ETSI TS 102 624-1 V1.2.1 (2009-11)

Technical Specification

**Broadband Radio Access Networks (BRAN);
HiperMAN;
Conformance Testing for the Network layer of
HiperMAN/WiMAX terminal devices;
Part 1: Protocol Implementation Conformance
Statement (PICS) proforma**

Reference

RTS/BRAN-004T010-1

Keywords

HiperMAN, layer 3, PICS, terminal, testing

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or
perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF).
In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive
within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

ETSI

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Broadband Radio Access Networks (BRAN).

The present document specifies the Protocol Implementation Conformance Statement (PICS) of the Network layer Release 1.5 for High Performance radio Metropolitan Area Network (HiperMAN) and WiMAX terminal devices.

The present document is part 1 of a multi-part deliverable covering HiperMAN; Conformance Testing for the Network Layer of HiperMAN/WiMAX terminal devices, as identified below:

    Part 1: **"Protocol Implementation Conformance Statement (PICS) proforma";**

    Part 2: "Test Suite Structure and Test Purposes (TSS&TP)";

    Part 3: "Abstract Test Suite (ATS)".

1 Scope

The present document specifies the Protocol Implementation Conformance Statement (PICS) proforma for WiMAX Network Layer Release 1.5 per ISO/IEC 9646-7 [23], ITU-T Recommendation X.296 [24] and EG 201 058 [i.4] for conformance of HiperMAN1.3.1/WiMAX compliant terminals.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:

  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;

  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] WiMAX Forum (Release 1.5): "WiMAX Forum Network Architecture, Stage 2: Architecture Tenets, Reference Model and Reference Points, Base Specification".

NOTE: Available at http://www.wimaxforum.org/resources/documents/technical/release

[2] WiMAX Forum (Release 1.5): "WiMAX Forum Network Architecture, Stage 3: Detailed Protocols and Procedures", Base Specification.

NOTE: Available at http://www.wimaxforum.org/resources/documents/technical/release

[3] IETF RFC 3484 (February 2003): "Default Address Selection for Internet Protocol version 6 (IPv6)".

[4] IETF RFS 5281 (August 2008): "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)".

[5] IETF RFC 2131 (March 1997): "Dynamic Host Configuration Protocol".

[6] IETF RFC 3748 (June 2004): "Extensible Authentication Protocol (EAP)".

[7] IETF RFC 4941 (September 2007): "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

[8] IETF RFC 2464 (December 1998): "Transmission of IPv6 Packets over Ethernet Networks".

[9] IETF RFC 2759 (January 2000): "Microsoft PPP CHAP Extensions, Version 2".

[10] IETF RFC 5216 (March 2008): "The EAP-TLS Authentication Protocol".

[11]   IETF RFC 3024 (January 2001): "Reverse Tunneling for Mobile IP, revised".

[12]   IETF RFC 3315 (July 2003): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[13]   IETF RFC 3344 (August 2002): "IP Mobility Support for IPv4".

[14]   IETF RFC 3775 (June 2004): "Mobility Support in IPv6".

[15]   IETF RFC 3776 (June 2004): "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents".

[16]   IETF RFC 4187 (January 2006): "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".

[17]   IETF RFC 4282 (December 2005): "The Network Access Identifier".

[18]   IETF RFC 4862 (September 2007): "IPv6 Stateless Address Autoconfiguration".

[19]   IETF RFC 4285 (January 2006): "Authentication Protocol for Mobile IPv6".

[20]   IETF RFC 4294 (April 2006): "IPv6 Node Requirements".

[21]   Void.

[22]   ISO/IEC 9646-1: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 1: General concepts".

[23]   ISO/IEC 9646-7: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 7: Implementation Conformance Statements".

[24]   ITU-T Recommendation X.296: "OSI conformance testing methodology and framework for protocol Recommendations for ITU-T applications - Implementation conformance statements".

[25]   Void.

[26]   WiMAX Forum (Release 1.5): "WiMAX Forum Network Architecture; Stage 3: Architecture, detailed Protocols and Procedures: WiMAX Over-The-Air General Provisioning System Specification".

NOTE: Available at http://www.wimaxforum.org/resources/documents/technical/release

[27]   WiMAX Forum (Release 1.5): "WiMAX Forum Network Architecture; Stage 3: Architecture, detailed Protocols and Procedures: Over-The-Air Provisioning & Activation Protocol based on TR-069 Specification".

NOTE: Available at http://www.wimaxforum.org/resources/documents/technical/release

[28]   WiMAX Forum (Release 1.5): "WiMAX Forum Network Architecture; Stage 3: Architecture, detailed Protocols and Procedures; WiMAX Over-The-Air Provisioning & Activation Protocol based on OMA DM Specifications".

NOTE: Available at http://www.wimaxforum.org/resources/documents/technical/release.

[29]   WiMAX Forum (Release 1.5): "WiMAX Forum Network Architecture; Stage 3: Architecture, detailed Protocols and Procedures; Emergency Services Support".

NOTE: Available at http://www.wimaxforum.org/resources/documents/technical/release.

[30]   WiMAX Forum (Release 1.5): "WiMAX Forum Network Architecture; Stage 3: Architecture, detailed Protocols and Procedures; IP Multimedia Subsystem (IMS) Interworking".

NOTE: Available at http://www.wimaxforum.org/resources/documents/technical/release

[31]   WiMAX Forum (Release 1.5): "WiMAX Forum Network Architecture; Protocol and Procedures for Location Based Services".

NOTE: Available at http://www.wimaxforum.org/resources/documents/technical/release

[32]   WiMAX Forum (Release 1.5): "WiMAX Forum Network Architecture; Stage 3: System Requirements, Network Protocols and Architecture for Multi-cast Broad-cast Services".

NOTE: Available at http://www.wimaxforum.org/resources/documents/technical/release

[33]   Broadband Forum (December 2007, Issue 1 Amnd. 2): "TR-069; CPE WAN Management Protocol v1.1".

[34]   IETF RFC 5246 (August 2008): "The Transport Layer Security (TLS) Protocol Version 1.2".

[35]   IETF RFC 4279 (December 2005): "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)".

[36]   Open Mobile Alliance OMA-TS-ULP-V2-0-20080627-C (June 2008): "UserPlane Location Protocol".

2.2   Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1]   IETF draft-ietf-mip6-hiopt-17 (May 2008): "DHCP Options for Home Information Discovery in MIPv6".

[i.2]   ETSI TS 102 624-2: "Broadband Radio Access Networks (BRAN); HiperMAN; Conformance Testing for the Network layer of HiperMAN/WiMAX terminal devices; Part 2: Test Suite Structure and Test Purposes (TSS&TP)".

[i.3]   ETSI TS 102 624-3: "Broadband Radio Access Networks (BRAN); HiperMAN; Conformance Testing for the Network layer of HiperMAN/WiMAX terminal devices; Part 3: Abstract Test Suite (ATS)".

[i.4]   ETSI EG 201 058: "Methods for Testing and Specification (MTS); Implementation Conformance Statement (ICS) proforma style guide".

3   Definitions and abbreviations

3.1   Definitions

For the purposes of the present document, the terms and definitions given in ISO/IEC 9646-1 [22], WiMAX Forum Network Architecture Stage 2 [1], WiMAX Forum Network Architecture Stage 3 [2], and ISO/IEC 9646-7 [23] apply.

3.2   Abbreviations

For the purposes of the present document, the abbreviations given in WiMAX Forum Network Architecture Stage 2 [1], WiMAX Forum Network Architecture Stage 3 [2], ISO/IEC 9646-1 [22] and the following apply:

AR   Access Router
ASN   Access Service Network
BS   Base Station
DAD   Duplicate Address Detection
DNS   Domain Name Service
IID   Interface Identifier
IUT   Implementation Under Test
PDU   Protocol Data Unit
PICS   Protocol Implementation Conformance Statement
MAC   Medium Access Control
MS   Mobile Station

MTU   Maximum Transmission Unit
NAI   Network Access Identifier
NAP   Network Access Provider
NSP   Network Service Provider
SUT   System Under Test

4   Conformance to this PICS Proforma Specification

If it claims to conform to the present document, the actual PICS proforma to be filled in by a supplier shall be technically equivalent to the text of the PICS proforma given in annex A, and shall preserve the numbering, naming, and ordering of the proforma items.

A PICS which conforms to the present document shall be a conforming PICS proforma completed in accordance with the guidance for completion given in clause A.1.

Annex A (normative):
Protocol ICS (PICS) for HiperMAN/WiMAX terminal devices Network layer

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the PICS proforma in this annex so that it can be used for its intended purposes and may further publish the completed PICS.

A.1 Guidance for completing PICS Proforma

A.1.1 Purposes and structure

The purpose of this PICS proforma is to provide a mechanism whereby a supplier of an implementation of the requirements defined in defined in references [1] and [2] may provide information about the implementation in a standardized manner.

The PICS proforma is subdivided into subclauses for the following categories of information:

- guidance for completing the PICS proforma;

- identification and implementation;

- identification of the standard;

- global statement of conformance;

- Mobile Station (MS);

- List of messages;

- Message Fields.

A.1.2 Abbreviations and conventions

Item column

- The Item column contains a number which identifies the item in the table.

Capability column

- The capability column describes in free text each respective item (e.g. parameters, timers, etc.). It implicitly means "Is <capability> supported by the implementation?".

Reference column

- The reference column indicates the section of [1] and [2] from which the requirement for the capability is derived and in some cases also the referenced IETF RFCs referenced in the base standard.

Status column

- The following notations, defined in ISO/IEC 9646-1 [22], are used in the status column.

m	Explicitly shown as mandatory in the standard. It is required to implement.
o	Explicitly mentioned as optional in the standard or is not explicitly mentioned but has capability negotiations. It may or may not be implemented.
oi	Qualified option - for mutually exclusive or selectable options from a set. One or more of the options from the set shall be supported.

IO-NNNN	Inter-operable Options: Item belongs to NNNN group of features for which it is requested to provide testing procedure and distinct labelling of BS equipment. More specifically:
	   - the item is not required to get general "WiMAX certified" label; and
	   - is required to get distinct "WiMAX certified with NNNN capability" label.

Support column

- The support column shall be filled in by the supplier of the implementation. The following common notations, defined in ISO/IEC 9646-1 [22] are used for the support column.

Y or y	Supported by implementation.
N or n	Not supported by implementation.
N/A, n/a or -	No answer required (allowed only if the status is n/a either directly or after the evaluation of a conditional status).

Values allowed column

- The values allowed column is only used when necessary in a table. It contains the type, the list, the range, or the length of values allowed. The following notations are used.

Range of values: Example:	<min value>..<max value> 5..20
List of values: EXAMPLE 1: EXAMPLE 2: EXAMPLE 3:	<value1>, <value2>, …, <valueN> 2, 4, 6, 8, 9 1101b, 1011b, 1111b 0x0A, 0x34, 0x2F
List of named values: Example:	<name1>(<val1>), <name2>(<val2>), …, <nameN>(<valN>) reject(1), accept(2)
Length: EXAMPLE:	Size (<min size>..<max size>) Size (1..8)

Values supported column

- The values supported column is only present when the values allowed column is present. It shall be filled in by the supplier of the implementation. In this column, the value or the ranges of values supported by the implementation shall be indicated.

Reference to items

- For each possible item answer in the support column within the PICS proforma a unique reference exists which may be used, for example, in conditional expressions. It is defined as the table identifier, followed by the "/" character, followed by the item number in the table. If there is more than one support column in a table, the columns are discriminated by letters (a, b, etc.).

EXAMPLE 1:	Table A.5/4 is the reference to the answer of item 4 in table A.5.
EXAMPLE 2:	Table A.6/3b is the reference to the second answer (i.e. in the second support column) of item 3 in table A.6.

Prerequisite Line

- A prerequisite line takes the form: Prerequisite: <predicate>.

- A prerequisite line after a clause or table title indicates that the entire clause or the entire table is not required to be completed if the predicate is FALSE.

Support of specific MAC PDUs or fields does not automatically mean support of the corresponding functionality. It means only that BS(MS) is capable of transmitting or receiving / parsing the message of specific format.

A.1.3 Instructions for completing the PICS Proforma

The supplier of the implementation shall complete the PICS proforma in each of the spaces provided. In particular, an explicit answer shall be entered, in the support or values supported column boxes provided, using the notation described in clause A.1.2.

If necessary, the supplier may provide additional comments in space at the bottom of the tables or separately.

A.2 Identification of the implementation

Identification of the Implementation Under Test (IUT) and the system in which it resides (the System Under Test (SUT)) should be filled in so as to provide as much detail as possible regarding version numbers and configuration options.

The product supplier and client information should both be filled in if they are different.

A person who can answer queries regarding information supplied in the PICS should be named as the contact person.

A.2.1 Date of statement

Date of statement (MM/DD/YYYY):	

A.2.2 Implementation Under Test (IUT) identification

IUT name:	
IUT version:	

A.2.3 System Under Test (SUT) identification

SUT name:	
Hardware configuration:	
Operating system:	

A.2.4 Product supplier

Name:	
Address:	
Telephone Nr.:	
Fax Nr:	
E-mail address:	
Additional information:	

A.2.5   Client (if different from product supplier)

Name:	
Address:	
Telephone Nr.:	
Fax Nr:	
E-mail address:	
Additional information:	

A.2.6   PICS contact person

(A person to contact if there are any queries concerning the content of the PICS.)

Name:	
Address:	
Telephone Nr.:	
Fax Nr:	
E-mail address:	
Additional information:	

A.3   Identification of the standard

This PICS proforma applies to the ETSI HiperMAN/Wimax Forum standard consisting of the following normative references:

- WiMAX Forum Network Architecture

A.4   Global statement of conformance

Are all mandatory capabilities implemented? (Yes/No)	

NOTE: Answering "No" to this question indicates non-conformance to the HiperMAN/Wimax standard. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is non-conforming, on pages attached to the PICS proforma.

A.5 Mobile Station in WiMAX Network Architecture

A.5.1 MS Capabilities

Table A.1: MS Capabilities

Item	MS Capability	Reference	Status	Support
1	Network Discovery and Selection	[2] 4.1	m	
2	Network Access Authentication	[2] 4.4.1	m	
3	IPv4 Address Management and Transport	[2] 4.2, 4.8	m	
4	IPv6 Address Management and Transport	[2] 4.8.4, 4.11	o	
5	OTA Provisioning and Activation	[26]	m	
6	Emergency Services	[29] 7.1	o	
7	IP IMS interworking	[30]	o	
8	Location Based Services	[31]	o	
9	Multi-cast Broad-cast Services	[32]	o	
Comments:				

A.5.2 Network Discovery and Selection

Table A.2: Network Discovery and Selection

Item	Procedures	Reference	Status	Support
1	Network Access Provider (NAP) Discovery	[2] 4.1.2.1	m	
2	Network Service Provider (NSP) Discovery	[2] 4.1.2.2	m	
3	Network Service Provider (NSP) Selection	[2] 4.1.2.3	m	
4	Access Service Network (ASN) attachment	[2] 4.1.2.4	m	
Comments:				

Table A.3: NSP selection

Item	NSP Selection Method	Reference	Status	Support
1	Manual Mode NSP Selection	[2] 4.1.2.1	o.3	
2	Automatic Mode NSP Selection	[2] 4.1.2.2	o.3	
o.3:	It is mandatory to support at least one of these items.			

Table A.4: ASN Attachment

Item	ASN Attachment Feature	Reference	Status	Support
1	NAI Construction	[2] 4.1.2.4, 4.4.1.3, [17] 2	m	
2	Locally Configured 24-bit NSP Identifier To Realm Mapping	[2] 4.1.2.4, [17] 2	o	
Comments: These capabilities are related to the ASN attachment capability item in Table A.2/4.				

A.5.3 Network Access Authentication

Table A.5: Network Access Authentication

Item	Authentication Entity	Reference	Status	Support
1	Subscriber Authentication	[2] 4.4.1.1	m	
2	Device Authentication	[2] 4.4.1.1	m	
Comments: The MS shall support authentication of Device credentials independent of whether the HNSP requires device authentication.				

Table A.6: Subscriber Authentication

Item	Authentication Method	Reference	Status	Support
1	EAP-AKA Subscriber Authentication	[2] 4.4.1.2	o.6	
2	EAP-TTLS Subscriber Authentication	[2] 4.4.1.2	o.6	
o.6: It is mandatory to support at least one of these items.				

Table A.7: Device Authentication

Item	Authentication Method	Reference	Status	Support
1	EAP-TLS Device Authentication	[2] 4.4.1.2	m	

Table A.8: EAP-TTLS Subscriber Authentication

Item	EAP-TTLS Method	Reference	Status	Support
Prerequisite: A6/2 - EAP-TTLS Subscriber Authentication				
1	TTLS Version 0	[2] 4.4.1.2.3, [4] 7	m	
2	MS-CHAPv2	[2] 4.4.1.2.3, [9] 1	m	
3	Fragmentation	[2] 4.4.1.2.3, [10] 2.1.5	m	

A.5.4 IPv4 Address Management and Transport

Table A.9: IPv4 Address Management

Item	Mobility Management Capability	Reference	Status	Support
1	Proxy MIPv4 (PMIP4) Mobility Management	[2] 4.8.2.1	o.9	
2	Client MIPv4 (CMIP4) Mobility Management	[2] 4.8.3.1	o.9	
3	Simple IPv4 Service	[2] 4.14.4.1	o.9	
o.9: It is mandatory to support at least one of these items.				
Note: For Simple IPv4 Service CSN anchored mobility service is not supported [1] 7.13.				

Table A.10: IPv4 Transport

Item	IPv4 Transport Capability	Reference	Status	Support
1	IPv4 Fragmentation with MTU Size	[2] 3.3.3	m	

Table A.11: PMIP4 Mobility Management

Item	Mobility management capability	Reference	Status	Support
Prerequisite: A.9/1 - PMIP4 mobility management				
1	PMIP4 Connection Setup	[2] 4.8.2.1.1	m	
2	PMIP4 Address Renewal	[2] 4.8.2.2.1	m	
3	PMIP4 Connection Termination	[2] 4.8.2.4.1	o	

Table A.12: PMIP4 DHCP Procedures

Item	DHCP Procedure	Reference	Status	Support
Prerequisite: A.9/1 - PMIP4 Mobility Management				
1	Allocating A New Network Address	[2] 4.8.2.1.1 [5] 3.1	m	
2	Reusing Previously Allocated Network Address	[5] 3.2	o	

Table A.13: CMIP4 Mobility Management

Item	Mobility Management Capability	Reference	Status	Support
Prerequisite: A.9/2 - CMIP4 Mobility Management				
1	CMIP4 Connection Setup	[2] 4.8.3.1.1, [1] 7.8.19.1	m	
2	CMIP4 Session Renewal	[2] 4.8.3.2.1, [1] 7.8.19.2	m	
3	CMIP4 CSN Anchored Mobility Handover	[2] 4.8.3.3.1	m	
4	CMIP4 Session Termination	[2] 4.8.3.4.1	m	
5	Registration Request Re-transmission	[2] 4.8.3 [13] 3.6.3	o	
6	Registration Request Timestamp-based Replay Protection	[2] 4.8.3 [13] 5.7	m	
7	Registration Request Nonce-based Replay Protection	[2] 4.8.3 [13] 5.7	o	
8	Encapsulating Delivery Method	[2] 4.8.3 [11] 3.3	m	

Table A.14: CMIP4 Initial Connection Setup Address Resolution

Item	Home Agent Address Resolution Procedure	Reference	Status	Support
Prerequisite: A.9/2 - CMIP4 Mobility Management				
1	Static Home Agent Address Assignment	[2] 4.8.3.1, [13] 3.6.1.2	m	
2	Dynamic Home Agent Address Resolution	[2] 4.8.3.1, [13] 3.6.1.2	m	
3	Static Home Address Assignment	[2] 4.8.3.1, [13] 3.6.1.2	m	
4	Dynamic Home Address Resolution	[2] 4.8.3.1, [13] 3.6.1.2	m	

A.5.5   IPv6 Address Management and Transport

Table A.15: IPv6 Address Management and Transport

Item	IPv6 Capability	Reference	Status	Support
Prerequisite: A.1/4 - IPv6 Address Management and Transport				
1	IPv6 Address Management	[2] 4.11	m	
2	Client MIPv6 (CMIP6) Mobility Management	[2] 4.8.3.1	o	
3	Simple IPv6 Service	[2] 4.14.5.1	o	
Note: For Simple IPv6 service no support for mobility management is offered at the IP layer [1] 7.13.2.				

Table A.16: IPv6 Transport

Item	IPv6 Transport capability	Reference	Status	Support
Prerequisite: A.1/4 - IPv6 Address Management and Transport				
1	IPv6 Fragmentation with MTU Size	[2] 3.3.3	m	

Table A.17: CMIP6 Mobility Management

Item	Mobility Management Capability	Reference	Status	Support
Prerequisite: A. 15/2 - CMIP6 mobility management				
1	MIP6 Connection Setup	[2] 4.8.4.1, 4.8.4.1.1	m	
2	MIP6 Session Renewal	[2] 4.8.4.3, 4.8.4.3.1	m	
3	MIP6 Inter Access Router Handover	[2] 4.8.4.2, 4.8.4.2.1	m	
4	MIP6 Session Termination	[2] 4.8.4.4, 4.8.4.4.1	m	

Table A.18: CMIP6 Session Operation

Item	CMIP6 Session Operation feature	Reference	Status	Support
Prerequisite: A.9/3 - CMIP6 Mobility Management				
1	Mobility Support in IPv6	[2] 4.8.4, [14] 11	m	
2	MIPv6-specific Mobility Message Authentication	[2] 4.8.4, [19] 4, 5	m	
3	Mobility Message Authentication Option	[2] 4.8.4, [15] 5	m	
4	Mobile Node Identifier Option	[2] 4.8.4, [15] 3	m	
5	Dynamic Discovery of Mobile IPv6 Home Network Information	[2] 4.8.4, [i.1] 3, 4	m	

Table A.19: IPv6 Operations

Item	IPv6 Operations Capability	Reference	Status	Support
Prerequisite: A.1/4 - IPv6 Address Management and Transport				
1	Point To Point Link Between MS And AR	[2] 4.11.2	m	
2	Link Establishment	[2] 4.11.3	m	
3	Interface Identifier (IID) Generation	[2] 4.11.4.1 [8] 4	m	
4	Duplicate Address Detection (DAD)	[2] 4.11.4.2, [1] 7.2.2.2.1, [20] 4.5.2	m	
5	Stateless Address Auto-configuration	[2] 4.11.4.3, 4.11.4, [20] 4.5.2, [18] 1	m	
6	Stateful Address Auto-configuration	[2] 4.11.4.4, 4.11.4, [20] 4.5.5, [12] 1	o	
7	DNS Discovery	[2] 4.11.5	m	
8	Uplink IPv6 Packet Transmission	[2] 4.11.6.1	m	
9	Downlink IPv6 Packet Transmission	[2] 4.11.6.2	m	
10	Privacy Extensions For Address Configuration In IPv6	[2] 4.11.4, [7] 3, [20] 4.5.3	o	
11	Default Address Selection For IPv6	[2] 4.11.4, [3] 3, 4, 5, 6, [20] 4.5.4	m	

A.5.6   OTA Provisioning and Activation

Table A.20: OTA Device Type

Item	Device Type	Reference	Status	Support
Prerequisite: A.1/5 - OTA Provisioning and Activation				
1	Model A - Operator/Service provider tied device	[26] 3.2	o.20	
2	Model B1 - Generic retail device, Non-operator/Service provider subsidized	[26] 3.2	o.20	
3	Model B2 - Generic retailt device, Operator/Service provider subsidized	[26] 3.2	o.20	
o.20: It is mandatory to support exactly one of these items				

Table A.21: OTA Model B Device Type Classification

Item	Model B Type Of Device	Reference	Status	Support
Prerequisite: A.1/5 and A.20/2 or A.20/3 - OTA Provisioning and Activation and Model B1 or Model B2				
1	WiMAX CPE Gateway	[26] 9.1.1	o.21	
2	Other WiMAX device	[26] 9.1.1	o.21	
o.21: It is mandatory to support exactly one of these items				

Table A.22: OTA Model A Device Provisioning Client Provisioning and Activation

Item	Provisioning and Activation Procedure	Reference	Status	Support
Prerequisite: A.1/5 and A.20/1 - OTA Provisioning and Activation and Device Type Model A				
1	OMA DM Based	[26] 6.1.2	o.22	
2	TR-069 Based	[26] 6.1.2	o.22	
o.22: It is mandatory to support at least one of these items				

Table A.23: OTA Model B CPE Gateway Device Provisioning Client Provisioning and Activation

Prerequisite: A.1/5 and A.21/1 - OTA Provisioning and Activation and Model B CPE Gateway				
Item	**Provisioning and Activation Procedure**	**Reference**	**Status**	**Support**
1	OMA DM Based	[26] 9.1.1	m	
2	TR-069 Based	[26] 9.1.1	m	

Table A.24: OTA Model B Non-CPE Gateway Device Provisioning Client Provisioning and Activation

Prerequisite: A.1/5 and A.21/2 - OTA Provisioning and Activation and Model B non-CPE Gateway				
Item	**Provisioning and Activation Procedure**	**Reference**	**Status**	**Support**
1	OMA DM Based	[26] 9.1.1	m	
2	TR-069 Based	[26] 9.1.1	o	

Table A.25: Model B OTA OMA Bootstrap Profiles

Prerequisite: A.22/1 - OMA DM Based Provisioning and Activation				
Item	**OMA Bootstrap Profile**	**Reference**	**Status**	**Support**
1	OMA Client Provisioning	[26] 6.3	o	
2	OMA Device Management	[26] 6.3	m	

Table A.26: Model B OTA OMA DM Bootstrapping

Prerequisite: A.1/5 and A.20/2 or A.20/3 - OTA Provisioning and Activation and Model B1 or Model B2				
Item	**OMA DM Bootstrap method**	**Reference**	**Status**	**Support**
1	Server-initiated bootstrap	[28] 6.2.1, 6.1	o.26	
2	Client-initiated bootstrap	[28] 6.2.1, 6.1	o.26	
o.26: It is mandatory to support at least one of these items				

Table A.27: OTA TR-069 Based Provisioning and Activation Capabilities

Prerequisite: A.22/2 or A.23/2 or A.24/2 - TR-069 Based Provisioning and Activation				
Item	**TR-069 client based Capability**	**Reference**	**Status**	**Support**
1	TR-069 protocol	[27] 5.2 [33] 2, 3	m	
2	WIB	[27] 5.2 [26] 8, 9.6	m	
3	Security	[27] 6 [26] 10	m	

Table A.28: OTA OMA DM Based Provisioning and Activation Capabilities

Prerequisite: A.22/1 or A.23/1 or A.24/1 - OMA Based Provisioning and Activation				
Item	**OMA client Capability**	**Reference**	**Status**	**Support**
1	OMA DM protocol	[28] 6.2.1	m	
2	WIB	[28] 6.2.1	o	
3	Security	[28] 7 [26] 10	m	

Table A.29: OTA OMA DM Protocol Procedures

Prerequisite: A.22/1 or A.23/1 or A.24/1 - OMA Based Provisioning and Activation				
Item	**OMA DM Protocol client based Capability**	**Reference**	**Status**	**Support**
1	Large Objects	[28] 5.1.4, A.8.3.9	o	
2	Continuous Management	[28] 6.6, A9.6.7	o	

Table A.30: OTA OMA DM Continuous Management Support

Prerequisite: A.29 /2 - OTA OMA DM Continuous Management				
Item	**OTA OMA DM Continuous Management procedure**	**Reference**	**Status**	**Support**
1	Receiving Notification Initiated Session Trigger message	[28] 6.6, A9.6.8	o.30	
2	Polling-based Client-initiated Periodic Polling	[28] 6.2.1, A9.6.9, A9.6.10	o.30	
o. 30:	It is mandatory to support at least one of these items			

Table A.31: OTA Security Cipher-suites

Prerequisite: A.1/5 - OTA Provisioning and Activation				
Item	**Cipher-suite**	**Reference**	**Status**	**Support**
1	TLS_RSA_WITH_AES_256_CBC_SHA	[26] 10 [34]	o.31	
2	TLS_RSA_WITH_AES_128_CBC_SHA	[26] 10 [34]	o.31	
3	TLS_RSA_WITH_3DES_EDE_CBC_SHA	[26] 10 [34]	o.31	
o.31:	It is mandatory to support at least one of these items			

A.5.7   Emergency Services

Table A.32: Emergency Services

Prerequisite: A.1/6 - Emergency Services support				
Item	**Emegency Services Capability**	**Reference**	**Status**	**Support**
1	VoIP Service	[29] 6	o	
2	Emergency Service Recognition	[29] 7.1, 8.3	o	

Table A.33: VoIP Service Protocol

Prerequisite: A.32/1 - VoIP Service				
Item	**VoIP protocol**	**Reference**	**Status**	**Support**
1	SIP protocol	[29] 9.2	o	

A.5.8   Location Based Services

Table A.34: Location Based Services

Prerequisite: A.1/6 - Location Based Services support				
Item	**Location Based Service Capability**	**Reference**	**Status**	**Support**
1	WiMAX Location Protocol (WLP) on R2	[32] 7.2, 9.5.1	o	
2	OMA Secure User Plane Location (SUPL) on R2	[32] 7.2, 9.5.2	o	
3	Assisted GPS	[32]	o	

Table A.35: WiMAX Location Protocol Capability

Prerequisite: A.34/1 - WLP support				
Item	**WLP capability**	**Reference**	**Status**	**Support**
1	DHCP based Location Server discovery	[32] 9.5.1.1	m	
2	HTTP Enabled Location Delivery transport	[32] 9.5.1.2	m	
3	WLP capability negotiation	[32] 9.5.1.4	o	
4	PSK-TLS secured transport	[32] 9.5.1.5 [35]	m	

Table A.36: Secure User Plane Location Capability

Prerequisite: A.34/2 - SUPL support				
Item	**SUPL capability**	**Reference**	**Status**	**Support**
1	Userplane Location Protocol	[32] 9.5.2.1 [36]	m	
2	PSK-TLS secured transport	[32] 9.5.2.5 [35]	m	

A.5.9   IP-IMS interworking

Table A.37: IP-IMS Client

Prerequisite: A.1/7 - IP IMS interworking				
Item	**IP IMS Client Capability**	**Reference**	**Status**	**Support**
1	IMS Access Procedures	[30] 4.2.1	m	
2	IMS Call Control and SIP extensions	[30] 4.2.1	m	
3	IMS Client Management	[30] 4.2.1	m	
4	UICC Services	[30] 4.2.1	o	
5	IMS AKA Based Authentication	[30] 9.3	m	
6	IPsec Protected IMS signaling	[30] 9.3	m	

A.5.10 Multi-cast Broad-cast Services

Table A.38: Multi-cast Broad-cast Service

Prerequisite: A.1/8 - Multi-cast Broad-cast Services				
Item	**MCBCS Capability**	**Reference**	**Status**	**Support**
1	Receive incoming call/service notification during MCBCS	[32] 2	m	

A.5.11 Messages

In the following message tables, statuses with values are the only valid cases, according to the direction of the PDU. When not applicable to a given direction, status not applicable (n/a) is defined.

Table A.39: DHCPv4 Messages

Prerequisite: A9/1 - PMIP4 Mobility Management (DHCPv4)						
Item	**DHCPv4 Message**	**Reference**	**Status**	**Support**	**Status**	**Support**
			MS sending		**MS receiving**	
1	DHCPDISCOVER	[2] 4.8.2.1.1, [5] 3.1	m		n/a	
2	DHCPOFFER	[2] 4.8.2.1.1, [5] 3.1	n/a		m	
3	DHCPREQUEST	[2] 4.8.2.1.1, [5] 3.1	m		n/a	
4	DHCPACK	[2] 4.8.2.1.1, [5] 3.1	n/a		m	
5	DHCPNAK	[2] 4.8.2.1.1, [5] 3.1	n/a		m	
6	DHCPDECLINE	[2] 4.8.2.1.1, [5] 3.1	m		n/a	
7	DHCPRELEASE	[2] 4.8.2.1.1, [5] 3.1	o		n/a	
8	DHCPINFORM	[2] 4.8.2.1.1, [5] 3.1	o		n/a	

Table A.40: EAP-TLS Device Authentication Messages

Item	**EAP-TLS Message**	**Reference**	**Status**	**Support**	**Status**	**Support**
			MS sending		**MS receiving**	
1	EAP-Request/Identity	[2] 4.4.1.2.1, [10] 4.2, [6] 3.1	n/a		m	
2	EAP-Response/Identity	[2] 4.4.1.2.1, [10] 4.3, [6] 3.1	m		n/a	
3	EAP-Request/EAP-TLS	[2] 4.8.3.1.1, [10] 4.2, [6] 2.2.1	n/a		m	
4	EAP-Response/EAP-TLS	[2] 4.8.3.1.1, [10] 4.3, [6] 2.2.1	m		n/a	
5	EAP-Success	[2] 4.8.3.1.1, [10] 3.1, [6] 2.2.2	n/a		m	
6	EAP-Failure	[2] 4.8.3.1.1, [10] 3.1, [6] 2.2.2	n/a		m	

Table A.41: EAP-AKA User Authentication Messages

Item	EAP-AKA Message	Reference	Status	Support	Status	Support
Prerequisite: A6/1 - EAP-AKA User Authentication						
			MS sending		MS receiving	
1	EAP-Request/AKA-Identity	[2] 4.4.1.2.2, [16] 9.1	n/a		m	
2	EAP-Response/AKA-Identity	[2] 4.4.1.2.2, [16] 9.2	m		n/a	
3	EAP-Request/AKA-Challenge	[2] 4.4.1.2.2, [16] 9.3	n/a		m	
4	EAP-Response/AKA-Challenge	[2] 4.4.1.2.2, [16] 9.4	m		n/a	
5	EAP-Response/AKA-Authentication-Reject	[2] 4.4.1.2.2, [16] 9.5	m		n/a	
6	EAP-Response/AKA-Synchronization-Failure	[2] 4.4.1.2.2, [16] 9.6	m		n/a	
7	EAP-Request/AKA-Reauthentication	[2] 4.4.1.2.2, [16] 9.7	n/a		o	
8	EAP-Response/AKA-Reauthentication	[2] 4.4.1.2.2, [16] 9.8	o		n/a	
9	EAP-Response/AKA-Client-Error	[2] 4.4.1.2.2, [16] 9.9	m		n/a	
10	EAP-Request/AKA-Notification	[2] 4.4.1.2.2, [16] 9.10	n/a		m	
11	EAP-Response/AKA-Notification	[2] 4.4.1.2.2, [16] 9.11	m		n/a	

Table A.42: EAP-TTLS User And Device Authentication Messages

Item	EAP-TTLS Message	Reference	Status	Support	Status	Support
Prerequisite: A.6/2 - EAP-TTLS User Authentication						
			MS sending		MS receiving	
1	EAP-Request/Identity	[2] 4.4.1.2.3, [4] 5.3	n/a		m	
2	EAP-Response/Identity	[2] 4.4.1.2.3, [4] 5.3	m		n/a	
3	EAP-Request/EAP-TTLS	[2] 4.4.1.2.3, [4] 7.1	n/a		m	
4	EAP-Response/EAP-TTLS	[2] 4.4.1.2.3, [4] 7.1	m		n/a	
5	EAP-Success	[2] 4.4.1.2.3, [4] 7.2	n/a		m	
6	EAP-Failure	[2] 4.4.1.2.3, [4] 9.2.1	n/a		m	

Table A.43: MIP4 Messages

Item	MIP4 Message	Reference	Status	Support	Status	Support
Prerequisite A9/2 - CMIP4 Mobility Management						
			MS sending		MS receiving	
1	MIP Agent Solicitation Message	[2] 4.8.3.3, [13] 2.2, 2.4	m		n/a	
2	MIP Agent Advertisement Message	[2] 4.8.3.3, [13] 2.2, 2.4	n/a		m	
3	MIP Registration Request (RRQ)	[2] 4.8.3.1.1, [13] 3.3	m		n/a	
4	MIP Registration Reply	[2] 4.8.3.1.1, [13] 3.4	n/a		m	

Table A.44: CMIP6 Messages

Prerequisite: A9/3 - CMIP6 Mobility Management						
Item	**CMIP6 Message**	**Reference**	**Status**	**Support**	**Status**	**Support**
			MS sending		**MS receiving**	
1	Binding Refresh Request Message	[2] 4.8.4, [14] 6.1.2	n/a		m	
2	Binding Update Message	[2] 4.8.4.1.1, [14] 6.1.7	m		n/a	
3	Binding Acknowledgement Message	[2] 4.8.4, [14] 6.1.8	n/a		m	
4	Binding Error Message	[2] 4.8.3.1.1, [14] 6.1.9	n/a		m	
5	Home Test Init Message	[1] 7.8.2.14, [2] 4.8.4, [14] 6.1.3	m		n/a	
6	Care-of Test Init Message	[1] 7.8.2.14, [2] 4.8.4, [14] 6.1.4	m		n/a	
7	Home Test Message	[1] 7.8.2.14, [2] 4.8.4, [14] 6.1.5	n/a		m	
8	Care-of Test Message	[1] 7.8.2.14, [2] 4.8.4, [14] 6.1.5	n/a		m	

Table A.45: DHCPv6 Messages

Prerequisite: A.19/6 or A.15/2 - Stateful Autoconfiguration In IPv6 Operations Or CMIP6 Mobility Management						
Item	**DHCPv6 Message**	**Reference**	**Status**	**Support**	**Status**	**Support**
			MS sending		**MS receiving**	
1	SOLICIT	[2] 4.8.4.1, 4.11.4.4 [12] 17.1.1	m		n/a	
2	ADVERTISE	[2] 4.8.4.1, 4.11.4.4 [12] 17.1.2	n/a		m	
3	REQUEST	[2] 4.8.4.1, 4.11.4.4 [12] 18.1.1	m		n/a	
4	CONFIRM	[2] 4.8.4.1, 4.11.4.4 [12] 18.1.2	m		n/a	
5	RENEW	[2] 4.8.4.1, 4.11.4.4 [12] 18.1.3	m		n/a	
6	REBIND	[2] 4.8.4.1, 4.11.4.4 [12] 18.1.4	m		n/a	
7	REPLY	[2] 4.8.4.1, 4.11.4.4 [12] 18.1.8	n/a		m	
8	RELEASE	[2] 4.8.4.1, 4.11.4.4 [12] 18.1.6	m		n/a	
9	DECLINE	[2] 4.8.4.1, 4.11.4.4 [12] 18.1.7	m		n/a	
10	RECONFIGURE	[2] 4.8.4.1, 4.11.4.4 [12] 19.4.1	n/a		m	
11	INFORMATION-REQUEST	[2] 4.8.4.1, 4.11.4.4 [12] 18.1.5	m		n/a	

Annex B (informative):
Bibliography

- IEEE 802.16e-2005: "IEEE Standard for Local and metropolitan area networks - Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems. Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1".

NOTE: Available at http://standards.ieee.org/getieee802/802.16.html.

- IETF RFC 4283 (November 2005): "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)".

History

Document history		
V.1.1.1	October 2008	Publication
V1.2.1	November 2009	Publication