



# Common Alerting Protocol Version 1.2

## Public Review Draft 01

28 April 2009

### Specification URIs:

#### This 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)

#### Previous Version:

[NA]

#### 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](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](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.

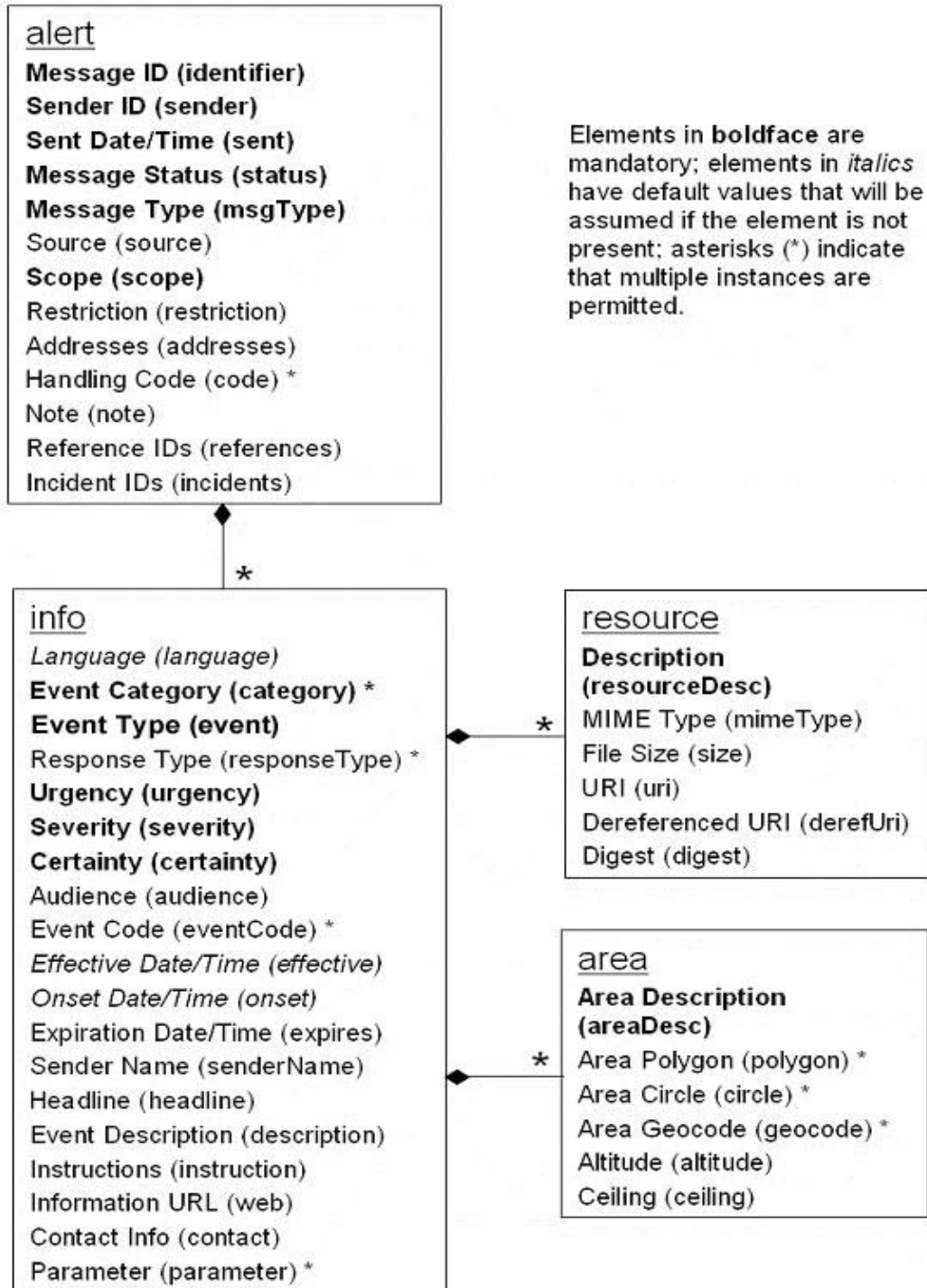
219 In this way, not only is the reliability and reach of the overall warning system maximized, but citizens also  
220 get corroboration of the alert through multiple channels, which increases the chance of the warning being  
221 acted upon.

#### 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
<b>3.2.1 "alert" Element and Sub-elements</b>			
<b>alert</b>	<b>cap. alert. group</b>	<b>The container for all component parts of the alert message (REQUIRED)</b>	<p>(1) Surrounds CAP alert message sub-elements.</p> <p>(2) MUST include the xmlns attribute referencing the CAP URN as the namespace, e.g.:</p> <pre>&lt;cap:alert xmlns:cap="urn:oasis:names:tc:emergency:cap:1.2"&gt;   [sub-elements] &lt;/cap:alert&gt;</pre> <p>(3) In addition to the specified sub-elements, MAY contain one or more &lt;info&gt; blocks.</p>
<b>identifier</b>	<b>cap. alert. identifier. identifier</b>	<b>The identifier of the alert message (REQUIRED)</b>	<p>(1) A number or string uniquely identifying this message, assigned by the sender.</p> <p>(2) MUST NOT include spaces, commas or restricted characters (&lt; and &amp;).</p>
<b>sender</b>	<b>cap. alert. sender. identifier</b>	<b>The identifier of the sender of the alert message (REQUIRED)</b>	<p>(1) Identifies the originator of this alert. Guaranteed by assigner to be unique globally; e.g., may be based on an Internet domain name.</p> <p>(2) MUST NOT include spaces, commas or restricted characters (&lt; and &amp;).</p>
<b>sent</b>	<b>cap. alert. sent. time</b>	<b>The time and date of the origination of the alert message (REQUIRED)</b>	<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
<b>status</b>	<b>cap. alert. status. code</b>	<b>The code denoting the appropriate handling of the alert message (REQUIRED)</b>	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
<b>msgType</b>	<b>cap. alert. msgType. code</b>	<b>The code denoting the nature of the alert message (REQUIRED)</b>	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.
<b>scope</b>	<b>cap. alert. scope. code</b>	<b>The code denoting the intended distribution of the alert message (REQUIRED)</b>	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)	<ul style="list-style-type: none"> <li>(1) Used when &lt;scope&gt; value is "Private".</li> <li>(2) Each recipient SHALL be identified by an identifier or an address.</li> <li>(3) Multiple space-delimited addresses MAY be included. Addresses including whitespace MUST be enclosed in double-quotes.</li> </ul>
code	cap. alert. code. code	The code denoting the special handling of the alert message (OPTIONAL)	<ul style="list-style-type: none"> <li>(1) Any user-defined flag or special code used to flag the alert message for special handling.</li> <li>(2) Multiple instances MAY occur.</li> </ul>
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)	<ul style="list-style-type: none"> <li>(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.</li> <li>(2) If multiple messages are referenced, they SHALL be separated by whitespace.</li> </ul>

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"> <li>(1) Used to collate multiple messages referring to different aspects of the same incident.</li> <li>(2) If multiple incident identifiers are referenced, they SHALL be separated by whitespace. Incident names including whitespace SHALL be surrounded by double-quotes.</li> </ul>
<b>3.2.2 "info" Element and Sub-elements</b>			
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"> <li>(1) Multiple occurrences are permitted within a single &lt;alert&gt;. If targeting of multiple &lt;info&gt; 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 &lt;info&gt; blocks containing the same language identifier SHALL be treated as a separate sequence.</li> <li>(2) In addition to the specified sub-elements, MAY contain one or more &lt;resource&gt; blocks and/or one or more &lt;area&gt; blocks.</li> </ul>
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"> <li>(1) Code Values: Natural language identifier per <b>[RFC 3066]</b>.</li> <li>(2) If not present, an implicit default value of "en-US" SHALL be assumed.</li> <li>(3) A null value in this element SHALL be considered equivalent to "en-US."</li> </ul>



Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
<b>category</b>	<b>cap. alertInfo. category. code</b>	<b>The code denoting the category of the subject event of the alert message (REQUIRED)</b>	<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 &lt;info&gt; block.</p>
<b>event</b>	<b>cap. alertInfo. event. text</b>	<b>The text denoting the type of the subject event of the alert message (REQUIRED)</b>	

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 &lt;instruction&gt;</p> <p>“Evacuate” – Relocate as instructed in the &lt;instruction&gt;</p> <p>“Prepare” – Make preparations per the &lt;instruction&gt;</p> <p>“Execute” – Execute a pre-planned activity identified in &lt;instruction&gt;</p> <p>“Avoid” – Avoid the subject event as per the &lt;instruction&gt;</p> <p>“Monitor” – Attend to information sources as described in &lt;instruction&gt;</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 &lt;instruction&gt;</p> <p>“None” – No action recommended</p> <p>(2) Multiple instances MAY occur within an &lt;info&gt; block.</p>
<b>urgency</b>	<b>cap. alertInfo. urgency. code</b>	<b>The code denoting the urgency of the subject event of the alert message (REQUIRED)</b>	<p>(1) The &lt;urgency&gt;, &lt;severity&gt;, and &lt;certainty&gt; 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	<b>The code denoting the severity of the subject event of the alert message (REQUIRED)</b>	<p>(1) The &lt;urgency&gt;, &lt;severity&gt;, and &lt;certainty&gt; 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	<b>The code denoting the certainty of the subject event of the alert message (REQUIRED)</b>	<p>(1) The &lt;urgency&gt;, &lt;severity&gt;, and &lt;certainty&gt; 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 &gt; ~50%)</p> <p>“Possible” - Possible but not likely (p &lt;= ~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>&lt;eventCode&gt;   &lt;valueName&gt;valueName&lt;/valueName&gt;   &lt;value&gt;value&lt;/value&gt; &lt;/eventCode&gt;</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 &lt;info&gt; 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 &lt;sent&gt;.</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 data-bbox="899 974 1386 1108">&lt;parameter&gt;   &lt;valueName&gt;valueName&lt;/valueName&gt;   &lt;value&gt;value&lt;/value&gt; &lt;/parameter&gt;</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 &lt;info&gt; block.</p>

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
<b>3.2.3 "resource" Element and Sub-elements</b>			
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	<b>The text describing the type and content of the resource file (REQUIRED)</b>	The human-readable text describing the type and content, such as "map" or "photo", of the resource file.
contentType	cap. alertInfoResource. contentType. identifier	The identifier of the MIME content type and sub-type describing the resource file (OPTIONAL)	MIME content type and sub-type as described in <b>[RFC 2046]</b> . (As of this document, the current IANA registered MIME types are listed at <a href="http://www.iana.org/assignments/media-types/">http://www.iana.org/assignments/media-types/</a> )
size	cap. alertInfoResource. size. integer	The integer indicating the size of the resource file (OPTIONAL)	Approximate size of the resource file in bytes.
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 &lt;uri&gt; 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 &lt;derefUri&gt; element and SHOULD extract the file contents and provide a &lt;uri&gt; 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 <b>[FIPS 180-2]</b> .
<b>3.2.4 "area" Element and Sub-elements</b>			
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 &lt;info&gt; block is the union of all the included &lt;area&gt; blocks.</p> <p>(2) MAY contain one or multiple instances of &lt;polygon&gt;, &lt;circle&gt; or &lt;geocode&gt;. If multiple &lt;polygon&gt;, &lt;circle&gt; or &lt;geocode&gt; elements are included, the area described by this &lt;area&gt; 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	<b>The text describing the affected area of the alert message (REQUIRED)</b>	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 <b>[WGS 84]</b> coordinate pairs. (See WGS 84 Note at end of this section)</p> <p>(2) A minimum of 4 coordinate pairs <b>MUST</b> be present and the first and last pairs of coordinates <b>MUST</b> be the same.</p> <p>(3) Multiple instances <b>MAY</b> occur within an &lt;area&gt; 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 <b>[WGS 84]</b> 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 <b>MAY</b> occur within an &lt;area&gt; 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>&lt;parameter&gt;   &lt;valueName&gt;valueName&lt;/valueName&gt;   &lt;value&gt;value&lt;/value&gt; &lt;/parameter&gt;</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 &lt;area&gt; 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 &lt;polygon&gt; and &lt;circle&gt; 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 &lt;ceiling&gt; 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 <b>[WGS 84]</b> 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 &lt;altitude&gt; element.</p> <p>(2) The ceiling measure is in feet above mean sea level per the <b>[WGS 84]</b> 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. &nbsp;) 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 [XMLSIG]. 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 MAY inform the user of their failure to  
283 validate the signature.

284 In other words, the presence of an element with the namespace URI [XMLSIG] 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 <schema xmlns = "http://www.w3.org/2001/XMLSchema"  
295   targetNamespace = "urn:oasis:names:tc:emergency:cap:1.2"  
296   xmlns:cap = "urn:oasis:names:tc:emergency:cap:1.2"  
297   xmlns:xs = "http://www.w3.org/2001/XMLSchema"  
298   elementFormDefault = "qualified"  
299   attributeFormDefault = "unqualified">  
300   <element name = "alert">  
301     <annotation>  
302       <documentation>CAP Alert Message (version 1.2)</documentation>  
303     </annotation>  
304     <complexType>  
305       <sequence>  
306         <element name = "identifier" type = "string"/>  
307         <element name = "sender" type = "string"/>  
308         <element name = "sent">  
309           <simpleType>  
310             <restriction base = "dateTime">  
311               <pattern value = "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,+] \d\d:\d\d"/>  
312             </restriction>  
313           </simpleType>  
314         </element>  
315         <element name = "status">  
316           <simpleType>  
317             <restriction base = "string">  
318               <enumeration value = "Actual"/>  
319               <enumeration value = "Exercise"/>  
320               <enumeration value = "System"/>  
321               <enumeration value = "Test"/>  
322               <enumeration value = "Draft"/>  
323             </restriction>  
324           </simpleType>  
325         </element>  
326         <element name = "msgType">  
327           <simpleType>  
328             <restriction base = "string">  
329               <enumeration value = "Alert"/>  
330               <enumeration value = "Update"/>  
331               <enumeration value = "Cancel"/>  
332               <enumeration value = "Ack"/>  
333               <enumeration value = "Error"/>  
334             </restriction>  
335           </simpleType>  
336         </element>  
337         <element name = "source" type = "string" minOccurs = "0"/>  
338         <element name = "scope">  
339           <simpleType>  
340             <restriction base = "string">  
341               <enumeration value = "Public"/>  
342               <enumeration value = "Restricted"/>  
343               <enumeration value = "Private"/>  
344             </restriction>  
345           </simpleType>  
346         </element>  
347       </sequence>  
348     </complexType>  
349   </element>  
350 </schema>
```

```

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

```

```

427     <complexType>
428       <sequence>
429         <element ref = "cap:valueName"/>
430         <element ref = "cap:value"/>
431       </sequence>
432     </complexType>
433 </element>
434 <element name = "effective" minOccurs = "0">
435   <simpleType>
436     <restriction base = "dateTime">
437       <pattern value = "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,+] \d\d:\d\d"/>
438     </restriction>
439   </simpleType>
440 </element>
441 <element name = "onset" minOccurs = "0">
442   <simpleType>
443     <restriction base = "dateTime">
444       <pattern value = "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,+] \d\d:\d\d"/>
445     </restriction>
446   </simpleType>
447 </element>
448 <element name = "expires" minOccurs = "0">
449   <simpleType>
450     <restriction base = "dateTime">
451       <pattern value = "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,+] \d\d:\d\d"/>
452     </restriction>
453   </simpleType>
454 </element>
455 <element name = "senderName" type = "string" minOccurs = "0"/>
456 <element name = "headline" type = "string" minOccurs = "0"/>
457 <element name = "description" type = "string" minOccurs = "0"/>
458 <element name = "instruction" type = "string" minOccurs = "0"/>
459 <element name = "web" type = "anyURI" minOccurs = "0"/>
460 <element name = "contact" type = "string" minOccurs = "0"/>
461 <element name = "parameter" minOccurs = "0" maxOccurs = "unbounded">
462   <complexType>
463     <sequence>
464       <element ref = "cap:valueName"/>
465       <element ref = "cap:value"/>
466     </sequence>
467   </complexType>
468 </element>
469 <element name = "resource" minOccurs = "0" maxOccurs = "unbounded">
470   <complexType>
471     <sequence>
472       <element name = "resourceDesc" type = "string"/>
473       <element name = "mimeType" type = "string" minOccurs = "0"/>
474       <element name = "size" type = "integer" minOccurs = "0"/>
475       <element name = "uri" type = "anyURI" minOccurs = "0"/>
476       <element name = "derefUri" type = "string" minOccurs = "0"/>
477       <element name = "digest" type = "string" minOccurs = "0"/>
478     </sequence>
479   </complexType>
480 </element>
481 <element name = "area" minOccurs = "0" maxOccurs = "unbounded">
482   <complexType>
483     <sequence>
484       <element name = "areaDesc" type = "string"/>
485       <element name = "polygon" type = "string" minOccurs = "0" maxOccurs = "unbounded"/>
486       <element name = "circle" type = "string" minOccurs = "0" maxOccurs = "unbounded"/>
487       <element name = "geocode" minOccurs = "0" maxOccurs = "unbounded">
488         <complexType>
489           <sequence>
490             <element ref = "cap:valueName"/>
491             <element ref = "cap:value"/>
492           </sequence>
493         </complexType>
494       </element>
495       <element name = "altitude" type = "string" minOccurs = "0"/>
496       <element name = "ceiling" type = "string" minOccurs = "0"/>
497     </sequence>
498   </complexType>
499 </element>
500 </sequence>
501 </complexType>
502 </element>
503 <any minOccurs = "0" maxOccurs = "unbounded" namespace = "http://www.w3.org/2000/09/xmldsig#"
504 processContents = "lax"/>
505 <any minOccurs = "0" namespace = "http://www.w3.org/2000/09/xmlenc#" processContents = "lax"/>
506 </sequence>
507 </complexType>
508 </element>

```

```
509 <element name = "valueName" type = "string"/>
510 <element name = "value" type = "string"/>
511 </schema>
512
513
514
```

## 515 3.5 Use of ASN.1 to Specify and Encode the CAP Alert Message

### 516 3.5.1 General

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

### 522 3.5.2 Formal Mappings and Specification

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

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

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

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

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

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

### 538 3.5.3 ASN.1 Schema

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



```

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

```

```

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

```

```

693         moderate,
694         severe,
695         unknown }
696
697 HowCertain ::= ENUMERATED {
698     likely,
699     observed,
700     possible,
701     unknown,
702     unlikely }
703
704 ResourceFile ::= SEQUENCE {
705     -- Information about an associated resource file
706     -- (see 3.2.3)
707     resourceDesc String,
708     -- Not standardised human-readable description of the type
709     -- and content of
710     -- an associated resource file (for example a map or
711     -- photograph) (see 3.2.3)
712     mimeType      String OPTIONAL,
713     size          INTEGER OPTIONAL, -- In bytes
714     uri          AnyURI OPTIONAL,
715     derefUri     String OPTIONAL,
716     -- An alternative to the URI giving the Base64-encoded
717     -- content of the resource file (see 3.2.3)
718     digest       String OPTIONAL
719     -- SHA-1 hash of the resource file for error detection
720     -- (see 3.2.3) -- }
721
722 Area ::= SEQUENCE {
723     -- Identification of an affected area
724     areaDesc      String,
725     -- Not standardised human-readable description of the area
726     polygon-list SEQUENCE OF polygon String,
727     -- Each element is a space-separated list of coordinate pairs
728     -- The complete list starts and ends with the same point and
729     -- defines the polygon that defines the area
730     -- (see 3.2.4).
731     circle-list SEQUENCE OF circle String,
732     -- A space-separated list of coordinates for a point and a radius
733     geocode-list SEQUENCE SIZE((0..MAX)) OF geocode SEQUENCE {
734     -- A geographic code designating the alert target area
735     -- (see 3.2.4)
736         valueName ValueName,
737         value      Value },
738     altitude      String OPTIONAL,
739     -- Specific or minimum altitude of the affected area
740     ceiling       String OPTIONAL
741     -- Maximum altitude of the affected area -- }
742
743 ValueName ::= String -- A not standardised name for
744     -- an information event code, a parameter or a geocode
745
746 Value ::= String -- The value of the information event code,
747     -- parameter or geocode
748
749 String ::= UTF8String (FROM (
750     {0,0,0,9} -- TAB
751     | {0,0,0,10} -- CR
752     | {0,0,0,13} -- LF
753     | {0,0,0,32}..{0,0,215,255} -- Space to the start of the S-zone
754     | {0,0,224,0}..{0,0,255,253} -- Rest of BMP after S-zone
755     | {0,1,0,0}..{0,16,255,253} -- Other planes -- ) )
756

```

```

757 StringChar ::= String (SIZE(1))
758
759 SpaceAndComma ::= UTF8String (FROM (
760     {0,0,0,32} -- SPACE
761     | {0,0,0,44} -- COMMA -- ) )
762
763 IdentifierString ::= String (FROM (StringChar EXCEPT SpaceAndComma))
764
765 Language ::= VisibleString(FROM ("a".."z" | "A".."Z" | "-" | "0".."9"))
766     (PATTERN "[a-zA-Z]#(1,8) (-[a-zA-Z0-9]#(1,8))*")
767     -- The semantics of Language is specified in IETF RFC 3066
768
769 DateTime ::= TIME (SETTINGS "Basic=Date-Time Date=YMD
770     Year=Basic Time=HMS Local-or-UTC=LD")
771     -- This is the ISO 8601 format using local time and a
772     -- time difference
773
774 stringWithNoCRLFHT ::= UTF8String (FROM (
775     {0,0,0,32}..{0,0,215,255}
776     | {0,0,224,0}..{0,0,255,253}
777     | {0,1,0,0}..{0,16,255,255}))
778
779 AnyURI ::= stringWithNoCRLFHT (CONSTRAINED BY {
780     /* Shall be a valid URI as defined in IETF RFC 2396 */)
781
782 ENCODING-CONTROL XER
783     GLOBAL-DEFAULTS MODIFIED-ENCODINGS
784     GLOBAL-DEFAULTS CONTROL-NAMESPACE
785     "http://www.w3.org/2001/XMLSchema-instance" PREFIX "xsi"
786     NAMESPACE ALL, ALL IN ALL AS "urn:oasis:names:tc:emergency:cap:1.2"
787     PREFIX "cap"
788     NAME Alert, Area AS UNCAPITALIZED
789     UNTAGGED SEQUENCE OF
790     DEFAULT-FOR-EMPTY AlertInformation.language AS "en-US"
791     TEXT AlertStatus:ALL,
792     AlertMessageType:ALL,
793     AlertScope:ALL,
794     InformationCategory:ALL,
795     InformationResponseType:ALL,
796     HowUrgent:ALL,
797     HowSevere:ALL,
798     HowCertain:ALL AS CAPITALIZED
799     WHITESPACE Language, AnyURI COLLAPSE
800 END

```

801

---

## 802 4 Conformance

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

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

810

### 811 4.1 Conformance Targets

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

- 814 a) CAP V1.2 Message
- 815 b) CAP V1.2 Message Producer
- 816 c) CAP V1.2 Message Consumer

817

### 818 4.2 Conformance as a CAP V1.2 Message

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

- 820 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)  
821 [open.org/emergency/cap/v1.2/CAP-v1.2.xsd](http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.xsd) and
- 822 b) the content of its elements and the values of its attributes meet all the additional mandatory  
823 requirements specified in Section 3.

824

### 825 4.3 Conformance as a CAP V1.2 Message Producer

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

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

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

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

841

#### 842 **4.4 Conformance as a CAP V1.2 Message Consumer**

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

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

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

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

---

## 850 Appendix A. CAP Alert Message Example

### 851 A.1. Homeland Security Advisory System Alert

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

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

890

891 **A.2. Severe Thunderstorm Warning**

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

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

940



### 941 **A.3. Earthquake Report (Update Message)**

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

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

992

## 993 A.4. AMBER Alert (Multilingual Message)

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

```
995 <?xml version = "1.0" encoding = "UTF-8"?>
996 <alert xmlns = "urn:oasis:names:tc:emergency:cap:1.2">
997   <identifier>KAR0-0306112239-SW</identifier>
998   <sender>KAR0@CLETS.DOJ.CA.GOV</sender>
999   <sent>2003-06-11T22:39:00-07:00</sent>
1000   <status>Actual</status>
1001   <msgType>Alert</msgType>
1002   <source>SW</source>
1003   <scope>Public</scope>
1004   <info>
1005     <language>en-US</language>
1006     <category>Rescue</category>
1007     <event>Child Abduction</event>
1008     <urgency>Immediate</urgency>
1009     <severity>Severe</severity>
1010     <certainty>Likely</certainty>
1011     <eventCode>
1012       <valueName>SAME</valueName>
1013       <value>CAE</value>
1014     </eventCode>
1015     <senderName>Los Angeles Police Dept - LAPD</senderName>
1016     <headline>Amber Alert in Los Angeles County</headline>
1017     <description>DATE/TIME: 06/11/03, 1915 HRS. VICTIM(S): KHAYRI DOE JR. M/B BLK/BRO 3'0", 40
1018 LBS. LIGHT COMPLEXION. DOB 06/24/01. WEARING RED SHORTS, WHITE T-SHIRT, W/BUE COLLAR.
1019 LOCATION: 5721 DOE ST., LOS ANGELES, CA. SUSPECT(S): KHAYRI DOE SR. DOB 04/18/71 M/B, BLK HAIR,
1020 BRO EYE. VEHICLE: 81' BUICK 2-DR, BLUE (4XXX000).</description>
1021     <contact>DET. SMITH, 77TH DIV, LOS ANGELES POLICE DEPT-LAPD AT 213 485-2389</contact>
1022     <area>
1023       <areaDesc>Los Angeles County</areaDesc>
1024       <geocode>
1025         <valueName>SAME</valueName>
1026         <value>006037</value>
1027       </geocode>
1028     </area>
1029   </info>
1030   <info>
1031     <language>es-US</language>
1032     <category>Rescue</category>
1033     <event>Abducción de Niño</event>
1034     <urgency>Immediate</urgency>
1035     <severity>Severe</severity>
1036     <certainty>Likely</certainty>
1037     <eventCode>
1038       <valueName>SAME</valueName>
1039       <value>CAE</value>
1040     </eventCode>
1041     <senderName>Departamento de Policía de Los Ángeles - LAPD</senderName>
1042     <headline>Alerta Amber en el condado de Los Ángeles</headline>
1043     <description>DATE/TIME: 06/11/03, 1915 HORAS. VÍCTIMAS: KHAYRI DOE JR. M/B BLK/BRO 3'0", 40
1044 LIBRAS. TEZ LIGERA. DOB 06/24/01. CORTOCIRCUITOS ROJOS QUE USAN, CAMISETA BLANCA, COLLAR DE
1045 W/BUE. LOCALIZACIÓN: 5721 DOE ST., LOS ÁNGELES. SOSPECHOSO: KHAYRI DOE ST. DOB 04/18/71 M/B,
1046 PELO DEL NEGRO, OJO DE BRO. VEHÍCULO: 81' BUICK 2-DR, AZUL (4XXX000)</description>
1047     <contact>DET. SMITH, 77TH DIV, LOS ANGELES POLICE DEPT-LAPD AT 213 485-2389</contact>
1048     <area>
1049       <areaDesc>condado de Los Ángeles</areaDesc>
1050       <geocode>
1051         <valueName>SAME</valueName>
1052         <value>006037</value>
1053       </geocode>
1054     </area>
1055   </info>
1056 </alert>
```

---

## 1057 **Appendix B. Acknowledgments**

### 1058 **OASIS Emergency Management Technical Committee**

1059 Doug Allport, Canadian Association for Public Alerting and Notification (CAPAN)  
1060 Patti Aymond, IEM  
1061 Himadri Banerjee, Previstar Inc.  
1062 Frank Bell, Individual  
1063 Art Botterell, Contra Costa County Community Warning System  
1064 John Bradley, Individual  
1065 Rex Brooks, Individual  
1066 Robert Bunge, NOAA's National Weather Service  
1067 Toby Considine, University of North Carolina at Chapel Hill  
1068 William Cox, Associate  
1069 Olivier Dubuisson, France Telecom  
1070 Sukumar Dwarkanath, Associate  
1071 David Ellis, Sandia National Laboratories  
1072 Thomas Ferrentino, Individual  
1073 Jack Fox, US Department of Homeland Security  
1074 Patrick Gannon, Warning Systems, Inc.  
1075 Timothy Gilmore, US Department of Homeland Security  
1076 James Goodson, US Department of Homeland Security  
1077 Tim Grapes, Evolution Technologies Inc.  
1078 Gary Ham, Individual  
1079 Harry Haury, NuParadigm Government Systems, Inc.  
1080 Werner Joerg, IEM  
1081 Elysa Jones, Warning Systems, Inc.  
1082 William Kalin, US Department of Homeland Security  
1083 Ram Kumar, Individual  
1084 Jeff Kyser, Warning Systems, Inc.  
1085 Ron Lake, Galdos Systems Inc.  
1086 David Lamendsdorf, Emergency Interoperability Consortium  
1087 Mike McDougall, Individual  
1088 Donald McGarry, Mitre Corporation  
1089 Tom Merkle, Lockheed Martin  
1090 Enoch Moses, ManTech Enterprise Integration Center (e-IC)  
1091 Brian Nelson, Sandia National Laboratories  
1092 Camille Osterloh, US Department of Homeland Security  
1093 John Pitale, Edmond Scientific Company  
1094 Mark Pleimann, Mitre Corporation  
1095 Donald Ponikvar, US Department of Homeland Security  
1096 Jacqueline Postell, US Department of Homeland Security  
1097 Carl Reed, Open Geospatial Consortium, Inc. (OGC)  
1098 Dean Reese, ESI Acquisition, Inc.  
1099 Kirby Rice, Associate  
1100 Howard Ryan, Desktop Alert Inc.  
1101 Tracy Ryan, Emergency Interoperability Consortium  
1102 Josh Shows, ESI Acquisition, Inc.  
1103 Aviv Siegel, AtHoc, Inc.  
1104 Andrew Sonner, Evolution Technologies Inc.  
1105 Christopher Springer, US Department of Homeland Security  
1106 Steve Streetman, US Department of Homeland Security  
1107 Lee Tincher, Evolution Technologies Inc.  
1108 James Trawick, viaRadio Corporation

1109 Alessandro Triglia, OSS Nokalva  
1110 Richard Vandame, US Department of Homeland Security  
1111 Matt Walton, Individual  
1112 Jeff Waters, US Department of Defense (DoD)  
1113 David Webber, Individual  
1114 Jacob Westfall, Individual  
1115 David Yarbrough, Northrop Grumman  
1116  
1117

## Appendix C. Revision History

Rev	Date	By Whom	What
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"> <li>• DateTime Data Type moved to Implementation Notes</li> <li>• Changes to &lt;status&gt; and &lt;note&gt; descriptions</li> <li>• Wording change to &lt;severity&gt; "Minor"</li> <li>• Schema changed to allow only one &lt;EncryptedData&gt; element and changed Security Note section to allow multiple &lt;Signature&gt; elements</li> </ul> <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"> <li>• Multiple XML signature/encryption elements</li> <li>• Editorial changes to History and Character Entity References sections</li> <li>• DateTime Data Type examples</li> <li>• Fixed DOM display</li> </ul>
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"> <li>• Includes CAP 1.1 Errata and ASN.1 Schema</li> <li>• DateTime Data Type to further define the acceptable date and time values</li> <li>• New &lt;responseType&gt; values of Avoid and AllClear</li> <li>• Clarification on acceptable &lt;polygon&gt; values and the use of character entity references</li> <li>• Schemas were updated to reflect changes and to validate when XML signature/encryption elements are present</li> <li>• Conformance section added</li> <li>• Updated CAP Alert Message Examples</li> </ul> <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	<p>Edits to conform object model, data dictionary and schema:</p> <ul style="list-style-type: none"> <li>• Reordered items in object diagram and data dictionary to match sequence required by schema.</li> <li>• Edited schema to make &lt;scope&gt; mandatory and to permit multiple instances of &lt;responseType&gt; and &lt;eventCode&gt;, in accordance with the data dictionary.</li> </ul>

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

1119