WiMAX Forum® Network Architecture

Architecture, detailed Protocols and Procedures

WIMAX Lawful Intercept - NORTH AMERICAN REGION

WMF-T33-107-R015v02
WMF Approved
(2011-11-14)

WiMAX Forum Proprietary

Copyright © 2011 WiMAX Forum. All Rights Reserved.

Copyright Notice, Use Restrictions, Disclaimer, and Limitation of Liability

Copyright 2011 WiMAX Forum. All rights reserved.

The WiMAX Forum® owns the copyright in this document and reserves all rights herein. This document is available for download from the WiMAX Forum and may be duplicated for internal use by the WiMAX Forum members, provided that all copies contain all proprietary notices and disclaimers included herein. Except for the foregoing, this document may not be duplicated, in whole or in part, or distributed without the express written authorization of the WiMAX Forum.

Use of this document is subject to the disclaimers and limitations described below. Use of this document constitutes acceptance of the following terms and conditions:

THIS DOCUMENT IS PROVIDED "AS IS" AND WITHOUT WARRANTY OF ANY KIND. TO THE GREATEST EXTENT PERMITTED BY LAW, THE WiMAX FORUM DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF TITLE, NONINFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE WiMAX FORUM DOES NOT WARRANT THAT THIS DOCUMENT IS COMPLETE OR WITHOUT ERROR AND DISCLAIMS ANY WARRANTIES TO THE CONTRARY.

Any products or services provided using technology described in or implemented in connection with this document may be subject to various regulatory controls under the laws and regulations of various governments worldwide. The user is solely responsible for the compliance of its products and/or services with any such laws and regulations and for obtaining any and all required authorizations, permits, or licenses for its products and/or services as a result of such regulations within the applicable jurisdiction.

NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE APPLICABILITY OR NON-APPLICABILITY OF ANY SUCH LAWS OR REGULATIONS OR THE SUITABILITY OR NON-SUITABILITY OF ANY SUCH PRODUCT OR SERVICE FOR USE IN ANY JURISDICTION.

NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE SUITABILITY OR NON-SUITABILITY OF A PRODUCT OR A SERVICE FOR CERTIFICATION UNDER ANY CERTIFICATION PROGRAM OF THE WiMAX FORUM OR ANY THIRD PARTY.

The WiMAX Forum has not investigated or made an independent determination regarding title or noninfringement of any technologies that may be incorporated, described or referenced in this document. Use of this document or implementation of any technologies described or referenced herein may therefore infringe undisclosed third-party patent rights or other intellectual property rights. The user is solely responsible for making all assessments relating to title and noninfringement of any technology, standard, or specification referenced in this document and for obtaining appropriate authorization to use such technologies, technologies, standards, and specifications, including through the payment of any required license fees.

NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES OF TITLE OR NONINFRINGEMENT WITH RESPECT TO ANY TECHNOLOGIES, STANDARDS OR SPECIFICATIONS REFERENCED OR INCORPORATED INTO THIS DOCUMENT.

IN NO EVENT SHALL THE WiMAX FORUM OR ANY MEMBER BE LIABLE TO THE USER OR TO A THIRD PARTY FOR ANY CLAIM ARISING FROM OR RELATING TO THE USE OF THIS DOCUMENT, INCLUDING, WITHOUT LIMITATION, A CLAIM THAT SUCH USE INFRINGES A THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS OR THAT IT FAILS TO COMPLY WITH APPLICABLE LAWS OR REGULATIONS. BY USE OF THIS DOCUMENT, THE USER WAIVES ANY SUCH CLAIM AGAINST THE WiMAX FORUM AND ITS MEMBERS RELATING TO THE USE OF THIS DOCUMENT.

The WiMAX Forum reserves the right to modify or amend this document without notice and in its sole discretion. The user is solely responsible for determining whether this document has been superseded by a later version or a different document.

"WiMAX," "Mobile WiMAX," "Fixed WiMAX," "WiMAX Forum," "WiMAX Certified," "WiMAX Forum Certified," the WiMAX Forum logo and the WiMAX Forum Certified logo are trademarks or registered trademarks of the WiMAX Forum. All other trademarks are the property of their respective owners. Wi-Fi® is a registered trademark of the Wi-Fi Alliance.

TABLE OF CONTENTS

1. INTRODUCTION 1
1.1 Background 1
1.2 Scope and Purpose 1

2. NORMATIVE REFERENCES 3

3. DEFINITIONS & ACRONYMS 5
3.1 Definitions 5
3.2 Acronyms 7

4. WIMAX SERVICESDESCRIPTION 8
4.1 WiMAX Services Model 8
4.2 General Surveillance Model 9
4.2.1 Electronic Surveillance Model 9
4.2.2 Intercept Access Points 10

5. WIMAX SUBJECT IDENTIFICATION 11
5.1 Login Identifier 11
5.2 Equipment Identifier 11

6. USER PERSPECTIVE 12
6.1 Introduction 12
6.2 Surveillance Events 12
6.2.1 Access Attempt 12
6.2.2 Access Accepted 12
6.2.3 Access Failed 12
6.2.4 Access Session End 12
6.2.5 Access Rejected 12
6.2.6 Access Signaling Message Report 12
6.2.7 Packet Data Session Start 13
6.2.8 Packet Data Session Failed 13
6.2.9 Packet Data Session End 13
6.2.10 Packet Data Session Already Established 13
6.2.11 Packet Data Header Report 14
6.2.12 Packet Data Summary Report 14
6.2.13 ServingSystem Event Reporting for Terminal Registration 14
6.2.14 Dynamic IP Address Management 14
6.3 General Requirements 15
6.3.1 Subject Communications 15
6.3.2 Communications Delivery 15
6.3.3 Timing Requirements 15
6.3.4 Performance and Quality 15
6.3.5 Security and Reliability over the interface between DF and CF 16
6.3.5 Encryption and Compression 16
6.3.6 Isolation 16
6.3.7 Privacy and Authentication 16
6.3.8 Transparency 16
6.3.9 Correlation 16
6.3.10 Location Information Reporting 17
6.3.11 Handling of Tunneled Packets 17

7. NETWORK PERSPECTIVE 18
7.1 Introduction 18
7.2 Definitions for "Mandatory," "Optional," and "Conditional" Parameters 18
7.3 Message Reporting 18
7.3.1 Access Attempt Message 18
7.3.2 Access Accepted Message 18
7.3.3 Access Failed Message 18
7.3.4 Access Session End Message 18
7.3.5 Access Rejected Message 18
7.3.6 Access Signaling Message Report Message 18
7.3.7 Packet Data Session Start Message 18
7.3.8 Packet Data Session Failed Message 18
7.3.9 Packet Data Session End Message 19
7.3.10 Packet Data Session Already Established Message 19
7.3.11 Packet Data Header Report Message 19
7.3.12 Packet Data Summary Report Message 19
7.4 Additional Message Reporting 19
7.4.1 ServingSystem Event Reporting for Terminal Registration 19

8. CMC DELIVERY 20

ANNEX A. (NORMATIVE) 21

A.1 ASN.1 DEFINITIONS 21

A.1.1 WIMAX CMII ABSTRACT SYNTAX MODULE 21

ANNEX B. RELIABLE DELIVERY (INFORMATIVE) 23

B.1 SHORT-TERM PULL BUFFERING 23

B.2 SHORT-TERM PUSH BUFFERING 23

ANNEX C. OPTIONAL MESSAGES (INFORMATIVE) 24

C.1 OPTIONAL SURVEILLANCE STATUS MESSAGES 24

C.1.1 SERVICE CHANGE 24

C.1.2 VIRTUAL PRIVATE NETWORK (VPN) SECURITY ASSOCIATION ESTABLISHMENT 24

C.1.3 VIRTUAL PRIVATE NETWORK (VPN) SECURITY ASSOCIATION RELEASE 24

C.1.4 SURVEILLANCE ACTIVATION 24

C.1.5 SURVEILLANCE CONTINUATION 24

C.1.6 SURVEILLANCE CHANGE 24

C.1.7 SURVEILLANCE DEACTIVATION 24

C.2 WIMAX CMII OPTIONAL MESSAGES ABSTRACT SYNTAX MODULE 24

ANNEX D. INTERCEPTED COMMUNICATION CONTENT DELIVERY (NORMATIVE) 26

D.1 WIMAX CMC DELIVERY FORMAT 26

D.2 WIMAX CMCC ABSTRACT SYNTAX MODULE 26

ANNEX E. CANADIAN LOCATION REPORTING (NORMATIVE) 27

E.1.1 LOCATION_UPDATE MESSAGE DEFINITION 27

E.1.2 LOCATION_UPDATE MESSAGE INFORMATION ELEMENTS DEFINITIONS 27

TABLE OF FIGURES

FIGURE 1– WIMAX LI NETWORK SERVICES MODEL 8
FIGURE 2 – ELECTRONIC SURVEILLANCE MODEL 9

TABLE OF TABLES

TABLE 1 – SERVINGSYSTEM MESSAGE PARAMETERS FOR TERMINAL REGISTRATION 19
TABLE 2 – LOCATION_UPDATE MESSAGE 27

1. Introduction

1.1 Background

This specification defines the interfaces between a service provider, that facilitates WiMAX® enforcement Agency (LEA) to assist the LEA in conducting Lawfully Authorized Electronic Surveillance (LAES) for subscription-based Internet Access and Services (IAS) arrangements.

As used in this specification, electronic surveillance refers to the interception and delivery of communications – i.e., Communications Content (CmC), Communications Identifying Information (CmII), or both – for a particular WiMAX subscriber as lawfully authorized. In this specification, an intercept subject, or more simply a subject, is a WiMAX subscriber whose communications have been authorized by a legal instrument to be intercepted and delivered to an LEA. The identification of the subject is limited to subject identifiers or subject-related identifiers used by the WiMAX network Service or a WiMAX Services Provider's (WiMAX-SP) equipment, facility, or communication service - e.g., network address, terminal identity, subscription identity.

As a precondition for WiMAX-SP assistance with LAES, an LEA must serve a WiMAX-SP with the necessary lawful authorization identifying the intercept subject, the communications and information to be provided, and service areas where the communications and information are to be provided. Once this lawful authorization is served on a WiMAX-SP, the WiMAX-SP shall perform the access, mediation as necessary, and delivery of the identified communications and information to the LEA via LEA-procured equipment, facilities, or services.

This specification is based on the solution found in ATIS-1000013-2007 Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services (IAS) [16], as modified by ATIS-1000013.a-2009 Supplement A to ATIS-1000013.2007 Lawfuly Authorized Electronic Surveillance (LAES) for Internet Access and Services (IAS) [20], and WiMAX Lawful Broadband Access Intercept Part 0 – Overview [19].

1.2 Scope and Purpose

The scope of LAES for WiMAX is on a WiMAX-SP's Network that provides the WiMAX subscriber services using the WiMAX network. LAES for the following are outside the scope of this document and for future study as necessary.

- Lawful Interception for non-IP services (e.g., Ethernet CS);
- Standalone ASN operators;
- Correlation of sessions within the same WiMAX-SP where multiple DFs report portions of the same session (e.g, because different DFs serve different geographic regions or different access technologies); and
- Advanced services (e.g., Location Based Services (LBS)).

For the U.S., this specification is provided for purposes of a "safe harbor" as specified in Section 107 of the Communications Assistance for Law Enforcement Act (CALEA) [1]: "a telecommunications carrier shall be found to be in compliance with the assistance capability requirements under Section 103, and a manufacturer of telecommunication transmission or switching equipment or a provider of telecommunication support services shall be found in compliance with Section 106, if the carrier, manufacturer, or support service provider is in compliance with publicly available technical

requirements or standards adopted by an industry association or standard-setting organization, or by the Commission under subsection (b), to meet the requirements of section 103."[1] [2][3][14][15].

This specification is also intended for use in Canada to meet the Canadian requirements and capabilities for LAES. See Annex E Canadian Requirements for Canadian specific requirements and capabilities.

[1] It is not the intent of this document to imply or impact any pending CALEA regulatory decisions related to IAS. This document provides the mechanisms to perform lawfully authorized electronic surveillance of IAS subject to the appropriate legal and regulatory environment. Where CALEA is found to be applicable to IAS, it is intended that a manufacturer or service provider that is in compliance with this document will have "safe harbor" under Section 107 of CALEA, Public Law 103-414, codified at 47 U.S.C. §1001, et seq.

2. Normative References

[1] Communications Assistance for Law Enforcement Act (CALEA), Public Law 103-414, October 25, 1994.[2]

[2] In the Matter of Communications Assistance for Law Enforcement Act, Order on Remand, CC Docket No. 97-213, 17 FCC Record 6898 (2002).[2]

[3] In the Matter of Communications Assistance for Law Enforcement Act, Third Report and Order, CC Docket No. 97-213, 14 FCC Record 16794 (1999).[2]

[4] Wire and Electronic Communications Interception and Interception of Oral Communications, Title 18 of the United States Code, Chapter 119, Sections 2510 – 2522.[2]

[5] ITU-T Recommendation X.680, Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation, July 2002.[3]

[6] Section 3 of the WiMAX Forum Specification adopts some of the definitions from ATIS-1000013.2007, as modified by ATIS-1000013.a-2009.

[7] IETF RFC 793, Transmission Control Protocol, September 1981. [4]

[8] Sections 4-8 of the WiMAX Forum Specification (excluding Section 7.4) reproduce in substantial part the corresponding sections of ATIS-1000013.2007, as modified by ATIS-1000013.a-2009, and adapts them for use in WiMAX™ networks.

[9] IETF RFC 791, Internet Protocol Darpa Internet Program Protocol Specification, September 1981.[4]

[10] IETF RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, December 1998.[4]

[11] Packet Technologies in Wireline Telecommunications Networks, Version 2, January 2006.[4]

[12] ANSI J-STD-025-B, Joint T1-TIA Standard on Lawfully Authorized Electronic Surveillance, August 2006.

[13] Annex A and Annex C use ATIS definitions from ATIS-1000013.2007, as modified by ATIS-1000013.a-2009, supplemented by definitions that are specific to WiMAX networks.

[14] *In the matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services, First Report and Order and Further Notice of Proposed Rulemaking*, ET Document No. 04-295, 20 FCC Rcd 14989 (2005).[2]

[15] *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services, Second Report and Order and Memorandum Opinion and Order*, ET Docket No. 04-295, 21 FCC Rcd 5360 (2006).[2]

[16] ATIS-1000013.2007 Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services.

[17] WiMAX Forum®, T32-001-R015v02 and T32-004-R015v01, "Architecture Tenets, Reference Model and Reference Points" Base Specification and Informative Annex, Release 1.5

[18] Annex D adopts the ASN.1 format directly from ATIS-1000013.a-2009.

[19] WiMAX Forum® T32-106-R015v01, "Architecture Tenets, Reference Model and Reference Points, WiMAX Broadband Access Lawful Intercept: Overview", Release 1.5.

[20] ATIS-1000013.a.2009 Supplement A to ATIS-1000013.2007 Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services.

[2] This document is available from the AskCALEA website at < http://www.askcalea.net >.

[3] This document is available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

[4] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < https://www.atis.org/docstore/default.aspx >

[21] ITU-T Recommendation X.690, Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguishing Encoding Rules (DER), July 2002.[3]

[22] IETF RFC 2131, Dynamic Host Configuration Protocol, March 1997.[4]

[23] IETF RFC 4960, Stream Control Transmission Protocol, September 2007.[4]

[24] IETF RFC 4340, Datagram Congestion Control Protocol (DCCP), March 2006.[4]

3. Definitions & Acronyms

3.1 Definitions

Access-Associated Communications Identifying Information (AACmII): *CmII* associated with communication between the subject and the IAS network for the purposes of login, logout, access authorization, access authentication, or resource allocation caused by the use of, or attempted use of, the WiMAX network by the subject.

WiMAX Network: See Section 2.1.29 of NWG Rel 1.0 Stage 2 Part 1 [17].

Access Service Network (ASN): See Section 2.1.2 of NWG Rel 1.0 Stage 2 Part 1 [17].

Connectivity Service Network (CSN): See Section 2.1.10 of NWG Rel 1.0 Stage 2 Part 1 [17].

Access Session: The interval during which the user is authorized to access the networks in the WiMAX. Packet data sessions occur within an access session.

Communication Content (CmC): The full IP packet streams to and from the subject.

Communication-Identifying Information (CmII): Information that identifies the origin, direction, destination, or termination of each communication generated or received by a subject by means of any equipment, facility, or service of a WiMAX-SP.

Communications Identifying Information can be one of two types:

1) Access Associated Communications Identifying Information; or
2) Content Associated Communications Identifying Information.

Communications Identifying Information is "reasonably available" to an IASP if it is present at an intercept access point and can be made available without the provider being unduly burdened with network modifications. CmII is delivered by the set of messages defined in this specification and the set of mandatory and conditional parameters contained therein.

Communication: Any wire or electronic communication, as defined in [4].

Content Associated Communications Identifying Information (CACmII): Communication Identifying Information associated with the delivery and routing of the subject's packets in the network (i.e., the headers of the IP packets).

Dynamic IP Address: An IP address that is temporarily assigned to a subscriber's equipment for a limited or specified duration.

Electronic Surveillance: The statutory-based legal authorization, process, and associated technical capabilities and activities of LEAs related to the interception of wire, oral, or electronic communications while in transmission. As used herein, also includes the acquisition of communication identifying information. As used herein, *surveillance* refers to a single communication intercept, pen register, or trap and trace. Its usage herein does not include administrative subpoenas for obtaining a subscriber's billing records and information about a subscriber's service that an LEA may employ before the start of a communication intercept, pen register, or trap and trace.

Full Content Broadband Intercept Order: Delivery of both CmC and AACmII information to LEA.

Intercept: Defined in [4] section 2510 (4) to be "the aural or other acquisition of the content of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."

Intercept Access Point (IAP): A point within an Internet Access and Services Provider domain where some of the communications or communications identifying information of an intercept subject's equipment, facilities, and services are accessed.

Intercept Subject: A WiMAX subscriber whose communications, communications identifying information, or both, have been authorized by a court to be intercepted and delivered to a Law Enforcement Agency. The identification of the intercept subject is limited to identifiers used

to access the particular equipment, facility, or communication service (e.g., network address, terminal identity, subscription identity).

Law Enforcement Agency (LEA): A government entity with the legal authority to conduct electronic surveillance (e.g., the Federal Bureau of Investigation or a state or local police department).

Limited Broadband Intercept Order: Delivery of only CmII (AACmII and CACmII)information to LEA, when authorized.

Location Information: Location information identifies the location of the subject's terminal

Packet: An IP packet [9, 10].

Packet Data Session: The interval during which the user is granted resources to send or receive packets to or from the WiMAX network. Packet data sessions occur within an access session.

Session: A set of multimedia senders and receivers and the data streams flowing from senders to receivers. Access Session and Packet Data Sessions are specific types of sessions.

Static IP Address: An IP address that is permanently assigned to a subscriber's equipment.

Stream: A set of IP packets sharing the same IP addresses and the IP next-layer protocol. The packets also share the same flow label if the protocol is IPv6 and layer-4 ports if the IP protocol is TCP, UDP, SCTP, or DCCP.

Subject: See *intercept subject*.

Subject Domain: The subject domain is composed of the intercept subject and the intercept subject's equipment and facilities. The intercept subject's equipment may include, but is not limited to, personal computers, PDAs, Mobile Station (MS), gaming equipment, hubs, routers, switches, firewalls, local wireless access points, and any other equipment used by the subject to access the Internet. The subject's facilities include, but are not limited to, all customer premise wiring and customer premise equipment (CPE), whether owned by the subject or provider, used to facilitate access to the Internet.

The physical equipment and facilities in the subject domain support the logical functions of registration (when required), reservation, and packet transfer to and from the Internet. The registration function may be a fixed capability between the CPE and provider equipment for some access capabilities.

Subscriber Identity: Uniquely identifies the subscriber to the WiMAX service. This is the alias used by the IASP to identify the intercept subject (e.g., userID, Service Acct ID, Charging User ID). There can be more than one form of identity used.

Surveillance: See *electronic surveillance*.

WiMAX Service Provider (WiMAX-SP): Operator of a WiMAX network providing access to physical facilities provided by the WiMAX network that allows the intercept subject to invoke and utilize services provided by an Internet service provider. The services could be provided by the WiMAX-SP or by a third party service provider (e.g., ISP).

3.2 Acronyms

AAA	Authorization, Authentication, and Accounting
AACmII	Access Associated CmII
ASN	Access Service Network
ANSI	American National Standards Institute
A-PDU *or* APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation One [5]
ATIS	Alliance for Telecommunication Industry Solutions
CACmII	Content Associated CmII
CALEA	Communications Assistance for Law Enforcement Act.
CF	Collection Function
CHAP	Challenge Handshake Authentication Protocol
CmC	Communication Content
CmII	Communication-Identifying Information.
CPE	Customer Premise Equipment
CSN	Connectivity Service Network
DCCP	Datagram Congestion Control Protocol
DHCP	Dynamic Host Configuration Protocol
DF	Delivery Function
FCC	Federal Communications Commission
GMT	Greenwich Mean Time
IAP	Intercept Access Point
IETF	Internet Engineering Task Force
IAS	Internet Access and Services
IP	Internet Protocol
LAES	Lawfully Authorized Electronic Surveillance
LEA	Law Enforcement Agency
LI	Lawful Intercept
MAC	Media Access Control
MF	Mediation Function
MOC	Mandatory Optional Conditional
MS	Mobile Station
PDU	Protocol Data Unit
RADIUS	Remote Authentication Dial In User Service
SCTP	Stream Control Transmission Protocol
TCP	Transmission Control Protocol [7]
UDP	User Datagram Protocol

4. WiMAX® ServicesDescription

4.1 WiMAX Services Model

The WiMAX LI Network Services Model is based on a combination of the ATIS Internet Access and Services model [16] and the WiMAX Network Reference Model [17]. The WiMAX LI Network Services Model consists of the following:

1. the Subject Domain involving the WiMAX subscriber's equipment; and
2. the WiMAX Network Services Provider's (NSP) Domain, serving the Subject, consists of:
   - an ASN(s); and
   - a CSN.

   For roaming situations, the WiMAX Visited Network consists of both an ASN(s) and a Visited CSN.

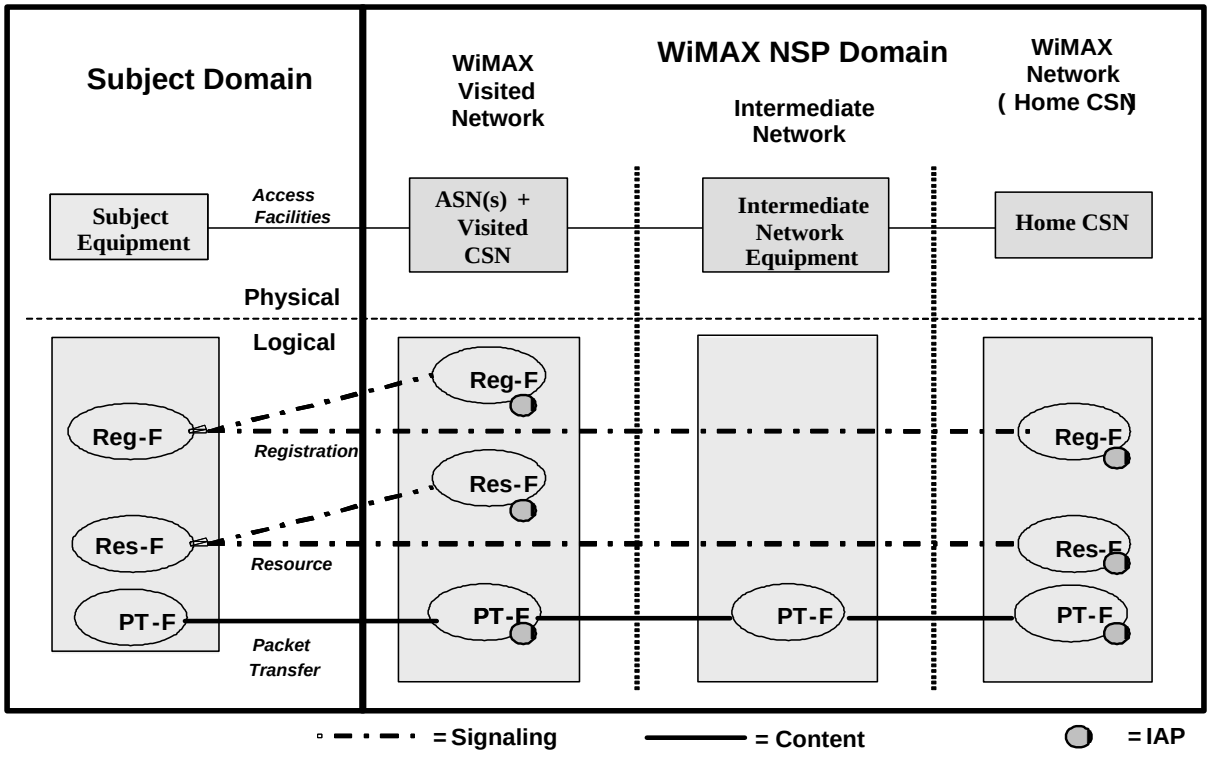

Figure 1– WiMAX LI Network Services Model

Description of components of Figure 1:

a. The following logical functions are presented in Figure 1:

- R*egistration Function (Reg-F)* – Registration for the purposes of this document is defined as any login or authentication process required of the subject by the service provider to gain access to the Internet.

- *Resource Function (Res-F)* – Resource reservation for the purposes of this document is defined as reserving resources (e.g., bandwidth) as necessary for access, and granting the subject access to the Internet. Resource reservation is recognized by providing the subject with one or more valid IP addresses, an IP address prefix or IP subnet address ranges that allow the subject to access the

Internet. Quarantined addresses, or addresses assigned for the purposes of registration are not included as resources assigned in the network.

- *Packet Transfer Function (PT-F)* - For the purposes of this document the packet transfer function is defined as the process of transferring Layer 3 IP packets to and from the WiMAX network. For packet transfer to occur, the subject needs to have completed Reg-F and Res-F if required. For the network to perform PT-F, the network elements need to be able to recognize the Layer 3 packet structure and be able to handle the packets. Only those network elements that recognize the Layer 3 packet structure (i.e., IP header fields) and handle the packets can perform the packet transfer function.

b. IAPs are possible Intercept Access Points. See section 6.1 Intercept Access Points.

4.2 General Surveillance Model

4.2.1 Electronic Surveillance Model

The functions needed to perform LAES are broadly categorized as access, delivery, collection, service provider administration, and law enforcement administration [12]. These functions are described herein without regard to their implementation. The relationship between these functional categories is shown in Figure 2. As shown, the Access Function (AF), Delivery Function (DF), and WiMAX-SP Administration Function are the responsibility of the WiMAX-SP, and the Collection Function (CF) and Law Enforcement Administration Function are the responsibility of the LEA. The use of these functions to perform an interception is initiated by receipt of a specific lawful authorization.

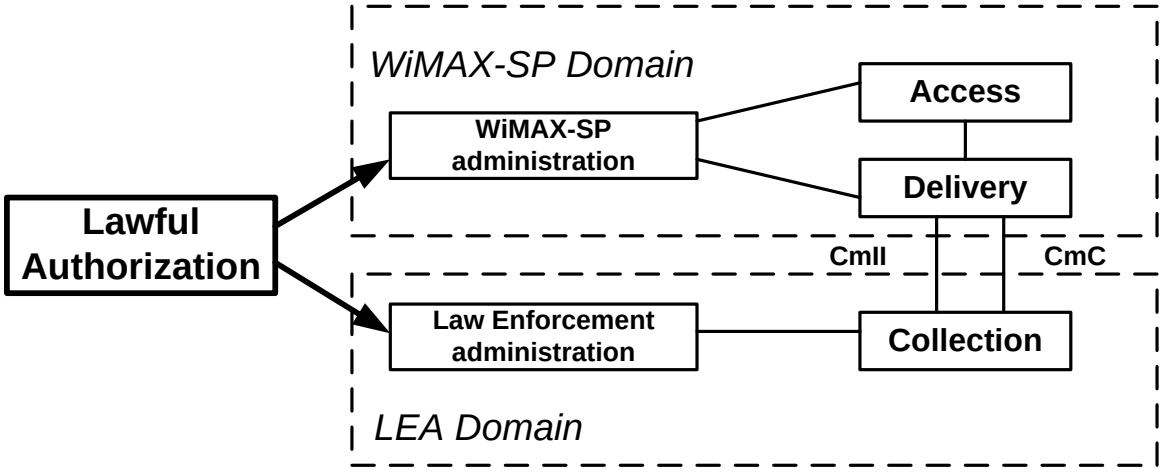

Figure 2 – Electronic Surveillance Model

The *Access Function*, consisting of one or more Intercept Access Points (IAPs), accesses and intercepts an intercept subject's CmC and CmII unobtrusively. The IAPs may vary between WiMAX-SPs.

The *Delivery Function* delivers intercepted communications to one or more CFs. The DF shall deliver intercepted communications in the form of CmC and CmII.

The *Collection Function* collects and analyzes the CmC and CmII received from the DF. It is defined to be the location where lawfully authorized intercepted CmC and CmII is collected by a LEA.

The *WiMAX-SP Administration Function* controls the IASP's AF and DF.

The *Law Enforcement Administration Function* controls the LEA's CF.

4.2.2 Intercept Access Points

With respect to WiMAX, IAPs) are places in the network where lawful intercept WiMAX CmII and CmC are intercepted. There are two fundamental types of WiMAX IAPs:

1. WiMAX Communication Identifying Information IAPs (CmII-IAPs); and
2. WiMAX Communication Content IAPs (CmC-IAPs).

CmII-IAPs and CmC-IAPs are associated with CmII and CmC intercept functions respectively that perform the actual interception of CmII and CmC. These CmII and CmC intercept functions are incorporated into one or more network elements. CmII and CmC intercept functions may be collocated within the same network element, or may be distributed among many network elements. The interfaces for transport of CmII and CmC information from the CMII and CMC IAPs to the LI Delivery Function is outside the scope of the WiMAX specifications.

4.2.2.1 CmII-IAPs

A CmII-IAP captures the information necessary to generate CmII. CmII may be categorized as Access Associated CmII (AACmII) or Content Associated CmII (CACmII).

a. *Access Associated CmII*: CmII associated with communication between the subject and the WiMAX-SP domain for the purposes of login, logout, access authorization, access authentication, or resource allocation caused by the use of, or attempted use of, the WiMAX network by the subject. All AACmII signaled between the subject and the network shall be reported to law enforcement.

b. *Content Associated CmII*: CmII associated with the delivery and routing of the subject's content in the network, derived from specific fields in the Layer 3 headers and Layer 4 headers of the IP packets as defined in 6.2.11 and 6.2.12. Two options exist for delivering CACmII:

- Delivering the records for the specified header fields of each intercepted packet to law enforcement; or
- Delivering summary records

4.2.2.2 CmC-IAPs

A CmC-IAP intercepts the full packets to and from an intercept subject.

The CmC-IAP intercepts the subject's content and presents it to the DF or to the Mediation Function (MF) [16]. The CmC-IAP can reside in a number of places. The CmC-IAP used in a WiMAX network is an WiMAX-SP design decision.

5. WiMAX® Subject Identification

The subject's access to the WiMAX services can be divided into two categories defined by the way the subject activity is identified in the network.

5.1 Login Identifier

The subject is uniquely identified through a login process. As a result of a successful login process, an intercept may be based on information, such as:

- A single IP address, a set of IP addresses or an IP subnet/IP prefix assigned to the subject at login;
- Account-session-id assigned to the subject's session at login; or
- The subject's Charging User Identifier (CUI).

Note that in the case of multiple logins by the subject, multiple cases of the above conditions may be required for the same subject.

When subject activity is identified in the network through login identification, the subject (or subject's equipment) may be required to transmit and receive "signaling" packets – e.g., Challenge Handshake Authentication Protocol (CHAP) packets and CHAP v2 packets – to perform Registration Function (Reg-F) and Reservation Function (Res-F) in order to gain access (e.g., authentication and authorization) to the network and to receive resources (e.g., IP address). Interception of the subject CmII and CmC is available only after the subject has been identified in the network. Signaling prior to the identification of the subject in the network, or during the period when a subject's equipment has been placed in this "quarantine" state, cannot be intercepted as the subject has not been identified in the network.

5.2 Equipment Identifier

The subject is identified through an address or interface that uniquely identifies the subject's equipment or session. The intercept resulting from equipment identification may be based on information such as:

- MAC address or set of MAC addresses associated with the subject's equipment;
- Static IP address, which could be a single IP address, a set of IP addresses or an IP subnet/IP prefix assigned to the subject's equipment;

Note that in some cases the subject may be associated with multiple equipment identifiers.

When subject activity is identified in the network through equipment identification, login AACmII may not be available.

6. User Perspective

6.1 Introduction

Section6 presents the user perspective requirements for LAES for WiMAX-SP network. The user in this case is the LEA.

Section 6.2 presents communication-related events that represent or generate communication-identifying information (termed "surveillance events") in the WiMAX-SP network.

Section 6.3 presents general capabilities needed for LAES for IAS.

6.2 Surveillance Events

This clause presents surveillance events that cause CmII to be reported. The events are based on ATIS-1000013.2007 [16], as modified by ATIS-1000013.a.2009 [20].

6.2.1 Access Attempt

This event occurs when Authentication, Authorization and Accounting (AAA) or Mobile IP registration detects an intercept subject attempting to enter or re-enter a WiMAX network.

6.2.2 Access Accepted

This event occurs when the intercept subject or associated CPE network device has successfully authenticated with the network AAA server, or Home Agent (or functional equivalent).

If the WiMAX-SP allows multi-login, where the same user identity and password is used multiple times to establish multiple concurrent and distinct access sessions, separate Access Accepted events shall be provided for each session.

6.2.3 Access Failed

This event occurs when network authentication has failed and an access session has not been successfully established.

6.2.4 Access Session End

This event occurs when the intercept subject's access has been disconnected and the access session is terminated. The following are example cases:

- The intercept subject initiates a disconnect request to the network;
- The subscriber equipment experiences a loss of power; or
- The network terminates the session due to expiration of timers or loss of signal to subject.

6.2.5 Access Rejected

This event occurs when an intercept subject's login procedure (authentication or authorization) to the network is successfully completed, but the intercept subject's access attempt is rejected for other reasons. The following is an example case:

- The Access Rejected message would be generated when a subject is already logged on, attempts a second login with a valid ID and password, but the network does not allow multiple logins.

6.2.6 Access Signaling Message Report

This event occurs when the IP network receives a signaling message from the intercept subject, sends a signaling message to the intercept subject, or sends or receives a signaling message on behalf of the

intercept subject. This message is used to encapsulate and send these access signaling messages -- e.g., Remote Authentication Dial In User Service (RADIUS[5]), or Diameter[6] - detected in the network.

The Access Signaling Message Report is used for extensibility and in lieu of the access messages described in 9.2.1 through 9.2.5 when information or events cannot be mapped into those messages. Appropriateness of the use of the Access Signaling Message Report for reporting AACmII depends on the interception and service architectures of the network.

6.2.7 Packet Data Session Start

This event occurs when a subject, or the subject's equipment, successfully completes any login process required by the network and whenever one or more IP addresses or prefixes/subnets are assigned to the subject's equipment.

6.2.8 Packet Data Session Failed

This event occurs when an intercept subject's login procedure to the network is successfully completed, but the intercept subject is denied access to the network. An example of this is:

- When the IP addresses or other network resources to accommodate the subject's use of the network are not available.

6.2.9 Packet Data Session End

This event occurs when an intercept subject's equipment ends a packet data session with the network. In cases in which the intercept is based on a subject's IP addresses or prefixes/subnets that are allocated dynamically (see clause 6.3.13), the Packet Data Session End event is considered to occur, and shall be reported, in the following cases:

- The IP address associated with a packet data session is explicitly released (e.g., by a DHCPRELEASE [Ref 22], Mobile IP of session release).

- The IP address associated with a packet data session is no longer assigned to the subject. This may include the following situations:

- The WiMAX network terminates a subject's session after a pre-established time period or inactivity period (e.g., a DHCP lease expiration)..

- The WiMAX network terminates the subject's session for other reasons (e.g., resource condition or administrative controls).

- The WiMAX network detects the intercept subject's equipment disruption of connectivity (e.g., loss of physical layer or data link layer) and after a specified time, terminates the subject's packet data session.

6.2.10 Packet Data Session Already Established

This event occurs when surveillance begins on an intercept subject's communications for any packet data session of the intercept subject that is already established[7], regardless of whether the intercept subject is actively transmitting or receiving packets, as in the following examples:

---

[5] For more information, see IETF RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*. This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

[6] For more information, see IETF RFC 3588, *Diameter Base Protocol*. This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

[7] There are a number of approaches to determine whether the subject's packet data session has already been established. One approach is to obtain the subject's session status by contacting service provider's user login database (e.g., RADIUS log records). In this approach, the determination of Packet Data Session Already Established relies on the completeness of Res-F. In another

- Lawful electronic surveillance commences on an intercept subject who already has an established access session with the subscribed-to WiMAX-SP (e.g., the login event may have occurred prior to surveillance starting), whether or not the intercept subject is actively transmitting or receiving packets at the time..

- Lawful electronic surveillance commences on an intercept subject who is identified by an equipment identifier (as described in 5.2) and delivery of either CmC or CACmII is initiated.

6.2.11 Packet Data Header Report

This event is used to provide CACmII packet header reports on a per packet basis (non-summarized reporting). The event is triggered by each packet of a packet stream sent or received by the subject. The report event provides source and destination information derived from the packet headers for each packet. IP addresses and the IP next-layer protocol are always reported, the flow label is reported if the packet is IPv6, and the layer-4 ports are reported if the IP protocol is TCP, UDP, SCTP [Ref 23], or DCCP [Ref 24].

6.2.12 Packet Data Summary Report

This event is used to provide CACmII summary reports . The event may be triggered by the start of a packet stream, interim report of a packet stream, or end of a packet stream. An interim report can also be triggered by: a) expiration of a timer; b) reaching a count limit; or c) a change in information being counted (e.g., the IP Address being counted changes). The report event provides source and destination information derived from the packet headers and summary information for the number of packets destined to or originated by the subject. IP addresses and the IP next-layer protocol are always reported, the flow label is reported if the packet is IPv6, and the layer-4 ports are reported if the IP protocol is TCP, UDP, SCTP [Ref 23], or DCCP [Ref 24].

The Packet Data Summary Report can be used as the single reporting event for CmII associated with IP headers from subscriber content when reporting the information in other events would be redundant.

Packet Data Summary Reports are reported per IAP.

6.2.13 ServingSystem Event Reporting for Terminal Registration

The serving system identification information includes the identity of the current system assigned to provide service for the MS. Information regarding the occurrence of the event (e.g., identity of the system providing the intercept access, time, date, and MS location information) should be included.

The ServingSystem event message shall be used to report the serving system identity currently serving the intercept subject (i.e., resulting from MS registration).

6.2.14 Dynamic IP Address Management

This section applies to situations where packets are isolated based on IP addresses. It is essential to track the assignment and release of dynamic IP addresses so the communications of the intercept subject are not missed and only the communications of the intercept subject are captured. The Packet Data Session Already Established event (clause 6.2.10) can report the current dynamic IP addresses of an intercept subject when the WiMAX-SP determines that the subject has already been assigned one or more dynamic IP addresses prior to the start of the intercept.

---

approach, the IAP uses the equipment identification to identify the subject and intercepts the subject's packets. The IAP then determines that the packet data session has already been established when data packets are intercepted.

6.3 General Requirements

6.3.1 Subject Communications

The WiMAX-SP shall insure that the complete communications (i.e., full packet stream to and from the subject's equipment under a full content order, or packet headers to and from the subject's equipment under an order that requires only the delivery of CmII) of the subject are intercepted.

6.3.2 Communications Delivery

Various delivery methods and associated technologies can be used to support the communications delivery interface between an WiMAX-SP and law enforcement. These delivery methods carry the CmII and CmC defined in this specification. Arrangement for these delivery methods (e.g., TCP/IP, UDP/IP) and the underlying technologies (e.g., private T1, internet, Ethernet/fiber) are made between the WiMAX-SP and the LEA and accordingly affect information carried in the CmC delivery header and the timeliness of the delivered CmII and CmC.

The format for delivery of CmII across the communications delivery interface is specified in Annex A.1. The format for delivery of CmC across the communications delivery interface is specified in Section 8 and Annex D.

6.3.3 Timing Requirements

6.3.3.1 Timing Requirements for CmII

Timing information includes two elements:

a. Event Time-stamp: Each surveillance message shall contain a time-stamp that is recorded within a specific amount of time from when the event triggering the surveillance message was detected (i.e., the time difference between the time the CmII triggering event was detected and the time recorded in the time-stamp).

b. *Event Timing*: Surveillance messages shall be sent to the LEA within a defined amount of time after the information pertaining to the CmII triggering event is available at the IAP. The preferred precision is in milliseconds when reasonably available.

The following timing requirements shall apply to the delivery of CmII:

- Each surveillance message shall be sent by the DF to the CF within eight (8) seconds of receipt by the IAP of the information pertaining to the CmII triggering event at least 95% of the time.
- Each surveillance message shall contain a time-stamp that is within 200 milliseconds from when the CmII event triggering the surveillance message was detected. The time-stamp shall include a Greenwich Mean Time (GMT) offset, if available.

6.3.3.2 Timing Requirements for CmC

The following timing requirements shall apply to the delivery of CmC:

- Time-stamps shall be provided with encapsulated intercepted packets delivered to the CF, unless timing is provided by other means such as a guaranteed method for timely delivery of content from access to the delivery function, in which case timestamping may occur at the delivery function.

6.3.4 Performance and Quality

The WiMAX-SP shall be capable of performing multiple intercepts per subject.

The WiMAX-SP shall be capable of performing intercepts on multiple subjects.

The WiMAX-SP shall be capable of performing intercepts for multiple LEAs for the same subject. The intercepts shall not be detectable among LEAs.

The quality of the communication delivery interface is defined by the negotiation between the WIMAX-SP and the LEA.

6.3.5 Security and Reliability over the interface between DF and CF

The equipment, facilities or services for delivering CmII and CmC over the interface between DF and CF are procured by the LEA, and their specifications are outside the scope of this Standard. Security and reliability are a function of those equipment, facilities, or services procured (e.g., private line, public internet, point-to-point). The WiMAX-SP shall offer method, appropriate to the equipment, facilities, or services procured to provide a high level of confidence that the intercepted CmII and CmC are delivered to the LEA securely and reliably. For example, a hashing method can be used for this purpose.

6.3.5 Encryption and Compression

If the WiMAX-SP uses encryption in the network, the WiMAX-SP shall deliver the intercepted data to the LEA in unencrypted form or provide the encryption keys and specify the encryption method. If the intercepted data is available at the IAP in both encrypted form and unencrypted form, the WiMAX-SP shall provide it to the LEA in unencrypted form.

If the WiMAX-SP uses compression in the network, the WiMAX-SP shall deliver the intercepted data to the LEA in uncompressed form, or identify the means to decompress. If the intercepted data is available at the IAP in both compressed form and uncompressed form, the WiMAX-SP shall provide it to the LEA in uncompressed form.

6.3.6 Isolation

While the intercept is active, the WiMAX-SP shall ensure that only authorized communications are intercepted, according to the surveillance order served.

The WiMAX-SP shall ensure that only communications associated with the subject's equipment are intercepted. Communications not associated with the subject's equipment, facilities, or services shall not be delivered to the LEA.

6.3.7 Privacy and Authentication

The WIMAX-SP shall not monitor or permanently record the subject communications.

The WIMAX-SP shall ensure that the captured communication originates from or is directed to the subject's equipment, facilities, or service.

6.3.8 Transparency

The WiMAX-SP shall perform the intercept in such a manner that the subject or the subject's terminal equipment cannot reasonably detect that the intercept is being performed.

The intercept shall be transparent to all non-authorized employees of the WiMAX-SP as well as to all other non-authorized persons.

Nothing, from the subject's point of view, should be detectable as the result of LI. The subject's service parameters shall not be impacted by the intercept in such a way that the surveillance is detectable. Note that replication of packets may cause some latency, but this latency should not be reasonably detectable by the subject.

6.3.9 Correlation

The WiMAX-SP shall ensure that the intercepted information is correlated to the appropriate type of intercept order (i.e., "limited" or "full content"), for a subject. When multiple intercept orders exist for the same subject, the reporting of each order is correlated to the specified type of intercept order.

6.3.10 Location Information Reporting

When location information is lawfully authorized and is reasonably available, the WiMAX Network shall report location type and the actual location. The WiMAX Network may report multiple sets of location information, for example:

locationType = ”name”, location = ”MyWiFiHotSpot”,

locationType = ”streetaddress”, location = ”100 First Street”,

locationType = ”IP”, location = ”255.255.255.255”.

The level of detail of the reported location information should be commensurate with the level of detail of the location information reasonably available at the IAP.

6.3.11 Handling of Tunneled Packets

There are a variety of circumstances and protocols where the intercept subject’s packets are tunneled by the WIMAX-SP (i.e., encapsulated within a packet that typically has different IP addresses). For a WiMAX-SP’s tunnel carrying an intercept subject’s packets, if that WiMAX-SP’s tunnel is originated or terminated in the WiMAX-SP’s network, interception shall be performed on the subject’s packets.

7. Network Perspective

7.1 Introduction

This clause identifies messages, describes the information to be reported for each WiMax CmII message, and describes the application level CmC delivery format and associated delivery information.

7.2 Definitions for "Mandatory," "Optional," and "Conditional" Parameters

The value in the Mandatory/Optional/Conditional (MOC) column in the Message Parameter tables in this document indicates whether inclusion of the indicated parameter in the indicated message is *Mandatory* (M), *Optional* (O), or *Conditional* (C).

- A *Mandatory (M)* value means that the sender of the message shall always include this parameter in the message.
- An *Optional (O)* value means that the sender of the message may include this parameter in the message.
- A *Conditional (C)* value means that the sender of the message shall include this parameter in the message when the criteria specified in the *Conditions* column are met.

7.3 Message Reporting

The messages and associated information listed in this clause are reported as specified in ATIS-1000013.2007 [16], as modified by ATIS-1000013.a.2009 [20] unless otherwise noted.

7.3.1 Access Attempt Message

See ATIS-1000013.2007 6.2.1 [16].

7.3.2 Access Accepted Message

See ATIS-1000013.2007 6.2.2 [16], as modified by ATIS-1000013.a.2009 [20].

7.3.3 Access Failed Message

See ATIS-1000013.2007 6.2.3 [16], as modified by ATIS-1000013.a.2009 [20].

7.3.4 Access Session End Message

See ATIS-1000013.2007 6.2.4 [16], as modified by ATIS-1000013.a.2009 [20].

7.3.5 Access Rejected Message

See ATIS-1000013.2007 6.2.5 [16], as modified by ATIS-1000013.a.2009 [20].

7.3.6 Access Signaling Message Report Message

See ATIS-1000013.2007 6.2.6 [16].

7.3.7 Packet Data Session Start Message

See ATIS-1000013.2007 6.2.7 [16], as modified by ATIS-1000013.a.2009 [20].

7.3.8 Packet Data Session Failed Message

See ATIS-1000013.2007 6.2.8 [16].

7.3.9 Packet Data Session End Message

See ATIS-1000013.2007 6.2.9 [16], as modified by ATIS-1000013.a.2009 [20].

7.3.10 Packet Data Session Already Established Message

See ATIS-1000013.2007 6.2.10 [16], as modified by ATIS-1000013.a.2009 [20].

7.3.11 Packet Data Header Report Message

See ATIS-1000013.2007 6.2.11 [16], as modified by ATIS-1000013.a.2009 [20].

7.3.12 Packet Data Summary Report Message

See ATIS-1000013.2007 6.2.12 [16], as modified by ATIS-1000013.a.2009 [20].

7.4 Additional Message Reporting

The messages in this clause are to be reported in addition to the ones specified in clause 7.3. The Information Element definitions (e.g. Case Identity, IAP System Identity, Location Information) are as specified in Section 6.1.1 of ATIS-1000013.2007 [16], as modified by ATIS-1000013.a.2009 [20].

7.4.1 ServingSystem Event Reporting for Terminal Registration

As defined in this Specification, the ServingSystem Event is used to report terminal registration. The ServingSystem Message shall be triggered when:

- the MS is authorized for service.

The 'SystemIdentity' parameter is used to report the serving system identity.

Table 1 – ServingSystem Message Parameters for Terminal Registration

Information Element	M/O/C	Conditions
Case Identity	M	
IAP System Identity	M	
Time Stamp	M	
Subscriber Identity	M	
SystemIdentity	C	Include when reasonably available to identify the WiMAX-SP.
Location Information	C	Provide when reasonably available and lawfully authorized.

8. CmC Delivery

Delivery of CmC for WiMAX® Internet Access is based on the Abstract Syntax Notation One (ASN.1) CmC delivery method in the ATIS Internet Access and Services standard [16], as modified by ATIS-1000013.a.2009 [20]. See Annex D. in this specification for the ASN.1 delivery format for WiMAX CmC delivery.

ANNEX A. (Normative)

A.1 ASN.1 Definitions

This annex provides the Abstract Syntax Notation One (ASN.1) [5] definitions for this specification. CmII and CmC corresponding to ASN.1 definitions shall be encoded according to Basic Encoding Rules (BER) [Ref 21].

A.1.1 WiMAX CmII Abstract Syntax Module

```
WiMAX-LAES-CmII-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wimax(3) cmii(0) version-2(1)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

Access-Attempt,
Access-Accepted,
Access-Failed,
Access-Session-End,
Access-Rejected,
Access-Signaling-Message-Report,
Packet-Data-Session-Start,
Packet-Data-Session-Failed,
Packet-Data-Session-End,
Packet-Data-Session-Already-Established,
Packet-Data-Header-Report,
Packet-Data-Summary-Report,
CaseIdentity,
IAPSystemIdentity,
Location,
SubscriberIdentity,
TimeStamp,
Value
FROM IAS-LAES-CmII-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-ias(1) cmii(0) version-2(1)};

wimax-LAES-CmII-Abstract-Syntax-Module-OID OBJECT IDENTIFIER ::=
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wimax(3) cmii(0) version-2(1)}

wimax-CmII-Protocol-Identifier OBJECT IDENTIFIER ::= {wimax-LAES-CmII-Abstract-Syntax-Module-
OID}

WiMAXProtocol ::= SEQUENCE
{
    wimax-CmII-Protocol-Identifier   OBJECT IDENTIFIER,
    wimaxMessage                     WiMAXMessage
}
```

```
WiMAXMessage ::= CHOICE {
    access-Attempt                      [0] Access-Attempt,
    access-Accepted                     [1] Access-Accepted,
    access-Failed                       [2] Access-Failed,
    access-Session-End                  [3] Access-Session-End,
    access-Rejected                     [4] Access-Rejected,
    access-Signaling-Message-Report     [5] Access-Signaling-Message-Report,
    session-Start                       [6] Packet-Data-Session-Start,
    session-Failed                      [7] Packet-Data-Session-Failed,
    session-End                         [8] Packet-Data-Session-End,
    session-Already-Established         [9] Packet-Data-Session-Already-Established,
    data-Header-Report                  [10] Packet-Data-Header-Report,
    data-Summary-Report                 [11] Packet-Data-Summary-Report,
    serving-System                      [12] ServingSystem
}

-- WiMAX Message Definitions

ServingSystem  ::=  SEQUENCE
{
    caseId                  [0] CaseIdentity,
    iAPSystemId             [1] IAPSystemIdentity,
    timestamp               [2] TimeStamp,
    subscriberIdentity      [3] SubscriberIdentity,
    systemIdentity          [4] SystemIdentity          OPTIONAL,
    locationInformation     [5] Location                OPTIONAL,
   ...
}

-- WiMAX Parameter Definitions

SystemIdentity ::= Value

END  -- WiMAX-LAES-CmII-Abstract-Syntax-Module
```

ANNEX B. Reliable Delivery (Informative)

It is important that intercept information be delivered in as reliable and robust a way possible from DF to law enforcement. To this end, there are a number of suggested mechanisms.

B.1 Short-Term Pull Buffering

ATIS-1000021 "Data Buffering (Short Term Storage) in an Internet Access and Services LAES Environment"[8] defines a mechanism where CmII and CmC are stored in files rather than being transported in real time. The files and their contents are described in detail in ATIS-100021 as well as the mechanisms to determine how often files are created and for accessing them. In summary, within a case, CmII is stored as ASN.1 messages, CmC is stored in Packet CAPture (PCAP) format, and log files provide auxiliary information, such as hashes of the CmII and CmC files. The LEA CF uses Secure Shell version 2 (SSH2) and Secure FTP (SFTP) to pull the files out, and may then verify hashes before deleting the files. SSH2 and SFTP provide the LEA with strong authentication and encryption. The specifics of the PCAP format used is also defined in ATIS-1000021.

B.2 Short-Term Push Buffering

An alternative mechanism may be created where the DF builds CmII and CmC files and "pushes" them up to the CF using SSH2 and SFTP. The specifics about file formats, file naming conventions, and file granularity (how often a new file is started) can be taken directly from ATIS-100021. Push buffering generally requires less storage space outside of the CF; it is recommended that transmission of intercept files be specifiable with a range of time values, with a maximum of at least 15 minutes, and with a range of size values, with a maximum of at least 10 MB. With push buffering, having a separate hash file per intercept file (rather than the log file) is preferable, but one should use at least the strength of hash specified in ATIS-1000021 (SHA-256).

[8] See ATIS-1000021-2007 Data Buffering (Short Term Storage) in an Internet Access and Services LAES Environment. < http://www.atis.org >

ANNEX C. Optional Messages (Informative)

C.1 Optional Surveillance Status Messages

The following optional messages as defined in Annex C.1 of ATIS-1000013.2007 [16], as modified by ATIS-1000013.a.2009 [20] are also defined for usage of WiMAX LI at the option of the WiMAX-SP:

C.1.1 Service Change

C.1.2 Virtual Private Network (VPN) Security Association Establishment

C.1.3 Virtual Private Network (VPN) Security Association Release

C.1.4 Surveillance Activation

C.1.5 Surveillance Continuation

C.1.6 Surveillance Change

C.1.7 Surveillance Deactivation

Events C.1.1.4-7 are used to provide surveillance status reports.

If the surveillance status report is used as a heartbeat, AND if no packets were detected for the duration of the summary timer, then the Packet Data Summary Report shall not be sent.

If the Surveillance Status Report is not used as a heartbeat mechanism, then null Packet Data Summary Reports shall be sent at the expiration of the Summary Timer.

The Surveillance Status Report should be sent to an LEA when a WiMAX-SP activates or deactivates a surveillance for a subject, when there is a change in status of a surveillance (e.g., partial or complete failure of upstream functions) and on a periodic basis to report that surveillance is still active (i.e., a “heartbeat”). The heartbeat is configurable in minutes and should not exceed ten minutes.

C.2 WiMAX CmII Optional Messages Abstract Syntax Module

```
WiMAX-LAES-CmII-Optional-Messages-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wimax(3) optional-cmii(1) version-2(1)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

ServiceChange,
VPNSecurityEstablishment,
VPNSecurityRelease,
SurveillanceActivation,
SurveillanceContinuation,
SurveillanceChange,
SurveillanceDeActivation
FROM IAS-LAES-CmII-Optional-Messages-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-ias(1) cmii-optional(2) version-2(1)};

wimax-LAES-CmII-Optional-Messages-Abstract-Syntax-Module-OID OBJECT IDENTIFIER ::=
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wimax(3) optional-cmii(1) version-2(1)}
```

```
wimax-CmII-Optional-Protocol-Identifier OBJECT IDENTIFIER ::=
{wimax-LAES-CmII-Optional-Messages-Abstract-Syntax-Module-OID}

WiMAXOptionalProtocol ::= SEQUENCE
{
    wimax-CmII-Optional-Protocol-Identifier   OBJECT IDENTIFIER,
    wimaxOptionalCmIIMessage                  WiMAXOptionalCmIIMessage
}

WiMAXOptionalCmIIMessage ::= CHOICE
{
    serviceChange                             [0] ServiceChange,
    vpnSecurityEstablishment                  [1] VPNSecurityEstablishment,
    vpnSecurityRelease                        [2] VPNSecurityRelease,
    surveillanceActivation                    [3] SurveillanceActivation,
    surveillanceContinuation                  [4] SurveillanceContinuation,
    surveillanceChange                        [5] SurveillanceChange,
    surveillanceDeActivation                  [6] SurveillanceDeActivation
}

END  -- WiMAX-LAES-CmII-Optional-Messages-Abstract-Syntax-Module
```

ANNEX D. Intercepted Communication Content Delivery (Normative)

D.1 WiMAX CmC Delivery Format

The ASN.1 in this annex is defined for the delivery of WiMAX CmC to the LEAs.

D.2 WiMAX CmCC Abstract Syntax Module

```
WiMAX-LAES-CmCC-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wimax(3) cmcc(2) version-2(1)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

IAS-CC-APDU
FROM IAS-LAES-CmCC-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-ias(1) cmcc(1) version-2(1)};

wimax-LAES-CmCC-Abstract-Syntax-Module-OID OBJECT IDENTIFIER ::=
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wimax(3) cmcc(2) version-2(1)}

wimax-CmCC-Protocol-ID OBJECT IDENTIFIER ::= {wimax-LAES-CmCC-Abstract-Syntax-Module-
OID}

WiMAX-CC-APDU ::= IAS-CC-APDU

END  -- WiMAX-LAES-CmCC-Abstract-Syntax-Module
```

ANNEX E. Canadian Location Reporting (Normative)

E.1 Location information reporting

Additional location information reporting beyond the basic capabilities provided in this specification (see section 7.0) may be required to meet Canadian regulator requirements or operator license requirements. A Location_Update message is defined in this annex to be used in conjunction with the other LAES reporting messages in this specification to report the location of the intercept subject.

The Location_Update message may be triggered by events such as the following:

- when an event is detectable in the network at an IAP and when location information is reasonably available at an IAP: or
- the mobile terminal is powered up and a connection is made to the wireless network; or
- the mobile terminal is powered down and is disconnected from the wireless network; or
- the mobile terminal is entering a new location area (e.g., normal location update); or
- the mobile terminal periodically provides an update of its location while connecting to the wireless network (e.g., periodic location update); or
- location information is available via location services or presence services; or
- location information is available at a shared Network Access Provider (NAP).

Note that IAP placement and where and when events are detected are implementation dependent.

E.1.1 Location_Update message definition

The Location_Update message is defined as specified in Table 2.

Table 2 – Location_Update Message

Information Element	MOC	Conditions
CaseIdentity	M	
IAPSystemIdentity	C	Provide when known.
ObservedSubjectIdentities	C	Provide when known.
TimeStamp	M	
Location_Information	M	

E.1.2 Location_Update message information elements definitions

The following information elements are defined for use with the Location_Update message:

1) C**ase Identity** – Identifies the case.
2) **IAP System Identity** – Identifies the network element containing the IAP.
3) **Observed Subject Identities** – Identities of the subject observed at the IAP (e.g., International Mobile Subscriber Identity (IMSI), Mobile Station ID (MSID), Simple Internet Protocol Uniform Resource Locator (SIP URL), User Name)

4) **Time Stamp** – Identifies the date and time of the Location_Update event.

5) **Location Information** – Location information associated with the intercept subject. The location information consists of the following information fields:

   a) **Location Type** – The type of the location reported (e.g., "Type = BS ID", "Type = geo coordinates").

   b) **Location** – The actual location (e.g., "BS ID = 10").

   c) **Time of Location** – The time the location was recorded if different from the time of the Location_Update event.

E.1.3 Location _Message ASN.1

```
Canadian-Messages-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wimax(3) canadian-cmii(3) version-2(1)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

CaseIdentity,
IAPSystemIdentity,
TimeStamp
FROM IAS-LAES-CmII-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) t1-ias(1) cmii(0) version-2(1)};

canadian-messages-OID OBJECT IDENTIFIER ::=
{iso(1) member-body(2) us(840) tia(113737) laes(2) t1(1) wimax(3) canadian-cmii(3) version-2(1)}

CanadianProtocol ::= SEQUENCE {
   protocolIdentifier        OBJECT IDENTIFIER (canadian-messages-OID),
   messages                  CanadianMessages
}

CanadianMessages ::= CHOICE {
    Location-update          [1] Location-Update
}

-- Message Definitions

Location-Update ::= SEQUENCE {
      caseId                 [0]  CaseIdentity,
      iAPSystemId            [1]  IAPSystemIdentity              OPTIONAL,
      observedSubjectIDs     [2]  ObservedSubjectIdentities      OPTIONAL,
      timestamp              [3]  TimeStamp,
      location-Information   [4]  Location-Information
}

-- Information Elements Definitions

Location-Information ::= SEQUENCE
{
      locationType           [0]  UTF8String,
      location               [1]  UTF8String,
      locationTime           [2]  TimeStamp                      OPTIONAL
}

ObservedSubjectIdentities ::= SET OF UTF8String

END  -- Canadian-Messages-Abstract-Syntax-Module
```

E.2 Delivery over the communications delivery interface

Delivery of CmII and CmC should be via a reliable delivery method. The specifics of the method for delivery over the communication delivery interface are determined by WiMAX-SP and LEA arrangements (See Section 6.3.7).