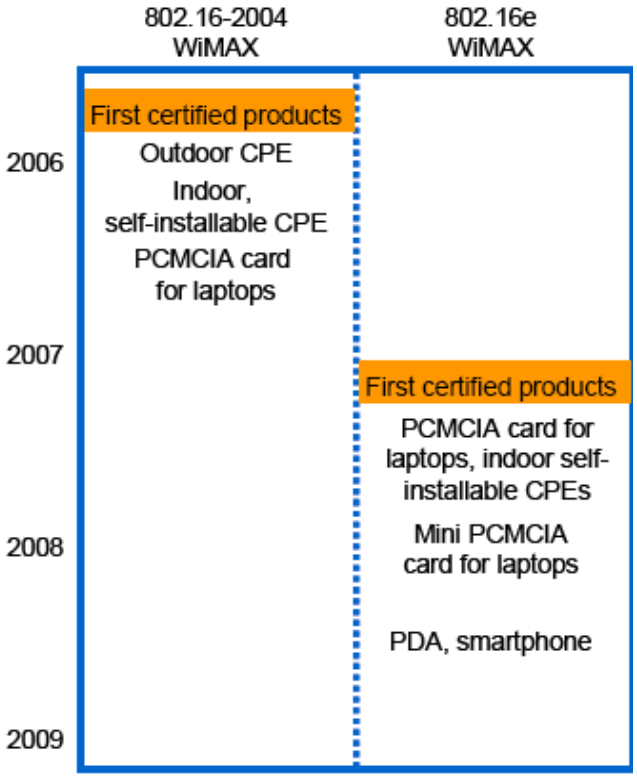


Figure C2. Expected commercial availability WiMAX user device equipment.
(courtesy: "Fixed, nomadic, portable and mobile applications for 802.16-2004 and 802.16e-2005 WiMAX networks.", Senza Fili Consulting, November 2005)

C4. Radio Access Network (RAN)

The RAN portion encompasses the Wireless PMP (Point to Multi Point) Access, the base station and the PtP (Point to Point) Wireless Backhaul segment. PMP access would depend on what types of antennae are used – omni versus sectorized versions. This affects footprint size, coverage design and on-air capacity management. The locations of the base stations would most probably be co-located on existing GSM/WCDMA sites (if deployed by service operators) in order to reduce capital expenditure costs. However, there may be instances where dedicated WIMAX sites are preferable in order to meet the service and RF demands. In the case of the PtP wireless backhaul segment, many options are currently available – microwave solutions, fixed wireless access (FWA) solutions, or even utilizing WIMAX as a backhaul medium. Optimal selection of backhaul depends on the deployment strategy of the service operators.

C5 IP Core Network

The IP core network may start from the edge/border routers bringing the traffic back into the core network via legacy ATM/SDH infrastructure. The traffic is then routed onwards to the destination, depending on application (e.g. Internet for web browsing, or to PSTN for VoIP calls terminating to a POTS phone).

C6 Deployment possibilities

It has been generally accepted that the initial WIMAX deployment would be in a fixed-CPE environment (ala wireless DSL modem). This would then evolve towards a fully mobile solution, where the chipsets are embedded into laptops and mobile devices such as PDAs and smartphones. The following diagram illustrates the various scenarios.

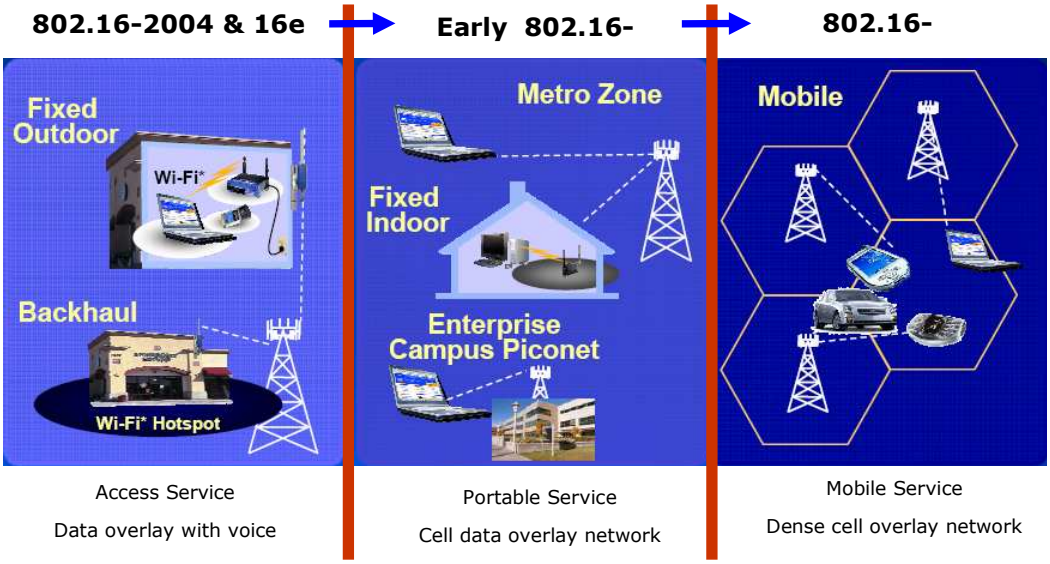


Figure C3. WIMAX Deployment Possibilities
(courtesy: Intel Mobility Group, Pan-Asian Wireless Broadband Summit 2005, Hong Kong)

C7. Preparation Stages

C7.1 Readiness of CPE/SoC (System on Chip)

It will not be feasible to roll-out new technologies if the end-user does not have the device to access the service. Thus, readiness and delivery of the CPE or System on Chip (SoC) is a crucial factor when considering WIMAX deployments. It is worth noting that the chipsets would evolve from the initial outdoor/indoor units to integrated SoCs, implying a major cost reduction through economies of scale.

The market should see commercial trials appearing as early as Q1 2006 with the following timeline being indicative of activities to come for equipment based on 802.16-2004.

- 802.16-2004 standard complete — Done
- Technology/Silicon samples — Done
- Systems Interoperability tests — Q2 '05
- Lab trials — Q4 '05
- Commercial trials — Q1 '06

C7.2 Readiness of core network

As WIMAX is an access technology, getting the data to and from the end-user will still rely on a service provider's IP core network. Smooth integration of the WIMAX base stations into the edge/border routers would be a key factor in ensuring quick deployment and minimal downtime on the relevant network elements.

Most service providers with IP core networks already have legacy billing and report generation systems in place. As data is still delivered via IP packets, it is a straightforward move to implement volume- or time-based policies. To address quality of service (QoS) concerns, the service providers may utilize traffic profiling mechanisms or rely on technologies like MPLS (Multi Protocol Label Switching).

C7.3 Readiness of localized standards

According to the WIMAX Forum, it is forecasted that 85% of deployments would be on the licensed spectrum, and the remainder on the unlicensed spectrum. The licensed bands would include the 2.3GHz, 2.5GHz and 3.5GHz spectrum, whereas the unlicensed band would be the 5.8GHz band.

C8. Options for Deployment

There are various ways to roll out the WIMAX technology, and the following are some suggestions:

C8.1 Designated Footprint Model

This scenario allows WIMAX operators to safely deploy WIMAX within a stipulated 'grid', for instance, a 10km x 10km area of coverage. This ensures that the users are aware of which service provider is rolling out the service, roll-outs can be concentrated within specific 'hotspots' and the broadband penetration rate increased by a significant factor.

C8.2 Zoning Model

Similar to the designated footprint model, this model has boundaries that are less stringent. Locations could be selected universities, hospitals, ports and free trade zones (FTZ). One could think of this scenario as a "hotspot" deployment.

C9. Issues and Concerns

As with any new access technology, concerns and issues will be raised and debated. The following are some examples of what might be key issues:

C9.1 How does the business model work?

The advantages proposed by the WiMAX technology (widespread coverage, non LOS operation, well defined device roadmap, higher throughput per user) would have to be tempered by considering what service providers are currently deploying. Data services like ADSL and WiFi and most recently, 3G, have their own CPE designs which tie up an operator's capex. Obtaining an integrated CPE which can access across multiple bearers (802.11, WCDMA, 802.16x) will drive up manufacturing costs, which customers should not absorb.

There are also existing access technologies like microwave SDH/PDH and Fixed Wireless Access (FWA) solutions being used within the access infrastructure. Operations and Engineering teams will have to study the feasibility of using WiMAX as a backhaul alternative, or simply as another access technology. By default, the use of the licensed spectrum for WiMAX incurs extra capex cost, on top of other spectrum fees already budgeted for.

The targeted market segment – residential versus enterprise customers – would drive the need for correct service expectations. Lower tolerance for packet-delay and security problems may be the key to the enterprise segment buying in to the WiMAX technology. Integrated WiMAX chipsets on cheap desktop PCs and laptops may be the key selling feature for the mass market.

C9.2 Inter-operator and inter-technology roaming

As the footprint of a WiMAX base station is larger than a GSM/WCDMA cell or a WiFi hotspot, it is envisioned that the end-users may still roam but within the coverage area. However, service providers would then need to figure out how to integrate a WiMAX roaming service onto existing inter-technology solutions (WiFi to GSM/WCDMA, for instance). The following are some varieties of roaming possibilities that providers may consider:

- Inter-technology roaming – the customer can roam amongst various bearers provided by an operator (e.g. WiFi to GSM/WCDMA to WiMAX on Operator A)

- Inter-operator roaming (similar bearer) – the customer can roam across different service operators while still using the same WiMAX bearer technology (e.g. WiMAX on Operator A, then roam onto WIMAX on Operator B), and

- Inter-operator roaming (multi-bearer) – a smorgasbord of access choices for the customer, where he or she can roam across operators and on various bearer technologies (e.g. WiMAX on Operator A, then roam onto WCDMA on Operator B).

The above features are part of the 802.16e-2005 which features full mobility for all WiMAX-compliant networks and devices.

APPENDIX D
(Informative)

Security (information on air interface security and network login security)

Unlike WLAN, WiMAX provides a media access control (MAC) layer that uses a grant request mechanism to authorize the exchange of data. This feature allows better exploitation of the radio resource, in particular with smart antennas and in dependent management of the traffic of every user. This simplifies the support of real-time and voice applications.

One of the inhibitors to widespread deployment of WLAN was the poor security feature of the first release. WiMAX proposes the full range of security features to ensure a secured data exchange process:

- Terminal authentication by exchanging certificates to prevent rogue devices
- User authentication using Extensible Authentication Protocol (EAP)
- Data encryption using the data encryption standard (DES) or advanced encryption standard (AES), both much more robust than the Wireless Equivalent Privacy (WEP) initially used by WLAN. Furthermore, each service is encrypted with its own security association and private keys.

D1. Network

D.1.1 Security architecture

Security is implemented as a privacy sublayer at the bottom of the MAC protocol layer. The goal is to provide subscribers with privacy, authentication or confidentiality across the broadband wireless network, while attempting to protect operators from theft of service.

The security feature comprises two component protocols as follows:

- An encapsulation protocol for encrypting data across the broadband network.
- A key management protocol to provide secure distribution of keying data from the BS to the SS

D1.2 Encapsulation protocol for encrypting packet data across BWA network.

  – Defines a set of cryptographic suites, pairing of data encryption and authentication algorithms and the rules for applying those algorithms to MAC PDU payload

D1.3 Encapsulating is always applied on the MAC PDU payload of the IEEE 802.16-2004 standard while the IEEE 802.16e-2005 states that encryption is applied to the MAC PDU payload when required by the selected chipersuite.

Figure below illustrate the layers

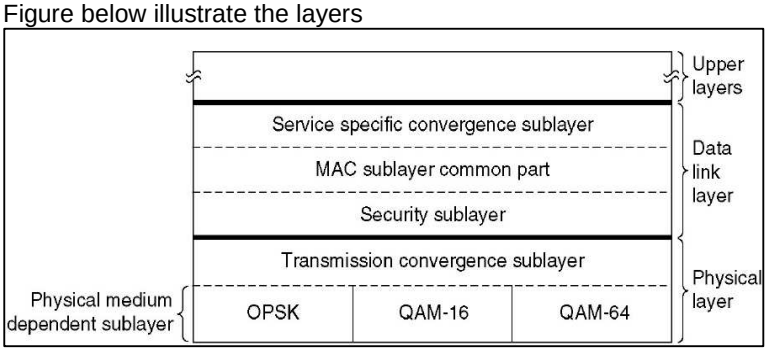


Figure D1. Security architecture

D2. Security associations

D2.1 A Security Association is the set of security information a BS and one or more of its client SSs share in order to support secure communications across the IEEE Std 802.16 network. 802.16 uses two SA types but explicitly defines only the data SA, which protects transport connections between one or more SS (subscriber station) and a BS (base station)

D2.2 The standard defines 3 types of SA (primary, static, dynamic)

- Primary SA is established during link initialization
- Static/Dynamic SA is established for transport connections
  - Either one SA is established for both uplink and downlink or one SA for each direction
  - Multicast groups also require SAs to be shared

D2.3 SAs are identified using SAID

D2.4 In PMKv2 (supported with IEEE 802.16e-2005), SAs are further defined as SAs for unicast connections, GSA (Group Security Associations) for multicast groups and MBSGSA (Multicast and Broadcast Group Security Association) for MBS services.

D2.5 Authorization SA: Using Key management protocol (PKM), the SS request BS for SA keying material.

- BS ensure that each SS has access only to SA its authorized.

D3. Key Management

D3.1 The Key Management Protocol (Privacy Key Management) allows for unilateral authentication with the IEEE 802.16-2004 standard (PKMv1) while providing both mutual and unilateral authentication with the IEEE 802.16e-2005 standard (PKMv2).

D3.2 The protocol provides the secure distribution of keying data from BS to SS. This is achieved by EAP (supported in IEEE 802.16e-2005) or X.509 digital certificates with RSA public-key encryption algorithm or a sequence starting with RSA authentication followed by EAP authentication (this sequence is supported with IEEE 802.16e-2005, PKMv2).

D3.3 In addition BS uses the protocol to enforce conditional access to network services (Protect from theft of service and cloned SS).

D3.4 PKM uses PKI crypto to establish a shared secret, referred to as Authorization Key (AK), between BS and SS. The AK is used to secure subsequent PKM exchanges of traffic encryption keys (TEK).

D3.5 PKM uses X.509 digital certification (in the case of RSA authentication) or operator-specified credentials (in the case of EAP authentication) to identify communication parties

- RSA Authentication: This protocol uses the X.509 digital certificates and RSA public-key encryption for authentication. The digital certificate contains the SSs Public Key, MAC address (identity). All SS have factory-installed RSA private/public key pair, or and internal algorithm to generate such pairs, used for PKI
- EAP Authentication: This protocol is used in conjunction with an operator defined EAP method. Hence credentials are as per operators' preference. Example, in the case of EAP-TLS, X.509 digital certificates is used for authentication while a Subscriber Identity Module is used with EAP-SIM.

D3.6 Key assignment and AK derivation

- SS initiates authorization by sending Authentication Information (strictly informative only) to its BS. This is followed by an Authorization Request
- BS responds to the request with an Authorization Reply message, initiating the authorization SA between BS and SS.
- The PKMv2 (supported in IEEE 802.16e-2005) provides for two authentication schemes. The RSA based authorization yields a shared pre-Primary AK (pre-PAK) which is then used to generate the PAK. The EAP based authorization on the other hand yields a Master Session Key (MSK) form which the Pairwise Maste Key (PMK) is derived. The AK is derived from the PMK and or PAK. The protocol also supports RSA-EAP mode of authentication as well as dual EAP mode.
- The PKMv2 also supports a 3-way SA-TEK handshake to optimize re-authentication mechanisms for fast handovers as well sa to prevent any man-in-the-middle-attacks.
- Upon authorization, SS starts a separate TEK (Traffic Encryption Key) state machine for each SAID identified in Authorization Reply message for Point-to-multipoint operations. For Mesh mode operations, SS starts a separate TEK state machine for each SAID for each neighbour node.
- TEK is encrypted using appropriate Key encryption key (KEK) derived from AK

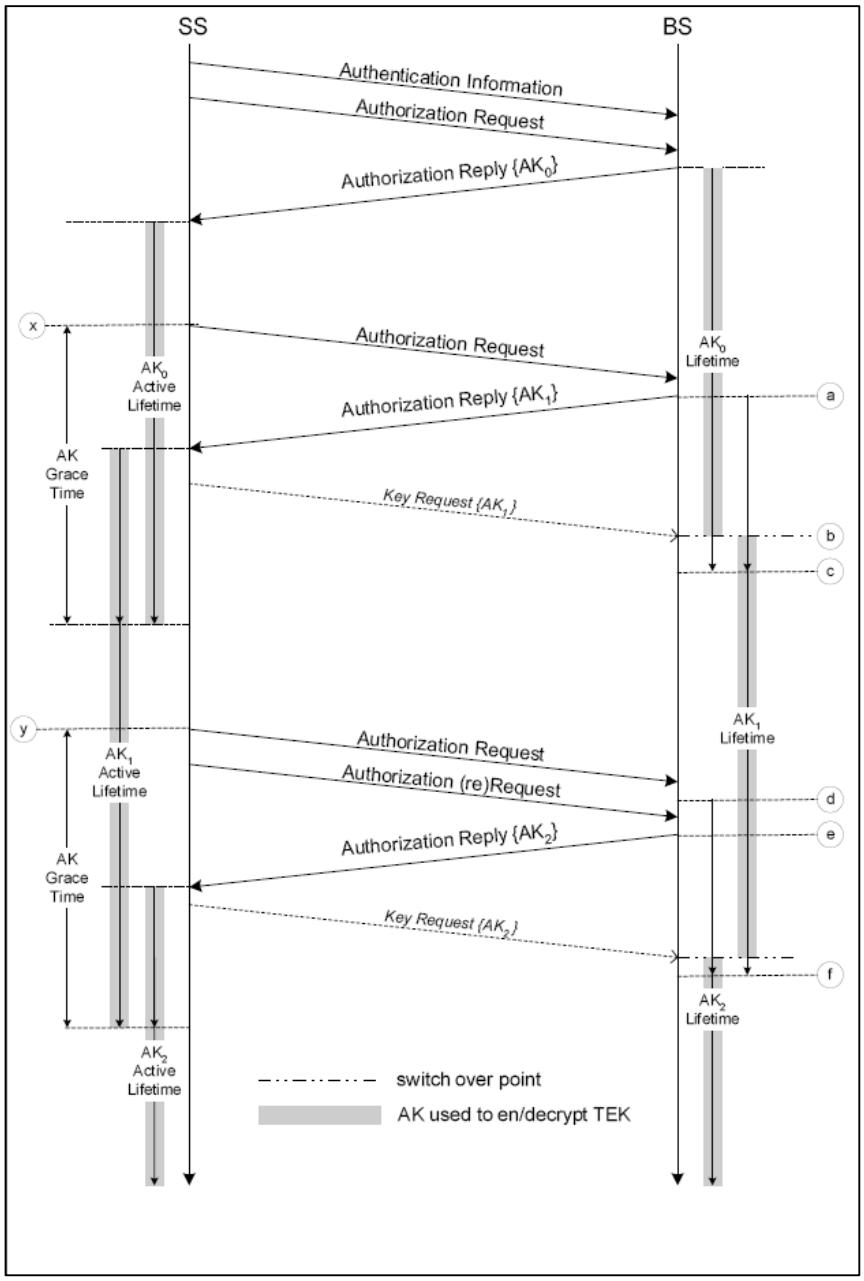


Figure D2. AK management in BS and SS

D4. Key Usage

- BS maintains two active TEK per SAID.
- Lifetimes of the TEK overlap.
- BS uses older of the two active TEKs for encrypting downlink traffic, and either one of TEKs to decrypt uplink traffic.
- SS uses the newer of its two TEKs to encrypt uplink traffic and either one of the TEKs to decrypt downlink traffic.

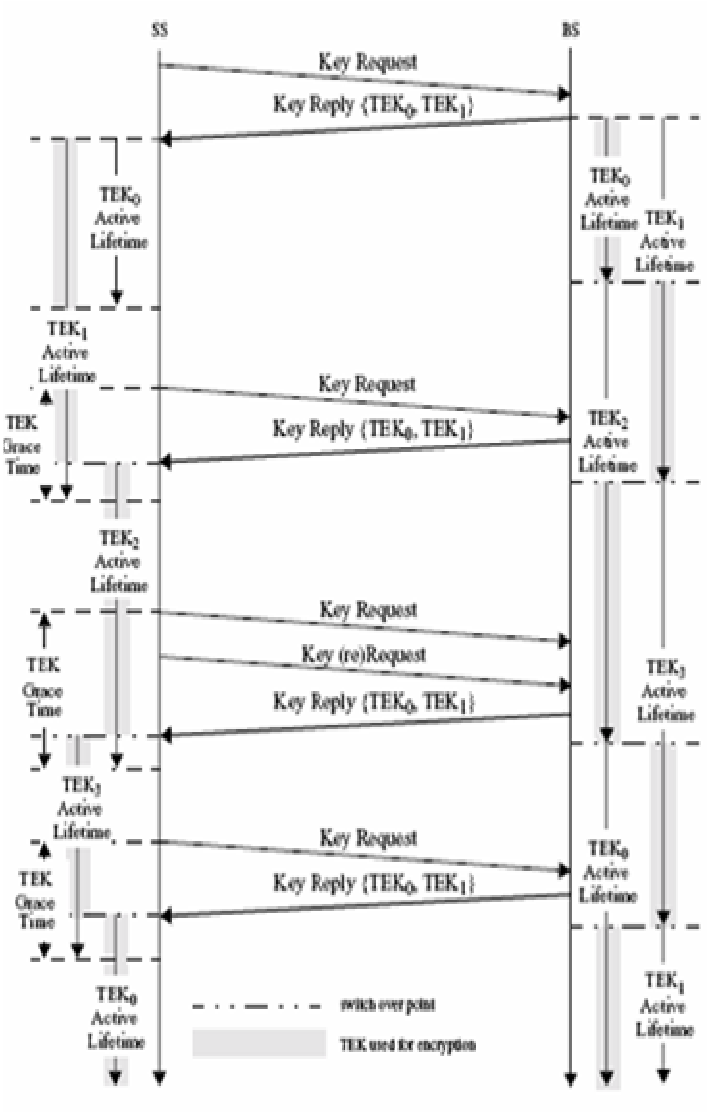


Figure D3.TEK management in BS and SS (IEEE 802.16e-2005)

D5. Data encryption

- Data encryption is based on two active shared secrets (TEK)
- Plaintext PDU payload is encrypted and authenticated using active TEK. Packet number is prepended and Ciphertext integrity check value (ICV) appended in the end.
- Different encryption algorithms can be used, of which the SA has information on the used suite
- The IEEE 802.16-2004 standard adopts DES-CBC encryption over the payload field
- IEEE 802.16e-2005 adopts AES-CCM as a new data cipher.
- In AES-CCM, the transmitter constructs a unique nonce as a per-packet encryption randomizer which guarantees uniqueness, which is done with the insertion of Packet Number (PN) into the Mac PDU.

- Extensible in the future with new crypto suites

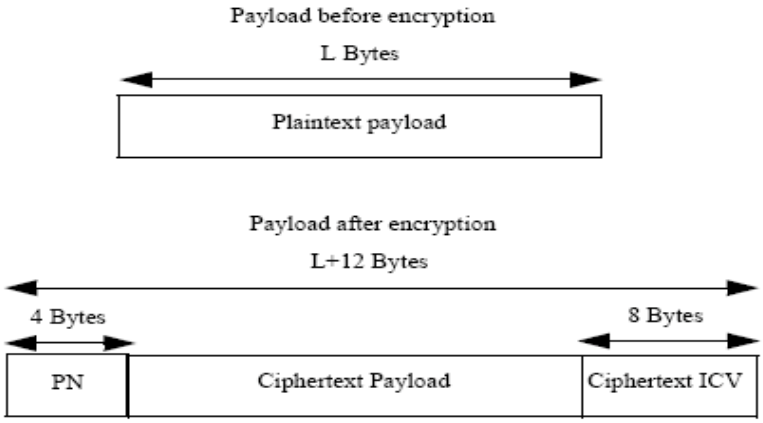


Figure D4. Payload structure with PN and ICV.

D6. Security threats and problems

Even though 802.16-2004 is designed to be secure, robust and flexible there are some considerations to be made:

- In the IEEE 802.16-2004 network, there is no mutual authentication, SS authenticates itself to BS, but BS does not authenticate itself to the SS. SS can't be protected from rogue BS and subjects itself to replay attacks. The IEEE 802.16e-2005 PKM features support both unilateral and mutual authentication which will provide an avenue to address rogue BS concerns.

- In IEEE 802.16-2004, BS contributes all bits to AK, where SS must trust that BS generates always fresh AKs, cryptographically separated from other AKs. Thus, there is a need for the BS random generator to be highly efficient and perfect. Recommendations for both parties to contribute nonce for AK generation have been raised to assure freshness AK.

- The PKMv1 protocol assumes that X.509 certificates are issued correctly. No parties with different public or private key pair are certified to use same MAC, otherwise masquerading is possible.

- The PKMv1 (IEEE 802.16-2004) protocol identifies each TEK with 2-bit sequence number, wrapping the number from 3 to 0 on every 4th key. This protocol is subject to replay attack. If replay succeeds then, TEK and subscriber data are exposed.

- Mesh operation mode and mobility add more complexity to key management, but this is addressed with 3-way SA-TEK handshake for handovers and prevention of man-in-the-middle-attacks in IEEE 802.16e-2005 PKMv2.

- In PKMv1, the SHA1 (Secure Hash Algorithm) algorithm is used in key derivation of HMAC. However SHA1 has known vulnerabilities. The IEEE 802.16e-2005 supports Cipher-based MAC as another means of management message integrity protection.

- Security design of the 802.16 does not protect the network from PHY layer attacks. Examples are like battery-draining frame generation and spectrum jamming. Some of these threats can be identified, for instance, a radio spectrum monitoring equipment will easily be able to detect jamming.

- War-drivers is another form of physical attack where they:

  - use your Internet bandwidth
  - advertise the availability of free Internet access to others

- Malicious hackers trying to steal or alter data inside network

- People launching attacks outside of your network from within your network (denial of service attacks)

D7. Summary of Security Solutions

In view of the security features of both the IEEE 802.16-2004 and the enhancements introduced with IEEE 802.16e-2005, the following are some other considerations/suggestions that can be introduced to improve the network security:

- Lock down network

- MAC address authentication

- Encryption: WEP/WPA/WPA2

- Monitoring

- Virtual Private Network (VPN)

APPENDIX E
(Informative)

Interconnect

The end-to-end interconnection from WiMAX CPEs to WiMAX infrastructure and other networks is simply illustrated in the following diagram;

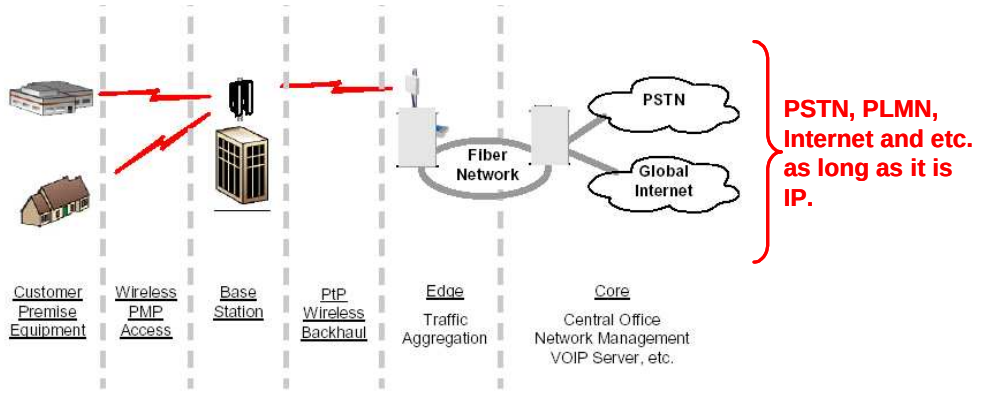


Figure E1. Interconnection of WiMAX systems and PSTN

The diagram shows that there is a plan to interconnect WiMAX systems to PSTN, internet and/or PLMN.

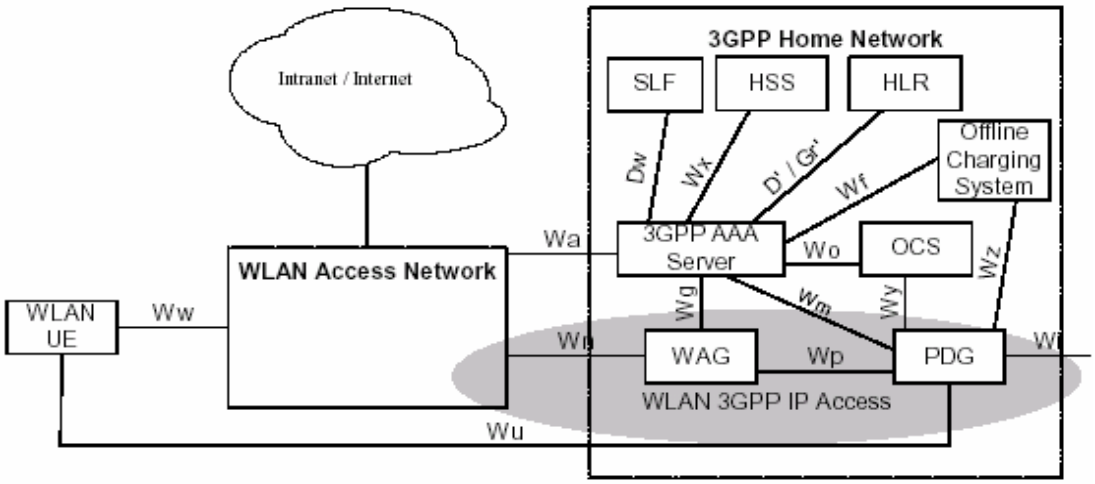
E1. WiMAX Interworking with PLMN

Our main references for the PLMN interconnection are the following technical specification from ETSI and 3GPP (3rd Generation Partnership Programme) documents;

ETSI TS 123 234 V6.4.0 (2005-03) “Universal Mobile Telecommunications System (UMTS); 3GPP system to Wireless Local Area Network (WLAN) interworking; System description (3GPP TS 23.234 version 6.4.0 Release 6)”.

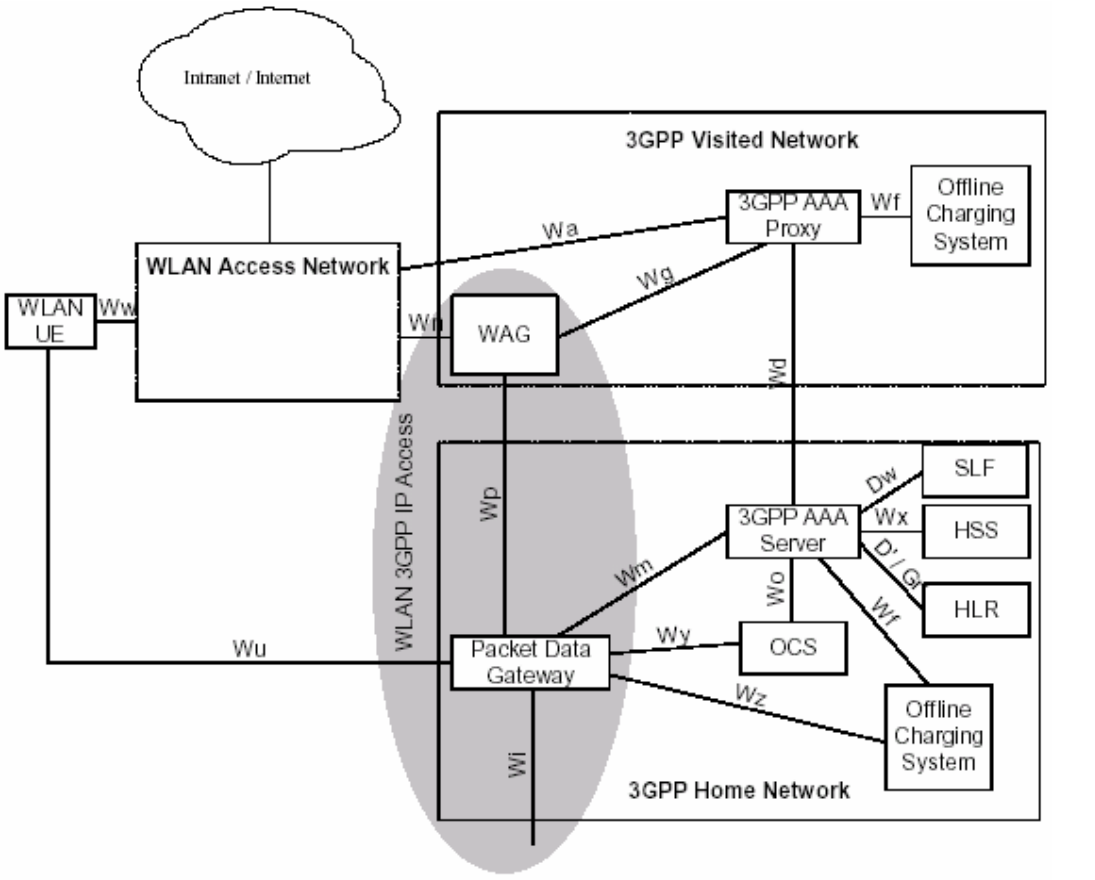
ETSI TS 122 234 V6.3.0 (2005-06) “Universal Mobile Telecommunications System (UMTS); Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking (3GPP TS 22.234 version 6.3.0 Release 6)”.

Figure E2 shown below is Non-Roaming Reference Model.



NOTE: The shaded area refers to WLAN 3GPP IP Access functionality.

Figure E2. Non-roaming Reference Model



NOTE: The shaded area refers to WLAN 3GPP IP Access functionality.

Figure E3. Roaming Reference Model

These ETSI documents describe the above diagrams in detailed for each of the interfaces and network elements. The following topics are also being discussed in these documents;

- Charging
- Roaming
- Numbering and addressing
- Service subscription

It is important to state here that these documents are applicable for both IEEE 802.11 system (Wi-Fi) and IEEE 802.16 system (WiMAX), even though these documents are referring the WLAN (wireless local area network) as an IEEE 802.11 network as 802.11 is a more mature system than 802.16 system. Additionally, a common PLMN network elements; namely WAG (WLAN IP access gateway) and PDG (packet data gateway) will be able to interconnect to either 802.11 systems or 802.16 systems or both systems at any time.

E2. WiMAX Network Reference Model (NRM).

Within WiMAX Forum, there is a working group called the Network Working Group (NWG). The purpose of the Network Working Group (NWG) is to create higher level networking specifications for fixed, nomadic, portable and mobile WiMAX systems, beyond what is defined in the scope of 802.16. The specific objective for the NWG is to deliver a reference architecture model and required specification(s) based on harmonized requirements from the Service Provider Working Group (SPWG) and profiles to be approved by the WiMAX Forum. (Source : WiMAX Forum)

The following diagram illustrates the Network Reference Model (NRM) specified by the NWG;

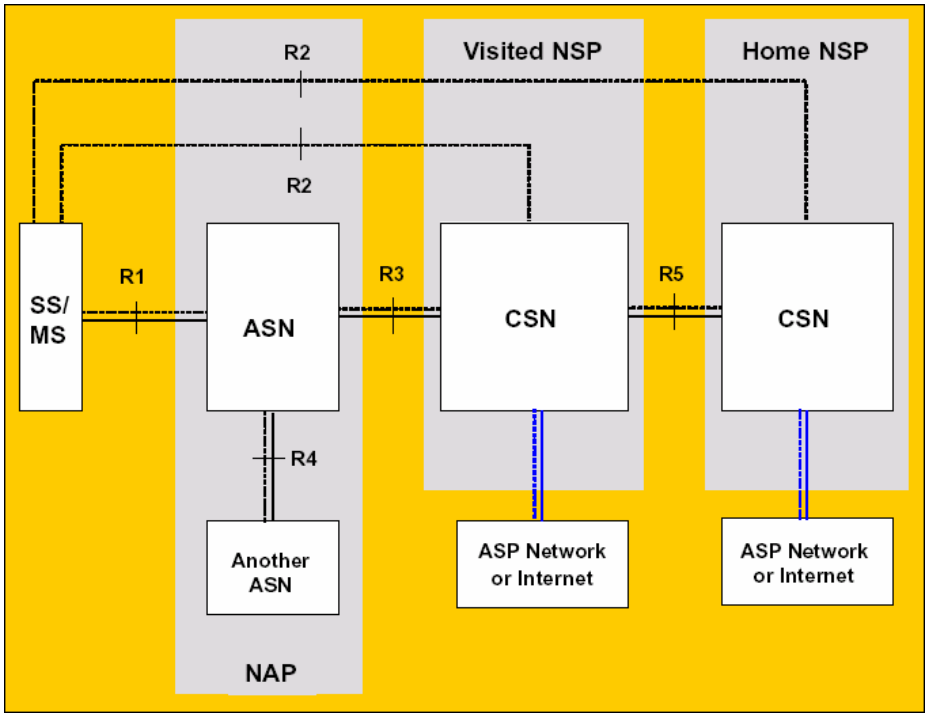


Figure E4. Network Reference Model (NRM)

The following diagram illustrates a more basic view of the many entities within the functional groupings of ASN and CSN.

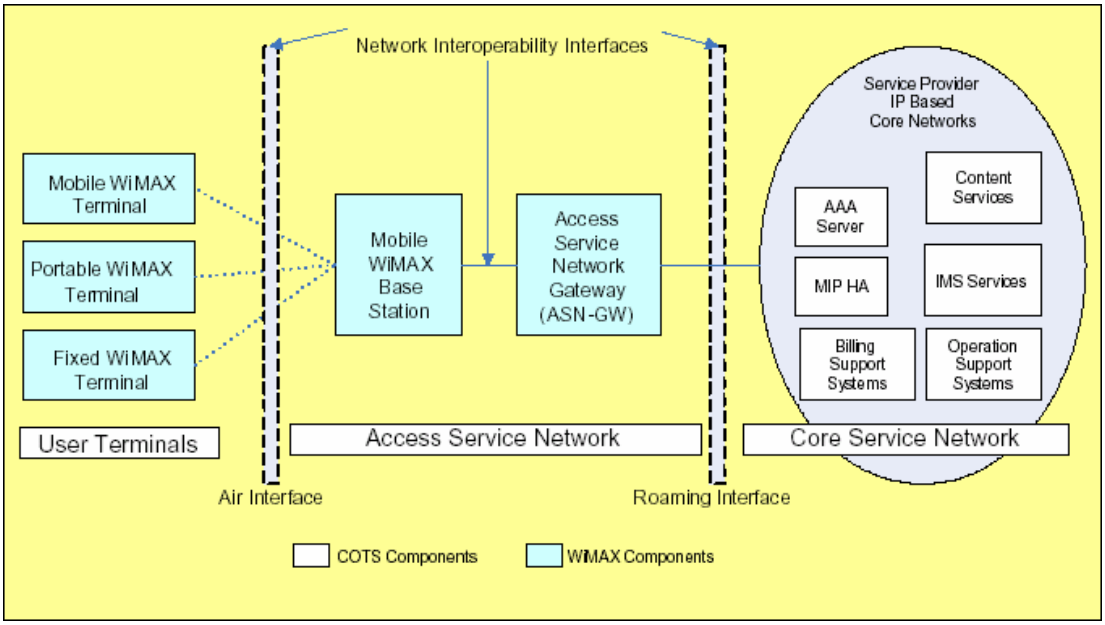


Figure E5. Basic view of the many entities within the functional groupings of ASN and CSN.

ACKNOWLEDGEMENTS

Encik Khoo Teng Lock (Chairman)	Motorola Technology Sdn Bhd
Encik Najib Fadil Bin Mohd Bisri (Secretary)	Telekom Malaysia Berhad
Encik Gijsson Chow	Alcatel Network Systems (M) Sdn. Bhd
Encik Pierre Cheyron	Alcatel Network Systems (M) Sdn. Bhd
Puan Pauline Goh	Alcatel Network Systems (M) Sdn. Bhd
Encik David Lim	Cambridge Broadband
Encik Ronhazli Adam	Celcom Berhad
Encik Kelvin Koo Jenn Mang	DiGi Telecommunications Sdn. Bhd
Encik Nor Azmi Jamaludin	DiGi Telecommunications Sdn. Bhd
Encik Steven Heah	DiGi Telecommunications Sdn. Bhd
Puan Moriani Mohamed	DiGi Telecommunications Sdn. Bhd
Encik Azmi Mokhtar	Ericsson (M) Sdn. Bhd
Encik Billy Lee	Huawei Technologies (M) Sdn. Bhd.
Encik Lim Chee Siong	Huawei Technologies (M) Sdn. Bhd.
Encik Tan Tze Loong	Intel Electronics (Malaysia) Sdn. Bhd.
Encik Ahmad Fakhri W. Shamsuddin	Jaring Bhd
Encik Amirul Ahmad	Malaysian Communications and Multimedia Commission (MCMC)
Encik Mohd Aris Bernawi	Malaysian Communications and Multimedia Commission (MCMC)
Encik Rizal Abd Malek	Malaysian Technical Standards Forum Bhd
Encik John Tay	Marconi (M) Sdn. Bhd
Encik Roberto Pastorino	Marconi (M) Sdn. Bhd
Cik Maslinda Rasli	Maxis Communications Berhad
Encik Anaz Shazlan	Maxis Communications Berhad
Puan Norehan Yahya	Maxis Communications Berhad
Puan Ong Wai Lee	Maxis Communications Berhad
Dr Tan Kay Ti	MiTV Corporation Sdn. Bhd
Encik Tengku Idham Tengku Ishak	MiTV Corporation Sdn. Bhd
Encik Sukhdev Singh	Palette Multimedia Bhd
Encik Pee, Wilson	Rohde & Schwartz Malaysia Sdn Bhd
Encik Danabalan	Siemens Malaysia Sdn. Bhd
Encik Kok Chee Choon, Don	Siemens Malaysia Sdn. Bhd
Encik Liew Chuw Yee	Siemens Malaysia Sdn. Bhd
Encik Tee Boon Tong	Siemens Malaysia Sdn. Bhd
Encik Azman Yunus	SMART Digital Communications Berhad
Puan Sukuna Krishnan	SMART Digital Communications Berhad
Cik Siti Noor Safina Azizan	Telekom Malaysia Berhad
Encik Zulkarnain Bin Hashim	Telekom Malaysia Berhad
Puan Rosilawati Ayub	Telekom Malaysia Berhad
Encik Azzemi Ariffin	Telekom Research & Development Sdn Bhd.
Encik Jaafar Haji Mohamad Abu Bakar	Telekom Research & Development Sdn Bhd.
Encik Cheah Cheng Lai	TIME dotCom Berhad
Encik Jasmi Mohd Daron	TIME dotCom Berhad
Puan Haslinda Mohd, Nazeri	TIME dotCom Berhad
Dr.Borhanuddin Mohd Ali	Universiti Putra Malaysia
Puan Nor Kamariah Nordin	Universiti Putra Malaysia

Encik Chew K.K.	Volans Technology Sdn Bhd
Encik Ng Yun Kwan	Volans Technology Sdn Bhd
Encik Prabaharan, Praba	ZTE Corporation Malaysia Sdn Bhd
Encik Wong, Dennis	ZTE Corporation Malaysia Sdn Bhd