



Common Alerting Protocol Version 1.2

Public Review Draft 02

29 September 2009

Specification URIs:

This Version:

<http://docs.oasis-open.org/emergency/cap/v1.2/pr02/CAP-v1.2-PR02.html>
<http://docs.oasis-open.org/emergency/cap/v1.2/pr02/CAP-v1.2-PR02.pdf>
<http://docs.oasis-open.org/emergency/cap/v1.2/pr02/CAP-v1.2-PR02.doc> (Authoritative)

Previous Version:

<http://docs.oasis-open.org/emergency/cap/v1.2/pr01/CAP-v1.2-PR01.html>
<http://docs.oasis-open.org/emergency/cap/v1.2/pr01/CAP-v1.2-PR01.pdf>
<http://docs.oasis-open.org/emergency/cap/v1.2/pr01/CAP-v1.2-PR01.doc> (Authoritative)

Latest Version:

<http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.html>
<http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.pdf>
<http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.doc> (Authoritative)

Technical Committee:

OASIS Emergency Management TC

Chair:

Elysa Jones, Warning Systems, Inc.

Editor:

Jacob Westfall, Individual

Related work:

This specification is related to:

- OASIS Standard CAP-V1.1, October 2005 http://www.oasis-open.org/committees/download.php/15135/emergency-CAPv1.1-Corrected_DOM.pdf
- OASIS Standard CAP-V1.1, Approved Errata October 2007 <http://docs.oasis-open.org/emergency/cap/v1.1/errata/CAP-v1.1-errata.pdf>

Declared XML Namespace:

urn:oasis:names:tc:emergency:cap:1.2

Abstract:

The Common Alerting Protocol (CAP) is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. CAP also facilitates the detection of emerging patterns in local warnings of various kinds, such as might indicate an undetected hazard or hostile act. And CAP provides a template for effective warning messages based on best practices identified in academic research and real-world experience.

Status:

This document was last revised or approved by the Emergency Management TC on the above date. The level of approval is also listed above. Check the "Latest Version" or "Latest Approved Version" location noted above for possible later revisions of this document.

Technical Committee members should send comments on this specification to the Technical Committee's email list. Others should send comments to the Technical Committee by using the "Send A Comment" button on the Technical Committee's web page at <http://www.oasis-open.org/committees/emergency/>.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Technical Committee web page (<http://www.oasis-open.org/committees/emergency/ipr.php>).

The non-normative errata page for this specification is located at <http://www.oasis-open.org/committees/emergency/>.

Notices

Copyright © OASIS® 2009. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The names "OASIS" and "CAP" are trademarks of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see <http://www.oasis-open.org/who/trademark.php> for above guidance.

Table of Contents

1	Introduction	6
1.1	Purpose.....	6
1.2	History.....	6
1.3	Structure of the CAP Alert Message.....	7
1.3.1	<alert>	7
1.3.2	<info>.....	7
1.3.3	<resource>	7
1.3.4	<area>	7
1.4	Applications of the CAP Alert Message.....	7
1.5	Terminology	8
1.6	Normative References	8
2	Design Principles and Concepts (non-normative)	9
2.1	Design Philosophy	9
2.2	Requirements for Design	9
2.3	Examples of Use Scenarios.....	10
2.3.1	Manual Origination	10
2.3.2	Automated Origination by Autonomous Sensor System	10
2.3.3	Aggregation and Correlation on Real-time Map.....	10
2.3.4	Integrated Public Alerting	11
2.3.5	Repudiating a False Alarm	11
3	Alert Message Structure (normative).....	12
3.1	Document Object Model	12
3.2	Data Dictionary	13
3.2.1	"alert" Element and Sub-elements	13
3.2.2	"info" Element and Sub-elements.....	16
3.2.3	"resource" Element and Sub-elements	23
3.2.4	"area" Element and Sub-elements	24
3.3	Implementation Notes	27
3.3.1	WGS 84 Note	27
3.3.2	DateTime Data Type	27
3.3.3	Character Entity References	27
3.3.4	Security Note	27
3.3.4.1	Digital Signatures.....	28
3.3.4.2	Encryption	28
3.4	XML Schema	28
3.5	Use of ASN.1 to Specify and Encode the CAP Alert Message	32
3.5.1	General.....	32
3.5.2	Formal Mappings and Specification	32
3.5.3	ASN.1 Schema	32
4	Conformance (normative).....	37
4.1	Conformance Targets	37
4.2	Conformance as a CAP V1.2 Message.....	37
4.3	Conformance as a CAP V1.2 Message Producer	37

4.4 Conformance as a CAP V1.2 Message Consumer	38
Appendix A. CAP Alert Message Example	39
A.1. Homeland Security Advisory System Alert.....	39
A.2. Severe Thunderstorm Warning	40
A.3. Earthquake Report (Update Message)	41
A.4. AMBER Alert (Multilingual Message)	42
Appendix B. Acknowledgments	43
OASIS Emergency Management Technical Committee	43
Appendix C. Revision History.....	45

1 Introduction

1.1 Purpose

The Common Alerting Protocol (CAP) provides an open, non-proprietary digital message format for all types of alerts and notifications. It does not address any particular application or telecommunications method. The CAP format is compatible with emerging techniques, such as Web services, as well as existing formats including the Specific Area Message Encoding (SAME) used for the United States' National Oceanic and Atmospheric Administration (NOAA) Weather Radio and the Emergency Alert System (EAS), while offering enhanced capabilities that include:

- Flexible geographic targeting using latitude/longitude shapes and other geospatial representations in three dimensions;
- Multilingual and multi-audience messaging;
- Phased and delayed effective times and expirations;
- Enhanced message update and cancellation features;
- Template support for framing complete and effective warning messages;
- Compatible with digital encryption and signature capability; and,
- Facility for digital images and audio.

Key benefits of CAP will include reduction of costs and operational complexity by eliminating the need for multiple custom software interfaces to the many warning sources and dissemination systems involved in all-hazard warning. The CAP message format can be converted to and from the "native" formats of all kinds of sensor and alerting technologies, forming a basis for a technology-independent national and international "warning internet."

1.2 History

The National Science and Technology Council report on "Effective Disaster Warnings" released in November, 2000 recommended that "a standard method should be developed to collect and relay instantaneously and automatically all types of hazard warnings and reports locally, regionally and nationally for input into a wide variety of dissemination systems."

An international working group of more than 130 emergency managers and information technology and telecommunications experts convened in 2001 and adopted the specific recommendations of the NSTC report as a point of departure for the design of a Common Alerting Protocol (CAP). Their draft went through several revisions and was tested in demonstrations and field trials in Virginia (supported by the ComCARE Alliance) and in California (in cooperation with the California Office of Emergency Services) during 2002 and 2003.

In 2002 the CAP initiative was endorsed by the national non-profit Partnership for Public Warning, which sponsored its contribution in 2003 to the OASIS standards process. In 2004, CAP version 1.0 was adopted as an OASIS Standard. In 2005, changes based on user feedback were incorporated into CAP and version 1.1 was released. As part of the International Telecommunication Union (ITU-T) adoption of CAP, a CAP 1.1 Errata was released in 2007 to support ASN.1 encoding. Version 1.2 is a minor release to resolve issues identified by the EM-TC CAP Call for Comments initiated in April 2008 and also incorporates feedback from CAP profile development efforts.

42 **1.3 Structure of the CAP Alert Message**

43 Each CAP Alert Message consists of an <alert> segment, which may contain one or more <info>
44 segments, each of which may include one or more <area> and/or <resource> segments. Under most
45 circumstances CAP messages with a <msgType> value of “Alert” SHOULD include at least one <info>
46 element. (See the document object model diagram in section 3.1, below.)

47 **1.3.1 <alert>**

48 The <alert> segment provides basic information about the current message: its purpose, its source and
49 its status, as well as a unique identifier for the current message and links to any other, related messages.
50 An <alert> segment may be used alone for message acknowledgements, cancellations or other system
51 functions, but most <alert> segments will include at least one <info> segment.

52 **1.3.2 <info>**

53 The <info> segment describes an anticipated or actual event in terms of its urgency (time available to
54 prepare), severity (intensity of impact) and certainty (confidence in the observation or prediction), as well
55 as providing both categorical and textual descriptions of the subject event. It may also provide
56 instructions for appropriate response by message recipients and various other details (hazard duration,
57 technical parameters, contact information, links to additional information sources, etc.) Multiple <info>
58 segments may be used to describe differing parameters (e.g., for different probability or intensity “bands”)
59 or to provide the information in multiple languages.

60 **1.3.3 <resource>**

61 The <resource> segment provides an optional reference to additional information related to the <info>
62 segment within which it appears in the form of a digital asset such as an image or audio file.

63 **1.3.4 <area>**

64 The <area> segment describes a geographic area to which the <info> segment in which it appears
65 applies. Textual and coded descriptions (such as postal codes) are supported, but the preferred
66 representations use geospatial shapes (polygons and circles) and an altitude or altitude range, expressed
67 in standard latitude / longitude / altitude terms in accordance with a specified geospatial datum.

68 **1.4 Applications of the CAP Alert Message**

69 The primary use of the CAP Alert Message is to provide a single input to activate all kinds of alerting and
70 public warning systems. This reduces the workload associated with using multiple warning systems while
71 enhancing technical reliability and target-audience effectiveness. It also helps ensure consistency in the
72 information transmitted over multiple delivery systems, another key to warning effectiveness.

73 A secondary application of CAP is to normalize warnings from various sources so they can be aggregated
74 and compared in tabular or graphic form as an aid to situational awareness and pattern detection.

75 Although primarily designed as an interoperability standard for use among warning systems and other
76 emergency information systems, the CAP Alert Message can be delivered directly to alert recipients over
77 various networks, including data broadcasts. Location-aware receiving devices could use the information
78 in a CAP Alert Message to determine, based on their current location, whether that particular message
79 was relevant to their users.

80 The CAP Alert Message can also be used by sensor systems as a format for reporting significant events
81 to collection and analysis systems and centers.

82

83 1.5 Terminology

84 The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD
85 NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described
86 in [RFC2119].

87 The words *warning*, *alert* and *notification* are used interchangeably throughout this document.

88 The term “coordinate pair” is used in this document to refer to a comma-delimited pair of decimal values
89 describing a geospatial location in degrees, unprojected, in the form “[latitude],[longitude]”. Latitudes in
90 the Southern Hemisphere and longitudes in the Western Hemisphere are signed negative by means of a
91 leading dash.

92 1.6 Normative References

- 93 [RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,
94 <http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.
- 95 [dateTime] N. Freed, XML Schema Part 2: Datatypes Second Edition,
96 <http://www.w3.org/TR/xmlschema-2/#dateTime>, W3C REC-xmlschema-2,
97 October 2004.
- 98 [FIPS 180-2] National Institute for Standards and Technology, Secure Hash Standard,
99 <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf>,
100 August 2002.
- 101 [namespaces] T. Bray, Namespaces in XML, <http://www.w3.org/TR/REC-xml-names/>, W3C
102 REC-xml-names-19990114, January 1999.
- 103 [RFC2046] N. Freed, Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types,
104 <http://www.ietf.org/rfc/rfc2046.txt>, IETF RFC 2046, November 1996.
- 105 [RFC2119] S. Bradner, Key words for use in RFCs to Indicate Requirement Levels,
106 <http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.
- 107 [RFC3066] H. Alvestrand, Tags for the Identification of Languages,
108 <http://www.ietf.org/rfc/rfc3066.txt>, IETF RFC 3066, January 2001.
- 109 [WGS 84] National Geospatial Intelligence Agency, Department of Defense World Geodetic
110 System 1984, http://earth-info.nga.mil/GandG/tr8350_2.html, NGA Technical
111 Report TR8350.2, January 2000.
- 112 [XML 1.0] T. Bray, Extensible Markup Language (XML) 1.0 (Third Edition),
113 <http://www.w3.org/TR/REC-xml/>, W3C REC-XML-20040204, February 2004.
- 114 [XMLSIG] Eastlake, D., Reagle, J. and Solo, D. (editors), *XML-Signature Syntax and*
115 *Processing*, <http://www.w3.org/TR/2002/REC-xmlsig-core-20020212/>, W3C
116 Recommendation, February 2002.
- 117 [XMLENC] Eastlake, D. and Reagle, J. (editors), *XML Encryption Syntax and Processing*,
118 <http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/>, W3C
119 Recommendation, December 2002.
- 120 [ITU-T X.680] ITU-T Recommendation X.680, *Information technology – Abstract Syntax*
121 *Notation One (ASN.1): Specification of basic notation*.
- 122 [ITU-T X.691] ITU-T Recommendation X.691, *Information technology – ASN.1 encoding rules:*
123 *Specification of Packed Encoding Rules (PER)*.
- 124 [ITU-T X.693] ITU-T Recommendation X.693, *Information technology – ASN.1 encoding rules:*
125 *Specification of XML Encoding Rules (XER)*.
- 126 [ITU-T X.694] ITU-T Recommendation X.694, *Information technology – ASN.1 encoding rules:*
127 *Mapping W3C XML schema definitions into ASN.1*.
- 128

129 2 Design Principles and Concepts (non-normative)

130 2.1 Design Philosophy

131 Among the principles which guided the design of the CAP Alert Message were:

- 132 • **Interoperability** – First and foremost, the CAP Alert Message should provide a means for
133 interoperable exchange of alerts and notifications among all kinds of emergency information
134 systems.
- 135 • **Completeness** – The CAP Alert Message format should provide for all the elements of an
136 effective public warning message.
- 137 • **Simple implementation** – The design should not place undue burdens of complexity on
138 technical implementers.
- 139 • **Simple XML and portable structure** – Although the primary anticipated use of the CAP Alert
140 Message is as an XML document, the format should remain sufficiently abstract to be adaptable
141 to other coding schemes.
- 142 • **Multi-use format** – One message schema supports multiple message types (e.g., alert / update /
143 cancellations / acknowledgements / error messages) in various applications (actual / exercise /
144 test / system message).
- 145 • **Familiarity** – The data elements and code values should be meaningful to warning originators
146 and non-expert recipients alike.
- 147 • **Interdisciplinary and international utility** – The design should allow a broad range of
148 applications in public safety and emergency management and allied applications and should be
149 applicable worldwide.

150 2.2 Requirements for Design

151 Note: The following requirements were used as a basis for design and review of the CAP
152 Alert Message format. This list is non-normative and not intended to be exhaustive.

153 The Common Alerting Protocol SHOULD:

- 154 • Provide a specification for a simple, extensible format for digital representation of warning
155 messages and notifications;
- 156 • Enable integration of diverse sensor and dissemination systems;
- 157 • Be usable over multiple transmission systems, including both TCP/IP-based networks and one-
158 way "broadcast" channels;
- 159 • Support credible end-to-end authentication and validation of all messages;
- 160 • Provide a unique identifier (e.g., an ID number) for each warning message and for each message
161 originator;
- 162 • Provide for multiple message types, such as:
 - 163 – Warnings
 - 164 – Acknowledgements
 - 165 – Expirations and cancellations
 - 166 – Updates and amendments
 - 167 – Reports of results from dissemination systems
 - 168 – Administrative and system messages
- 169 • Provide for multiple message types, such as:

- 170 – Geographic targeting
- 171 – Level of urgency
- 172 – Level of certainty
- 173 – Level of threat severity
- 174 • Provide a mechanism for referencing supplemental information (e.g., digital audio or image files,
175 additional text);
- 176 • Use an established open-standard data representation;
- 177 • Be based on a program of real-world cross-platform testing and evaluation;
- 178 • Provide a clear basis for certification and further protocol evaluation and improvement; and,
- 179 • Provide a clear logical structure that is relevant and clearly applicable to the needs of emergency
180 response and public safety users and warning system operators.

181 **2.3 Examples of Use Scenarios**

182 Note: The following examples of use scenarios were used as a basis for design and
183 review of the CAP Alert Message format. These scenarios are non-normative and not
184 intended to be exhaustive or to reflect actual practices.

185 **2.3.1 Manual Origination**

186 The Incident Commander at an industrial fire with potential of a major explosion decides to issue a public
187 alert with three components: a) An evacuation of the area within half a mile of the fire; b) a shelter-in-
188 place instruction for people in a polygon roughly describing a downwind dispersion 'plume' extending
189 several miles downwind and half a mile upwind from the fire; and c) a request for all media and civilian
190 aircraft to remain above 2500 feet above ground level when within a half mile radius of the fire.

191 Using a portable computer and a web page (and a pop-up drawing tool to enter the polygon) the Incident
192 Commander issues the alert as a CAP message to a local alerting network.

193 **2.3.2 Automated Origination by Autonomous Sensor System**

194 A set of automatic tsunami warning sirens has been installed along a popular Northwest beach. A
195 wireless network of sensor devices collocated with the sirens controls their activation. When triggered,
196 each sensor generates a CAP message containing its location and the sensed data at that location that is
197 needed for the tsunami determination. Each siren activates when the combination of its own readings and
198 those reported at by other devices on the network indicate an immediate tsunami threat. In addition, a
199 network component assembles a summary CAP message describing the event and feeds it to regional
200 and national alerting networks.

201 **2.3.3 Aggregation and Correlation on Real-time Map**

202 At the State Operations Center a computerized map of the state depicts, in real time, all current and
203 recent warning activity throughout the state. All major warning systems in the state – the Emergency
204 Alert System, siren systems, telephone alerting and other systems – have been equipped to report the
205 details of their activation in the form of a CAP message. (Since many of them are now activated by way
206 of CAP messages, this is frequently just a matter of forwarding the activation message to the state
207 center.)

208 Using this visualization tool, state officials can monitor for emerging patterns of local warning activity and
209 correlate it with other real time data (e.g., telephone central office traffic loads, 9-1-1 traffic volume,
210 seismic data, automatic vehicular crash notifications, etc.).

211

212 **2.3.4 Integrated Public Alerting**

213 As part of an integrated warning system funded by local industry, all warning systems in a community can
214 be activated simultaneously by the issuance, from an authorized authority, of a single CAP message.

215 Each system converts the CAP message data into the form suitable for its technology (text captioning on
216 TV, synthesized voice on radio and telephone, activation of the appropriate signal on sirens, etc.).

217 Systems that can target their messages to particular geographic areas implement the targeting specified
218 in the CAP message with as little 'spillover' as their technology permits.

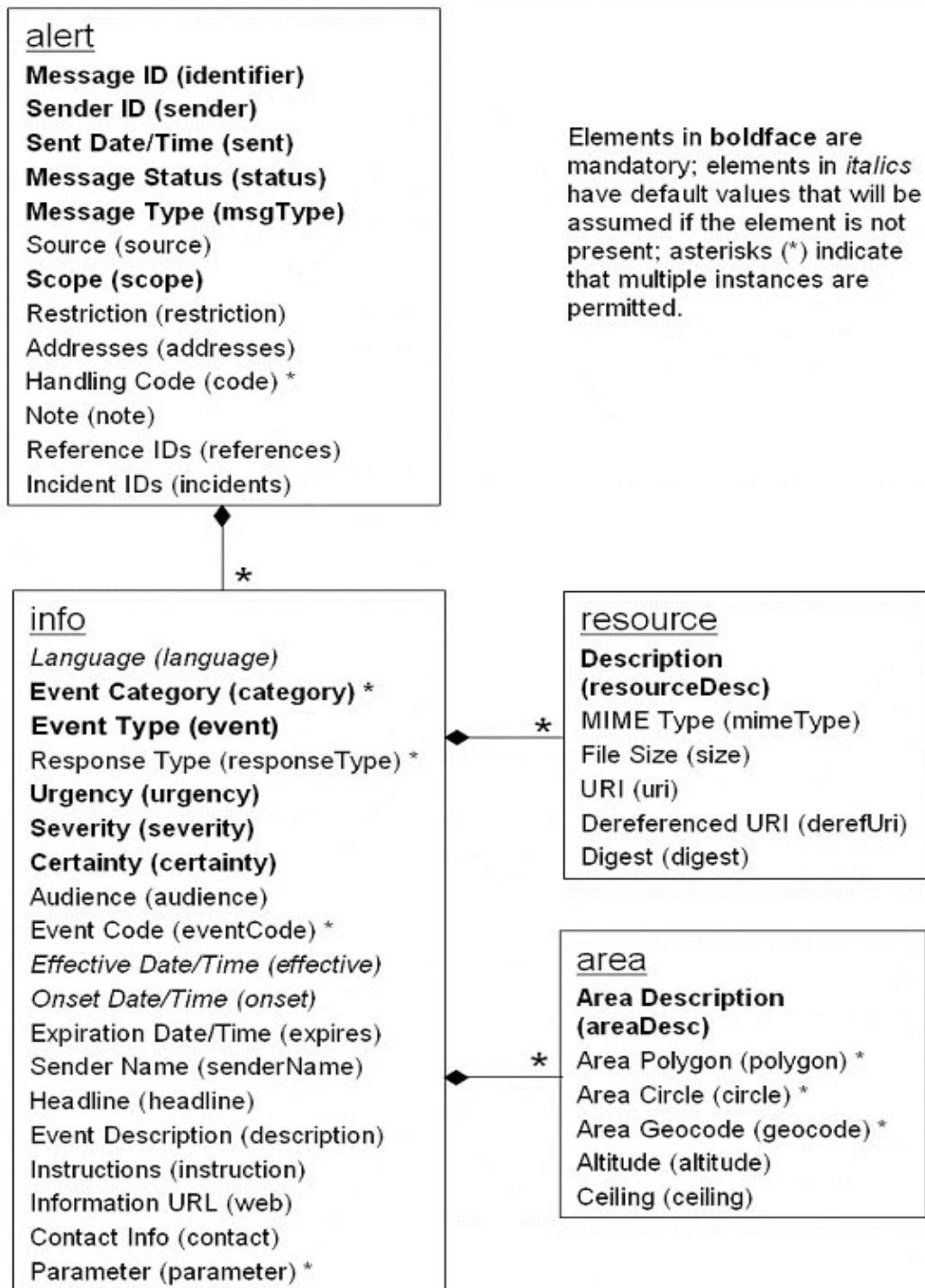
219 In this way, not only is the reliability and reach of the overall warning system maximized, but citizens also
220 get corroboration of the alert through multiple channels, which increases the chance of the warning being
221 acted upon.

222 **2.3.5 Repudiating a False Alarm**

223 Inadvertently the integrated alerting network has been activated with an inaccurate warning message.
224 This activation comes to officials' attention immediately through their own monitoring facilities (e.g., 2.3.3
225 above). Having determined that the alert is, in fact, inappropriate, the officials issue a cancellation
226 message that refers directly to the erroneous prior alert. Alerting systems that are still in the process of
227 delivering the alert (e.g., telephone dialing systems) stop doing so. Broadcast systems deliver the
228 cancellation message. Other systems (e.g., highway signs) simply reset to their normal state.

3 Alert Message Structure (normative)

3.1 Document Object Model



234 **3.2 Data Dictionary**

235 Note: Unless explicitly constrained within this Data Dictionary or the XML Schema
 236 (Section 3.4), CAP elements MAY have null values. Implementers MUST check for this
 237 condition wherever it might affect application performance.

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
3.2.1 "alert" Element and Sub-elements			
alert	cap. alert. group	The container for all component parts of the alert message (REQUIRED)	(1) Surrounds CAP alert message sub-elements. (2) MUST include the xmlns attribute referencing the CAP URN as the namespace, e.g.: <pre><cap:alert xmlns:cap="urn:oasis:names:tc:emergency:cap:1.2"> [sub-elements] </cap:alert></pre> (3) In addition to the specified sub-elements, MAY contain one or more <info> blocks.
identifier	cap. alert. identifier. identifier	The identifier of the alert message (REQUIRED)	(1) A number or string uniquely identifying this message, assigned by the sender. (2) MUST NOT include spaces, commas or restricted characters (< and &).
sender	cap. alert. sender. identifier	The identifier of the sender of the alert message (REQUIRED)	(1) Identifies the originator of this alert. Guaranteed by assigner to be unique globally; e.g., may be based on an Internet domain name. (2) MUST NOT include spaces, commas or restricted characters (< and &).
sent	cap. alert. sent. time	The time and date of the origination of the alert message (REQUIRED)	(1) The date and time SHALL be represented in the DateTime Data Type (See Implementation Notes) format (e.g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT). (2) Alphabetic timezone designators such as "Z" MUST NOT be used. The timezone for UTC MUST be represented as "-00:00".

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
status	cap. alert. status. code	The code denoting the appropriate handling of the alert message (REQUIRED)	Code Values: "Actual" - Actionable by all targeted recipients "Exercise" - Actionable only by designated exercise participants; exercise identifier SHOULD appear in <note> "System" - For messages that support alert network internal functions "Test" - Technical testing only, all recipients disregard "Draft" – A preliminary template or draft, not actionable in its current form
msgType	cap. alert. msgType. code	The code denoting the nature of the alert message (REQUIRED)	Code Values: "Alert" - Initial information requiring attention by targeted recipients "Update" - Updates and supercedes the earlier message(s) identified in <references> "Cancel" - Cancels the earlier message(s) identified in <references> "Ack" - Acknowledges receipt and acceptance of the message(s) identified in <references> "Error" - Indicates rejection of the message(s) identified in <references>; explanation SHOULD appear in <note>
source	cap. alert. source. identifier	The text identifying the source of the alert message (OPTIONAL)	The particular source of this alert; e.g., an operator or a specific device.
scope	cap. alert. scope. code	The code denoting the intended distribution of the alert message (REQUIRED)	Code Values: "Public" - For general dissemination to unrestricted audiences "Restricted" - For dissemination only to users with a known operational requirement (see <restriction>, below) "Private" - For dissemination only to specified addresses (see <addresses>, below)

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
restriction	cap. alert. restriction. text	The text describing the rule for limiting distribution of the restricted alert message (CONDITIONAL)	Used when <scope> value is "Restricted".
addresses	cap. alert. addresses. group	The group listing of intended recipients of the private alert message (CONDITIONAL)	<p>(1) Required when <scope> is "Private", optional when <scope> is "Public" or "Restricted". Used when <scope> value is "Private".</p> <p>(2) Each recipient SHALL be identified by an identifier or an address.</p> <p>(3) Multiple space-delimited addresses MAY be included. Addresses including whitespace MUST be enclosed in double-quotes.</p>
code	cap. alert. code. code	The code denoting the special handling of the alert message (OPTIONAL)	<p>(1) Any user-defined flag or special code used to flag the alert message for special handling.</p> <p>(2) Multiple instances MAY occur.</p>
note	cap. alert. note. text	The text describing the purpose or significance of the alert message (OPTIONAL)	The message note is primarily intended for use with <status> "Exercise" and <msgType> "Error".
references	cap. alert. references. group	The group listing identifying earlier message(s) referenced by the alert message (OPTIONAL)	<p>(1) The extended message identifier(s) (in the form <i>sender,identifier,sent</i>) of an earlier CAP message or messages referenced by this one.</p> <p>(2) If multiple messages are referenced, they SHALL be separated by whitespace.</p>

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
incidents	cap. alert. incidents. group	The group listing naming the referent incident(s) of the alert message (OPTIONAL)	<ul style="list-style-type: none"> (1) Used to collate multiple messages referring to different aspects of the same incident. (2) If multiple incident identifiers are referenced, they SHALL be separated by whitespace. Incident names including whitespace SHALL be surrounded by double-quotes.
3.2.2 "info" Element and Sub-elements			
info	cap. alertInfo. info. group	The container for all component parts of the info sub-element of the alert message (OPTIONAL)	<ul style="list-style-type: none"> (1) Multiple occurrences are permitted within a single <alert>. If targeting of multiple <info> blocks in the same language overlaps, information in later blocks may expand but may not override the corresponding values in earlier ones. Each set of <info> blocks containing the same language identifier SHALL be treated as a separate sequence. (2) In addition to the specified sub-elements, MAY contain one or more <resource> blocks and/or one or more <area> blocks.
language	cap. alertInfo. language. code	The code denoting the language of the info sub-element of the alert message (OPTIONAL)	<ul style="list-style-type: none"> (1) Code Values: Natural language identifier per [RFC 3066]. (2) If not present, an implicit default value of "en-US" SHALL be assumed. (3) A null value in this element SHALL be considered equivalent to "en-US."

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
category	cap. alertInfo. category. code	The code denoting the category of the subject event of the alert message (REQUIRED)	<p>(1) Code Values:</p> <p>“Geo” - Geophysical (inc. landslide)</p> <p>“Met” - Meteorological (inc. flood)</p> <p>“Safety” - General emergency and public safety</p> <p>“Security” - Law enforcement, military, homeland and local/private security</p> <p>“Rescue” - Rescue and recovery</p> <p>“Fire” - Fire suppression and rescue</p> <p>“Health” - Medical and public health</p> <p>“Env” - Pollution and other environmental</p> <p>“Transport” - Public and private transportation</p> <p>“Infra” - Utility, telecommunication, other non-transport infrastructure</p> <p>“CBRNE” – Chemical, Biological, Radiological, Nuclear or High-Yield Explosive threat or attack</p> <p>“Other” - Other events</p> <p>(2) Multiple instances MAY occur within an <info> block.</p>
event	cap. alertInfo. event. text	The text denoting the type of the subject event of the alert message (REQUIRED)	

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
responseType	cap. alertInfo. responseType. code	The code denoting the type of action recommended for the target audience (OPTIONAL)	<p>(1) Code Values:</p> <p>“Shelter” – Take shelter in place or per <instruction></p> <p>“Evacuate” – Relocate as instructed in the <instruction></p> <p>“Prepare” – Make preparations per the <instruction></p> <p>“Execute” – Execute a pre-planned activity identified in <instruction></p> <p>“Avoid” – Avoid the subject event as per the <instruction></p> <p>“Monitor” – Attend to information sources as described in <instruction></p> <p>“Assess” – Evaluate the information in this message. (This value SHOULD NOT be used in public warning applications.)</p> <p>“AllClear” – The subject event no longer poses a threat or concern and any follow on action is described in <instruction></p> <p>“None” – No action recommended</p> <p>(2) Multiple instances MAY occur within an <info> block.</p>
urgency	cap. alertInfo. urgency. code	The code denoting the urgency of the subject event of the alert message (REQUIRED)	<p>(1) The <urgency>, <severity>, and <certainty> elements collectively distinguish less emphatic from more emphatic messages.</p> <p>(2) Code Values:</p> <p>“Immediate” - Responsive action SHOULD be taken immediately</p> <p>“Expected” - Responsive action SHOULD be taken soon (within next hour)</p> <p>“Future” - Responsive action SHOULD be taken in the near future</p> <p>“Past” - Responsive action is no longer required</p> <p>“Unknown” - Urgency not known</p>

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
severity	cap. alertInfo. severity. code	The code denoting the severity of the subject event of the alert message (REQUIRED)	<p>(1) The <urgency>, <severity>, and <certainty> elements collectively distinguish less emphatic from more emphatic messages.</p> <p>(2) Code Values:</p> <p>“Extreme” - Extraordinary threat to life or property</p> <p>“Severe” - Significant threat to life or property</p> <p>“Moderate” - Possible threat to life or property</p> <p>“Minor” – Minimal to no known threat to life or property</p> <p>“Unknown” - Severity unknown</p>
certainty	cap. alertInfo. certainty. code	The code denoting the certainty of the subject event of the alert message (REQUIRED)	<p>(1) The <urgency>, <severity>, and <certainty> elements collectively distinguish less emphatic from more emphatic messages.</p> <p>(2) Code Values:</p> <p>“Observed” – Determined to have occurred or to be ongoing</p> <p>“Likely” - Likely (p > ~50%)</p> <p>“Possible” - Possible but not likely (p <= ~50%)</p> <p>“Unlikely” - Not expected to occur (p ~ 0)</p> <p>“Unknown” - Certainty unknown</p> <p>(3) For backward compatibility with CAP 1.0, the deprecated value of “Very Likely” SHOULD be treated as equivalent to “Likely”.</p>
audience	cap. alertInfo. audience. text	The text describing the intended audience of the alert message (OPTIONAL)	

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
eventCode	cap. alertInfo. eventCode. code	A system-specific code identifying the event type of the alert message (OPTIONAL)	<p>(1) Any system-specific code for event typing, in the form:</p> <pre><eventCode> <valueName>valueName</valueName> <value>value</value> </eventCode></pre> <p>where the content of "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., valueName = "SAME" and value="CEM").</p> <p>(2) Values of "valueName" that are acronyms SHOULD be represented in all capital letters without periods (e.g., SAME, FIPS, ZIP).</p> <p>(3) Multiple instances MAY occur within an <info> block.</p>
effective	cap. alertInfo. effective. time	The effective time of the information of the alert message (OPTIONAL)	<p>(1) The date and time SHALL be represented in the DateTime Data Type (See Implementation Notes) format (e.g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16: 49 PDT).</p> <p>(2) Alphabetic timezone designators such as "Z" MUST NOT be used. The timezone for UTC MUST be represented as "-00:00".</p> <p>(3) If this item is not included, the effective time SHALL be assumed to be the same as in <sent>.</p>
onset	cap. alertInfo. onset. time	The expected time of the beginning of the subject event of the alert message (OPTIONAL)	<p>(1) The date and time SHALL be represented in the DateTime Data Type (See Implementation Notes) format (e.g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16: 49 PDT).</p> <p>(2) Alphabetic timezone designators such as "Z" MUST NOT be used. The timezone for UTC MUST be represented as "-00:00".</p>

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
expires	cap. alertInfo. expires. time	The expiry time of the information of the alert message (OPTIONAL)	<p>(1) The date and time SHALL be represented in the DateTime Data Type (See Implementation Notes) format (e.g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT).</p> <p>(2) Alphabetic timezone designators such as "Z" MUST NOT be used. The timezone for UTC MUST be represented as "-00:00".</p> <p>(3) If this item is not provided, each recipient is free to set its own policy as to when the message is no longer in effect.</p>
senderName	cap. alertInfo. senderName. text	The text naming the originator of the alert message (OPTIONAL)	The human-readable name of the agency or authority issuing this alert.
headline	cap. alertInfo. headline. text	The text headline of the alert message (OPTIONAL)	A brief human-readable headline. Note that some displays (for example, short messaging service devices) may only present this headline; it SHOULD be made as direct and actionable as possible while remaining short. 160 characters MAY be a useful target limit for headline length.
description	cap. alertInfo. description. text	The text describing the subject event of the alert message (OPTIONAL)	An extended human readable description of the hazard or event that occasioned this message.
instruction	cap. alertInfo. instruction. text	The text describing the recommended action to be taken by recipients of the alert message (OPTIONAL)	An extended human readable instruction to targeted recipients. If different instructions are intended for different recipients, they should be represented by use of multiple <info> blocks.

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
web	cap alertInfo. web. identifier	The identifier of the hyperlink associating additional information with the alert message (OPTIONAL)	A full, absolute URI for an HTML page or other text resource with additional or reference information regarding this alert.
contact	cap. alertInfo. contact. text	The text describing the contact for follow-up and confirmation of the alert message (OPTIONAL)	
parameter	cap. alertInfo. parameter. code	A system-specific additional parameter associated with the alert message (OPTIONAL)	<p>(1) Any system-specific datum, in the form:</p> <pre><parameter> <valueName>valueName</valueName> <value>value</value> </parameter></pre> <p>where the content of "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., valueName = "SAME" and value="CIV").</p> <p>(2) Values of "valueName" that are acronyms SHOULD be represented in all capital letters without periods (e.g., SAME, FIPS, ZIP).</p> <p>(3) Multiple instances MAY occur within an <info> block.</p>

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
3.2.3 "resource" Element and Sub-elements			
resource	cap alertInfoResource. resource. group	The container for all component parts of the resource sub-element of the info sub-element of the alert element (OPTIONAL)	(1) Refers to an additional file with supplemental information related to this <info> element; e.g., an image or audio file. (2) Multiple instances MAY occur within an <info> block.
resourceDesc	cap. alertInfoResource. resourceDesc. text	The text describing the type and content of the resource file (REQUIRED)	The human-readable text describing the type and content, such as "map" or "photo", of the resource file.
contentType	cap. alertInfoResource. contentType. text	The identifier of the MIME content type and sub-type describing the resource file (REQUIRED OPTIONAL)	MIME content type and sub-type as described in [RFC 2046]. (As of this document, the current IANA registered MIME types are listed at http://www.iana.org/assignments/media-types/)
size	cap. alertInfoResource. size. integer	The integer indicating the size of the resource file (OPTIONAL)	(1) Approximate size of the resource file in bytes. (1) (2) <u>For <uri> based resources, <size> SHOULD be included if available.</u>
uri	cap. alertInfoResource. uri. identifier	The identifier of the hyperlink for the resource file (OPTIONAL)	A full absolute URI, typically a Uniform Resource Locator that can be used to retrieve the resource over the Internet OR a relative URI to name the content of a <derefUri> element if one is present in this resource block.

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
derefUri	cap alertInfoResource. derefUri. data	The base-64 encoded data content of the resource file (CONDITIONAL)	<p>(1) MAY be used either with or instead of the <uri> element in messages transmitted over one-way (e.g., broadcast) data links where retrieval of a resource via a URI is not feasible.</p> <p>(2) Clients intended for use with one-way data links MUST support this element.</p> <p>(3) This element MUST NOT be used unless the sender is certain that all direct clients are capable of processing it.</p> <p>(4) If messages including this element are forwarded onto a two-way network, the forwarder MUST strip the <derefUri> element and SHOULD extract the file contents and provide a <uri> link to a retrievable version of the file.</p> <p>(5) Providers of one-way data links MAY enforce additional restrictions on the use of this element, including message-size limits and restrictions regarding file types.</p>
digest	cap. alertInfoResource. digest. code	The code representing the digital digest ("hash") computed from the resource file (OPTIONAL)	Calculated using the Secure Hash Algorithm (SHA-1) per [FIPS 180-2] .
3.2.4 "area" Element and Sub-elements			
area	cap. alertInfoArea. area. group	The container for all component parts of the area sub-element of the info sub-element of the alert message (OPTIONAL)	<p>(1) Multiple occurrences permitted, in which case the target area for the <info> block is the union of all the included <area> blocks.</p> <p>(2) MAY contain one or multiple instances of <polygon>, <circle> or <geocode>. If multiple <polygon>, <circle> or <geocode> elements are included, the area described by this <area> block is represented by the union of all the included elements.</p>

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
areaDesc	cap. alertInfoArea. areaDesc. text	The text describing the affected area of the alert message (REQUIRED)	A text description of the affected area.
polygon	cap. alertInfoArea. polygon. group	The paired values of points defining a polygon that delineates the affected area of the alert message (OPTIONAL)	<p>(1) Code Values: The geographic polygon is represented by a whitespace-delimited list of [WGS 84] coordinate pairs. (See WGS 84 Note at end of this section)</p> <p>(2) A minimum of 4 coordinate pairs MUST be present and the first and last pairs of coordinates MUST be the same.</p> <p>(3) Multiple instances MAY occur within an <area> block.</p>
circle	cap. alertInfoArea. circle. group	The paired values of a point and radius delineating the affected area of the alert message (OPTIONAL)	<p>(1) Code Values: The circular area is represented by a central point given as a [WGS 84] coordinate pair followed by a space character and a radius value in kilometers. (See WGS 84 Note at end of this section)</p> <p>(2) Multiple instances MAY occur within an <area> block.</p>

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
geocode	cap. alertInfoArea. geocode. code	The geographic code delineating the affected area of the alert message (OPTIONAL)	<p>(1) Any geographically-based code to describe a message target area, in the form:</p> <pre><geocodeparameter> <valueName>valueName</valueName> <value>value</value> </geocodeparameter></pre> <p>where the content of "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., valueName = "SAME" and value="006113").</p> <p>(2) Values of "valueName" that are acronyms SHOULD be represented in all capital letters without periods (e.g., SAME, FIPS, ZIP).</p> <p>(3) Multiple instances MAY occur within an <area> block.</p> <p>(4) This element is primarily for compatibility with other systems. Use of this element presumes knowledge of the coding system on the part of recipients; therefore, for interoperability, it SHOULD be used in concert with an equivalent description in the more universally understood <polygon> and <circle> forms whenever possible.</p>
altitude	cap. alertInfoArea. altitude. quantity	The specific or minimum altitude of the affected area of the alert message (OPTIONAL)	<p>(1) If used with the <ceiling> element this value is the lower limit of a range. Otherwise, this value specifies a specific altitude.</p> <p>(2) The altitude measure is in feet above mean sea level per the [WGS 84] datum.</p>
ceiling	cap. alertInfoArea. ceiling. quantity	The maximum altitude of the affected area of the alert message (CONDITIONAL)	<p>(1) MUST NOT be used except in combination with the <altitude> element.</p> <p>(2) The ceiling measure is in feet above mean sea level per the [WGS 84] datum.</p>

239 **3.3 Implementation Notes**

240 **3.3.1 WGS 84 Note**

241 Geographic locations in CAP are defined using **[WGS 84]** (World Geodetic System 1984), equivalent to
242 EPSG (European Petroleum Survey Group) code 4326 (2 dimensions). CAP does not assign
243 responsibilities for coordinate transformations from and to other Spatial Reference Systems. See section
244 1.5 Terminology for the format of coordinate pairs within CAP elements.

245 **3.3.2 DateTime Data Type**

246 All **[dateTime]** elements (<sent>, <effective>, <onset>, and <expires>) SHALL be specified in the form
247 "YYYY-MM-DDThh:mm:ssXzh:zm" where:

- 248 • YYYY indicates the year
- 249 • MM indicates the month
- 250 • DD indicates the day
- 251 • T indicates the symbol "T" marking the start of the required time section
- 252 • hh indicates the hour
- 253 • mm indicates the minute
- 254 • ss indicates the second
- 255 • X indicates either the symbol "+" if the preceding date and time are in a time zone ahead of UTC,
256 or the symbol "-" if the preceding date and time are in a time zone behind UTC. If the time is in
257 UTC, the symbol "-" will be used.
- 258 • zh indicates the hours of offset from the preceding date and time to UTC, or "00" if the preceding
259 time is in UTC
- 260 • zm indicates the minutes of offset from the preceding date and time to UTC, or "00" if the
261 preceding time is in UTC

262 For example, a value of "2002-05-30T09:30:10-05:00" would indicate May 30, 2002 at 9:30:10 AM
263 Eastern Standard Time, which would be 2:30:10PM Universal Coordinated Time (UTC). That same
264 time might be indicated by "2002-05-30T14:30:10-00:00".

265 **3.3.3 Character Entity References**

266 The use of character entity references, such as HTML entities (e.g.) is discouraged.

267 **3.3.4 Security Note**

268 Because CAP is an XML-based format, existing XML security mechanisms can be used to secure and
269 authenticate its content. While these mechanisms are available to secure CAP Alert Messages, they
270 should not be used indiscriminately.

271 Note that this section adds two elements to CAP by reference. These are: <Signature> and
272 <EncryptedData>. Both elements are children of the <alert> element and are optional. If the
273 <EncryptedData> element exists, no other elements will be visible until after the message is decrypted.
274 This makes the minimal CAP message an <alert> element which encloses an <EncryptedData> element.
275 The maximal CAP message, if an <EncryptedData> element is present is an <alert> element enclosing a
276 single <EncryptedData> element and one or more <Signature> elements.

277 3.3.4.1 Digital Signatures

278 The <alert> element of a CAP Alert Message MAY have an Enveloped Signature, as described by XML-
279 Signature and Syntax Processing [XMLENSIG]. Other XML signature mechanisms MUST NOT be used in
280 CAP Alert Messages.

281 Processors MUST NOT reject a CAP Alert Message containing such a signature simply because they are
282 not capable of verifying it; they MUST continue processing and SHOULD MAY inform the user of their
283 failure to validate the signature.

284 In other words, the presence of an element with the namespace URI [XMLENSIG] and a local name of
285 <Signature> as a child of the <alert> element must not cause a processor to fail merely because of its
286 presence.

287 3.3.4.2 Encryption

288 The <alert> element of a CAP Alert Message MAY be encrypted, using the mechanisms described by
289 XML Encryption Syntax and Processing [XMLENC]. Other XML encryption mechanisms MUST NOT be
290 used in CAP Alert Messages; however, transport-layer encryption mechanisms may be used
291 independently of this requirement.

292 3.4 XML Schema

```
293 <?xml version = "1.0" encoding = "UTF-8"?>  
294 <!-- Copyright 2009 (c) 2009 Oasis Open -->  
295 <schema xmlns = "http://www.w3.org/2001/XMLSchema"  
296   targetNamespace = "urn:oasis:names:tc:emergency:cap:1.2"  
297   xmlns:cap = "urn:oasis:names:tc:emergency:cap:1.2"  
298   xmlns:xs = "http://www.w3.org/2001/XMLSchema"  
299   elementFormDefault = "qualified"  
300   attributeFormDefault = "unqualified"  
301   version = "1.2">  
302   <element name = "alert">  
303     <annotation>  
304       <documentation>CAP Alert Message (version 1.2)</documentation>  
305     </annotation>  
306     <complexType>  
307       <sequence>  
308         <element name = "identifier" type = "xs:string"/>  
309         <element name = "sender" type = "xs:string"/>  
310         <element name = "sent">  
311           <simpleType>  
312             <restriction base = "xs:dateTime">  
313               <pattern value = "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[[-,+]\\d\d:\d\d"/>  
314             </restriction>  
315           </simpleType>  
316         </element>  
317         <element name = "status">  
318           <simpleType>  
319             <restriction base = "xs:string">  
320               <enumeration value = "Actual"/>  
321               <enumeration value = "Exercise"/>  
322               <enumeration value = "System"/>  
323               <enumeration value = "Test"/>  
324               <enumeration value = "Draft"/>  
325             </restriction>  
326           </simpleType>  
327         </element>  
328         <element name = "msgType">  
329           <simpleType>  
330             <restriction base = "xs:string">  
331               <enumeration value = "Alert"/>  
332               <enumeration value = "Update"/>  
333               <enumeration value = "Cancel"/>  
334               <enumeration value = "Ack"/>  
335               <enumeration value = "Error"/>  
336             </restriction>  
337           </simpleType>  
338         </element>  
339       </sequence>  
340       <element name = "source" type = "xs:string" minOccurs = "0"/>  
341       <element name = "scope">  
342         <simpleType>  
343           <restriction base = "xs:string">
```

```

344     <enumeration value = "Public"/>
345     <enumeration value = "Restricted"/>
346     <enumeration value = "Private"/>
347   </restriction>
348 </simpleType>
349 </element>
350 <element name = "restriction" type = "xs:string" minOccurs = "0"/>
351 <element name = "addresses" type = "xs:string" minOccurs = "0"/>
352 <element name = "code" type = "xs:string" minOccurs = "0" maxOccurs = "unbounded"/>
353 <element name = "note" type = "xs:string" minOccurs = "0"/>
354 <element name = "references" type = "xs:string" minOccurs = "0"/>
355 <element name = "incidents" type = "xs:string" minOccurs = "0"/>
356 <element name = "info" minOccurs = "0" maxOccurs = "unbounded">
357   <complexType>
358     <sequence>
359       <element name = "language" type = "xs:language" default = "en-US" minOccurs = "0"/>
360       <element name = "category" maxOccurs = "unbounded">
361         <simpleType>
362           <restriction base = "xs:string">
363             <enumeration value = "Geo"/>
364             <enumeration value = "Met"/>
365             <enumeration value = "Safety"/>
366             <enumeration value = "Security"/>
367             <enumeration value = "Rescue"/>
368             <enumeration value = "Fire"/>
369             <enumeration value = "Health"/>
370             <enumeration value = "Env"/>
371             <enumeration value = "Transport"/>
372             <enumeration value = "Infra"/>
373             <enumeration value = "CBRNE"/>
374             <enumeration value = "Other"/>
375           </restriction>
376         </simpleType>
377       </element>
378       <element name = "event" type = "xs:string"/>
379       <element name = "responseType" minOccurs = "0" maxOccurs = "unbounded">
380         <simpleType>
381           <restriction base = "xs:string">
382             <enumeration value = "Shelter"/>
383             <enumeration value = "Evacuate"/>
384             <enumeration value = "Prepare"/>
385             <enumeration value = "Execute"/>
386             <enumeration value = "Avoid"/>
387             <enumeration value = "Monitor"/>
388             <enumeration value = "Assess"/>
389             <enumeration value = "AllClear"/>
390             <enumeration value = "None"/>
391           </restriction>
392         </simpleType>
393       </element>
394       <element name = "urgency">
395         <simpleType>
396           <restriction base = "xs:string">
397             <enumeration value = "Immediate"/>
398             <enumeration value = "Expected"/>
399             <enumeration value = "Future"/>
400             <enumeration value = "Past"/>
401             <enumeration value = "Unknown"/>
402           </restriction>
403         </simpleType>
404       </element>
405       <element name = "severity">
406         <simpleType>
407           <restriction base = "xs:string">
408             <enumeration value = "Extreme"/>
409             <enumeration value = "Severe"/>
410             <enumeration value = "Moderate"/>
411             <enumeration value = "Minor"/>
412             <enumeration value = "Unknown"/>
413           </restriction>
414         </simpleType>
415       </element>
416       <element name = "certainty">
417         <simpleType>
418           <restriction base = "xs:string">
419             <enumeration value = "Observed"/>
420             <enumeration value = "Likely"/>
421             <enumeration value = "Possible"/>
422             <enumeration value = "Unlikely"/>
423             <enumeration value = "Unknown"/>
424           </restriction>
425         </simpleType>

```

```

426 </element>
427 <element name = "audience" type = "xs:string" minOccurs = "0"/>
428 <element name = "eventCode" minOccurs = "0" maxOccurs = "unbounded">
429   <complexType>
430     <sequence>
431       <element ref = "cap:valueName"/>
432       <element ref = "cap:value"/>
433     </sequence>
434   </complexType>
435 </element>
436 <element name = "effective" minOccurs = "0">
437   <simpleType>
438     <restriction base = "xs:dateTime">
439       <pattern value = "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,]\d\d:\d\d"/>
440     </restriction>
441   </simpleType>
442 </element>
443 <element name = "onset" minOccurs = "0">
444   <simpleType>
445     <restriction base = "xs:dateTime">
446       <pattern value = "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,]\d\d:\d\d"/>
447     </restriction>
448   </simpleType>
449 </element>
450 <element name = "expires" minOccurs = "0">
451   <simpleType>
452     <restriction base = "xs:dateTime">
453       <pattern value = "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,]\d\d:\d\d"/>
454     </restriction>
455   </simpleType>
456 </element>
457 <element name = "senderName" type = "xs:string" minOccurs = "0"/>
458 <element name = "headline" type = "xs:string" minOccurs = "0"/>
459 <element name = "description" type = "xs:string" minOccurs = "0"/>
460 <element name = "instruction" type = "xs:string" minOccurs = "0"/>
461 <element name = "web" type = "xs:anyURI" minOccurs = "0"/>
462 <element name = "contact" type = "xs:string" minOccurs = "0"/>
463 <element name = "parameter" minOccurs = "0" maxOccurs = "unbounded">
464   <complexType>
465     <sequence>
466       <element ref = "cap:valueName"/>
467       <element ref = "cap:value"/>
468     </sequence>
469   </complexType>
470 </element>
471 <element name = "resource" minOccurs = "0" maxOccurs = "unbounded">
472   <complexType>
473     <sequence>
474       <element name = "resourceDesc" type = "xs:string"/>
475       <element name = "mimeType" type = "xs:string" minOccurs = "0"/>
476       <element name = "size" type = "xs:integer" minOccurs = "0"/>
477       <element name = "uri" type = "xs:anyURI" minOccurs = "0"/>
478       <element name = "derefUri" type = "xs:string" minOccurs = "0"/>
479       <element name = "digest" type = "xs:string" minOccurs = "0"/>
480     </sequence>
481   </complexType>
482 </element>
483 <element name = "area" minOccurs = "0" maxOccurs = "unbounded">
484   <complexType>
485     <sequence>
486       <element name = "areaDesc" type = "xs:string"/>
487       <element name = "polygon" type = "xs:string" minOccurs = "0" maxOccurs =
488 "unbounded"/>
489       <element name = "circle" type = "xs:string" minOccurs = "0" maxOccurs =
490 "unbounded"/>
491       <element name = "geocode" minOccurs = "0" maxOccurs = "unbounded">
492         <complexType>
493           <sequence>
494             <element ref = "cap:valueName"/>
495             <element ref = "cap:value"/>
496           </sequence>
497         </complexType>
498       </element>
499       <element name = "altitude" type = "xs:decimalstring" minOccurs = "0"/>
500       <element name = "ceiling" type = "xs:decimalstring" minOccurs = "0"/>
501     </sequence>
502   </complexType>
503 </element>
504 </sequence>
505 </complexType>
506 </element>

```

```
507     <any minOccurs = "0" maxOccurs = "unbounded" namespace = "http://www.w3.org/2000/09/xmldsig#"
508 processContents = "lax"/>
509     <any minOccurs = "0" namespace = "http://www.w3.org/2000/09/xmlenc#" processContents = "lax"/>
510     </sequence>
511 </complexType>
512 </element>
513 <element name = "valueName" type = "xs:string"/>
514 <element name = "value" type = "xs:string"/>
515 </schema>
516
517
518
```

519 3.5 Use of ASN.1 to Specify and Encode the CAP Alert Message

520 3.5.1 General

521 The ASN.1 (see ITU-T Rec X.680) schema in 3.5.3 provides an alternative formulation of the XML
522 schema defined in 3.4. If the ASN.1 Extended XML Encoding Rules (see ITU-T Rec X.693) are applied
523 to this ASN.1 schema, the permitted XML is identical to that supported by the XML schema in 3.4. If the
524 ASN.1 Unaligned Packed Encoding Rules (see ITU-T Rec X.691) are applied to it, the resulting binary
525 encodings are more compact than the corresponding XML encodings.

526 3.5.2 Formal Mappings and Specification

527 The normative specification of the compact binary encoding is in 3.5.3 with the application of the ASN.1
528 Unaligned Packed Encoding Rules (see ITU-T Rec. X.691).

529 The semantics of the fields in the ASN.1 specification are identical to those of the XSD specification, and
530 the mapping of the fields from the XSD specification to the ASN.1 specification is formally defined in ITU-
531 T Rec. X.694.

532 Implementations can produce and process the CAP alert XML messages using either ASN.1-based or
533 XSD-based tools (or other ad hoc software).

534 Implementations can produce and process the CAP alert compact binary messages using ASN.1-based
535 tools (or by other ad hoc software).

536 Any XML encoded CAP alert messages can be converted to compact binary messages by decoding with
537 an ASN.1 tool configured for the Extended XML Encoding Rules and re-encoding the resulting abstract
538 values with an ASN.1 tool configured for Unaligned Packed Encoding Rules.

539 Any compact binary CAP alert messages can be converted to XML encoded messages by decoding with
540 an ASN.1 tool configured for Unaligned Packed Encoding Rules and re-encoding the resulting abstract
541 values with an ASN.1 tool configured for Extended XML Encoding Rules.

542 3.5.3 ASN.1 Schema

```
543 CAP-1-2 {itu-t recommendation x cap(1303) version1-2(2)}
544 DEFINITIONS XER INSTRUCTIONS AUTOMATIC TAGS ::=
545 -- CAP Alert Message (version 1.2)
546 BEGIN
547
548 Alert ::= SEQUENCE {
549     identifier IdentifierString,
550     -- Unambiguous identification of the message
551     -- from all messages from
552     -- this sender, in a format defined by the sender and
553     -- identified in the "sender" field below.
554     sender String,
555     -- The globally unambiguous identification of the sender.
556     -- This specification does not define the root of
557     -- a global identification tree (there is no international
558     -- agreement on such a root), so it relies
559     -- on human-readable text to define globally and
560     -- unambiguously the sender.
561     -- An internet domain name or use of "iri://ITU-T/..."
562     -- are possible, but
563     -- the choice needs to be clearly stated in human-readable form.
564     sent DateTime (CONSTRAINED BY {/* XML representation of the XSD
565 pattern "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[[-,+] \d\d:\d\d\d" */}),
566     status AlertStatus,
567     msgType AlertMessageType,
568     source String OPTIONAL,
569     -- Not standardised human-readable identification
```

```

570     -- of the source of the alert.
571     scope      AlertScope,
572     restriction String OPTIONAL,
573     -- Not standardised human-readable restrictions
574     -- on the distribution of the alert message
575     addresses  String OPTIONAL,
576     -- A space separated list of addressees for private messages
577     -- (see 3.2.1)
578     code-list  SEQUENCE SIZE((0..MAX)) OF code String,
579     -- A sequence codes for special handling
580     -- (see 3.2.1)
581     -- The format and semantics of the codes are not defined in this
582     -- specification.
583     note      String OPTIONAL,
584     -- Not standardised human-readable clarifying text for the alert
585     -- (see 3.2.1)
586     references String OPTIONAL,
587     -- Space-separated references to earlier messages
588     -- (see 3.2.1)
589     incidents  String OPTIONAL,
590     -- Space-separated references to related incidents
591     -- (see 3.2.1)
592     info-list  SEQUENCE SIZE((0..MAX)) OF info AlertInformation }
593
594 AlertStatus ::= ENUMERATED {
595     actual,
596     draft,
597     exercise,
598     system,
599     test }
600
601 AlertMessageType ::= ENUMERATED {
602     ack,
603     alert,
604     cancel,
605     error,
606     update }
607
608 AlertScope ::= ENUMERATED {
609     private,
610     public,
611     restricted }
612
613 AlertInformation ::= SEQUENCE {
614     language      Language -- DEFAULT "en-US" -- ,
615     -- The language used in this value of the Info type
616     -- (see 3.2.2)
617     category-list SEQUENCE (SIZE(1..MAX)) OF
618     category InformationCategory,
619     event         String,
620     -- Not standardised human-readable text describing the
621     -- type of the event (see 3.2.2)
622     responseType-list SEQUENCE SIZE((0..MAX)) OF
623     responseType InformationResponseType,
624     urgency       HowUrgent,
625     severity      HowSevere,
626     certainty     HowCertain,
627     audience     String OPTIONAL,
628     -- Not standardised human-readable text describing the
629     -- intended audience for the message (see 3.2.2)
630     eventCode-list SEQUENCE SIZE((0..MAX)) OF eventCode SEQUENCE {
631     valueName ValueName,
632     value      Value },

```

```

633     effective      DateTime (CONSTRAINED BY { /* XML representation of the
634 XSD pattern "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[[-,+] \d\d:\d\d" */}) OPTIONAL,
635     onset          DateTime (CONSTRAINED BY { /* XML representation of the
636 XSD pattern "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[[-,+] \d\d:\d\d" */}) OPTIONAL,
637     expires        DateTime (CONSTRAINED BY { /* XML representation of the
638 XSD pattern "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[[-,+] \d\d:\d\d" */}) OPTIONAL,
639     senderName     String OPTIONAL,
640         -- Not standardised human-readable name of the authority
641         -- issuing the message (see 3.2.2)
642     headline       String (SIZE (1..160,...)) OPTIONAL,
643         -- Not standardised human-readable short statement (headline)
644         -- of the alert (see 3.2.2)
645     description    String OPTIONAL,
646         -- Not standardised human-readable extended description of
647         -- the event (see 3.2.2)
648     instruction    String OPTIONAL,
649         -- Not standardised human-readable recommended action
650         -- (see 3.2.2)
651     web            AnyURI OPTIONAL,
652     contact        String OPTIONAL,
653         -- Not standardised human-readable contact details for
654         -- follow-up (see 3.2.2)
655     parameter-list SEQUENCE SIZE((0..MAX)) OF parameter SEQUENCE {
656         -- System-specific parameters (see 3.2.2)
657         valueName ValueName,
658         value      Value },
659     resource-list  SEQUENCE SIZE((0..MAX)) OF resource ResourceFile,
660     area-list      SEQUENCE SIZE((0..MAX)) OF Area }
661
662 InformationCategory ::= ENUMERATED {
663     cBRNE,
664     env,
665     fire,
666     geo,
667     health,
668     infra,
669     met,
670     other,
671     rescue,
672     safety,
673     security,
674     transport }
675
676 InformationResponseType ::= ENUMERATED {
677     allClear(7),
678     assess(0),
679     avoid(8),
680     evacuate(1),
681     execute(2),
682     monitor(3),
683     none(4),
684     prepare(5),
685     shelter(6) }
686
687 HowUrgent ::= ENUMERATED {
688     expected,
689     future,
690     immediate,
691     past,
692     unknown }
693
694 HowSevere ::= ENUMERATED {
695     extreme,
696     minor,

```

```

697         moderate,
698         severe,
699         unknown }
700
701 HowCertain ::= ENUMERATED {
702     likely,
703     observed,
704     possible,
705     unknown,
706     unlikely }
707
708 ResourceFile ::= SEQUENCE {
709     -- Information about an associated resource file
710     -- (see 3.2.3)
711     resourceDesc String,
712     -- Not standardised human-readable description of the type
713     -- and content of
714     -- an associated resource file (for example a map or
715     -- photograph)(see 3.2.3)
716     mimeType String OPTIONAL,
717     size INTEGER OPTIONAL, -- In bytes
718     uri AnyURI OPTIONAL,
719     derefUri String OPTIONAL,
720     -- An alternative to the URI giving the Base64-encoded
721     -- content of the resource file (see 3.2.3)
722     digest String OPTIONAL
723     -- SHA-1 hash of the resource file for error detection
724     -- (see 3.2.3) -- }
725
726 Area ::= SEQUENCE {
727     -- Identification of an affected area
728     areaDesc String,
729     -- Not standardised human-readable description of the area
730     polygon-list SEQUENCE OF polygon String,
731     -- Each element is a space-separated list of coordinate pairs
732     -- The complete list starts and ends with the same point and
733     -- defines the polygon that defines the area
734     -- (see 3.2.4).
735     circle-list SEQUENCE OF circle String,
736     -- A space-separated list of coordinates for a point and a radius
737     geocode-list SEQUENCE SIZE((0..MAX)) OF geocode SEQUENCE {
738     -- A geographic code designating the alert target area
739     -- (see 3.2.4)
740         valueName ValueName,
741         value Value },
742     altitude REALString OPTIONAL,
743     -- Specific or minimum altitude of the affected area
744     ceiling REALString OPTIONAL
745     -- Maximum altitude of the affected area -- }
746
747 ValueName ::= String -- A not standardised name for
748     -- an information event code, a parameter or a geocode
749
750 Value ::= String -- The value of the information event code,
751     -- parameter or geocode
752
753 String ::= UTF8String (FROM (
754     {0,0,0,9} -- TAB
755     | {0,0,0,10} -- CR
756     | {0,0,0,13} -- LF
757     | {0,0,0,32}..{0,0,215,255} -- Space to the start of the S-zone
758     | {0,0,224,0}..{0,0,255,253} -- Rest of BMP after S-zone
759     | {0,1,0,0}..{0,16,255,253} -- Other planes -- ) )
760

```

```

761 StringChar ::= String (SIZE(1))
762
763 SpaceAndComma ::= UTF8String (FROM (
764     {0,0,0,32} -- SPACE
765     | {0,0,0,44} -- COMMA -- ) )
766
767 IdentifierString ::= String (FROM (StringChar EXCEPT SpaceAndComma))
768
769 Language ::= VisibleString(FROM ("a".."z" | "A".."Z" | "-" | "0".."9"))
770     (PATTERN "[a-zA-Z]#(1,8)(-[a-zA-Z0-9]#(1,8))*")
771     -- The semantics of Language is specified in IETF RFC 3066
772
773 DateTime ::= TIME (SETTINGS "Basic=Date-Time Date=YMD
774     Year=Basic Time=HMS Local-or-UTC=LD")
775     -- This is the ISO 8601 format using local time and a
776     -- time difference
777
778 stringWithNoCRLFHT ::= UTF8String (FROM (
779     {0,0,0,32}..{0,0,215,255}
780     | {0,0,224,0}..{0,0,255,253}
781     | {0,1,0,0}..{0,16,255,255}))
782
783 AnyURI ::= stringWithNoCRLFHT (CONSTRAINED BY {
784     /* Shall be a valid URI as defined in IETF RFC 2396 */})
785
786 ENCODING-CONTROL XER
787     GLOBAL-DEFAULTS MODIFIED-ENCODINGS
788     GLOBAL-DEFAULTS CONTROL-NAMESPACE
789     "http://www.w3.org/2001/XMLSchema-instance" PREFIX "xsi"
790     NAMESPACE ALL, ALL IN ALL AS "urn:oasis:names:tc:emergency:cap:1.2"
791     PREFIX "cap"
792     NAME Alert, Area AS UNCAPITALIZED
793     UNTAGGED SEQUENCE OF
794     DEFAULT-FOR-EMPTY AlertInformation.language AS "en-US"
795     TEXT AlertStatus:ALL,
796         AlertMessageType:ALL,
797         AlertScope:ALL,
798         InformationCategory:ALL,
799         InformationResponseType:ALL,
800         HowUrgent:ALL,
801         HowSevere:ALL,
802         HowCertain:ALL AS CAPITALIZED
803     WHITESPACE Language, AnyURI COLLAPSE
804 END

```

805

806 4 Conformance

807 An implementation conforms to this specification if it satisfies all of the MUST or REQUIRED level
808 requirements defined within this specification.

809 This specification references a number of other specifications. In order to comply with this specification,
810 an implementation MUST implement the portions of referenced specifications necessary to comply with
811 the required provisions of this specification. Additionally, the implementation of the portions of the
812 referenced specifications that are specifically cited in this specification MUST comply with the rules for
813 those portions as established in the referenced specification.

814

815 4.1 Conformance Targets

816 The following conformance targets are defined in order to support the specification of conformance to this
817 standard:

- 818 a) CAP V1.2 Message
- 819 b) CAP V1.2 Message Producer
- 820 c) CAP V1.2 Message Consumer

821

822 4.2 Conformance as a CAP V1.2 Message

823 An XML 1.0 document is a conforming CAP V1.2 Message if and only if:

- 824 a) it is valid according to the schema located at [http://docs.oasis-](http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.xsd)
825 [open.org/emergency/cap/v1.2/CAP-v1.2.xsd](http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.xsd) and
- 826 b) the content of its elements and the values of its attributes meet all the additional mandatory
827 requirements specified in Section 3.

828

829 4.3 Conformance as a CAP V1.2 Message Producer

830 A software entity is a conforming CAP V1.2 Message Producer if and only if:

- 831 a) it is constructed in such a way that any XML document produced by it and present in a place in
832 which a conforming CAP V1.2 Message is expected (based on contextual information) is indeed a
833 conforming CAP V1.2 Message according to this standard.

834 The condition in (a) above can be satisfied in many different ways. Here are some examples of possible
835 scenarios:

- 836 | – a ~~distribution element standard protocol~~ (for example, EDXL-DE) transfers messages carrying
837 CAP V1.2 Messages; a client has sent a request for a CAP V1.2 Message to a server which
838 claims to be a conforming CAP V1.2 Message Producer, and has received a response which is
839 therefore expected to carry a conforming CAP V1.2 Message;
- 840 – a local test environment has been set up, and the application under test (which claims to be a
841 conforming CAP V1.2 Message Producer) has the ability to produce a CAP V1.2 Message and
842 write it to a file in a directory in response to a request coming from the testing tool; the testing tool
843 has sent many requests to the application under test and is now verifying all the files present in
844 the directory, which is expected to contain only conforming CAP V1.2 Messages;

845

846 **4.4 Conformance as a CAP V1.2 Message Consumer**

847 A software entity is a conforming CAP V1.2 Message Consumer if and only if:

848 a) it is constructed in such a way that it is able to successfully validate and ingest a conforming CAP
849 V1.2 Message according to this standard.

850 The condition in (a) above can be satisfied in many different ways. Here is one example of a possible
851 scenario:

852 – a client receives and processes a CAP V1.2 Message from a server which claims to be a
853 conforming CAP V1.2 Message Producer

854

855

856

Appendix A. CAP Alert Message Example

857

XML examples are included below and are also available as separate files, along with ASN.1 binary

858

encoded examples, in the CAP 1.2 document repository <http://docs.oasis-open.org/emergency/cap/v1.2/>

859

A.1. Homeland Security Advisory System Alert

860

The following is a speculative example in the form of a CAP XML message.

861

```
<?xml version = "1.0" encoding = "UTF-8"?>
862 <alert xmlns = "urn:oasis:names:tc:emergency:cap:1.2">
863   <identifier>43b080713727</identifier>
864   <sender>hsas@dhs.gov</sender>
865   <sent>2003-04-02T14:39:01-05:00</sent>
866   <status>Actual</status>
867   <msgType>Alert</msgType>
868   <scope>Public</scope>
869   <info>
870     <category>Security</category>
871     <event>Homeland Security Advisory System Update</event>
872     <urgency>Immediate</urgency>
873     <severity>Severe</severity>
874     <certainty>Likely</certainty>
875     <senderName>U.S. Government, Department of Homeland Security</senderName>
876     <headline>Homeland Security Sets Code ORANGE</headline>
877     <description>The Department of Homeland Security has elevated the Homeland Security Advisory
878 System threat level to ORANGE / High in response to intelligence which may indicate a heightened
879 threat of terrorism.</description>
880     <instruction> A High Condition is declared when there is a high risk of terrorist attacks. In
881 addition to the Protective Measures taken in the previous Threat Conditions, Federal departments
882 and agencies should consider agency-specific Protective Measures in accordance with their
883 existing plans.</instruction>
884     <web>http://www.dhs.gov/dhspublic/display?theme=29</web>
885     <parameter>
886       <valueName>HSAS</valueName>
887       <value>ORANGE</value>
888     </parameter>
889     <resource>
890       <resourceDesc>Image file (GIF)</resourceDesc>
891       <uri>http://www.dhs.gov/dhspublic/getAdvisoryImage</uri>
892     </resource>
893     <area>
894       <areaDesc>U.S. nationwide and interests worldwide</areaDesc>
895     </area>
896   </info>
897 </alert>
```

898

899 A.2. Severe Thunderstorm Warning

900 The following is a speculative example in the form of a CAP XML message.

```
901 <?xml version = "1.0" encoding = "UTF-8"?>
902 <alert xmlns = "urn:oasis:names:tc:emergency:cap:1.2">
903   <identifier>KSTO1055887203</identifier>
904   <sender>KSTO@NWS.NOAA.GOV</sender>
905   <sent>2003-06-17T14:57:00-07:00</sent>
906   <status>Actual</status>
907   <msgType>Alert</msgType>
908   <scope>Public</scope>
909   <info>
910     <category>Met</category>
911     <event>SEVERE THUNDERSTORM</event>
912     <responseType>Shelter</responseType>
913     <urgency>Immediate</urgency>
914     <severity>Severe</severity>
915     <certainty>Observed</certainty>
916     <eventCode>
917       <valueName>SAME</valueName>
918       <value>SVR</value>
919     </eventCode>
920     <expires>2003-06-17T16:00:00-07:00</expires>
921     <senderName>NATIONAL WEATHER SERVICE SACRAMENTO CA</senderName>
922     <headline>SEVERE THUNDERSTORM WARNING</headline>
923     <description> AT 254 PM PDT..NATIONAL WEATHER SERVICE DOPPLER RADAR INDICATED A SEVERE
924 THUNDERSTORM OVER SOUTH CENTRAL ALPINE COUNTY...OR ABOUT 18 MILES SOUTHEAST OF KIRKWOOD...MOVING
925 SOUTHWEST AT 5 MPH. HAIL...INTENSE RAIN AND STRONG DAMAGING WINDS ARE LIKELY WITH THIS
926 STORM.</description>
927     <instruction>TAKE COVER IN A SUBSTANTIAL SHELTER UNTIL THE STORM PASSES.</instruction>
928     <contact>BARUFFALDI/JUSKIE</contact>
929     <area>
930       <areaDesc>EXTREME NORTH CENTRAL TUOLUMNE COUNTY IN CALIFORNIA, EXTREME NORTHEASTERN
931 CALAVERAS COUNTY IN CALIFORNIA, SOUTHWESTERN ALPINE COUNTY IN CALIFORNIA</areaDesc>
932       <polygon>38.47,-120.14 38.34,-119.95 38.52,-119.74 38.62,-119.89 38.47,-120.14</polygon>
933       <geocode>
934         <valueName>SAME</valueName>
935         <value>006109</value>
936       </geocode>
937       <geocode>
938         <valueName>SAME</valueName>
939         <value>006009</value>
940       </geocode>
941       <geocode>
942         <valueName>SAME</valueName>
943         <value>006003</value>
944       </geocode>
945     </area>
946   </info>
947 </alert>
```

948

949 A.3. Earthquake Report (Update Message)

950 The following is a speculative example in the form of a CAP XML message.

```
951 <?xml version = "1.0" encoding = "UTF-8"?>
952 <alert xmlns = "urn:oasis:names:tc:emergency:cap:1.2">
953   <identifier>TRI13970876.2</identifier>
954   <sender>trinet@caltech.edu</sender>
955   <sent>2003-06-11T20:56:00-07:00</sent>
956   <status>Actual</status>
957   <msgType>Update</msgType>
958   <scope>Public</scope>
959   <references>trinet@caltech.edu,TRI13970876.1,2003-06-11T20:30:00-07:00</references>
960   <info>
961     <category>Geo</category>
962     <event>Earthquake</event>
963     <urgency>Past</urgency>
964     <severity>Minor</severity>
965     <certainty>Observed</certainty>
966     <senderName>Southern California Seismic Network (TriNet) operated by Caltech and
967     USGS</senderName>
968     <headline>EQ 3.4 Imperial County CA</headline>
969     <description>A minor earthquake measuring 3.4 on the Richter scale occurred near Brawley,
970     California at 8:53 PM Pacific Daylight Time on Wednesday, June 11, 2003. (This event has now been
971     reviewed by a seismologist)</description>
972     <web>http://www.trinet.org/scsn/scsn.html</web>
973     <parameter>
974       <valueName>EventID</valueName>
975       <value>13970876</value>
976     </parameter>
977     <parameter>
978       <valueName>Version</valueName>
979       <value>1</value>
980     </parameter>
981     <parameter>
982       <valueName>Magnitude</valueName>
983       <value>3.4 Ml</value>
984     </parameter>
985     <parameter>
986       <valueName>Depth</valueName>
987       <value>11.8 mi.</value>
988     </parameter>
989     <parameter>
990       <valueName>Quality</valueName>
991       <value>Excellent</value>
992     </parameter>
993     <area>
994       <areaDesc>1 mi. WSW of Brawley, CA; 11 mi. N of El Centro, CA; 30 mi. E of OCOTILLO
995       (quarry); 1 mi. N of the Imperial Fault</areaDesc>
996       <circle>32.9525,-115.5527 0</circle>
997     </area>
998   </info>
999 </alert>
```

1000

1001 A.4. AMBER Alert (Multilingual Message)

1002 The following is a speculative example in the form of a CAP XML message.

```
1003 <?xml version = "1.0" encoding = "UTF-8"?>
1004 <alert xmlns = "urn:oasis:names:tc:emergency:cap:1.2">
1005   <identifier>KAR0-0306112239-SW</identifier>
1006   <sender>KARO@CLETS.DOJ.CA.GOV</sender>
1007   <sent>2003-06-11T22:39:00-07:00</sent>
1008   <status>Actual</status>
1009   <msgType>Alert</msgType>
1010   <source>SW</source>
1011   <scope>Public</scope>
1012   <info>
1013     <language>en-US</language>
1014     <category>Rescue</category>
1015     <event>Child Abduction</event>
1016     <urgency>Immediate</urgency>
1017     <severity>Severe</severity>
1018     <certainty>Likely</certainty>
1019     <eventCode>
1020       <valueName>SAME</valueName>
1021       <value>CAE</value>
1022     </eventCode>
1023     <senderName>Los Angeles Police Dept - LAPD</senderName>
1024     <headline>Amber Alert in Los Angeles County</headline>
1025     <description>DATE/TIME: 06/11/03, 1915 HRS. VICTIM(S): KHAYRI DOE JR. M/B BLK/BRO 3'0", 40
1026 LBS. LIGHT COMPLEXION. DOB 06/24/01. WEARING RED SHORTS, WHITE T-SHIRT, W/BLEU COLLAR.
1027 LOCATION: 5721 DOE ST., LOS ANGELES, CA. SUSPECT(S): KHAYRI DOE SR. DOB 04/18/71 M/B, BLK HAIR,
1028 BRO EYE. VEHICLE: 81' BUICK 2-DR, BLUE (4XXX000).</description>
1029     <contact>DET. SMITH, 77TH DIV, LOS ANGELES POLICE DEPT-LAPD AT 213 485-2389</contact>
1030     <area>
1031       <areaDesc>Los Angeles County</areaDesc>
1032       <geocode>
1033         <valueName>SAME</valueName>
1034         <value>006037</value>
1035       </geocode>
1036     </area>
1037   </info>
1038   <info>
1039     <language>es-US</language>
1040     <category>Rescue</category>
1041     <event>Abducción de Niño</event>
1042     <urgency>Immediate</urgency>
1043     <severity>Severe</severity>
1044     <certainty>Likely</certainty>
1045     <eventCode>
1046       <valueName>SAME</valueName>
1047       <value>CAE</value>
1048     </eventCode>
1049     <senderName>Departamento de Policía de Los Ángeles - LAPD</senderName>
1050     <headline>Alerta Amber en el condado de Los Ángeles</headline>
1051     <description>DATE/TIME: 06/11/03, 1915 HORAS. VÍCTIMAS: KHAYRI DOE JR. M/B BLK/BRO 3'0", 40
1052 LIBRAS. TEZ LIGERA. DOB 06/24/01. CORTOCIRCUITOS ROJOS QUE USAN, CAMISETA BLANCA, COLLAR DE
1053 W/BLEU. LOCALIZACIÓN: 5721 DOE ST., LOS ANGELES. SOSPECHOSO: KHAYRI DOE ST. DOB 04/18/71 M/B,
1054 PELO DEL NEGRO, OJO DE BRO. VEHÍCULO: 81' BUICK 2-DR, AZUL (4XXX000)</description>
1055     <contact>DET. SMITH, 77TH DIV, LOS ANGELES POLICE DEPT-LAPD AT 213 485-2389</contact>
1056     <area>
1057       <areaDesc>condado de Los Ángeles</areaDesc>
1058       <geocode>
1059         <valueName>SAME</valueName>
1060         <value>006037</value>
1061       </geocode>
1062     </area>
1063   </info>
1064 </alert>
```

1065 **Appendix B. Acknowledgments**

1066 **OASIS Emergency Management Technical Committee**

- 1067 Doug Allport, Canadian Association for Public Alerting and Notification (CAPAN)
- 1068 Patti Aymond, IEM
- 1069 Himadri Banerjee, Previstar Inc.
- 1070 Frank Bell, Individual
- 1071 Art Botterell, Contra Costa County Community Warning System
- 1072 John Bradley, Individual
- 1073 Rex Brooks, Individual
- 1074 Robert Bunge, NOAA's National Weather Service
- 1075 Toby Considine, University of North Carolina at Chapel Hill
- 1076 William Cox, Cox, Associate
- 1077 Olivier Dubuisson, France Telecom
- 1078 Sukumar Dwarkanath, Associate
- 1079 David Ellis, Sandia National Laboratories
- 1080 Thomas Ferrentino, Individual
- 1081 Jack Fox, US Department of Homeland Security
- 1082 Patrick Gannon, Warning Systems, Inc.
- 1083 Timothy Gilmore, US Department of Homeland Security
- 1084 James Goodson, US Department of Homeland Security
- 1085 Tim Grapes, Evolution Technologies Inc.
- 1086 Gary Ham, Individual
- 1087 Harry Haury, NuParadigm Government Systems, Inc.
- 1088 Werner Joerg, IEM
- 1089 Elysa Jones, Warning Systems, Inc.
- 1090 Jeff Jortner, Sandia National Laboratories
- 1091 William Kalin, US Department of Homeland Security
- 1092 Ram Kumar, Individual
- 1093 Jeff Kyser, Warning Systems, Inc.
- 1094 Ron Lake, Galdos Systems Inc.
- 1095 David Lamendsdorf, Emergency Interoperability Consortium
- 1096 Mike McDougall, Individual
- 1097 Donald McGarry, Mitre Corporation
- 1098 Tom Merkle, Lockheed Martin
- 1099 Enoch Moses, ManTech Enterprise Integration Center (e-IC)
- 1100 Brian Nelson, Sandia National Laboratories
- 1101 Camille Osterloh, US Department of Homeland Security
- 1102 John Pitale, Edmond Scientific Company
- 1103 Mark Pleimann, Mitre Corporation
- 1104 Donald Ponikvar, US Department of Homeland Security
- 1105 Jacqueline Postell, US Department of Homeland Security
- 1106 Carl Reed, Open Geospatial Consortium, Inc. (OGC)
- 1107 Dean Reese, ESI Acquisition, Inc.
- 1108 Kirby Rice, Associate
- 1109 Howard Ryan, Desktop Alert Inc.
- 1110 Tracy Ryan, Emergency Interoperability Consortium
- 1111 Josh Shows, ESI Acquisition, Inc.
- 1112 Aviv Siegel, AtHoc, Inc.
- 1113 Andrew Sonner, Evolution Technologies Inc.
- 1114 Christopher Springer, US Department of Homeland Security
- 1115 Steve Streetman, US Department of Homeland Security
- 1116 Lee Tincher, Evolution Technologies Inc.

1117 James Trawick, viaRadio Corporation
1118 Alessandro Triglia, OSS Nokalva
1119 Richard Vandame, US Department of Homeland Security
1120 Matt Walton, Individual
1121 Jeff Waters, US Department of Defense (DoD)
1122 David Webber, Individual
1123 Jacob Westfall, Individual
1124 David Yarbrough, Northrop Grumman
1125
1126

Appendix C. Revision History

Rev	Date	By Whom	What
1.2	2009-09-29	Jacob Westfall	Technical Committee approved the v. 1.2 draft submitted by the Messaging Subcommittee with a change made to responseType in the ASN.1 schema.
1.2	2009-09-17	Jacob Westfall	<p>Messaging Subcommittee approved changes based on initial public comment period:</p> <ul style="list-style-type: none"> • Expanded the scope of the <addresses> element • Changed <mimeType> to be a required element and added note for <size> • Qualified the base schema types in the schema • Changed the schema typing for <altitude> and <ceiling> to be a decimal instead of a string • ASN.1 examples were added <p>Various editorial corrections</p>
1.2	2009-04-28	Jacob Westfall	<p>Technical Committee approved the v. 1.2 draft with the following additional changes:</p> <ul style="list-style-type: none"> • DateTime Data Type moved to Implementation Notes • Changes to <status> and <note> descriptions • Wording change to <severity> "Minor" • Schema changed to allow only one <EncryptedData> element and changed Security Note section to allow multiple <Signature> elements <p>Various editorial corrections and clarifications</p>
1.2	2009-04-14	Jacob Westfall	<p>Messaging Subcommittee approved v. 1.2 draft for submission to full Technical Committee:</p> <ul style="list-style-type: none"> • Multiple XML signature/encryption elements • Editorial changes to History and Character Entity References sections • DateTime Data Type examples • Fixed DOM display
1.2	2009-03-31	Jacob Westfall	<p>Applied changes per recommendations identified by CAP comments process and profile development:</p> <ul style="list-style-type: none"> • Includes CAP 1.1 Errata and ASN.1 Schema • DateTime Data Type to further define the acceptable date and time values • New <responseType> values of Avoid and AllClear • Clarification on acceptable <polygon> values and the use of character entity references • Schemas were updated to reflect changes and to validate when XML signature/encryption elements are present • Conformance section added • Updated CAP Alert Message Examples <p>Various editorial corrections and clarifications</p>

1.1 Errata	2007-10-02		CAP 1.1 Errata approved (see CAP 1.1 Errata document for prior change history)
1.1	2005-09-30		CAP 1.1 adopted as OASIS Standard (see CAP 1.1 specification document for prior change history)
1.1	2005-07-27	Art Botterell	Edits to conform object model, data dictionary and schema: <ul style="list-style-type: none"> Reordered items in object diagram and data dictionary to match sequence required by schema. Edited schema to make <scope> mandatory and to permit multiple instances of <responseType> and <eventCode>, in accordance with the data dictionary.
1.1	2005-07-23	Art Botterell	Applied changes per recommendations of Messaging Subcommittee based on initial public comment period: <ul style="list-style-type: none"> Modified XML syntax of <eventCode> , <parameter> and <geocode> Added "Draft" value for <status> Changed CAP namespace to URN form Tightened usage of dateTime formats in <sent>, <effective>, <onset> and <expiration> Corrected schema to correct value of "CBRNE" in <event> Conformed examples in Appendix A to new namespace.
1.1	2005-04-28	Elysa Jones	Technical Committee approved the v. 1.1 draft with the following additional changes: <ul style="list-style-type: none"> Normative language added to specify uniqueness of <identifier> Change [dateTime] format for <sent>, <effective>, <onset> and <expires> elements Change <language> element RFC from 1166 to 3066 and added null Changed the <mineType> element RFC 1521 to 2046 Added <derefURI> element Security Note updated and added Digital Signature and Encryption note paragraphs
1.1	2005-01-04	Art Botterell	Messaging Subcommittee approved v. 1.1 draft for submission to full Technical Committee: <ul style="list-style-type: none"> Added <responseType> element Made <category> element mandatory Amended enumerated values for the <certainty> element Deleted the <password> element Various editorial corrections and clarifications
1.0	2004-04-01	Art Botterell	CAP 1.0 adopted as OASIS Standard (see CAP 1.0 specification document for prior change history.)