TIA STANDARD

Lawfully Authorized Electronic Surveillance (LAES) for cdma2000® Wireless LAN (WLAN)-Interworking

TIA-1118 **December 2009**

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
tiaonline.org

NOTICE

TIA Engineering Standards and Publications are designed to serve the public interest through eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for their particular need. The existence of such Standards and Publications shall not in any respect preclude any member or non-member of TIA from manufacturing or selling products not conforming to such Standards and Publications. Neither shall the existence of such Standards and Publications preclude their voluntary use by Non-TIA members, either domestically or internationally.

Standards and Publications are adopted by TIA in accordance with the American National Standards Institute (ANSI) patent policy. By such action, TIA does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the Standard or Publication.

This Standard does not purport to address all safety problems associated with its use or all applicable regulatory requirements. It is the responsibility of the user of this Standard to establish appropriate safety and health practices and to determine the applicability of regulatory limitations before its use.

(From Project No. 3-0304-B-1, formulated under the cognizance of the TIA TR-45 Mobile & Personal Communications Systems, TR-45.8 Subcommittee on Core Networks Technology).

Published by

©TELECOMMUNICATIONS INDUSTRY ASSOCIATION
Standards and Technology Department
2500 Wilson Boulevard
Arlington, VA 22201 U.S.A.

PRICE: Please refer to current Catalog of
TIA TELECOMMUNICATIONS INDUSTRY ASSOCIATION STANDARDS AND ENGINEERING PUBLICATIONS
or call IHS, USA and Canada
(1-877-413-5187) International (303-397-2896)
or search online at http://www.tiaonline.org/standards/catalog/

NOTICE OF DISCLAIMER AND LIMITATION OF LIABILITY

The document to which this Notice is affixed (the "Document") has been prepared by one or more Engineering Committees or Formulating Groups of the Telecommunications Industry Association ("TIA"). TIA is not the author of the Document contents, but publishes and claims copyright to the Document pursuant to licenses and permission granted by the authors of the contents.

TIA Engineering Committees and Formulating Groups are expected to conduct their affairs in accordance with the TIA Engineering Manual ("Manual"), the current and predecessor versions of which are available at http://www.tiaonline.org/standards/procedures/manuals/TIA's function is to administer the process, but not the content, of document preparation in accordance with the Manual and, when appropriate, the policies and procedures of the American National Standards Institute ("ANSI"). TIA does not evaluate, test, verify or investigate the information, accuracy, soundness, or credibility of the contents of the Document. In publishing the Document, TIA disclaims any undertaking to perform any duty owed to or for anyone.

If the Document is identified or marked as a project number (PN) document, or as a standards proposal (SP) document, persons or parties reading or in any way interested in the Document are cautioned that: (a) the Document is a proposal; (b) there is no assurance that the Document will be approved by any Committee of TIA or any other body in its present or any other form; (c) the Document may be amended, modified or changed in the standards development or any editing process.

The use or practice of contents of this Document may involve the use of intellectual property rights ("IPR"), including pending or issued patents, or copyrights, owned by one or more parties. TIA makes no search or investigation for IPR. When IPR consisting of patents and published pending patent applications are claimed and called to TIA's attention, a statement from the holder thereof is requested, all in accordance with the Manual. TIA takes no position with reference to, and disclaims any obligation to investigate or inquire into, the scope or validity of any claims of IPR. TIA will neither be a party to discussions of any licensing terms or conditions, which are instead left to the parties involved, nor will TIA opine or judge whether proposed licensing terms or conditions are reasonable or non-discriminatory. TIA does not warrant or represent that procedures or practices suggested or provided in the Manual have been complied with as respects the Document or its contents.

If the Document contains one or more Normative References to a document published by another organization ("other SSO") engaged in the formulation, development or publication of standards (whether designated as a standard, specification, recommendation or otherwise), whether such reference consists of mandatory, alternate or optional elements (as defined in the TIA Engineering Manual, 4th edition) then (i) TIA disclaims any duty or obligation to search or investigate the records of any other SSO for IPR or letters of assurance relating to any such Normative Reference; (ii) TIA's policy of encouragement of voluntary disclosure (see Engineering Manual Section 6.5.1) of Essential Patent(s) and published pending patent applications shall apply; and (iii) Information as to claims of IPR in the records or publications of the other SSO shall not constitute identification to TIA of a claim of Essential Patent(s) or published pending patent applications.

TIA does not enforce or monitor compliance with the contents of the Document. TIA does not certify, inspect, test or otherwise investigate products, designs or services or any claims of compliance with the contents of the Document.

ALL WARRANTIES, EXPRESS OR IMPLIED, ARE DISCLAIMED, INCLUDING WITHOUT LIMITATION, ANY AND ALL WARRANTIES CONCERNING THE ACCURACY OF THE CONTENTS, ITS FITNESS OR APPROPRIATENESS FOR A PARTICULAR PURPOSE OR USE, ITS MERCHANTABILITY AND ITS NONINFRINGEMENT OF ANY THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS. TIA EXPRESSLY DISCLAIMS ANY AND ALL RESPONSIBILITIES FOR THE ACCURACY OF THE CONTENTS AND MAKES NO REPRESENTATIONS OR WARRANTIES REGARDING THE CONTENT'S COMPLIANCE WITH ANY APPLICABLE STATUTE, RULE OR REGULATION, OR THE SAFETY OR HEALTH EFFECTS OF THE CONTENTS OR ANY PRODUCT OR SERVICE REFERRED TO IN THE DOCUMENT OR PRODUCED OR RENDERED TO COMPLY WITH THE CONTENTS.

TIA SHALL NOT BE LIABLE FOR ANY AND ALL DAMAGES, DIRECT OR INDIRECT, ARISING FROM OR RELATING TO ANY USE OF THE CONTENTS CONTAINED HEREIN, INCLUDING WITHOUT LIMITATION ANY AND ALL INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, LITIGATION, OR THE LIKE), WHETHER BASED UPON BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING NEGATION OF DAMAGES IS A FUNDAMENTAL ELEMENT OF THE USE OF THE CONTENTS HEREOF, AND THESE CONTENTS WOULD NOT BE PUBLISHED BY TIA WITHOUT SUCH LIMITATIONS.

REVISION HISTORY

Ver.	Date	Comment
1.0	April 2009	Initial Publication

ABSTRACT

This Standard for Lawfully Authorized Electronic Surveillance (LAES) for cdma2000®[1] Wireless Local Area Network (WLAN)-Interworking addresses the interfaces between a Service Provider (SP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting Electronic Surveillance for cdma2000® WLAN service. This Standard supports LAES for cdma2000® packet data services interworking with a WLAN.

This Standard provides capabilities for the reporting of Communication-Identifying Information (CII) and Communication Content (CC).

[1] cdma2000® is a registered trademark of the Telecommunications Industry Association (TIA-USA)

CONTENTS

LIST OF FIGURES

LIST OF TABLES

FOREWORD

(This foreword is not part of this Standard.)

This Standard was developed by TIA Subcommittee TR-45.8, Core Networks – Mobile and Personal Communications Standards[2].

There are two annexes to this Standard. Annex A is informative and describes aspects of the *e*-Interface. Annex B is informative and describes optional messages.

[2] This document was originally balloted under TIA Subcommittee TR-45.6

1 Introduction

1.1 General

This Standard addresses the interfaces between a Service Provider (SP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting Lawfully Authorized Electronic Surveillance (LAES) for cdma2000® Wireless Local Area Network (WLAN)-Interworking.

1.2 Purpose

The purpose of this Standard is to facilitate an SP's assistance to law enforcement. This Standard defines a method to support Electronic Surveillance for cdma2000® WLAN-Interworking.

1.3 Scope

The scope of this Standard is to define the Electronic Surveillance capabilities to support LAES on the interfaces between an SP and an LEA to assist the LEA in conducting Electronic Surveillance for cdma2000® WLAN-Interworking. This Standard supports LAES for cdma2000® packet data services interworking with a WLAN. This Standard addresses IEEE 802.11 [802.11]. Other types of WLAN air interfaces are for further study. LAES for WLAN networks is outside the scope of this document.

1.4 Organization

This Standard is organized as follows:

Section 2: "References" is a list of references used in the preparation of this Standard.

Section 3: "Definitions and Acronyms" defines words and acronyms that are used in this Standard.

Section 4: "Electronic Surveillance Architecture" defines the WLAN-Interworking model, scenarios, and Electronic Surveillance architecture.

Section 5: "Stage 1 Description: User Perspective" defines Electronic Surveillance from the law enforcement user point of view.

Section 6: "Stage 2 Description: Network Perspective" defines Electronic Surveillance from the network point of view.

Section 7: "Stage 3 Description: Implementation Perspective" provides the implementation perspective of Electronic Surveillance for cdma2000® WLAN-Interworking.

Annex A (Informative): "Aspects of the *e*-interface" provides informative text on aspects of the *e*-interface.

Annex B (Informative): "Optional Messages" provides informative text on Stages 1-3 for optional Electronic Surveillance messages.

2 References

2.1 Normative References

The following standards contain provisions that, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. ANSI and TIA maintain registers of currently valid national standards published by them.

American National Standards

[025B] ANS J-STD-025-B-2006, *Lawfully Authorized Electronic Surveillance.*

Other Standards

[802.11] ISO/IEC 8802-11: 1999, *IEEE Standards for Information Technology -- Telecommunications and Information Exchange between Systems -- Local and Metropolitan Area Network -- Specific Requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (and amendments)*[3].

[X-680] ITU-T Recommendation X.680, Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation, July 2002[4].

[X-690] ITU-T Recommendation X.690, Information technology – ASN.1 encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), July 2002[5].

[Y-101] ITU-T Recommendation Y.101, Global Information Infrastructure Terminology: Terms and definitions; March 2000[6].

[NAM] S.R0037-B v1.0, *IP Network Architecture Model for cdma2000® Spread Spectrum Systems;* June 2007[7].

[3] IEEE, 3 Park Avenue, 17th Floor, New York, NY, 10016-5997 USA

[4] International Telecommunication Union, Telecommunication Standardization Bureau (ITU-T), Place des Nations, CH-1211 Geneva 20

[5] Ibid.

[6] Ibid.

[7] Third Generation Partnership Project 2 (3GPP2), 2500 Wilson Boulevard, Suite 300, Arlington, Virginia 22201 (USA)

[WLAN Rqts] S.R0087-A v1.0, *cdma2000 - WLAN Interworking Stage 1 Requirements*; March 2006[8].

[WLAN 000] X.S0028-000-0 v1.0, *cdma2000 Packet Data Services: Wireless Local Area Network (WLAN) Interworking – List of Parts;* April 2007[9].

[WLAN 100] X.S0028-100-0 v1.0, *cdma2000 Packet Data Services: Wireless Local Area Network (WLAN) Interworking; Access to the Internet*; March 2007[10].

[WLAN 200] X.S0028-200-A v1.0, *cdma2000 Packet Data Services: Wireless Local Area Network (WLAN) Interworking: Access to Operator Service and Mobility*; June 2008[11].

Other

[CALEA] United States Congress, *Communications Assistance for Law Enforcement (CALEA)*, Public Law 102-414, October 25, 1994, codified at 47 U.S.C. § 1001 *et seq*[12].

[99-230] Federal Communication Commission (FCC 99-230, CC Docket No. 97-213, *Third Report and Order*; Released August 31, 1999[13].

[8] Ibid.

[9] Ibid.

[10] Ibid.

[11] Ibid.

[12] United States Congress, East Capitol Street, NE and 1st Street, NE, Washington, DC 20002

[13] Federal Communications Commission (FCC). 445 12th Street SW, Washington, DC 20554

3 Definitions, Acronyms and Abbreviations

3.1 Definitions

Associate

A communications user whose equipment, facilities, or services are communicating with a Subject.

Authentication

An aspect of security that ensures that the originators of messages are who they claim to be.

Authentication, Authorization and Accounting (AAA)

The AAA provides IP based Authentication, Authorization, and Accounting functions for the cdma2000® packet data network. The AAA maintains security associations with peer AAA entities to support intra- and/or inter-administrative domain AAA functions. These functions are separate from the Home Location Register (HLR) services.

Authorization

An action by a Service Provider to make wireless service available to a subscriber.

Broker AAA (B-AAA)

The B-AAA resides in a Broker System. The WLAN AAA, if available, interacts with the MS's H-AAA server, possibly through one or more B-AAA(s) in Broker System(s) to provide WLAN access for the MS.

Broker System

The Broker System is an intermediate network between the WLAN and Home cdma2000® Network. There may be zero or more Broker Systems between the WLAN and the Home cdma2000® Network.

Collection Function (CF)

The location where the intercepted CC and CII is collected by a Law Enforcement Agency (LEA).

Communication Content (CC)

Defined in 18 U.S.C. § 2510(8) to be "when used with respect to any wire or electronic communications, includes any information concerning the substance, purport, or meaning of that communication."

Communication-Identifying Information (CII)

Signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of an SP.

Communication Session

A period of time, delineated by session establishment and session termination, over which a subscriber is allowed to use service provider network resources for the purpose of sending or receiving packets.

Confidentiality

An aspect of security that ensures information is not accessed by unauthorized entities.

Core Network

Defined in [Y-101] to be "a portion of the delivery system composed of networks, system equipment, and infrastructures, connecting the service providers to the access network."

Delivery Function (DF)

A logical entity in the Service Provider's network that delivers intercepted CC and CII toward one or more CFs for each LEA requesting intercept. A DF formats CC, CII or both, received from the Intercept Access Point (IAP) for delivery to the CFs.

'*e*' interface

The interface between a DF and a CF.

Electronic Surveillance

The associated technical capabilities and activities of LEAs related to the interception of wire, oral, or electronic communications. As used in this Standard, Electronic Surveillance also includes the acquisition of CII and refers to a single communication intercept, pen register, or trap and trace. Its usage does not include administrative subpoenas for obtaining a subscriber's toll 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. For the purposes of this Standard, Lawful Intercept (LI), Lawfully Authorized Electronic Surveillance (LAES), and Surveillance are synonymous with Electronic Surveillance.

Home AAA (H-AAA)

The H-AAA is the AAA server managed by the Home cdma2000® Network operator that provides the MS access to the WLAN-Interworking service.

Home Agent (HA)

See [NAM].

Home cdma2000® Network

The cdma2000® Network where the subscriber's subscription information is retained.

Home Location Register/Authentication Center (HLR/AC)

The HLR/AC optionally provides the Home AAA with security credentials for WLAN access.

Intercept Access Point (IAP)

A point within a communications system where some of the CC or CII of a Subject's equipment, facilities and services are accessed and then forwarded to the DF.

Law Enforcement Agency (LEA)

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

Lawful Authorization

A court order or other legal authorization or process pursuant to 18 U.S.C. 25[8] or any other relevant federal or state statute that authorizes Electronic Surveillance.

Lawful Intercept (LI)

See Electronic Surveillance.

Lawfully Authorized Electronic Surveillance (LAES)

See Electronic Surveillance.

Message Integrity

An aspect of security that ensures messages are not altered by unauthorized entities in a way that is not detectable.

Mobile Station (MS)

A wireless terminal used by subscribers to access network services over a radio interface.

Non-Repudiation

An aspect of security that ensures that the originators of messages cannot deny that they in fact sent the message.

Packet Data Interworking Function (PDIF)

The PDIF acts as a security gateway protecting resources and provides access to cdma2000® packet data services (e.g., IMS) in a Serving cdma2000® Network. The PDIF is located in the Serving cdma2000® Network.

Packet Data Session

For the purpose of this Standard, a Packet Data Session is a Communication Session. See Communication Session.

Pen Register

Is defined in 18 U.S.C. § 3127(3) as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications

services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business".

Serving cdma2000® Network

The cdma2000® Network currently providing cdma2000® packet data services to a subscriber. The Serving cdma2000® Network may be a Home cdma2000® Network or a Visited cdma2000® Network.

Session Continuity

Continuity of a packet data session while switching of network connection takes place between the available access networks (e.g., between a WLAN and a cdma2000® Network, or between WLANs).

Subject

A subscriber whose CII and CC, or CII only, have been lawfully authorized to be intercepted and delivered to an LEA. The identification of the Subject is limited to identifiers used to access the particular equipment, facility, or communication service (e.g., network address, MS identity, subscription identity).

Surveillance

See Electronic Surveillance.

Trap and Trace

Is defined in 18 U.S.C. § 3127(4) as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication".

Unobtrusive

Not readily or undesirably noticeable, or blatant; inconspicuous.

Visited AAA (V-AAA)

The V-AAA is the AAA server in the Visited cdma2000® Network. The V-AAA is present only when the Serving cdma2000® Network is a Visited cdma2000® Network. It interacts with the MS's H-AAA and the PDIF, possibly through one or more Broker System(s), to provide WLAN access for the MS. It also participates in the collection of accounting information and tunnel termination procedures when Visited cdma2000® operator policies apply.

Visited cdma2000® Network

The cdma2000® Network managed by an operator other than the subscriber's Home cdma2000® operator and from which the subscriber is receiving service when roaming.

Wireless Local Area Network (WLAN)

A Local Area Network that provides wireless access via an IEEE 802.11 or other type of wireless interface.

WLAN-AAA (W-AAA)

The WLAN AAA interacts with the MS's H-AAA server, possibly through one or more B-AAA(s) in Broker System(s) to provide WLAN access for the MS.

WLAN Session

A continuous period of time, delineated by WLAN session establishment and termination, over which a subscriber accesses a WLAN for the purpose of sending or receiving packets.

3.2 Acronyms and Abbreviations

3GPP2	Third Generation Partnership Project Two
AAA	Authentication, Authorization, and Accounting
ANS	American National Standard
ANSI	American National Standards Institute
ASN.1	Abstract Syntax Notation One
ATIS	Alliance for Telecommunications Industry Solutions
B-AAA	Broker AAA
BER	Basic Encoding Rules
CALEA	Communications Assistance for Law Enforcement Act
CC	Communication Content
CF	Collection Function
CII	Communication-Identifying Information
CLIC	cdma2000® Lawful Interception Correlation
CoA	Care of Address
DF	Delivery Function
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
GMT	Greenwich Mean Time
H-AAA	Home AAA
HA	Home Agent
HO	Handoff
HLR/AC	Home Location Register/Authentication Center
IAP	Intercept Access Point
ID	Identity
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPv4	IP version 4
IPv6	IP version 6
ITU-T	International Telecommunication Union, Telecommunication Standardization Sector
LAES	Lawfully Authorized Electronic Surveillance

LAN	Local Area Network
LEA	Law Enforcement Agency
LI	Lawful Intercept
MAC	Media Access Control
MCC	Mobile Country Code
MMD	Multimedia Domain
MNC	Mobile Network Code
MS	Mobile Station
MSID	Mobile Station Identity
NAI	Network Access Identifier
NIST	National Institute of Standards and Technology
OID	Object Identifier
PDIF	Packet Data Interworking Function
PoC	Push-to-Talk over Cellular
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
SP	Service Provider
TIA	Telecommunications Industry Association
U.S.C.	United States Code
V-AAA	Visited AAA
W-AAA	WLAN AAA
WLAN	Wireless LAN
WLAN-I	WLAN-Interworking

4 Electronic Surveillance Architecture

This section provides the reference architectures for the WLAN-Interworking scenarios supported in this Standard as well as the Electronic Surveillance reference architecture.

4.1 WLAN-Interworking Model

Figure 1 from [WLAN Rqts] depicts the logical model for the cdma2000® WLAN-Interworking system.

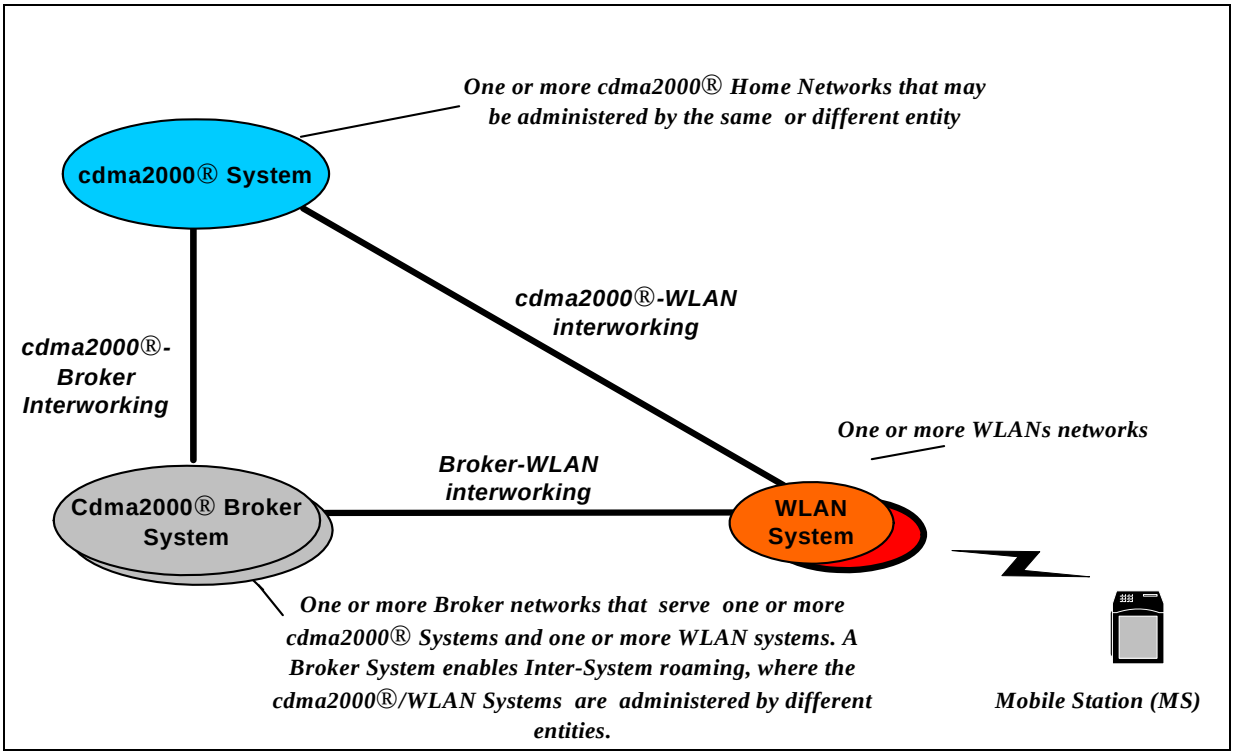

Figure 1 WLAN-Interworking Model

Several different technologies fall into the WLAN category, but these different access technologies do not impact the Internet Protocol (IP) layer or the layers above (e.g., transport). Therefore, WLAN-Interworking is not limited to any specific WLAN technology.

4.1.1 WLAN-Interworking Entities and Relationships

A WLAN is a collection of wireless Local Area Network entities that provide wireless access via some air interface technology.

A Broker System is a collection of intermediaries that facilitate WLAN-Interworking with a cdma2000® Network with which there is no direct relationship.

A cdma2000® Network can either be a Home Network or a Visited Network. A Home Network is a collection of Home cdma2000® Network entities where the subscriber's

subscription information exists. A Visited Network is a collection of Visited cdma2000® Network entities.

Ownership of the WLAN in the model may be one or more of the following general classes:

- The WLAN owner is a cdma2000® Network operator.
- The WLAN owner is a public network operator who is not a cdma2000® Network operator (e.g., fixed network operators, operators of mobile networks other than cdma2000® Networks or public WLAN operators).
- The WLAN owner is not a public network operator, but an entity providing WLAN access (e.g., building manager, airport authority) to provide local services and Internet access as well as WLAN-Interworking with a cdma2000® Network.
- The WLAN owner is a business entity providing a WLAN for internal use but also allows WLAN-Interworking.

SPs have a responsibility to support LAES for WLAN-Interworking as defined in this Standard if they are a WLAN owner, cdma2000® SP, or both.

4.2 Scenarios

The intent of WLAN-Interworking is to extend cdma2000® packet data and multimedia services and/or capabilities to the WLAN environment. The scenarios supported by this Standard are found in [WLAN 100] and [WLAN 200]. Scenario 1 is outside the scope of this Standard.

The network entities in Figures 2 through 4 are described in Section 3.1.

4.2.1 Scenario 2: cdma2000®-Based Access Control and Charging and Access to the Internet via the WLAN system

Figure 2 (modified from [WLAN 100]) depicts the WLAN-Interworking architecture for Scenario 2.

The cdma2000® subscriber is authenticated and authorized by the cdma2000® Home Network Authentication, Authorization, and Accounting (AAA) entity. The WLAN assigns an IP address to the subscriber and carries the subscriber's bearer traffic directly to or from the Internet.

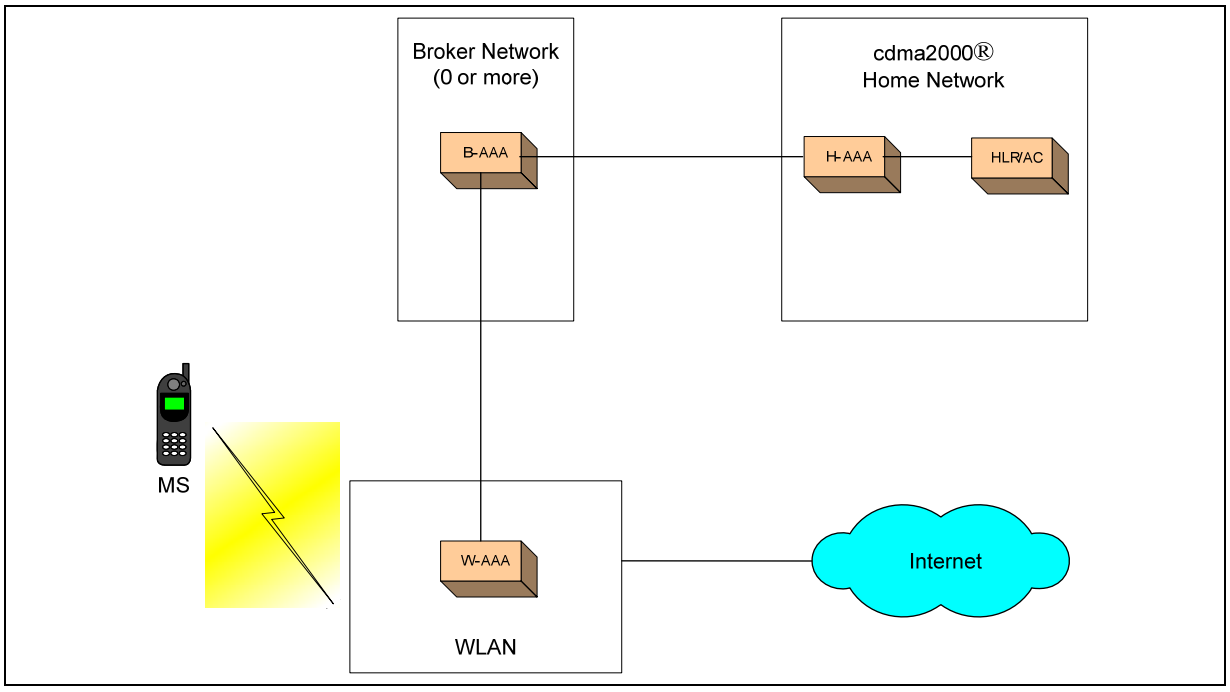

Figure 2 WLAN-Interworking Scenario 2

4.2.2 Scenario 3: Access to cdma2000® Packet Data Services via the WLAN system

Figure 3 (modified from [WLAN 200]) provides the reference model for scenario 3. The cdma2000® subscriber accesses the Home cdma2000® Network for AAA. Packet data services (e.g., IMS) are provided to the cdma2000® subscriber from the Serving cdma2000® Network.

Both Multimedia Domain (MMD) and IP Multimedia Subsystem (IMS) services require separate authentication and authorization mechanisms. These are performed after successful authentication and authorization with the Packet Data Interworking Function (PDIF) and successful secure IP tunnel set-up between the Mobile Station (MS) and the PDIF.

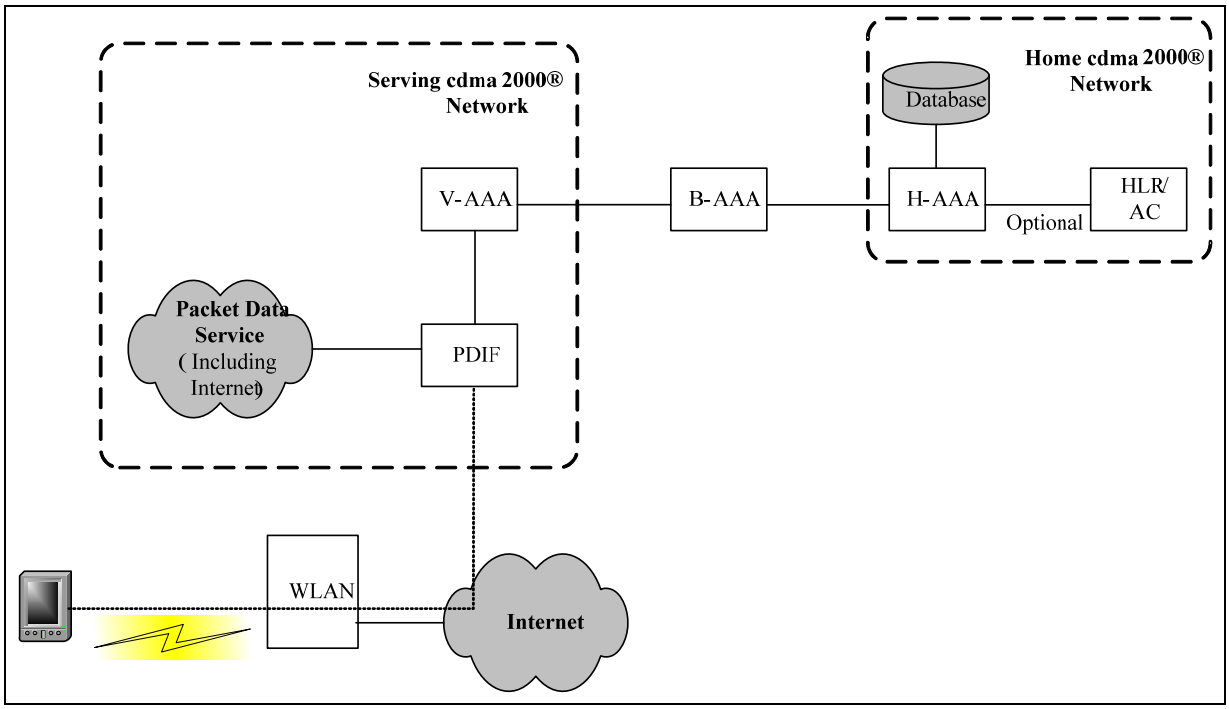

Figure 3 WLAN-Interworking Scenario 3

4.2.3 Scenario 4: Session Continuity

Figure 4 (modified from [WLAN 200]) depicts the reference model for Scenario 4. In WLAN-Interworking, the Home Agent (HA) is always located in the Serving cdma2000® Network.

The continuity of a packet data session, while switching network connections, takes place between the available access networks. The objective of session continuity is to allow the MS to continue the same sessions for all access independent IP services (i.e., cdma2000® packet data services that are transparent to and independent of any specific access technology) while it moves among available access systems. The session may be preserved, but there may be a loss of packets during the handoff (HO) between the access technologies depending on the capabilities of the MS and the radio access networks of the access technologies to perform the HO.

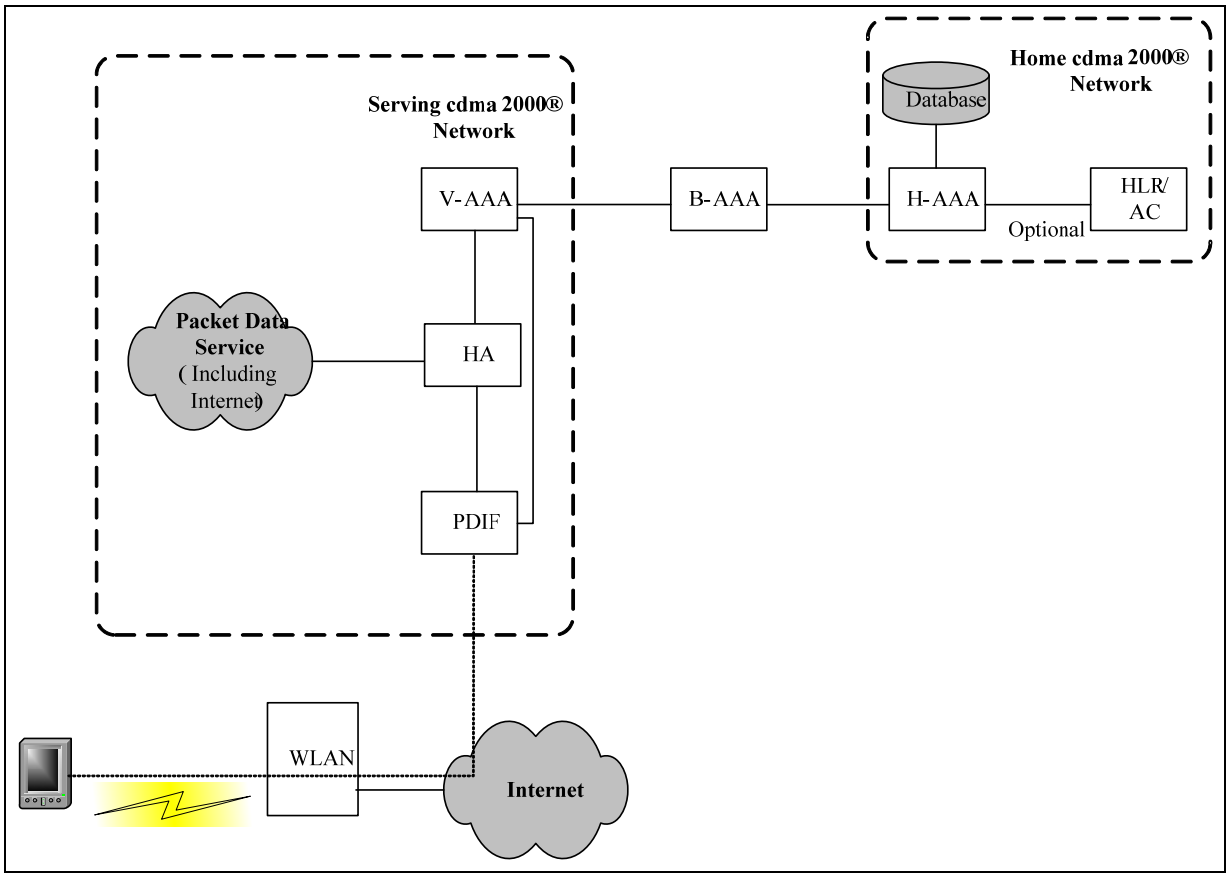

Figure 4 WLAN-Interworking Scenario 4

4.3 Electronic Surveillance Architecture

Figure 5 shows both the high-level cdma2000® and WLAN-I LAES architectures. As shown, the WLAN-I LAES functions need not affect an existing cdma2000® packet data LAES implementation. The multiple Distribution Functions (DFs) (shown in Figure 5) may be realized by separate or single physical entities. In the same way, the multiple Collection Functions (CFs) (shown in Figure 5) may be realized by separate or single entities.

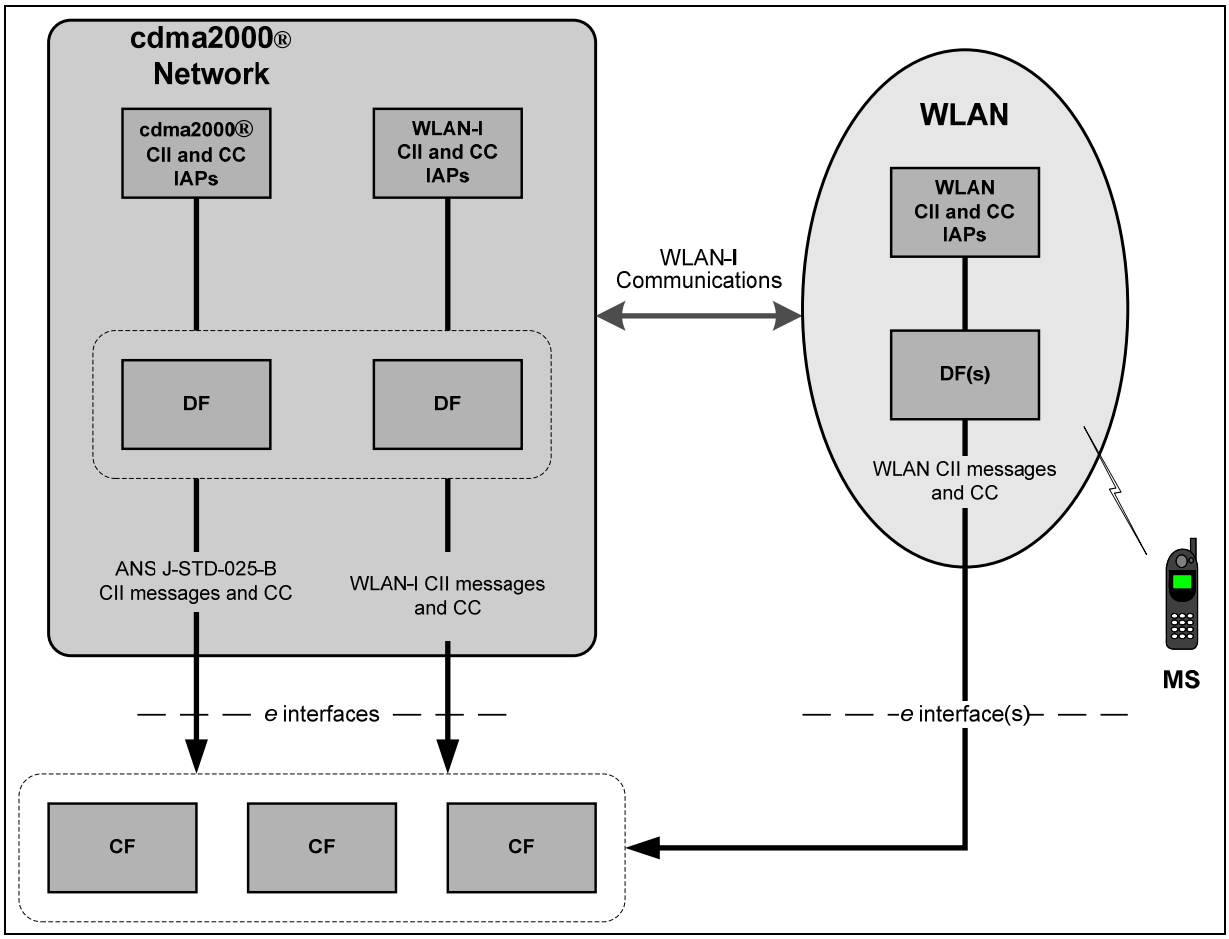

Figure 5 LAES Architecture for WLAN-Interworking

The *e*-interface for WLAN-I CII messages and CC is the only interface considered for standardization in this Standard. The *e*-interface for WLAN CII messages and CC is outside the scope of this Standard. See [025B] for cdma2000® CII messages and CC.

5 Stage 1 Description: User Perspective

This section describes the features and services of LAES from a user's perspective in a cdma2000® Network for the WLAN-Interworking scenarios 2-4 as described in [WLAN Rqts].

5.1 Introduction

This section presents the law enforcement user perspective (Stage 1) requirements for LAES for WLAN-Interworking in cdma2000® Networks; communication-related events that represent or generate CII; and general capabilities needed for LAES for cdma2000® WLAN service. In this Standard, the user is the LEA.

5.2 Assumptions

5.2.1 Authentication and Verification

To ensure that the intercepted communications is received from or sent to the Subject's equipment, facilities, or services, the assumption is the SP authenticates the subscribers' access to the SP's network and services. The mechanism(s) an SP uses for authentication is beyond the scope of this Standard.

While an intercept is active, the intercepted communications to be delivered to the LEA are assumed to be associated with the Subject's equipment, facilities, or services as a result of the authentication process. The mechanism(s) the SP uses to isolate and associate the intercepted communications with the authenticated Subject's equipment, facilities, or services is beyond the scope of this Standard.

The SP's LAES operational and administrative procedures are beyond the scope of this Standard. It is assumed that the SP has operations, procedures, and verification processes to ensure the LI is performed per the lawful authorization.

5.3 General Requirements

This section describes law enforcement requirements for WLAN-Interworking LAES.

5.3.1 Identification and Interception of Subject Communications

The SP shall intercept the communications of the Subject's equipment, facilities, or services as specified in the lawful authorization.

Only communications associated with the Subject's equipment, facilities, or services may be intercepted. Communications associated with the Subject's equipment, facilities, or services must be isolated, and communications not associated with the Subject's equipment, facilities, or services must not be delivered to the LEA.

If the Subject uses different communications services (e.g., voice, Push-to-Talk over Cellular (PoC), data) that are each lawfully authorized for Electronic Surveillance, the SP shall provide the logical separation of the various communications for reporting and delivery. For

cdma2000® packet data services, filtering of data packets for any other service is not required.

The network must use specific and unique identifiers to identify the Subject communications. These identifiers are derived from the lawful authorization which may identify multiple MSs. The case identity identifies the Subject.

The Subject can be identified within an SP's network in a variety of ways. These may include, but are not limited to the following examples: IP address(es), Media Access Control (MAC) address(es), Network Access Identifier (NAI), and Mobile Station Identity (MSID).

The SP should expeditiously isolate and enable the LEA to access CII that is reasonably available to the SP in a manner that allows it to be associated with the CC to which it pertains.

All communications lawfully authorized for the Electronic Surveillance (i.e., both to and from the Subject's equipment, facilities, or services) must be intercepted for the entire period authorized by that legal authority.

Electronic Surveillance must be conducted in an unobtrusive manner (i.e., in a manner that prevents the Subject or the Subject's equipment, facilities, or services from readily noticing or readily detecting that an intercept is being conducted). If service parameters (e.g., bandwidth, latency, availability) may be impacted in any way by the Electronic Surveillance, such impacts should be avoided or should be minimized to the greatest extent possible so as not to jeopardize unobtrusiveness.

The SP shall use appropriate measures that enable the isolation and interception of all wire and electronic communications to or from a Subject's equipment, facilities, or services (see Section 103(a) of [CALEA], 47 U.S.C. §1002(a)). Such measures include those that provide a high level of probability that the intercept will not be corrupted due to lost, dropped, or omitted packets.

5.3.2 Simultaneous Interceptions

In the United States, the SP shall be able to provision and conduct multiple simultaneous interceptions within its network and network elements. This includes the ability:

1. to access and monitor all simultaneous communications originated or received by the Subject;
2. for multiple LEAs to simultaneously monitor the same Subject while maintaining confidentiality of these different Electronic Surveillances among the different LEAs; and
3. to support up to five (5) simultaneous and separate lawful interceptions on the same Subject.

The SP must ensure that only lawfully authorized information is delivered to the LEA authorized to receive it.

The maximum number of CFs required to be supported by an SP is an implementation aspect. The number of CFs per LEA is mutually agreed between an LEA and the SP.

5.3.3 Correlation

The CII events for a lawfully authorized Electronic Surveillance shall be correlated when delivered to the LEA. Correlation is provided between WLAN-I CII and CC. Correlation between WLAN-I CII/CC and cdma2000® CII/CC is not provided.

If Electronic Surveillance of more than one service (see 5.3.1) is specified in the lawful authorization, the Electronic Surveillance information delivered to the LEA shall be correlated for each service for which Electronic Surveillance is lawfully authorized.

If there is more than one lawful authorization on a Subject, the Electronic Surveillance information delivered to the LEA (or LEAs) must be correlated for each lawful authorization.

CII events shall be correlated with the associated intercepted CC that is delivered to the LEA, pursuant to a lawful authorization for Electronic Surveillance. Specific and unique identifiers shall be used to correlate the Subject's CII and CC.

5.3.4 Compression

An SP shall be responsible for decompressing, or ensuring the LEA's ability to decompress, any Subject communication or signaling when the compression mechanism was provided by the SP and the SP possesses the information necessary to decompress the communication or signaling. An SP that provides the LEA with information about how to decompress a communication or signaling (e.g., identifying the type of compression software used to compress the communication or signaling, directing the LEA to the appropriate vendor that can provide decompression equipment) fully satisfies its obligation under the preceding sentence.

LEA prefers the content in uncompressed form on the *e*-interface.

5.3.5 Encryption

An SP shall be responsible for decrypting, or ensuring the LEA's ability to decrypt, any Subject communication or signaling encrypted when the encryption mechanism was provided by the SP and the SP possesses the information necessary to decrypt the communication or signaling. An SP that provides the LEA with information about how to decrypt a communication or signaling (e.g., identifying the type of encryption software used to encrypt the communication or signaling, directing the LEA to the appropriate vendor that can provide decryption equipment, or providing the encryption key used to encrypt the communication or signaling) fully satisfies its obligation under the preceding sentence.

LEA prefers the content in decrypted form on the *e*-interface.

5.3.6 Location

When specifically authorized, the Subject's location information shall be provided to an LEA as CII during WLAN Access Message events (see 6.2.1). The SP shall provide to the LEA the most precise location information that is reasonably available at the IAP.

5.3.7 Session Continuity

When the Subject's cdma2000® packet data session is continued while switching access network connections (e.g., WLAN to cdma2000® network access), an LEA requires that the SP:

- Continue to intercept and report CII and CC for the session as long as the communications are continued to be carried by the SP.
- Provide correlation information to the LEA to enable an LEA to correlate the pre- and post- transitions sessions.

This requirement is *for further study*.

5.3.8 Confidentiality and Access Control of the Lawful Authorization

The SP shall protect information regarding an LEA's interception of CC and CII. The SP shall use means designed to protect the confidentiality of LI activities to safeguard against non-authorized employees of the SP as well as other non-authorized persons from becoming aware of the fact that LI is being conducted.

Access to, or knowledge of, an intercept and intercepted communications and data must be protected and limited to only authorized persons or employees.

Access to or knowledge of lawful intercept capabilities and intercept-related equipment shall be protected per the requirements of Section 103(a)(4) of [CALEA], 47 U.S.C. §1002(a)(4).

5.3.9 Timing

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 of the CII 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 CII triggering event is available at the IAP.

A time-stamp shall include a Greenwich Mean Time (GMT) offset, if available at the IAP or DF.

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

- 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 CII triggering event at least 95% of the time.
- Each surveillance message shall contain a time-stamp that is within 200 milliseconds from when the CII event triggering the surveillance message was detected.

The following timing requirements shall apply to the delivery of intercepted content:

- The CC header shall include a time-stamp (see 5.5).

- Intercepted communications content shall be expeditiously transmitted by the IAP towards the DF with its interception. The timeliness of CC delivery from the DF to the CF is determined by the SP-LEA agreement.

5.4 Communications-Identifying Information Events

WLAN-I CII events are reported to the LEA when the information is reasonably available at the IAP. [025B] CII events may also be reported if detected.

The following are the CII events for WLAN-Interworking.

5.4.1 WLAN Access Attempt

This event is triggered when a network registration has been attempted (i.e., the Subject or associated network element successfully[14] provides an appropriate form of unique identifying information (e.g., NAI, MAC address, MSID) to an AAA server (or other equivalent functional entity)). If multiple access attempts and multi-link protocols are allowed, the SP shall provide a separate WLAN Access Attempt event report for each.

5.4.2 WLAN Access Attempt Successful

This event is triggered when the network authenticates and authorizes the Subject's WLAN access. If multiple access attempts and multi-link protocols are allowed, then the SP shall provide separate WLAN Access Attempt Successful event reports.

5.4.3 WLAN Access Attempt Failure

This event is triggered when the network authentication and authorization has failed with the network's AAA server (or other equivalent functional entity) and an access session has not been established. If multiple access attempts and multi-link protocols are allowed, then the SP shall provide separate WLAN Access Attempt Failure event reports.

5.4.4 WLAN Access Rejected

This event is triggered when a Subject's authentication and authorization is successfully completed, but the Subject's access attempt is rejected for other reasons. For example, this event would occur 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.

5.4.5 WLAN Access Termination

This event is triggered when the Subject's WLAN access session is terminated and the WLAN connection is released.

5.4.6 WLAN Tunnel Establishment Initiation

This event is triggered when a Subject's MS or an associated network entity attempts to negotiate the establishment of a WLAN tunnel (i.e., the tunnel between the MS and the

[14] A successful attempt is one where the network can recognize the attempt as being from the Subject.

PDIF). Both successful and unsuccessful establishment attempts will be reported. The SP shall provide the reason for failure for unsuccessful attempts.

5.4.7 WLAN Tunnel Disconnect

The event is triggered when a Subject's WLAN tunnel (i.e., between the MS and the PDIF) is disconnected.

5.4.8 WLAN Session or Tunnel Already Active

This event is triggered when Electronic Surveillance is started and the Subject has one or more active WLAN Access sessions or one or more WLAN Tunnels (i.e., the tunnel between the MS and PDIF) established.

5.4.9 IP Packet Header Reporting Methods

Within an SP's network, one of the following packet header reporting methods may be used:

- IP Packet Header Report
- IP Packet Summary Report

These reports need not be provided for Electronic Surveillances in which interception of the Subject's entire communication has been lawfully authorized (i.e., when both CII and CC are authorized to be intercepted and delivered to the LEA).

Note 1: At the time of publication, the reporting of port numbers as CII is under review by the FCC in the context of a petition for rulemaking (RM-11376)[15] concerning [025B].

5.4.9.1 IP Packet Header Report

This event is used to provide packet header reports on a per CC packet basis (i.e., non-summarized reporting).

The IP Packet Header Report event shall be reported for each packet of a packet stream sent or received by the Subject. This report event provides source and destination information (i.e., IP address(es) and any port information (see Note 1) available in the IP header) derived from the packet headers for each packet.

5.4.9.2 IP Packet Summary Report

This event is used to provide packet data summary reports instead of individual IP Packet Header Report messages for the Subject's CC.

This event reports source and destination information (i.e., IP address(es) and any port information (see Note 1) available in the IP header) derived from the packet headers, and provides summary information for the number of packets transmitted or received by the Subject for a source and destination pairs.

---

[15] The petition for rulemaking is available for viewing by accessing the FCC's electronic comment filing system website at http://gullfoss2.fcc.gov/prod/ecfs/comsrch_v2.cgi and entering "RM-11376" in Block 1 - Proceeding to see all of the filings in the proceeding, including the petition.

The Packet Summary Report is reported when any of the following triggers occur:

- the expiration of a timer;
- a change in information being reported (e.g., the IP Address changes).

The timer shall have a maximum value of 15 minutes.

5.5 Communications Content

When an LEA is lawfully authorized to receive the Subject's WLAN-I CC, the SP shall access and deliver WLAN-I CC for the duration of all WLAN-Interworking sessions that are sent to and received from the Subject's equipment, facilities, or service.

WLAN-I CC is delivered to the LEA using the cdma2000® lawful interception correlation (CLIC) header) see [025B] section 5.5.6).

6 Stage 2 Description: Network Perspective

This section describes the events that trigger WLAN-Interworking CII surveillance messages. This section also describes the contents of the surveillance messages.

6.1 Surveillance Message Parameters

Each message in this Standard includes a set of parameters. There is an indication for each parameter as to whether its inclusion in a message is Mandatory (M), Optional (O), or Conditional (C).

- Mandatory (M):the parameter shall always be included in the message;
- Optional (O): the parameter may be included in the message;
- Conditional (C): the parameter shall be included when the conditions specified in the Usage text for the parameter are met. If no conditions are listed, then the default condition is "if available".

Syntactically in Abstract Syntax Notation One (ASN.1), Optional and Conditional parameters are considered Optional.

6.2 WLAN-Interworking Messages

The following messages have been developed for this Standard:

- WLAN Access
- WLAN Tunnel
- WLAN Active Tunnel Session
- WLAN IP Packet Header
- WLAN IP Packet Summary

6.2.1 WLAN Access Message

The WLAN Access message reports events related to the establishment or termination of a WLAN session. The message is triggered when any of the following occur:

- the AAA server receives a request to authenticate and authorize access for the Subject;
- the AAA server successfully authenticates and authorizes access for the Subject;
- the AAA server rejects the Subject's request to authenticate and authorize access or fails to successfully authenticate and authorize access for the Subject;
- the AAA server receives notification that a WLAN session of the Subject has been terminated.

The WLAN Access message includes the following parameters:

Table 1 WLAN Access Message Parameters

Parameter	MOC	Usage/Conditions
CaseIdentity	M	Identifies the Subject.
IAPSystemIdentity	C	Identifies the network entity containing the IAP when the underlying data carriage does not imply that network entity.
TimeStamp	M	Identifies the date and time that the event was detected.
ObservedSubjectIdentity	M	Subject's observed identity or identities for each interception. Report all known identities (e.g., MSID, NAI, MAC Address).
SubjectIPAddress	C	The Subject's IP Address (IPv4 or IPv6).
WLAN_Identity	M	Reports all known WLAN identities (e.g., Called_Station_ID, NAS_IP_Address, and NAS_Identifier from [WLAN100]).
WLANOperatorName	C	Identifies the name of the WLAN operator providing WLAN access to the Subject. See Note 2.
WLAN_AP_Name	C	Identifies the name of the WLAN access point. See Note 2.
WLANLocationInformation	C	When authorized, location information regarding the WLAN as provided in the signaling exchanged with the AAA server. See Note 2.
ServiceAccessType	C	Identifies the type of system access as defined in [WLAN100].
HaIPAddress	C	IPv4 address of the HA, only provided for Mobile IPv4 access. Only reported if available with the WLAN access termination event.
FaCoA	C	Foreign Agent provided Care of Address, only provided for Mobile IPv4 access. Only reported if available with the WLAN access termination event.
WLANAccessEvent	M	Access Attempt, Access Successful, Access Failure, Access Reject or Access Termination
WLANAccessFailure	C	Reason for Failure or Rejection

Note 2: these parameters are included based on on-going work in the IETF concerning RADIUS location information and does not reflect the availability of the information.

6.2.2 WLAN Tunnel Message

The WLAN Tunnel message reports when the network attempts to negotiate a WLAN tunnel between the MS and the PDIF or when an established WLAN tunnel is disconnected.

The message is triggered when any of the following occur:

- the network successfully establishes a WLAN tunnel;
- the network is unable to establish a WLAN tunnel;
- the Subject's WLAN tunnel is disconnected.

The WLAN Tunnel message includes the following parameters:

Table 2 WLAN Tunnel Message Parameters

Parameter	MOC	Usage/Conditions
CaseIdentity	M	Identifies the Subject.
IAPSystemIdentity	C	Identifies the network entity containing the IAP when the underlying data carriage does not imply that network entity.
TimeStamp	M	Identifies the date and time that the event was detected.
ObservedSubjectIdentity	M	Subject's observed identity or identities for each interception. Report all known identities (e.g., MSID, NAI, MAC Address).
ServingSystemIdentity	M	Identifies the cdma2000® Network entity that is currently serving the Subject.
SubjectIPAddress	C	The Subject's IP Address (IPv4 or IPv6).
CorrelationNumber	C	Unique number for each established tunnel for correlating CC and CII when both are reported.
WLAN_MS_IPAddress	C	The WLAN IP address (i.e., for the Subject's equipment) that is used for Internet access, if different from the SubjectIPAddress.
TunnelAddress	M	Identifies the IP address of the Tunnel the Subject is using.
CarrierIdentity	C	Identifies the visited carrier, if known. This identifier is comprised of 3-octet Mobile Country Code (MCC) followed by a 2-octet or 3-octet Mobile Network Code (MNC).
WLANTunnelEvent	M	Successful, Unsuccessful, Subject Disconnect or Network Disconnect.
WLANTunnelEndReason	C	Reason for unsucessful tunnel establishment or reason for disconnect.

6.2.3 WLAN Active Tunnel Session Message

The WLAN Active Tunnel Session message reports when the Electronic Surveillance is started and the Subject has one or more active WLAN sessions or tunnels established. Multiple messages are reported, one for each session or tunnel, when the Subject has multiple WLAN sessions or tunnels established.

The message is triggered when an Electronic Surveillance is started and:

- the Subject is active in one or more WLAN sessions, or
- the Subject has one or more active WLAN tunnels.

The WLAN Active Tunnel Session message includes the following parameters:

Table 3 WLAN Active Tunnel Session Message Parameters

Parameter	MOC	Usage/Conditions
CaseIdentity	M	Identifies the Subject.
IAPSystemIdentity	C	Identifies the network entity containing the IAP when the underlying data carriage does not imply that network entity.
TimeStamp	M	Identifies the date and time that the event was detected.
ObservedSubjectIdentity	M	Subject's observed identity or identities for each interception. Report all known identities (e.g., MSID, NAI, MAC Address).
SubjectIPAddress	C	The Subject's IP Address (IPv4 or IPv6).
CorrelationNumber	C	Unique number for each established tunnel for correlating CC and CII when both are reported.
TunnelorSession	C	Identifies what is active (i.e., Tunnel or Session).
WLAN_MS_IPAddress	C	The WLAN IP address (i.e., for the Subject's equipment) that is used for Internet access, if different from the SubjectIPAddress.
TunnelAddress	C	Identifies the IP address of the Tunnel the Subject is using, if TunnelorSession parameter is "Tunnel".
CarrierIdentity	C	Identifies the visited carrier, if known. This identifier is comprised of a 3-octet Mobile Country Code (MCC) followed by a 2-octet or 3-octet Mobile Network Code (MNC).
WLANOperatorName	C	Identifies the name of the WLAN operator providing WLAN access to the Subject.

6.2.4 WLAN IP Packet Header Report Message

The WLAN IP Packet Header message reports information about each packet of a packet stream sent or received by the Subject. This message is optional for Electronic Surveillances in which the interception of the Subject's CC has been lawfully authorized (i.e., when both CII and CC are authorized to be intercepted and delivered to the LEA).

The message is triggered when any of the following occur:

- the Subject sends a packet;
- the Subject receives a packet.

The WLAN IP Packet Header message includes the following parameters:

Table 4 WLAN IP Packet Header Message Parameters

Parameter	MOC	Usage/Conditions
CaseIdentity	M	Identifies the Subject.
IAPSystemIdentity	C	Identifies the network entity containing the IAP when the underlying data carriage does not imply that network entity.
TimeStamp	M	Identifies the date and time that the event was detected.

Parameter	MOC	Usage/Conditions
ObservedSubjectIdentity	M	Subject's observed identity or identities for each interception. Report all known identities (e.g., MSID, NAI, MAC Address).
StreamID	M	Identifies the packet stream of the header.
SourceIPAddress	M	Identifies the IP Address of the source.
DestinationIPAddress	M	Identifies the IP Address of the destination.
SourcePortNumber	O	Identifies the port number of the source. See Note 1.
DestinationPortNumber	O	Identifies the port number of the destination. See Note 1.
TransportProtocol_ID	M	Identifies the Transport Layer Protocol Used.
CorrelationNumber	C	Unique number for each established tunnel for correlating CC and CII when both are reported.

6.2.5 WLAN IP Packet Summary Report Message

The WLAN IP Packet Summary message provides a summary report instead of multiple WLAN IP Packet Header messages. This message is optional for Electronic Surveillances in which the interception of the Subject's CC has been lawfully authorized (i.e., when both CII and CC are authorized to be intercepted and delivered to the LEA).

The message is triggered when any of the following occur:

- at the expiration of a timer;
- when there is a change in the information being reported (e.g., the IP Address changes).

The timer shall have a maximum value of 15 minutes.

The WLAN IP Packet Summary message includes the following parameters:

Table 5 WLAN IP Packet Summary Message Parameters

Parameter	MOC	Usage/Conditions
CaseIdentity	M	Identifies the Subject.
IAPSystemIdentity	C	Identifies the network entity containing the IAP when the underlying data carriage does not imply that network entity.
TimeStamp	M	Identifies the date and time that the event was detected.
ObservedSubjectIdentity	M	Subject's observed identity or identities for each interception. Report all known identities (e.g., MSID, NAI, MAC Address).
StreamID	M	Identifies the packet stream of the header.
SourceIPAddress	M	Identifies the IP Address of the source.
DestinationIPAddress	M	Identifies the IP Address of the destination.
SourcePortNumber	O	Identifies the port number of the source. See Note 1.

Parameter	MOC	Usage/Conditions
DestinationPortNumber	O	Identifies the port number of the destination. See Note 1.
Count	M	Identifies how many packets of the same header were transmitted or received.
TransportProtocol_ID	M	Identifies the Transport Layer Protocol Used.
CorrelationNumber	C	Unique number for each established tunnel for correlating CC and CII when both are reported.

7 Stage 3 Description: Implementation Perspective

7.1 ASN.1 Definitions

This section provides the ASN.1 [X-680] definitions for this Standard. CII and CC corresponding to ASN.1 definitions shall be encoded according to Basic Encoding Rules (BER) [X.690].

The following object identifiers are assigned for WLAN-Interworking:

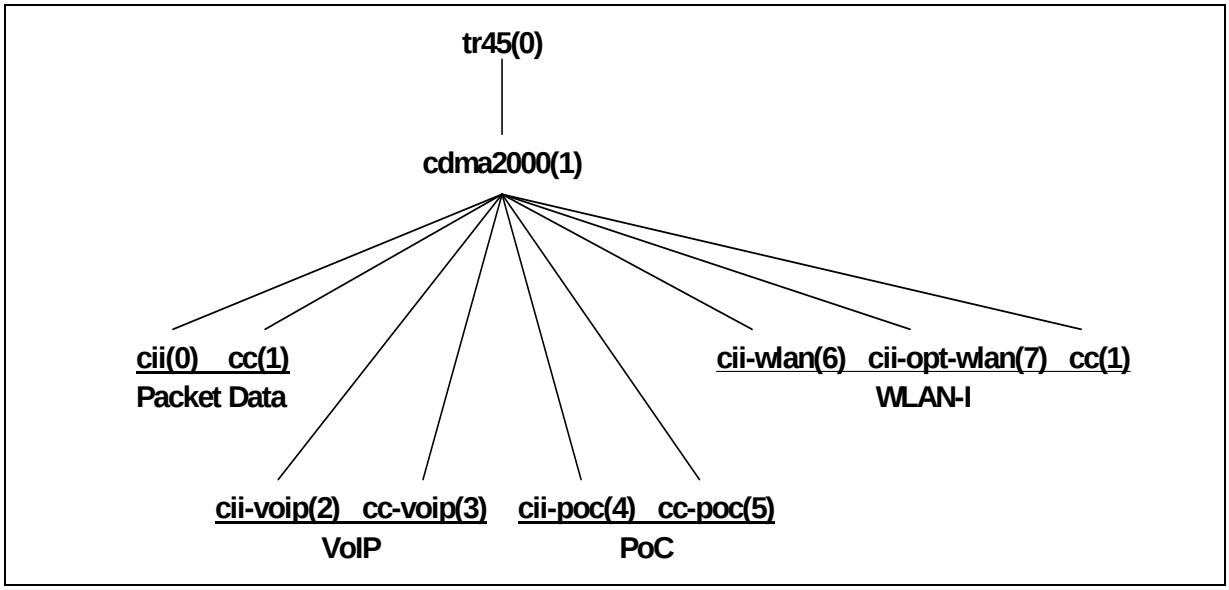

Figure 6 WLAN-Interworking Object Identifiers

7.1.1 WLAN CII Abstract Syntax Module

```
WLAN-LAES-CII-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) tr45(0) cdma2000(1) cii-wlan(6)
version-1(0)}
DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

CaseIdentity, TimeStamp, CorrelationNumber
FROM CDMA2000CIIModule
{iso(1) member-body(2) us(840) tia(113737) laes(2) tr45(0) cdma2000(1) cii(0)
version-1(0)};

wlan-LAES-CII-Abstract-Syntax-Module-OID OBJECT IDENTIFIER ::=
{iso(1) member-body(2) us(840) tia(113737) laes(2) tr45(0) cdma2000(1) cii-wlan(6)
version-1(0)}

wlanProtocolIdentifier OBJECT IDENTIFIER ::= {wlan-LAES-CII-Abstract-Syntax-
Module-OID}
```

```
WlanProtocol ::= SEQUENCE
{
   wlanProtocolIdentifier     OBJECT IDENTIFIER,
   wlanMessage                WlanMessage
}

WlanMessage ::= CHOICE
{
   wlanAccess                 [0] WlanAccess,
   wlanTunnel                 [1] WlanTunnel,
   wlanActiveTunnelSession    [2] WlanActiveTunnelSession,
   wlanIPPacketHeader         [3] WlanIPPacketHeader,
   wlanIPPacketSummary        [4] WlanIPPacketSummary
}

-- Message Definitions

WlanAccess ::= SEQUENCE
{
   caseId                     [0] CaseIdentity,
   iAPSystemId                [1] IAPSystemIdentity         OPTIONAL,
   timestamp                  [2] TimeStamp,
   observedSubjectIdentity    [3] SubjectIdentity,
   subjectIPAddress           [4] IpAddress                 OPTIONAL,
   wlan_Identity              [5] WLAN_Identity,
   wlanOperatorName           [6] WlanOperatorName          OPTIONAL,
   wlan_AP_Name               [7] UTF8String                OPTIONAL,
   wlanLocationInformation    [8] WlanLocationInformation   OPTIONAL,
   serviceAccessType          [9] ServiceAccessType         OPTIONAL,
   haIPAddress                [10] IpAddress                OPTIONAL,
   faCoA                      [11] IpAddress                OPTIONAL,
   wlanAccessEvent            [12] WlanAccessEvent,
   wlanAccessFailure          [13] WlanAccessFailure        OPTIONAL,
   ...
}

WlanTunnel ::= SEQUENCE
{
   caseId                     [0] CaseIdentity,
   iAPSystemId                [1] IAPSystemIdentity         OPTIONAL,
   timestamp                  [2] TimeStamp,
   observedSubjectIdentity    [3] SubjectIdentity,
   servingSystemIdentity      [4] ServingSystemIdentity,
   subjectIPAddress           [5] IpAddress                 OPTIONAL,
   correlationNumber          [6] CorrelationNumber         OPTIONAL,
   wlan_MS_IpAddress          [7] IpAddress                 OPTIONAL,
   tunnelAddress              [8] IpAddress,
   carrierIdentity            [9] CarrierIdentity           OPTIONAL,
   wlanTunnelEvent            [10] WlanTunnelEvent,
   wlanTunnelEndReason        [11] WlanTunnelEndReason      OPTIONAL,
   ...
}

WlanActiveTunnelSession ::= SEQUENCE
{
   caseId                     [0] CaseIdentity,
   iAPSystemId                [1] IAPSystemIdentity         OPTIONAL,
   timestamp                  [2] TimeStamp,
   observedSubjectIdentity    [3] SubjectIdentity,
   subjectIPAddress           [4] IpAddress                 OPTIONAL,
   correlationNumber          [5] CorrelationNumber         OPTIONAL,
   tunnelorSession            [6] TunnelorSession           OPTIONAL,
```

```
   wlan_MS_IpAddress          [7] IpAddress                OPTIONAL,
   tunnelAddress              [8] IpAddress                OPTIONAL,
   carrierIdentity            [9] CarrierIdentity          OPTIONAL,
   wlanOperatorName           [10] WlanOperatorName        OPTIONAL,
   ...
}

WlanIPPacketHeader ::= SEQUENCE
{
   caseId                     [0] CaseIdentity,
   iAPSystemId                [1] IAPSystemIdentity        OPTIONAL,
   timestamp                  [2] TimeStamp,
   observedSubjectIdentity    [3] SubjectIdentity,
   streamID                   [4] StreamID,
   sourceIPAddress            [5] IpAddress,
   destinationIPAddress       [6] IpAddress,
   sourcePortNumber           [7] PortNumber               OPTIONAL,
   destinationPortNumber      [8] PortNumber               OPTIONAL,
   transportProtocol_ID       [9] TransportProtocol_ID,
   correlationNumber          [10] CorrelationNumber       OPTIONAL,
   ...
}

WlanIPPacketSummary ::= SEQUENCE
{
   caseId                     [0] CaseIdentity,
   iAPSystemId                [1] IAPSystemIdentity        OPTIONAL,
   timestamp                  [2] TimeStamp,
   observedSubjectIdentity    [3] SubjectIdentity,
   streamID                   [4] StreamID,
   sourceIPAddress            [5] IpAddress,
   destinationIPAddress       [6] IpAddress,
   sourcePortNumber           [7] PortNumber               OPTIONAL,
   destinationPortNumber      [8] PortNumber               OPTIONAL,
   count                      [9] PacketCount,
   transportProtocol_ID       [10] TransportProtocol_ID,
   correlationNumber          [11] CorrelationNumber       OPTIONAL,
   ...
}

-- Parameter Definitions

AccessPointName ::= IdentityType

CarrierIdentity ::= IdentityType

IAPSystemIdentity ::= IdentityType

IdentityType ::= CHOICE
{
   stringVS         [0] VisibleString,
   stringUTF8       [1] UTF8String,
   integer          [2] INTEGER,
   octets           [3] OCTET STRING,
   numeric          [4] NumericString
}

IPAddress ::= CHOICE
{
    ipV4            [1] IPvalue,
    ipV6            [2] IPvalue
}
```

```
IPvalue ::= OCTET STRING (SIZE(4..16)) – binary encoding

Location ::= SET OF SEQUENCE
{
   locationType     [0] UTF8String,
   location         [1] UTF8String
}

PacketCount ::= INTEGER

PortNumber ::= OCTET STRING

ServingSystemIdentity ::= IdentityType

StreamID ::= OCTET STRING

SubjectIdentity ::= SET
{
   msid          [0] MsID            OPTIONAL,
   macAddress    [1] MacAddress      OPTIONAL,
   nai           [2] NaI             OPTIONAL
}

MacAddress ::= OCTET STRING

MsID ::= OCTET STRING

NaI ::= OCTET STRING

TunnelorSession ::= ENUMERATED
{
   session          (0),
   tunnel           (1)
}

TransportProtocol_ID ::= IdentityType

WlanAccessEvent ::= ENUMERATED
{
   accessAttempt       (0),
   accessSuccessful    (1),
   accessFailure       (2),
   accessReject        (3),
   accessTermination   (4)
}

WlanAccessFailure ::= UTF8String

WlanIdentity ::= SET OF IdentityType

WlanLocationInformation ::= Location

WlanOperatorName ::= IdentityType

WlanTunnelEndReason ::= UTF8String

WlanTunnelEvent ::= ENUMERATED
{
   successful          (0),
   unsuccessful        (1),
   subject_disconnect  (2),
   network_disconnect  (3)
}
```

```
END -- of WLAN-LAES-CII-Abstract-Syntax-Module
```

A Annex A (Informative): Aspects of the *e*-Interface

This Annex is informative and is not considered part of this Standard.

A.1 Security and Integrity

Security services applicable to the *e*-interface (e.g., authentication, confidentiality, message integrity, and non-repudiation) are determined by arrangements between the SP and LEA.

If a hashing mechanism is used to provide a security service (e.g., message integrity), see FIPS Publication 180-2 with change notice[16], and the National Institute of Standards and Technology (NIST) policy on hash functions for Federal agencies[17].

A.2 Quality

The Quality of Service (QoS) on the *e*-interface is determined by arrangements between the SP and LEA.

A.3 Reliability

Measures that enable the delivery of all intercepted wire and electronic communications to and from a Subject's equipment, facilities, or services to the LEA (see Section 103(a) of [CALEA], 47 U.S.C. §1002(a)) are determined by arrangements between the SP and LEA. These measures include those that provide a high level of probability that the delivery of the intercepted wire and electronic communications will not be corrupted due to lost, dropped or omitted packets.

Metrics used on the *e*-interface for reliability are determined by arrangements between the SP and LEA.

[16] Federal Information Processing Standards (FIPS) 180-2, National Institute of Standards and Technology, Department of Commerce, August 1, 2002.

[17] This policy is currently located at: www.csrc.nist.gov/groups/ST/hash/policy.html.

B Annex B (Informative): Optional Messages

This Annex is informative and is not considered part of this Standard.

B.1 Stage 1 Description of Optional Messages

B.1.1 WLAN Surveillance Status Reporting Event

The WLAN surveillance status event defined in this Annex may be optionally reported and need not be reported for conformance to this Standard.

WLAN Surveillance Status reporting provides the LEA with information indicating that Electronic Surveillance on a Subject is active. WLAN Surveillance Status reporting is triggered when Electronic Surveillance on the Subject is started (e.g., provisioned or communication delivery is activated at the DF), stopped (e.g., de-provisioned or communication delivery is deactivated at the DF), and periodically during the Electronic Surveillance. The reporting shall occur at least once every 15 minutes.

B.2 Stage 2 Description of Optional Messages

B.2.1 WLAN Surveillance Status Message

The WLAN Surveillance Status message reports the status of a specific Electronic Surveillance. An Electronic Surveillance is either inactive (i.e., no reporting is occurring), active (i.e., all surveillance network entities are operational and reporting is occurring), or faulty (i.e., some of the surveillance network entities are not operational).

The message is triggered:

- at the start of an Electronic Surveillance;
- at the end of an Electronic Surveillance;
- when there is a change in the Electronic Surveillance status (e.g., from active to faulty or from faulty to active);
- periodically during the Electronic Surveillance.

The message shall be sent at least once every 15 minutes.

The WLAN Surveillance Status message includes the following parameters:

Table 6 WLAN Surveillance Status Message Parameters

Parameter	MOC	Usage/Conditions
CaseIdentity	M	Identifies the Subject.
IAPSystemIdentity	C	Identifies the network entity containing the IAP when the underlying data carriage does not imply that network entity.

Parameter	MOC	Usage/Conditions
TimeStamp	M	Identifies the date and time that the event was detected.
ObservedSubjectIdentity	M	Subject's observed identity or identities for each interception. Report all known identities (e.g., MSID, NAI, MAC Address).
WLANSurveillanceEvent	M	Start, Stop, Change, Periodic.
WLANSurveillanceStatus	M	Inactive, Active, Faulty.

B.3 Optional Messages Abstract Syntax Module

This section provides the ASN.1 [X-680] definitions for the optional messages. CII and CC corresponding to ASN.1 definitions are encoded according to BER [X.690].

```
WLAN-LAES-CII-Optional-Messages-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) tr45(0) cdma2000(1) cii-opt-
wlan(7) version-1(0)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

IMPORTS

CaseIdentity, TimeStamp
FROM Laesp-j-std-025-b
{iso(1) member-body(2) us(840) tia(113737) laes(2) tr45(0) j-std-025(0) j-std-025-
b(2) version-1(0)}

IAPSystemIdentity, SubjectIdentity
FROM WLAN-I-LAES-CII-Abstract-Syntax-Module
{iso(1) member-body(2) us(840) tia(113737) laes(2) tr45(0) cdma2000(1) cii-wlan(6)
version-1(0)};

wlan-LAES-CII-Optional-Messages-Abstract-Syntax-Module-OID   OBJECT IDENTIFIER  ::=
{iso(1) member-body(2) us(840) tia(113737) laes(2) tr45(0) cdma2000(1) cii-opt-
wlan(7) version-1(0)}

wlanOptionalProtocolIdentifier  OBJECT IDENTIFIER  ::=
          {wlan-LAES-CII-Optional-Messages-Abstract-Syntax-Module-OID},

WlanOptionalProtocol ::= SEQUENCE
{
   wlanOptionalProtocolIdentifier    OBJECT IDENTIFIER,
   wlanOptionalMessage               WlanOptionalMessage
}

WlanOptionalMessage ::= CHOICE
{
   wlanSurveillanceStatus     [0] WlanSurveillanceStatus
}

-- Message Definitions

WlanSurveillanceStatus ::= SEQUENCE
{
   caseId                     [0] CaseIdentity,
   iAPSystemId                [1] IAPSystemIdentity        OPTIONAL,
   timestamp                  [2] TimeStamp,
```

```
   observedSubjectIdentity    [3] SubjectIdentity,
   wlanSurveillanceEvent      [4] WLANSurveillanceEvent,
   wlanSurveillanceStatus     [5] WLANSurveillanceStatus,
   ...
}

-- Parameter Definitions

WLANSurveillanceEvent ::= ENUMERATED
{
   start            (0),
   stop             (1),
   change           (2),
   periodic         (3)
}

WLANSurveillanceStatus ::= ENUMERATED
{
   inactive         (0),
   active           (1),
   faulty           (2)
}

END -- of WLAN-LAES-CII-Optional-Messages-Abstract-Syntax-Module
```

THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

TIA represents the global information and communications technology (ICT) industry through standards development, advocacy, tradeshows, business opportunities, market intelligence and world-wide environmental regulatory analysis. With roots dating back to 1924, TIA enhances the business environment for broadband, mobile wireless, information technology, networks, cable, satellite and unified communications.

TIA members' products and services empower communications in every industry and market, including healthcare, education, security, public safety, transportation, government, the military, the environment and entertainment. TIA co-owns the SUPERCOMM® tradeshow and is accredited by the American National Standards Institute (ANSI).

TIA
ADVANCING GLOBAL COMMUNICATIONS

TIA
ADVANCING GLOBAL COMMUNICATIONS

HEADQUARTERS
2500 Wilson Boulevard
Suite 300
Arlington, VA 22201-3834
+1.703.907.7700
+1.703.907.7727 (fax)

tiaonline.org