ATIS-0700037

ATIS Standard on -

Enhanced Wireless Emergency Alert (eWEA) Federal Alert Gateway to CMSP Gateway Interface Specification

(A Revised Version of J-STD-101)

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-0700037

ATIS Standard on

Enhanced Wireless Emergency Alert (eWEA) Federal Alert Gateway to CMSP Gateway Interface Specification

(A Revised Version of J-STD-101)

Alliance for Telecommunications Industry Solutions

Approved December 28, 2017

Abstract

This Standard defines the interface between the Federal Alert Gateway and the Commercial Mobile Service Provider (CMSP) Gateway for WEA alerts. This ATIS specification supersedes J-STD-101*, Joint ATIS/TIA Federal Alert Gateway to CMSP Gateway Interface Specification,* and the associated J-STD-101 Supplements.

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Wireless Technologies and Systems Committee (WTSC) develops and recommends standards and technical reports related to wireless and/or mobile services and systems, including service descriptions and wireless technologies. WTSC develops and recommends positions on related subjects under consideration in other North American, regional, and international standards bodies.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

This ATIS Standard is a revision of J-STD-101, *Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification*, and its Supplement A in J-STD-101.a, Supplement B in J-STD-101.b, and Supplement C in ATIS-0700033.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, WTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, WTSC, which was responsible for its development, had the following leadership:

D. Zelmer, WTSC Chair (AT&T)

M. Younge, WTSC Vice Chair (T-Mobile)

P. Musgrove, WTSC SN Chair (AT&T)

G. Schumacher, WTSC SN Vice Chair (Sprint)

D. Sennett, Technical Editor (AT&T)

The Systems & Networks (SN) subcommittee was responsible for the development of this document.

Table of Contents

Table of Figures

Table of Tables

ATIS Standard on –

Enhanced Wireless Emergency Alert (eWEA) Federal Alert Gateway to CMSP Gateway Interface Specification (A Revised Version of J-STD-101)

Preface

The authority-to-individual emergency alerting capability to mobile devices was originally called Commercial Mobile Alert System (CMAS) in the first three Reports and Orders from the FCC. This standard was originally developed based upon the CMAS terminology and CMAS was operational in April 2012. However, in February 2013, the FCC renamed Commercial Mobile Alert System (CMAS) to Wireless Emergency Alerts (WEA) with associated updates to the appropriate sections of Part 11 of the 47 CFR. Subsequently, the FCC has issued additional enhancements and rules for this government-to-individual emergency alerting capability to mobile devices, and these are identified as modifications to WEA.

Consequently, this specification may use both the term CMAS and the term WEA. These terms should be considered as equivalent terms with WEA being the preferred term.

This ATIS specification is the Enhanced Wireless Emergency Alert (eWEA) standard for the WEA Federal Alert Gateway to CMSP Gateway interface and is based upon the WEA enhancements identified in the September 2016 FCC Report & Order on WEA Enhancements [Ref 41]. This ATIS specification supersedes the J-STD-101, *Joint ATIS/TIA Federal Alert Gateway to CMSP Gateway Interface Specification*, and the associated J-STD-101 Supplements. Any assumptions, requirements, and principles from J-STD-101 and the associated J-STD-101 Supplements that are applicable in eWEA are included in this ATIS specification.

In this specification, each unique requirement is numbered in the format of [JCMAS-C-RQMT-nnnn]. Any new requirements incorporated into this specification will have a suffix of R2A in the format of [JCMAS-C-RQMT-nnnn$_{R2A}$]. Any previous requirements that have been modified in this specification will have a suffix of R2M in the format of [JCMAS-C-RQMT-nnnn$_{R2M}$]. Any previous requirements that have been deleted in this specification will have a suffix of R2D in the format of [JCMAS-C-RQMT-nnnn$_{R2D}$] and the content of the deleted requirement will be replaced with the phrase “<Void>”.

1 Scope, Purpose, & Application

1.1 Scope

The scope of this Standard is the definition of the interface between the Federal Alert Gateway and the Commercial Mobile Service Provider (CMSP) Gateway for WEA alerts. Any processing in either the Federal network or the CMSP network that is not related to this interface is beyond the scope of this Standard.

1.2 Purpose

This Standard is based upon the four Reports & Orders issued to date by the Federal Communications Commission (FCC) in regards to the Wireless Emergency Alerts [Refs 9, 22, 24, & 41]. Modifications to this Standard may be required as future relevant Reports & Orders are released by the FCC.

The Federal government will perform the function of aggregating all state, local, and Federal alerts and will provide one logical interface to each CMSP that elects to support WEA alerts.

The purpose of this Standard is to define the interface between the Federal Alert Gateway and the CMSP Gateway for WEA alerts. The applicable assumptions, requirements, and principles from J-STD-101*, Joint ATIS/TIA Federal*

Alert Gateway to CMSP Gateway Interface Specification, and the associated J-STD-101 Supplements are included in this ATIS specification.

1.3 Application

This Standard is applicable to CMSPs and to the Federal government entity responsible for the administration of the Federal Alert Gateway.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this ATIS Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this ATIS Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[Ref 1] IETF RFC 7230, *Hypertext Transfer Protocol (HTTP/1.1*): Message Syntax and Routing.[1]

[Ref 2] IETF RFC 3986, *Uniform Resource Identifier (URI): Generic Syntax*.[1]

[Ref 3] IETF RFC 4301, *Security Architecture for the Internet Protocol*.[1]

[Ref 4] OASIS Standard CAP-V1.2*, Common Alerting Protocol, v.1.2*.[2]

[Ref 5] INCITS 38-2009[R2014], *Codes for the Identification of the States and Equivalent Areas within the United States, Puerto Rico, and the Insular Areas*; International Committee for Information Technology Standards (INCITS).[3]

[Ref 6] INCITS 31-2009[R2014], *Codes for the Identification of Counties and Equivalent Areas of the United States, Puerto Rico, and the Insular Areas*; International Committee for Information Technology Standards (INCITS).[4]

[Ref 7] Federal Information Processing Standards Publication 180-4*, Secure Hash Standard; National Institute of Standards and Technology (NIST)*.[5]

[Ref 8] IETF RFC 8141, *Uniform Resource Names (URNs)*.[1]

[Ref 9] FCC 08-99, *Federal Communications Commission First Report and Order In the Matter of The Commercial Mobile Alert System*; April 9, 2008.[6]

[Ref 10] IETF RFC 4303, *IP Encapsulating Security Payload (ESP)*.[1]

[Ref 11] National Weather Service Instruction 10-1712, *Operations and Services Dissemination Policy NWSPD 10-17 NOAA Weather Radio (NWR) All Hazards Specific Area Message Encoding (SAME)*.[7]

[Ref 12] IETF RFC 7296, *Internet Key Exchange Protocol Version 2 (IKEv2)*.[1]

[Ref 13] IETF 7321, *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*.[1]

[Ref 14] IETF RFC 3715, *IPsec-Network Address Translation (NAT) Compatibility Requirements*.[1]

[Ref 15] IETF RFC 4158, *Internet X.509 Public Key Infrastructure: Certification Path Building*.[1]

---

[1] This document is available from the Internet Engineering Task Force (IETF) at: < http://www.ietf.org >.

[2] This document is available from the Organization for the Advancement of Structured Information Standards (OASIS) at: < http://www.oasis-open.org/specs/index.php >.

[3] This document is available from the International Committee for Information Technology Standards (INCITS) at: < https://standards.incits.org/apps/group_public/project/details.php?project_id=206 >.

[4] This document is available from the International Committee for Information Technology Standards (INCITS) at: < https://standards.incits.org/apps/group_public/project/details.php?project_id=204 >.

[5] This document is available from the National Institute of Technology and Standards (NIST) at: < http://www.nist.gov/aes >.

[6] This document is available from the Federal Communications Commission at: < http://www.fcc.gov/ >.

[7] This document is available from the National Weather Service at: < http://www.weather.gov/ >.

[Ref 16] IETF RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*.[1]

[Ref 17] IETF RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*.[1]

[Ref 18] IETF RFC 8017, *PKCS #1: RSA Cryptography Specifications Version 2.2*.[1]

[Ref 19] IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.[1]

[Ref 20] WARN Act, *Security and Accountability For Every Port Act of 2006 (SAFE Port Act)*, Pub.L. 109-347, *Title VI-Commercial Mobile Service Alerts (WARN Act)*.[8]

[Ref 21] W3C Recommendation, *Extensible Markup Language (XML) 1.1 (Second Edition)*.[9]

[Ref 22] FCC 08-164, *Federal Communications Commission Second Report and Order and Further Notice of Proposed Rulemaking In the Matter of The Commercial Mobile Alert System*; July 8, 2008.[6]

[Ref 23] IETF RFC 793, *Transmission Control Protocol*.[1]

[Ref 24] FCC 08-184, *Federal Communications Commission Third Report and Order and Further Notice of Proposed Rulemaking In the Matter of The Commercial Mobile Alert System*; August 7, 2008.[6]

[Ref 25] FCC 08-166, *Federal Communications Commission Order on Reconsideration and Erratum In the Matter of The Commercial Mobile Alert System*; July 15, 2008.[6]

[Ref 26] ATIS-0700036, *Enhanced Wireless Emergency Alert (eWEA) Mobile Device Behavior Specification (a revised version of J-STD-100)*.[10]

[Ref 27] IETF RFC 1122, *Requirements for Internet Hosts – Communication Layers*.[1]

[Ref 28] IETF STD 5 (RFC 791), *Internet Protocol (IPv4) Specification*.[1]

[Ref 29] IETF STD 5 (RFC 792), *Internet Control Message Protocol*.[1]

[Ref 30] IETF RFC 8200, *Internet Protocol, Version 6 (IPv6) Specification*.[1]

[Ref 31] W3C Recommendation, *Namespaces in XML 1.1 (Second Edition)*.[9]

[Ref 32] IETF RFC 4291, *IP Version 6 Addressing Architecture*.[1]

[Ref 33] W3C Recommendation, *XML Schema Part 0: Primer Second Edition*.[9]

[Ref 34] IETF RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*.[1]

[Ref 35] W3C Recommendation, *Exclusive XML Canonicalization Version 1.0*.[9]

[Ref 36] FCC 07-214; *Federal Communications Commission Notice of Proposed Rulemaking in the Matter of the Commercial Mobile Alert System;* December 14, 2007.[6]

[Ref 37] IETF RFC 7231, *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content*.[1]

[Ref 38] W3C Recommendation, *XML Signature Syntax and Processing, Version 1.1*.[9]

[Ref 39] NIST SP 800-77, *Guide to IPsec VPNs*.[5]

[Ref 40] IETF RFC 4868, *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPSec*.[1]

[Ref 41] FCC 16-127, *Federal Communications Commission Report and Order and Further Notice of Proposed Rulemaking In the Matter of Wireless Emergency Alerts Amendments to Part 11 of the Commission's Rules Regarding the Emergency Alert System*; September 29, 2016.[6]

[Ref 42] ATIS-0700035, *Enhanced Wireless Emergency Alert (eWEA) Service Description*.[10]

[Ref 43] W3C Recommendation, *XML Schema Definition Language (XSD) 1.1 Part 1: Structures*.[9]

[Ref 44] W3C Recommendation, *XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes*.[9]

---

[8] This document is available from the U.S. Government Printing Office at: < http://www.gpo.gov/ >.

[9] This document is available from the World Wide Web Consortium (W3C) at: < http://www.w3.org/ >.

[10] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at: < http://www.atis.org >.

[Ref 45] W3C Recommendation, *XML Encryption Syntax and Processing*.[9]

[Ref 46] IETF RFC 2961, *Additional XML Security Uniform Resource Identifiers (URIs)*.[1]

[Ref 47] IETF RFC 1738, *Uniform Resource Locators (URL)*.[1]

3 Definitions, Acronyms, & Abbreviations

3.1 Definitions

Alert Message: An Alert Message is a message that is intended to provide the recipient information regarding an emergency, and that meets the requirements for transmission by a Participating Commercial Mobile Service Provider as defined in the FCC First Report and Order for the Commercial Mobile Alert System.

CMSP Gateway: A CMSP administered system, identified by a unique IP address or Fully Qualified Domain Name, interfacing to the Federal Alert Gateway and exchanging information per this Standard.

CMSP Gateway Group: A CMSP Gateway Group is the set of CMSP Gateways whose IP addresses or Fully Qualified Domain Names are visible to the Federal Alert Gateway across the Reference Point "C" interface. A CMSP Gateway Group will consist of one or two CMSP Gateways.

Common Alerting Protocol: The Common Alerting Protocol (CAP) refers to Organization for the Advancement of Structured Information Standards (OASIS) Standard CAP-V1.2, July 2011 [Ref 4], or any subsequent version of CAP adopted by OASIS and implemented by the CMAS.

Commercial Mobile Alert System: The Commercial Mobile Alert System (CMAS) refers to the voluntary emergency alerting system defined in the FCC First Report and Order [Ref 9], whereby Commercial Mobile Service Providers may elect to transmit Alert Messages to the public.

Commercial Mobile Service Provider: A Commercial Mobile Service Provider (or CMS Provider) is an FCC licensee providing commercial mobile service as defined in section 332 (d)(1) of the Communications Act of 1934 (47 U.S.C. 332(d)(1)). Section 332(d)(1) defines the term commercial mobile service as any mobile service (as defined in 47 U.S.C. 153) that is provided for profit and makes interconnected service available (a) to the public; or (b) to such classes of eligible users as to be effectively available to a substantial portion of the public, as specified by regulation by the Federal Communications Commission.

County and County Equivalent: Counties are considered to be the "first-order subdivisions" of each State and statistically equivalent entity, regardless of their local designations (county, parish, borough, etc.). Thus, the following entities are considered to be equivalent to counties for legal and/or statistical purposes: the parishes of Louisiana; the boroughs and census areas of Alaska; the District of Columbia; the independent cities of Maryland, Missouri, Nevada, and Virginia; that part of Yellowstone National Park in Montana; and various entities in the possessions and associated areas. Per the INCITS 31-2009 standard [Ref 6], the FIPS codes for county and county equivalents are maintained by the American National Standards Institute (ANSI) and are publicly available at < http://www.census.gov/geo/www/ansi/ansi.html >. As of 30 June 2017, there were 3,235 identified county and county equivalents.

Enhanced Wireless Emergency Alert (eWEA): A continued provision of effective WEA Alert Messages while leveraging advancements in technology to improve WEA's capabilities as defined in the 29 September 2016 FCC Report and Order on WEA Enhancements, FCC 16-127 [Ref 41].

Participating Commercial Mobile Service Provider: A Participating Commercial Mobile Service Provider (or a Participating CMS Provider) is a Commercial Mobile Service Provider that has voluntarily elected to transmit Alert Messages.

Public Safety Message: An essential public safety advisory that prescribes one or more actions likely to save lives and/or safeguard property as defined in the FCC Report and Order on WEA enhancements [Ref 41].

3.2 Acronyms & Abbreviations

AES	Advanced Encryption Standard
AH	Authentication Header

AMBER	America's Missing Broadcast Emergency Response
ANSI	American National Standards Institute
ATIS	Alliance for Telecommunications Industry Solutions
C-OTA	C-Interface Over The Air
CA	Certificate Authority
CAP	Common Alerting Protocol
CBC	Cipher Block Chaining
CFR	Code of Federal Regulations
CMA	Commercial Mobile Alert
CMAC	Commercial Mobile Alert for C Interface
CMAM	Commercial Mobile Alert Message
CMAS	Commercial Mobile Alert System
CMSAAC	Commercial Mobile Service Alert Advisory Committee
CMSP	Commercial Mobile Service Provider
COTS	Commercial Off-the Shelf
DHS	Department of Homeland Security
DTV	Digital Television
EAN	Emergency Alert Notification
EOC	Emergency Operations Center
ESP	Encapsulating Security Payload
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FIFO	First In First Out
FIPS[11]	Federal Information Processing Series – or – Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
GNIS	Geographic Names Information System
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange protocol
INCITS	International Committee for Information Technology Standards
IP	Internet Protocol
IPsec	IP Security
MODP	Modular Exponential Diffie-Hellman
NCE	Noncommercial Educational Broadcast Television Station
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
OCSP	Online Certificate Status Protocol
PBS	Public Broadcasting Service
PKI	Public Key Infrastructure

[11] In the context of identifiers of states, counties, and county equivalents, FIP means "Federal Information Processing Series". In the context of NIST standards, FIP means "Federal Information Processing Standard".

QoS	Quality of Service
RFC	Request for Comment
RMT	Required Monthly Test
RSA	Rivest, Shamir, and Adleman
RWT	Required Weekly Test
SA	Security Association
SHA-1	Secure Hash Algorithm One
TCP	Transmission Control Protocol
TIA	Telecommunications Industry Association
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WARN	Warning, Alert, & Response Network
WEA	Wireless Emergency Alert
XML	eXtensible Markup Language

4 Legislative & Regulatory Background

The Warning Alert and Response Network (WARN) Act[12] [Ref 20] is part of the Security and Accountability For Every Port Act of 2006 (SAFE Port Act) which was passed by Congress in September 2006 and was signed into law by President Bush on 13 October 2006.

Based upon the WARN Act, "*the Commission[13] shall complete a proceeding to adopt relevant technical standards, protocols, procedures, and other technical requirements based on the recommendations of such Advisory Committee[14] necessary to enable commercial mobile service alerting capability for commercial mobile service providers that voluntarily elect to transmit emergency alerts*".[15]

Within the WARN Act, Congress defined CMSPs as "*any licensee providing commercial mobile service (as defined in section 332(d)(1) of the Communications Act of 1934 (47 U.S.C. 332(d)(1)))*."[16]

Though legislation and regulatory provisions are included in this document, it is the detailed requirements in clauses 5, 7.1, 7.2, 7.6, and 7.7 – including their associated subclauses – that will be verified to certify the performance of this interface. These lower level requirements have been developed to satisfy the legislative requirements.

4.1 Key WARN Act Provisions

The following is a summary of provisions in the WARN Act. Note that not all provisions may be applicable to this Standard, but are listed here for completeness. The provisions stated below are taken from the WARN Act [Ref 4] and the reader should assume that term "commercial mobile service operators" and "commercial mobile service licensee" are synonymous with the term "commercial mobile service provider (CMSP)" defined in clause 3, *Definitions, Acronyms, & Abbreviations*.

[12] Security and Accountability For Every Port Act of 2006 (SAFE Port Act), Pub.L. 109-347, Title VI-Commercial Mobile Service Alerts (WARN Act).

[13] The "Commission" referenced in the WARN Act is the Federal Communications Commission.

[14] The "Advisory Committee" referenced in this quote is the Commercial Mobile Service Alerts Advisory Committee (CMSAAC) as in WARN Act § 602(a).

[15] WARN Act § 602(a).

[16] WARN Act § 602(b)(1)(A).