



**ATIS-0700037.v003**

ATIS Standard on -

**Wireless Emergency Alert (WEA) 3.0 Federal Alert Gateway  
to CMSP Gateway Interface Specification**



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](http://www.atis.org).

---

### Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF NOR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to <https://www.atis.org/policy/patent-assurances/> to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

---

*Published by*

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

Copyright © 2022 by Alliance for Telecommunications Industry Solutions  
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

**ATIS-0700037.v003**

ATIS Standard on

# **Wireless Emergency Alert (WEA) 3.0 Federal Alert Gateway to CMSP Gateway Interface Specification**

**Alliance for Telecommunications Industry Solutions**

Approved March 2, 2022

## **Abstract**

This Standard defines the interface between the Federal Alert Gateway and the Commercial Mobile Service Provider (CMSP) Gateway for WEA alerts.

## 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.

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:

- M. Younge, WTSC Chair (T-Mobile USA)
- T. Brooks, WTSC SN Chair & Technical Editor (T-Mobile USA)
- P. Musgrove, WTSC SN Vice Chair (AT&T)

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

# Table of Contents

---

Preface .....	1
1 Scope, Purpose, & Application .....	1
1.1 Scope.....	1
1.2 Purpose .....	1
1.3 Application .....	2
2 References .....	2
2.1 Normative References .....	2
2.2 Informative References.....	4
3 Definitions, Acronyms, & Abbreviations .....	4
3.1 Definitions .....	4
3.2 Acronyms & Abbreviations.....	5
4 Requirements .....	6
4.1.1 <i>Reference Point “C” Interface Overview</i> .....	6
4.2 Federal Alert Gateway Requirements.....	9
4.2.1 <i>Federal Alert Gateway Requirements for CMSP Profile</i> .....	9
4.2.2 <i>Federal Alert Gateway Requirements for Connection Establishment</i> .....	10
4.2.3 <i>Federal Alert Gateway Requirements for Message Transmission</i> .....	10
4.2.4 <i>Federal Alert Gateway Requirements for Message Reception</i> .....	12
4.3 CMSP Gateway Requirements .....	13
4.3.1 <i>CMSP Gateway Requirements for Federal Alert Gateway Profile</i> .....	13
4.3.2 <i>CMSP Gateway Requirements for Connection Establishment</i> .....	13
4.3.3 <i>CMSP Gateway Requirements for Message Transmission</i> .....	14
4.3.4 <i>CMSP Gateway Requirements for Message Reception</i> .....	15
4.3.5 <i>CMSP Gateway Requirements for Logging of Message Reception</i> .....	16
4.4 Quality of Service Requirements .....	16
4.4.1 <i>Prioritization</i> .....	16
4.4.2 <i>Message Queuing</i> .....	17
4.5 Security Requirements .....	17
4.5.1 <i>PKI Infrastructure Requirements</i> .....	18
4.5.2 <i>IPsec Requirements</i> .....	19
4.5.3 <i>Non-Repudiation</i> .....	21
5 Reference Point “C” Call Flows .....	22
5.1 CMAC Alert Message Call Flows.....	22
5.1.1 <i>CMAC Message without CAP Message Retrieval Call Flow</i> .....	23
5.1.2 <i>CMAC Message with CAP Message Retrieval Call Flow</i> .....	24
5.1.3 <i>Failure to Retrieve CAP Message Call Flows</i> .....	26
5.1.4 <i>Invalid CMAC Message Call Flow</i> .....	30
5.2 Link Test Message Call Flows .....	32
5.2.1 <i>Link Test Message to CMSP Gateway Call Flow</i> .....	32
5.2.2 <i>Invalid Link Test Message to CMSP Gateway Call Flow</i> .....	33
5.2.3 <i>Link Test Message from CMSP Gateway Call Flow</i> .....	33
5.2.4 <i>Invalid Link Test Message from CMSP Gateway Call Flow</i> .....	34
5.3 Required Monthly Test (RMT) Call Flow.....	35
5.4 Transmission Control Message Call Flows.....	36
5.4.1 <i>Cease Transmissions Call Flow</i> .....	36
5.4.2 <i>Resume Transmissions Call Flow</i> .....	37
6 Federal Alert Gateway to CMSP Gateway Protocol Requirements & Definition .....	38

6.1	Application Layer .....	39
6.1.1	CMAC Protocol .....	39
6.1.2	HTTP.....	41
6.2	Message Structure.....	41
6.2.1	CMAC_Alert_Attributes Segment .....	41
6.2.2	CMAC_alert_info Segment .....	42
6.2.3	CMAC_Alert_Area Segment.....	42
6.2.4	CMAC_Alert_Text Segment.....	42
6.2.5	CMAC_Digital_Signature Segment .....	42
6.2.6	CMAC Alert Message Document Object Model.....	42
6.2.7	CMAC Message Types .....	44
6.3	Element Definition.....	47
6.3.1	CMAC_Alert_Attributes Segment Element Definition .....	47
6.3.2	CMAC_alert_info Segment Element Definition .....	51
6.3.3	CMAC_Alert_Area Segment Element Definition .....	52
6.3.4	CMAC_Alert_Text Segment Element Definition .....	53
6.3.5	CMAC_Digital_Signature Segment Element Definition .....	55
6.3.6	Definition of CMAC_cmas_geocode Element.....	55
6.3.7	Definition of CMAC_cap_geocode Element .....	55
6.4	CMAC Message XML Schema Definition .....	56
6.5	CMAC Message Types & Example XML .....	59
6.5.1	Alert Message .....	60
6.5.2	Update Message .....	65
6.5.3	Cancel Message .....	71
6.5.4	Ack Message .....	73
6.5.5	Error Message .....	73
6.5.6	Link Test Message.....	75
6.5.7	RMT Message.....	76
6.5.8	Transmission Control – Cease Message.....	78
6.5.9	Transmission Control – Resume Message.....	79
6.6	DBGF Bypass Request.....	79
6.7	Transport Protocol .....	80
6.7.1	Transmission Control Protocol (TCP).....	80
6.7.2	Internet Protocol (IP).....	80
6.8	Error Handling.....	80
6.8.1	TCP/IP Error Handling .....	80
6.8.2	HTTP Level Error Handling.....	81
6.8.3	CMAC Error Handling .....	81
A	Public Broadcasting Service Digital Television Interface to CMSP Gateway.....	83
A.1	Scope.....	83
A.2	Reference Point “C1” Related Requirements .....	84
A.3	Reference Point “C1” Call Flows .....	86
A.3.1	Reference Point “C1” Valid Message Call Flow .....	86
A.3.2	Reference Point “C1” Invalid Message Call Flow .....	87
A.4	Reference Point “C1” Messages.....	87
B	Reference Point “C” Interface Startup Procedure .....	89
C	Qualification Provisions .....	90
C.1	Glossary.....	90
C.2	Responsibility for Verification.....	90
C.2.1	Developmental Test & Evaluation (DT&E).....	90
C.2.2	Verification Methods .....	91
C.2.3	Security Test & Evaluation.....	91
C.3	System Monitoring .....	91
C.4	Performance Monitoring .....	91

D Configurable Parameters .....	92
E Example of End to End Message Identification .....	94

## Table of Figures

Figure 4.1 – Federal Alert Gateway to CMSP Gateway Message Type Summary .....	7
Figure 5.1 – CMAC Message without CAP Message Retrieval Call Flow .....	23
Figure 5.2 – CMAC Message with CAP Message Retrieval Call Flow .....	25
Figure 5.3 – Federal Alert Gateway Failure to Retrieve CAP Message Call Flow .....	27
Figure 5.4 – CMSP Gateway Detection of Failure to Retrieve Corresponding CAP Message .....	29
Figure 5.5 – Invalid CMAC Message Call Flow .....	31
Figure 5.6 – Link Test Message to CMSP Gateway Call Flow .....	32
Figure 5.7 – Invalid Link Test Message from Federal Alert Gateway Call Flow .....	33
Figure 5.8 – Link Test Message from CMSP Gateway Call Flow .....	34
Figure 5.9 – Invalid Link Test Message from CMSP Gateway Call Flow .....	35
Figure 5.10 – Required Monthly Test Call Flow .....	36
Figure 5.11 – Cease Transmissions Call Flow .....	37
Figure 5.12 – Resume Transmissions Call Flow .....	38
Figure 6.1 – Reference Point “C” Document Object Model .....	43
Figure A.1 – Public Broadcasting Service WEA Architecture .....	83
Figure A.2 – Reference Point “C1” Valid Message Call Flow .....	86
Figure A.3 – Reference Point “C1” Invalid Message Call Flow .....	87
Figure B.1 – Reference Point “C” Interface Startup Procedures .....	89
Figure E.1 – End-to-End Mapping of Message Identifiers .....	94
Figure E.2 – Message Identifiers with Multiple CMSP Gateways .....	95
Figure E.3 – Example Database for Correlating Message Identifiers .....	96

## Table of Tables

Table 4.1 – Characteristics of Messages from Federal Alert Gateway .....	7
Table 4.2 – Characteristics of Messages from CMSP Gateway .....	8
Table 4.3 – CMSP Profile Definition .....	9
Table 4.4 – Federal Alert Gateway Profile Definition .....	13
Table 4.5 – Required Algorithms for Implementation of ESP .....	19
Table 4.6 – Required Algorithms for Implementation of IKE v2 .....	20
Table 4.7 – Summary of References for IPsec .....	20
Table 4.8 – XML Signature Algorithm Summary .....	21
Table 6.1 – CMAC Message Segments .....	44
Table 6.2 – Federal Alert Gateway Initiated Messages .....	45
Table 6.3 – CMSP Gateway Initiated Messages .....	46
Table 6.4 – CMAC_Alert_Attributes Segment Element Definition .....	47
Table 6.5 – CMAC_alert_info Segment Element Definition .....	51
Table 6.6 – CMAC_Alert_Area Segment Element Definition .....	52
Table 6.7 – CMAC_Alert_Text Segment Element Definition .....	54
Table 6.8 – CMAC_Digital_Signature Segment Element Definition .....	55
Table 6.9 – Elements of Alert Attributes Segment for Alert Message .....	60
Table 6.10 – Elements of Alert Info Segment for Alert Message .....	61

Table 6.11 – Elements of Alert Area Segment for Alert Message.....	61
Table 6.12 – Elements of Alert Text Segment for Alert Message .....	62
Table 6.13 – Elements of Alert Attributes Segment for Update Message.....	65
Table 6.14 – Elements of Alert Info Segment for Update Message .....	66
Table 6.15 – Elements of Alert Area Segment for Update Message .....	67
Table 6.16 – Elements of Alert Text Segment for Update Message .....	67
Table 6.17 – Elements of Alert Attributes Segment for Cancel Message .....	71
Table 6.18 – Elements of Alert Attributes Segment for Ack Message .....	73
Table 6.19 – Elements of Alert Attributes Segment for Error Message .....	74
Table 6.20 – Elements of Alert Attributes Segment for Link Test Message.....	75
Table 6.21 – Elements of Alert Attributes Segment for RMT Message.....	76
Table 6.22 – Elements of Alert Info Segment for RMT Message.....	76
Table 6.23 – Elements of Alert Text Segment for RMT Message.....	77
Table 6.24 – Elements of Alert Attributes Segment for Transmission Control – Cease Message .....	78
Table 6.25 – Elements of Alert Attributes Segment for Transmission Control – Resume Message .....	79
Table 6.26 – Definition of CMAC Response Codes.....	82
Table A.1 – Reference Point “C1” CMAC Message Segments.....	87
Table D.1 – Configurable Parameters .....	92

ATIS Standard on –

# Wireless Emergency Alert (WEA) 3.0 Federal Alert Gateway to CMSP Gateway Interface Specification

## Preface

The authority-to-individual emergency alerting capability to mobile devices was originally called Commercial Mobile Alert System (CMAS) in the first three Reports & 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 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 Wireless Emergency Alert (WEA) 3.0 standard for the WEA Federal Alert Gateway to CMSP Gateway interface and is based upon the cumulative WEA enhancements identified up through the January 2018 FCC Second Report & Order and Second Order on Reconsideration, FCC 18-4 [Ref 48].

The use of the term WEA in this specification refers to WEA 3.0, unless otherwise specifically indicated

This specification is targeted at Participating CMSPs per the FCC definition described in ATIS-0700035, *Wireless Emergency Alert (3.0) Service Description* [Ref 100]. All references to CMSPs in this specification refer to Participating CMSPs.

The WEA regulatory background is described in detail in the Service Description in ATIS-0700035 [Ref 100].

In this specification, each unique requirement is numbered in the format of [WEA-C-RQMT-nnnn]. Any new requirements added for WEA 3.0 incorporated into this specification will have a suffix of R3A in the format of [WEA-C-RQMT-nnnnR3A]. Any WEA 2.0 requirements that have been modified for WEA 3.0 in this specification will have a suffix of R3M in the format of [WEA-C-RQMT-nnnnR3M]. Any WEA 2.0 requirements that have been deleted from WEA 3.0 in this specification will have a suffix of R3D in the format of [WEA-C-RQMT-nnnnR3D] 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 five Reports & Orders issued to date by the Federal Communications Commission (FCC) in regard to the Wireless Emergency Alerts [Refs 9, 22, 24, 48 and 51]. 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.