ATIS-0700033

ATIS Standard on -

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

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 OFMERCHANTABILITY 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

ATIS-0700033

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

Alliance for Telecommunications Industry Solutions

Approved August 31, 2017

Abstract

This Supplement provides the modifications to support the removal of the embedded references restriction for WEA alert messages and for errata to J-STD-101, *Joint ATIS/TIA CMAS 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)
D. Sennett, Technical Editor (AT&T)

The WTSC SN Subcommittee was responsible for the development of this document.

Table of Contents

ATIS Standard on –

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

1 Scope & Purpose

The scope of this Supplement is J-STD-101, *Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification*.

The purpose of this Supplement is to provide modifications to support the removal of the embedded references restriction for Wireless Emergency Alert (WEA) alert message and for errata to the *Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification*.

Upon publication, this Supplement shall be used in conjunction with J-STD-101 and its associated published Supplements A and B.

2 Modifications

2.1 Modifications to Clause 5.1.1, Federal Alert Gateway Considerations from FCC First Report and Order

1. The title of Clause 5.1.1 is modified as shown below:

   5.1.1 Federal Alert Gateway Considerations from FCC First Report and Order & from WEA Enhancement Report and Order

2. The following new paragraph is added immediately before item #1 in Clause 5.1.1:

   On September 29, 2016, the FCC issued a Report and Order on WEA enhancements [Ref 41]. These enhancements modified some of the following Federal Alert Gateway considerations.

3. The existing item #5 in Clause 5.1.1 is replaced with the following new item #5 in Clause 5.1.1:

   5. In 47 CFR Section 10.441 of *Appendix A, Final Rules,* of the FCC Report and Order on WEA Enhancements [Ref 41], all restrictions have been removed for all WEA messages regarding embedded references (e.g., URL or telephone number). Embedded references are allowed in all WEA messages. The previous 47 CFR Section 10.440 defining the embedded references restrictions has been removed in *Appendix A, Final Rules* of the FCC Report and Order on WEA Enhancements [Ref 41].

      NOTE: Even though a WEA alert may contain embedded references, having this information in the broadcast WEA message may increase the likelihood of causing severe network congestion resulting in the inability of subscribers to make calls.

2.2 Modifications to Clause 5.1.2, CMSP Gateway Considerations from FCC First Report and Order

1. The title of Clause 5.1.2 is modified as shown below:

5.1.2 CMSP Gateway Considerations from FCC First Report and Order & from WEA Enhancement Report and Order

2. Modify the first paragraph of Clause 5.1.2 as shown below:

   The following considerations are specified in the FCC First Report and Order [Ref 9]. On September 29, 2016, the FCC issued a Report and Order on WEA enhancements [Ref 41]. These enhancements modified some of the following Federal Alert Gateway considerations.

3. Modify the item #7 of Clause 5.1.2 as shown below:

   7. The CMS Provider Gateway may reject CMAMs received over the Reference Point “C” Interface that do not meet the Alert Message Requirements of the First Report and Order [Ref 9] Subpart D. Specifically, CMAMs may be rejected:

      - If the Alert does not meet the classification of Section 10.400 of the First Report and Order [Ref 9]
        - Presidential
        - Imminent Threat where the CAP Severity is extreme or severe, Urgency is immediate or expected, and Certainty is observed or likely
        - Child Abduction Alert/AMBER Alert
      - If the CMAM text exceeds 90 English characters (Section 10.430 of the First Report and Order [Ref 9])
      - ~~If the CMAM text contains an embedded reference, such as a Uniform Resource Locator (URL) or a telephone number (Section 10.440 of the First Report and Order [Ref 9]) except as permitted for Presidential alerts and child abduction emergency messages (see clause 5.1.1, Federal Alert Gateway Considerations from FCC First Report and Order).~~
      - If the CMAM does not contain one or more geocodes required by the CMSP to perform geographic targeting (Section 10.450 of the First Report and Order [Ref 9]).

2.3 Modification to Clause 5.1.4.4, Testing Functionality Considerations of CMSP Gateway

Modify item #2 of Clause 5.1.4.4, *Testing Functionality Considerations of CMSP Gateway*, as shown below:

2. A Participating CMS Provider will ~~only~~ be required to retain an automated log of RMT messages received by the CMS Provider Gateway from the Federal Alert Gateway. Contents and retention period of this log will be configurable based on CMSP policy and consistent with standard industry practice and is beyond the scope of this Standard.

2.4 Modification to Clause 5.3.1, CMSP Gateway Requirements for Federal Alert Gateway Profile

Modify the introductory paragraph of Clause 5.3.1, *CMSP Gateway Requirements for Federal Alert Gateway Profile*, as shown below:

One or more Federal Alert Gateways will send messages to each CMSP Gateway. The IP addresses, or Fully Qualified Domain Names, for each Federal Alert Gateway will be maintained in a Federal Alert Gateway profile, which is maintained in the CMSP Gateway. A CMSP Gateway may receive messages from any of the Federal Alert ~~Gateway~~ Gateways in the profile that are active at any time. No more than 2 Federal Alert Gateways are active at any given time per CMSP Gateway Group. For example, an Alert message may be sent from one

Federal Alert Gateway and an Update related to that message may later be sent from a different Federal Alert Gateway.

2.5 Modifications to Clause 7.1.1, CMAC Protocol

1. Modify item #2 of Clause 7.1.1, *CMAC Protocol*, as shown below:

    2. [JCMAS-C-RQMT-2510] Each Alert message shall contain the mandatory message elements and associated values provided in the following tables:

        - Table 15: CMAC_Digital_Signature Segment Element Definition
        - Table 16: Elements of Alert Attributes Segment for Alert Message
        - Table 17: Elements of Alert Info Segment for Alert Message
        - Table 18: Elements of Alert Area Segment for Alert Message

2. Modify item #3 of Clause 7.1.1, *CMAC Protocol*, as shown below:

    3. [JCMAS-C-RQMT-2520] Each Update message shall contain the mandatory message elements and associated values provided in the following tables:

        - Table 15: CMAC_Digital_Signature Segment Element Definition
        - Table 19: Elements of Alert Attributes Segment for Update Message
        - Table 20: Elements of Alert Info Segment for Update Message
        - Table 21: Elements of Alert Area Segment for Update Message

3. Modify item #7 of Clause 7.1.1, *CMAC Protocol*, as shown below:

    7. [JCMAS-C-RQMT-2560] Each Cancel message shall contain the mandatory message elements and associated values provided in the following tables:

        - Table 15: CMAC_Digital_Signature Segment Element Definition
        - Table 22: Elements of Alert Attributes Segment for Cancel Message

4. Modify item #8 of Clause 7.1.1, *CMAC Protocol*, as shown below:

    8. [JCMAS-C-RQMT-2570] Each RMT message shall contain the mandatory message elements and associated values provided in the following tables:

        - Table 15: CMAC_Digital_Signature Segment Element Definition
        - Table 26: Elements of Alert Attributes Segment for RMT Message
        - Table 27: Elements of Alert Info Segment for RMT Message

2.6 Modification to Clause 7.3, Element Definition

Modify the bullet items of the first paragraph of Clause 7.3, *Element Definition*, as shown below:

7.3 Element Definition

This clause defines the elements for each segment of the CMAC message. These element definitions are grouped as follows:

- Element definitions for the CMAC_Alert_Attributes segment
- Element definitions for the CMAC_alert_info segment

- Element definitions for the CMAC_Alert_Area segment
- Element definitions for the CMAC_Digital_Signature segment
- Definition of the CMAC_cmas_geocode element
- ~~Definition of the CMAC response codes~~

2.7 Modification to Clause 7.3.1.1, Notes on CMAC_special_handling Element

Modify the last paragraph of Clause 7.3.1.1, *Notes on CMAC_special_handling Element*, as shown below:

> The CMAC_special_handling element is also used to identify the RMT and Child Abduction message types that have associated special handling requirements in the CMSP Gateway. For example, RMTs require special handling because of the distribution over a 24 hour period~~; Child Abduction messages require special handling to bypass checks on embedded telephone numbers or URLs~~.

2.8 Modification to Table 15 CMAC_Digital_Signature Segment Element Definition in Clause 7.3.4

The CMAC_Digital_Signature element of Table 15, *CMAC_Digital_Signature Segment Element Definition* of Clause 7.3.4, *CMAC_Digital_Signature Segment Element Definition*, is modified as shown below:

Table 15: CMAC_Digital_Signature Segment Element Definition

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_Digital_Signature	C	XML digital signature elements and syntax are defined by W3C recommendations [Ref 38]. CMAC_Digital_Signature is mandatory for the ~~CMSP~~ Federal Alert Gateway to support non-repudiation and will be applied to Alert, Update, Cancel, and RMT messages. CMAC_Digital_Signature may be used by the CMSP Gateway to support non-repudiation. Child of <CMAC_Alert_Attributes>.

2.9 Modifications to Table 27 Elements of Alert Info Segment for RMT Message in Clause 7.5.7

Table 27, *Elements of Alert Info Segment for RMT Message* of Clause 7.5.7, *RMT Message*, is modified as shown below:

Table 27: Elements of Alert Info Segment for RMT Message

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_category	M	Value of “Other”.
CMAC_event_code	M	Value of “RMT”.
CMAC_severity	M	Value of “Severe”.
CMAC_urgency	M	Value of “Expected”.
CMAC_certainty	M	Value of “Likely”.

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_expires_date_time	M	Date and time in UTC the Alert Message expires in XML dateTime format (24 hours after initiation).
CMAC_sender_name	O	Indicates the name or other identification of the RMT initiator at the Federal Alert Gateway. May be used for CMSP Gateway logging purposes only.
CMAC_text_language	M	Value of “English”.
CMAC_text_alert_message_length	M	Length in characters of the text message ~~(74 characters for message specified in CMAC_text_alert_message)~~.
CMAC_text_alert_message	M	Text message per *Table 13: CMAC_Alert_Info Segment Element Definition* of Clause 7.3.2, *CMAC_Alert_Info Segment Element Definition*. ~~Value of “This is a test of the Commercial Mobile Alert System. This is only a test.”~~

2.10 Modification to Clause 7.6, Transport Protocol

The first paragraph of Clause 7.6, *Transport Protocol,* is modified as shown below:

> Transmission Control Protocol (TCP) [Ref 23] is the transport protocol used to transmit XML Alert Messages, RMT Messages, and system messages between the Federal Alert Gateway and the CMSP Gateway on the Reference Point “C” interface.

2.11 Modification to Table 31 CAP Value Field Mapping to CMAC_text_alert_message in Annex A

The sender entry of Table 31, *CAP Value Field Mapping to CMAC_text_alert_message*, in Annex A is modified as shown below:

Who is sending the alert		
CAP Field	**Value**	**Text String**
sender	Identifies the originator of this alert. Guaranteed by assigner to be unique globally; e.g., may be based on an Internet Fully Qualified Domain Name - could also come from the sender’s name in the Trust Model.	Translated by the Federal Alert Gateway to an acronym or short abbreviation picked by the sender ~~Note~~ NOTE: URLs, phone numbers, and email addresses of the sender are not sent to the mobile device.

2.12 Modifications to Table 32 Reference Point “C” Interface Requirements Traceability Table in Annex C.5

1. The “*Clause 5.1.1 item #3*” entry of Table 32, *Reference Point “C” Interface Requirements Traceability Table*, of Annex C.5 is modified as shown below:

Clause 5.1.1 item #3: The Federal Alert Gateway will only send CMAMs over the Reference Point "C" interface that meet the classification of alerts in the First Report and Order [Ref 9] section 10.330. Specifically, the Federal Alert Gateway will only generate CMAMs for Presidential alerts, Imminent Threat Alerts (where the corresponding CAP message Severity is extreme or severe, Urgency is immediate or expected, and Certainty is observed or likely), or a Child Abduction Emergency/AMBER Alert. Alerts not meeting this classification will not be sent over Reference Point "C".	Clause 7.1.1 item #2: [JCMAS-C-RQMT-2510] Each Alert message shall contain the mandatory message elements and associated values provided in the following tables: • Table 15: *CMAC_Digital_Signature Segment Element Definition* • Table 16: *Elements of Alert Attributes Segment for Alert Message* • Table 17: *Elements of Alert Info Segment for Alert Message* • Table 18: *Elements of Alert Area Segment for Alert Message* Clause 7.7.3.2 item #1: [JCMAS-C-RQMT-3600] Messages containing information that conflicts with the CMAC protocol shall be logged and discarded.

2. The "*Clause 5.1.1 item #4*" entry of Table 32, *Reference Point "C" Interface Requirements Traceability Table*, of Annex C.5 is modified as shown below:

Clause 5.1.1 item #4: The Federal Alert Gateway will generate a CMAM text message to be provided over the Reference Point "C" interface that does not exceed 90 English characters of alphanumeric text (see the First Report and Order [Ref 9], section 10.430).	Clause 7.1.1 item #2: [JCMAS-C-RQMT-2510] Each Alert message shall contain the mandatory message elements and associated values provided in the following tables: • Table 15: *CMAC_Digital_Signature Segment Element Definition* • Table 16: *Elements of Alert Attributes Segment for Alert Message* • Table 17: *Elements of Alert Info Segment for Alert Message* • Table 18: *Elements of Alert Area Segment for Alert Message* Clause 7.7.3.2 item #1: [JCMAS-C-RQMT-3600] Messages containing information that conflicts with the CMAC protocol shall be logged and discarded.

3. The "*Clause 5.1.1 item #5*" entry of Table 32, *Reference Point "C" Interface Requirements Traceability Table*, of Annex C.5 is modified as shown below:

Clause 5.1.1 item #5: In 47 CFR Section 10.441 of *Appendix A Final Rules* of the FCC Report and Order on WEA Enhancements [Ref 41], all restrictions have been removed for all WEA messages regarding embedded references (e.g., URL or telephone number). Embedded references are allowed in all WEA messages. The previous 47 CFR Section 10.440 defining the embedded restrictions has been removed *in Appendix A Final Rules* of the FCC Report and Order on WEA Enhancements [Ref 41]. NOTE: Even though a WEA alert may contain embedded references, having this information in the broadcast WEA message may increase the likelihood of causing severe network congestion resulting in the inability of subscribers to make calls. ~~The Federal Alert Gateway will ensure that, except for Presidential alert messages, the generated CMAM text message does not contain an embedded reference, such as a Uniform Resource Locator (URL) or telephone number in accordance with the First Report and Order [Ref 9] section 10.440. Although not explicitly addressed in the First Report and Order [Ref 9], the inclusion of a telephone number in child abduction emergency messages should be allowed.~~	Outside the scope of this Standard.

4. The "*Clause 5.1.2 item #7*" entry of Table 32, *Reference Point "C" Interface Requirements Traceability Table*, of Annex C.5 is modified as shown below:

Clause 5.1.2 item #7: The CMS Provider Gateway may reject CMAMs received over the Reference Point "C" Interface that do not meet the Alert Message Requirements of the First Report and Order [Ref 9] Subpart D. Specifically, CMAMs may be rejected: • if the Alert does not meet the classification of Section 10.400 of the First Report and Order [Ref 9] o Presidential o Imminent Threat where the CAP Severity is extreme or severe, Urgency is immediate or expected, and Certainty is observed or likely o Child Abduction Alert/AMBER Alert • if the CMAM text exceeds 90 English characters (section 10.430 of the First Report and Order [Ref 9]) ~~• if the CMAM text contains an embedded reference, such as a Uniform Resource Locator (URL) or a telephone number (Section 10.440 of the First Report and Order [Ref 9]) except for Presidential alerts or child abduction emergency messages (see clause 5.2 *Federal Alert Gateway Requirements*)~~ • if the CMAM does not contain one or more geocodes required by the CMSP to perform geographic targeting (Section 10.450 of the First Report and Order [Ref 9])	Clause 7.1.1 item #2: [JCMAS-C-RQMT-2510] Each Alert message shall contain the mandatory message elements and associated values provided in the following tables: • Table 15: *CMAC_Digital_Signature Segment Element Definition* • Table 16: *Elements of Alert Attributes Segment for Alert Message* • Table 17: *Elements of Alert Info Segment for Alert Message* • Table 18: *Elements of Alert Area Segment for Alert Message* Clause 7.7.3.2 item #1: [JCMAS-C-RQMT-3600] Messages containing information that conflicts with the CMAC protocol shall be logged and discarded.

5. The "*Clause 5.1.4.2 item #7*" entry of Table 32, *Reference Point "C" Interface Requirements Traceability Table*, of Annex C.5 is modified as shown below:

Clause 5.1.4.2 item #3: Real event codes or alert messages will not be used for this periodic interface testing.	Clause 7.1.1 item #8: [JCMAS-C-RQMT-2570] Each RMT message shall contain the mandatory message elements and associated values provided in the following tables: • Table 15: *CMAC_Digital_Signature Segment Element Definition* • Table 26: *Elements of Alert Attributes Segment for RMT Message* • Table 27: *Elements of Alert Info Segment for RMT Message*

6. The "*Clause 5.1.4.3 item #1*" entry of Table 32, *Reference Point "C" Interface Requirements Traceability Table*, of Annex C.5 is modified as shown below:

Clause 5.1.4.3 item #1: The Federal Alert Gateway will support the capability to initiate an RMT on the Reference Point "C" interface using a defined test message. Real event codes or alert messages will not be used for the CMAS RMT message.	Clause 7.1.1 item #8: [JCMAS-C-RQMT-2570] Each RMT message shall contain the mandatory message elements and associated values provided in the following tables: • Table 15: *CMAC_Digital_Signature Segment Element Definition* • Table 26: *Elements of Alert Attributes Segment for RMT Message* • Table 27: *Elements of Alert Info Segment for RMT Message*

2.13 Modifications to Table 33 Requirements Matrix in Annex C.6

1. The [JCMAS-C-RQMT-2510] requirement entry of Table 33, *Requirements Matrix*, of Annex C.6 is modified as shown below:

7.1.1	[JCMAS-C-RQMT-2510] Each Alert message shall contain the mandatory message elements and associated values provided in the following tables: • Table 15: *CMAC_Digital_Signature Segment Element Definition* • Table 16: *Elements of Alert Attributes Segment for Alert Message* • Table 17: *Elements of Alert Info Segment for Alert Message* • Table 18: *Elements of Alert Area Segment for Alert Message*

2. The [JCMAS-C-RQMT-2520] requirement entry of Table 33, *Requirements Matrix*, of Annex C.6 is modified as shown below:

7.1.1	[JCMAS-C-RQMT-2520] Each Update message shall contain the mandatory message elements and associated values provided in the following tables: • Table 15: *CMAC_Digital_Signature Segment Element Definition* • Table 19: *Elements of Alert Attributes Segment for Update Message* • Table 20: *Elements of Alert Info Segment for Update Message* • Table 21: *Elements of Alert Area Segment for Update Message*

3. The [JCMAS-C-RQMT-2560] requirement entry of Table 33, *Requirements Matrix*, of Annex C.6 is modified as shown below:

7.1.1	[JCMAS-C-RQMT-2560] Each Cancel message shall contain the mandatory message elements and associated values provided in the following ~~table~~ tables: • Table 15: *CMAC_Digital_Signature Segment Element Definition* • Table 22: *Elements of Alert Attributes Segment for Cancel Message*

4. The [JCMAS-C-RQMT-2570] requirement entry of Table 33, *Requirements Matrix*, of Annex C.6 is modified as shown below:

7.1.1	[JCMAS-C-RQMT-2570] Each RMT message shall contain the mandatory message elements and associated values provided in the following tables: • Table 15: *CMAC_Digital_Signature Segment Element Definition* • Table 26: *Elements of Alert Attributes Segment for RMT Message* • Table 27: *Elements of Alert Info Segment for RMT Message*

3 Additions

3.1 Addition of New Preface Clause

The following new Preface is added after the Table of Contents and before Clause 1, *Introduction*:

Preface

The authority-to-individuals 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-citizen emergency alerting capability to mobile devices capability 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.

3.2 Addition of New [Ref 41] in Clause 2, Normative References

An additional reference [Ref 41] is added to *Clause 2, Normative References*, as shown below:

[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.[4]

3.3 Addition to Clause 3.2, Acronym & Abbreviations

An additional acronym is added to *Clause 3.2, Acronyms & Abbreviations,* as shown below:

WEA	Wireless Emergency Alert

3.4 Addition to Clause 7.3.1.1, Notes on CMAC_special_handling Element

The following sentence is added as the new last paragraph of Clause 7.3.1.1, *Notes on CMAC_special_handling Element*, as shown below:

The CMAC_special_handling element is used, for example, to support subscriber opt-out option for Child Abduction messages.