The CMSAAC recommends that the CMSP Gateway support receiving a test message from the Alert Gateway for testing Reference Point C. This test message shall not be delivered to the CMSP Infrastructure nor broadcast to subscribers.

The CMSAAC recommends that the CMSP Gateway support the receipt and processing of Alert Gateway keep-alive test messages periodically. The frequency shall be configurable based on policy to be determined by the authorized government entity and the CMSPs.

The CMSAAC recommends that the keep-alive test messages *not* be sent if there are real messages to be sent.

9.5.1 General CMAS Testing Recommendations

An important part of a successful CMAS will be the ability to effectively test and troubleshoot the various components and interfaces.

The CMSAAC recommends that this test and troubleshooting capability be integrated into the architecture and protocol of the CMAS up front, to maximize effectiveness.

The CMSAAC recommends the following primary aspects of CMAS Testing and Troubleshooting capability to allow thorough testing and troubleshooting of the end-to-end CMAS without wearying the public:

1. Provision for testing of the CMAS, including the delivery mechanisms, without requiring all subscribers to see a test message.

    a. This might be accomplished by providing signaling in the application layer which indicates a test message – which would not be displayed by 'normal terminals', but could be displayed by 'test terminals'. CMSPs could configure which devices were 'test terminals'.

    b. Provide the ability to send test messages to a single CMSP/network without impact to other CMSPs.

    c. Provide the ability to test the CMAS up to the CMSP Gateway without impacting the CMSP infrastructure.

2. Provide CMSP access to the CMAM logs from the Alert Gateway.

3. Messages used for testing purposes shall be clearly differented from messages for actual events

9.5.2 Alert Gateway Testing

The CMSAAC recommends that the Alert Gateway support several types of testing:

a. Functional testing for the C interface (not expected to be sent to the subscribers)

b. Connection testing for new CMSP

The CMSAAC further recommends the following requirements for Alert Gateway testing:

1. The Alert Gateway will support initiating a test message for each service profile implemented for Reference Point C upon request by a particular CMSP. The test message will only be sent to a specific CMSP Gateway. The message will not be broadcast to subscribers.

2. The Alert Gateway will support initiating a test message for each service profile implemented for Reference Point C for all CMSP Gateways. The message will not be broadcast to subscribers.

3. The Alert Gateway will support keep-alive test messages periodically over the C interface. The frequency will be configurable based on policy to be determined by the authorized government entity and the CMSPs. The keep-alive test messages will not be sent if there are real messages to be sent.

4. All test messages for the C interface will be clearly marked and identified as test messages.

10 Interface Protocols for CMAS Alerts

The following two interfaces are applicable for the support of CMAS alerts in the CMSP networks:

- Alert Gateway – CMSP Interface which is Reference Point C
- CMSP – Mobile Device Interface for CMAS alert content which is Reference Point E

Both of these interfaces are defined in this section.

10.1 Reference Point A Protocol

The CMSAAC recommends that Reference Point A interface requirements consist of the following:

1. The message sent to the Alert Aggregator must consist of one of the following:

    a. A valid CAP 1.1 message with all mandatory elements.
    - Message ID
    - Sender ID
    - Sent Date/Time
    - Message Status
    - Message Type
    - Scope
    - Event Category
    - Urgency
    - Severity
    - Certainty
    - Resource description
    - Area Description – A FIPS geo-code, a polygon or circle (WGS-84 format) will be used to support the area description.

2. The Alert Aggregator will provide a mechanism to validate the identity of the individual sending the message to allow non-repudiation.

3. The implementer of the alert aggregator will provide a documented, non-proprietary, specification for transport that will support appropriate security and reliability.

10.2 Reference Point B Protocol

The CMSAAC recommends that Reference Point B interface requirements consist of the following:

1. The implementer of the Alert Gateway will provide a documented non-proprietary specification for the B interface which will support appropriate security and reliability.

10.3 Alert Gateway Interfaces & Mapping Requirements

10.3.1 Alert Gateway Interface Requirements

The CMSAAC recommends the following requirements for the Alert Gateway interfaces:

1. The Alert Gateway will support an open, non-proprietary interface to the Alert Aggregator (e.g. IP).
2. The Alert Gateway will initially support CAP v1.1 as the application layer protocol for communicating with the Alert Aggregator.
3. The Alert Gateway will uniquely identify each CMSP Gateway identified by a unique IP address or domain name.
4. The Alert Gateway will support the "C" interface protocol as defined in Section 10.4 below.
5. The Alert Gateway will support all CMAM formats that can be delivered to CMSP Gateway.
6. The Alert Gateway will support the common service profile formats as referred to in Section 6 above for text, audio, video and multimedia transmission of alert messages to the CMSP Gateways.
7. The Alert Gateway will support receiving acknowledgement from the CMSP Gateway that the CMAM has been received or rejected by the CMSP Gateway.
8. If any mandatory parameter/attribute is not included in the CAP message sent over the B interface, the Alert Gateway will use a default parameter value if available, or reject the CAP message if a default parameter value is not available.

10.3.2 Alert Gateway Interface Mapping Requirements

The Alert Gateway will map the CMAMs received in CAP format into the CMAC format supported by the CMSP Gateway.

1. If eventCode = "EAN", the CMAM will be handled as a Presidential Alert. The Alert Gateway will not forward messages with eventCode = "EAT" or "NIC" to the CMSP Gateway.
2. The Alert Gateway will deliver CMAMs using the same language as issued by the alert originator and will not do language translation as a gateway function.
3. Each CMAM will only include one language. The CMA issued in multiple languages will be issued by separate messages.
4. All CMAM alert, update & cancellation messages will come only from the alert originators, including Presidential alert. The Alert Gateway will pass these messages to the CMSP Gateway. The Alert Gateway is not required to generate alerts, alert updates and/or cancellations.
5. The Alert Gateway will not alter the content of text alert messages, with the exception of
   a. If CAP expires is not available, the default parameter value of one hour shall be used.
   b. Constructing the text alert message using CAP elements such as category, eventCode and responseType. The algorithm for constructing the text alert message is described in Section 5.3 above.

6. For Presidential Alert, the Alert Gateway will use the following CAP elements to construct the message:

    a. *Use CAP parameter (with valueName = CMAMtext), if available and less than the* maximum CMA message length limit. If not, then

    b. Use Alert Gateway generated automatic text: "The President has issued an emergency alert. Check local media for more details."

7. For AMBER Alert, the Alert Gateway will use the following CAP elements to construct the message:

    a. Use CAP parameter (with valueName = CMAMtext), if available and less than the maximum CMA message length limit. If not, the Alert Gateway will reject the message.

8. For alerts other than the Presidential Alert or AMBER Alert, the Alert Gateway will support free-format text generation or automatic text generation.

9. For free-format text generation, the Alert Gateway will use the CAP parameter (with valueName = CMAMtext) to construct the message. If the CAP parameter (with valueName = CMAMtext) is not available or exceeds the maximum CMA message length limit, the Alert Gateway will reject the message.

10. For automatic text generation, the Alert Gateway will support the following rules to construct the message:

    a. What's happening: The Alert Gateway will use the expanded text as defined in Table 5.1 for the CAP eventCode element if available. If eventCode is not provided, the Alert Gateway will use the expanded text as defined in Table 5.1 for the CAP category element.

    b. Area Affected: The Alert Gateway will use the phrase "in this area".

    c. Recommended action: The Alert Gateway will use the CAP responseType element if available. If responseType is not provided, the Alert Gateway will not include this information.

    d. Area Affected: The Alert Gateway will use the phrase "in this area".

    e. Expiration time with time zone: The Alert Gateway will translate the time according to Table 5.1 for the CAP expires element if provided. The Alert Gateway will use the time zone provided in the CAP expires element or may use the time zone in the affected area. If not provided, the Alert Gateway will use one hour from the current time as a default. If the affected area has more than one time zone, the Alert Gateway will use one of the time zones.

    f. Sending Agency: The Alert Gateway will translate it according to Table 5.1 for the CAP sender element. The translated sending agency should not exceed the maximum length of 12 characters in order to fit into the maximum CMA message length limit. The translated sending agency will be truncated to 12 characters if it causes the constructed message to exceed the maximum CMA message length limit.

11. If the CAP message received by the Alert Gateway is not formatted correctly, the Gateway will reject the message and inform the Alert Originator.

12. *If a CAP message contains multiple INFO blocks with the same headline but different area elements,* the Alert Gateway will collapse it into a single CMAM with a single INFO block and multiple area elements before sending it to the CMSP Gateway.

13. If a CAP message contains multiple INFO blocks with the different headlines, the Alert Gateway will create separate CMAM with each INFO block. The Alert Gateway will process the INFO blocks in the order contained in the CAP message.

14. The Alert Gateway will not do translations of the character sets.

15. The Geo-mapping of targeted area (cell sites) will be the responsibility of CMSPs and not a function of the Alert Gateway.

16. The Alert Gateway will provide the geo-targeting information over Reference Point C in accordance with the CMSP profile stored within the Alert Gateway.

17. The Alert Gateway will provide Geocode as specified in Section 10.4 below to the CMSP Gateway.

18. The Alert Gateway will translate latitude/longitude coordinates into appropriate State or County Geocode if no State or County Geocode is provided by alert originator.

19. The Alert Gateway will not be required to translate State or County Geocode into latitude/longitude coordinates.

20. The Alert Gateway will specify an agreed upon maximum number of latitude/longitude coordinates per polygon to be sent to the CMSP Gateway.

21. If Geocode, polygon or circle is not provided for a Presidential alert, the Alert Gateway will use "Nation wide" by default.

22. If Geocode, polygon or circle is not provided for any non-presidential alert or update, the Alert Gateway will reject the message and return an error to the alert originator.

23. For audio, video and multi-media CMAMs, if the CAP message includes the associated files, the Alert Gateway will

    a. Re-format, if necessary, the associated files into standardized format as specified in the associated service profile (See Section 6 above).

    b. Store the associated files on the Alert Gateway to be retrieved by the CMSP Gateways.

    c. Send the message with proper URL so that CMSP Gateways can retrieve the files if they so choose.

24. For audio, video and multi-media CMAMs, if the CAP message includes only the URL but not the associated files, the Alert Gateway will

    a. Retrieve the associated files from the URL in the CAP message

    b. Re-format, if necessary, the associated files into standardized format as specified in the associated service profile (See Section 6 above).

    c. Store the associated files on the Alert Gateway to be retrieved by the CMSP Gateway.

    d. Send the message with proper URL so that CMSP Gateway can retrieve the files if they so choose.

25. The Alert Gateway, via Reference Point C, will always provide the CMSP Gateway, the CMAC_geocode as defined in Section 10.4 below. Additionally, if available, the Alert Gateway will provide one or more of the following parameters to identify the alert area: CMAC_polygon, CMAC_circle or CMAC_gnis format.

26. The Alert Gateway will be responsible to generate the CMAC geocode(s) corresponding to the alert area from the CAP "area" element. The CMAC geocode(s) corresponding to the alert area will be generated from either the area described by the polygon or circle, conversion of the SAME code or ZIP code for the alert area, or using the FIPS value if specified in the original CAP alert message.

27. If the original CAP message does not contain a polygon, circle, or geocode, the Alert Gateway will reject the message unless the message originator was the President, in which case the alert area will be assumed Nationwide in the absence of the area information.

28. CAP will be the protocol used on the "B" interface to carry the CMAM into the Alert Gateway. Not all the elements and values allowed by CAP are useful for CMAMs. Also some elements are optional in CAP but required by CMAMs. The Alert Gateway will apply the following mapping and filtering rules for all the messages received via the "B" interface as shown in Table 10-1. The following is a description of the column shown in Table 10-1:

Column 1: Lists the CAP element.

Column 2: Lists the code values applicable to CMAMs.

Column 3: Lists the filtering and mapping rules to be used by the Alert Gateway. "Pass" means the element and code value will be passed from the "B" interface to the "C" interface. "Mapped" means the CAP element and code value will be mapped into the appropriate CMAC attribute. "Reject" means the Alert Gateway will reject the CAP message received from the "B" interface and no message will be sent over the "C" interface. "Ignored" means the CAP element is not applicable to CMAM and will be ignored by the Alert Gateway. "Generated" means the Alert Gateway will generate the appropriate CMAC elements and attributes.

Column 4: Lists the corresponding "C" interface CMAC elements as defined in Section 10.4 below.

Table 10-1 Parameter mapping from "B" Interface CAP message in to "C" Interface CMAC message

CAP Element	(CMA) Permitted Values	Alert Gateway Filtering Rules	CMAC Element
N/A		Generated by the Alert Gateway	CMAC protocol version
N/A		Generated by the Alert Gateway	CMAC sending Alert Gateway id
alert	N/A	Ignored.	N/A
identifier (free format)		Mapped from the free format into a 2 octet binary number	CMAC_message_identifier (2 octet binary number)
sender		Pass	CMAC_sender
sent		Mapped into UTC format	CMAC_sent_date_time
status	"Actual" "Exercise" "System" "Test"	Pass with permitted values; Reject message with "Draft"	CMAC_status

msgType	"Alert" "Update" "Cancel" "Error"	Pass with permitted values; Reject message with "Ack"	CMAC_message_type
source	N/A	Ignored	
scope	"Public"	Reject message if "Public" is not in field.	N/A
restriction		Reject message if this element is included	N/A
addresses		Reject message if this element is included	N/A
code		Ignored	N/A
note		Pass	CMAC_cancel_error_node
references		Mapped from the free format into a 2 octet binary number	CMAC_referenced_message_identifier (2-octet binary number)
incidents	N/A	Ignored	N/A
N/A		Generated by the Alert Gateway	CMAC_original_cap_alert_uri
info		Ignored	
language		Pass	CMAC_text_language
category		Mapped	CMAC_category
event	N/A	Ignored	N/A
responseType	All but "Assess"	Reject message with "Assess" in field, pass all others	CMAC_response_type
urgency	"Immediate" "Expected"	Pass with permitted values or rejecting message with other values	CMAC_urgency
severity	"Extreme" "Severe"	Pass with permitted values or rejecting message with other values	CMAC_severity
certainty	"Observed" "Likely"	Pass with permitted values or rejecting message with other values	CMAC_certainty
audience	N/A	Ignored	N/A
eventCode	"EAN" "CAE"	Map "EAN" to "Presidential"; Map "CAE" to "Child Abduction"; Map other values to "No special handling"	CMAC_special_handling
eventCode		Mapped	CMAC_event_code
effective	N/A	Ignored	N/A
onset	N/A	Ignored	N/A

expires		Passed; Reject message if already expired; *Apply default value of one hour if* not provided	CMAC_expires_date_time
senderName		Mapped	CMAC_sender_name
headline		Passed conditionally when eventCode= "EAN" or "CAE"; Ignored when eventCode has other values.	CMAC_text_alert_message
description	N/A	Ignoring	CMAC_text_alert_message
N/A	ASCII 7-bit	Ignoring	CMAC_text_encoding
N/A	Less than 90 characters	Generated by the Alert Gateway	CMAC_text_message_length
N/A		Generated by the Alert Gateway as specified in Section 5.5	CMAC_text_alert_message
instruction	N/A	Ignored	N/A
web		Mapped to a local link on the Alert Gateway	CMAC_web_link
contact	N/A	Ignored	N/A
parameter	N/A	Passed conditionally when eventCode= "EAN" or "CAE"; Passed conditionally when eventCode has other values and parameter valueName = "CMAMtext"; Ignored otherwise	CMAC_text_alert_message
resource	N/A	Ignored	N/A
resourceDesc		Mapped	CMAC_resource_description
mimeType		Mapped	CMAC_mime_type
size		Mapped	CMAC_resource_size
uri		Mapped to a local link on the Alert Gateway	CMAC_uri
derefUri	N/A	Ignored	N/A
degest		Ignored	
area	N/A	Ignored	N/A
areaDesc		Passed	CMAC_area_description
polygon		Passed	CMAC_polygon
circle		Passed	CMAC_circle
geocode		Passed, or generated based on polygon and/or circle	CMAC_cmas_geocode
geocode		Generated based on polygon and/or circle	CMAC_cmas_gnis
altitude	N/A	Ignored	N/A

ceiling	N/A	Ignored	N/A

29. If an incoming CAP message fails the Alert Gateway validation or filtering rules, an error message will be sent over the "B" interface to the alert originator. The error message may contain additional information in the "note" element. The "note" element in the error response to the alert originator may contain multiple error messages. The following are some examples of error responses.

    a. CMA error #1: Unsupported code value of "<value> " in element "<element name>" (e.g. scope="Private")

    b. CMA error #2: Missing required element "<element name>" (e.g. element Y = eventCode)

    c. CMA error #3: Unsupported element "<element name>" (e.g. element Z = restriction)

    d. CMA error #4: Text message length exceeds maximum limit

10.4 Reference Point C Protocol

The C reference point is the interface from the Alert Gateway to the CMSP Gateway. The C reference point is used to map the CAP elements into the CMSP protocol on the C reference point ("CMAC"), as follows:

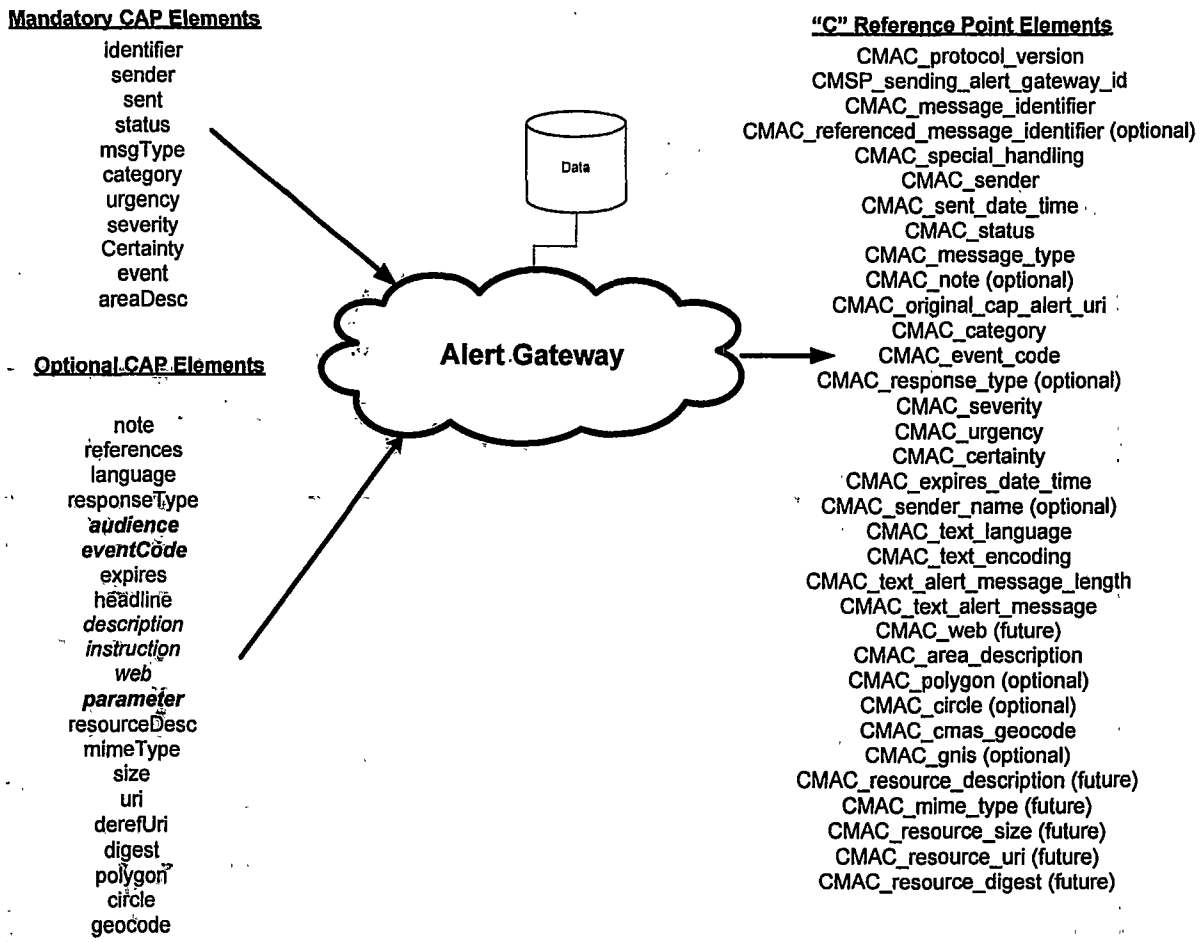

Figure 10-1 Relationship of CAP Elements to Reference Point C Elements

10.4.1 Structure of the CMA "C" Reference Point Protocol

The CMSAAC recommends that each CMAC Alert message consist of the following segments:

- CMAC Alert Attributes segment
- CMAC Alert Info segment
- CMAC Alert Area segment
- CMAC Alert Resource segment

The CMSAAC recommends that the CMAC Alert Message document object model be as follows:

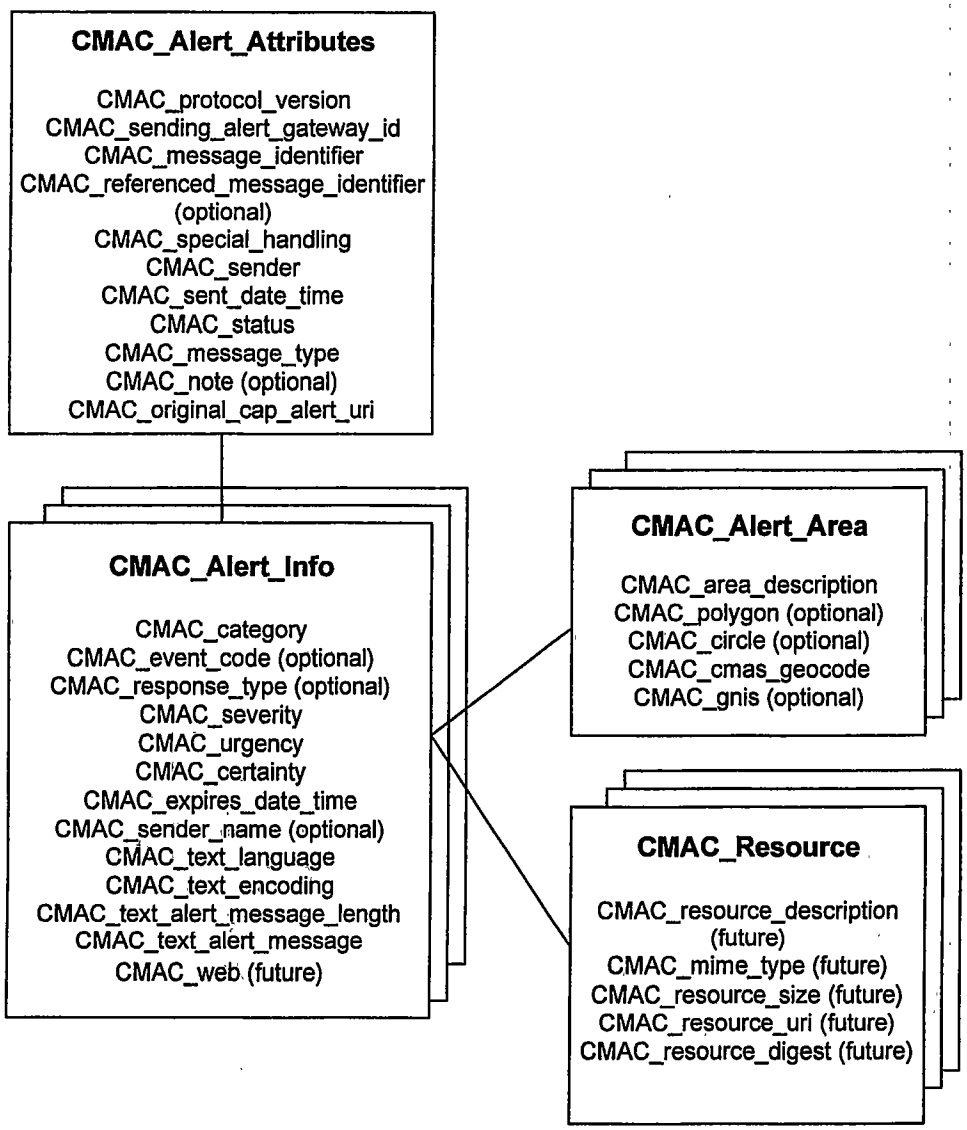

Figure 10-2 CMAC Message Structure

The CMSAAC recommends that a CMAC Alert Message must contain:

- one CMAC_Alert_Attributes segment
- one or more CMAC_Alert_Info segments
- one or more CMAC_Alert_Area segements.

The CMAC_Resource segment is optional for future use in streaming audio, streaming video, and multimedia CMAs.

10.4.2 CMAC Data Dictionary

10.4.2.1 CMAC_Alert_Attributes Segment

Table 10-2 CMAC_Alert_Attributes Segment

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_alert	M	(1) Surrounds CMAC alert message subelements. (2) MUST include the xmlns attribute referencing the CMAC URN as the namespace, e.g.: <cmac:CMAC_alert xmlns:cmac="urn:xxx:xxxxx:xx:cmac:1.0"> [sub-elements] </cmac:CMAC_alert> (3) In addition to the specified subelements, MAY contain one or more <CMAC_alert_info> blocks.
CMAC_protocol_version	M	The version of the CMAC protocol. Used by the CMSP Gateway only. Specified by the Alert Gateway.
CMAC_sending_alert_gateway_id	M	URI of the Alert Gateway sending the CMAC message. Specified by thet Alert Gateway.
CMAC_message_identifier	M	A 2-octet binary value uniquely identifying this message, assigned by the Alert Gateway and derived from the CAP identifier element. This element is sent to the mobile device.
CMAC_referenced_message_identifier	C	A 2-octet binary value uniquely identifying a referenced CMAM, assigned by the Alert Gateway. Required for an Update, Cancel or Ack CMAC_message_type. Derived from the CAP references element.

CMAC Element	**Mandatory/ Optional/** ***Conditional***	***CMAC Definition***
CMAC_special_handling	O	Specifies if this alert message requires special handling. Specified by the Alert Gateway, derived from CAP elements. Code Values: **"Presidential"** **"Child Abduction"** **"No Special Handling"**
CMAC_sender	M	Identifies the originator of this alert. Used by the CMSP for logging purposes only. 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 originator in UTC in XML dateTime format. Derived from the CAP sent element.
CMAC_status	M	Alert Gateway uses the CAP status element to populate this element. Code Values: **"Actual"** - Actionable by all targeted recipients **"Exercise"**- Actionable only by designated exercise participants, for CMSP use. **"System"** - For messages that support alert network internal functions. In addition this is used for the "keep alive" message between the Alert Gateway and the CMSP Gateway. **"Test"** - Technical testing of the C Reference Point only, for CMSP Gateway use only.

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_message_type	M	Alert Gateway uses the CAP msgType element to populate this element. Code Values: **"Alert"** - Initial information requiring attention by targeted recipients **"Update"** - Updates and supercedes the earlier message(s) identified in < CMAC_referenced_ message_identifier > **"Cancel"** - Cancels the earlier message(s) identified in < CMAC_ referenced_ message_ identifier > **"Ack"** - Acknowledges receipt and acceptance of the message(s) identified in < CMAC_referenced_ message_ identifier > additional explanation may appear in <CMAC_note> **"Error"** indicates rejection of the message(s) identified in < CMAC_referenced_ message_ identifier >; explanation SHOULD appear in <CMAC_note>
CMAC_note	O	Optional element. Used for CMSP logging purposes for a cancel or error message type, or to provide a response back to the Alert Gateway. Alert Gateway uses the CAP note element to populate this element on messages from the Alert Gateway to the CMSP Gateway. The CMSP Gateway uses this element on messages to the Alert Gateway.
CMAC_original_cap_alert_uri	M	This element contains the uri where the CMSP may retrieve the original complete CAP version of the alert from the Alert Gateway. Specified by the Alert Gateway.

10.4.2.2 CMAC_Alert_Info Segment

Multiple occurrences are permitted within the CAP from the alert originator; the CMSAAC recommends that each occurrence be a separate CMAM from the Alert Gateway. The CMSAAC further recommends that each language be sent as a separate CMAM with a unique message identifier. It is anticipated that a separate CMAS_Alert_Info element with associated sub-elements will be created for the CMAMs to be given to the CMSPs for broadcast via the CMSP selected technologies consistent with the requirements and procedures defined by the CMSAAC.

Table 10-3 CMAC_Alert_Info Segment

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition

CMAC Element	Mandatory/ *Optional/* Conditional	CMAC Definition
CMAC_alert_info		(1) Only a single occurrence is permitted within a single <CMAC_alert>. If there are multiple "info" segements in the original CAP message, the Alert Gateway shall format as separate CMAC messages each with a unique identifier. (2) In addition to the specified subelements, MAY contain one or more <CMAC_resource> blocks and/or one or more <CMAC_area> blocks.
CMAC_category	M	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_event_code	O	Alert Gateway uses the CAP eventCode element to populate this element. Optional element used by the CMSP Gateway only. A system-specific code for event typing, in the form: <CMAC_event_code> <CMAC_valueName>valueName</CMAC_valueName> <CMAC_value>value</CMAC_value> </CMAC_event_code> where the content of "CMAC_valueName" 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., CMAC_valueName ="SAME" and value="TOR"). Values of "CMAC_valueName" that are acronyms SHOULD be represented in all capital letters without periods (e.g., SAME).

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
		The following SAME codes are supported in CMAS: o Civil Danger Warning CDW o Civil Emergency Message CEM o Evacuation Immediate EVI o Hazardous Materials Warning HMW o Law Enforcement Warning LEW o Local Area Emergency LAE o Nuclear Power Plant Warning NUW o Radiological Hazard Warning RHW o Shelter in Place Warning SPW o Avalanche Warning AVW o Blizzard Warning BZW o Child Abduction Emergency CAE o Coastal Flood Warning CFW o Dust Storm Warning DSW o Earthquake Warning EQW o Fire Warning FRW o Flash Flood Warning FFW o Flood Warning FLW o High Wind Warning HWW o Hurricane Warning HUW o Severe Thunderstorm Warning SVR o Special Marine Warning SMW o Tornado Warning TOR o Tropical Storm Warning TRW o Tsunami Warning TSW o Volcano Warning VOW o Winter Storm Warning WSW
CMAC_response_type	O	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 **"Assess"** – Evaluate the information in this message. (This value SHOULD NOT be used in public warning applications.) **"None"** – No action recommended Multiple instances MAY occur within a single <CMAC_info> block. This element is passed to the mobile device.

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_severity	M	Alert Gateway uses the CAP severity element to populate this element. Code Values sent to the mobile device: **"Extreme"** - Extraordinary threat to life or property **"Severe"** - Significant threat to life or property
CMAC_urgency	M	Alert Gateway uses the CAP urgency element to populate this element. Code Values sent to the mobile device: **"Immediate"** - Responsive action SHOULD be taken immediately **"Expected"** - Responsive action SHOULD be taken soon (within next hour)
CMAC_certainty	M	Alert Gateway uses the CAP certainty element to populate this element. Code Values sent to the mobile device: **"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 is represented in UTC [dateTime] format. Maximum duration is 24 hours. 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. Alert Gateway uses the CAP senderName element to populate this element.
CMAC_text_language	M	Specifies the language of the text in the CMAC_text_alert_message, for use by the mobile device. Code Values: **"English"** **"Spanish"** **"French"** (future Canada use only) **"Other"** – for future use Specified by the Alert Gateway and derived from the CAP language element.
CMAC_text_encoding	M	Specifies the data encoding scheme of the text in the CMAC_text_alert_message, for use by the mobile device. Code Values: **"UTF-8"** Specified by the Alert Gateway.

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_text_alert_message_length	M	The length, in characters, of the text in the CMAC_text_alert_message. Note the number of octets in the CMAC_text_alert_message can be derived from this parameter and the CMAC_text_encoding parameter. Specified by the Alert Gateway.
CMAC_text_alert_message	M	The text of the alert message for use by the mobile device. This field is defined by the CMAS Text Profile and may contain up to 90 English characters using a 7-bit encoding scheme. Other languages or data encoding schemes will change the number of characters supported. Specified by the Alert Gateway, which may be derived or obtained via CAP elements.
CMAC_web_link	O	Optional element for future use. The identifier of the hyperlink associating additional information with the alert message. This data must be in a domain accessible by the CMSP Gateway. Alert Gateway uses the CAP web element to populate this element.

10.4.2.3 CMAC_Area Segment:

Multiple occurrences are permitted

Table 10-4 CMAC_Area Segment

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_area	M	(1) Multiple occurrences permitted, in which case the target area for the <CMAC_alert_info> block is the union of all the included <CMAC_area> blocks. (2) MAY contain one or multiple instances of <CMAC_polygon> or <CMAC_circle>, and shall contain at least one instance of <CMAC_geocode>. If multiple <CMAC_polygon>, <CMAC_circle> or <CMAC_geocode> elements are included, the area described by this <area> is the union of those represented by the included elements.
CMAC_area_description	M	The text describing the affected area of the alert message for use by the CMSP for logging purposes only. Alert Gateway uses the CAP areaDesc element to populate this element.
CMAC_polygon	O	Optional element. The paired values of points defining a polygon that delineates the affected area of the alert message. Alert Gateway uses the CAP polygon element to populate this element.

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_circle	O	Optional element. The paired values of a point and radius delineating the affected area of the alert message. Alert Gateway uses the CAP circle element to populate this element.
CMAC_cmas_geocode	M	The CMAS-defined geographic code delineating the affected area of the alert message. This is an extension to the FIPS code (see Section 10.4.5). Alert Gateway uses the CAP geocode, polygon, circle, and/or sender elements to derive this element.
CMSC_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 Alert Gateway.

10.4.2.4 CMAC_Resource Segment:

Multiple occurrences are permitted. The CMAC_Resource segment is not used for the Text Profile but may be applicable to future streaming audio, streaming video, and multimedia alerts.

Table 10-5 CMAC_Resource Segment

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_resource	O	(1) Refers to an additional file with supplemental information related to this <CMAC_alert_info> element; e.g., an image or audio file (2) Multiple occurrences MAY occur within a single <CMAC_alert_info> block
CMAC_resource_description	O	Optional element. The human-readable text describing the content and kind, such as "map" or "photo," of the resource file. For use by the CMSP Gateway for logging purposes only. Alert Gateway uses the CAP resourceDesc element to populate this element.
CMAC_mime_type	O	Optional element. The identifier of the MIME content type and sub-type describing the resource file. Alert Gateway uses the CAP mimeType element to populate this element.
CMAC_resource_size	O	Optional element. The integer indicating the size of the resource file. Alert Gateway uses the CAP size element to populate this element.

CMAC Element	Mandatory/ Optional/ Conditional	CMAC Definition
CMAC_resource_uri	O	Optional element. The identifier of the hyperlink for the resource file. Alert Gateway uses the CAP uri element to populate this element.
CMAC_digest	O	Optional element. The code representing the digital digest ("hash") computed from the resource file. Calculated using the Secure Hash Algorithm (SHA-1) per [FIPS 180-2]. Alert Gateway uses the CAP digest element to populate this element.

10.4.3 Example CMAC XML Schema

```
<?xml version = "1.0" encoding = "UTF-8"?>
<schema xmlns = "http://www.w3.org/2001/XMLSchema"
    targetNamespace = "cmac:1.0"
    xmlns:cmac = "cmac:1.0"
    xmlns:xs = "http://www.w3.org/2001/XMLSchema"
    elementFormDefault = "qualified"
    attributeFormDefault = "unqualified">
  <element name = "CMAC_Alert_Attributes">
    <annotation>
      <documentation>CMAC Alert Message (version 1.0)</documentation>
    </annotation>
    <complexType>
      <sequence>
        <element name = "CMAC_protocol_version" type = "string"/>
        <element name = "CMAC_sending_alert_gateway_id" type = "anyURI"/>
        <element name = "CMAC_message_identifier" type = "string"/>
        <element name = "CMAC_referenced_message_identifier" type = "string" minOccurs = "0" />
        <element name = "CMAC_special_handling">
          <simpleType>
            <restriction base = "string">
              <enumeration value = "Presidential"/>
              <enumeration value = "Child Abduction"/>
              <enumeration value = "No Special Handling"/>
            </restriction>
          </simpleType>
        </element>
        <element name = "CMAC_sender" type = "string"/>
        <element name = "CMAC_sent_date_time" type = "dateTime"/>
        <element name = "CMAC_status">
          <simpleType>
            <restriction base = "string">
              <enumeration value = "Actual"/>
              <enumeration value = "Exercise"/>
              <enumeration value = "System"/>
              <enumeration value = "Test"/>
            </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"/>
    </restriction>
  </simpleType>
<element name = "CMAC_note" type = "string" minOccurs = "0"/>
<element name = "CMAC_original_cap_alert_uri" type = "anyURI"/>
</element>
<element name = "CMAC_alert_info" minOccurs = "0">
  <complexType>
    <sequence>
      <element name = "category" maxOccurs = "unbounded">
        <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_event_code" minOccurs = "0" maxOccurs = "unbounded">
        <complexType>
          <sequence>
            <element ref = "cmac:valueName"/>
            <element ref = "cmac:value"/>
          </sequence>
        </complexType>
      </element>
      <element name = "CMAC_responseType" maxOccurs = "unbounded">
        <simpleType>
          <restriction base = "string">
            <enumeration value = "Shelter"/>
            <enumeration value = "Evacuate"/>
            <enumeration value = "Prepare"/>
            <enumeration value = "Execute"/>
            <enumeration value = "Monitor"/>
            <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" minOccurs = "0"/>
      <element name = "CMAC_sender_name" type = "string" minOccurs = "0"/>
      <element name = "CMAC_text_language" />
        <simpleType>
          <restriction base = "string">
            <enumeration value = "English"/>
            <enumeration value = "Spanish"/>
            <enumeration value = "French"/>
            <enumeration value = "Other"/>
          </restriction>
        </simpleType
      <element name = "CMAC_text_encoding" />
        <simpleType>
          <restriction base = "string">
            <enumeration value = " UTF-8"/>
          </restriction>
        </simpleType
      </element>
      <element name = "CMAC_text_alert_message_length" type = "string" />
      <element name = "CMAC_text_alert_message" type = "string" />
      <element name = "CMAC_web" type = "anyURI" minOccurs = "0"/>
      <element name = "CMAC_alert_resource" minOccurs = "0" maxOccurs = "unbounded" >
      <complexType>
        <sequence>
          <element name = "CMAC_resource_desciption" type = "string"/>
          <element name = "CMAC_mime_type" type = "string" minOccurs = "0"/>
          <element name = "CMAC_resource_size" type = "integer" minOccurs = "0"/>
          <element name = "CMAC_resource_uri" type = "anyURI" minOccurs = "0"/>
          <element name = "CMAC_digest" type = "string" minOccurs = "0"/>
        </sequence>
      </complexType>
      </element>
      <element name = "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_cmac_geocode" type="string" maxOccurs = "unbounded">
                <element name = "CMAC_gnis" type = "string" minOccurs = "0" maxOccurs = "unbounded"/>
                </element>
              </sequence>
            </complexType>
          </element>
        </sequence>
      </complexType>
    </element>
    </sequence>
  </complexType>
</element>
<element name = "valueName" type = "string"/>
<element name = "value" type = "string"/>
</schema>
```

10.4.4 Element Mapping from B Reference Point (CAP) to C Reference Point (CMAC) to E Reference Point (CMAE) Elements

Note: elements listed in **bold** are mandatory.

Table 10-6 Mapping Reference Point B Elements to Reference Point C Elements

CAP Element	CMAC Element	CMAE Element
N/A	**CMAC_protocol_version**	N/A
N/A	N/A	**CMAE_protocol_version**
N/A	**CMAC_sending_alert_gateway_id**	N/A
identifier	**CMAC_message_identifier**	**CMAE_identifier**
references	CMAC_referenced_message_identifier	N/A
N/A	CMAC_special_handling	**CMAE_alert_handling**
sender	**CMAC_sender**	N/A
sent	**CMAC_sent_date_time**	N/A
status	**CMAC_status**	N/A
msgType	**CMAC_message_type**	**CMAE_alert_type**
source	N/A	N/A
scope	N/A	N/A
restriction	N/A	N/A
code	N/A	N/A

CAP Element	CMAC Element	CMAE Element
note	CMAC_ note	N/A
incidents	N/A	N/A
N/A	**CMAC_original_cap_alert_uri**	N/A
category	**CMAC_category**	**CMAE_category**
event	N/A	N/A
eventCode	CMAC_event_code	N/A
responseType	CMAC_response_type	**CMAE_response_type**
severity	**CMAC_severity**	**CMAE_severity**
urgency	**CMAC_urgency**	**CMAE_urgency**
certainty	**CMAC_certainty**	**CMAE_certainty**
audience	N/A	N/A
effective	N/A	N/A
onset	N/A	N/A
expires	**CMAC_expires_date_time**	**CMAE_expires**
senderName	CMAC_sender_name	N/A
language	**CMAC_text_language**	**CMAE_language**
N/A	**CMAC_text_encoding**	**CMAE_char_set**
N/A	**CMAC_text_alert_message_length**	**CMAE_alert_text_length**
parameter (when value = "CMAMtext")	**CMAC_text_alert_message**	**CMAE_alert_text**
headline	N/A	N/A
description	N/A	N/A
instruction	N/A	N/A
web	CMAC_web_link	N/A
contact	N/A	N/A
parameter (when value not = "CMAMtext")	N/A	N/A
areaDesc	**CMAC_area_description**	N/A
polygon	CMAC_polygon	N/A
circle	CMAC_circle	N/A
geocode	**CMAC_cmas_geocode**	N/A
geocode	CMSC_gnis	N/A
altitude	N/A	N/A
ceiling	N/A	N/A
resourceDesc	CMAC_resource_description	N/A
mimeType	CMAC_mime_type	N/A

CAP Element	CMAC Element	CMAE Element
size	CMAC_resource_size	N/A
uri	CMAC_resource_uri	N/A
derefUri	N/A	N/A
digest	CMAC_digest	N/A
N/A	N/A	CMAE_associated_multimedia_indicator
N/A	N/A	CMAE_CMSP_defined_parameter
N/A	N/A	CMAE_reserved

10.4.5 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 CMSAAC recommends that the CMAC_cmas_geocode be assigned as follows:

1. The CMAC_cmas_geocode indication for a specific county will be as defined in Federal Information Processing Standard 6-4 (FIPS 6-4), titled "Counties and Equivalent Entities of the United States, Its Possessions, and Associated Areas", dated 31 August 1990.

2. The CMAC_cmas_geocode indication for an entire state will be the two digit FIPS State Numeric Code as defined in Federal Information Processing Standard 5-2 (FIPS 5-2), titled "Codes for the Identification of the States, the District of Columbia and the Outlying Areas of the United States, and Associated Areas", dated 28 May 1987 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 US000.

4. In the future, it is possible that alerts may be targeted for regions of the country (e.g., Gulf States). The more efficient and error resistant solution would be to have CMAC_cmas_geocode values for regional areas such as FEMA regions or National Weather Service (NWS) regions. The FEMA regions would be assigned values in the format of US0xx and the NWS regions would be assigned values in the format of US1xx.