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.

Published by

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

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

Table of Figures

Table of Tables

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-nnnn$_{R3A}$]. 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-nnnn$_{R3M}$]. 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-nnnn$_{R3D}$] 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.

1.3 Application

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

FCC Report and Order and Further Notice of Proposed Rulemaking (FCC 21-77) [Ref 26], re-designates WEA Presidential Alerts to include alerts from both the President and from the FEMA Administrator, and renames the Presidential Alert to National Alert. Protocol encoding on the C-interface however still uses the value "Presidential".

2 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.

2.1 Normative References

[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.*[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*.[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 8221, *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*.[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 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]

[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, *Wireless Emergency Alert (WEA) 3.0 Mobile Device Behavior Specification*.[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] Void.

[Ref 42] Void.

[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]

[Ref 48] FCC 18-4, *Federal Communications Commission Second Report and Order and Second Order on Reconsideration in the Matter of Wireless Emergency Alerts Amendments to Part 11 of the Commission's Rules Regarding the Emergency Alert System; January 30, 2018.* [6]

[Ref 49] ATIS-0700010, *Wireless Emergency Alert (WEA) 3.0 via EPS Public Warning System Specification.*[10]

[Ref 50] PBS Technical Specification – PWS-005, *WARN (Warning, Alert and Response Network) Receiver Requirements (C-OTA DTV Receiver/Decoder), August 31, 2021, Version 4.0.*[11]

[Ref 51] FCC 21-77, *Federal Communications Commission Report and Order and Further Notice of Proposed Rulemaking in the Matter of Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System;* June 17, 2021.[6]

2.2 Informative References

[Ref 100] ATIS-0700035, *Enhanced Wireless Emergency Alert (WEA) 3.0 Service Description.*[10]

[Ref 101] NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment.* [5]

3 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < https://glossary.atis.org/ >.

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 CMAS.

CMSP Gateway: A CMSP administered system, identified by a unique Internet Protocol (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 the 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

[11] A copy of the PBS PWS-005, *OTA Receiver & Decoder*, version 1.1, specification can be obtained by sending an email message to < amsilverman@pbs.org >.

(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 International Committee for Information Technology Standards (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.

Device-based Geo-Fencing (DBGF): The process by which a WEA capable device compares Warning Area Geometries received from a network cell broadcast message with the device's current location to determine whether the device should present the associated alert message.

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].

Wireless Emergency Alert (WEA) 3.0: A continued provision of effective WEA Alert Messages while leveraging advancements in technology to improve WEA's capabilities as defined in the January 30, 2018 FCC Second Report and Order and Second Order on Reconsideration on WEA Enhancements, FCC 18-4 [Ref 48].

3.2 Acronyms & Abbreviations

ACK	Acknowledgement
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
CMSP	Commercial Mobile Service Provider
COTS	Commercial Off-the Shelf
DBGF	Device-Based Geo-Fencing
DHS	Department of Homeland Security
DTV	Digital Television
EAN	Emergency Alert Notification
ESP	Encapsulating Security Payload
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FIFO	First In First Out

FIPS[12]	Federal Information Processing Series – or – Federal Information Processing Standards
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
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
PBS	Public Broadcasting Service
PKI	Public Key Infrastructure
RFC	Request for Comment
RMT	Required Monthly Test
RSA	Rivest, Shamir, and Adleman
SA	Security Association
SHA-1	Secure Hash Algorithm One
TCP	Transmission Control Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WEA	Wireless Emergency Alert
XML	eXtensible Markup Language

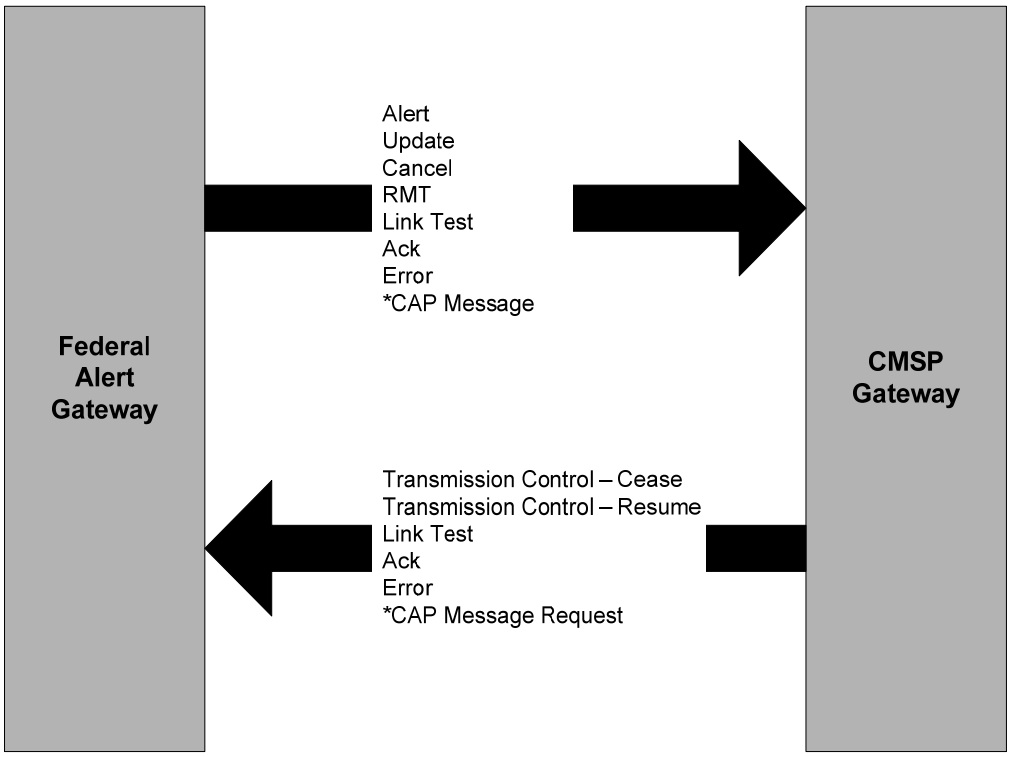
4 Requirements

This clause defines the requirements for the interface between the Federal Alert Gateway and the CMSP Gateway.

4.1.1 Reference Point "C" Interface Overview

The complete set of message types exchanged between the Federal Alert Gateway and the CMSP Gateway is shown in the following figure. Note that all messages are exchanged using the eXtensible Markup Language (XML)-based [Refs 21 & 31] Commercial Mobile Alert for C Interface (CMAC) protocol (see Clause 6.1.1, *CMAC Protocol*) over Hypertext Transfer Protocol (HTTP) (see Clause 6.1.2, *HTTP*) except the CAP Message Request and the CAP Message exchanges that use HTTP without the CMAC protocol.

[12] 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".



* CAP Message and CAP Message Request use HTTP but not the CMAC protocol

Figure 4.1 – Federal Alert Gateway to CMSP Gateway Message Type Summary

A WEA Alert message or a WEA Update message can be a National Alert, a Child Abduction/ America's Missing Broadcast Emergency Response (AMBER) Alert message, an Imminent Threat Alert message, a Public Safety message, or a State/Local WEA Test message.

The following table provides the characteristics of the messages from the Federal Alert Gateway to the CMSP Gateway:

Table 4.1 – Characteristics of Messages from Federal Alert Gateway

Message Type	Format	Description	Transmission Frequency (Peak)
Alert	CMAC	Emergency alert information translated by the Federal Alert Gateway from a CAP Alert message. An Alert message can be a National Alert, a Child Abduction/AMBER Alert message, an Imminent Threat Alert message, a Public Safety message, or a State/Local WEA Test message.	Four Alert, Update, and Cancel messages per minute including Public Safety messages and State/Local WEA Test messages. NOTE: Most alerts expire and are not cancelled.
Update	CMAC	Emergency alert information translated by the Federal Alert Gateway from a CAP Update message. Contains information that updates a previous Alert or Update message. An Update message can be a National Alert, a Child Abduction/AMBER Alert message, an Imminent Threat Alert message, a Public Safety message, or a State/Local WEA Test message.	

Message Type	Format	Description	Transmission Frequency (Peak)
Cancel	CMAC	Emergency alert information translated by the Federal Alert Gateway from a CAP Cancel message. Contains information that cancels a previous Alert or Update message.	
Required Monthly Test (RMT)	CMAC	Generated by the Federal Alert Gateway to test the CMSP Gateway and Infrastructure on a monthly basis.	Once per month per CMSP Gateway Group.
Link Test	CMAC	Generated periodically by the Federal Alert Gateway to let the CMSP Gateway know the Federal Alert Gateway and the interface are available.	Per the configured Link Test Period, per CMSP Gateway.
Ack	CMAC	Sent by the Federal Alert Gateway in response to a received CMAC message that did not have errors.	A function of the number of CMSP Gateway messages.
Error	CMAC	Sent by the Federal Alert Gateway in response to a received CMAC message that did have errors.	Variable.
CAP Retrieval Message	HTTP	Provided by the Federal Alert Gateway in response to a request for retrieval of the CAP message from the CMSP Gateway.	One message per request from CMSP Gateway.

The following table provides the characteristics of the messages from the CMSP Gateway to the Federal Alert Gateway:

Table 4.2 – Characteristics of Messages from CMSP Gateway

Message Type	Format	Description	Transmission Frequency (Peak)
Transmission Control – Cease	CMAC	Sent by the CMSP Gateway to notify the Federal Alert Gateway to discontinue transmission of messages to the CMSP Gateway.	Variable and should be used very infrequently during CMSP Gateway maintenance, failures, or processing overload conditions.
Transmission Control – Resume	CMAC	Sent by the CMSP Gateway to notify the Federal Alert Gateway to resume transmission of messages to the CMSP Gateway.	Variable and should be used very infrequently to exit CMSP Gateway maintenance, failures, or processing overload conditions.
Link Test	CMAC	May be generated by the CMSP Gateway to find out if the Federal Alert Gateway and the interface are available.	Used occasionally by the CMSP Gateway to check the connection with the Federal Alert Gateway upon startup, failure recovery, lack of reception of message responses, lack of Link Test reception, etc.
Ack	CMAC	Sent by the CMSP Gateway in response to a received CMAC message that did not have errors.	A function of the number of Federal Alert Gateway messages.
Error	CMAC	Sent by the CMSP Gateway in response to a received CMAC message that did have errors.	Variable.
CAP Retrieval	HTTP	Sent by CMSP Gateway to request the CAP message corresponding to a received CMAC Alert, Update, or Cancel message.	Variable, each CAP message may be retrieved once per CMSP Gateway Group.

4.2 Federal Alert Gateway Requirements

In addition to the Federal Alert Gateway requirements contained within this clause and sub-clauses, there are also additional Federal Alert Gateway requirements in other clauses of this Standard. For example, there are protocol requirements for the Federal Alert Gateway contained in Clause 6.2.7.1, *Federal Alert Gateway Initiated Messages*.

4.2.1 Federal Alert Gateway Requirements for CMSP Profile

The Federal Alert Gateway will maintain a CMSP Profile for each CMSP Gateway Group (this includes one or two CMSP Gateways). The profile will provide the information necessary for the Federal Alert Gateway to communicate with each CMSP Gateway. It will also indicate whether or not the CMSP wishes to have geo-location filtering applied. If geo-location filtering is desired, a list of the States is provided to define the filtering area. The Federal Alert Gateway will send alerts having an alert area that includes any part of the listed states to the CMSP Gateway. A Fully Qualified Domain Name or IP address will be maintained for each CMSP Gateway.

[WEA-C-RQMT-0100] The Federal Alert Gateway message exchange with the CMSP Gateway shall be per the CMSP profile.

NOTE: A CMSP profile will exist for each CMSP Gateway Group.

[WEA-C-RQMT-0110] The Federal Alert Gateway shall maintain verifiable identities for approved CMSP Gateways.

NOTE: The CMSPs are verifiable through Internet Key Exchange (IKE) authentication.

[WEA-C-RQMT-0120] The Federal Alert Gateway shall maintain a CMSP profile that includes the parameters identified in Table 4.3: *CMSP Profile Definition* in Clause 4.2.1.1, *Federal Alert Gateway Definition of CMSP Profile*.

[WEA-C-RQMT-0130] The Federal Alert Gateway shall send all Alert, Update, and Cancel CMAC messages to the CMSP Gateway unless Geo-Location Filtering is selected in the CMSP profile.

[WEA-C-RQMT-0140] The Federal Alert Gateway shall send to the CMSP Gateway only Alert, Update, and Cancel CMAC messages having alert areas with some overlap with the listed states if Geo-Location Filtering is selected in the CMSP profile.

4.2.1.1 Federal Alert Gateway Definition of CMSP Profile

[WEA-C-RQMT-0200] The CMSP Profile in the Federal Alert Gateway shall contain the parameters defined in the following table:

Table 4.3 – CMSP Profile Definition

Parameter	Description	Range of Values
CMSP Name	Unique identification of CMSP.	Text string
CMSP Gateway A Address	IP address or Fully Qualified Domain Name. Uniquely identifies the CMSP Gateway. Provides a verifiable identity for IKE authentication.	IP address / Text string
CMSP Gateway B Address alternate	IP address or Fully Qualified Domain Name. Uniquely identifies the CMSP Gateway. Provides a verifiable identity for IKE authentication.	IP address / Text string (optional)
Geo-Location Filtering	Should alerts be forwarded to the CMSP only when the alert area falls within a predefined list of states?	"Yes" (filter based on list of states) "No" (forward all alerts regardless of alert area)

Parameter	Description	Range of Values
List of Geo-Location Filtering States	List of all states in which the CMSP would like to receive alerts if value of Geo-Location Filtering parameter is "Yes".	Two-digit Federal Information Processing Series (FIPS) State Numeric Codes, per INCITS 38-2009 [Ref 5].
C-Interface Message Version	Indicates which version of the C-Interface message protocol is supported by the CMSP Gateway.	"2.0" – C-Interface XML for WEA 3.0.

NOTE: For information about port number assignments, see Clause 6.1.2, *HTTP*.

4.2.2 Federal Alert Gateway Requirements for Connection Establishment

The Federal Alert Gateway will establish an IP Security (IPsec) tunnel and a Transmission Control Protocol (TCP) connection with all CMSP Gateways in the CMSP Gateway Profile. If an IPsec tunnel and a TCP connection cannot be established, then the Federal Alert Gateway will retry at least per Reconnect Number times before giving up. Each time the Federal Alert Gateway has a new CMAC message to send to a CMSP Gateway, it will try to establish an IPsec tunnel and a TCP connection if they are not already established.

[WEA-C-RQMT-0300] At startup, the Federal Alert Gateway shall attempt to establish an IPsec tunnel and a TCP connection with all CMSP Gateways in the CMSP Gateway Profile.

NOTE: Only two Federal Alert Gateways can be connected to a CMSP Gateway Group.

[WEA-C-RQMT-0310] The Federal Alert Gateway shall attempt to establish an IPsec tunnel and a TCP connection every time it has a new message to send to a CMSP Gateway with which no IPsec tunnel or TCP connection exists unless the Federal Alert Gateway had received a Transmission Control – Cease from the CMSP Gateway.

[WEA-C-RQMT-0320] The Federal Alert Gateway shall try establishing an IPsec tunnel and a TCP connection at least per Reconnect Number times.

NOTE: Reconnect Number is a configuration parameter (See *Annex D*).

[WEA-C-RQMT-0330] The Federal Alert Gateway shall accept IPsec tunnel and TCP connection requests from any CMSP Gateway in its CMSP Gateway Profile and establish an IPsec tunnel and a TCP connection with that CMSP Gateway, unless the connection would result in a CMSP Gateway Group being connected with more than two Federal Alert Gateways.

NOTE: All CMSP Gateways in a CMSP Gateway Group are allowed to be connected to at most the same two Federal Alert Gateways.

4.2.3 Federal Alert Gateway Requirements for Message Transmission

The Federal Alert Gateway sends alert (Alert, Update, or Cancel) and test messages (RMT or Link Test) to the CMSP Gateway. Alert, Update, and Cancel messages are triggered by the reception of a CAP message at the Federal Alert Gateway. If the CAP message is validated (i.e., meets the criteria for a WEA alert as defined in the FCC First Report and Order, FCC 08-99 [Ref 9]) and the FCC Report and Order on WEA enhancements, FCC 16-127 [Ref 41]) and translated successfully into the CMAC format, a CMAC message will result. Link Test Messages are generated by the Federal Alert Gateway to indicate to the CMSP Gateway that the Federal Alert Gateway and the interface are available. The RMT is generated to test the CMSP Gateway and CMSP Infrastructure on a monthly basis. The Federal Alert Gateway also responds to CMSP Gateway messages with either an Ack or an Error message. The format for each of the messages is detailed in Clause 6.5, *CMAC Message Types & Example XML*.

For a redundant CMSP Gateway configuration, the Federal Alert Gateway sends all Alert, Update, Cancel, and RMT messages first to CMSP Gateway A unless it received a Transmission Control – Cease message from CMSP Gateway A to discontinue transmission. If the Federal Alert Gateway cannot send an Alert, Update, Cancel, or RMT message to CMSP Gateway A, then it will send the message to CMSP Gateway B unless it received a Transmission Control – Cease message from CMSP Gateway B.

The Federal Alert Gateway sends all Link Test Messages to each CMSP Gateway that did not send a Transmission Control – Cease message to discontinue transmission.

[WEA-C-RQMT-0400] The Federal Alert Gateway shall send the following message types to the CMSP Gateway per the CMAC protocol:

- Alert (Clause 6.5.1, *Alert Message*).
- Update (Clause 6.5.2, *Update Message*).
- Cancel (Clause 6.5.3, *Cancel Message*).
- RMT (Clause 6.5.7, *RMT Message*).
- Link Test (Clause 6.5.6, *Link Test Message*).
- Ack (Clause 6.5.4, *Ack Message*).
- Error (Clause 6.5.5, *Error Message*).

[WEA-C-RQMT-0410] The Federal Alert Gateway shall send an Alert message to the CMSP Gateway Group when triggered by the reception of a CAP Alert message that meets the criteria for a WEA alert as defined the FCC First Report and Order, FCC 08-99 [Ref 9] and the FCC Report and Order on WEA enhancements, FCC 16-127 [Ref 41].

[WEA-C-RQMT-0414] The Federal Alert Gateway shall send a single Alert message to the CMSP Gateway Group with English alert text content in both the 90-character maximum alert text element and the 360-character maximum alert text element, based upon the received CAP Alert message.

[WEA-C-RQMT-0416] If Spanish alert text was provided by the alert originators in the received CAP Alert message, the Federal Alert Gateway shall send a single Alert message to the CMSP Gateway Group with Spanish alert text content in both the 90-character maximum alert text element and the 360-character maximum alert text element, along with English alert text content in both the 90-character maximum alert text element and the 360-character maximum alert text element.

[WEA-C-RQMT-0420] The Federal Alert Gateway shall send an Update message to the CMSP Gateway Group when triggered by the reception of a CAP Update message that meets the criteria for a WEA alert as defined in the FCC First Report and Order [Ref 9] and the FCC Report and Order on WEA enhancements [Ref 41].

[WEA-C-RQMT-0425] If the Federal Alert Gateway receives a single CAP Update message that does not meet the criteria for a WEA alert as defined in the FCC First Report and Order, FCC 08-99 [Ref 9] and the FCC Report and Order on WEA enhancements, FCC 16-127 [Ref 41] and the Federal Alert Gateway cannot resolve the discrepancy with the alert originator, the Federal Alert Gateway shall send a Cancel message to the CMSP Gateway Group to cancel the original WEA alert that is referenced in the Update message.

[WEA-C-RQMT-0427] The Federal Alert Gateway shall send a single Update message to the CMSP Gateway Group with English alert text content in both the 90-character maximum alert text element and the 360-character maximum alert text element, based upon the received CAP Update message.

[WEA-C-RQMT-0428] If Spanish alert text was provided by the alert originators in the received CAP Update message, the Federal Alert Gateway shall send a single Update message to the CMSP Gateway Group with Spanish alert text content in both the 90-character maximum alert text element and the 360-character maximum alert text element, along with English alert text content in both the 90-character maximum alert text element and the 360-character maximum alert text element.

[WEA-C-RQMT-0430] The Federal Alert Gateway shall send a Cancel message to the CMSP Gateway Group when triggered by the reception of a CAP Cancel message that meets the criteria for a WEA alert as defined in the FCC First Report and Order, FCC 08-99 [Ref 9] and the FCC Report and Order on WEA enhancements, FCC 16-127 [Ref 41].

[WEA-C-RQMT-0440] The Federal Alert Gateway shall send an RMT message to the CMSP Gateway Group once per month.

[WEA-C-RQMT-0450] The Federal Alert Gateway shall send a Link Test Message every Link Test Period minute to each CMSP Gateway that did not send a Transmission Control – Cease message.

NOTE: Link Test Period is a configuration parameter (See *Annex D*).

[WEA-C-RQMT-0460] The Federal Alert Gateway shall send an Ack message to the CMSP Gateway when a CMSP Gateway message has been received without error, except when the CMSP Gateway has sent an Ack or an Error message to the Federal Alert Gateway.

NOTE: See Clause 6.8 for a description of the error checks.

[WEA-C-RQMT-0470] The Federal Alert Gateway shall send an Error message to the CMSP Gateway when a CMSP Gateway message has been received with any error.

NOTE: See Clause 6.8 for a description of the error checks. Also see error codes in Table 6.26 – *Definition of CMAC Response Codes*.

[WEA-C-RQMT-0480] The Federal Alert Gateway shall send all Alert, Update, Cancel, and RMT messages to CMSP Gateway A unless it received a Transmission Control – Cease message from CMSP Gateway A to discontinue transmission.

[WEA-C-RQMT-0490] The Federal Alert Gateway shall send an Alert, Update, Cancel, or RMT message to CMSP Gateway B under any of the following conditions, unless it received a Transmission Control – Cease message from CMSP Gateway B to discontinue transmission:

a. The Federal Alert Gateway received a Transmission Control – Cease message from CMSP Gateway A and discontinued transmission; OR

b. The Federal Alert Gateway cannot establish a connection to CMSP Gateway A after trying Reconnect Number times; OR

c. The Federal Alert Gateway does not receive an Ack/Error response from CMSP Gateway A after transmitting the message Retransmit Number times.

[WEA-C-RQMT-0493$_{R3M}$] The Federal Alert Gateway shall support 2.0 CMAC messages (defined in Clause 6.5).

[WEA-C-RQMT-0496] The Federal Alert Gateway shall use the version of CMAC messages provisioned in the CMSP's profile when transmitting messages to the associated CMSP. See WEA-C-RQMT-0200.

4.2.4 Federal Alert Gateway Requirements for Message Reception

The Federal Alert Gateway receives Transmission Control – Cease and Transmission Control – Resume messages from the CMSP Gateway. It may also receive Link Test Messages from the CMSP Gateway as a means for the CMSP Gateway to check the availability of the interface and the Federal Alert Gateway. The Federal Alert Gateway also receives Ack and Error messages from the CMSP Gateway in response to messages sent to the CMSP Gateway. The format for each of these messages is detailed in Clause 6.5, *CMAC Message Types & Example XML*.

[WEA-C-RQMT-0500] The Federal Alert Gateway shall receive and process the following message types from the CMSP Gateway per the CMAC protocol:

- Transmission Control – Cease (Clause 6.5.8, *Transmission Control – Cease Message*).
- Transmission Control – Resume (Clause 6.5.9, *Transmission Control – Resume Message*),
- Link Test (Clause 6.5.6, *Link Test Message*),
- Ack (Clause 6.5.4, *Ack Message*).
- Error (Clause 6.5.5, *Error Message*).

[WEA-C-RQMT-0510] The Federal Alert Gateway shall receive and log each Transmission Control – Cease message from the CMSP Gateway.

[WEA-C-RQMT-0520] The Federal Alert Gateway shall receive and log each Transmission Control – Resume message from the CMSP Gateway.

[WEA-C-RQMT-0530] The Federal Alert Gateway shall receive and log Link Test Messages from the CMSP Gateway.

[WEA-C-RQMT-0540] The Federal Alert Gateway shall receive and log Ack messages from the CMSP Gateway.

[WEA-C-RQMT-0550] The Federal Alert Gateway shall receive and log Error messages from the CMSP Gateway.

[WEA-C-RQMT-0560] The Federal Alert Gateway shall respond to all messages from a CMSP Gateway even if that CMSP Gateway has sent a Transmission Control – Cease message.

4.3 CMSP Gateway Requirements

In addition to the CMSP Gateway requirements contained within this clause and sub-clauses, there are also additional CMSP Gateway requirements in other clauses of this Standard. For example, there are protocol requirements for the CMSP Gateway contained in Clause 6.2.7.2, *CMSP Gateway Initiated Messages*.

4.3.1 CMSP Gateway Requirements for Federal Alert Gateway Profile

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 Gateways in the profile that are active at any time. No more than two 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.

[WEA-C-RQMT-0700] CMSP Gateway message exchange with the Federal Alert Gateway shall be per the Federal Alert Gateway profile.

[WEA-C-RQMT-0710] The CMSP Gateway shall accept and process messages received from any of the Federal Alert Gateways identified in the Federal Alert Gateway profile.

[WEA-C-RQMT-0720] The CMSP Gateway shall maintain verifiable identities for approved Federal Alert Gateways.

NOTE: The Federal Alert Gateways are verifiable through IKE authentication.

4.3.1.1 CMSP Gateway Definition of Federal Alert Gateway Profile

[WEA-C-RQMT-0600] The CMSP Gateway shall maintain a Federal Alert Gateway profile that includes the parameters identified in the following table:

Table 4.4 – Federal Alert Gateway Profile Definition

Parameter	Description	Range of Values
Federal Alert Gateway Address (n)	IP address or Fully Qualified Domain Name (See Note 1). Uniquely identifies the Federal Alert Gateway. Provides a verifiable identity for IKE authentication. One to n Federal Alert Gateways. n = 12 maximum	IP address / Text string

NOTE 1: When a Domain Name uniquely identifies the Federal Alert Gateway, the IP address of the Federal Alert Gateway may be provisioned in the CMSP's network (i.e., at the option of the CMSP) for Domain Name Service implemented in the CMSP's network.

NOTE 2: For information about port number assignments, see Clause 6.1.2.

4.3.2 CMSP Gateway Requirements for Connection Establishment

The CMSP Gateway will establish an IPsec tunnel and a TCP connection with two Federal Alert Gateways in the Federal Alert Gateway Profile. It will first try the first two Federal Alert Gateways listed in the profile. If an IPsec tunnel and a TCP connection cannot be established, then the CMSP Gateway will retry at least per Reconnect Number times and move down the list of Federal Alert Gateways until two IPsec tunnels and TCP connections are established. Each time the CMSP Gateway has a new message to send (i.e., Link Test, Transmission Control – Cease, Transmission Control – Resume, CAP Retrieval) to a Federal Alert Gateway, it will try to establish an IPsec tunnel and a TCP connection if they are not already established. If the CMSP Gateway has an IPsec tunnel and a

TCP connection established with less than two Federal Alert Gateways and if it receives a new IPsec tunnel or a TCP connection request from any Federal Alert Gateway in its Federal Alert Gateway Profile, then the CMSP Gateway will accept the request and establish an IPsec tunnel and a TCP connection with that Federal Alert Gateway.

[WEA-C-RQMT-0800] At startup, the CMSP Gateway shall attempt to establish an IPsec tunnel and a TCP connection with the first two Federal Alert Gateways in the Federal Alert Gateway Profile, if an IPsec tunnel and a TCP connection does not already exist with two Federal Alert Gateways.

[WEA-C-RQMT-0820] If the CMSP Gateway is unable to establish an IPsec tunnel and a TCP connection with the Federal Alert Gateways, the CMSP Gateway shall go down the list of Federal Alert Gateways in the Federal Alert Gateway Profile until it establishes an IPsec tunnel and a TCP connection or completes the list without establishing the connections.

[WEA-C-RQMT-0830] The CMSP Gateway shall try establishing an IPsec tunnel and a TCP connection with each Federal Alert Gateway at least per Reconnect Number times before moving to the next Gateway in the list.

NOTE: Reconnect Number is a configuration parameter (See *Annex D*).

[WEA-C-RQMT-0840] When the CMSP Gateway has a new message (i.e., Link Test, Transmission Control – Cease, Transmission Control – Resume, CAP Retrieval) to send to a particular Federal Alert Gateway and the CMSP Gateway does not have an IPsec tunnel and TCP connections to that particular Federal Alert Gateway, the CMSP Gateway shall attempt to establish an IPsec tunnel and a TCP connection with that particular Federal Alert Gateway

[WEA-C-RQMT-0850] The CMSP Gateway shall accept new IPsec tunnel and TCP connection requests from any Federal Alert Gateway in its Federal Alert Gateway Profile if the CMSP Gateway has an IPsec tunnel and a TCP connection with less than two Federal Alert Gateways.

4.3.3 CMSP Gateway Requirements for Message Transmission

The CMSP Gateway will send a Transmission Control – Cease message to the Federal Alert Gateway to discontinue transmission of all messages (e.g., for a planned or unplanned outage) and a Transmission Control – Resume to resume transmission of all messages. Transmission from different Federal Alert Gateways are controlled disjointly, so the CMSP Gateway has to send a separate Transmission Control – Cease or Transmission Control – Resume message to each active Federal Alert Gateway to cease or resume transmission from that Federal Alert Gateway. However, since there are up to 12 Federal Alert Gateways, if there is a switchover of active Federal Alert Gateways after a CMSP Gateway has requested a Transmission Control – Cease, the new active Federal Alert Gateway may not be aware of the CMSP Gateway transmission cease request. When the new active Federal Alert Gateway attempts to establish communications with the CMSP Gateway, the CMSP Gateway may either refuse to establish a connection, or send a Transmission Control – Cease following connection establishment.

The CMSP Gateway may also send Link Test Messages to the Federal Alert Gateway to check the availability of the interface and the Federal Alert Gateway. The CMSP Gateway may send a Link Test Message to any Federal Alert Gateway in its Federal Alert Gateway Profile to check that particular interface, but must never allow more than two IPsec tunnels and TCP connections at any given time. The CMSP Gateway also sends Ack and Error messages to the Federal Alert Gateway in response to messages received from the Federal Alert Gateway. An acknowledgement response from the CMSP Gateway to the Federal Alert Gateway indicates that the alert message has been received and validated and that broadcast of the alert message will be attempted for the best approximation of the intersection of the CMSP coverage and the alert area. The format for each of these messages is detailed in Cause 6.5, *CMAC Message Types & Example XML*.

[WEA-C-RQMT-0900] The CMSP Gateway shall send the following message types to the Federal Alert Gateway per the CMAC protocol:

- Transmission Control – Cease (Clause 6.5.8, *Transmission Control – Cease Message*)
- Transmission Control – Resume (Clause 6.5.9, *Transmission Control – Resume Message*)
- Link Test (Clause 6.5.6, *Link Test Message*)
- Ack (Clause 6.5.4, *Ack Message*)
- Error (Clause 6.5.5, *Error Message*)

[WEA-C-RQMT-0910] The CMSP Gateway shall send an Error message to a Federal Alert Gateway when a message has been received from that Federal Alert Gateway with an error.

NOTE: See Clause 6.8 for a description of the error checks. Also see error codes in Table 6.26 – *Definition of CMAC Response Codes*.

[WEA-C-RQMT-0920] The CMSP Gateway shall send a Transmission Control – Cease message to a Federal Alert Gateway to discontinue the transmission of messages from that Federal Alert Gateway.

NOTE: For a CMSP Gateway to stop reception from both Federal Alert Gateways, the CMSP Gateway must send the Transmission Control – Cease to both Federal Alert Gateways.

[WEA-C-RQMT-0930] The CMSP Gateway shall send a Transmission Control – Resume message to a Federal Alert Gateway to resume the transmission of messages from that Federal Alert Gateway.

NOTE: It is valid to send a Transmission Control – Resume message when there was no previous Transmission Control – Cease message sent.

NOTE: To resume reception from both Federal Alert Gateways, the CMSP Gateway must send Transmission Control – Resume to both Federal Alert Gateways.

[WEA-C-RQMT-0940] The CMSP Gateway shall send a Link Test Message to the Federal Alert Gateway to determine the status of communication with the Federal Alert Gateway.

NOTE: The initiation of a Link Test is optional for the CMSP Gateway.

[WEA-C-RQMT-0950] The CMSP Gateway shall send an Ack message to a Federal Alert Gateway when a message has been received from that Federal Alert Gateway without error.

NOTE: See Clause 6.8 for a description of the error checks.

4.3.4 CMSP Gateway Requirements for Message Reception

The CMSP Gateway receives alert (Alert, Update, or Cancel) and test information (RMT or Link Test) from the Federal Alert Gateway. Alert, Update, and Cancel messages are triggered by the reception of a CAP message at the Federal Alert Gateway. An Alert, Update, or Cancel message is of type National, Imminent Threat, Child Abduction/AMBER Alert, Public Safety message, or a State/Local WEA Test message. If the CAP message is validated (i.e., meets the criteria for a WEA alert as defined in the FCC First Report and Order, FCC 08-99 [Ref 9] and the FCC Report and Order on WEA enhancements, FCC 16-127 [Ref 41]) and translated successfully into the CMAC format by the Federal Alert Gateway, a CMAC message will result. The RMT is received from the Federal Alert Gateway by the CMSP Gateway to test the CMSP Infrastructure on a monthly basis. The CMSP Gateway receives Link Test Messages from the Federal Alert Gateway to indicate to the CMSP Gateway that the Federal Alert Gateway and the interface are available. The CMSP Gateway also responds to Federal Alert Gateway messages with either an Ack or an Error message. The format for each of the messages is detailed in Clause 6.5, *CMAC Message Types & Example XML*.

[WEA-C-RQMT-1000] The CMSP Gateway shall receive and process the following message types from the Federal Alert Gateway in the CMAC protocol:

- Alert (Clause 6.5.1, *Alert Message*).
- Update (Clause 6.5.2, *Update Message*).
- Cancel (Clause 6.5.3, *Cancel Message*).
- RMT (Clause 6.5.7, *RMT Message*).
- Link Test (Clause 6.5.6, *Link Test Message*).
- Ack (Clause 6.5.4, *Ack Message*).
- Error (Clause 6.5.5, *Error Message*).

[WEA-C-RQMT-1010] The CMSP Gateway shall receive and log Alert messages from the Federal Alert Gateway.

NOTE: The CMSP Gateway will attempt to distribute the WEA alert through its infrastructure. This function is beyond the scope of this Standard.

[WEA-C-RQMT-1020] The CMSP Gateway shall receive and log Update messages from the Federal Alert Gateway.

NOTE: The CMSP Gateway will stop broadcasting the referenced WEA alert and will attempt to broadcast the Update through its infrastructure. This function is beyond the scope of this Standard.

[WEA-C-RQMT-1030] The CMSP Gateway shall receive and log Cancel messages from the Federal Alert Gateway.

NOTE: The CMSP Gateway will attempt to stop broadcasting the referenced WEA alert. This function is beyond the scope of this Standard.

[WEA-C-RQMT-1040] If the CMSP Gateway receives an "Update" message and cannot make an association with the "referenced message", the CMSP Gateway shall process the "Update" as a new "Alert" message.

[WEA-C-RQMT-1050] The CMSP Gateway shall receive and log RMT messages from the Federal Alert Gateway.

NOTE: The CMSP Gateway will attempt to distribute the RMT information over the next 24 hour period. This function is beyond the scope of this Standard.

[WEA-C-RQMT-1060] The CMSP Gateway shall receive and log Link Test Messages from the Federal Alert Gateway.

[WEA-C-RQMT-1070] The CMSP Gateway shall receive and log Ack messages from the Federal Alert Gateway.

[WEA-C-RQMT-1080] The CMSP Gateway shall receive and log Error messages from the Federal Alert Gateway.

[WEA-C-RQMT-1090] If in any given monthly RMT cycle more than one RMT message is received by the CMSP, the CMSP Gateway shall accept only the first RMT message and shall reject all subsequent RMT messages within that calendar month.

[WEA-C-RQMT-1100] If the CMSP Gateway determines that an RMT message is invalid (e.g., not originated by the Federal Alert Gateway Administrator), the CMSP Gateway shall reject the RMT message.

[WEA-C-RQMT-1110] If conditions at the CMSP Gateway preclude distribution of the RMT, the CMSP Gateway shall respond to the RMT message with an Error message (see Table 6.26 – *Definition of CMAC Response Codes*).

[WEA-C-RQMT-1120] If conditions at the CMSP Gateway preclude distribution of the State/Local WEA Test message, the CMSP Gateway shall respond to the State/Local WEA Test message with an Error message (see Table 6.26 – *Definition of CMAC Response Codes*).

4.3.5 CMSP Gateway Requirements for Logging of Message Reception

The CMSP Gateway receives alert (Alert, Update, or Cancel) and test information (RMT or Link Test) from the Federal Alert Gateway.

Section 10.320(g) of 47 U.S.C on WEA Enhancements, FCC 16-127 [Ref 41] requires Participating CMS Providers to log Alert messages.

[WEA-C-RQMT-1150] The CMSP Gateway shall log reception of Alert, Update, Cancel, and RMT messages, along with a timestamp when the message is received, and shall log Ack and Error responses sent from the CMSP Gateway along with a timestamp.

The format for each of the messages is detailed in Clause 6.5, *CMAC Message Types & Example XML*.

4.4 Quality of Service Requirements

4.4.1 Prioritization

The Federal Alert Gateway will determine if a message is a National Alert from the CAP eventCode element ["Emergency Alert Notification" (EAN)] and set CMAC_special_handling to "Presidential". For Cancel messages

that do not include an eventCode element, the Federal Alert Gateway may use the eventCode element of the referenced CAP message.

[WEA-C-RQMT-1200] A National Alert received by the Federal Alert Gateway shall be sent to the CMSP Gateway before any other alerts that may be waiting in a message queue for processing.

NOTE: This applies to all three types of National Alert messages (Alert, Update, and Cancel).

[WEA-C-RQMT-1210] The Federal Alert Gateway shall send all alerts other than National Alerts to the CMSP Gateway on a First In – First Out (FIFO) basis.

4.4.2 Message Queuing

The Federal Alert Gateway will queue outgoing CMAC messages to a CMSP Gateway if it cannot send the message to any CMSP Gateway in the CMSP Gateway Group. The Federal Alert Gateway will remove from the queue messages that are no longer valid for broadcast (i.e., cancelled, updated, expired). When an IPsec tunnel and a TCP connection are established with a CMSP Gateway in the CMSP Gateway Group, the Federal Alert Gateway will send the queued messages to that CMSP Gateway.

The following requirements apply to the entire group of Federal Alert Gateways interacting with a CMSP Gateway:

[WEA-C-RQMT-1300] The Federal Alert Gateway shall queue outgoing CMAC messages to a CMSP Gateway Group as long as the message is still valid for broadcast (up to 24 hours maximum) if it cannot send the message to any CMSP Gateway in the CMSP Gateway Group and receive an Ack/Error response.

[WEA-C-RQMT-1310] The Federal Alert Gateway shall remove messages from the queue that are no longer valid for broadcast (i.e., cancelled, updated, expired).

[WEA-C-RQMT-1320] The Federal Alert Gateway shall send all queued messages in FIFO order, except National Alerts, to a CMSP Gateway when an IPsec tunnel and a TCP connection are established with that CMSP Gateway.

NOTE: National Alerts are placed at the top of the queue (see Clause 4.4.1, *Prioritization*).

4.5 Security Requirements

The Reference Point “C” Interface will use IP Security (IPsec) protocols [Ref 3] to provide IP (i.e., network layer) security. The IPsec protocols support cryptographically-based security services including:

- Access control.
- Data integrity.
- Confidentiality.
- Data origin authentication.
- Detection and rejection of replays.

IPsec Virtual Private Network (VPN) tunneling will be used to establish secure communications between the Federal Alert Gateway and the CMSP Gateway. IPsec VPN tunneling provides this security by authenticating and encrypting the IP packets exchanged between the Federal Alert Gateway and the CMSP Gateway. This exchange certifies authenticity and guaranties integrity of the data transmitted.

The types of messages that traverse between Federal Alert Gateway and CMSP Gateway are CMAC messages (e.g., Alert, Update, Cancel, Transmission Control – Cease, Transmission Control – Resume, RMT, Ack, Link Test, Error, CAP requests, CAP responses), IPsec session establishment keys, passwords, and other tunneling administrative information. It is anticipated that all security-related requirements can be met with Commercial-Off-The-Shelf (COTS) cryptographic modules to implement IPsec. Annex B provides an overview of the interface startup procedure.

4.5.1 PKI Infrastructure Requirements

A Public Key Infrastructure (PKI) will be used to facilitate communications between the Federal Alert Gateway and the CMSP Gateway. A PKI is an architecture that provides the means to bind public keys to their owners' private keys and helps in the distribution of reliable credentials in large heterogeneous networks. These public keys will be bound to each Federal Alert Gateway and CMSP Gateway by public key certificates. These certificates, which contain information such as the owner's name and the associated public key, are issued by a reliable Certificate Authority (CA).

The Department of Homeland Security (DHS) constrains the implementation of PKI within DHS and its subordinate agencies to use the DHS CA or to use their own agency CA that is subordinate to the DHS CA [Ref 15]. DHS also provides for cross-certification between DHS CAs and external CAs through the Federal Bridge Certificate Authority. The Federal Bridge Certification Authority was established to provide a Federal trust anchor in the certification path of certificates issued by non-Federal entities.

The process by which the authenticity of a certificate is determined is described as certification path processing. Certification path processing establishes a chain of trust between a trust anchor and a certificate. This chain of trust is composed of a series of certificates known as a certification path. A certification path begins with a certificate whose signature can be verified using a trust anchor and ends with the target certificate. The process of validating a certificate is often known as "walking the chain of trust".

[WEA-C-RQMT-1400] Federal Alert Gateways shall use X.509 Certificates [Ref 19] that have been issued by a PKI infrastructure that is cross-certified with the Federal PKI Bridge.

[WEA-C-RQMT-1410] CMSP Gateways shall use X.509 Certificates [Ref 19] that have been issued by a PKI infrastructure that is cross-certified with the Federal PKI Bridge.

4.5.1.1 X.509 Certificates

Once an appropriate CA is established, an X.509 certificate will be used for establishing authentication in the IKE between the Federal Alert Gateway and the CMSP Gateway. The certificate is an identifier that contains either the Federal Alert Gateway or CMSP Gateway name, issuer name, and the public key. In addition, the certificates include a digital signature, an issuance and expiration date, and identifiers that specify the cryptographic algorithm to be used with the public key and signature.

[WEA-C-RQMT-1500] The format for certificates between the CMSP Gateway and the Federal Alert Gateway shall be X.509 version 3 (X.509v3) certificate [Ref 19].

[WEA-C-RQMT-1510] The Federal Alert Gateway and the CMSP Gateway shall check the revocation status of the peer's X.509 certificate using the Online Certificate Status Protocol (OCSP), specified in RFC 6960 [Ref 34].

[WEA-C-RQMT-1520] Federal Alert Gateway and CMSP Gateways establishing security associations shall use OCSP over HTTP using the Nonce and Archive Cutoff options only.

NOTE: No other options will be used.

4.5.1.2 IPsec X.509 Identifiers

Communication between the Federal Alert Gateway and the CMSP Gateway will require the establishment of IPsec Security Associations (SAs). To ensure that IPsec SAs have not been established with a compromised entity, and for auditing purposes, the CMSP Gateway and the Federal Alert Gateway will control the established connections.

[WEA-C-RQMT-1600] The identifiers for establishing an IPsec tunnel shall be the CMSP Gateway and Federal Alert Gateway Fully Qualified Domain Names or IP addresses.

NOTE: See Federal Alert Gateway profile in Table 4.4 and CMSP Profile in Table 4.3.

[WEA-C-RQMT-1610] The Fully Qualified Domain Names and IP addresses shall be unique identifiers.

NOTE: See Federal Alert Gateway profile in Table 4.4 and CMSP Profile in Table 4.3.

[WEA-C-RQMT-1620] The Federal Alert Gateway shall close the associated communication sockets, if the intended communication is with a CMSP Gateway and none of the distinguished names on the received certificate appear on the CMSP Gateway profile.

[WEA-C-RQMT-1630] The CMSP Gateway shall close the associated communication sockets, if the intended communication is with a Federal Alert Gateway and none of the distinguished names on the received certificate appear in the Federal Alert Gateway profile.

4.5.2 IPsec Requirements

IPsec is a suite of protocols for securing Internet communications at the network layer and operates within the IP. It is frequently used to establish VPNs, requiring both parties to share keying material, and enabling secure communication between two gateways. As such, the IPsec descriptions below describe message flow requirements between the Federal Alert Gateway and the CMSP Gateway and not these systems themselves. IPsec provides the cryptographic security functions for both IPv4 and IPv6. This clause specifies the IPsec requirements to be applied.

[WEA-C-RQMT-1700] IPsec version 3 (IPsec v3) [Refs 3, 10, 11, & 12] shall be used on the Federal Alert Gateway to CMSP Gateway Interface.

[WEA-C-RQMT-1710] An IPsec v3 tunnel shall be established to protect all messages when transmitted between the Federal Alert Gateway and the CMSP Gateway.

[WEA-C-RQMT-1720] The encrypted information shall include all CMAC messages as well as the associated keys.

4.5.2.1 IPsec Tunneling Requirements

A 112-bit strength algorithm suite is sufficient to overcome advances in computing power over the life of a system operating after 2010. The requirements in the following sub-clauses are consistent with a 112-bit strength algorithm.

4.5.2.1.1 IPsec ESP Encryption

Encapsulating Security Payload (ESP) is used to provide confidentiality, data origin authentication, detection and rejection of replays, and data integrity. ESP operates in tunnel mode (with new IP header inserted) to protect the original IP header.

[WEA-C-RQMT-1800] The Authentication Header (AH) option shall not be used.

NOTE: AH is not compatible with Network Address Translation [Ref 14].

[WEA-C-RQMT-1810] The IPsec protocol shall utilize ESP [Ref 13].

[WEA-C-RQMT-1820] The algorithms in Table 4.5: *Required Algorithms for Implementation of ESP* shall be used to implement the ESP.

Table 4.5 – Required Algorithms for Implementation of ESP

Function	Encryption	AES Key Length	Integrity	Peer Authentication
Required Algorithm	AES in CBC Mode [Ref 16]	128	HMAC-SHA-256 [Ref 40]	2048-bit RSA with SHA-256 [Refs 7 & 18]

4.5.2.1.2 IPsec Key Exchange Protocol

The IPsec SAs concept provides for the establishment of a secure network data exchange between two peer entities: the Federal Alert Gateway and the CMSP Gateway. Before secure data is exchanged between peers, SAs are established, allowing the peers to both agree on how to exchange data and support a secure communication. This agreement involves the use of the IKE.

[WEA-C-RQMT-1900] The Federal Alert Gateway to CMSP Gateway Interface shall use key exchange per IKE v2 [Ref 12].

[WEA-C-RQMT-1910] Manual keying shall not be used.

NOTE: Automatic keying was chosen for key management to ensure re-keying capability, scalability, and detection of replays.

[WEA-C-RQMT-1920] The algorithms in Table 4.6 – *Required Algorithms for Implementation of IKE v2* shall be used to implement the IKE v2.

Table 4.6 – Required Algorithms for Implementation of IKE v2

Function	Pseudo-Random Function	Diffie-Hellman Group	Integrity	Peer Authentication
Required Algorithm	HMAC SHA-1 [Ref 17]	2048-bit MODP	HMAC-SHA-256 [Ref 40]	2048-bit RSA with SHA-256 [Refs 7 & 18]

[WEA-C-RQMT-1930] All algorithms shall be upgradable with a new library and configuration change.

[WEA-C-RQMT-1940] Algorithm upgrades shall not require a full system hardware upgrade.

[WEA-C-RQMT-1950] All algorithm functions shall be implemented in according with the Requests for Comment (RFCs) in Table 4.7 – *Summary of References for IPsec*.

Table 4.7 – Summary of References for IPsec

Version	Security Architecture	Privacy	Authentication
IPsec-v3	RFC 4301 [Ref 3]	RFC 4303 [Ref 10]	RFC 4303 [Ref 10]

[WEA-C-RQMT-1960] <Void>.

4.5.2.1.3 IPsec Policy

The policy described in this clause is a port-based IPsec policy which governs the transmission of all messages between the Federal Alert Gateway and the CMSP Gateway. The IPsec policy determines, at the network layer, which packets will have IPsec applied to them, which packets will be dropped, and which packets will be passed through without IPsec. The port-based IPsec policy eliminates the need for secure name resolution.

[WEA-C-RQMT-2000] The only valid IPsec SAs shall be between a CMSP Gateway and a Federal Alert Gateway.

[WEA-C-RQMT-2010] The Federal Alert Gateway and CMSP Gateway IPsec implementation shall be capable of supporting port-based traffic filtering policies.

4.5.2.1.3.1 IPsec Outbound Policy

The only outbound packets that are not IPsec-encrypted are IKEv2 messages destined for port 500. Outbound packets that are not destined for port 500 are IPsec-encrypted using the cryptographic material for the SA with the destination addresses.

[WEA-C-RQMT-2100] Outbound packets to destinations for which SAs are not allowed shall be discarded.

[WEA-C-RQMT-2110] Outbound IKEv2 message packets destined for port 500 shall not be IPsec encrypted.

NOTE: This is because one cannot have IPsec before key management creates the keys.

[WEA-C-RQMT-2120] All outbound packets not destined for port 500 shall be IPsec encrypted using the cryptographic material for the SA with the destination address.

4.5.2.1.3.2 IPsec Inbound Policy

[WEA-C-RQMT-2200] Inbound IKEv2 message packets destined for port 500 shall not be IPsec decrypted.

[WEA-C-RQMT-2210] Inbound packets that are not destined for Port 500 shall be IPsec decrypted using the cryptographic material for the SA with the source address.

[WEA-C-RQMT-2220] Inbound packets not destined for Port 500 and for which there is no SA for the source shall be discarded.

4.5.2.1.3.3 Security Association Lifetime

All security associations have an associated lifetime. This lifetime is either a maximum time duration or maximum number of bytes that can be sent through the SA. The Federal Alert Gateway to CMSP Gateway SA lifetimes will be defined as maximum time duration.

SAs are renewed either after they are expired or by rekeying shortly before they are expired. Rekeying prevents any discontinuities in message transfer and reduces traffic overhead required for new key establishment [Ref 39].

[WEA-C-RQMT-2300] SA Renewal and Rekey shall be configurable by Federal Alert Gateway and CMSP Gateway system administrators.

NOTE: SA renewal and rekey are configuration parameters (See Annex D).

[WEA-C-RQMT-2310] IPsec SA shall have a maximum lifetime of IPSec SA Maximum Lifetime.

NOTE: IPsec SA Maximum Lifetime is a configuration parameter (See Annex D).

[WEA-C-RQMT-2320] IKE SA shall have a maximum lifetime of IKE SA Maximum Lifetime.

NOTE: IKE SA Maximum Lifetime is a configuration parameter (See Annex D).

[WEA-C-RQMT-2330] Federal Alert Gateway and CMSP Gateway shall support SA renewal after expiration.

[WEA-C-RQMT-2340] Federal Alert Gateway and CMSP Gateway shall support SA rekey before expiration.

4.5.3 Non-Repudiation

Non-repudiation is a mechanism to prevent the sender of a message from later denying having sent the message. Non-repudiation on the interface between the Federal Alert Gateway and the CMSP Gateway will be implemented via XML Signatures [Ref 38]. The Federal Alert Gateway will digitally sign each CMAC Alert, Update, Cancel, and RMT message. The XML Signature is not permitted for the other messages. The signing certificate utilized by the Federal Alert Gateway is issued from a certificate authority governed by description in Clause 4.5.1, *PKI Infrastructure Requirements*. The certificate used for that XML Signature is issued to the Federal Alert Gateway hardware (not to a human user). The CMSP Gateway may optionally use the XML Signature for non-repudiation or ignore it, but it must be able to process the CMAC with the XML Signature. The algorithms for XML Signatures are summarized in the following table:

Table 4.8 – XML Signature Algorithm Summary

XML Signature Algorithm	Requirement	Comment or Reference
Signature Algorithm	RSA SHA-256	[Ref 46]
Canonicalization	Exclusive	[Ref 35]

XML Signature Algorithm	Requirement	Comment or Reference
Digest	SHA-256	[Ref 45]
Transforms	Enveloped Signatures	[Ref 38]
Certificate	X.509	[Ref 19]

The following requirements apply to XML Signatures [Ref 38] applied to CMAC messages:

[WEA-C-RQMT-2400] The XML Signature Method shall be RSA-SHA256 [Ref 7] for XML Signatures applied to CMAC messages.

[WEA-C-RQMT-2410] The Digest Method [Ref 45] shall be SHA-256 [Ref 7] for XML Signatures applied to CMAC messages.

[WEA-C-RQMT-2420] The Canonicalization Method [Ref 35] shall be Exclusive Canonicalization for XML Signatures applied to CMAC messages.

[WEA-C-RQMT-2430] The Enveloped Signature method [Ref 38] shall be used for XML Signatures applied to CMAC messages.

[WEA-C-RQMT-2440] The Federal Alert gateway shall implement non-repudiation as described in [Ref 38] for CMAC Alert, Update, Cancel, and RMT messages.

[WEA-C-RQMT-2450] The presence of a XML Signature [Ref 38] shall not cause the CMSP Gateway to fail to receive and process the message.

The CMSP Gateway may implement non-repudiation by processing the XML Signature [Ref 38].

NOTE: It is optional for the CMSP to implement non-repudiation. However, the CMSP Gateway does have to receive and process the CMAC messages with XML Signatures attached.

5 Reference Point “C” Call Flows

This clause contains the call flows for the transactions that can occur across the Reference Point “C” Interface. These call flows are grouped as follows:

- CMAC alert message call flows.
- Link test message call flows.
- Required monthly test (RMT) call flow.
- Transmission Control call flows.

Note that the call flows may describe general operations within the Federal Alert Gateway and CMSP Gateway. However, specific details of these operations are beyond the scope of this Standard.

5.1 CMAC Alert Message Call Flows

From the point of view of the Reference Point “C” Interface, the CMAC alert, update, and cancel message types have the same call flow. The variances in the call flows result from retrieval of the corresponding CAP message, from CMAC alert message transmission control, and from invalid messages across the Reference Point “C” interface. Consequently, this clause provides the following call flows which are applicable to WEA alert, update, and cancel message types:

- CMAC alert message without CAP message retrieval call flow.
- CMAC alert message with CAP message retrieval call flow.
- Invalid CMAC alert message call flow.

- Failure to retrieve CAP message call flows.

5.1.1 CMAC Message without CAP Message Retrieval Call Flow

The CMAC alert, update, and cancel message types have the same call flow across the Reference Point "C" Interface. The following figure with its descriptions of the associated call flow steps define the call flow for CMAC alert, update, and cancel message types:

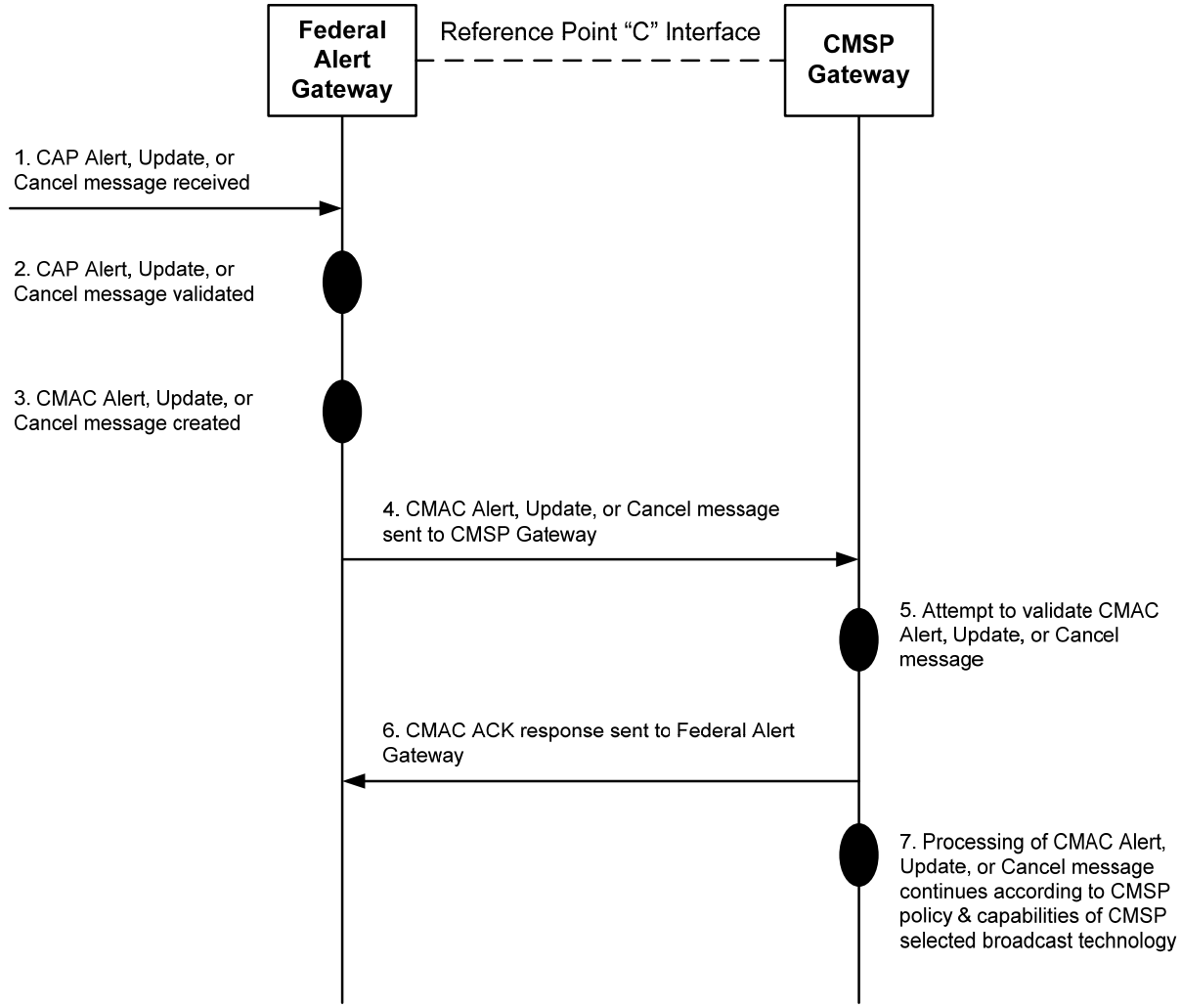


Figure 5.1 – CMAC Message without CAP Message Retrieval Call Flow

1. A CAP Alert, Update, or Cancel message is received by the Federal Alert Gateway. This function is beyond the scope of this Standard.
2. The received CAP Alert, Update, or Cancel message is validated by the Federal Alert Gateway (i.e., meets the criteria for a WEA alert as defined in the FCC First Report and Order [Ref 9] and the FCC Report and Order on WEA enhancements [Ref 41]). The received CAP message is stored on the Federal Alert Gateway for potential retrieval by the CMSP Gateway.

   NOTE: The behavior of the Federal Alert Gateway is beyond the scope of this Standard.
3. The Federal Alert Gateway constructs a CMAC Alert, Update, or Cancel message using attributes from the received CAP message.
4. The Federal Alert Gateway sends the CMAC Alert, Update, or Cancel message to the CMSP Gateway via the Reference Point "C" Interface.

5. The CMSP Gateway attempts to validate the received CMAC message and the received CMAC message passes validation.
6. The CMSP Gateway sends a CMAC Acknowledgement (ACK) message back to the Federal Alert Gateway via the Reference Point “C” Interface.
7. The processing of the received CMAC Alert, Update, or Cancel message continues according to CMSP policy and according to the capabilities of the CMSP selected technology for the broadcast of WEA alerts.

5.1.2 CMAC Message with CAP Message Retrieval Call Flow

Whenever the CMSP Gateway receives a CMAC alert, update, or cancel message from the Federal Alert Gateway, the CMSP Gateway has the option, based upon CMSP policy, to retrieve the corresponding CAP message. CMSP use of the corresponding CAP message is beyond the scope of this Standard. The following figure with its descriptions of the associated call flow steps provides an example call flow for the retrieval of the CAP message across the Reference Point “C” Interface after a valid CMAC alert, update, or cancel message type has been received by the CMSP Gateway. Note this retrieval may occur at a different point in the CMSP Gateway processing, depending on CMSP policy:

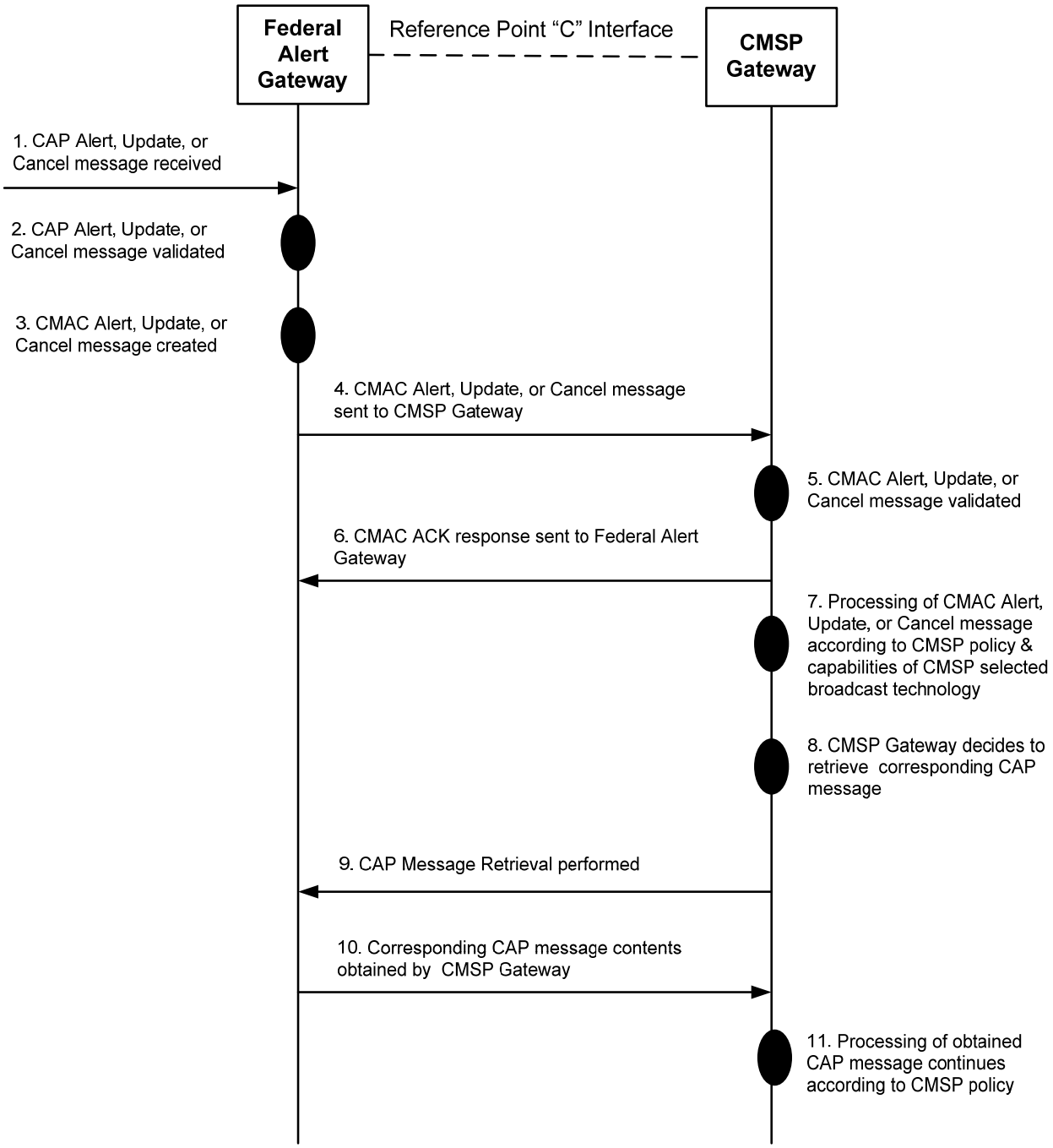


Figure 5.2 – CMAC Message with CAP Message Retrieval Call Flow

1. A CAP Alert, Update, or Cancel message is received by the Federal Alert Gateway. This function is beyond the scope of this Standard.
2. The received CAP Alert, Update, or Cancel message is validated by the Federal Alert Gateway (i.e., meets the criteria for a WEA alert as defined in the FCC First Report and Order [Ref 9] and the FCC Report and Order on WEA enhancements [Ref 41]). The received CAP message is stored on the Federal Alert Gateway for potential retrieval by the CMSP Gateway.

   NOTE: The behavior of the Federal Alert Gateway is beyond the scope of this Standard.
3. The Federal Alert Gateway constructs a CMAC Alert, Update, or Cancel message using attributes from the received CAP message.

4. The Federal Alert Gateway sends the CMAC Alert, Cancel, or Update message to the CMSP Gateway via the Reference Point “C” Interface.
5. The CMSP Gateway validates the received CMAC message and the received CMAC message passes validation.
6. The CMSP Gateway sends a CMAC Ack message back to the Federal Alert Gateway via the Reference Point “C” Interface.
7. The processing of the received CMAC Alert, Update, or Cancel message continues according to CMSP policy and according to the capabilities of the CMSP-selected technology for the broadcast of WEA alerts.
8. Based upon CMSP policy, the CMSP Gateway may retrieve the corresponding CAP message from the Federal Alert Gateway.
9. The CMSP Gateway sends the CAP message retrieval request to the Federal Alert Gateway via the Reference Point “C” interface.

   NOTE: The CMSP Gateway is able to determine the CAP version from the CAP XML header information [Ref 4].
10. The Federal Alert Gateway sends the contents of the corresponding CAP message to the CMSP Gateway via the Reference Point “C” interface.
11. The processing of the received CAP message continues according to CMSP policy.

5.1.3 Failure to Retrieve CAP Message Call Flows

The following scenarios illustrate failures to retrieve the corresponding CAP message associated with a CMAC alert, update, or cancel type message.

5.1.3.1 Federal Alert Gateway Failure to Retrieve Corresponding CAP Message

The following scenario illustrates the Federal Alert Gateway determining that it is unable to retrieve the corresponding CAP message.

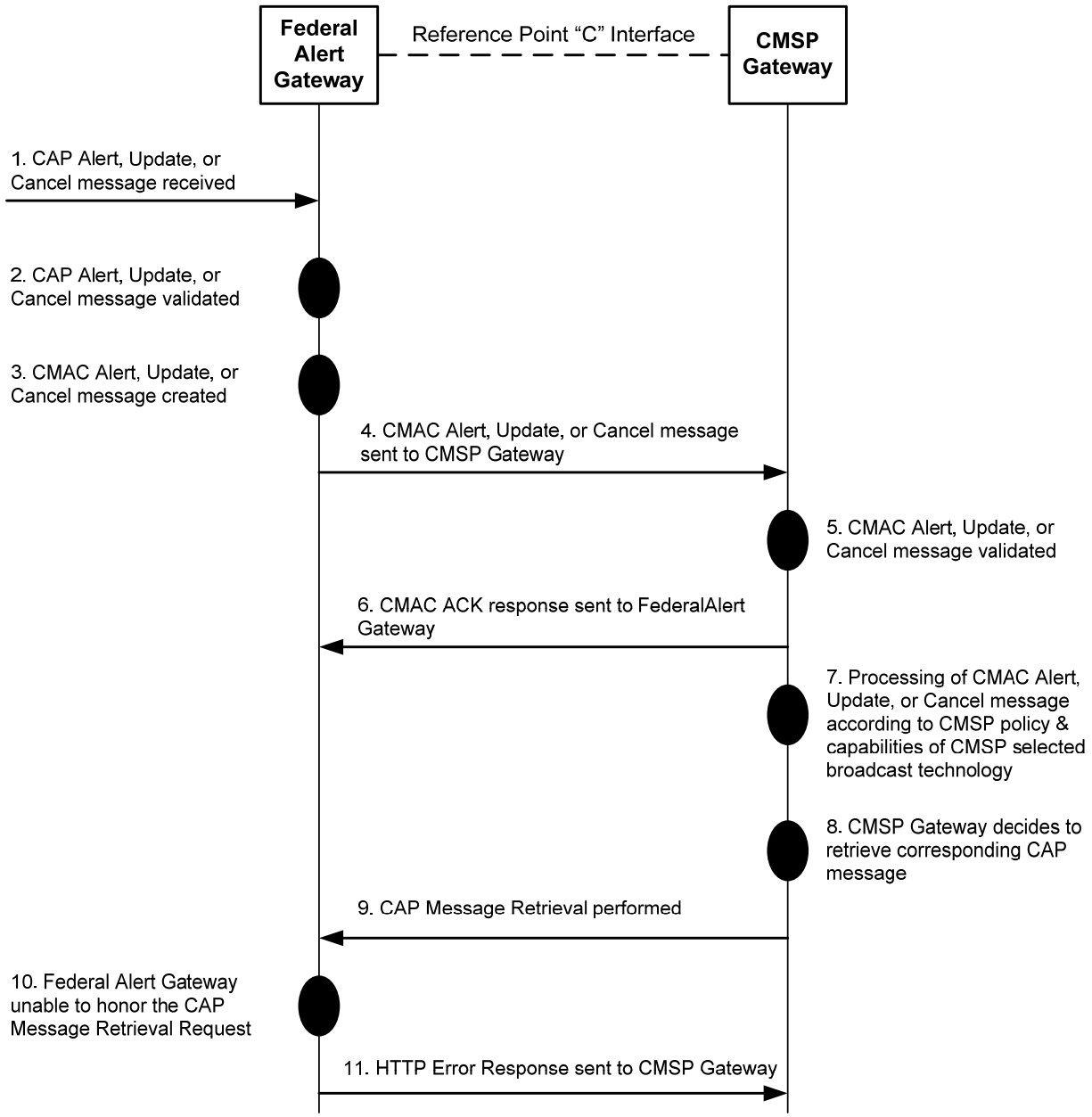


Figure 5.3 – Federal Alert Gateway Failure to Retrieve CAP Message Call Flow

1. A CAP Alert, Update, or Cancel message is received by the Federal Alert Gateway. This function is beyond the scope of this Standard.
2. The received CAP Alert, Update, or Cancel message is validated by the Federal Alert Gateway (i.e., meets the criteria for a WEA alert as defined in the FCC First Report and Order [Ref 9] and the FCC Report and Order on WEA enhancements [Ref 41]). The received CAP message is stored on the Federal Alert Gateway for potential retrieval by the CMSP Gateway.

   NOTE: The behavior of the Federal Alert Gateway for an invalid CAP message is beyond the scope of this Standard.
3. The Federal Alert Gateway constructs a CMAC Alert, Update, or Cancel message using attributes from the received CAP message.
4. The Federal Alert Gateway sends the CMAC Alert, Cancel, or Update message to the CMSP Gateway via the Reference Point "C" Interface.
5. The CMSP Gateway validates the received CMAC message and the received CMAC message passes

validation.

6. The CMSP Gateway sends a CMAC Ack message back to the Federal Alert Gateway via the Reference Point “C” Interface.
7. The processing of the received CMAC Alert, Update, or Cancel message continues according to CMSP policy and according to the capabilities of the CMSP-selected technology for the broadcast of WEA alerts.
8. Based upon CMSP policy, the CMSP Gateway decides to retrieve the corresponding CAP message from the Federal Alert Gateway
9. The CMSP Gateway sends the CAP message retrieval request to the Federal Alert Gateway via the Reference Point “C” interface.
10. The Federal Alert Gateway determines that it is unable to honor the retrieval request from the CMSP Gateway (e.g., error in the CMSP Gateway request, Federal Alert Gateway unable to retrieve corresponding CAP message at this time).
11. The Federal Alert Gateway sends an HTTP Error Response to the CMSP Gateway via the Reference Point “C” interface with an indication of the type of error encountered.

    NOTE: Any additional behavior by the Federal Alert Gateway when an HTTP error response is sent to the CMSP Gateway is beyond the scope of this Standard.

5.1.3.2 CMSP Gateway Detection of Failure to Retrieve Corresponding CAP Message

The following scenario illustrates the CMSP Gateway detecting a failure to retrieve the corresponding CAP Message.

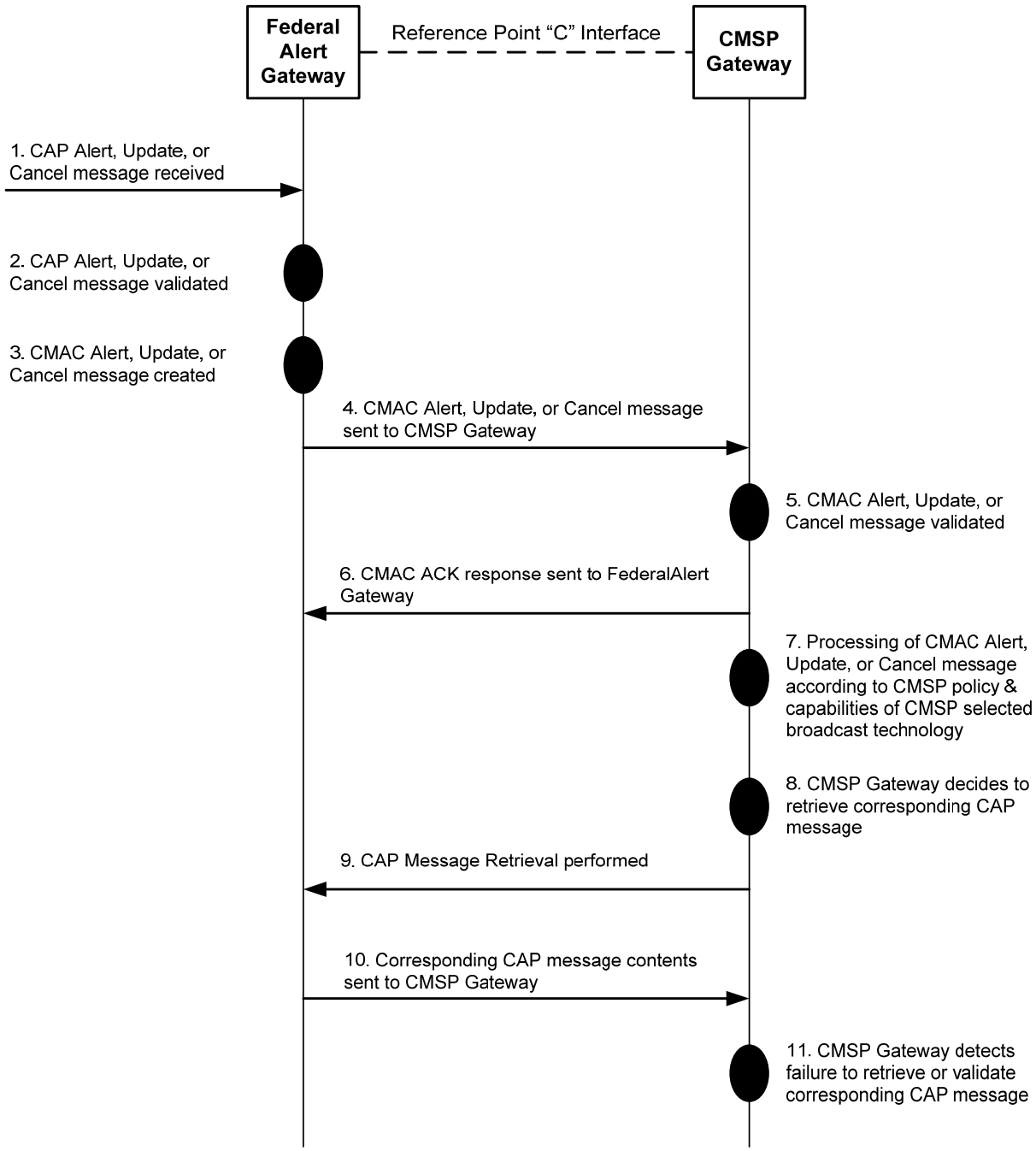


Figure 5.4 – CMSP Gateway Detection of Failure to Retrieve Corresponding CAP Message

1. A CAP Alert, Update, or Cancel message is received by the Federal Alert Gateway. This function is beyond the scope of this Standard.
2. The received CAP Alert, Update, or Cancel message is validated by the Federal Alert Gateway (i.e., meets the criteria for a WEA alert as defined in the FCC First Report and Order [Ref 9] and the FCC Report and Order on WEA enhancements [Ref 41]). The received CAP message is stored on the Federal Alert Gateway for potential retrieval by the CMSP Gateway.

   NOTE: The behavior of the Federal Alert Gateway for an invalid CAP message is beyond the scope of this Standard.

3. The Federal Alert Gateway constructs a CMAC Alert, Update, or Cancel message using attributes from the received CAP message.

4. The Federal Alert Gateway sends the CMAC Alert, Update, or Cancel message to the CMSP Gateway via the Reference Point “C” Interface.
5. The CMSP Gateway validates the received CMAC message and the received CMAC message passes validation.
6. The CMSP Gateway sends a CMAC Acknowledgement Ack message back to the Federal Alert Gateway via the Reference Point “C” Interface.
7. The processing of the received CMAC Alert, Update, or Cancel message continues according to CMSP policy and according to the capabilities of the CMSP-selected technology for the broadcast of WEA alerts.
8. Based upon CMSP policy, the CMSP Gateway decides to retrieve the corresponding CAP message from the Federal Alert Gateway
9. The CMSP Gateway sends the CAP message retrieval request to the Federal Alert Gateway via the Reference Point “C” interface.
10. The Federal Alert Gateway retrieves the corresponding CAP message and sends the contents to the CMSP Gateway via the Reference Point “C” interface.
11. The CMSP Gateway determines that there is a failure to retrieve the corresponding CAP message (e.g., CAP message not received, CAP message received but not validated).

    NOTE: The CMSP Gateway behavior when there is a failure to retrieve the CAP message is beyond the scope of this Standard.

5.1.4 Invalid CMAC Message Call Flow

All CMAC alert messages received by CMSP Gateway over the Reference Point “C” Interface are validated for content, format, and structure. The following figure with its descriptions of the associated call flow steps define the call flow for invalid CMAC Alert, Update, or Cancel messages received by the CMSP Gateway over the Reference Point “C” Interface:

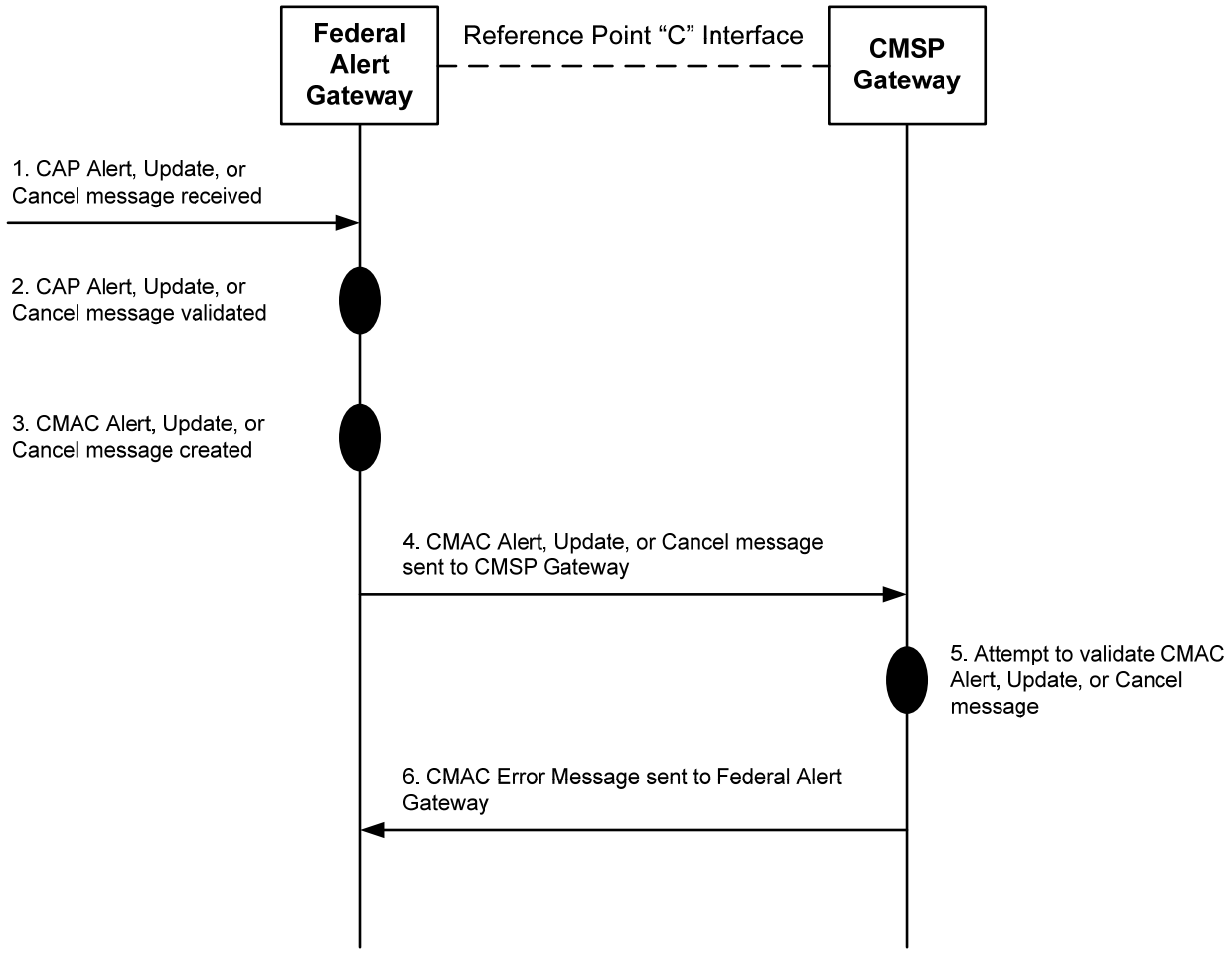


Figure 5.5 – Invalid CMAC Message Call Flow

1. A CAP Alert, Update, or Cancel message is received by the Federal Alert Gateway. This function is beyond the scope of this Standard.
2. The received CAP Alert, Update, or Cancel message is validated by the Federal Alert Gateway (i.e., meets the criteria for a WEA alert as defined in the FCC First Report and Order [Ref 9] and the FCC Report and Order on WEA enhancements [Ref 41]). The received CAP message is stored on the Federal Alert Gateway for potential retrieval by the CMSP Gateway.

   NOTE: The behavior of the Federal Alert Gateway is beyond the scope of this Standard.
3. The Federal Alert Gateway constructs a CMAC Alert, Update, or Cancel message using attributes from the received CAP message.
4. The Federal Alert Gateway sends the CMAC Alert, Update, or Cancel message to the CMSP Gateway via the Reference Point "C" Interface.
5. The CMSP Gateway attempts to validate the received CMAC message and the received CMAC message fails validation.
6. If the CMSP Gateway trusts the received CMAC message, and the characteristic of the validation failure allows a valid CMAC Error response message to be created, then the CMSP Gateway sends a CMAC Error message with the validation failure reason back to the Federal Alert Gateway via the Reference Point "C" Interface.

   NOTE: The behavior of the Federal Alert Gateway when a CMAC Error message with the validation failure reason is received from the CMSP Gateway is beyond the scope of this Standard.

5.2 Link Test Message Call Flows

One of the WEA requirements is to verify the availability of the Reference Point "C" Interface and the availability of the WEA functionality. The Link Test Message between the Federal Alert Gateway and the CMSP Gateway is used to comply with this requirement. This clause provides the following link test call flows:

- Link Test Message to CMSP Gateway call flow.
- Invalid Link Test Message to CMSP Gateway call flow.
- Link Test Message from CMSP Gateway call flow.
- Invalid Link Test Message from CMSP Gateway call flow.

5.2.1 Link Test Message to CMSP Gateway Call Flow

The Federal Alert Gateway will periodically issue Link Test Messages to the CMSP Gateway to verify the availability of the Reference Point "C" interface and the CMSP Gateway. The following figure with its descriptions of the associated call flow steps define the call flow for a Link Test Message sent from the Federal Alert Gateway to the CMSP Gateway over the Reference Point "C" Interface:

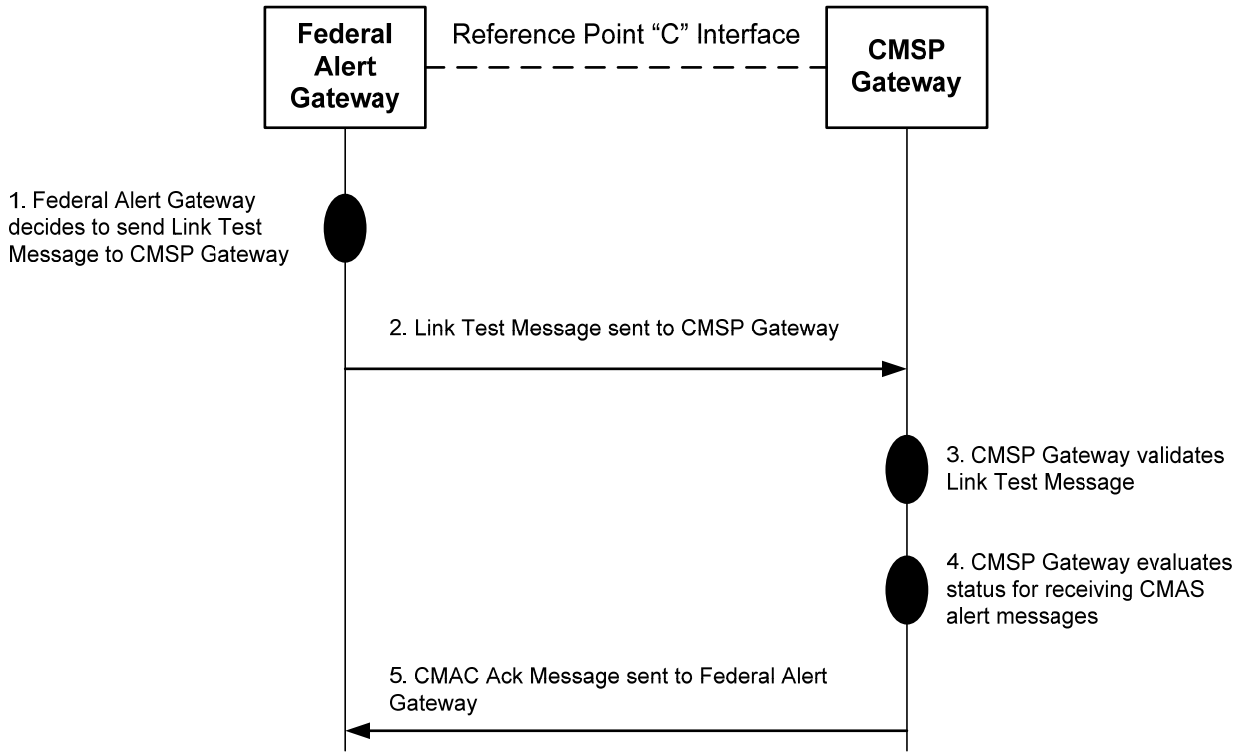


Figure 5.6 – Link Test Message to CMSP Gateway Call Flow

1. The Federal Alert Gateway decides to send a link test to the CMSP Gateway and constructs the Link Test Message.

   NOTE: The methodology and frequency for the creation of the Link Test Messages by the Federal Alert Gateway is beyond the scope of this Standard.

2. The Federal Alert Gateway sends the Link Test Message to the CMSP Gateway via the Reference Point "C" Interface.
3. The CMSP Gateway validates the received Link Test Message and the received Link Test Message passes validation.
4. The CMSP Gateway determines its ability to receive WEA alert messages. This determination is beyond the scope of this Standard.
5. The CMSP Gateway sends a CMAC Ack Message back to the Federal Alert Gateway.

5.2.2 Invalid Link Test Message to CMSP Gateway Call Flow

Link Test Messages received by CMSP Gateway over the Reference Point “C” Interface are validated for content, format, and structure. The following figure with its descriptions of the associated call flow steps define the call flow for invalid Link Test Message sent to the CMSP Gateway over the Reference Point “C” Interface:

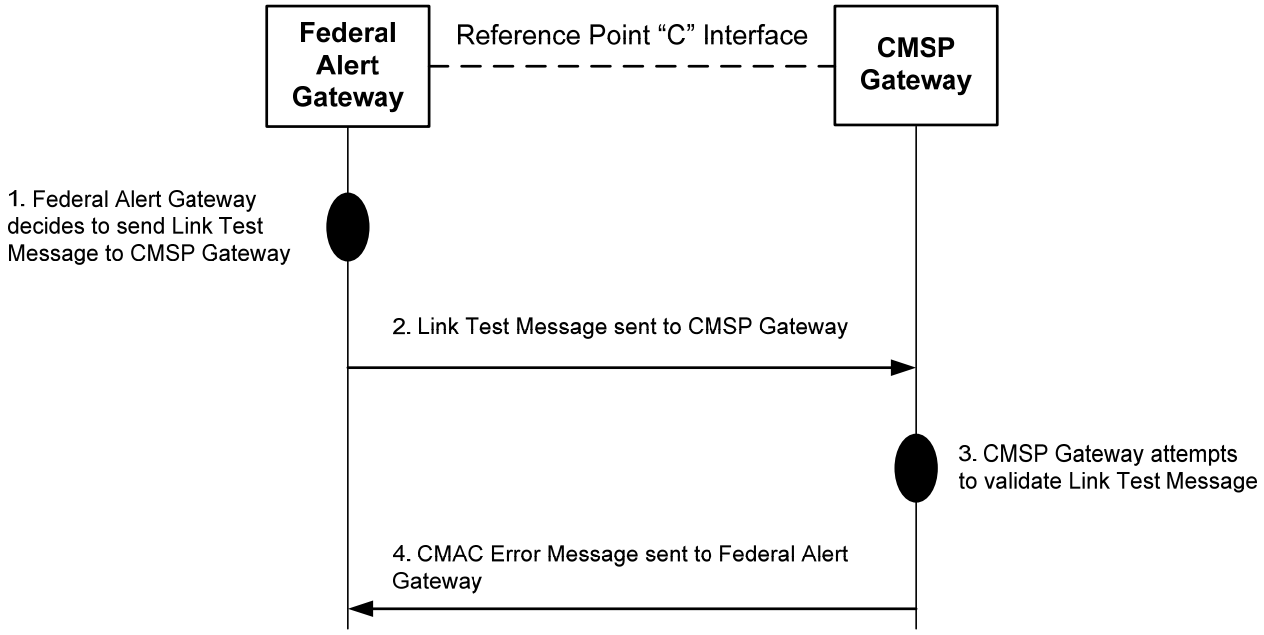


Figure 5.7 – Invalid Link Test Message from Federal Alert Gateway Call Flow

1. The Federal Alert Gateway decides to send a link test to the CMSP Gateway and constructs the Link Test Message.

   NOTE: The methodology and frequency for the creation of the Link Test Messages by the Federal Alert Gateway is beyond the scope of this Standard.

2. The Federal Alert Gateway sends the Link Test Message to the CMSP Gateway via the Reference Point “C” Interface.
3. The CMSP Gateway attempts to validate the received Link Test Message and the received Link Test Message fails validation.
4. The CMSP Gateway sends a CMAC Error message with the validation failure reason back to the Federal Alert Gateway via the Reference Point “C” Interface.

   NOTE: The behavior of the Federal Alert Gateway when a CMAC Error message with the validation failure reason is received from the CMSP Gateway is beyond the scope of this Standard.

5.2.3 Link Test Message from CMSP Gateway Call Flow

As a CMSP implementation option, the CSMP Gateway can send a Link Test Message to the Federal Alert Gateway to verify the availability of the Reference Point “C” interface and the WEA functionality. The following figure with its descriptions of the associated call flow steps define the call flow for a Link Test Message sent from the CMSP Gateway to the Federal Alert Gateway over the Reference Point “C” Interface:

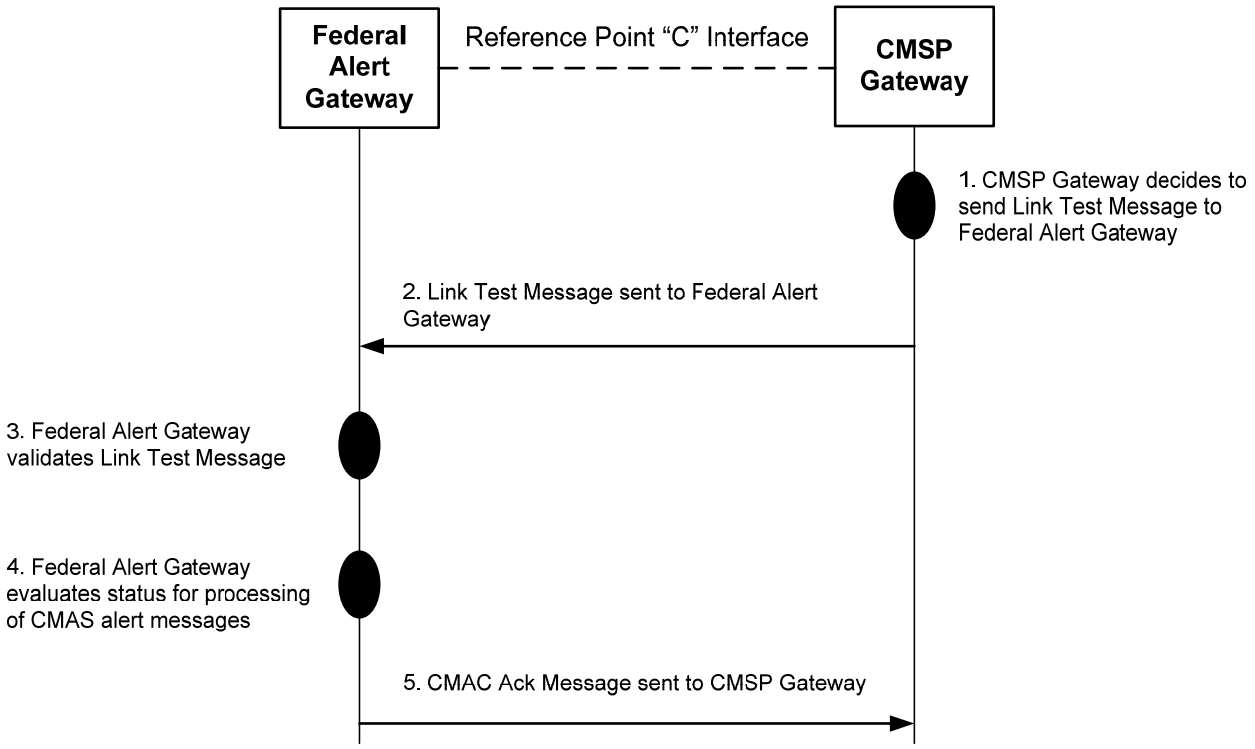


Figure 5.8 – Link Test Message from CMSP Gateway Call Flow

1. The CMSP Gateway decides to send a link test to the Federal Alert Gateway and constructs the Link Test Message.

   NOTE: The methodology and frequency for the creation of the Link Test Messages by the CMSP Gateway is beyond the scope of this Standard.

2. The CMSP Gateway sends the Link Test Message to the Federal Alert Gateway via the Reference Point "C" Interface.
3. The Federal Alert Gateway validates the received Link Test Message and the received Link Test Message passes validation.
4. The Federal Alert Gateway determines the availability of the WEA functionality.

   NOTE: The methodologies to determine the availability of the WEA functionality are subject to the policies of the Federal administrator of the Federal Alert Gateway and are beyond the scope of this Standard.

5. The Federal Alert Gateway sends a CMAC Ack Message back to the CMSP Gateway.

5.2.4 Invalid Link Test Message from CMSP Gateway Call Flow

Link Test Messages received by Federal Alert Gateway over the Reference Point "C" Interface are validated for content, format, and structure. The following figure with its descriptions of the associated call flow steps define the call flow for invalid Link Test Message sent to the Federal Alert Gateway over the Reference Point "C" Interface:

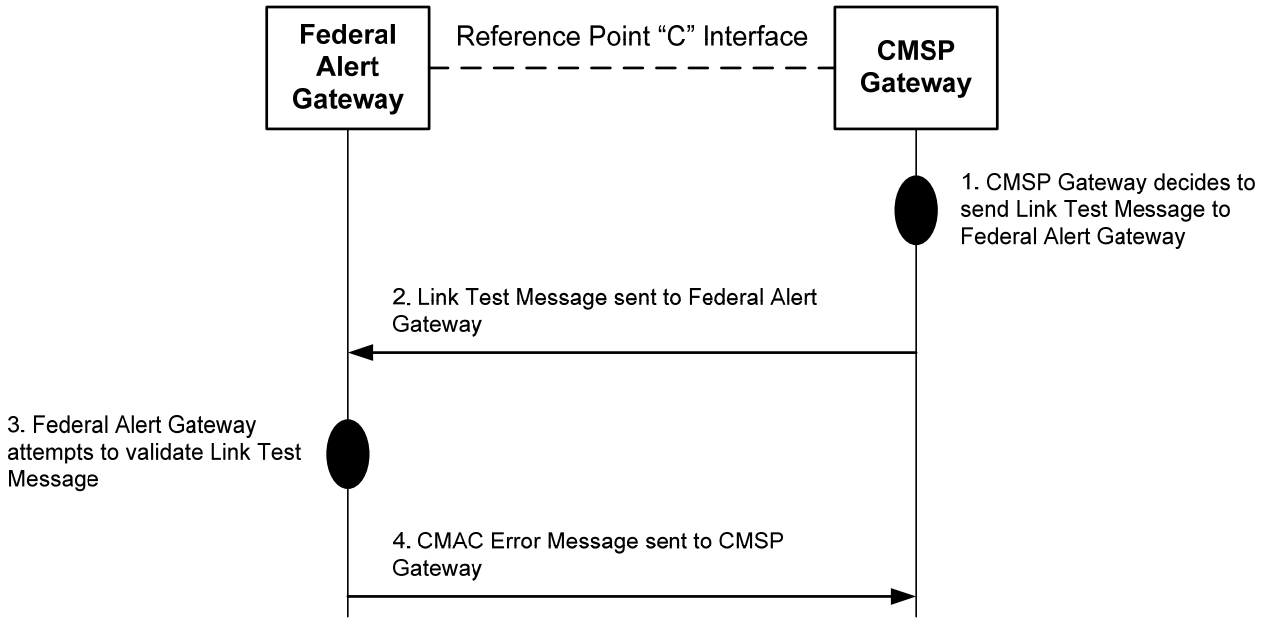


Figure 5.9 – Invalid Link Test Message from CMSP Gateway Call Flow

1. The CMSP Gateway decides to send a link test to the Federal Alert Gateway and constructs the Link Test Message.

   NOTE: The methodology and frequency for the creation of the Link Test Messages by the CMSP Gateway is beyond the scope of this Standard.

2. The CMSP Gateway sends the Link Test Message to the Federal Alert Gateway via the Reference Point "C" Interface.
3. The Federal Alert Gateway attempts to validate the received Link Test Message and the received Link Test Message fails validation.
4. The Federal Alert Gateway sends a CMAC Error message with the validation failure reason back to the CMSP Gateway via the Reference Point "C" Interface.

   NOTE: Any additional behavior by the Federal Alert Gateway when a CMAC Error message with the validation failure reason is sent to the CMSP Gateway is beyond the scope of this Standard.

5.3 Required Monthly Test (RMT) Call Flow

The Federal Alert Gateway may issue an RMT Message to the CMSP Gateway. The following figure with its descriptions of the associated call flow steps define the call flow for a RMT Message sent from the Federal Alert Gateway to the CMSP Gateway over the Reference Point "C" Interface:

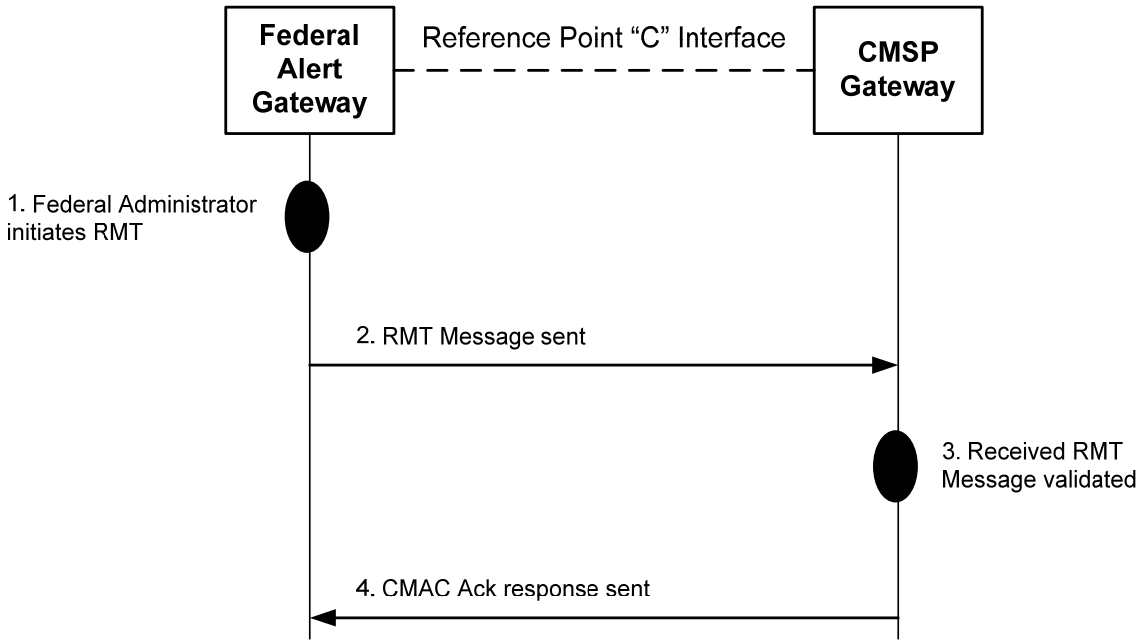


Figure 5.10 – Required Monthly Test Call Flow

1. An authorized Federal Administrator initiates an RMT at the Federal Alert Gateway. This function is beyond the scope of this Standard.
2. The Federal Alert Gateway sends the RMT Message to the CMSP Gateway via the Reference Point "C" Interface.
3. The CMSP Gateway validates the received RMT Message and the received RMT Message passes validation.
4. The CMSP Gateway sends a CMAC Ack Message back to the Federal Alert Gateway via the Reference Point "C" Interface.

NOTE: Upon receipt of the RMT Message, if the CMSP determines an unforeseen condition in the CMSP infrastructure that precludes distribution of the RMT Message, the CMSP Gateway sends an Error message back to the Federal Alert Gateway indicating that an unforeseen condition in CMSP infrastructure precludes distribution of the RMT Message. The CMSP determination of types of unforeseen conditions and procedures for precluding RMT processing are beyond the scope of this Standard.

5.4 Transmission Control Message Call Flows

The CMSP Gateway may request message traffic on Reference Point "C" destined for the CMSP Gateway be ceased or resumed via maintenance commands on the CMSP Gateway or internal error processing. This clause provides the following transmission control call flows:

- Cease transmissions call flow.
- Resume transmissions call flow.

5.4.1 Cease Transmissions Call Flow

The CMSP Gateway may request transmissions of all messages destined for the CMSP Gateway be ceased via maintenance command on the CMSP Gateway or internal error processing.

The following figure with its descriptions of the associated call flow steps defines the call flow for a Transmission Control – Cease Message sent from the CMSP Gateway to the Federal Alert Gateway over the Reference Point "C" Interface:

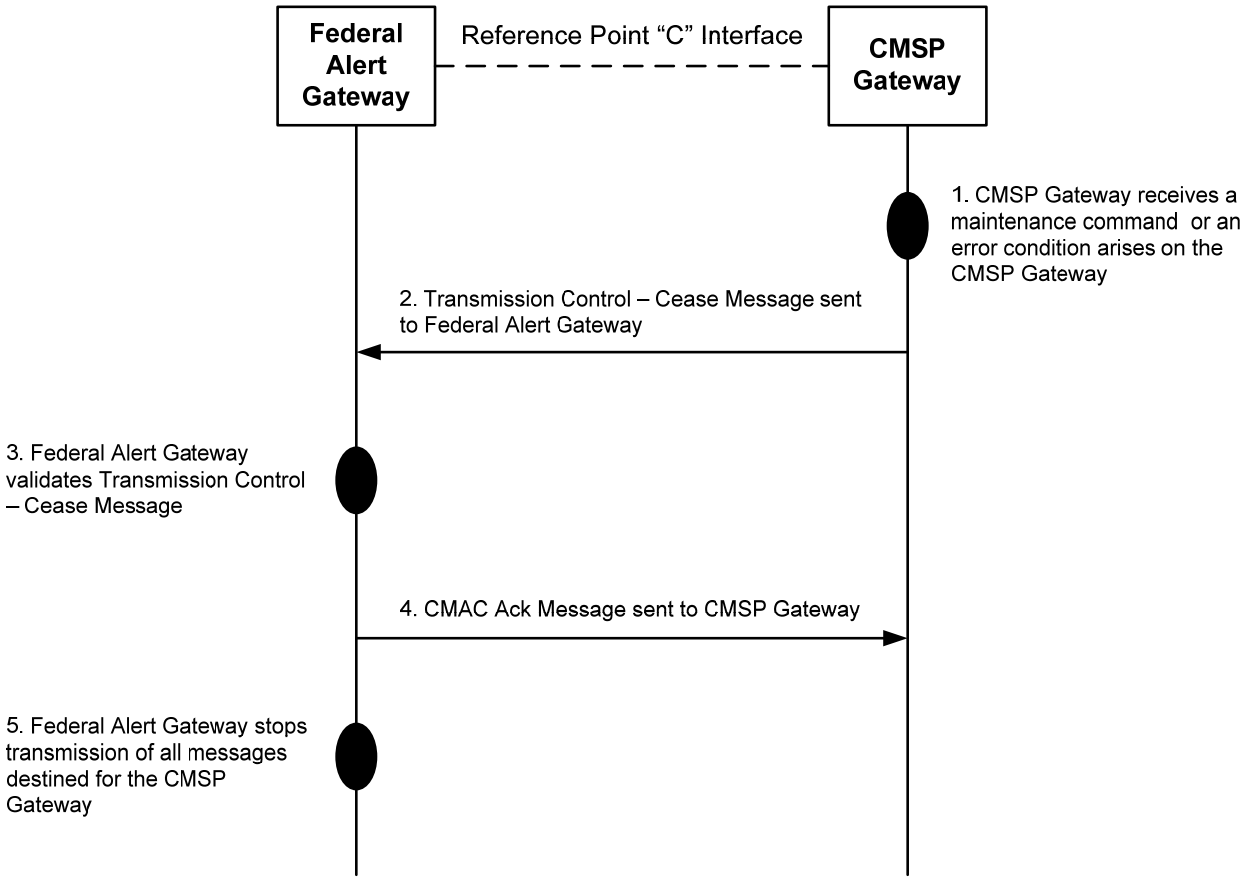


Figure 5.11 – Cease Transmissions Call Flow

1. The CMSP Gateway receives a maintenance command to request the Federal Alert Gateway stop transmissions of all messages destined for the CMSP Gateway or an error condition arises, which prevents the CMSP Gateway from processing any further messages from the Federal Alert Gateway.
2. The CMSP Gateway sends the Transmission Control – Cease Message to the Federal Alert Gateway via the Reference Point "C" Interface.
3. The Federal Alert Gateway validates the received Transmission Control – Cease Message from the CMSP Alert Gateway.
4. The Federal Alert Gateway sends a CMAC Ack Message back to the CMSP Gateway.

   NOTE: The CMSP Alert Gateway may choose to ignore the Transmission Control Acknowledgement Message.
5. The Federal Alert Gateway stops transmissions of all messages destined for the CMSP Gateway.

5.4.2 Resume Transmissions Call Flow

Once the maintenance or error condition that triggered the stop of message transmission over the Reference Point "C" Interface is cleared, the CMSP Gateway informs the Federal Alert Gateway that transmission of messages may resume. The following figure with its descriptions of the associated call flow steps defines the call flow for a Transmission Control – Resume Message sent from the CMSP Gateway to the Federal Alert Gateway over the Reference Point "C" Interface:

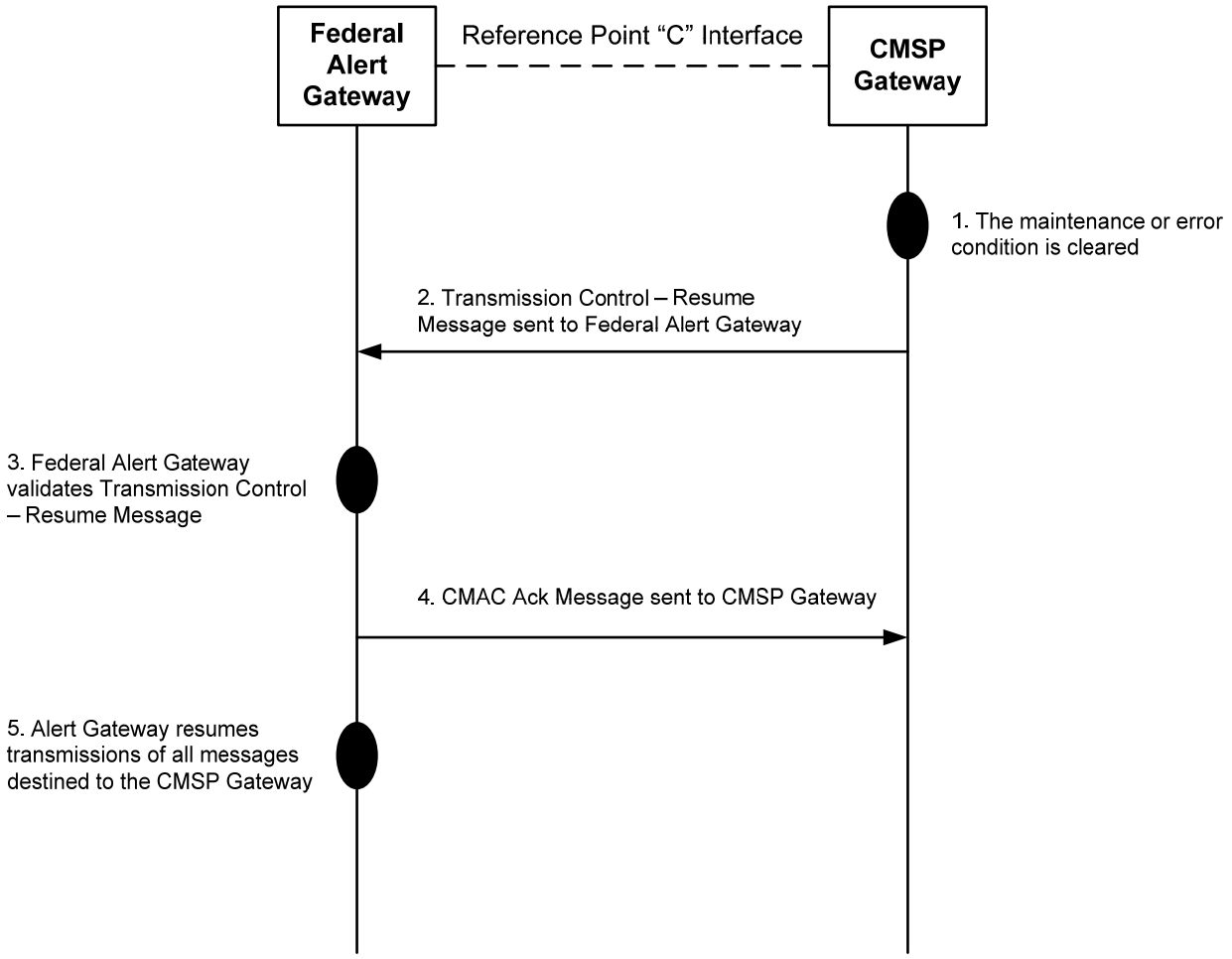


Figure 5.12 – Resume Transmissions Call Flow

1. The maintenance or error condition that triggered the stop of message transmission over the Reference Point "C" Interface is cleared.
2. The CMSP Gateway sends the Transmission Control – Resume Message to the Federal Alert Gateway via the Reference Point "C" Interface.
3. The Federal Alert Gateway validates the received Transmission Control – Resume Message from the CMSP Alert Gateway.
4. The Federal Alert Gateway sends a CMAC Ack Message back to the CMSP Gateway.
5. The Federal Alert Gateway may resume transmission of messages destined to the CMSP Gateway.

6 Federal Alert Gateway to CMSP Gateway Protocol Requirements & Definition

The Commercial Mobile Alert (CMA) Reference Point "C" protocol supports delivery and acknowledgement of a new, updated, or cancelled commercial mobile alert message between the Federal Alert Gateway and the CMSP Gateway. The protocol also enables testing, verification of network entity availability, and transmission control.

This description of the protocol between the Federal Alert Gateway and the CMSP Gateway is structured as follows:

- Application Layer.
- Message structure.
- Mapping of Common Alerting Protocol and Reference Point "C" Protocol.

- Element definition.
- XML definition.
- Transport protocol.
- Reference Point “C” Interface Security.

6.1 Application Layer

6.1.1 CMAC Protocol

The majority of the messages exchanged between the Federal Alert Gateway and the CMSP Gateway (see Table 4.1, *Characteristics of Messages from Federal Alert Gateway*, and Table 4.2, *Characteristics of Messages from CMSP Gateway*) will be in the CMAC format. Retrieval of the CAP message (as well as the CAP message itself) does not use CMAC. The CMAC protocol content by message type is captured in Clause 6.5, *CMAC Message Types & Example XML*, while the details of the CMAC Protocol are captured in Clauses 6.2, *Message Structure,* and Clause 6.3, *Element Definition*.

Note that for each CMAC message, Conditional and Optional elements defined in the protocol are to be included as applicable to the particular message.

[WEA-C-RQMT-2500] The CMAC_protocol_version element shall be set to "2.0” for this version of the Standard.

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

- Table 6.8 – CMAC_Digital_Signature Segment Element Definition.
- Table 6.9 – Elements of Alert Attributes Segment for Alert Message.
- Table 6.10 – Elements of Alert Info Segment for Alert Message.
- Table 6.11 – Elements of Alert Area Segment for Alert Message.
- Table 6.12 – Elements of Alert Text Segment for Alert Message.

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

- Table 6.8 – CMAC_Digital_Signature Segment Element Definition.
- Table 6.13 – Elements of Alert Attributes Segment for Update Message.
- Table 6.14 – Elements of Alert Info Segment for Update Message.
- Table 6.15 – Elements of Alert Area Segment for Update Message.
- Table 6.16 – Elements of Alert Text Segment for Update Message.

[WEA-C-RQMT-2530] The conditional CMAC_special_handling element shall be included in Alert, Update, and Cancel messages if the Federal Alert Gateway determines that the message is a National Alert, a Child Abduction/AMBER Alert, a Required Monthly Test, a Public Safety message, or a State/Local WEA Test message.

[WEA-C-RQMT-2540] The CMAC_Alert_Area shall contain at least one instance of <CMAC_cmas_geocode> element.

NOTE: The CMAC_Alert_Area may contain multiple <CMAC_cmas_geocode> elements and could additionally contain one or more instances of <CMAC_cap_geocode>, <CMAC_gnis>, <CMAC_polygon>, or <CMAC_circle>.

[WEA-C-RQMT-2545]: If one or more <CMAC_polygon> or <CMAC_circle> elements are included in any of the Alert Area segments associated with a single alert, then only those elements shall be used to define the Warning Area.

[WEA-C-RQMT-2545$_{R3A}$] If the sum of the number of paired values of points (i.e., latitude/longitude pairs) used to define all the polygon(s) plus the number of circles is greater than the allowed maximum of 100 (see WEA-C-RQMT-2550), the Federal Alert Gateway shall not forward the alert to the CMSP Gateway.

[WEA-C-RQMT-2546$_{R3A}$] If the total number of shapes is greater than the 10 shapes (e.g., polygons and circles) allowed (see WEA-C-RQMT-2551), the Federal Alert Gateway shall not forward the alert to the CMSP Gateway.

[WEA-C-RQMT-2550$_{R3M}$] The sum of the number of paired values of points (i.e., latitude/longitude pairs) used to define all the polygon in the CMAC_polygon elements plus the number of circles in the CMAC_circle elements shall be limited to a maximum of 100.

[WEA-C-RQMT-2551$_{R3A}$] The sum of CMAC_Alert_Areas shall contain a combined maximum of 10 polygons and circles.

[WEA-C-RQMT-2553] When one or more occurrences of the CMAC_Alert_Text segment are included; one occurrence shall be for English.

[WEA-C-RQMT-2557] When multiple occurrences of the CMAC_Alert_Text segment are included; each occurrence of the CMAC_Alert_Text segment shall have a different language.

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

- Table 6.8 – CMAC_Digital_Signature Segment Element Definition.
- Table 6.17 – Elements of Alert Attributes Segment for Cancel Message.

[WEA-C-RQMT-2565] The Cancel message shall discontinue the broadcast of all languages of the referenced Alert or Update message.

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

- Table 6.8 – CMAC_Digital_Signature Segment Element Definition.
- Table 6.21 – Elements of Alert Attributes Segment for RMT Message.
- Table 6.22 – Elements of Alert Info Segment for RMT Message.

[WEA-C-RQMT-2580] Each Link Test Message shall contain the mandatory message elements and associated values provided in the following table:

- Table 6.20 – Elements of Alert Attributes Segment for Link Test Message.

[WEA-C-RQMT-2590] Each Ack message shall contain the mandatory message elements and associated values provided in the following table:

- Table 6.18 – Elements of Alert Attributes Segment for Ack Message.

[WEA-C-RQMT-2600] Each Error message shall contain the mandatory message elements and associated values provided in the following table:

- Table 6.19 – Elements of Alert Attributes Segment for Error Message.

[WEA-C-RQMT-2610] Each Transmission Control – Cease message shall contain the mandatory message elements and associated values provided in Table 6.24 – *Elements of Alert Attributes Segment for Transmission Control – Cease Message*.

[WEA-C-RQMT-2620] Each Transmission Control – Resume message shall contain the mandatory message elements and associated values provided in Table 6.25 – *Elements of Alert Attributes Segment for Transmission Control – Resume Message*.

[WEA-C-RQMT-2630] All CMAC messages shall adhere to the XML Schema [Refs 33, 43, & 44] in Clause 6.4, *CMAC Message XML Definition*.

[WEA-C-RQMT-2640] The value of the CMAC_message_number shall be increased monotonically for each and every message issued by the sending gateway.

[WEA-C-RQMT-2650] Each State/Local WEA Test message shall contain the mandatory message elements and associated values equivalent to those of an Imminent Threat message (Alert, Update, or Cancel) with the exception that the CMAC_special_handling element shall be set to "State Local WEA Test".

[WEA-C-RQMT-2670] Each Public Safety message shall contain the mandatory message elements and associated values equivalent to those of an Imminent Threat message (Alert, Update, or Cancel) with the exception that the CMAC_special_handling element shall be set to "Public Safety".

6.1.2 HTTP

HTTP will be the application level protocol used by the Federal Alert Gateway and the CMSP Gateway to exchange CMAC messages. The HTTP is a request/response protocol. The HTTP methods will be limited to GET and POST. The HTTP POST method will be used by the Federal Alert Gateway (client) to send all messages in the CMAC protocol to the CMSP Gateway (server), except Ack and Error messages. Similarly, the CMSP Gateway (client) will use the HTTP POST method to send all messages in the CMAC protocol to the Federal Alert Gateway (server), except Ack and Error messages. Ack and Error messages will be sent in the CMAC protocol XML in HTTP responses to the HTTP POSTs. HTTP 200 OK response status code is used for all CMAC level responses (Ack and Error). The following describes the use of specific HTTP response status codes:

- 200 OK response status code indicates the CMAC message recipient has successfully received the CMAC message in the HTTP POST. Details of CMAC processing will be indicated in the CMAC level response (Ack or Error) in the response body.
- 400 Bad Request status code indicates that CMAC message validation has failed and the validation results prevent a valid CMAC Error response from being created.
- All other HTTP response status codes indicate a HTTP-level error.

The CMSP Gateway may retrieve the original CAP message (Alert, Update, or Cancel) that triggered a particular CMAC message (Alert, Update, or Cancel). CAP message retrieval is not performed using the CMAC protocol. The CMSP Gateway will use the HTTP GET method with the CMAC_cap_alert_uri provided in the CMAC message to retrieve the CAP message. The HTTP GET method will contain a Host request_header, whose value is the host part of the CMAC_cap_alert_uri.The HTTP GET method may also contain Connection and If_Unmodified_Since request headers.

[WEA-C-RQMT-2700] HTTP communications shall be per RFC 7230 [Ref 1] and RFC 7231 [Ref 37] except for the Request_URI specified below in WEA-C-RQMT-2750.

[WEA-C-RQMT-2710] HTTP communications carrying CMAC messages shall be to port TCP 8080.

[WEA-C-RQMT-2720] HTTP communications for CAP message retrieval shall be to port TCP 80.

[WEA-C-RQMT-2730] HTTP methods shall be limited to POST when CMAC Alert, Update, Cancel, RMT, and Link Test messages are sent over HTTP.

[WEA-C-RQMT-2740] HTTP methods shall be limited to GET when HTTP is used without the CMAC protocol.

[WEA-C-RQMT-2750] The HTTP POST method shall use "*" as the Request_URI.

[WEA-C-RQMT-2760] The HTTP GET method shall contain a Host request_header, whose value shall be the host part of the CMAC_cap_alert_uri.

[WEA-C-RQMT-2770] All CMAC Ack and Error messages shall be sent in HTTP 200 OK response messages.

[WEA-C-RQMT-2780] An HTTP 4xx Client Error or 5xx Server Error response message shall be sent to indicate a failure of the Federal Alert Gateway to retrieve the requested CAP message.

6.2 Message Structure

Each CMA Reference Point "C" protocol message consists of a <CMAC_Alert_Attributes> segment, which may contain a <CMAC_alert_info> segment. The <CMAC_alert_info> segment may contain one or more <CMAC_Alert_Area> segments and will contain one or more <CMAC_Alert_Text> segments. (See Figure 6.1 – *Reference Point "C" Document Object Model* in Clause 6.2.6, *CMAC Alert Message Document Object Model*.)

6.2.1 CMAC_Alert_Attributes Segment

The <CMAC_Alert_Attributes> segment provides basic information about the current message: its purpose, its source and its status, as well as unique identifier for the current message and a link to any other related message. A <CMAC_Alert_Attributes> segment may be used alone for message acknowledgements, cancels, or other system functions, but most <CMAC_Alert_Attributes> segments will include one <CMAC_alert_info> segment.

6.2.2 CMAC_alert_info Segment

The <CMAC_alert_info> segment describes the information for the alert. This information includes urgency, severity, and certainty for the alert message.

6.2.3 CMAC_Alert_Area Segment

The <CMAC_Alert_Area> segment describes a geographic area to which the <CMAC Alert Info> segment in which it appears applies.

6.2.4 CMAC_Alert_Text Segment

The <CMAC_Alert_Text> segment provides the text of the alert message as the short 90-character maximum length alert message text and as the long 360-character maximum length alert message text with both the short and long alert message text being in the same language for the same occurrence of the <CMAC_Alert_Text> segment. If the <CMAC_Alert_Text> segment is included, one occurrence of the <CMAC_Alert_Text> segment will be in English.

6.2.5 CMAC_Digital_Signature Segment

The <CMAC_Digital_Signature> segment describes the security information required for the creation of a XML Signature [Ref 38]. This information includes Digest Algorithms, Signature Algorithms, Key Algorithms, and X.509 Certificate Identifiers.

6.2.6 CMAC Alert Message Document Object Model

The following figure shows the CMAC Alert Message document object model:

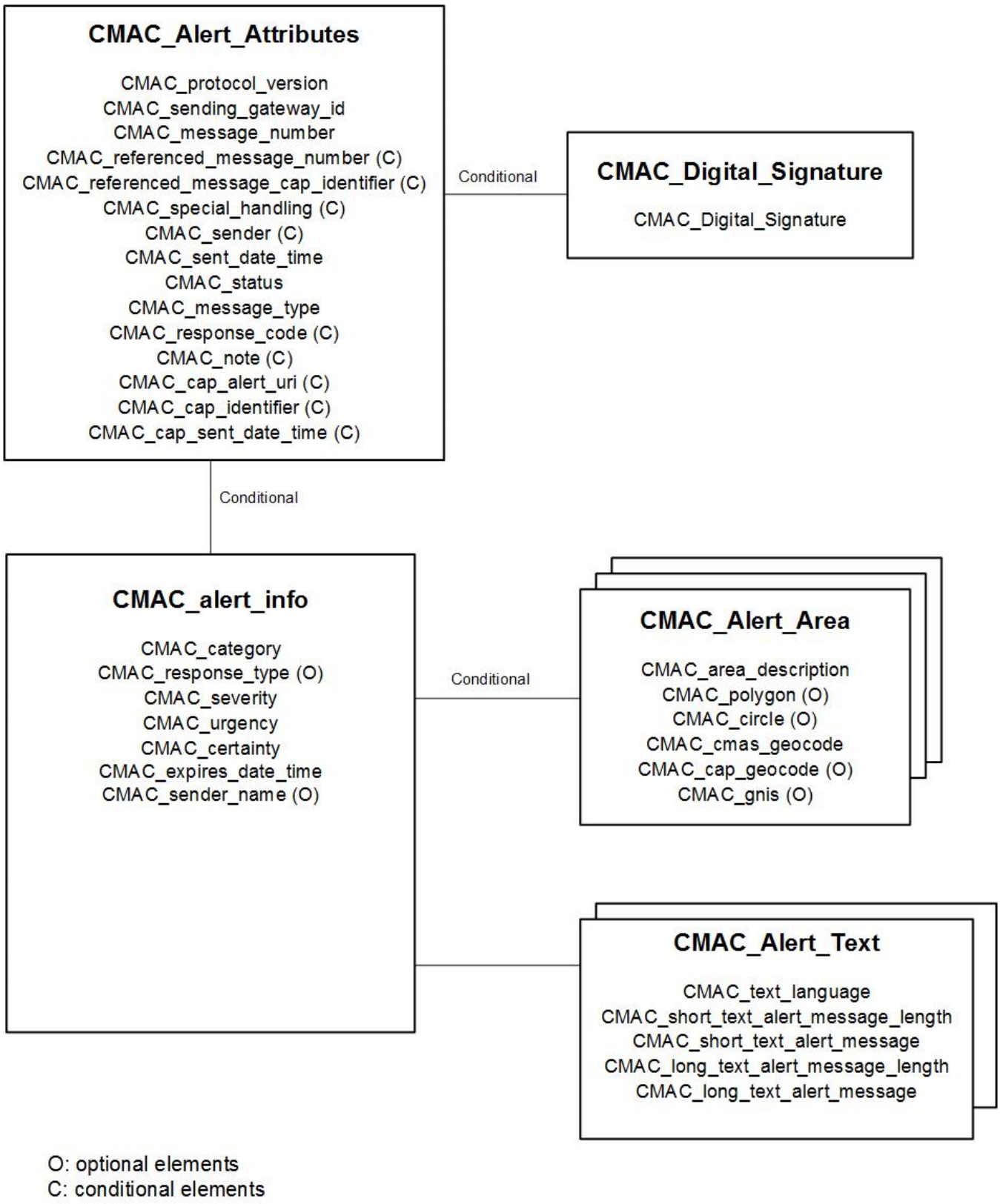


Figure 6.1 – Reference Point "C" Document Object Model

6.2.7 CMAC Message Types

The CMAC messages transmitted between the Federal Alert Gateway and the CMSP Gateway over the Reference Point "C" Interface can contain various segments. The following table defines the segments for each type of CMAC message:

Table 6.1 – CMAC Message Segments

CMAC Message	CMAC Message Segments
CMAC Alert Message	one <CMAC_Alert_Attributes> segment one <CMAC_alert_info> segment one or more <CMAC_Alert_Area> segments one or more <CMAC_Alert_Text> segments one <CMAC_Digital_Signature> segment
CMAC Update Message	one <CMAC_Alert_Attributes> segment one <CMAC_alert_info> segment one or more <CMAC_Alert_Area> segments one or more <CMAC_Alert_Text> segments one <CMAC_Digital_Signature> segment
CMAC Cancel Message	one <CMAC_Alert_Attributes> segment one <CMAC_Digital_Signature> segment
CMAC Link Test Message	one <CMAC_Alert_Attributes> segment
CMAC RMT Message	one <CMAC_Alert_Attributes> segment one <CMAC_alert_info> segment one or more <CMAC_Alert_Text> segments one <CMAC_Digital_Signature> segment
CMAC Transmission Control – Cease Message	one <CMAC_Alert_Attributes> segment
CMAC Transmission Control – Resume Message	one <CMAC_Alert_Attributes> segment
CMAC Ack Message	one <CMAC_Alert_Attributes> segment
CMAC Error Message	one <CMAC_Alert_Attributes> segment

The CMAC protocol requires a response to each message, with the exception of Ack and Error messages. Table 6.2 – *Federal Alert Gateway Initiated Messages* in Clause 6.2.7.1, *Federal Alert Gateway Initiated Messages,* and Table 6.3 – *CMSP Gateway Initiated Messages* in Clause 6.2.7.2, *CMSP Gateway Initiated Messages,* define the responses that are appropriate for messages initiated by the Federal Alert Gateway and by the CMSP Gateway, respectively. The Notes column in each table summarizes the meaning of the response.

6.2.7.1 Federal Alert Gateway Initiated Messages

The following table summarizes the message types that may be initiated by the Federal Alert Gateway and the expected responses from the CMSP Gateway.

Table 6.2 – Federal Alert Gateway Initiated Messages

CMAC Message Type	Potential CMSP Gateway Responses	Notes
Alert	Ack Error	An “Ack” indicates the CMSP Gateway has successfully received the message and will attempt to distribute the alert information. An “Error” indicates a problem with the message was identified by the CMSP Gateway and no further processing will be performed.
Update	Ack Error	An “Ack” indicates the CMSP Gateway has successfully received the message and will attempt to distribute the updated alert information. An “Error” indicates a problem with the message was identified by the CMSP Gateway and no further processing will be performed.
Cancel	Ack Error	An “Ack” indicates the CMSP Gateway has successfully received the message and will attempt to cancel distribution of the updated alert information. An “Error” indicates a problem with the message was identified by the CMSP Gateway and no further processing will be performed.
Link Test	Ack Error	An “Ack” indicates the CMSP Gateway has successfully received the Link Test message and was able to respond. An “Error” indicates that the Link Test message was received by the CMSP Gateway, but a problem was identified.
RMT	Ack Error	An “Ack” indicates the CMSP Gateway has successfully received the message and will attempt to distribute the RMT information over the next 24-hour period. An “Error” indicates a problem with the message was identified by the CMSP Gateway and no further processing will be performed.

[WEA-C-RQMT-2800] If the Federal Alert Gateway receives an invalid or malformed acknowledgement or error response message from the CMSP Gateway, the Federal Alert Gateway should log this condition and shall not reply to the CMSP Gateway with an error response.

[WEA-C-RQMT-2810] The CMSP Gateway shall respond to each message from the Federal Alert Gateway with one of the potential CMSP Gateway responses valid for that particular message type per Table 6.2 – *Federal Alert Gateway Initiated Messages*.

[WEA-C-RQMT-2820] The CMSP Gateway shall not send a message in response to an Ack or Error message from the Federal Alert Gateway.

[WEA-C-RQMT-2830] If the Federal Alert Gateway does not receive an expected response message (Ack or Error) from the CMSP Gateway within the Message Response Time, the Federal Alert Gateway shall retransmit the message additional times, per the Retransmit Number.

NOTE: The Retransmit Number and the Message Response Time are defined in Annex D, *Configurable Parameters*.

[WEA-C-RQMT-2840] The Federal Alert Gateway shall declare a CMSP Gateway failure condition and generate a system notification if a message is retransmitted Retransmit Number of times and a response is not received.

NOTE: System notification messages will be sent to the Federal Alert Gateway administrator or other appropriate personnel.

[WEA-C-RQMT-2850] The Federal Alert Gateway shall send WEA Alert, Update, and RMT messages to the CMSP Gateway with both the 90-character maximum alert message text and the 360-character maximum alert message text for each language.

6.2.7.2 CMSP Gateway Initiated Messages

The following table summarizes the message types that may be initiated by the CMSP Gateway and the expected responses from the Federal Alert Gateway.

Table 6.3 – CMSP Gateway Initiated Messages

CMAC Message Type	Potential Federal Alert Gateway Responses	Notes
Link Test	Ack Error	An "Ack" indicates the Federal Alert Gateway has successfully received the Link Test message and was able to respond. An "Error" indicates that the Link Test message was received by the Federal Alert Gateway, but a problem was identified.
Transmission Control – Cease	Ack Error	An "Ack" indicates the Federal Alert Gateway has successfully received the Transmission Control – Cease Message and will cease transmission of WEA alert messages to the CMSP Gateway. An "Error" indicates that the Transmission Control – Cease Message was received by the Federal Alert Gateway, but a problem was identified.
Transmission Control – Resume	Ack Error	An "Ack" indicates the Federal Alert Gateway has successfully received the Transmission Control – Resume Message and will resume transmission of WEA alert messages to the CMSP Gateway. An "Error" indicates that the Transmission Control – Resume Message was received by the Federal Alert Gateway, but a problem was identified.
CAP Message request (at HTTP level)	No CMAC message response	The CAP message or an error response is returned at the HTTP level (a CMAC formatted message is not used).

[WEA-C-RQMT-2900] If the CMSP Gateway receives an invalid or malformed acknowledgement or error response message from the Federal Alert Gateway, the CMSP Gateway should log this condition and shall not reply to the Federal Alert Gateway with an error response.

[WEA-C-RQMT-2910] The Federal Alert Gateway shall respond to each message from the CMSP Gateway with one of the potential Federal Alert Gateway responses valid for that particular message type per Table 6.3 – *CMSP Gateway Initiated Messages*.

[WEA-C-RQMT-2920] The Federal Alert Gateway shall not send a message in response to an Ack or Error message from the CMSP Gateway.

[WEA-C-RQMT-2930] The CMSP Gateway shall declare a Federal Alert Gateway failure condition and generate a system notification if a message is retransmitted Retransmit Number of times and a response is not received.

NOTE: System notification messages will be sent to the CMSP Gateway administrator or other appropriate personnel.

6.3 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_Alert_Text segment.
- Element definitions for the CMAC_Digital_Signature segment.
- Definition of the CMAC_cmas_geocode element.

The definitions of Mandatory, Optional, and Conditional used in the element definition tables within this clause are as follows:

Mandatory (M)	This element is required when the associated segment is included in the CMAC message.
Optional (O)	This element may be included in the segment. The entry in the CMAC Definition column defines when the element is optional and the interpretation of the missing optional element.
Conditional (C)	This element may be required in the segment depending on the contents of other elements. The entry in the CMAC Definition column for this conditional element defines the conditions and values for this conditional element.

6.3.1 CMAC_Alert_Attributes Segment Element Definition

The following table contains the definition of the elements of the CMAC_Alert_Attributes segment.

Table 6.4 – CMAC_Alert_Attributes Segment Element Definition

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_Alert_Attributes	M	(1) Surrounds CMAC Alert Attributes segment sub-elements. (2) Must include the xmlns attribute referencing the CMAC Uniform Resource Name (URN) [Ref 8] as the namespace, e.g., <cmac:CMAC_Alert_Attributes xmlns:cmac="cmac:2.0"> [sub-elements] </cmac:CMAC_Alert_Attributes> (3) In addition to the specified sub-elements, may contain a <CMAC_alert_info> block.
CMAC_protocol_version	M	The version of the CMAC protocol. Used by the CMSP Gateway and the Federal Alert Gateway to identify the protocol version of the CMAC protocol.
CMAC_sending_gateway_id	M	URI [Ref 2] or IP address of the Federal Alert Gateway or the CMSP Gateway sending the CMAC message.

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_message_number	M	A numerical value which is mapped to a 4-octet binary value to identify the message. When assigned by the Federal Alert Gateway for Alert, Update, and Cancel Messages, the value is associated with the message identified by the CAP identifier element. The Federal Alert Gateway is responsible for mapping the CAP identifier element to the CMAC_message_number element. When assigned by the Federal Alert Gateway for other CMAC Messages, the value is specified by the Federal Alert Gateway. For messages initiated by the CMSP Gateway, the value is assigned by the CMSP Gateway. NOTE: To uniquely identify a message and its source, the receiving entity uses the CMAC_message_number in conjunction with the CMAC_cap_identifier if appropriate for the message type. See Annex E for an example on identification of messages on an end to end basis.
CMAC_referenced_message_number	C	Required for Update, Cancel, Ack, and Error CMAC message types. A numerical value which is mapped to a 4-octet binary value identifying a referenced Commercial Mobile Alert Message (CMAM), assigned by the Federal Alert Gateway or CMSP Gateway. When initiated by the Federal Alert Gateway, this element may be associated with the message identified in the CAP references element. The Federal Alert Gateway is responsible for mapping the CAP references element to the CMAC_referenced_message_number element. NOTE: To uniquely identify a referenced message and its source, the receiving entity uses the CMAC_referenced_message_number in conjunction with the CMAC_referenced_message_cap_identifier.
CMAC_referenced_message_cap_ identifier	C	Required for Update and Cancel CMAC message types. Specifies the CAP identifier of the message corresponding to the referenced CMAM.
CMAC_special_handling	C	Required for Alert, Update, and Cancel CMAC message types which need special handling (i.e., National, Child Abduction, State/Local WEA Test, Public Safety) and for RMT message type. Specifies if this alert message requires special handling. Specified by the Federal Alert Gateway, and may be derived from CAP elements. Code Values: “**Presidential**”* “**Child Abduction**” “**Required Monthly Test**” “**Public Safety**” "**State Local WEA Test**" *Note that “Presidential” as a protocol value has not yet been changed to “National”. (See Clause 6.3.1.1, *Notes on CMAC_special_handling Element*)

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_sender	C	Required for Alert, Update, and Cancel CMAC message types. Identifies the originator of this alert. May be used by the CMSP for logging purposes only. Federal Alert Gateway uses the CAP sender element to populate this element.
CMAC_sent_date_time	M	The date and time the message is sent by the gateway in UTC in XML dateTime format.
CMAC_status	M	This element is used to identify actual alert messages from messages used for internal system use only. Federal Alert Gateway may use the CAP status element to populate this element. Code Values: "**Actual**" – Actionable by all targeted recipients. "**System**" – For messages that support alert network internal functions (Link Test, Transmission Control – Cease, Transmission Control – Resume, RMT, Ack, and Error).
CMAC_message_type	M	This element identifies the message type. For an Alert, Update, or Cancel message, the Federal Alert Gateway may use the CAP msgType element to populate this element. This element is also used to identify response messages and link test messages. Code Values: "**Alert**" – Initial information requiring attention by targeted recipients. "**Update**" – Updates and supersedes the earlier message(s) identified in <CMAC_referenced_message_number>. "**Cancel**" – Cancels the earlier message(s) identified in <CMAC_ referenced_ message_ number>. "**Ack**" – Acknowledges receipt and acceptance of the message(s) identified in <CMAC_referenced_message_number>. "**Error**" – Indicates rejection of the message(s) identified in <CMAC_referenced_message_number>; explanation should appear in <CMAC_note>. "**RMT**" – Indicates a required monthly test message. "**Link Test**" – Indicates a "link test" message sent by the Federal Alert Gateway or the CMSP Gateway to verify the availability of the other Gateway. "**Transmission Control – Cease**" – Indicates the far end is to cease transmission (see Clause 6.5.8, *Transmission Control – Cease Message*). "**Transmission Control – Resume**" – Indicates the far end may resume transmissions (see Clause 6.5.9, *Transmission Control – Resume Message*).
CMAC_response_code	C	Required for Error CMAC message type. This element contains the WEA Response Codes (see Clause 6.8.3.3, *Error Response Codes*) that may be returned in response to a received WEA message. Both the CMSP Gateway and the Federal Alert Gateway use this element in Error messages. Multiple instances may occur within a single <CMAC_Alert_Attributes> block. Each occurrence of the CMAC_response_code element should have a corresponding occurrence of the CMAC_note element.

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_note	C	Required for Error CMAC message type. May also be optionally used in Alert, Update, or Cancel messages from the Federal Alert Gateway to the CMSP Gateway. Multiple instances may occur within a single <CMAC_Alert_Attributes> block to correspond to multiple occurrences of CMAC_response_code. The note included in this element corresponds to the CMAC_response_code. The Federal Alert Gateway may use the CAP note element to populate this element in messages from the Federal Alert Gateway to the CMSP Gateway. The CMAC_note may be used to convey alert attribute requests. See section 6.6 *DBGF Bypass Request* for more details on alert attributes values which can be requested.
CMAC_cap_alert_uri	C	Required for Alert, Update, and Cancel CMAC message types. This element contains the uri where the CMSP may retrieve the corresponding complete CAP version of the alert from the Federal Alert Gateway. Specified by the Federal Alert Gateway.
CMAC_cap_identifier	C	Required for Alert, Update, and Cancel CMAC message types. This element contains the identifier field of the CAP message to be used by the CMSP Gateway for validating the corresponding CAP message. Specified by the Federal Alert Gateway.
CMAC_cap_sent_date_time	C	Required for Alert, Update, and Cancel CMAC message types. This element contains the sent date and time of the alert message as specified in the corresponding CAP message received at the Federal Alert Gateway. Specified by the Federal Alert Gateway. The Federal Alert Gateway uses CAP sent element to populate this element.

6.3.1.1 Notes on CMAC_special_handling Element

The CMAC_special_handling element is used to indicate that the received CMAC message requires special handling in the CMSP Gateway. For example, CMAC_special_handling may indicate a National Alert and therefore indicates that special priority handling is required.

The CMAC_special_handling element is contained within the CMAC_Alert_Attributes segment which is the required segment for all CMAC messages.

The CMAC_special_handling element is also used to identify the RMT and Child Abduction message types which have associated special handling requirements in the CMSP Gateway. For example, RMTs require special handling because of the distribution over a 24-hour period.

The CMAC_special_handling element is also used to identify the Public Safety message type that has associated special handling in the CMSP Gateway.

The CMAC_special_handling element is also used to identify the State/Local WEA Test message type that has associated special handling in the CMSP Gateway.

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

6.3.2 CMAC_alert_info Segment Element Definition

The following table contains the definition of the elements of the CMAC_alert_info segment.

Table 6.5 – CMAC_alert_info Segment Element Definition

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_alert_info	M	(1) Surrounds CMAC alert info segment sub-elements. (2) Only a single occurrence is permitted within a single <CMAC_alert_info>. (3) In addition to the specified sub-elements, may contain one or more <CMAC_Alert_Area> blocks. (4) In addition to the specified sub-elements, will contain one or more <CMAC_Alert_Text> blocks.
CMAC_category	M	Federal Alert Gateway uses the CAP category element to populate this element. Code Values used by CMSP Gateway only: "**Geo**" – Geophysical (inc. landslide). "**Met**" – Meteorological (inc. flood). "**Safety**" – General emergency and public safety. "**Security**" – Law enforcement, military, homeland and local/private security. "**Rescue**" – Rescue and recovery. "**Fire**" – Fire suppression and rescue. "**Health**" – Medical and public health. "**Env**" – Pollution and other environmental. "**Transport**" – Public and private transportation. "**Infra**" – Utility, telecommunication, other non-transport infrastructure. "**CBRNE**" – Chemical, Biological, Radiological, Nuclear or High-Yield Explosive threat or attack. "**Other**" - Other events.
CMAC_response_type	O	Federal Alert Gateway uses the CAP responseType element to populate this element. Code values: "**Shelter**" – Take shelter in place. "**Evacuate**" – Relocate. "**Prepare**" – Make preparations. "**Execute**" – Execute a pre-planned activity. "**Monitor**" – Attend to information sources. "**Avoid**" – Avoid hazard. "**Assess**" – Evaluate the information in this message. (This value should not be used in public warning applications.) "**None**" – No action recommended.
CMAC_severity	M	Federal Alert Gateway uses the CAP severity element to populate this element. Code Values: "**Extreme**" – Extraordinary threat to life or property. "**Severe**" – Significant threat to life or property.

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_urgency	M	Federal Alert Gateway uses the CAP urgency element to populate this element. Code Values: "**Immediate**" – Responsive action should be taken immediately. "**Expected**" – Responsive action should be taken soon (within next hour).
CMAC_certainty	M	Federal Alert Gateway uses the CAP certainty element to populate this element. Code Values: "**Observed**" – Determined to have occurred or to be ongoing. "**Likely**" – Likely (probability > ~50%).
CMAC_expires_date_time	M	The expiry time of the information of the alert message for use by the CMSP Gateway. The date and time are represented in UTC [dateTime] format. Maximum duration is 24 hours. Specified by the Federal Alert Gateway. For Alert and Update Messages, the value is derived from the CAP expires element.
CMAC_sender_name	O	Optional element for logging purposes at the CMSP Gateway. The human-readable name of the agency or authority issuing this alert. For Alert and Update Messages, the Federal Alert Gateway uses the CAP senderName element to populate this element. For RMT Messages, the Federal Alert Gateway uses the name or other identification of the RMT initiator at the Federal Alert Gateway to populate this element.

6.3.3 CMAC_Alert_Area Segment Element Definition

The following table contains the definition of the elements of the CMAC_Alert_Area segment.

Table 6.6 – CMAC_Alert_Area Segment Element Definition

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_Alert_Area	M	(1) Surrounds CMAC alert area segment sub-elements. (2) Multiple occurrences permitted, in which case the combined Alert Area is the geometric union of all <CMAC_Alert_Area> blocks. (3) The CMAC_Alert_Area segment may contain one or multiple instances of <CMAC_cap_geocode>, <CMAC_gnis>, <CMAC_polygon> or <CMAC_circle>, and will contain at least one instance of <CMAC_cmas_geocode>. (4) If <CMAC_polygon> or <CMAC_circle> elements are included, only those elements determine the Alert Area. The CMSP targeting policies are beyond the scope of this Standard.

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_area_description	M	The text describing the affected area of the alert message for use by the CMSP for logging purposes only. Federal Alert Gateway uses the CAP areaDesc element to populate this element.
CMAC_polygon	O	Optional element. If included, the CMSP shall use this element to perform geo-targeting. The paired values of points defining a polygon that delineates the affected area of the alert message. Federal Alert Gateway uses the CAP polygon element to populate this element. The maximum is specified in [WEA-C-RQMT-2550] and [WEA-C-RQMT-2551] previously.
CMAC_circle	O	Optional element. If included, the CMSP shall use this element to perform geo-targeting. The paired values of a point and radius delineating the affected area of the alert message. Federal Alert Gateway uses the CAP circle element to populate this element. The maximum is specified in [WEA-C-RQMT-2550] and [WEA-C-RQMT-2551] previously.
CMAC_cmas_geocode	M	The WEA-defined geographic code delineating the affected area of the alert message. This is an extension to the FIPS code (see Clause 6.3.6, *Definition of CMAC_cmas_geocode Element*). Federal Alert Gateway uses the CAP geocode, polygon, circle, and/or sender elements to derive this element.
CMAC_cap_geocode	O	Contains the value(s) of geocode in the CAP message. The CMAC_cap_geocode is only present if the Federal Alert Gateway receives a CAP message which has the optional CAP geocode element present. (See Clause 6.3.7, *Definition of CMAC_cap_geocode*.) The Federal Alert Gateway uses the CAP geocode element to populate this element. Multiple instances of CMAC_cap_geocode may exist.
CMAC_gnis	O	Optional element. This value is the geographic code delineating the affected area of the alert message using the U.S.G.S. Geographic Names Information System (GNIS) code. Derived by the Federal Alert Gateway.

6.3.4 CMAC_Alert_Text Segment Element Definition

The following table contains the definition of the elements of the CMAC_Alert_Text segment.

Table 6.7 – CMAC_Alert_Text Segment Element Definition

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_Alert_Text	M	(1) Surrounds CMAC text area segment sub-elements. (2) Multiple occurrences permitted with each occurrence providing alert text in a different language. (3) If CMAC_Alert_Text segment is present; one occurrence of the CMAC_Alert_Text segment must be for English.
CMAC_text_language	M	Specifies the language of the text in the CMAC_short_text_alert_message and in the CMAC_long_text_alert_message, for use by the mobile device. Code Values: "**English**" "**Spanish**"
CMAC_short_text_alert_message_length	M	The length, in characters, of the text in the CMAC_short_text_alert_message. Maximum value: 90. Specified by the Federal Alert Gateway.
CMAC_short_text_alert_message	M	The text of the alert message for use by the mobile device. This field contains up to 90 characters. Specified by the Federal Alert Gateway, which may be derived or obtained via CAP elements. NOTE: If the Alert Originators include Uniform Resource Locators (URLs) with characters that are not supported by the GSM 7-bit alphabet, these unsupported characters will be removed or replaced which could result in the URLs in the broadcast alert messages not being valid. To avoid this situation, the Alert Originators should not use the characters "{", "}", "|", "\", "^", "~", "[", "]", and "`" in their embedded URLs. See IETF RFC 1738 [Ref 47] regarding unsafe characters.
CMAC_long_text_alert_message_length	M	The length, in characters, of the text in the CMAC_long_text_alert_message. Maximum value: 360. Specified by the Federal Alert Gateway.
CMAC_long_text_alert_message	M	The text of the alert message for use by the mobile device. This field contains up to 360 characters. Specified by the Federal Alert Gateway, which may be derived or obtained via CAP elements. NOTE: If the Alert Originators include URLs with characters that are not supported by the GSM 7-bit alphabet, these unsupported characters will be removed or replaced which could result in the URLs in the broadcast alert messages not being valid. To avoid this situation, the Alert Originators should not use the characters "{", "}", "|", "\", "^", "~", "[", "]", and "`" in their embedded URLs. See IETF RFC 1738 [Ref 47] regarding unsafe characters.

6.3.5 CMAC_Digital_Signature Segment Element Definition

The following table contains the definition of the elements of the CMAC_Digital_Signature segment.

Table 6.8 – CMAC_Digital_Signature Segment Element Definition

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_Digital_Signature	M	XML Signature elements and syntax are defined by the World Wide Web Consortium (W3C) recommendations [Ref 38]. CMAC_Digital_Signature is mandatory for the 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>.

6.3.6 Definition of CMAC_cmas_geocode Element

The CMAC_cmas_geocode is five characters where the first two characters or digits identify the state or region and the last three digits identify the specific counties, regions, or equivalent entities. The CMAC_cmas_geocode is as follows:

1. The CMAC_cmas_geocode indication for a specific county will be as specified by INCITS 31-2009, *Codes for the Identification of Counties and Equivalent Areas of the United States, Puerto Rico, and the Insular Areas* [Ref 6].
2. The CMAC_cmas_geocode indication for an entire state will be the two digit FIPS State Numeric Code as specified by INCITS 31-2009, *Codes for the Identification of Counties and Equivalent Areas of the United States, Puerto Rico, and the Insular Areas* [Ref 5], followed by three zeroes (000).
3. The CMAC_cmas_geocode indication for an entire United States including all states, the District of Columbia, possessions, and associated areas will be all zeros (00000).
4. If the Federal Alert Gateway receives geo-targeting information in a different format than that defined in this Standard, the Federal Alert gateway will convert the geo-targeting information into the CMAC_cmas_geocode format.
5. The CMAC_cmas_geocode will not include the CAP area altitude or ceiling elements.

6.3.7 Definition of CMAC_cap_geocode Element

A CMSP is not required to use the CMAC_cap_geocode element to perform geo-targeting. It is an optional element which may be used by the CMSP for geo-targeting purposes.

CMAC_cap_geocode is an optional element, and is only passed on the Reference Point “C” interface if the CAP Geocode field is populated. The Federal Alert Gateway passes the value of the CAP Geocode in this element.

The contents of the CMAC_cap_geocode element are defined in the CAP protocol [Ref 4]. The contents of the CMAC_cap_geocode element may be any geographically-based code to describe message target area, and contains a “valueName” which is a user-assigned string designating the domain of the code, and the content of “value” is a string (which may represent a number) denoting the value itself (e.g., valueName ="SAME" and value="006113"). Values of “valueName” that are acronyms should be represented in all capital letters without periods (e.g., SAME).

If the CMAC_cap_geocode has a valueName of “SAME”, the format is defined in the 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) [Ref 11].[13] CMAC_cap_geocode contains six characters which are identified as “PSSCCC”. The first character, P, allows for subdividing the area defined by the "CCC" into smaller parts in the case of a very large or uniquely shaped area, or because of widely varying elevation, climate, population, or geographic features. The two SS characters identify the state or region. The source of state and territory codes to be used in this field is the INCITS 38-2009, *Codes for the Identification of the States and Equivalent Areas within the United States, Puerto Rico, and the Insular Areas* [Ref 5]. The last three CCC characters identify the specific counties, regions, or equivalent entities. The source of county, region, or equivalent entity codes to be used in this field is the INCITS 31-2009, *Codes for the Identification of Counties and Equivalent Areas of the United States, Puerto Rico, and the Insular Areas* [Ref 6].

6.4 CMAC Message XML Schema Definition

The following is version 2.0 of the XML Schema [Refs 33, 43, & 44] definition for the CMAC message transmitted across the Reference Point “C” Interface:

NOTE: “Presidential” as a protocol value has not yet been changed to “National”.

```
<?xml version = "1.0" encoding = "UTF-8"?>
<schema xmlns = "http://www.w3.org/2001/XMLSchema"
    targetNamespace = "cmac:2.0"
    xmlns:cmac = "cmac:2.0"
    xmlns:xs = "http://www.w3.org/2001/XMLSchema"
    elementFormDefault = "qualified"
    attributeFormDefault = "unqualified">
    <element name = "CMAC_Alert_Attributes">
    <annotation>
       <documentation>CMAC Alert Message (version 2.0)</documentation>
    </annotation>
    <complexType>
        <sequence>
            <element name = "CMAC_protocol_version" type = "string"/>
            <element name = "CMAC_sending_gateway_id" type = "anyURI"/>
            <element name = "CMAC_message_number">
                 <simpleType>
                     <restriction base = "hexBinary">
                         <length value = "4" fixed = "true"/>
                     </restriction>
                 </simpleType>
            </element>
            <element name = "CMAC_referenced_message_number" minOccurs="0">
                 <simpleType>
                     <restriction base = "hexBinary">
                         <length value = "4" fixed = "true"/>
                     </restriction>
                 </simpleType>
            </element>
            <element name = "CMAC_referenced_message_cap_identifier" type = "string"
                minOccurs = "0"/>
            <element name = "CMAC_special_handling" minOccurs = "0">
               <simpleType>
                  <restriction base = "string">
                     <enumeration value = "Presidential"/>
                     <enumeration value = "Child Abduction"/>
                     <enumeration value = "Required Monthly Test"/>
                     <enumeration value = "Public Safety"/>
                     <enumeration value = "State Local WEA Test"/>
                  </restriction>
               </simpleType>
            </element>
            <element name = "CMAC_sender" type = "string" minOccurs = "0"/>
```

[13] Available at: < http://www.nws.noaa.gov/directives/sym/pd01017012curr.pdf >.

```
<element name = "CMAC_sent_date_time" type = "dateTime"/>
<element name = "CMAC_status">
   <simpleType>
      <restriction base = "string">
         <enumeration value = "Actual"/>
         <enumeration value = "System"/>
      </restriction>
   </simpleType>
</element>
<element name = "CMAC_message_type">
   <simpleType>
      <restriction base = "string">
         <enumeration value = "Alert"/>
         <enumeration value = "Update"/>
         <enumeration value = "Cancel"/>
         <enumeration value = "Ack"/>
         <enumeration value = "Error"/>
         <enumeration value = "RMT"/>
         <enumeration value = "Link Test"/>
         <enumeration value = "Transmission Control - Cease"/>
         <enumeration value = "Transmission Control - Resume"/>
      </restriction>
   </simpleType>
</element>
<element name = "CMAC_response_code" type = "string" minOccurs = "0"
   maxOccurs = "unbounded"/>
<element name = "CMAC_note" type = "string" minOccurs = "0"
   maxOccurs = "unbounded"/>
<element name = "CMAC_cap_alert_uri" type = "anyURI" minOccurs = "0"/>
<element name = "CMAC_cap_identifier" type = "string" minOccurs = "0"/>
<element name = "CMAC_cap_sent_date_time" type = "dateTime" minOccurs = "0"/>
<element name = "CMAC_alert_info" minOccurs = "0">
   <complexType>
      <sequence>
         <element name = "CMAC_category">
            <simpleType>
               <restriction base = "string">
                  <enumeration value = "Geo"/>
                  <enumeration value = "Met"/>
                  <enumeration value = "Safety"/>
                  <enumeration value = "Security"/>
                  <enumeration value = "Rescue"/>
                  <enumeration value = "Fire"/>
                  <enumeration value = "Health"/>
                  <enumeration value = "Env"/>
                  <enumeration value = "Transport"/>
                  <enumeration value = "Infra"/>
                  <enumeration value = "CBRNE"/>
                  <enumeration value = "Other"/>
               </restriction>
            </simpleType>
         </element>
         <element name = "CMAC_response_type" minOccurs = "0">
            <simpleType>
               <restriction base = "string">
                  <enumeration value = "Shelter"/>
                  <enumeration value = "Evacuate"/>
                  <enumeration value = "Prepare"/>
                  <enumeration value = "Execute"/>
                  <enumeration value = "Monitor"/>
                  <enumeration value = "Avoid"/>
                  <enumeration value = "Assess"/>
                  <enumeration value = "None"/>
               </restriction>
            </simpleType>
         </element>
```

```
<element name = "CMAC_severity">
   <simpleType>
      <restriction base = "string">
         <enumeration value = "Extreme"/>
         <enumeration value = "Severe"/>
         </restriction>
      </simpleType>
   </element>
   <element name = "CMAC_urgency">
      <simpleType>
         <restriction base = "string">
            <enumeration value = "Immediate"/>
            <enumeration value = "Expected"/>
          </restriction>
       </simpleType>
    </element>
    <element name = "CMAC_certainty">
       <simpleType>
          <restriction base = "string">
             <enumeration value = "Observed"/>
             <enumeration value = "Likely"/>
          </restriction>
       </simpleType>
    </element>
    <element name = "CMAC_expires_date_time" type = "dateTime"/>
    <element name = "CMAC_sender_name" type = "string"
       minOccurs = "0"/>
       <element name = "CMAC_Alert_Area" minOccurs = "0"
          maxOccurs = "unbounded">
          <complexType>
             <sequence>
                <element name = "CMAC_area_description"
                   type = "string"/>
                <element name = "CMAC_polygon" type = "string"
                   minOccurs = "0" maxOccurs = "unbounded"/>
                <element name = "CMAC_circle" type = "string"
                   minOccurs = "0" maxOccurs = "unbounded"/>
                <element name = "CMAC_cmas_geocode" type= "string"
                   maxOccurs = "unbounded"/>
                <element name = "CMAC_cap_geocode"
                     minOccurs= "0" maxOccurs= "unbounded">
                   <complexType>
                     <sequence>
                        <element ref = "cmac:valueName"/>
                        <element ref = "cmac:value"/>
                     </sequence>
                  </complexType>
                </element>
                <element name = "CMAC_gnis" type = "string"
                   minOccurs = "0" maxOccurs = "unbounded"/>
             </sequence>
          </complexType>
       </element>
       <element name = "CMAC_Alert_Text"
          maxOccurs = "unbounded">
          <complexType>
             <sequence>
               <element name = "CMAC_text_language">
                  <simpleType>
                    <restriction base = "string">
                      <enumeration value = "English"/>
                      <enumeration value = "Spanish"/>
                    </restriction>
                  </simpleType>
                </element>
                <element name =
```

```
                                    "CMAC_short_text_alert_message_length"
                                      type = "integer"/>
                                    <element name =
                                      "CMAC_short_text_alert_message"
                                        type = "string"/>
                                    <element name =
                                      "CMAC_long_text_alert_message_length"
                                        type = "integer"/>
                                    <element name =
                                      "CMAC_long_text_alert_message"
                                        type = "string"/>
                                  </sequence>
                                </complexType>
                              </element>
                            </sequence>
                          </complexType>
                        </element>
                        <element name="CMAC_Digital_Signature" minOccurs = "0">
                          <complexType>
                            <sequence>
                              <any namespace="http://www.w3.org/2000/09/xmldsig#"
                              processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
                            </sequence>
                          </complexType>
                        </element>
                      </sequence>
                    </complexType>
                  </element>
    <element name = "valueName" type = "string"/>
    <element name = "value" type = "string"/>
</schema>
```

6.5 CMAC Message Types & Example XML

This clause defines the XML structure and XML contents for the following types of CMAC messages including example messages for each message:

- Alert Message
- Update Message
- Cancel Message
- Ack Message
- Error Message
- Link Test
- RMT Message
- Transmission Control – Cease Message
- Transmission Control – Resume Message

The definitions of Mandatory, Optional, and Conditional used in the element definition tables within this clause are as follows:

Mandatory (M)	This element is required when the associated segment is included in the CMAC message.
Optional (O)	This element may be included in the segment. The entry in the Value column defines when the element is optional and the interpretation of the missing optional element.
Conditional (C)	This element may be required in the segment depending on the contents of other elements. The entry in the Value column for this conditional element defines the conditions and values for this conditional element.

6.5.1 Alert Message

A WEA Alert Message initiated by the Federal Alert Gateway will consist of a CMAC message containing one CMAC_Alert_Attributes segment, one CMAC_alert_info segment, one or more CMAC_Alert_Area segments, one or more CMAC_Alert_Text segments, and one CMAC_Digital_Signature segment. The CMAC_status is set to "Actual" and the CMAC_message_type is set to "Alert" to indicate the Alert Message.

The following table summarizes the required CMAC elements of the CMAC_Alert_Attributes segment for an Alert Message (see Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition,* Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition,* for the element encoding formats):

Table 6.9 – Elements of Alert Attributes Segment for Alert Message

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_protocol_version	M	Per Table 6.4 – CMAC_Alert_Attributes Segment Element Definition of Clause 6.3.1, CMAC_Alert_Attributes Segment Element Definition.
CMAC_sending_gateway_id	M	Federal Alert Gateway identifier which initiated the CMAC message.
CMAC_message_number	M	Message number for this CMAM assigned by the Federal Alert Gateway. NOTE: To uniquely identify a message, the CMSP Gateway uses the CMAC_message_number in conjunction with the CMAC_cap_identifier.
CMAC_special_handling	C	Conditional element included per Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition* of Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition*. For a Child Abduction Emergency, value of "Child Abduction". For a National Alert message, value of "Presidential".* For a Public Safety message, value of "Public Safety". For a WEA Test message, value of "State Local WEA Test". *Note that "Presidential" as a protocol value has not yet been changed to "National".
CMAC_sender	M	Identifies the originator of the alert per Table 6.4 – CMAC_Alert_Attributes Segment Element Definition of Clause 6.3.1, CMAC_Alert_Attributes Segment Element Definition.
CMAC_sent_date_time	M	Date and time in UTC the Alert Message is sent by the Federal Alert Gateway in XML dateTime format.
CMAC_status	M	Value of "Actual".
CMAC_message_type	M	Value of "Alert".
CMAC_cap_alert_uri	M	Specifies the uri where the CMSP Gateway may retrieve the corresponding complete CAP version of the Alert Message per Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition* of Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition*.
CMAC_cap_identifier	M	Specifies the identifier value in the corresponding CAP message.
CMAC_cap_sent_date_time	M	Specifies the date and time the corresponding CAP message was sent.

The following table summarizes the required CMAC elements of the CMAC_alert_info segment for an Alert Message (see Clause 6.3.2, *CMAC_alert_info Segment Element Definition,* Table 6.5 – *CMAC_alert_info Segment Element Definition,* for the element encoding formats):

Table 6.10 – Elements of Alert Info Segment for Alert Message

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_category	M	Per Table 6.5 – *CMAC_alert_info Segment Element Definition* of Clause 6.3.2, *CMAC_alert_info Segment Element Definition*.
CMAC_response_type	O	Per Table 6.5 – *CMAC_alert_info Segment Element Definition* of Clause 6.3.2, *CMAC_alert_info Segment Element Definition*.
CMAC_severity	M	Per Table 6.5 – *CMAC_alert_info Segment Element Definition* of Clause 6.3.2, *CMAC_alert_info Segment Element Definition*.
CMAC_urgency	M	Per Table 6.5 – *CMAC_alert_info Segment Element Definition* of Clause 6.3.2, *CMAC_alert_info Segment Element Definition*.
CMAC_certainty	M	Per Table 6.5 – *CMAC_alert_info Segment Element Definition* of Clause 6.3.2, *CMAC_alert_info Segment Element Definition*.
CMAC_expires_date_time	M	Per Table 6.5 – *CMAC_alert_info Segment Element Definition* of Clause 6.3.2, *CMAC_alert_info Segment Element Definition*.
CMAC_sender_name	O	Optional element which may be included per Table 6.5 – *CMAC_alert_info Segment Element Definition* of Clause 6.3.2, *CMAC_alert_info Segment Element Definition.*

The following table summarizes the required CMAC elements of the CMAC_Alert_Area segment for an Alert Message (see Clause 6.3.3, *CMAC_Alert_Area Segment Element Definition,* Table 6.6 – *CMAC_Alert_Area Segment Element Definition,* for the element encoding formats):

Table 6.11 – Elements of Alert Area Segment for Alert Message

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_area_description	M	Per Table 6.6 – CMAC_Alert_Area Segment Element Definition of Clause 6.3.3, CMAC_Alert_Area Segment Element Definition.
CMAC_polygon	O	Per Table 6.6 – CMAC_Alert_Area Segment Element Definition of Clause 6.3.3, CMAC_Alert_Area Segment Element Definition.
CMAC_circle	O	Per Table 6.6 – CMAC_Alert_Area Segment Element Definition of Clause 6.3.3, CMAC_Alert_Area Segment Element Definition.
CMAC_cmas_geocode	M	Geocode indicating the updated alert area. (See Clause 6.3.6, *Definition of CMAC_cmas_geocode Element*).
CMAC_cap_geocode	O	Per Table 6.6 – CMAC_Alert_Area Segment Element Definition of Clause 6.3.3, CMAC_Alert_Area Segment Element Definition.
CMAC_gnis	O	Per Table 6.6 – CMAC_Alert_Area Segment Element Definition of Clause 6.3.3, CMAC_Alert_Area Segment Element Definition.

The following table summarizes the required CMAC elements of the CMAC_Alert_Text segment for an Alert Message (see Clause 6.3.4, *CMAC_Alert_Text Segment Element Definition*, Table 6.7 – *CMAC_Alert_Text Segment Element Definition,* for the element encoding formats):

Table 6.12 – Elements of Alert Text Segment for Alert Message

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_text_language	M	Per Table 6.7 – *CMAC_Alert_Text Segment Element Definition,* of Clause 6.3.4, *CMAC_Alert_Text Segment Element Definition*.
CMAC_short_text_alert_message_length	M	Length in characters of the short text message per Table Table 6.7 – CMAC_Alert_Text Segment Element Definition–, of Clause 6.3.4, *CMAC_Alert_Text Segment Element Definition*.
CMAC_short_text_alert_message	M	90-character maximum short text message per Table 6.7 – CMAC_Alert_Text Segment Element Definition, of Clause 6.3.4, *CMAC_Alert_Text Segment Element Definition*.
CMAC_long_text_alert_message_length	M	Length in characters of the LONG text message per Table 6.7 – CMAC_Alert_Text Segment Element Definition, of Clause 6.3.4, *CMAC_Alert_Text Segment Element Definition*.
CMAC_long_text_alert_message	M	360-character maximum long text message per Table 6.7 – CMAC_Alert_Text Segment Element Definition, of Clause 6.3.4, *CMAC_Alert_Text Segment Element Definition*.

Example Non-National Imminent Threat WEA Alert Message

As an example of a non-National Imminent Threat WEA Alert Message, consider the following WEA Reference Point “C” Interface Alert Message that would be constructed by Federal Alert Gateway based upon the alert message received from the National Weather Service (NWS) via the Federal Alert Gateway on the Reference Point “B” interface:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<CMAC_Alert_Attributes xmlns = "cmac:2.0">
   <CMAC_protocol_version>2.0</CMAC_protocol_version>
   <CMAC_sending_gateway_id>http://wea_alert_gateway.gov</CMAC_sending_gateway_id>
   <CMAC_message_number>00001056</CMAC_message_number>
   <CMAC_sender>w-nws.webmaster@noaa.gov</CMAC_sender>
   <CMAC_sent_date_time>2017-06-03T01:32:50Z</CMAC_sent_date_time>
   <CMAC_status>Actual</CMAC_status>
   <CMAC_message_type>Alert</CMAC_message_type>
   <CMAC_cap_alert_uri>http://wea_alert_gateway.gov/CMAM1056</CMAC_cap_alert_uri>
   <CMAC_cap_identifier>NOAA-NWS-ALERTS Texas 2017-06-01:32:50Z</CMAC_cap_identifier>
   <CMAC_cap_sent_date_time>2017-06-03T01:32:50Z</CMAC_cap_sent_date_time>
   <CMAC_alert_info>
      <CMAC_category>Met</CMAC_category>
      <CMAC_severity>Severe</CMAC_severity>
      <CMAC_urgency>Expected</CMAC_urgency>
      <CMAC_certainty>Likely</CMAC_certainty>
      <CMAC_expires_date_time>2017-06-03T02:30:00Z</CMAC_expires_date_time>
      <CMAC_sender_name>NWS San Angelo TX</CMAC_sender_name>
      <CMAC_Alert_Area>
            <CMAC_area_description>Fisher; Jones; Taylor;
Callahan</CMAC_area_description>
            <CMAC_polygon>32.21,-99.62 32.27,-100.15 32.52,-100.15 32.52,-100.16 32.72,-
100.17 32.85,-99.61 32.21,-99.62</CMAC_polygon>
            <CMAC_cmas_geocode>48151</CMAC_cmas_geocode>
            <CMAC_cmas_geocode>48253</CMAC_cmas_geocode>
            <CMAC_cmas_geocode>48441</CMAC_cmas_geocode>
```

```
            <CMAC_cmas_geocode>48059</CMAC_cmas_geocode>
            <CMAC_cap_geocode>
                <valueName>SAME</valueName>
                <value>048151</value>
            </CMAC_cap_geocode>
            <CMAC_cap_geocode>
                <valueName>SAME</valueName>
                <value>048253</value>
            </CMAC_cap_geocode>
            <CMAC_cap_geocode>
                <valueName>SAME</valueName>
                <value>048441</value>
            </CMAC_cap_geocode>
            <CMAC_cap_geocode>
                <valueName>SAME</valueName>
                <value>048059</value>
            </CMAC_cap_geocode>
      </CMAC_Alert_Area>
      <CMAC_Alert_Text>
          <CMAC_text_language>English</CMAC_text_language>
          <CMAC_short_text_alert_message_length>52
            </CMAC_short_text_alert_message_length>
          <CMAC_short_text_alert_message>Flash Flood Warning this area until 9:30 PM CDT.
NWS</CMAC_short_text_alert_message>
          <CMAC_long_text_alert_message_length>187
            </CMAC_long_text_alert_message_length>
          <CMAC_long_text_alert_message>Flash Flood Warning this area until 9:30 PM CDT.
Avoid flood areas. Do not drive on flooded roads. Check local radio and television
stations for more information. National Weather Service</CMAC_long_text_alert_message>
        </CMAC_Alert_Text>
        <CMAC_Alert_Text>
          <CMAC_text_language>Spanish</CMAC_text_language>
          <CMAC_short_text_alert_message_length>68
            </CMAC_short_text_alert_message_length>
          <CMAC_short_text_alert_message>Aviso de inundación de destello esta área hasta
las 9:30 PM CDT. NWS</CMAC_short_text_alert_message>
          <CMAC_long_text_alert_message_length>247
            </CMAC_long_text_alert_message_length>
          <CMAC_long_text_alert_message>Advertencia de inundación de emergencia esta área
hasta las 9:30 PM CDT. Evite las zonas de inundación. No conduzca en carreteras
inundadas. Consulte las emisoras de radio y televisión locales para obtener más
información. National Weather Service</CMAC_long_text_alert_message>
      </CMAC_Alert_Text>
   </CMAC_alert_info>
</CMAC_Alert_Attributes>
```

The XML Signature component has been omitted from the above example WEA message. The XML Signature would be created in accordance with [Ref 38].

The short 90-character maximum English WEA Alert Message would be broadcast as:

Flash Flood Warning this area until 9:30 PM CDT.

The long 360-character maximum English WEA Alert Message would be broadcast as:

Flash Flood Warning this area until 9:30 PM CDT. Avoid flood areas. Do not drive on flooded roads. Check local radio and television stations for more information. National Weather Service

The short 90-character maximum Spanish WEA Alert Message would be broadcast as:

Aviso de inundación de destello esta área hasta las 9:30 PM CDT. NWS

The 360-character maximum Spanish WEA Alert Message would be broadcast as:

> Advertencia de inundación de emergencia esta área hasta las 9:30 PM CDT. Evite las zonas de inundación. No conduzca en carreteras inundadas. Consulte las emisoras de radio y televisión locales para obtener más información. National Weather Service

Example National Alert Message

The following is an example of a Federal Alert Gateway Initiated National Alert Message:

NOTE: “Presidential” as a protocol value has not yet been changed to “National”.

```
<?xml version = "1.0" encoding = "UTF-8"?>
<CMAC_Alert_Attributes xmlns = "cmac:2.0">
   <CMAC_protocol_version>2.0</CMAC_protocol_version>
   <CMAC_sending_gateway_id>http://wea_alert_gateway.gov</CMAC_sending_gateway_id>
   <CMAC_message_number>00001056</CMAC_message_number>
   <CMAC_special_handling>Presidential</CMAC_special_handling>
   <CMAC_sender>wh.webmaster@whitehouse.gov</CMAC_sender>
   <CMAC_sent_date_time>2017-07-09T11:35:00Z</CMAC_sent_date_time>
   <CMAC_status>Actual</CMAC_status>
   <CMAC_message_type>Alert</CMAC_message_type>
   <CMAC_cap_alert_uri>http://wea_alert_gateway.gov/CMAM1056</CMAC_cap_alert_uri>
   <CMAC_cap_identifier>White House Alert 2017-07-09T18:22:17-7:00</CMAC_cap_identifier>
   <CMAC_cap_sent_date_time>2017-07-09T18:22:17-07:00</CMAC_cap_sent_date_time>
   <CMAC_alert_info>
      <CMAC_category>Security</CMAC_category>
      <CMAC_severity>Extreme</CMAC_severity>
      <CMAC_urgency>Expected</CMAC_urgency>
      <CMAC_certainty>Likely</CMAC_certainty>
      <CMAC_expires_date_time>2017-07-09T23:15:00Z</CMAC_expires_date_time>
      <CMAC_Alert_Area>
         <CMAC_area_description>entire United States</CMAC_area_description>
         <CMAC_cmas_geocode>00000</CMAC_cmas_geocode>
      </CMAC_Alert_Area>
      <CMAC_Alert_Text>
          <CMAC_text_language>English</CMAC_text_language>
          <CMAC_short_text_alert_message_length>53
            </CMAC_short_text_alert_message_length>
          <CMAC_short_text_alert_message>President has issued an alert in this area until
11:15PM PDT Monitor Radio or TV</CMAC_short_text_alert_message>
          <CMAC_long_text_alert_message_length>129
            </CMAC_long_text_alert_message_length>
          <CMAC_long_text_alert_message>The US President has issued an alert in this area
until 11:15PM PDT Monitor local Radio or TV stations for additional
information</CMAC_long_text_alert_message>
        </CMAC_Alert_Text>
        <CMAC_Alert_Text>
          <CMAC_text_language>Spanish</CMAC_text_language>
          <CMAC_short_text_alert_message_length>90
            </CMAC_short_text_alert_message_length>
          <CMAC_short_text_alert_message>Presidente ha emitido una alerta en esta área
hasta las 11:15 PM PDT Monitor de radio o TV</CMAC_short_text_alert_message>
          <CMAC_long_text_alert_message_length>175
            </CMAC_long_text_alert_message_length>
          <CMAC_long_text_alert_message>El Presidente de los Estados Unidos ha emitido
una alerta en esta área hasta las 11:15 PM PDT Monitoree las estaciones locales de radio
o TV para obtener información adicional</CMAC_long_text_alert_message>
      </CMAC_Alert_Text>
   </CMAC_alert_info>
</CMAC_Alert_Attributes>
```

The XML Signature component has been omitted from the above example WEA message. The XML Signature would be created in accordance with [Ref 38].

The short 90-character maximum English WEA National Alert Message would be broadcast as:

President has issued an alert in this area until 11:15 PM PDT Monitor Radio or TV

The long 360-character maximum English WEA National Alert Message would be broadcast as:

The US President has issued an alert in this area until 11:15 PM PDT Monitor local Radio or TV stations for additional information

The short 90-character maximum Spanish WEA National Alert Message would be broadcast as:

Presidente ha emitido una alerta en esta área hasta las 11:15 PM PDT Monitor de radio o TV

The long 360-character maximum Spanish WEA National Alert Message would be broadcast as:

El Presidente de los Estados Unidos ha emitido una alerta en esta área hasta las 11:15 PM PDT Monitoree las estaciones locales de radio o TV para obtener información adicional

6.5.2 Update Message

A WEA Update Message will consist of a CMAC message containing one CMAC_Alert_Attributes segment, one CMAC_alert_info segment, one or more CMAC_Alert_Area segments, one or more CMAC_Alert_Text segments, and one CMAC_Digital_Signature segment. The CMAC_status is set to “Actual” and the CMAC_message_type is set to “Update” to indicate the Update Message, with the <CMAC_referenced_message_number> containing the message number for the message to be updated.

The following table summarizes the required CMAC elements of the CMAC_Alert_Attributes segment for an Update Message (see Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition,* Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition,* for the element encoding formats):

Table 6.13 – Elements of Alert Attributes Segment for Update Message

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_protocol_version	M	Per Table 6.4 – CMAC_Alert_Attributes Segment Element Definition of Clause 6.3.1, CMAC_Alert_Attributes Segment Element Definition.
CMAC_sending_gateway_id	M	Federal Alert Gateway identifier which initiated the CMAC message.
CMAC_message_number	M	Message number for this CMAM assigned by the Federal Alert Gateway. NOTE: To uniquely identify a message, the CMSP Gateway uses the CMAC_message_number in conjunction with the CMAC_cap_identifier.
CMAC_referenced_message_number	M	Message number of the corresponding message to be updated.
CMAC_referenced_message_cap_ identifier	M	Identifier of the corresponding cap message of the corresponding alert message to be updated.

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_special_handling	C	Conditional element included per Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition,* of Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition*. For a Child Abduction Emergency, value of “Child Abduction”. For a National Alert message, value of “Presidential”.* For a Public Safety message, value of “Public Safety”. For a WEA Test message, value of "State Local WEA Test". *Note that “Presidential” as a protocol value has not yet been changed to “National”.
CMAC_sender	M	Identifies the originator of the alert update per Table 6.4 – CMAC_Alert_Attributes Segment Element Definition of Clause 6.3.1, CMAC_Alert_Attributes Segment Element Definition.
CMAC_sent_date_time	M	Date and time in UTC. The Update Message is sent by the Federal Alert Gateway in XML dateTime format.
CMAC_status	M	Value of “Actual”.
CMAC_message_type	M	Value of “Update”.
CMAC_cap_alert_uri	M	Specifies the uri where the CMSP Gateway may retrieve the corresponding complete CAP version of the Alert Message per Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition,* of Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition*.
CMAC_cap_identifier	M	Specifies the identifier value in the corresponding CAP message.
CMAC_cap_sent_date_time	M	Specifies the date and time the corresponding CAP message was sent.

The following table summarizes the required CMAC elements of the CMAC_alert_info segment for an Update Message (see Clause 6.3.2, *CMAC_alert_info Segment Element Definition,* Table 6.5 – *CMAC_alert_info Segment Element Definition,* for the element encoding formats):

Table 6.14 – Elements of Alert Info Segment for Update Message

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_category	M	Per Table 6.5 – *CMAC_alert_info Segment Element Definition*, of Clause 6.3.2, *CMAC_alert_info Segment Element Definition*.
CMAC_response_type	O	Per Table 6.5 – *CMAC_alert_info Segment Element Definition*, of Clause 6.3.2, *CMAC_alert_info Segment Element Definition*.
CMAC_severity	M	Per Table 6.5 – *CMAC_alert_info Segment Element Definition*, of Clause 6.3.2, *CMAC_alert_info Segment Element Definition*.
CMAC_urgency	M	Per Table 6.5 – *CMAC_alert_info Segment Element Definition*, of Clause 6.3.2, *CMAC_alert_info Segment Element Definition*.
CMAC_certainty	M	Per Table 6.5 – *CMAC_alert_info Segment Element Definition*, of Clause 6.3.2, *CMAC_alert_info Segment Element Definition*.
CMAC_expires_date_time	M	Per Table 6.5 – *CMAC_alert_info Segment Element Definition*, of Clause 6.3.2, *CMAC_alert_info Segment Element Definition*.

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_sender_name	O	Optional element which may be included per Table 6.5 – *CMAC_alert_info Segment Element Definition*, of Clause 6.3.2, *CMAC_alert_info Segment Element Definition*.

The following table summarizes the required CMAC elements of the CMAC_Alert_Area segment for an Update Message (see Clause 6.3.3, *CMAC_Alert_Area Segment Element Definition,* Table 6.6 – *CMAC_Alert_Area Segment Element Definition,* for the element encoding formats):

Table 6.15 – Elements of Alert Area Segment for Update Message

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_area_description	M	Per Table 6.6 – *CMAC_Alert_Area Segment Element Definition*, of Clause 6.3.3, *CMAC_Alert_Area Segment Element Definition*.
CMAC_polygon	O	Per Table 6.6 – *CMAC_Alert_Area Segment Element Definition*, of Clause 6.3.3, *CMAC_Alert_Area Segment Element Definition*.
CMAC_circle	O	Per Table 6.6 – *CMAC_Alert_Area Segment Element Definition*, of Clause 6.3.3, *CMAC_Alert_Area Segment Element Definition*.
CMAC_cmas_geocode	M	Geocode indicating the updated alert area. (See Clause 6.3.6, *Definition of CMAC_cmas_geocode Element*). This updated alert area may be different than the alert area of the message being updated.
CMAC_cap_geocode	O	Per Table 6.6 – *CMAC_Alert_Area Segment Element Definition*, of Clause 6.3.3, *CMAC_Alert_Area Segment Element Definition*.
CMAC_gnis	O	Per Table 6.6 – *CMAC_Alert_Area Segment Element Definition*, of Clause 6.3.3, *CMAC_Alert_Area Segment Element Definition*.

The following table summarizes the required CMAC elements of the CMAC_Alert_Text segment for an Update Message (see Clause 6.3.4, *CMAC_Alert_Text Segment Element Definition*, Table 6.7 – *CMAC_Alert_Text Segment Element Definition,* for the element encoding formats):

Table 6.16 – Elements of Alert Text Segment for Update Message

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_text_language	M	Per Table 6.7 – *CMAC_Alert_Text Segment Element Definition,* of Clause 6.3.4, *CMAC_Alert_Text Segment Element Definition*.
CMAC_short_text_alert_message_length	M	Length in characters of the short text message per Table 6.7 – *CMAC_Alert_Text Segment Element Definition,* of Clause 6.3.4, *CMAC_Alert_Text Segment Element Definition*.
CMAC_short_text_alert_message	M	90-character maximum short text message per Table 6.7 – *CMAC_Alert_Text Segment Element Definition,* of Clause 6.3.4, *CMAC_Alert_Text Segment Element Definition*.
CMAC_long_text_alert_message_length	M	Length in characters of the long text message per Table 6.7– *CMAC_Alert_Text Segment Element Definition,* of Clause 6.3.4, *CMAC_Alert_Text Segment Element Definition*.

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_text_language	M	360-character maximum long text message per Table 6.7– *CMAC_Alert_Text Segment Element Definition,* of Clause 6.3.4, *CMAC_Alert_Text Segment Element Definition*.

Example non-National Imminent Threat WEA Update Message

The following is an example format of a non-National Imminent Threat WEA Update Message initiated by the Federal Alert Gateway. In this example, the Alert Message example of Clause 6.5.1, *Alert Message,* has been updated with a new expiration time of 11:30 PM:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<CMAC_Alert_Attributes xmlns = "cmac:2.0">
   <CMAC_protocol_version>2.0</CMAC_protocol_version>
   <CMAC_sending_gateway_id>http://wea_alert_gateway.gov</CMAC_sending_gateway_id>
   <CMAC_message_number>00001095</CMAC_message_number>
   <CMAC_referenced_message_number>00001056</CMAC_referenced_message_number>
   <CMAC_referenced_message_cap_identifier>NOAA-NWS-ALERTS Texas 2017-06-01:32:50-
00:00</CMAC_referenced_message_cap_identifier>
   <CMAC_sender>w-nws.webmaster@noaa.gov</CMAC_sender>
   <CMAC_sent_date_time>2017-06-03T02:32:50Z</CMAC_sent_date_time>
   <CMAC_status>Actual</CMAC_status>
   <CMAC_message_type>Update</CMAC_message_type>
   <CMAC_cap_alert_uri>http://wea_alert_gateway.gov/CMAM1095</CMAC_cap_alert_uri>
   <CMAC_cap_identifier>NOAA-NWS-ALERTS Texas 2017-06-02:32:50-
00:00</CMAC_cap_identifier>
   <CMAC_cap_sent_date_time>2017-06-03T01:32:50-00:00</CMAC_cap_sent_date_time>
   <CMAC_alert_info>
      <CMAC_category>Met</CMAC_category>
      <CMAC_severity>Severe</CMAC_severity>
      <CMAC_urgency>Expected</CMAC_urgency>
      <CMAC_certainty>Likely</CMAC_certainty>
      <CMAC_expires_date_time>2017-06-03T04:30:00Z</CMAC_expires_date_time>
      <CMAC_sender_name>NWS San Angelo TX</CMAC_sender_name>
        <CMAC_Alert_Area>
            <CMAC_area_description>Fisher; Jones; Taylor;
Callahan</CMAC_area_description>
            <CMAC_polygon>32.21,-99.62 32.27,-100.15 32.52,-100.15 32.52,-100.16 32.72,-
100.17 32.85,-99.61 32.21,-99.62</CMAC_polygon>
            <CMAC_cmas_geocode>48151</CMAC_cmas_geocode>
            <CMAC_cmas_geocode>48253</CMAC_cmas_geocode>
            <CMAC_cmas_geocode>48441</CMAC_cmas_geocode>
            <CMAC_cmas_geocode>48059</CMAC_cmas_geocode>
            <CMAC_cap_geocode>
                <valueName>SAME</valueName>
                <value>048151</value>
            </CMAC_cap_geocode>
            <CMAC_cap_geocode>
                <valueName>SAME</valueName>
                <value>048253</value>
            </CMAC_cap_geocode>
            <CMAC_cap_geocode>
                <valueName>SAME</valueName>
                <value>048441</value>
            </CMAC_cap_geocode>
            <CMAC_cap_geocode>
                <valueName>SAME</valueName>
                <value>048059</value>
            </CMAC_cap_geocode>
        </CMAC_Alert_Area>
```

```
        <CMAC_Alert_Text>
          <CMAC_text_language>English</CMAC_text_language>
          <CMAC_short_text_alert_message_length>53
            </CMAC_short_text_alert_message_length>
          <CMAC_short_text_alert_message>Flash Flood Warning this area until 11:30 PM
CDT. NWS</CMAC_short_text_alert_message>
          <CMAC_long_text_alert_message_length>188
            </CMAC_long_text_alert_message_length>
          <CMAC_long_text_alert_message>Flash Flood Warning this area until 11:30 PM CDT.
Avoid flood areas. Do not drive on flooded roads. Check local radio and television
stations for more information. National Weather Service</CMAC_long_text_alert_message>
        </CMAC_Alert_Text>
        <CMAC_Alert_Text>
          <CMAC_text_language>Spanish</CMAC_text_language>
          <CMAC_short_text_alert_message_length>69
            </CMAC_short_text_alert_message_length>
          <CMAC_short_text_alert_message>Aviso de inundación de destello esta área hasta
las 11:30 PM CDT. NWS</CMAC_short_text_alert_message>
          <CMAC_long_text_alert_message_length>248
            </CMAC_long_text_alert_message_length>
          <CMAC_long_text_alert_message>Advertencia de inundación de emergencia esta área
hasta las 11:30 PM CDT. Evite las zonas de inundación. No conduzca en carreteras
inundadas. Consulte las emisoras de radio y televisión locales para obtener más
información. National Weather Service</CMAC_long_text_alert_message>
        </CMAC_Alert_Text>
   </CMAC_alert_info>
</CMAC_Alert_Attributes>
```

The XML Signature component has been omitted from the above example WEA message. The XML Signature would be created in accordance with [Ref 38].

The short 90-character maximum English WEA Update Message would be broadcast as:

> Flash Flood Warning this area until 11:30 PM CDT. NWS

The long 360-character maximum English WEA Update Message would be broadcast as:

> Flash Flood Warning this area until 11:30 PM CDT. Avoid flood areas. Do not drive on flooded roads. Check local radio and television stations for more information. National Weather Service

The short 90-character maximum Spanish WEA Update Message would be broadcast as:

> Aviso de inundación de destello esta área hasta las 11:30 PM CDT. NWS

The long 360-character maximum Spanish WEA Update Message would be broadcast as:

> Advertencia de inundación de emergencia esta área hasta las 11:30 PM CDT. Evite las zonas de inundación. No conduzca en carreteras inundadas. Consulte las emisoras de radio y televisión locales para obtener más información. National Weather Service

Example National WEA Update Message

The following is an example format of a National Alert Update Message initiated by the Federal Alert Gateway. In this example, the Alert Message example of Clause 6.5.1, *Alert Message,* has been updated with a new expiration time of 8:15 PM:

NOTE: “Presidential” as a protocol value has not yet been changed to “National”.

```
<?xml version = "1.0" encoding = "UTF-8"?>
<CMAC_Alert_Attributes xmlns = "cmac:2.0">
   <CMAC_protocol_version>2.0</CMAC_protocol_version>
   <CMAC_sending_gateway_id>http://wea_alert_gateway.gov</CMAC_sending_gateway_id>
   <CMAC_message_number>00001056</CMAC_message_number>
   <CMAC_special_handling>Presidential</CMAC_special_handling>
   <CMAC_sender>wh.webmaster@noaa.gov</CMAC_sender>
   <CMAC_sent_date_time>2017-07-09T11:35:00Z</CMAC_sent_date_time>
   <CMAC_status>Actual</CMAC_status>
   <CMAC_message_type>Update</CMAC_message_type>
   <CMAC_cap_alert_uri>http://wea_alert_gateway.gov/CMAM1056</CMAC_cap_alert_uri>
   <CMAC_cap_identifier>White House Alert 2017-07-09T18:22:17-7:00</CMAC_cap_identifier>
   <CMAC_cap_sent_date_time>2017-07-09T18:22:17-07:00</CMAC_cap_sent_date_time>
   <CMAC_alert_info>
      <CMAC_category>Security</CMAC_category>
      <CMAC_severity>Extreme</CMAC_severity>
      <CMAC_urgency>Expected</CMAC_urgency>
      <CMAC_certainty>Likely</CMAC_certainty>
      <CMAC_expires_date_time>2017-07-09T23:15:00Z</CMAC_expires_date_time>
      <CMAC_Alert_Area>
         <CMAC_area_description>entire United States</CMAC_area_description>
         <CMAC_cmas_geocode>00000</CMAC_cmas_geocode>
      </CMAC_Alert_Area>
      <CMAC_Alert_Text>
          <CMAC_text_language>English</CMAC_text_language>
          <CMAC_short_text_alert_message_length>53
            </CMAC_short_text_alert_message_length>
          <CMAC_short_text_alert_message>President has issued an alert in this area until
8:15PM PDT Monitor Radio or TV</CMAC_short_text_alert_message>
          <CMAC_long_text_alert_message_length>128
            </CMAC_long_text_alert_message_length>
          <CMAC_long_text_alert_message>The US President has issued an alert in this area
until 8:15PM PDT Monitor local Radio or TV stations for additional
information</CMAC_long_text_alert_message>
        </CMAC_Alert_Text>
        <CMAC_Alert_Text>
          <CMAC_text_language>Spanish</CMAC_text_language>
          <CMAC_short_text_alert_message_length>89
            </CMAC_short_text_alert_message_length>
          <CMAC_short_text_alert_message>Presidente ha emitido una alerta en esta área
hasta las 8:15 PM PDT Monitor de radio o TV</CMAC_short_text_alert_message>
          <CMAC_long_text_alert_message_length>174
            </CMAC_long_text_alert_message_length>
          <CMAC_long_text_alert_message>El Presidente de los Estados Unidos ha emitido
una alerta en esta área hasta las 8:15 PM PDT Monitoree las estaciones locales de radio o
TV para obtener información adicional</CMAC_long_text_alert_message>
        </CMAC_Alert_Text>
   </CMAC_alert_info>
</CMAC_Alert_Attributes>
```

The XML Signature schema component has been omitted from the above example WEA message. The XML Signature would be created in accordance with [Ref 38].

The short 90-character maximum English WEA National Alert Update Message would be broadcast as:

> President has issued an alert in this area until 8:15PM PDT Monitor Radio or TV

The long 360-character maximum English WEA National Alert Update Message would be broadcast as:

> The US President has issued an alert in this area until 8:15PM PDT Monitor local Radio or TV stations for additional information

The short 90-character maximum Spanish WEA National Alert Update Message would be broadcast as:

Presidente ha emitido una alerta en esta área hasta las 8:15 PM PDT Monitor de radio o TV

The long 360-character maximum Spanish WEA National Alert Update Message would be broadcast as:

El Presidente de los Estados Unidos ha emitido una alerta en esta área hasta las 8:15 PM PDT Monitoree las estaciones locales de radio o TV para obtener información adicional

6.5.3 Cancel Message

A WEA Cancel Message will consist of a CMAC message containing one CMAC_Alert_Attributes segment and one CMAC_Digital_Signature segment. The CMAC_status is set to “Actual” and the CMAC_message_type is set to “Cancel” to indicate the Cancel Message, with the <CMAC_referenced_message_number> containing the message number for the message to be cancelled.

The following table summarizes the required CMAC elements of the CMAC_Alert_Attributes segment for an Alert Cancel Message (see Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition,* Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition,* for the element encoding formats):

Table 6.17 – Elements of Alert Attributes Segment for Cancel Message

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_protocol_version	M	Per Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition*, of Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition*.
CMAC_sending_gateway_id	M	Federal Alert Gateway identifier which initiated the CMAC message.
CMAC_message_number	M	Message number for this CMAM assigned by the Federal Alert Gateway. NOTE: To uniquely identify a message, the CMSP Gateway uses the CMAC_message_number in conjunction with the CMAC_cap_identifier.
CMAC_referenced_message_number	M	Message number of the corresponding message to be cancelled.
CMAC_referenced_message_cap_ identifier	M	Identifier of the corresponding cap message of the corresponding alert message to be cancelled.
CMAC_special_handling	C	Conditional element included per Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition,* of Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition*. For a Child Abduction Emergency, value of “Child Abduction”. For a National Alert message, value of “Presidential”.* For a Public Safety message, value of “Public Safety”. For a WEA Test message, value of "State Local WEA Test". * Note that “Presidential” as a protocol value has not yet been changed to “National”.
CMAC_sender	M	Identifies the originator of the alert cancellation per Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition,* of Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition*.
CMAC_sent_date_time	M	Date and time in UTC the Cancel Message is sent by the Federal Alert Gateway in XML dateTime format.
CMAC_status	M	Value of “Actual”.

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_message_type	M	Value of “Cancel”.
CMAC_cap_alert_uri	M	Specifies the uri where the CMSP Gateway may retrieve the corresponding complete CAP version of the Alert Message per Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition,* of Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition*.
CMAC_cap_identifier	M	Specifies the identifier value in the corresponding CAP message.
CMAC_cap_sent_date_time	M	Specifies the date and time the corresponding CAP message was sent.

The following is an example format of a non-National Alert Cancel Message initiated by the Federal Alert Gateway. In this example, the Alert Message example of Clause 6.5.1, *Alert Message,* has been cancelled:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<CMAC_Alert_Attributes xmlns = "cmac:2.0">
   <CMAC_protocol_version>2.0</CMAC_protocol_version>
   <CMAC_sending_gateway_id>http://wea_alert_gateway.gov</CMAC_sending_gateway_id>
   <CMAC_message_number>00001098</CMAC_message_number>
   <CMAC_referenced_message_number>00001056</CMAC_referenced_message_number>
   <CMAC_referenced_message_cap_identifier>NOAA-NWS-ALERTS Texas 2017-06-
01:32:50Z</CMAC_referenced_message_cap_identifier>
   <CMAC_sender>w-nws.webmaster@noaa.gov</CMAC_sender>
   <CMAC_sent_date_time>2017-06-03T02:32:50Z</CMAC_sent_date_time>
   <CMAC_status>Actual</CMAC_status>
   <CMAC_message_type>Cancel</CMAC_message_type>
   <CMAC_cap_alert_uri>http://wea_alert_gateway.gov/CMAM1098</CMAC_cap_alert_uri>
   <CMAC_cap_identifier>NOAA-NWS-ALERTS Texas 2017-06-02:32:50-
00:00</CMAC_cap_identifier>
   <CMAC_cap_sent_date_time>2017-06-03T02:32:10-00:00</CMAC_cap_sent_date_time>
</CMAC_Alert_Attributes>
```

The XML Signature schema component has been omitted from the above example WEA message. The XML Signature would be created in accordance with [Ref 38].

The following is an example format of a National Alert Cancel Message initiated by the Federal Alert Gateway. In this example, the Alert Message example of Clause 6.5.1, *Alert Message,* has been cancelled:

NOTE: “Presidential” as a protocol value has not yet been changed to “National”.

```
<?xml version = "1.0" encoding = "UTF-8"?>
<CMAC_Alert_Attributes xmlns = "cmac:2.0">
   <CMAC_protocol_version>2.0</CMAC_protocol_version>
   <CMAC_sending_gateway_id>http://wea_alert_gateway.gov</CMAC_sending_gateway_id>
   <CMAC_message_number>00001098</CMAC_message_number>
   <CMAC_referenced_message_number>00001056</CMAC_referenced_message_number>
   <CMAC_referenced_message_cap_identifier>White House Alert 2017-07-09T18:22:17-
7:00</CMAC_referenced_message_cap_identifier>
   <CMAC_special_handling>Presidential</CMAC_special_handling>
   <CMAC_sender>wh.webmaster@whitehouse.gov</CMAC_sender>
   <CMAC_sent_date_time>2017-07-09T13:07:00Z</CMAC_sent_date_time>
   <CMAC_status>Actual</CMAC_status>
   <CMAC_message_type>Cancel</CMAC_message_type>
   <CMAC_cap_alert_uri>http://wea_alert_gateway.gov/CMAM1098</CMAC_cap_alert_uri>
   <CMAC_cap_identifier>White House Alert 2017-07-09T20:07:00-7:00</CMAC_cap_identifier>
   <CMAC_cap_sent_date_time>2017-07-09T20:07:00-07:00</CMAC_cap_sent_date_time>
```

```
</CMAC_Alert_Attributes>
```

The XML Signature schema component has been omitted from the above example WEA message. The XML Signature would be created in accordance with [Ref 38].

6.5.4 Ack Message

The CMAC Ack Message contains only a CMAC_Alert_Attributes segment. In the Ack Message, the sending Gateway will provide the identifier of that Gateway in the CMAC_sending_gateway_id element, and indicate the time the message is acknowledged in the CMAC_sent_date_time element. The CMAC_referenced_message_number will contain the message number of the message that is being acknowledged and the CMAC_status element will indicate this is a “System” message.

The following table summarizes the required CMAC elements for an Ack Message (see Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition,* Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition,* for the element encoding formats):

Table 6.18 – Elements of Alert Attributes Segment for Ack Message

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_protocol_version	M	Per Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition*, of Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition*.
CMAC_sending_gateway_id	M	CMSP Gateway identifier or Federal Alert Gateway Identifier.
CMAC_message_number	M	Message number assigned by the sending Gateway.
CMAC_referenced_message_number	M	The message number value contained in the CMAC message received from the sending Gateway which is being acknowledged.
CMAC_sent_date_time	M	Date and time the acknowledgement is sent by the sending Gateway in UTC in XML dateTime format.
CMAC_status	M	Value of “System”.
CMAC_message_type	M	Value of “Ack”.

The following is the format of an example Ack Message from the CMSP Gateway to the Federal Alert Gateway upon receipt of a WEA Alert, Update, or Cancel message:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<CMAC_Alert_Attributes xmlns = "cmac:2.0">
   <CMAC_protocol_version>2.0</CMAC_protocol_version>
   <CMAC_sending_gateway_id>http://wea_cmsp_alert_gateway_uri</CMAC_sending_gateway_id>
   <CMAC_message_number>00001056</CMAC_message_number>
   <CMAC_referenced_message_number>00001056</CMAC_referenced_message_number>
   <CMAC_sent_date_time>2017-06-17T07:57:05Z</CMAC_sent_date_time>
   <CMAC_status>System</CMAC_status>
   <CMAC_message_type>Ack</CMAC_message_type>
</CMAC_Alert_Attributes>
```

6.5.5 Error Message

The CMAC Error Message contains only a CMAC_Alert_Attributes segment. An error condition is indicated by the CMAC_message_type element containing “Error” with one or more CMAC_response_code elements containing

response codes and with one or more CMAC_note elements containing CMAC response descriptions (see Clause 6.8.3.3, *Error Response Codes*).

The following table summarizes the required CMAC elements for a CMSP Gateway error indication of a Federal Alert Gateway-initiated Alert, Update, or Cancel message (see Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition,* Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition,* for the element encoding format):

Table 6.19 – Elements of Alert Attributes Segment for Error Message

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_protocol_version	M	Per Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition*, of Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition*.
CMAC_sending_gateway_id	M	CMSP Gateway identifier or Federal Alert Gateway Identifier.
CMAC_message_number	M	Message number assigned by the sending Gateway.
CMAC_referenced_message_number	M	The message number value contained in the CMAC message received from the sending Gateway which is being sent an error response.
CMAC_sent_date_time	M	Date and time the error response is sent by the sending Gateway in UTC in XML dateTime format.
CMAC_status	M	Value of “System”.
CMAC_message_type	M	Value of “Error”.
CMAC_response_code	M	CMAC response code from Clause 6.8.3.3, *Error Response Codes*. Multiple occurrences of the CMAC_response_code may occur in this error response.
CMAC_note	M	CMAC Response description from Clause 6.8.3.3, *Error Response Codes*. Multiple occurrence of the CMAC_note may occur in this error response.

The following is the format of an example CMSP Gateway error message sent from the CMSP Gateway to the Federal Alert Gateway:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<CMAC_Alert_Attributes xmlns = "cmac:2.0">
   <CMAC_protocol_version>2.0</CMAC_protocol_version>
   <CMAC_sending_gateway_id>http://wea_cmsp_gateway_uri</CMAC_sending_gateway_id>
   <CMAC_message_number>00001056</CMAC_message_number>
   <CMAC_referenced_message_number>00001056</CMAC_referenced_message_number>
   <CMAC_sent_date_time>2017-06-25T07:50:05Z</CMAC_sent_date_time>
   <CMAC_status>System</CMAC_status>
   <CMAC_message_type>Error</CMAC_message_type>
   <CMAC_response_code>104</CMAC_response_code>
   <CMAC_note>invalid-element CMAC_expires_date_time</CMAC_note>
</CMAC_Alert_Attributes>
```

The above example indicates the CMSP Gateway received the Alert or Update message after the message expiration time.

The following is the format of an example Link Test error message with multiple error conditions reported, sent from the CMSP Gateway to the Federal Alert Gateway:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<CMAC_Alert_Attributes xmlns = "cmac:2.0">
   <CMAC_protocol_version>2.0</CMAC_protocol_version>
   <CMAC_sending_gateway_id>http://wea_cmsp_gateway_uri</CMAC_sending_gateway_id>
   <CMAC_message_number>00001056</CMAC_message_number>
   <CMAC_referenced_message_number>00001056</CMAC_referenced_message_number>
   <CMAC_sent_date_time>2017-06-25T07:50:05Z</CMAC_sent_date_time>
   <CMAC_status>System</CMAC_status>
   <CMAC_message_type>Error</CMAC_message_type>
   <CMAC_response_code>104</CMAC_response_code>
   <CMAC_response_code>105</CMAC_response_code>
   <CMAC_note>invalid-element CMAC_sent_date_time</CMAC_note>
   <CMAC_note>missing-element CMAC_status</CMAC_note>
</CMAC_Alert_Attributes>
```

The above example indicates the CMSP Gateway is returning an error response to the Federal Alert Gateway for multiple error conditions. The first occurrence of the CMAC_response_code element is associated with the first occurrence of the CMAC_note element and the second occurrence of the CMAC_response_code element is associated with the second occurrence of the CMAC_note element.

6.5.6 Link Test Message

The Link Test Message will be a CMAC message containing only a CMAC_Alert_Attributes segment. A Link Test Message will be indicated by a CMAC_status element with as value of “System” and a CMAC_message_type element value of “Link Test”. The sending Gateway will indicate the time the message was initiated in the CMAC_sent_date_time element. The sending Gateway will assign a unique message number to the Link Test Message, specified in the CMAC_message_number element.

The following table summarizes the required CMAC elements for a Link Test Message (see Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition,* Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition,* for the encoding formats):

Table 6.20 – Elements of Alert Attributes Segment for Link Test Message

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_protocol_version	M	Per Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition*, of Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition*.
CMAC_sending_gateway_id	M	CMSP Gateway or Federal Alert Gateway identifier.
CMAC_message_number	M	Message number assigned by the sending Gateway.
CMAC_sent_date_time	M	Date and time the Link Test message is sent by the sending Gateway in UTC in XML dateTime format.
CMAC_status	M	Value of “System”.
CMAC_message_type	M	Value of “Link Test”.

The following is an example of the format for a Link Test Message initiated from the Federal Alert Gateway and sent to the CMSP Gateway:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<CMAC_Alert_Attributes xmlns = "cmac:2.0">
   <CMAC_protocol_version>2.0</CMAC_protocol_version>
   <CMAC_sending_gateway_id>http://wea_federal_alert_gateway_uri
   </CMAC_sending_gateway_id>
   <CMAC_message_number>00001056</CMAC_message_number>
   <CMAC_sent_date_time>2017-06-25T07:50:00Z</CMAC_sent_date_time>
   <CMAC_status>System</CMAC_status>
   <CMAC_message_type>Link Test</CMAC_message_type>
</CMAC_Alert_Attributes>
```

6.5.7 RMT Message

The Federal Alert Gateway may issue a Required Monthly Test (RMT) Message to the CMSP Gateway over the Reference Point "C" interface (see Clause 6.3, *Required Monthly Test (RMT) Call Flow*). The RMT Message will be a CMAC message containing a CMAC_Alert_Attributes segment, one CMAC_alert_info segment, one CMAC_Alert_Text segment, and one CMAC_Digital_Signature segment. The CMAC_Alert_Area segment is not required for an RMT Message as the CMSP determines the area to broadcast the RMT.

An RMT Message will be indicated by a CMAC_status element with a value of "System", a CMAC_special_handling element with a value of "Required Monthly Test", and a CMAC_message_type element value of "RMT". The Federal Alert Gateway will assign a unique message number to the RMT Message, specified in the CMAC_message_number element.

The following table summarizes the required CMAC elements of the CMAC_Alert_Attributes segment for a Federal Alert Gateway-initiated RMT Message (see Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition,* Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition,* for the element encoding format):

Table 6.21 – Elements of Alert Attributes Segment for RMT Message

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_protocol_version	M	Per Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition*, of Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition*.
CMAC_sending_gateway_id	M	Federal Alert Gateway identifier.
CMAC_message_number	M	Message number assigned by the Federal Alert Gateway.
CMAC_special_handling	M	Value of "Required Monthly Test".
CMAC_sent_date_time	M	Date and time the RMT Message is sent by the Federal Alert Gateway in UTC in XML dateTime format.
CMAC_status	M	Value of "System".
CMAC_message_type	M	Value of "RMT".

The following table summarizes the required CMAC elements of the CMAC_alert_info segment for a Federal Alert Gateway-initiated RMT Message (see Clause 6.3.2, *CMAC_alert_info Segment Element Definition,* Table 6.5 – *CMAC_alert_info Segment Element Definition,* for the element encoding format):

Table 6.22 – Elements of Alert Info Segment for RMT Message

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_category	M	Value of "Other".

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

The following table summarizes the required CMAC elements of the CMAC_Alert_Text segment for an Alert Message (see Clause 6.3.4, *CMAC_Alert_Text Segment Element Definition*, Table 6.7 – *CMAC_Alert_Text Segment Element Definition,* for the element encoding formats):

Table 6.23 – Elements of Alert Text Segment for RMT Message

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_text_language	M	Per Table 6.7 – CMAC_Alert_Text Segment Element Definition, of Clause 6.3.4, *CMAC_Alert_Text Segment Element Definition*.
CMAC_short_text_alert_message_length	M	Length in characters of the short text message per Table 6.7 – CMAC_Alert_Text Segment Element Definition, of Clause 6.3.4, *CMAC_Alert_Text Segment Element Definition*.
CMAC_short_text_alert_message	M	90-character maximum short text message per Table 6.7 – CMAC_Alert_Text Segment Element Definition, of Clause 6.3.4, *CMAC_Alert_Text Segment Element Definition*.
CMAC_long_text_alert_message_length	M	Length in characters of the long text message perTable 6.7 – CMAC_Alert_Text Segment Element Definition, of Clause 6.3.4, *CMAC_Alert_Text Segment Element Definition*.
CMAC_long_text_alert_message	M	360-character maximum long text message per Table 6.7 – CMAC_Alert_Text Segment Element Definition, of Clause 6.3.4, *CMAC_Alert_Text Segment Element Definition*.

The following is an example of the format for an RMT Message initiated from the Federal Alert Gateway and sent to the CMSP Gateway:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<CMAC_Alert_Attributes xmlns = "cmac:2.0">
   <CMAC_protocol_version>2.0</CMAC_protocol_version>
   <CMAC_sending_gateway_id>http://cmaswea_federal_alert_gateway_uri
      </CMAC_sending_gateway_id>
   <CMAC_message_number>00001056</CMAC_message_number>
   <CMAC_special_handling>Required Monthly Test</CMAC_special_handling>
   <CMAC_sent_date_time>2017-06-25T07:50:00Z</CMAC_sent_date_time>
   <CMAC_status>System</CMAC_status>
   <CMAC_message_type>RMT</CMAC_message_type>
   <CMAC_alert_info>
      <CMAC_category>Other</CMAC_category>
      <CMAC_severity>Severe</CMAC_severity>
      <CMAC_urgency>Expected</CMAC_urgency>
```

```
      <CMAC_certainty>Likely</CMAC_certainty>
      <CMAC_expires_date_time>2017-07-09T23:15:00Z</CMAC_expires_date_time>
      <CMAC_sender_name>John Doe</CMAC_sender_name>
      <CMAC_Alert_Text>
          <CMAC_text_language>English</CMAC_text_language>
          <CMAC_short_text_alert_message_length>74
            </CMAC_short_text_alert_message_length>
          <CMAC_short_text_alert_message>This is a test of the Wireless Emergency Alert
System. This is only a test</CMAC_short_text_alert_message>
          <CMAC_long_text_alert_message_length>74
            </CMAC_long_text_alert_message_length>
          <CMAC_long_text_alert_message>This is a test of the Wireless Emergency Alert
System. This is only a test</CMAC_long_text_alert_message>
      </CMAC_Alert_Text>
   </CMAC_alert_info>
</CMAC_Alert_Attributes>
```

6.5.8 Transmission Control – Cease Message

Upon a maintenance command or other error condition at the CMSP Gateway, the CMSP Gateway may issue a Transmission Control – Cease Message to the Federal Alert Gateway over the Reference Point "C" interface to cease message traffic on Reference Point "C" destined for that CMSP Gateway. The Transmission Control – Cease Message will be a CMAC message containing only a CMAC_Alert_Attributes segment. A Transmission Control – Cease Message will be indicated by a CMAC_status element with a value of "System" and a CMAC_message_type element value of "Transmission Control – Cease". The CMSP Gateway will indicate the time the message was initiated in the CMAC_sent_date_time element. The CMSP Gateway will assign a unique message number to the Transmission Control message, specified in the CMAC_message_number element.

The following table summarizes the required CMAC elements for a CMSP Gateway-initiated Transmission Control – Cease Message used to cease transmission (see Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition,* Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition,* for the element encoding formats):

Table 6.24 – Elements of Alert Attributes Segment for Transmission Control – Cease Message

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_protocol_version	M	Per Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition*, of Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition*.
CMAC_sending_gateway_id	M	CMSP Gateway identifier.
CMAC_message_number	M	Message number assigned by the CMSP Gateway.
CMAC_sent_date_time	M	Date and time the Transmission Control message is sent by the CMSP Gateway in UTC in XML dateTime format.
CMAC_status	M	Value of "System".
CMAC_message_type	M	Value of "Transmission Control – Cease".

The following is an example of the format for a Transmission Control – Cease Message initiated from the CMSP Gateway and sent to the Federal Alert Gateway to cease transmissions:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<CMAC_Alert_Attributes xmlns = "cmac:2.0">
   <CMAC_protocol_version>2.0</CMAC_protocol_version>
   <CMAC_sending_gateway_id>http://wea_cmsp_gateway_uri</CMAC_sending_gateway_id>
   <CMAC_message_number>00001056</CMAC_message_number>
   <CMAC_sent_date_time>2017-06-25T14:50:00Z</CMAC_sent_date_time>
```

```
   <CMAC_status>System</CMAC_status>
   <CMAC_message_type>Transmission Control - Cease</CMAC_message_type>
</CMAC_Alert_Attributes>
```

6.5.9 Transmission Control – Resume Message

Once the maintenance or error condition is cleared, the CMSP Gateway will inform the Federal Alert Gateway that transmission of messages may resume using a Transmission Control – Resume Message indicated by a CMAC_status element with as value of “System” and a CMAC_message_type element value of “Transmission Control – Resume”. The CMSP Gateway will indicate the time the message was initiated in the CMAC_sent_date_time element. The CMSP Gateway will assign a unique message number to the Transmission Control – Resume Message, specified in the CMAC_message_number element.

The following table summarizes the required CMAC elements for a CMSP Gateway-initiated Transmission Control – Resume Message used to resume transmission (see Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition,* Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition,* for the element encoding formats):

Table 6.25 – Elements of Alert Attributes Segment for Transmission Control – Resume Message

CMAC Element	Mandatory/ Optional/ Conditional	Value
CMAC_protocol_version	M	Per Table 6.4 – *CMAC_Alert_Attributes Segment Element Definition*, of Clause 6.3.1, *CMAC_Alert_Attributes Segment Element Definition*.
CMAC_sending_gateway_id	M	CMSP Gateway identifier.
CMAC_message_number	M	Message number assigned by the CMSP Gateway.
CMAC_sent_date_time	M	Date and time the Transmission Control message is sent by the CMSP Gateway in UTC in XML dateTime format.
CMAC_status	M	Value of “System”.
CMAC_message_type	M	Value of “Transmission Control - Resume”.

The following is an example of the format for a Transmission Control – Resume Message initiated from the CMSP Gateway and sent to the Federal Alert Gateway to resume transmissions:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<CMAC_Alert_Attributes xmlns = "cmac:2.0">
   <CMAC_protocol_version>2.0</CMAC_protocol_version>
   <CMAC_sending_gateway_id>http://wea_cmsp_gateway_uri</CMAC_sending_gateway_id>
   <CMAC_message_number>00001056</CMAC_message_number>
   <CMAC_sent_date_time>2017-06-25T14:55:00Z</CMAC_sent_date_time>
   <CMAC_status>System</CMAC_status>
   <CMAC_message_type>Transmission Control - Resume</CMAC_message_type>
</CMAC_Alert_Attributes>
```

6.6 DBGF Bypass Request

When circles or polygons are included by the alert originator, the WEA alert message requires DBGF by default. The alert originator can request that DBGF be bypassed for this alert. The Invocation of DBGF is specified in *Wireless Emergency Alert (WEA) 3.0 via EPS Public Warning System Specification* ATIS-0700010 [Ref 49].

[WEA-C-RQMT-2940$_{R3A}$] The Federal Alert Gateway shall be able to indicate that bypassing DBGF is requested in the CMAC alert or update.

[WEA-C-RQMT-2950$_{R3A}$] If DBGF bypass is requested in the CMAC alert or update and bypassing DBGF is allowed by regulatory policy, then the CMSP shall bypass DBGF procedures for the WEA.

[WEA-C-RQMT-2960$_{R3A}$] DBGF bypass requests shall be ignored for CMAC messages without polygon or circle elements.

[WEA-C-RQMT-2964$_{R3A}$] If the DBGF Bypass is requested by an Alert Originator not authorized to make this request, the receiving Federal Alert Gateway shall not forward the alert to the CMSP Gateway.

[WEA-C-RQMT-2965$_{R3A}$] If the DBGF Bypass is requested by an Alert Originator authorized to make this request, the receiving Federal Alert Gateway shall populate the CMAC_note field accordingly.

A DBGF Bypass request is indicated by the Federal Alert Gateway by the inclusion of the string "Bypass Device-Based Geo-Fencing" in an instance of CMAC_note as shown below.

```
<CMAC_note>Bypass Device-Based Geo-Fencing</CMAC_note>
```

6.7 Transport 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.

TCP and IP will be implemented as detailed in the following requirements. Each Federal Alert Gateway to CMSP Gateway connection will be defined by a unique socket pair, consisting of the source IP address, source port number, destination IP address, and destination port number, where the source and destination IP addresses are obtained from the IP address or Fully Qualified Domain Name contained in the CMSP profile and Federal Alert Gateway profile.

[WEA-C-RQMT-3000] The Federal Alert Gateway to CMSP Gateway interface shall be in accordance with RFC 1122 [Ref 27].

6.7.1 Transmission Control Protocol (TCP)

TCP will be the transport level protocol used by the Federal Alert Gateway and the CMSP Gateway to exchange messages. TCP is a connection-oriented protocol and thus requires establishment of a connection to another system to facilitate data transfer. The interface will use persistent connections. A Gateway will close a connection only after providing notification to the other Gateway.

[WEA-C-RQMT-3100] TCP shall be implemented for the transport layer in accordance with RFC 793 [Ref 23].

[WEA-C-RQMT-3110] TCP connections shall be persistent.

6.7.2 Internet Protocol (IP)

IP will be the network layer protocol used by the Federal Alert Gateway and the CMSP Gateway to exchange CMAC messages. Both IP Version 4 (IPv4) and IP Version 6 (IPv6) will be supported.

[WEA-C-RQMT-3200] The interface shall support IP Version 4 for the network layer in accordance with IETF STD 5 (RFC 791) [Ref 28].

[WEA-C-RQMT-3210] The network layer shall support Internet Control Message Protocol (ICMP) in accordance with IETF STD 5 (RFC 792) for IP Version 4 [Ref 29].

[WEA-C-RQMT-3220] The interface shall support IP Version 6 for the network layer in accordance with RFC 8200 [Ref 30] and RFC 4291 [Ref 32].

6.8 Error Handling

6.8.1 TCP/IP Error Handling

This interface uses the reliable TCP protocol to correct any transmission errors that occur at IP or lower layers. Using TCP isolates such errors from HTTP and CMAC protocol layers. TCP uses a retransmission mechanism to correct any errors in received packets.

[WEA-C-RQMT-3300] Any packets received in error shall be discarded at TCP level by the receiving gateway.

[WEA-C-RQMT-3310] When a packet is received in error, a correct packet shall be retransmitted by the sending gateway per TCP protocol.

[WEA-C-RQMT-3320] Both the CMSP Gateway and the Federal Alert Gateway shall log failures to establish a TCP session.

[WEA-C-RQMT-3330] Both the CMSP Gateway and the Federal Alert Gateway shall log failures to establish a secure IP tunnel.

6.8.2 HTTP Level Error Handling

As only HTTP GET and POST methods will be used on this interface, all other HTTP methods are to be rejected.

[WEA-C-RQMT-3400] The Federal Alert Gateway shall reject all HTTP methods other than POST with a 4xx Client Error response when the CMSP Gateway sends a CMAC message.

[WEA-C-RQMT-3410] The CMSP Gateway shall reject all HTTP methods other than POST with a 4xx Client Error response.

[WEA-C-RQMT-3420] The Federal Alert Gateway shall reject HTTP methods other than GET with a 4xx Client Error response when the CMSP Gateway requests to retrieve a CAP message.

[WEA-C-RQMT-3430] The Federal Alert Gateway shall send a 4xx Client Error or 5xx Server Error response message when it is unable to retrieve the CAP message requested by a CMSP Gateway.

6.8.3 CMAC Error Handling

6.8.3.1 XML Schema Validation

[WEA-C-RQMT-3500] Messages not conforming to the CMAC XML Schema [Refs 33, 43, & 44] shall be logged and discarded.

NOTE: See Clause 6.4, *CMAC Message XML Definition,* for the CMAC XML Schema.

[WEA-C-RQMT-3510] An Error message shall be sent in response to messages not conforming to the CMAC XML Schema [Refs 33, 43, & 44].

6.8.3.2 CMAC Message Content Validation

The format of each CMAC message is detailed as follows:

- Alert (Clause 6.5.1, *Alert Message*).
- Update (Clause 6.5.2, *Update Message*).
- Cancel (Clause 6.5.3, *Cancel Message*).
- RMT (Clause 6.5.7, *RMT Message*).
- Link Test (Clause 6.5.6, *Link Test Message*).
- Ack (Clause 6.5.4, *Ack Message*).
- Error (Clause 6.5.5, *Error Message*).
- Transmission Control – Cease (Clause 6.5.8, *Transmission Control – Cease Message*).
- Transmission Control – Resume (Clause 6.5.9, *Transmission Control – Resume Message*).

[WEA-C-RQMT-3600] Messages containing information that conflicts with the CMAC protocol shall be logged and discarded.

[WEA-C-RQMT-3610] An Error message shall be sent in response to messages containing information that conflicts with the CMAC protocol.

NOTE: See Table 6.26 – *Definition of CMAC Response Codes*, for error response codes.

6.8.3.3 Error Response Codes

Error response codes (see Table 6.26) are used by the Federal Alert Gateway and the CMSP Gateway in Error messages only. Though Ack and Error messages may contain errors, the response codes would not be used as those errors will not be reported in Error messages.

Each Error message will contain one or more of the response codes listed in Table 6.26 – *Definition of CMAC Response Codes*.

The following table defines the response codes and the response description that may be returned in the CMAC_response_code and CMAC_note elements in response to a received CMAC message via the Reference Point "C" interface. In addition, the following table defines the associated message types for the response codes and provides any explanatory notes.

Table 6.26 – Definition of CMAC Response Codes

Response Code	Response Description included in CMAC_note Element	Associated Message Type	Notes
100	invalid-federal-alert-gateway-id	Error	The sending gateway identifier is not valid.
101	protocol–version-not-supported	Error	The gateway does not support the indicated protocol version.
102	server-error	Error	General error in the server.
103	invalid-format	Error	The received XML has an invalid format. This can indicate XML well-formedness [Ref 21] errors or validations error results from application of the XML CMAC Schema defined in this specification to the received CMAC message.
104	invalid-element XXX	Error	XXX replaced with the name of the invalid element. (e.g., "CMAC_Alert_Area" exceeds the limits for alert areas defined in [WEA-C-RQMT-2550] and [WEA-C-RQMT-2551]).
105	missing-element XXX	Error	XXX replaced with name of missing element.
106	operation-not-allowed	Error	The requested operation is not allowed.
107	operation-pre-empted	Error	The requested operation (e.g., an RMT) was pre-empted and not completed.
108	RMT-distribution-precluded	Error	Unforeseen condition in CMSP infrastructure precludes distribution of RMT.
109	test-message-distribution-precluded	Error	Unforeseen condition in CMSP infrastructure precludes distribution of State/Local WEA Test message.

Annex A
(normative)

A Public Broadcasting Service Digital Television Interface to CMSP Gateway

This annex defines the requirements for the interface (referred to as Reference Point "C1") from the C-Interface Over the Air (C-OTA) Digital Television (DTV) Receiver and Decoder to the CMSP Gateway. CMAC messages are inserted in the DTV stream broadcast by Public Broadcasting Service (PBS); the C-OTA DTV Receiver and Decoder picks up and decodes the transmission and sends CMAC messages to the CMSP Gateway over the Reference Point "C1" Interface.

A.1 Scope

The scope of this Annex is the definition of the interface between the C-OTA DTV Receiver and Decoder and the CMSP Gateway as shown in Figure A.1. The definitions of the other interfaces shown in Figure A.1 are outside the scope of this Annex.

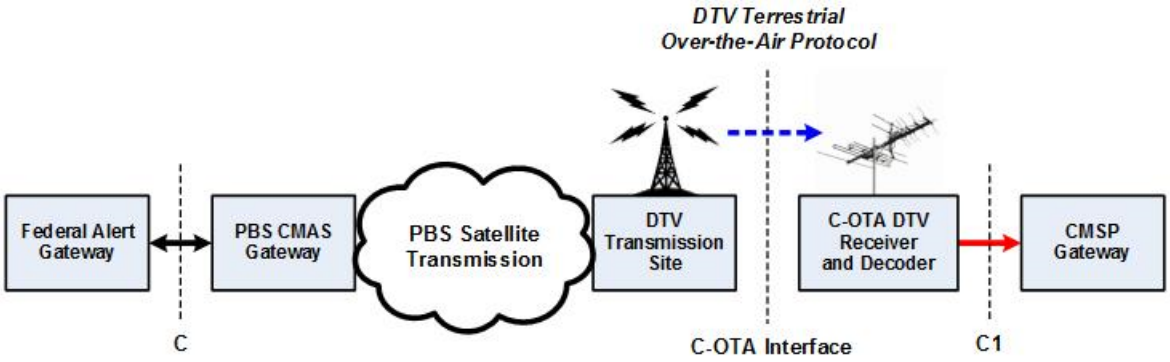


Figure A.1 – Public Broadcasting Service WEA Architecture

The Federal Alert Gateway sends CMAC messages to the PBS CMAS Gateway via the "C" Interface. Subsequently, the PBS Gateway retrieves the corresponding CAP messages.

The CMAC messages and their corresponding CAP messages are inserted in the PBS transport stream transmitted via satellite to terrestrial DTV transmission sites.

The CMAC and CAP messages are in the DTV signal broadcast from the DTV Transmission Sites using the C-OTA interface.

The C-OTA DTV Receiver and Decoder picks up the DTV signal and "extracts" the CMAC and CAP messages. The CMAC messages are sent to the CMSP Gateway over the Reference Point "C1" Interface.

NOTE: The CMSP Gateway does not send any CMAC messages to the C-OTA DTV Receiver and Decoder.

The CMSP Gateway is not capable of initiating messages toward, or responding to messages from, the Federal Alert Gateway over the "C1" interface.

Any processing in the Federal Alert Gateway, the PBS CMAS Gateway, the PBS Satellite Transmission network, the C-OTA DTV Receiver and Decoder, and the CMSP Gateway that is not related to the Reference Point "C1" is outside the scope of this Annex.

A.2 Reference Point "C1" Related Requirements

In general, it should be assumed that all requirements in the main body of this Standard apply to the Federal Alert Gateway and the CMSP Gateway for the Reference Point "C1" interface, taking into account the Reference Point "C1" interface supports a subset of the CMAC messages. The following are Reference Point "C1" related requirements which may supersede C interface requirements:

[WEA-C1-RQMT-0010] The Federal Alert Gateway shall provide CMAC messages to the PBS CMAS Gateway over the "C" Interface.

[WEA-C1-RQMT-0020] The Federal Alert Gateway shall send all CMAC messages to the PBS CMAS Gateway. The Federal Alert Gateway shall not perform geo-location filtering of CMAC messages to the PBS CMAS Gateway.

[WEA-C1-RQMT-0030] From the perspective of the "C" Interface, the PBS CMAS Gateway shall support the requirements of the CMSP Gateway as defined in this Standard, including the retrieval of CAP messages.

NOTE: The PBS CMAS Gateway passes the <CMAC_note>Bypass Device-Based Geo-Fencing</CMAC_note>, if received, to the CMSP Gateway without any processing described in Clause 6.6.

[WEA-C1-RQMT-0040] The PBS CMAS Gateway shall not embed CMAC messages that failed validation onto a DTV broadcast signal.

[WEA-C1-RQMT-0050] The PBS CMAS Gateway shall retrieve the associated CAP message for each CMAC Alert, Update and Cancel message.

[WEA-C1-RQMT-0060] A DTV Transmission Site shall embed CMAC and CAP messages onto a DTV broadcast signal using the DTV Terrestrial Over-the-Air Protocol. The process of embedding CMAC and CAP messages onto the DTV Terrestrial Over-the-Air Protocol is performed in PBS's network prior to broadcasting.

[WEA-C1-RQMT-0070] The "C1" interface shall present to the CMSP Gateway only CMAC and CAP messages that were authenticated by, and received from, the Federal Alert Gateway.

[WEA-C1-RQMT-0080] Geo-targeted CMAC messages received at the C-OTA DTV Receiver and Decoder shall be identical to the CMAC message received at the PBS CMAS gateway.

NOTE: A CMSP Gateway covering a wide geographic area may be deployed anywhere in the nation; thus, the CMAC messages delivered to the PBS CMAS gateway and received by the C-OTA DTV Receiver and Decoder contains all alert information, including the geotargeting information, provided by the Federal Alert Gateway which the CMSP Gateway will use to transmit the alerts. To support this CMSP architecture, all DTV Transmission Sites nationwide will broadcast the same identical CMAC message. Any other transmission of geotargeted CMAMs by the PBS CMAS Gateway, PBS Satellite Transmission, DTV Transmission Site, or the C-OTA DTV Receiver and Decoder is beyond the scope of this Standard.

[WEA-C1-RQMT-0090] A C-OTA DTV Receiver and Decoder shall send each unique WEA message across the "C1" Interface only once.

[WEA-C1-RQMT-0100] A C-OTA DTV Receiver and Decoder shall receive the DTV over-the-air signal and to extract the CMAC and CAP messages from the DTV Terrestrial Over-the-Air Protocol. The extraction of the CMAC and CAP message from the DTV Terrestrial Over-the-Air Protocol, as well as function of the C-OTA DTV Receiver and Decoder beyond the "C1" Interface protocol is specified in *WARN (Warning, Alert and Response Network) Receiver Requirements (C-OTA DTV Receiver/Decoder), August 31, 2021, Version 4.0* Technical Specification – PWS-005 [Ref 50].

NOTE: Use of CAP messages is beyond the scope of this Standard.

[WEA-C1-RQMT-0110] The "C1" interface shall be in the domain of the CMSP and the security of the "C1" interface shall be contained within the security domain of the CMSP.

[WEA-C1-RQMT-0120] A CMSP Gateway shall forward Alert and Cancel messages when it receives Alert, Update or Cancel messages over the "C1" interface when the "C" interface is not available.

[WEA-C1-RQMT-0130] A CMSP Gateway shall not forward any Alert and Cancel messages when it receives Alert, Update, or Cancel messages over the "C1" interface when the "C" interface is available.

NOTE: The "C" interface is assumed to be available when Link Test messages are received at a regular interval over the "C" interface. The C interface is assumed to be “not available” when all inbound links from the Federal Alert Gateways are down, not when only the inbound link from one Federal Alert Gateway is not available.

[WEA-C1-RQMT-0132] A CMSP GW shall acknowledge a received RMT message over the "C1" interface by sending an email as specified by FEMA.

NOTE: Sending of the email may be automatic or manual.

[WEA-C1-RQMT-0134] The Reference Point “C1” interface shall not include provisions for the following functions:

a. Acknowledgements.
b. CAP Retrieval.
c. Transmission Control Procedure.

[WEA-C1-RQMT-0140] The C-OTA DTV Receiver and Decoder shall send all the valid CMAC and CAP messages that it receives to the CMSP Gateway.

[WEA-C1-RQMT-0150] TCP [Ref 23] shall be the transport protocol used to transmit XML Alert Messages between the C-OTA DTV Receiver and Decoder and the CMSP Gateway on the Reference Point “C1” interface.

a. [WEA-C1-RQMT-0160] TCP shall be implemented for the transport layer in accordance with RFC 793 [Ref 23]. TCP connections shall be persistent.

[WEA-C1-RQMT-0170] IP shall be the network layer protocol used by the C-OTA DTV Receiver and Decoder and the CMSP Gateway to exchange CMAC messages. Both IP Version 4 (IPv4) and IP Version 6 (IPv6) shall be supported.

a. [WEA-C1-RQMT-0180] The Reference Point “C1” interface shall support IP Version 4 for the network layer in accordance with IETF STD 5 (RFC 791) [Ref 28].
b. [WEA-C1-RQMT-0190] The Reference Point “C1” interface shall support IP Version 6 for the network layer in accordance with RFC 8200 [Ref 30] and RFC 4291 [Ref 32].
c. [WEA-C1-RQMT-0200] The network layer shall support Internet Control Message Protocol (ICMP) in accordance with IETF STD 5 (RFC 792) for IP Version 4 [Ref 29].

[WEA-C1-RQMT-0210] HTTP shall be the application level protocol used by the C-OTA DTV Receiver and Decoder and the CMSP Gateway to exchange CMAC messages. The HTTP is a request/response protocol. The HTTP methods shall be limited to POST for the Reference Point “C1” interface. The HTTP POST method shall be used by the C-OTA DTV Receiver and Decoder (client) to send all messages in the CMAC protocol to the CMSP Gateway (server).

a. [WEA-C1-RQMT-0220] HTTP communications shall be per RFC 7230 [Ref 1].
b. [WEA-C1-RQMT-0230] HTTP communications carrying CMAC and CAP messages shall be to port TCP 8080.
c. [WEA-C1-RQMT-0240] HTTP methods shall be limited to POST when CMAC Alert, Update, Cancel, RMT, Link Test, and CAP messages are sent over HTTP.
d. [WEA-C1-RQMT-0250] The HTTP POST method shall use “00” as the Request_URI for CMAC messages and "01" as Request_URI for CAP messages.

[WEA-C1-RQMT-0260] The Reference Point “C1” interface shall use the reliable TCP protocol to correct any transmission errors that occur at IP or lower layers per Clause 6.7.1 and Clause 6.7.2.

[WEA-C1-RQMT-0270] The CMSP Gateway shall perform CMAC Error Handling per Sections 6.8.3.1 and 6.8.3.2 with the exception of sending an error message for the following message types:

a. Alert (Clause 6.5.1, *Alert Message*).
b. Update (Clause 6.5.2, *Update Message*).
c. Cancel (Clause 6.5.3, *Cancel Message*).
d. RMT (Clause 6.5.7, *RMT Message*).
e. Link Test (Clause 6.5.6, *Link Test Message*).

[WEA-C1-RQMT-0280] A CMSP Gateway that receives a CMAC message over the Reference Point “C1” Interface that fails validation shall not broadcast the CMAC message and shall discard the CMAC message.

[WEA-C1-RQMT-0290] The CMSP Gateway shall keep a log of all messages received over the Reference Point “C1” interface, including messages that fail validation and are discarded.

[WEA-C1-RQMT-0300] Reference Point "C1" Interface shall support Non-Repudiation per Section 4.5.3. The Federal Alert Gateway shall digitally sign each CMAC Alert, Update, Cancel, and RMT message. This XML Signature [Ref 38] shall be included in the CMAC message on the Reference Point "C1" interface. The CMSP Gateway may optionally use the XML Signature for non-repudiation or ignore it, but it must be able to process the CMAC with the XML Signature.

A.3 Reference Point "C1" Call Flows

A.3.1 Reference Point "C1" Valid Message Call Flow

All valid CMAC and CAP types have the same call flow across the Reference Point "C1" Interface. The following figure with its descriptions of the associated call flow steps defines the call flow for CMAC Alert, Update, Cancel, RMT, and Link Test message types:

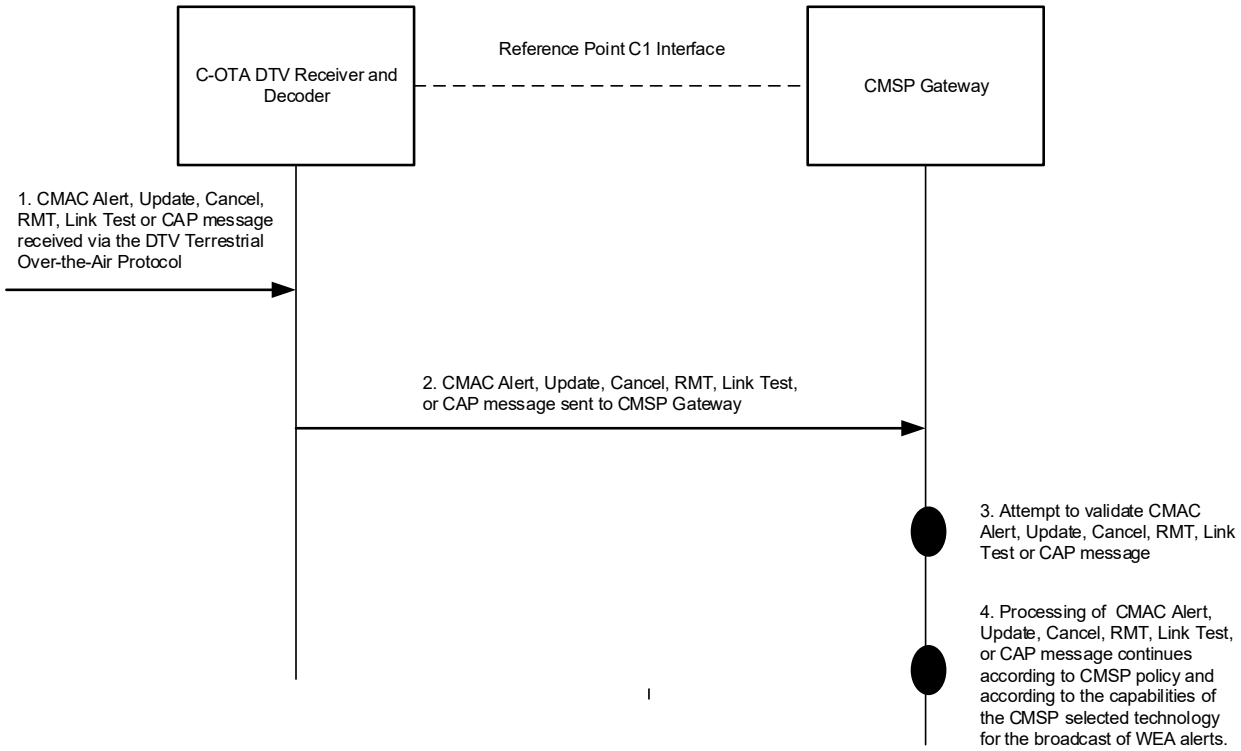


Figure A.2 – Reference Point "C1" Valid Message Call Flow

1. A CMAC Alert, Update, Cancel, RMT, Link Test, or CAP message is received by the C-OTA DTV Receiver and Decoder from the DTV Terrestrial Over-the-Air Protocol. This function is beyond the scope of this Standard.
2. The C-OTA DTV Receiver and Decoder sends the CMAC Alert, Update, Cancel, RMT, Link Test, or CAP message to the CMSP Gateway via the Reference Point "C1" Interface.
3. The CMSP Gateway attempts to validate the received CMAC message and the received CMAC message passes validation.

   NOTE: CAP messages are not validated by the PBS CMAS Gateway.
4. The processing of the received CMAC Alert, Update, Cancel, RMT, Link Test, or CAP message continues according to CMSP policy and according to the capabilities of the CMSP selected technology for the broadcast of WEA alerts.

A.3.2 Reference Point "C1" Invalid Message Call Flow

The following figure with its descriptions of the associated call flow steps defines the call flow for an invalid CMAC Alert, Update, Cancel, RMT, or Link Test message types:

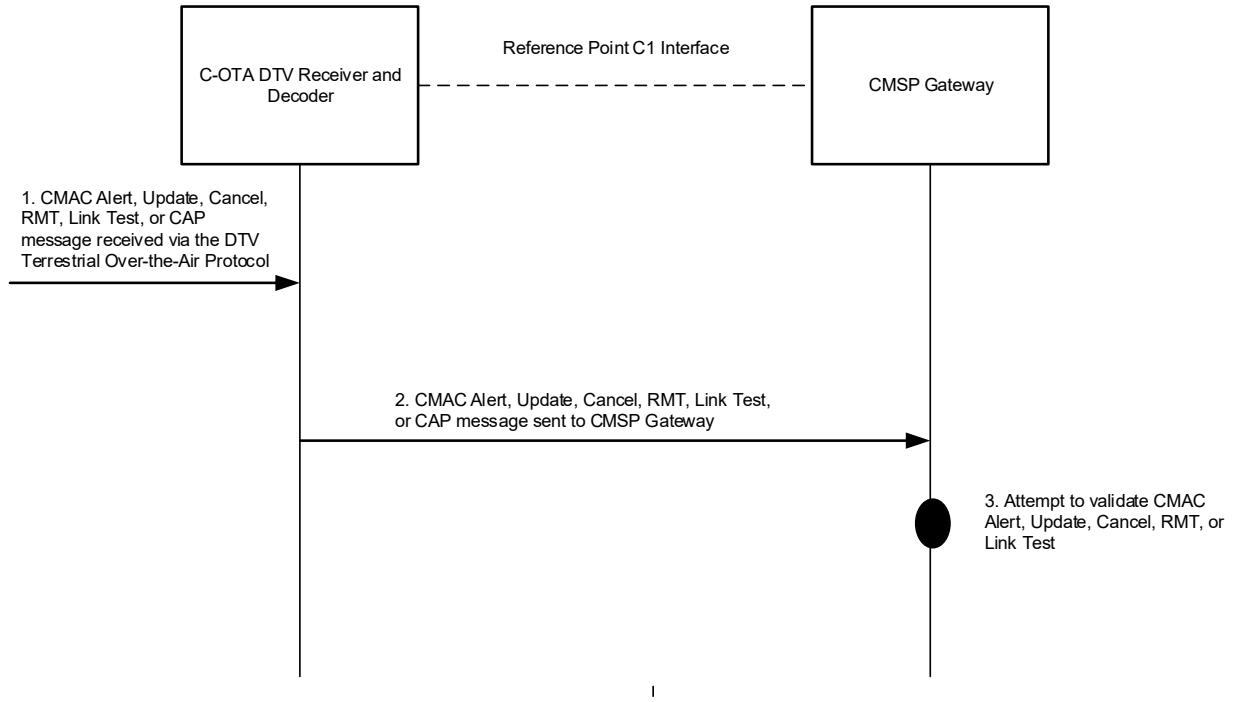


Figure A.3 – Reference Point "C1" Invalid Message Call Flow

1. A CMAC Alert, Update, Cancel, RMT, Link Test, or CAP message is received by the C-OTA DTV Receiver and Decoder from the DTV Terrestrial Over-the-Air Protocol. This function is beyond the scope of this Standard.
2. The C-OTA DTV Receiver and Decoder sends the CMAC Alert, Update, Cancel, RMT, Link Test or CAP message to the CMSP Gateway via the Reference Point "C1" Interface.
3. The CMSP Gateway attempts to validate the received CMAC message and the received CMAC message fails validation. The invalid CMAC message is logged and discarded by the CMSP Gateway.

   NOTE: CAP messages are not validated by the PBS CMAS Gateway.

A.4 Reference Point "C1" Messages

The following table specifies the complete subset of CMAC messages that shall be supported on the "C1" Interface:

Table A.1 – Reference Point "C1" CMAC Message Segments

CMAC Message	CMAC Message Segments	Reference
CMAC Alert Message	one <CMAC_Alert_Attributes> segment	6.3.1
	one <CMAC_alert_info> segment	6.3.2
	one or more <CMAC_Alert_Area> segments	6.3.3
	one or more <CMAC_Alert_Text> segments	6.3.4
	one <CMAC_Digital_Signature> segment	6.3.5

CMAC Message	CMAC Message Segments	Reference
CMAC Update Message	one <CMAC_Alert_Attributes> segment one <CMAC_alert_info> segment one or more <CMAC_Alert_Area> segments one or more <CMAC_Alert_Text> segments one <CMAC_Digital_Signature> segment	6.3.1 6.3.2 6.3.3 6.3.4 6.3.5
CMAC Cancel Message	one <CMAC_Alert_Attributes> segment one <CMAC_Digital_Signature> segment	6.3.1 6.3.5
CMAC Link Test Message	one <CMAC_Alert_Attributes> segment	6.3.1
CMAC RMT Message	one <CMAC_Alert_Attributes> segment one <CMAC_alert_info> segment one or more <CMAC_Alert_Text> segments one <CMAC_Digital_Signature> segment	6.3.1 6.3.2 6.3.4 6.3.5

Annex B
(informative)

B Reference Point "C" Interface Startup Procedure

Figure B.1 – *Reference Point "C" Interface Startup Procedures,* illustrates the steps involved at Reference Point "C" interface startup. The Federal Alert Gateway and each CMSP Gateway must establish an IPsec tunnel and a TCP connection before they can start CMAC message transfer. Initially, there is no IPsec tunnel available between the two gateways and the interface is in the "Unavailable" state. The only messages allowed through the interface at this state are IKEv2 messages.

IKEv2 establishes the IPsec tunnel with a sequence of request/response message pairs exchanged between the Federal Alert Gateway and the CMSP Gateway. Either gateway may initiate IKEv2 exchanges.

Once the IPsec tunnel is established, either gateway may initiate the TCP 3-way handshake, which establishes a TCP connection. Either gateway may start sending CMAC messages once the TCP connection is established. Both gateways must be ready to receive and process CMAC messages as soon as the TCP connection is established.

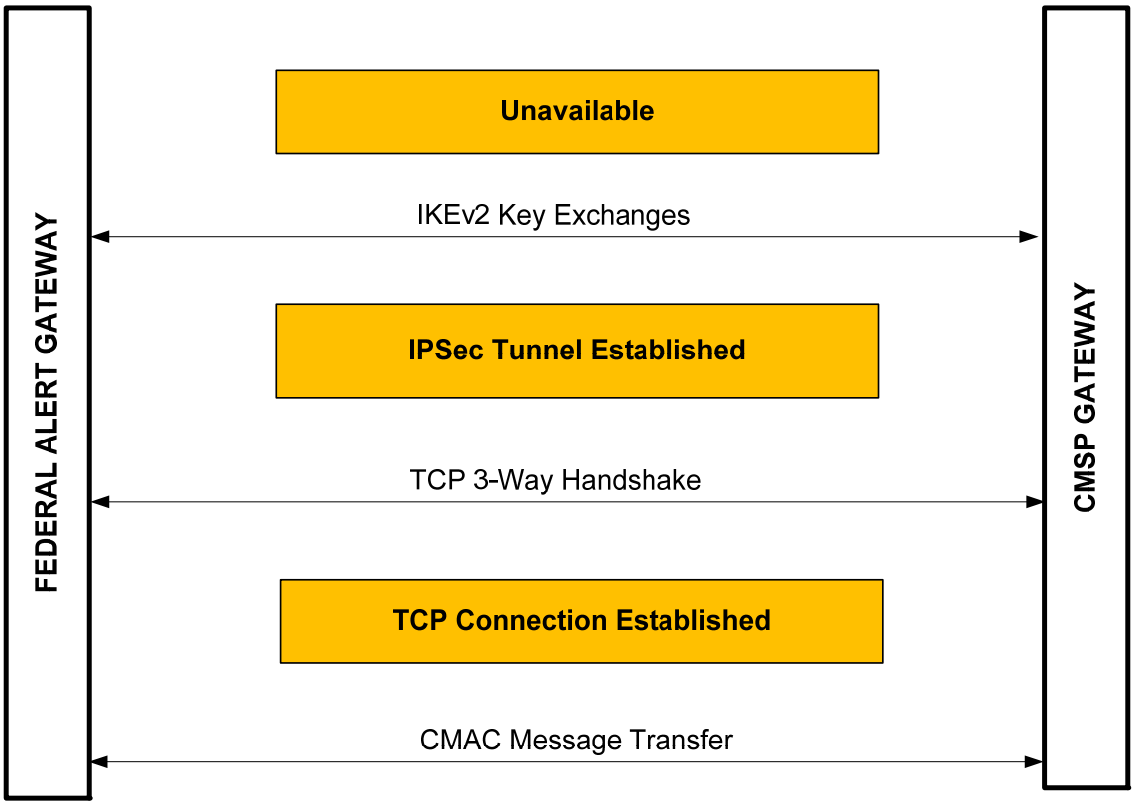


Figure B.1 – Reference Point "C" Interface Startup Procedures

Annex C
(informative)

C Qualification Provisions

This informative annex details the process for the verification of the requirements in this document and the ongoing monitoring that will follow. Clause C.2, *Responsibility for Verification,* addresses qualification responsibilities. Clause C.2.1, *Developmental Test and Evaluation (DT&E),* details the Developmental Test and Evaluation, which includes Federal Alert Gateway Acceptance, CMSP Gateway Acceptance, and Regression testing. Clause C.2.2, *Verification Methods,* describes the verification methods available for verifying the requirements. Clause C.2.3, *Security Test and Evaluation*, describes the security testing and evaluation. Clauses C.3, *System Monitoring,* and C.4, *Performance Monitoring,* summarize the Federal Alert Gateway system monitoring and performance monitoring, respectively.

C.1 Glossary

Regression Testing. Testing of computer software and/or systems to assure correct performance after changes were made to code that previously performed in a known manner. Regression testing seeks to uncover regression faults that occur when software functionality that previously worked as desired stops working or no longer works in the same way that was previously planned. Regression faults typically occur as an unintended consequence of program changes.

Verification. The process of confirming that a system or system element is designed and/or built as intended; in other words, that the system or element meets design-to or build-to specification. Verification answers the question: "Is the product as we expected it to be?"

C.2 Responsibility for Verification

Verification of the Federal Alert Gateway to CMSP Gateway interface, performed during Developmental Test and Evaluation (DT&E), will involve the Federal Emergency Management Agency (FEMA) and the CMSPs. FEMA, or its designated organization or contractor, will develop a WEA Test and Evaluation Master Plan (TEMP) and WEA Test Case Specifications. Testing of the interface between Federal Alert Gateway and CMSP Gateway will be included in the TEMP and the Test Case Specifications. The TEMP will detail the plan, process, and responsibilities for conducting the tests, while the Test Case Specifications will contain the specific steps necessary to verify the requirements contained in the Requirements Traceability matrix. FEMA will be responsible for planning and defining the Federal Alert Gateway and CMSP Gateway acceptance test process. The CMSPs will be responsible for supporting the test of their CMSP Gateway(s) through the process. Regression testing will be performed as necessary when changes impacting the interface are implemented.

C.2.1 Developmental Test & Evaluation (DT&E)

Both the Federal Alert Gateway and the CMSP Gateway should be tested to the extent possible in a standalone configuration, using test tools, before being integrated. The Federal Alert Gateway and each CMSP Gateway must pass acceptance test before being used operationally in WEA.

C.2.1.1 Federal Alert Gateway Acceptance Test

The Federal Alert Gateway acceptance test will be performed while connected to one or more CMSP Gateways or a test bed, per the TEMP and the Test Case Specifications.

C.2.1.2 CMSP Gateway Acceptance Test

Each CMSP Gateway will be subjected to a set of acceptance tests, per the TEMP and Test Case Specifications, before it is used operationally in WEA. CMSP Gateway acceptance test will involve the CMSP Gateway being connected to a Federal Alert Gateway, or a test bed with Federal Alert Gateway functionality implemented, per the

TEMP and Test Case Specifications. In addition to the requirements in this document, compliance with FCC Part 10 will be verified.

C.2.1.3 Regression Test

A regression test of either the Federal Alert Gateway or CMSP Gateway may be necessary under certain conditions, including configuration changes at either the CMSP Gateway or the Federal Alert Gateway. The regression tests may include all of the tests necessary for acceptance testing, or may require only a portion of them. The TEMP and Test Case Specifications will identify the circumstances under which regression test must be performed and the tests that comprise regression testing.

C.2.2 Verification Methods

The acceptable methods for verifying each requirement are the following:

- *Inspection*: This method is used to determine compliance without using special laboratory equipment, procedures, or services and consists of a nondestructive static-state examination of hardware, software, and/or technical data and documentation.
- *Demonstration*: This is a method in which qualitative determination of properties is made for a configuration item, including software and/or the use of technical data and documentation. The items being verified are observed, but not quantitatively measured, in a dynamic state.
- *Analysis*: This is a method in which hardware or software designs are compared with known scientific and technical principles, procedures, and practices to estimate the capability of the proposed design to meet the mission and system requirements.
- *Test*: This is a method in which performance is measured during or after the controlled application of functional and/or environmental stimuli. Quantitative measurements are analyzed to determine the degree of compliance. The process uses standardized laboratory equipment, procedures, and/or services.

C.2.3 Security Test & Evaluation

A post-assessment Security Test & Evaluation (ST&E) will be conducted to determine the adequacy of the security mechanisms and security policy, per the guidelines in *Technical Guide to Information Security Testing and Assessment* NIST SP 800-115 [Ref 101].[14] FEMA will be responsible for planning and defining the Federal Alert Gateway ST&E process.

C.3 System Monitoring

The Federal Alert Gateway will implement real-time monitoring of the interface to each CMSP Gateway and will provide system notifications to the appropriate Federal Alert Gateway system administrator or other FEMA personnel when problems are identified. The problems reported will include, for example, unsuccessful TCP/IP connections, problems in establishing secure connections, and lack of responses to transmitted Link Test Messages. The Federal Alert Gateway may switch the status of a CMSP Gateway to unavailable based on certain alerts.

C.4 Performance Monitoring

The Federal Alert Gateway will maintain metrics for each CMSP Gateway interface. The metrics will be available to Federal Alert Gateway system administrators upon request and will also result in system notifications if acceptable thresholds are exceeded in the reporting interval. Monitored performance parameters may include, for example,

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

round-trip times between transmitting a message and receiving the corresponding acknowledgement, and number of alert messages processed and transmitted to each CMSP Gateway.

Annex D
(normative)

D Configurable Parameters

This annex defines the configurable parameters which are associated with the Reference Point "C" interface. The CMSP Profile and the Federal Alert Gateway Profile contain configurable parameters, as defined in Table 4.3 and Table 4.4, respectively.

The following table identifies additional configurable parameters, describes their usage, and identifies the maximum parameter range.

Table D.1 – Configurable Parameters

Parameter Name	Parameter Description	Parameter Range
Message Response Time	The Federal Alert Gateway expects to receive a response from the CMSP Gateway within this interval of time.	1 to 10 seconds, in 1 second increments.
Reconnect Number	The number of times that the Federal Alert Gateway or the CMSP Gateway will attempt to establish an IPsec tunnel and a TCP connection when the initial attempt is unsuccessful.	0 to 10.
Retransmit Number	The number of times that the Federal Alert Gateway will attempt to send a CMAC message to the CMSP Gateway when the expected response is not received.	0 to 10.
Link Test Period	The time interval between Link Test Messages transmitted by the Federal Alert Gateway. The time interval is reset when the Federal Alert Gateway transmits any message to the CMSP Gateway.	1 to 120 minutes, in 1 minute increments.
IPsec SA Maximum Lifetime	IPsec SA Maximum Lifetime is the maximum time duration before the IPsec security association expires. This parameter should be ~10 minutes for testing and a few hours for operations.	Range 10-480 minutes, in minute increments. Default Value of 480 minutes (8 hours).
IKE SA Maximum Lifetime	IKE SA Maximum Lifetime is the maximum time duration before the IKE security association expires. This parameter should be ~20 minutes for testing. The IKE SA Maximum Lifetime should be set higher than the IPsec SA Maximum Lifetime.	Range 20- 1440 minutes, in 10 minute increments. Default Value of 1440 minutes (24 hours).
SA Renewal	Maximum time elapsed after SA expiration before a new SA is initiated. NOTE: A "Null" value for SA renewal indicates that SAs are not automatically renewed after expiration.	"Null" or a value in the range from 0 to 60 minutes.
Rekey	Minimum time before SA expiration when a new SA is initiated. NOTE: A "Null" value for Rekey time period indicates that SAs are not automatically replaced before expiration. Any other value for Rekey time period will cause SAs to be rekeyed before expiration, thus making the SA renewal parameter moot.	"Null" or a value in the range from 0 to 60 minutes.

Annex E
(informative)

E Example of End to End Message Identification

This informative annex and the following figure show an example of the end-to-end mapping of message identifiers throughout the WEA architecture:

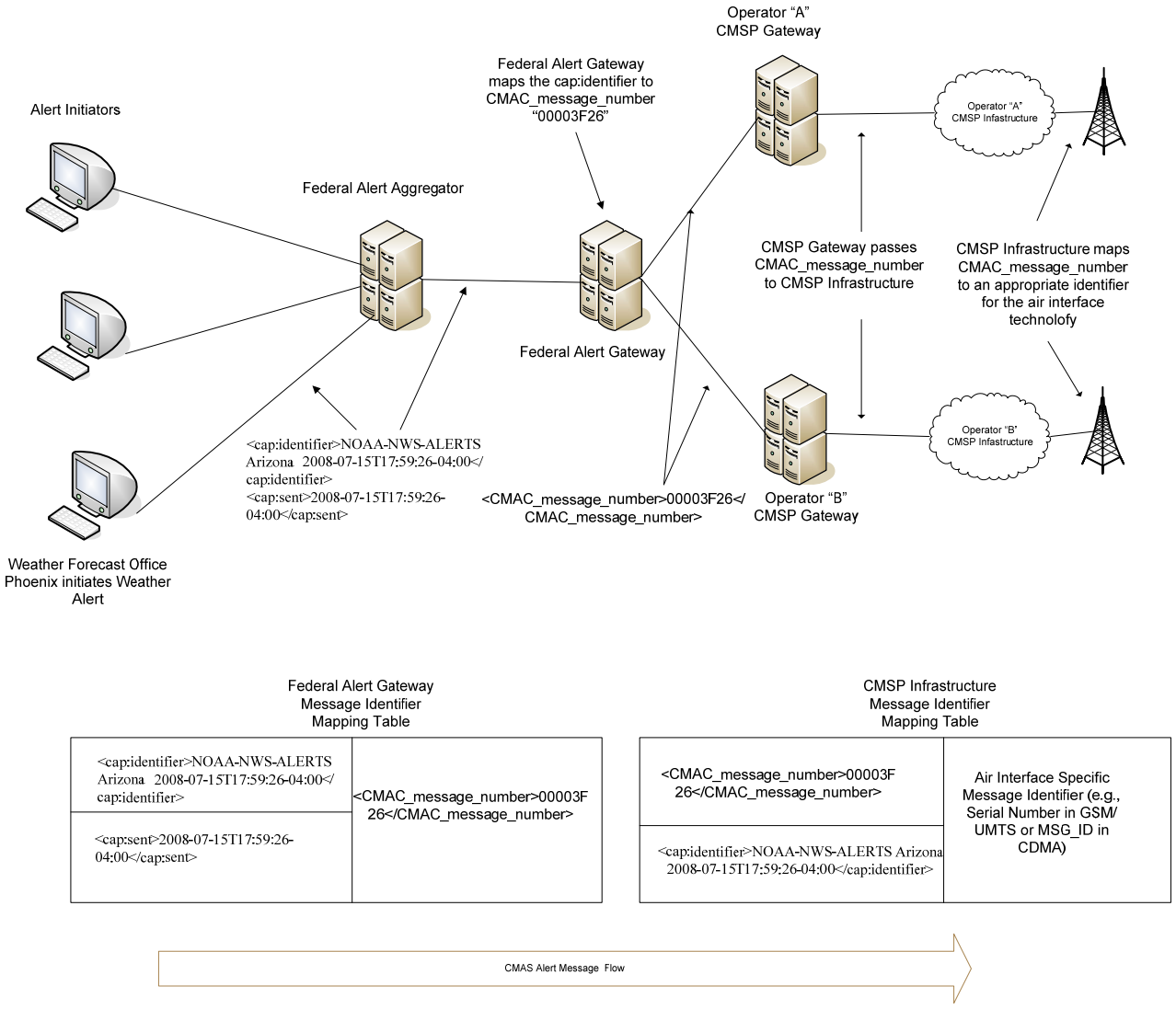


Figure E.1 – End-to-End Mapping of Message Identifiers

At the alert initiator and across Reference Points "A" and "B", the message identifier follows the CAP identifier element, and is a text string. When received by the Federal Alert Gateway, the Federal Alert Gateway generates a 4-octet CMAC_message_number corresponding to the message specified by the CAP identifier element, and stores the correlation between the CAP identifier and the CMAC_message_number.

Across the Reference Point "C" interface, the CMAC_message_number and the CMAC_cap_identifier may be used by the CMSP Gateway to uniquely identify a message. The CMSP infrastructure is responsible for mapping these elements into an air interface-specific identifier (this mapping is beyond the scope of this Standard).

As the number of messages increases, as well as large number of CMSP Gateways, the greater the chance the same CMAC message number may be used for multiple events assigned by different gateways, as follows:

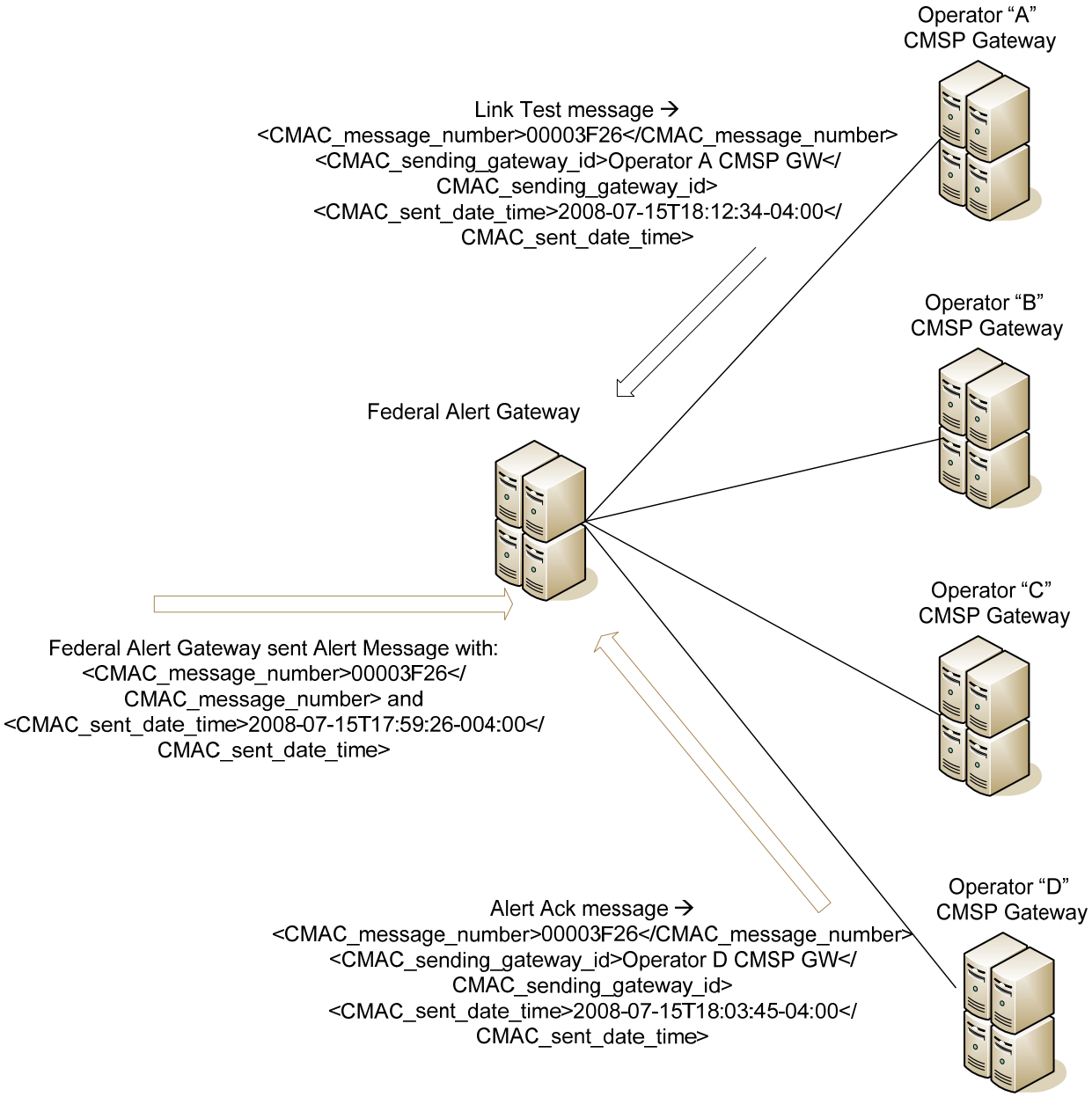


Figure E.2 – Message Identifiers with Multiple CMSP Gateways

In the above example, the Federal Alert Gateway may assign a CMAC_message_number of 00003F26 to an incoming alert message; simultaneously, the Operator "A" CMSP Gateway assigned a CMAC_message_number of 00003F26 to a Link Test Message, and the Operator "D" CMSP Gateway responded to the alert message with CMAC_message_number 00003F26. The Federal Alert Gateway is responsible for managing these message numbers, which may be viewed as follows:

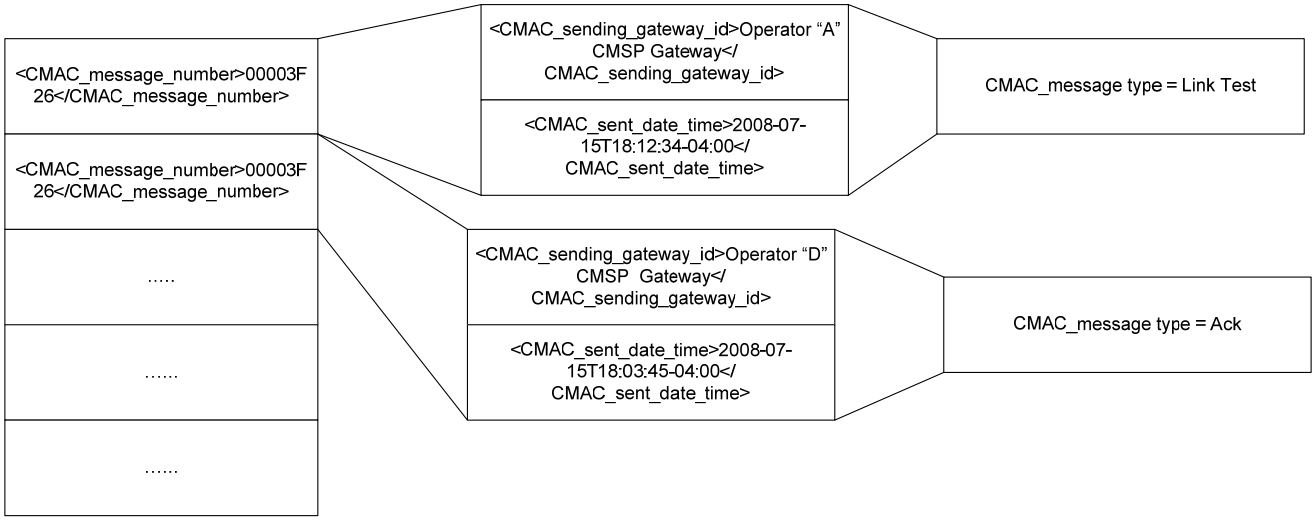


Figure E.3 – Example Database for Correlating Message Identifiers