



J-STD-101

**JOINT ATIS/TIA CMAS FEDERAL ALERT GATEWAY TO
CMSP GATEWAY INTERFACE SPECIFICATION**

JOINT STANDARD



ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 300 companies actively formulate standards in ATIS' 20 Committees, covering issues including: IPTV, Service Oriented Networks, Home Networking, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support. In addition, numerous Incubators, Focus and Exploratory Groups address emerging industry priorities including "Green", IP Downloadable Security, Next Generation Carrier Interconnect, IPv6 and Convergence.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications' Sectors, and a member of the Inter-American Telecommunication Commission (CITEL).

< <http://www.atis.org/> >



The Telecommunications Industry Association (TIA) is the leading trade association representing the global information and communications technology (ICT) industries through standards development, government affairs, business opportunities, market intelligence, certification and world-wide environmental regulatory compliance. With support from its 600 members, TIA enhances the business environment for companies involved in telecommunications, broadband, mobile wireless, information technology, networks, cable, satellite, unified communications, emergency communications and the greening of technology. TIA is accredited by ANSI.

< <http://www.tiaonline.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, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES ANY AND ALL USE OF OR RELIANCE UPON THIS 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.
--

J-STD-101, *Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification*

Is an ATIS & TIA Joint Standard developed by the **WTSC-G3GSN** Subcommittee under the **ATIS Wireless Technologies and Systems Committee (WTSC)** and the **TR-45.8 Core Networks - Mobile and Personal Communications Standards** Subcommittee under the **TIA Engineering Committee TR-45**.

Published by

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

Telecommunications Industry Association
Standards & Technology Department
2500 Wilson Boulevard, Suite 300
Arlington, VA 22201

Copyright © 2009 by Alliance for Telecommunications Industry Solutions and Telecommunications Industry Association
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/> >.

Printed in the United States of America.

JOINT ATIS/TIA CMAS FEDERAL ALERT GATEWAY TO CMSP GATEWAY INTERFACE SPECIFICATION

Alliance for Telecommunications Industry Solutions

Approved October 2009

Abstract

This Standard defines the interface between the Federal Alert Gateway and the Commercial Mobile Service Provider (CMSP) Gateway for CMAS 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 Telecommunications Industry Association (TIA) is the leading trade association representing the global information and communications technology (ICT) industries through standards development, government affairs, business opportunities, market intelligence, certification and world-wide environmental regulatory compliance. Engineering Committee TR-45 develops performance, compatibility, interoperability and service standards for mobile and personal communications systems. These standards pertain to, but are not restricted to, service information, wireless terminal equipment, wireless base station equipment, wireless switching office equipment, ancillary apparatus, auxiliary applications, inter-network and intersystem operations, interfaces, and wireless packet data technologies.

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.

The participating companies and organizations responsible for the development of this Standard are as follows.

TR. 45

Alcatel-Lucent
 AT&T
 CDMA Development Group
 CommFlow Resources
 Ericsson
 LG Electronics
 Motorola

Qualcomm
 Samsung
 SigmaDelta Communications Group
 Spring Nextel
 Verizon
 ZTE

WTSC

Aircell LLC
 Alcatel-Lucent
 AT&T
 Department of Defense
 Department of Homeland Security/FEMA
 Embarq
 Ericsson
 FBI-ESTS
 Harris Stratex Networks
 Huawei Technologies
 Intel
 Interdigital
 Kineto Wireless
 LG Info Comm
 Mavenir Systems
 National Communication Systems
 NII Holdings

Nokia Siemens Networks
 Nokia, Inc.
 Nortel Networks
 One2Many
 Public Safety and Emergency Preparedness Canada
 Qualcomm Incorporated
 Qwest
 Research In Motion
 Rogers Wireless
 Sprint
 T-Mobile
 Telcordia Technologies
 Telecommunication Systems
 Tellabs Operations
 True Position
 US Department of Commerce
 Verizon

The **ATIS WTSC-G3GSN** Subcommittee and the **TIA TR-45.8** Subcommittee were responsible for the development of this document.

TABLE OF CONTENTS

1 SCOPE, PURPOSE, & APPLICATION	1
1.1 SCOPE.....	1
1.2 PURPOSE.....	1
1.3 APPLICATION.....	1
2 NORMATIVE REFERENCES	1
3 DEFINITIONS, ACRONYMS, & ABBREVIATIONS	3
3.1 DEFINITIONS	3
3.2 ACRONYMS & ABBREVIATIONS.....	4
4 LEGISLATIVE & REGULATORY BACKGROUND	6
4.1 KEY WARN ACT PROVISIONS	6
4.2 FCC CMAS REPORT AND ORDERS	7
4.2.1 <i>FCC First Report and Order</i>	8
4.2.2 <i>FCC Second Report and Order</i>	8
4.2.3 <i>FCC Third Report and Order</i>	9
4.3 REFERENCE DIAGRAM.....	10
4.3.1 <i>Reference Point “C”</i>	10
4.3.2 <i>Federal Alert Gateway</i>	11
4.3.3 <i>CMSP Gateway</i>	11
4.3.4 <i>Reference Point C Interface via Digital Television Transmission Towers</i>	11
5 REQUIREMENTS	12
5.1 GENERAL REFERENCE POINT “C” SYSTEM REQUIREMENTS	12
5.1.1 <i>Federal Alert Gateway Considerations from FCC First Report and Order</i>	13
5.1.2 <i>CMSP Gateway Considerations from FCC First Report and Order</i>	14
5.1.3 <i>CMSP Gateway Considerations from CMSAAC Recommendations</i>	15
5.1.4 <i>RMT and Periodic Testing Considerations</i>	16
5.1.4.1 <i>Required Monthly Test (RMT) Considerations</i>	17
5.1.4.2 <i>Periodic Interface Testing Considerations</i>	18
5.1.4.3 <i>Federal Alert Gateway Testing Considerations</i>	18
5.1.4.4 <i>Testing Functionality Considerations of CMSP Gateway</i>	18
5.1.5 <i>Reference Point “C” Interface Overview</i>	18
5.2 FEDERAL ALERT GATEWAY REQUIREMENTS	21
5.2.1 <i>Federal Alert Gateway Requirements for CMSP Profile</i>	21
5.2.1.1 <i>Federal Alert Gateway Definition of CMSP Profile</i>	22
5.2.2 <i>Federal Alert Gateway Requirements for Connection Establishment</i>	22
5.2.3 <i>Federal Alert Gateway Requirements for Message Transmission</i>	23
5.2.4 <i>Federal Alert Gateway Requirements for Message Reception</i>	25
5.3 CMSP GATEWAY REQUIREMENTS	25
5.3.1 <i>CMSP Gateway Requirements for Federal Alert Gateway Profile</i>	25
5.3.1.1 <i>CMSP Gateway Definition of Federal Alert Gateway Profile</i>	26
5.3.2 <i>CMSP Gateway Requirements for Connection Establishment</i>	26
5.3.3 <i>CMSP Gateway Requirements for Message Transmission</i>	27
5.3.4 <i>CMSP Gateway Requirements for Message Reception</i>	28
5.4 QUALITY OF SERVICE REQUIREMENTS.....	29
5.4.1 <i>Prioritization</i>	29
5.4.2 <i>Message Queuing</i>	29
5.5 SECURITY REQUIREMENTS	30
5.5.1 <i>PKI Infrastructure Requirements</i>	30
5.5.1.1 <i>X509 Certificates</i>	31
5.5.1.2 <i>IPsec X.509 Identifiers</i>	31
5.5.2 <i>IPsec Requirements</i>	32
5.5.2.1 <i>IPsec Tunneling Requirements</i>	32
5.5.2.1.1 <i>IPsec ESP Encryption</i>	32
5.5.2.1.2 <i>IPsec Key Exchange Protocol</i>	33
5.5.2.1.3 <i>IPsec Policy</i>	33
5.5.2.1.3.1 <i>IPsec Outbound Policy</i>	34
5.5.2.1.3.2 <i>IPsec Inbound Policy</i>	34
5.5.2.1.3.3 <i>Security Association Lifetime</i>	34

5.5.3	Non-Repudiation	34
6	REFERENCE POINT “C” CALL FLOWS	35
6.1	CMAC ALERT MESSAGE CALL FLOWS	36
6.1.1	CMAC Message without CAP Message Retrieval Call Flow	36
6.1.2	CMAC Message with CAP Message Retrieval Call Flow	38
6.1.3	Failure to Retrieve CAP Message Call Flows	40
6.1.3.1	Federal Alert Gateway Failure to Retrieve Corresponding CAP Message	40
6.1.3.2	CMSP Gateway Detection of Failure to Retrieve Corresponding CAP Message	42
6.1.4	Invalid CMAC Message Call Flow	44
6.2	LINK TEST MESSAGE CALL FLOWS	46
6.2.1	Link Test Message to CMSP Gateway Call Flow	46
6.2.2	Invalid Link Test Message to CMSP Gateway Call Flow	47
6.2.3	Link Test Message from CMSP Gateway Call Flow	48
6.2.4	Invalid Link Test Message from CMSP Gateway Call Flow	49
6.3	REQUIRED MONTHLY TEST (RMT) CALL FLOW	49
6.4	TRANSMISSION CONTROL MESSAGE CALL FLOWS	50
6.4.1	Cease Transmissions Call Flow	50
6.4.2	Resume Transmissions Call Flow	52
7	FEDERAL ALERT GATEWAY TO CMSP GATEWAY PROTOCOL REQUIREMENTS AND DEFINITION	53
7.1	APPLICATION LAYER	53
7.1.1	CMAC Protocol	53
7.1.2	HTTP	54
7.2	MESSAGE STRUCTURE	55
7.2.1	CMAC_Alert_Attributes Segment	55
7.2.2	CMAC_Alert_Info Segment	56
7.2.3	CMAC_Alert_Area Segment	56
7.2.4	CMAC_Digital_Signature Segment	56
7.2.5	CMAC Alert Message Document Object Model	56
7.2.6	CMAC Message Types	57
7.2.6.1	Federal Alert Gateway Initiated Messages	58
7.2.6.2	CMSP Gateway Initiated Messages	60
7.3	ELEMENT DEFINITION	61
7.3.1	CMAC_Alert_Attributes Segment Element Definition	61
7.3.1.1	Notes on CMAC_special_handling Element	65
7.3.2	CMAC_Alert_Info Segment Element Definition	65
7.3.3	CMAC_Alert_Area Segment Element Definition	69
7.3.4	CMAC_Digital_Signature Segment Element Definition	70
7.3.5	Definition of CMAC_cmas_geocode Element	70
7.3.6	Definition of CMAC_cap_geocode Element	71
7.4	CMAC MESSAGE XML DEFINITION	71
7.5	CMAC MESSAGE TYPES & EXAMPLE XML	75
7.5.1	Alert Message	75
7.5.2	Update Message	80
7.5.3	Cancel Message	84
7.5.4	Ack Message	86
7.5.5	Error Message	87
7.5.6	Link Test Message	89
7.5.7	RMT Message	90
7.5.8	Transmission Control – Cease Message	92
7.5.9	Transmission Control – Resume Message	92
7.6	TRANSPORT PROTOCOL	93
7.6.1	Transmission Control Protocol (TCP)	94
7.6.2	Internet Protocol (IP)	94
7.7	ERROR HANDLING	94
7.7.1	TCP/IP Error Handling	94
7.7.2	HTTP Level Error Handling	94
7.7.3	CMAC Error Handling	95
7.7.3.1	Schema Validation	95
7.7.3.2	CMAC Message Content Validation	95
7.7.3.3	Error Response Codes	95
A	GENERATION OF CMAC_TEXT_ALERT_MESSAGE FROM CAP PARAMETERS	97

B REFERENCE POINT “C” INTERFACE STARTUP PROCEDURE.....	100
C QUALIFICATION PROVISIONS.....	101
C.1 GLOSSARY	101
C.2 RESPONSIBILITY FOR VERIFICATION	101
C.2.1 Developmental Test and Evaluation (DT&E).....	101
C.2.1.1 Federal Alert Gateway Acceptance Test.....	102
C.2.1.2 CMSP Gateway Acceptance Test.....	102
C.2.1.3 Regression Test.....	102
C.2.2 Verification Methods	102
C.2.3 Security Test and Evaluation.....	102
C.3 SYSTEM MONITORING	103
C.4 PERFORMANCE MONITORING.....	103
C.5 REFERENCE POINT “C” INTERFACE REQUIREMENTS TRACEABILITY	103
C.6 REFERENCE POINT “C” INTERFACE REQUIREMENTS MATRIX	114
D CONFIGURABLE PARAMETERS	123
E EXAMPLE OF END TO END MESSAGE IDENTIFICATION.....	124

TABLE OF FIGURES

FIGURE 1: CMAS REFERENCE ARCHITECTURE.....	10
FIGURE 2: FEDERAL ALERT GATEWAY TO CMSP GATEWAY MESSAGE TYPE SUMMARY	19
FIGURE 3: CMAC MESSAGE WITHOUT CAP MESSAGE RETRIEVAL CALL FLOW	37
FIGURE 4: CMAC MESSAGE WITH CAP MESSAGE RETRIEVAL CALL FLOW	39
FIGURE 5: FEDERAL ALERT GATEWAY FAILURE TO RETRIEVE CAP MESSAGE CALL FLOW	41
FIGURE 6: CMSP GATEWAY DETECTION OF FAILURE TO RETRIEVE CORRESPONDING CAP MESSAGE	43
FIGURE 7: INVALID CMAC MESSAGE CALL FLOW	45
FIGURE 8: LINK TEST MESSAGE TO CMSP GATEWAY CALL FLOW	46
FIGURE 9: INVALID LINK TEST MESSAGE FROM FEDERAL ALERT GATEWAY CALL FLOW	47
FIGURE 10: LINK TEST MESSAGE FROM CMSP GATEWAY CALL FLOW	48
FIGURE 11: INVALID LINK TEST MESSAGE FROM CMSP GATEWAY CALL FLOW	49
FIGURE 12: REQUIRED MONTHLY TEST CALL FLOW	50
FIGURE 13: CEASE TRANSMISSIONS CALL FLOW	51
FIGURE 14: RESUME TRANSMISSIONS CALL FLOW.....	52
FIGURE 15: REFERENCE POINT “C” DOCUMENT OBJECT MODEL	57
FIGURE 16: REFERENCE POINT “C” INTERFACE STARTUP PROCEDURES	100
FIGURE 17: END-TO-END MAPPING OF MESSAGE IDENTIFIERS.....	124
FIGURE 18: MESSAGE IDENTIFIERS WITH MULTIPLE CMSP GATEWAYS.....	125
FIGURE 19: EXAMPLE DATABASE FOR CORRELATING MESSAGE IDENTIFIERS.....	126

TABLE OF TABLES

TABLE 1: CHARACTERISTICS OF MESSAGES FROM FEDERAL ALERT GATEWAY	20
TABLE 2: CHARACTERISTICS OF MESSAGES FROM CMSP GATEWAY	21
TABLE 3: CMSP PROFILE DEFINITION.....	22
TABLE 4: FEDERAL ALERT GATEWAY PROFILE DEFINITION	26
TABLE 5: REQUIRED ALGORITHMS FOR IMPLEMENTATION OF ESP.....	32
TABLE 6: REQUIRED ALGORITHMS FOR IMPLEMENTATION OF IKE v2.....	33
TABLE 7: SUMMARY OF REFERENCES FOR IPSEC	33
TABLE 8: XML SIGNATURE ALGORITHM SUMMARY	35
TABLE 9: CMAC MESSAGE SEGMENTS	58
TABLE 10: FEDERAL ALERT GATEWAY INITIATED MESSAGES	59
TABLE 11: CMSP GATEWAY INITIATED MESSAGES	60
TABLE 12: CMAC_ALERT_ATTRIBUTES SEGMENT ELEMENT DEFINITION	62
TABLE 13: CMAC_ALERT_INFO SEGMENT ELEMENT DEFINITION	66
TABLE 14: CMAC_ALERT_AREA SEGMENT ELEMENT DEFINITION.....	69
TABLE 15: CMAC_DIGITAL_SIGNATURE SEGMENT ELEMENT DEFINITION	70
TABLE 16: ELEMENTS OF ALERT ATTRIBUTES SEGMENT FOR ALERT MESSAGE	76
TABLE 17: ELEMENTS OF ALERT INFO SEGMENT FOR ALERT MESSAGE	77

J-STD-101

TABLE 18: ELEMENTS OF ALERT AREA SEGMENT FOR ALERT MESSAGE.....	78
TABLE 19: ELEMENTS OF ALERT ATTRIBUTES SEGMENT FOR UPDATE MESSAGE	81
TABLE 20: ELEMENTS OF ALERT INFO SEGMENT FOR UPDATE MESSAGE	82
TABLE 21: ELEMENTS OF ALERT AREA SEGMENT FOR UPDATE MESSAGE.....	83
TABLE 22: ELEMENTS OF ALERT ATTRIBUTES SEGMENT FOR CANCEL MESSAGE	85
TABLE 23: ELEMENTS OF ALERT ATTRIBUTES SEGMENT FOR ACK MESSAGE.....	87
TABLE 24: ELEMENTS OF ALERT ATTRIBUTES SEGMENT FOR ERROR MESSAGE	88
TABLE 25: ELEMENTS OF ALERT ATTRIBUTES SEGMENT FOR LINK TEST MESSAGE	89
TABLE 26: ELEMENTS OF ALERT ATTRIBUTES SEGMENT FOR RMT MESSAGE	90
TABLE 27: ELEMENTS OF ALERT INFO SEGMENT FOR RMT MESSAGE	91
TABLE 28: ELEMENTS OF ALERT ATTRIBUTES SEGMENT FOR TRANSMISSION CONTROL – CEASE MESSAGE	92
TABLE 29: ELEMENTS OF ALERT ATTRIBUTES SEGMENT FOR TRANSMISSION CONTROL – RESUME MESSAGE	93
TABLE 30: DEFINITION OF CMAC RESPONSE CODES.....	96
TABLE 31: CAP VALUE FIELD MAPPING TO CMAC_TEXT_ALERT_MESSAGE.....	98
TABLE 32: REFERENCE POINT “C” INTERFACE REQUIREMENTS TRACEABILITY TABLE.....	103
TABLE 33: REQUIREMENTS MATRIX.....	114
TABLE 34: CONFIGURABLE PARAMETERS	123

ATIS & TIA Joint Standard on –

Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification

1 SCOPE, PURPOSE, & APPLICATION

This Standard is a joint Standard between the Alliance for Telecommunications Industry Solutions (ATIS) and the Telecommunications Industry Association (TIA) with the support of the American Association of Paging Carriers (AAPC).

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 CMAS alerts. Any processing in either the Federal network or the CMSP network which is not related to this interface is beyond the scope of this Standard.

1.2 Purpose

This Standard is based upon the three Reports & Orders issued to date by the Federal Communications Commission (FCC) in regards to the Commercial Mobile Alert System [Refs 9, 22, & 24]. 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 Commercial Mobile Service Provider (CMSP) who elects to support CMAS alerts.

The purpose of this Standard is to define the interface between the Federal Alert Gateway and the Commercial Mobile Service Provider (CMSP) Gateway for CMAS alerts.

1.3 Application

This Standard is applicable to Commercial Mobile Service Providers 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 and TIA 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 and TIA Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.