



ATIS-0700038.v002

ATIS Standard on -

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

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 OR 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 [<http://www.atis.org/legal/patentinfo.asp>] 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 © 2019 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> >.

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

Alliance for Telecommunications Industry Solutions

Approved: September 10, 2019

Abstract

This Standard defines the testing of the interface between the Federal Alert Gateway and the Commercial Mobile Service Provider (CMSP) Gateway for WEA alerts based upon the requirements in ATIS-0700037.v002, *Wireless Emergency Alert (eWEA) Federal Alert Gateway to CMSP Gateway Interface Specification*.

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:

- 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)
- P. Sanders, Technical Editor (one2many)

The WTSC Systems and 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 Normative References	2
3 Definitions, Acronyms, & Abbreviations	3
3.1 Definitions	3
3.2 Acronyms & Abbreviations	4
4 Testing Methodology & Environment	5
4.1 Test Environment Architecture	5
4.2 Test Tools	9
4.2.1 Alert Origination Simulator	9
4.3 Test Personnel	9
4.3.1 Federal Test Support	9
4.3.2 CMSP Test Support	9
4.4 Pre-Test Requirements	9
4.4.1 Pre-Test Notes	10
4.4.2 Pre-Test Requirements Addressed	10
4.4.3 Pre-Test Verification Items	10
4.5 Pre-Test Configuration Information	11
4.5.1 Configuration Worksheet for Federal Alert Gateway	11
4.5.2 Configuration Worksheet for CMSP Gateway	13
4.6 Configurations for Test Cases	14
5 Test Cases	15
5.1 Federal Alert Gateway Stand-Alone Test Cases	15
5.1.1 CMAS-TC-101 – Federal Alert Gateway Profile Data Test	16
5.2 CMSP Gateway Stand-Alone Test Cases	17
5.2.1 CMAS-TC-201 – CMSP Gateway Profile Data Test	18
5.3 Inter-Gateway Test Cases	19
5.3.1 CMAS-TC-001 – Alert Message Test	20
5.3.2 CMAS-TC-002 – Digital Signature Test	27
5.3.3 CMAS-TC-003 – Update Message Test	29
5.3.4 CMAS-TC-004 – Cancel Message Test	35
5.3.5 CMAS-TC-005 – Required Monthly Test (RMT) Test	38
5.3.6 CMAS-TC-006 – Link Test Messages Test	40
5.3.7 CMAS-TC-007 – Transmission Control Test	44
5.3.8 CMAS-TC-008 – General Connectivity Test via Link Test Message	48
5.3.9 CMAS-TC-009 – General Connectivity Test via Transmission Control Resume Message	55
5.3.10 CMAS-TC-010 – Geo-Location Filtering Test	62
5.3.11 CMAS-TC-011 – Messaging Queuing Test	66
5.3.12 CMAS-TC-012 – CAP Retrieval Test	69
6 Cross Reference of Requirements to Test Cases	71
Annex A Summary of Reference Point “C” Interface Requirements	80
Annex B Input CAP Messages	91
B.1 CAP Message #1 – Imminent Threat Alert	91

B.2	CAP Message #2 – Presidential Alert	92
B.3	CAP Message #3 – AMBER Alert	94
B.4	CAP Message #4 – Imminent Threat Update	95
B.5	CAP Message #5 – Presidential Update	97
B.6	CAP Message #6 – AMBER Update	98
B.7	CAP Message #7 – Invalid CMAS Criteria Update	99
B.8	CAP Message #8 – Imminent Threat Cancel	101
B.9	CAP Message #9 – Imminent Threat Alert for Geo Location Filtering.....	101
B.10	CAP Message #10 – Imminent Threat Update for Geo Location Filtering	103
B.11	CAP Message #11 – Imminent Threat Cancel for Geo Location Filtering.....	104
B.12	CAP Message #12 – Public Safety Alert	105
B.13	CAP Message #13 – State/Local WEA Test Alert	106
B.14	CAP Message #14 – Public Safety Update	108
B.15	CAP Message #15 – State/Local WEA Test Update	109
Annex C Expected CMAC Messages		111
C.1	CMAC Message #1 – Expected Results of CAP Message #1	111
C.1.1	CMAC Message #1 – Imminent Threat Alert (Expected Result of CAP Message #1).....	111
C.1.2	CMAC Message #1A – Imminent Threat Alert with Expanded Digital Signature Segment (Expected Result of CAP Message #1).....	113
C.2	CMAC Message #2 – Presidential Alert (Expected Result of CAP Message #2)	114
C.3	CMAC Message #3 – AMBER Alert (Expected Result of CAP Message #3).....	115
C.4	CMAC Message #4 – Imminent Threat Update (Expected Result of CAP Message #4).....	116
C.5	CMAC Message #5 – Presidential Update (Expected Result of CAP Message #5).....	118
C.6	CMAC Message #6 – AMBER Update (Expected Result of CAP Message #6).....	120
C.7	CMAC Message #7 – Invalid WEA Criteria Cancel (Expected Result of CAP Message #7) ..	122
C.8	CMAC Message #8 – Imminent Threat Cancel (Expected Result of CAP Message #8)	122
C.9	CMAC Message #9 – RMT	123
C.10	CMAC Message #10 – Federal Alert Gateway Initiated Link Test	124
C.11	CMAC Message #11 – CMSP Gateway Initiated Link Test	125
C.12	CMAC Message #12 – Transmission Control – Cease	125
C.13	CMAC Message #13 – Transmission Control – Resume	126
C.14	CMAC Message #14 – Public Safety Alert (Expected Result of CAP Message #12).....	126
C.15	CMAC Message #15 – State/Local WEA Test Alert (Expected Result of CAP Message #13) 127	
C.16	CMAC Message #16 – Public Safety Update (Expected Result of CAP Message #14)	128
C.17	CMAC Message #17 – State/Local WEA Test Update (Expected Result of CAP Message #15) 130	
Annex D Expected ACK Messages		133
D.1	Ack Message #1 (Expected Result of CMAC Message #1)	133
D.2	Ack Message #2 (Expected Result of CMAC Message #2)	133
D.3	Ack Message #3 (Expected Result of CMAC Message #3)	134
D.4	Ack Message #4 (Expected Result of CMAC Message #11)	134
D.5	Ack Message #5 (Expected Result of CMAC Message #14)	134
D.6	Ack Message #6 (Expected Result of CMAC Message #15)	135
Annex E Requirements Not Verified by Tests in This Specification		136

Table of Figures

Figure 4.1: C-Interface Test Architecture for Single CMSP Gateway	6
Figure 4.2: C-Interface Test Architecture for Dual CMSP Gateways	7
Figure 4.3: C-Interface Test Architecture for Dual Federal Alert Gateways and Dual CMSP Gateways.....	8

Table of Tables

Table 4.1: Configuration Worksheet for Federal Alert Gateway.....	11
Table 4.2: Configuration Worksheet for CMSP Gateway.....	13
Table 5.1: Steps for Test Case CMAS-TC-101 – Federal Alert Gateway Profile Data Test	17
Table 5.2: Steps for Test Case CMAS-TC-201 – CMSP Gateway Profile Data Test.....	19
Table 5.3: Steps for Test Case CMAS-TC-001 - Alert Message Test.....	22
Table 5.4: Steps for Test Case CMAS-TC-002 – Digital Signature Test	28
Table 5.5: Steps for Test Case CMAS-TC-003 – Update Message Test.....	31
Table 5.6: Steps for Test Case CMAS-TC-004 – Cancel Message Test	37
Table 5.7: Steps for Test Case CMAS-TC-005 – Required Monthly Test (RMT) Test.....	40
Table 5.8: Steps for Test Case CMAS-TC-006 – Link Test Messages Test.....	42
Table 5.9: Steps for Test Case CMAS-TC-007 – Transmission Control Test.....	46
Table 5.10: Steps for Test Case CMAS-TC-008 – General Connectivity Test via Link Test Message	50
Table 5.11: Steps for Test Case CMAS-TC-009 – General Connectivity Test via Transmission Control Resume Message	57
Table 5.12: Steps for Test Case CMAS-TC-010 – Geo-Location Filtering Test.....	63
Table 5.13: Steps for Test Case CMAS-TC-011 – Message Queuing Test.....	67
Table 5.14: Steps for Test Case CMAS-TC-012 – CAP Retrieval Test	71
Table 6.1: Cross Reference Matrix of Requirements to Test Cases	72

ATIS Standard on –

Wireless Emergency Alert (WEA) 3.0 Federal Alert Gateway to CMSP Gateway Interface Test 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 and Orders from the Federal Communications Commission (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 specification contains references to the uniquely numbered requirements in ATIS-0700037.v002 [Ref 1]. Any requirements which have been added, modified, or deleted from the eWEA version of the C-Interface specification will have suffixes applied to their requirement numbers. Any new requirements will have a suffix of R3A in the format of [WEA-C-RQMT-nnnnR3A]. Any modified requirements will have a suffix of R3M in the format of [WEA-C-RQMT-nnnnR3M]. Any deleted requirements will have a suffix of R3D in the format of [WEA-C-RQMT-nnnnR3D].

This ATIS specification is the Wireless Emergency Alert (WEA) 3.0 standard for the testing of the WEA Federal Alert Gateway to CMSP Gateway interface, and it is based upon the requirements in ATIS-0700037.v002 [Ref 1]. This ATIS specification supersedes ATIS-700038, *Enhanced Wireless Emergency Alert (eWEA) Federal Alert Gateway to CMSP Gateway Interface Test Specification*. Any assumptions, requirements, and test cases from ATIS-0700038 applicable in WEA 3.0 are included in this test specification.

1 Scope, Purpose, & Application

1.1 Scope

This Standard defines operational testing procedures for the communications between the Federal Alert Gateway and the Commercial Mobile Service Provider (CMSP) Gateway over the C-Interface. This includes operational testing of all processing functionality within the Federal Emergency Management Agency (FEMA)-administered WEA entities and the CMSP-administered WEA entities that directly impacts communications over the C-Interface. Operational testing of all other processing within the FEMA and CMSP entities including the CMSP infrastructure is beyond the scope of this Standard.

1.2 Purpose

The purpose of interface testing is to evaluate whether systems or components transmit data and control information correctly to each other. In addition, the tests defined in this Standard may be used during regression testing when updates are made to either the Federal Alert Gateway or the CMSP Gateway.

Specifically, ATIS-0700038.v002 [Ref 1] defines a set of tests to verify the following minimal set of functionalities during interface and regression testing:

- Ability to complete the C-Interface startup procedures.
- Ability to bring up the IP Security (IPSec) tunnel.
- Ability to bring up the Transmission Control Protocol (TCP)/Internet Protocol (IP) connection.