Common Alerting Protocol Version 1.2

Public Review Draft 03

02 March 2010

Specification URIs:
This Version:

http://docs.oasis-open.org/emergency/cap/v1.2/pr03/CAP-v1.2-PR03.html

http://docs.oasis-open.org/emergency/cap/v1.2/pr03/CAP-v1.2-PR03.pdf

http://docs.oasis-open.org/emergency/cap/v1.2/pr03/CAP-v1.2-PR03.doc (Authoritative)

Previous Version:

http://docs.oasis-open.org/emergency/cap/v1.2/pr02/CAP-v1.2-PR02.html

http://docs.oasis-open.org/emergency/cap/v1.2/pr02/CAP-v1.2-PR02.pdf

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

Latest Version:

http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.html

http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.pdf

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

Technical Committee:

OASIS Emergency Management TC

Chair:

Elysa Jones, Warning Systems, Inc.

Editor:

Jacob Westfall, Individual

Related work:

This specification is related to:

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

Declared XML Namespace:

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

Copyright © OASIS Open 2010. All Rights Reserved.

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/.

Copyright © OASIS Open 2010. All Rights Reserved.

Notices

Copyright © OASIS® 20~~09~~10. 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~~7~~
~~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

Copyright © OASIS Open 2010. All Rights Reserved.

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

Copyright © OASIS Open 2010. All Rights Reserved.

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.

Copyright © OASIS Open 2010. All Rights Reserved.

1.3 Structure of the CAP Alert Message

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

1.3.1 <alert>

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

1.3.2 <info>

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

1.3.3 <resource>

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

1.3.4 <area>

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

1.4 Applications of the CAP Alert Message

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

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

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

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

Copyright © OASIS Open 2010. All Rights Reserved.

1.5 Terminology

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

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

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

1.6 Normative References

[RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, http://www.ietf.org/rfc/rfc2119.txt, IETF RFC 2119, March 1997.

[dateTime] N. Freed, XML Schema Part 2: Datatypes Second Edition, http://www.w3.org/TR/xmlschema-2/#dateTime, W3C REC-xmlschema-2, October 2004.

[FIPS 180-2] National Institute for Standards and Technology, Secure Hash Standard, http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf, August 2002.

[namespaces] T. Bray, Namespaces in XML, http://www.w3.org/TR/REC-xml-names/, W3C REC-xml-names-19990114, January 1999.

[RFC2046] N. Freed, Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types, http://www.ietf.org/rfc/rfc2046.txt, IETF RFC 2046, November 1996.

~~**[RFC2119]** S. Bradner, Key words for use in RFCs to Indicate Requirement Levels, http://www.ietf.org/rfc/rfc2119.txt, IETF RFC 2119, March 1997.~~

[RFC3066] H. Alvestrand, Tags for the Identification of Languages, http://www.ietf.org/rfc/rfc3066.txt, IETF RFC 3066, January 2001.

[WGS 84] National Geospatial Intelligence Agency, Department of Defense World Geodetic System 1984, http://earth-info.nga.mil/GandG/tr8350_2.html, NGA Technical Report TR8350.2, January 2000.

[XML 1.0] T. Bray, Extensible Markup Language (XML) 1.0 (Third Edition), http://www.w3.org/TR/REC-xml/, W3C REC-XML-20040204, February 2004.

[XMLSIG] Eastlake, D., Reagle, J. and Solo, D. (editors), *XML-Signature Syntax and Processing*, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/, W3C Recommendation, February 2002.

~~**[XMLENC]** Eastlake, D. and Reagle, J. (editors), *XML Encryption Syntax and Processing*, http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/, W3C Recommendation, December 2002.~~

[ITU-T X.680] ITU-T Recommendation X.680, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

[ITU-T X.691] ITU-T Recommendation X.691, *Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)*.

[ITU-T X.693] ITU-T Recommendation X.693, Information technology – *ASN.1 encoding rules: Specification of XML Encoding Rules (XER)*.

[ITU-T X.694] ITU-T Recommendation X.694, *Information technology – ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1*.

Copyright © OASIS Open 2010. All Rights Reserved.

2 Design Principles and Concepts (non-normative)

2.1 Design Philosophy

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

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

2.2 Requirements for Design

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

The Common Alerting Protocol SHOULD:

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

Copyright © OASIS Open 2010. All Rights Reserved.

- Geographic targeting
- Level of urgency
- Level of certainty
- Level of threat severity

- Provide a mechanism for referencing supplemental information (e.g., digital audio or image files, additional text);
- Use an established open-standard data representation;
- Be based on a program of real-world cross-platform testing and evaluation;
- Provide a clear basis for certification and further protocol evaluation and improvement; and,
- Provide a clear logical structure that is relevant and clearly applicable to the needs of emergency response and public safety users and warning system operators.

2.3 Examples of Use Scenarios

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

2.3.1 Manual Origination

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

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

2.3.2 Automated Origination by Autonomous Sensor System

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

2.3.3 Aggregation and Correlation on Real-time Map

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

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

Copyright © OASIS Open 2010. All Rights Reserved.

2.3.4 Integrated Public Alerting

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

Each system converts the CAP message data into the form suitable for its technology (text captioning on TV, synthesized voice on radio and telephone, activation of the appropriate signal on sirens, etc.). Systems that can target their messages to particular geographic areas implement the targeting specified in the CAP message with as little 'spillover' as their technology permits.

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

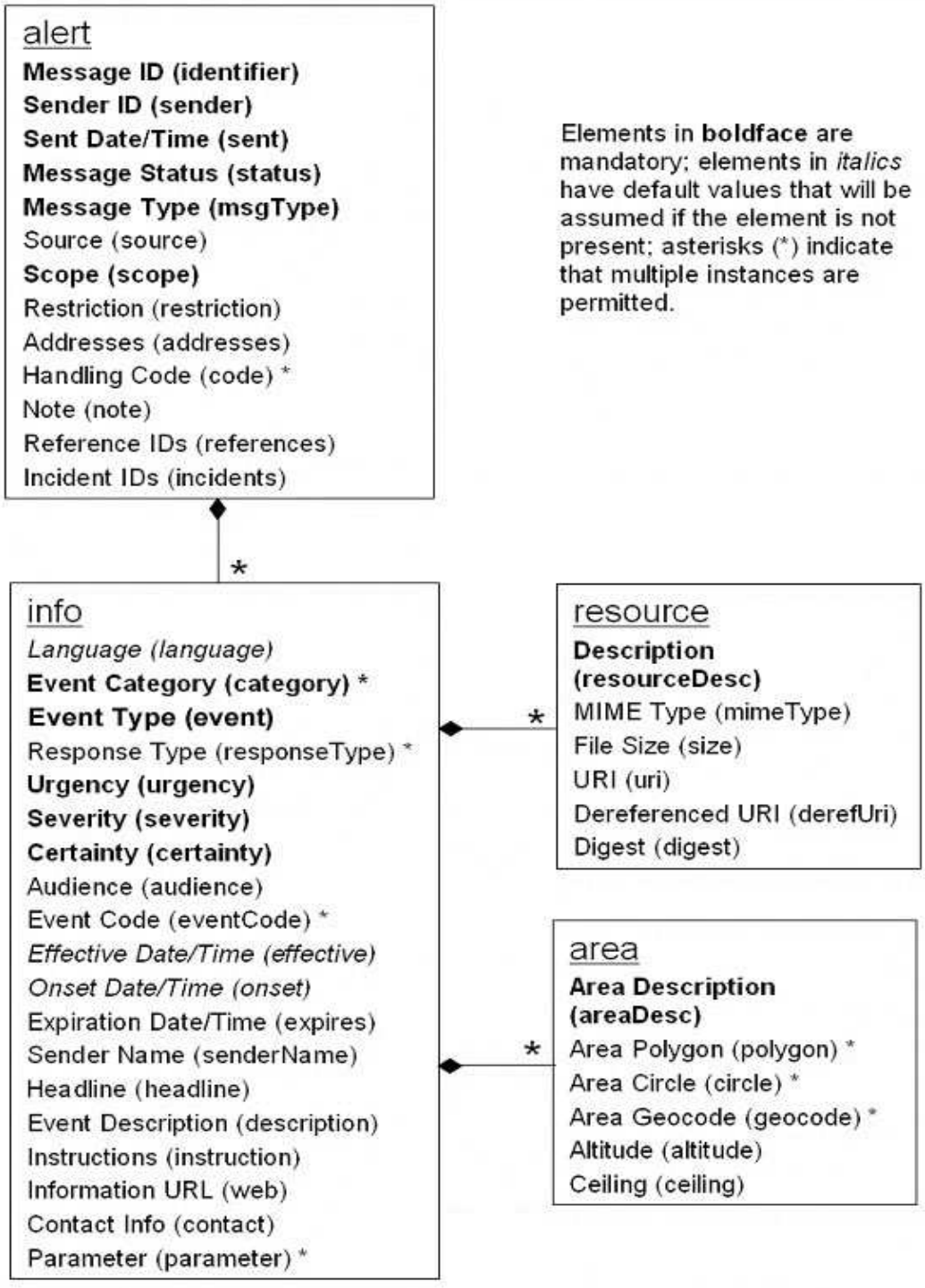
2.3.5 Repudiating a False Alarm

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

Copyright © OASIS Open 2010. All Rights Reserved.

3 Alert Message Structure (normative)

3.1 Document Object Model



Copyright © OASIS Open 2010. All Rights Reserved.

3.2 Data Dictionary

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

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
3.2.1 "alert" Element and Sub-elements			

alert	**cap.
	alert.
	group**
		The container for all component parts of the alert message (REQUIRED)	(1) Surrounds CAP alert message sub-elements.
			(2) MUST include the xmlns attribute referencing the CAP URN as the namespace, e.g.:
			`<cap:alert xmlns:cap="urn:oasis:names:tc:emergency:cap:1.2">`
			`  [sub-elements]`
			`</cap:alert>`
			(3) In addition to the specified sub-elements, MAY contain one or more <info> blocks.

identifier	**cap. alert. identifier. identifier**	**The identifier of the alert message (REQUIRED)**	(1) A number or string uniquely identifying this message, assigned by the sender. (2) MUST NOT include spaces, commas or restricted characters (< and &).
sender	**cap. alert. sender. identifier**	**The identifier of the sender of the alert message (REQUIRED)**	(1) Identifies the originator of this alert. Guaranteed by assigner to be unique globally; e.g., may be based on an Internet domain name. (2) MUST NOT include spaces, commas or restricted characters (< and &).
sent	**cap. alert. sent. time**	**The time and date of the origination of the alert message (REQUIRED)**	(1) The date and time SHALL be represented in the DateTime Data Type (See Implementation Notes) format (e.g., "`2002-05-24T16:49:00-07:00`" for 24 May 2002 at 16:49 PDT). (2) Alphabetic timezone designators such as "Z" MUST NOT be used. The timezone for UTC MUST be represented as "-00:00".

Copyright © OASIS Open 2010. All Rights Reserved.

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

Copyright © OASIS Open 2010. All Rights Reserved.

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)	(1) Required when <scope> is “Private”, optional when <scope> is “Public” or “Restricted”.~~Used when <scope> value is "Private".~~ (2) Each recipient SHALL be identified by an identifier or an address. (3) Multiple space-delimited addresses MAY be included. Addresses including whitespace MUST be enclosed in double-quotes.
code	cap. alert. code. code	The code denoting the special handling of the alert message (OPTIONAL)	(1) Any user-defined flag or special code used to flag the alert message for special handling. (2) Multiple instances MAY occur.
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)	(1) The extended message identifier(s) (in the form *sender,identifier,sent)* of an earlier CAP message or messages referenced by this one. (2) If multiple messages are referenced, they SHALL be separated by whitespace.

Copyright © OASIS Open 2010. All Rights Reserved.

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)	(1) Used to collate multiple messages referring to different aspects of the same incident. (2) If multiple incident identifiers are referenced, they SHALL be separated by whitespace. Incident names including whitespace SHALL be surrounded by double-quotes.

3.2.2 "info" Element and Sub-elements

info	cap. alertInfo. info. group	The container for all component parts of the info sub-element of the alert message (OPTIONAL)	(1) Multiple occurrences are permitted within a single <alert>. If targeting of multiple <info> blocks in the same language overlaps, information in later blocks may expand but may not override the corresponding values in earlier ones. Each set of <info> blocks containing the same language identifier SHALL be treated as a separate sequence. (2) In addition to the specified sub-elements, MAY contain one or more <resource> blocks and/or one or more <area> blocks.
language	cap. alertInfo. language. code	The code denoting the language of the info sub-element of the alert message (OPTIONAL)	(1) Code Values: Natural language identifier per **[RFC 3066].** (2) If not present, an implicit default value of "en-US" SHALL be assumed. (3) A null value in this element SHALL be considered equivalent to “en-US.”

Copyright © OASIS Open 2010. All Rights Reserved.

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

Copyright © OASIS Open 2010. All Rights Reserved.

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

Copyright © OASIS Open 2010. All Rights Reserved.

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

Copyright © OASIS Open 2010. All Rights Reserved.

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)	(1) Any system-specific code for event typing, in the form:
			`<eventCode>`
			`  <valueName>`*`valueName`*`</valueName>`
			`  <value>`*`value`*`</value>`
			`</eventCode>`
			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").
			(2) Values of “valueName” that are acronyms SHOULD be represented in all capital letters without periods (e.g., SAME, FIPS, ZIP).
			(3) Multiple instances MAY occur within an <info> block.

effective	cap. alertInfo. effective. time	The effective time of the information of the alert message (OPTIONAL)	(1) The date and time SHALL be represented in the DateTime Data Type (See Implementation Notes) format (e.g., “`2002-05-24T16:49:00-07:00`” for 24 May 2002 at 16: 49 PDT). (2) Alphabetic timezone designators such as “Z” MUST NOT be used. The timezone for UTC MUST be represented as “-00:00”. (3) If this item is not included, the effective time SHALL be assumed to be the same as in <sent>.
onset	cap. alertInfo. onset. time	The expected time of the beginning of the subject event of the alert message (OPTIONAL)	(1) The date and time SHALL be represented in the DateTime Data Type (See Implementation Notes) format (e.g., “`2002-05-24T16:49:00-07:00`” for 24 May 2002 at 16: 49 PDT). (2) Alphabetic timezone designators such as “Z” MUST NOT be used. The timezone for UTC MUST be represented as “-00:00”.

Copyright © OASIS Open 2010. All Rights Reserved.

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)	(1) The date and time SHALL be represented in the DateTime Data Type (See Implementation Notes) format (e.g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT). (2) Alphabetic timezone designators such as "Z" MUST NOT be used. The timezone for UTC MUST be represented as "-00:00". (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.
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.

Copyright © OASIS Open 2010. All Rights Reserved.

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)	(1) Any system-specific datum, in the form:
			`<parameter>`
			`  <valueName>`*`valueName`*`</valueName>`
			`  <value>`*`value`*`</value>`
			`</parameter>`
			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`").
			(2) Values of “valueName” that are acronyms SHOULD be represented in all capital letters without periods (e.g., SAME, FIPS, ZIP).
			(3) Multiple instances MAY occur within an <info> block.

Copyright © OASIS Open 2010. All Rights Reserved.

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain
3.2.3 "resource" Element and Sub-elements			
resource	cap alertInfoResource. resource. group	The container for all component parts of the resource sub-element of the info sub-element of the alert element (OPTIONAL)	(1) Refers to an additional file with supplemental information related to this <info> element; e.g., an image or audio file. (2) Multiple instances MAY occur within an <info> block.
resourceDesc	**cap.** **alertInfoResource.** **resourceDesc.** **text**	**The text describing the type and content of the resource file (REQUIRED)**	The human-readable text describing the type and content, such as “map” or “photo”, of the resource file.
mimeType	**cap.** **alertInfoResource.** **mimeType.** **identifier**	**The identifier of the MIME content type and sub-type describing the resource file (REQUIREDO PTIONAL)**	MIME content type and sub-type as described in **[RFC 2046].** (As of this document, the current IANA registered MIME types are listed at http://www.iana.org/assignments/media-types/)
size	cap. alertInfoResource. size. integer	The integer indicating the size of the resource file (OPTIONAL)	(1) Approximate size of the resource file in bytes. (2) For <uri> based resources, <size> SHOULD be included if available.
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.

Copyright © OASIS Open 2010. All Rights Reserved.

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)	(1) MAY be used either with or instead of the <uri> element in messages transmitted over one-way (e.g., broadcast) data links where retrieval of a resource via a URI is not feasible. (2) Clients intended for use with one-way data links MUST support this element. (3) This element MUST NOT be used unless the sender is certain that all direct clients are capable of processing it. (4) If messages including this element are forwarded onto a two-way network, the forwarder MUST strip the <derefUri> element and SHOULD extract the file contents and provide a <uri> link to a retrievable version of the file. (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.
digest	cap. alertInfoResource. digest. code	The code representing the digital digest ("hash") computed from the resource file (OPTIONAL)	Calculated using the Secure Hash Algorithm (SHA-1) per **[FIPS 180-2]**.

3.2.4 "area" Element and Sub-elements

area	cap. alertInfoArea. area. group	The container for all component parts of the area sub-element of the info sub-element of the alert message (OPTIONAL)	(1) Multiple occurrences permitted, in which case the target area for the <info> block is the union of all the included <area> blocks. (2) MAY contain one or multiple instances of <polygon>, <circle> or <geocode>. If multiple <polygon>, <circle> or <geocode> elements are included, the area described by this <area> block is represented by the union of all the included elements.

Copyright © OASIS Open 2010. All Rights Reserved.

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

Copyright © OASIS Open 2010. All Rights Reserved.

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

Copyright © OASIS Open 2010. All Rights Reserved.

3.3 Implementation Notes

3.3.1 WGS 84 Note

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

3.3.2 DateTime Data Type

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

- YYYY indicates the year
- MM indicates the month
- DD indicates the day
- T indicates the symbol “T” marking the start of the required time section
- hh indicates the hour
- mm indicates the minute
- ss indicates the second
- X indicates either the symbol “+” if the preceding date and time are in a time zone ahead of UTC, or the symbol “-‘ if the preceding date and time are in a time zone behind UTC. If the time is in UTC, the symbol “-“ will be used.
- zh indicates the hours of offset from the preceding date and time to UTC, or “00” if the preceding time is in UTC
- zm indicates the minutes of offset from the preceding date and time to UTC, or “00” if the preceding time is in UTC

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

3.3.3 Character Entity References

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

3.3.4 Security Note

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

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

Copyright © OASIS Open 2010. All Rights Reserved.

3.3.4.1 Digital Signatures

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

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

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

~~3.3.4.2Encryption~~

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

3.4 XML Schema

```
<?xml version = "1.0" encoding = "UTF-8"?>
<!-- Copyright OASIS Open 2010 All Rights Reserved -->
<schema xmlns = "http://www.w3.org/2001/XMLSchema"
   targetNamespace = "urn:oasis:names:tc:emergency:cap:1.2"
   xmlns:cap = "urn:oasis:names:tc:emergency:cap:1.2"
   xmlns:xs = "http://www.w3.org/2001/XMLSchema"
   elementFormDefault = "qualified"
   attributeFormDefault = "unqualified"
   version = "1.2">
  <element name = "alert">
    <annotation>
      <documentation>CAP Alert Message (version 1.2)</documentation>
    </annotation>
    <complexType>
      <sequence>
        <element name = "identifier" type = "xs:string"/>
        <element name = "sender" type = "xs:string"/>
        <element name = "sent">
          <simpleType>
            <restriction base = "xs:dateTime">
              <pattern value = "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,+]\d\d:\d\d"/>
            </restriction>
          </simpleType>
        </element>
        <element name = "status">
          <simpleType>
            <restriction base = "xs:string">
              <enumeration value = "Actual"/>
              <enumeration value = "Exercise"/>
              <enumeration value = "System"/>
              <enumeration value = "Test"/>
              <enumeration value = "Draft"/>
            </restriction>
          </simpleType>
        </element>
        <element name = "msgType">
          <simpleType>
            <restriction base = "xs:string">
              <enumeration value = "Alert"/>
              <enumeration value = "Update"/>
              <enumeration value = "Cancel"/>
              <enumeration value = "Ack"/>
              <enumeration value = "Error"/>
            </restriction>
          </simpleType>
        </element>
        <element name = "source" type = "xs:string" minOccurs = "0"/>
        <element name = "scope">
          <simpleType>
            <restriction base = "xs:string">
              <enumeration value = "Public"/>
```


Copyright © OASIS Open 2010. All Rights Reserved.

```
            <enumeration value = "Restricted"/>
            <enumeration value = "Private"/>
          </restriction>
        </simpleType>
      </element>
      <element name = "restriction" type = "xs:string" minOccurs = "0"/>
      <element name = "addresses" type = "xs:string" minOccurs = "0"/>
      <element name = "code" type = "xs:string" minOccurs = "0" maxOccurs = "unbounded"/>
      <element name = "note" type = "xs:string" minOccurs = "0"/>
      <element name = "references" type = "xs:string" minOccurs = "0"/>
      <element name = "incidents" type = "xs:string" minOccurs = "0"/>
      <element name = "info" minOccurs = "0" maxOccurs = "unbounded">
        <complexType>
          <sequence>
            <element name = "language" type = "xs:language" default = "en-US" minOccurs = "0"/>
            <element name = "category" maxOccurs = "unbounded">
              <simpleType>
                <restriction base = "xs:string">
                  <enumeration value = "Geo"/>
                  <enumeration value = "Met"/>
                  <enumeration value = "Safety"/>
                  <enumeration value = "Security"/>
                  <enumeration value = "Rescue"/>
                  <enumeration value = "Fire"/>
                  <enumeration value = "Health"/>
                  <enumeration value = "Env"/>
                  <enumeration value = "Transport"/>
                  <enumeration value = "Infra"/>
                  <enumeration value = "CBRNE"/>
                  <enumeration value = "Other"/>
                </restriction>
              </simpleType>
            </element>
            <element name = "event" type = "xs:string"/>
            <element name = "responseType" minOccurs = "0" maxOccurs = "unbounded">
              <simpleType>
                <restriction base = "xs:string">
                  <enumeration value = "Shelter"/>
                  <enumeration value = "Evacuate"/>
                  <enumeration value = "Prepare"/>
                  <enumeration value = "Execute"/>
                  <enumeration value = "Avoid"/>
                  <enumeration value = "Monitor"/>
                  <enumeration value = "Assess"/>
                  <enumeration value = "AllClear"/>
                  <enumeration value = "None"/>
                </restriction>
              </simpleType>
            </element>
            <element name = "urgency">
              <simpleType>
                <restriction base = "xs:string">
                  <enumeration value = "Immediate"/>
                  <enumeration value = "Expected"/>
                  <enumeration value = "Future"/>
                  <enumeration value = "Past"/>
                  <enumeration value = "Unknown"/>
                </restriction>
              </simpleType>
            </element>
            <element name = "severity">
              <simpleType>
                <restriction base = "xs:string">
                  <enumeration value = "Extreme"/>
                  <enumeration value = "Severe"/>
                  <enumeration value = "Moderate"/>
                  <enumeration value = "Minor"/>
                  <enumeration value = "Unknown"/>
                </restriction>
              </simpleType>
            </element>
            <element name = "certainty">
              <simpleType>
                <restriction base = "xs:string">
                  <enumeration value = "Observed"/>
                  <enumeration value = "Likely"/>
                  <enumeration value = "Possible"/>
                  <enumeration value = "Unlikely"/>
                  <enumeration value = "Unknown"/>
                </restriction>
              </simpleType>
            </element>
```


Copyright © OASIS Open 2010. All Rights Reserved.

```
              <element name = "audience" type = "xs:string" minOccurs = "0"/>
              <element name = "eventCode" minOccurs = "0" maxOccurs = "unbounded">
                <complexType>
                  <sequence>
                    <element ref = "cap:valueName"/>
                    <element ref = "cap:value"/>
                  </sequence>
                </complexType>
              </element>
              <element name = "effective" minOccurs = "0">
               <simpleType>
                 <restriction base = "xs:dateTime">
                   <pattern value = "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,+]\d\d:\d\d"/>
                 </restriction>
               </simpleType>
              </element>
              <element name = "onset"  minOccurs = "0">
               <simpleType>
                 <restriction base = "xs:dateTime">
                   <pattern value = "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,+]\d\d:\d\d"/>
                 </restriction>
               </simpleType>
              </element>
              <element name = "expires"  minOccurs = "0">
               <simpleType>
                 <restriction base = "xs:dateTime">
                   <pattern value = "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,+]\d\d:\d\d"/>
                 </restriction>
               </simpleType>
              </element>
              <element name = "senderName" type = "xs:string" minOccurs = "0"/>
              <element name = "headline" type = "xs:string" minOccurs = "0"/>
              <element name = "description" type = "xs:string" minOccurs = "0"/>
              <element name = "instruction" type = "xs:string" minOccurs = "0"/>
              <element name = "web" type = "xs:anyURI" minOccurs = "0"/>
              <element name = "contact" type = "xs:string" minOccurs = "0"/>
              <element name = "parameter" minOccurs = "0" maxOccurs = "unbounded">
                <complexType>
                  <sequence>
                    <element ref = "cap:valueName"/>
                    <element ref = "cap:value"/>
                  </sequence>
                </complexType>
              </element>
              <element name = "resource" minOccurs = "0" maxOccurs = "unbounded">
                <complexType>
                  <sequence>
                    <element name = "resourceDesc" type = "xs:string"/>
                    <element name = "mimeType" type = "xs:string" minOccurs = "0"/>
                    <element name = "size" type = "xs:integer" minOccurs = "0"/>
                    <element name = "uri" type = "xs:anyURI" minOccurs = "0"/>
                    <element name = "derefUri" type = "xs:string" minOccurs = "0"/>
                    <element name = "digest" type = "xs:string" minOccurs = "0"/>
                  </sequence>
                </complexType>
              </element>
              <element name = "area" minOccurs = "0" maxOccurs = "unbounded">
                <complexType>
                  <sequence>
                    <element name = "areaDesc" type = "xs:string"/>
                    <element name = "polygon" type = "xs:string" minOccurs = "0" maxOccurs =
"unbounded"/>
                    <element name = "circle" type = "xs:string" minOccurs = "0" maxOccurs =
"unbounded"/>
                    <element name = "geocode" minOccurs = "0" maxOccurs = "unbounded">
                      <complexType>
                        <sequence>
                          <element ref = "cap:valueName"/>
                          <element ref = "cap:value"/>
                        </sequence>
                      </complexType>
                    </element>
                    <element name = "altitude" type = "xs:decimalstring" minOccurs = "0"/>
                    <element name = "ceiling" type = "xs:decimalstring" minOccurs = "0"/>
                  </sequence>
                </complexType>
              </element>
            </sequence>
          </complexType>
        </element>
        <any minOccurs = "0" maxOccurs = "unbounded" namespace = "http://www.w3.org/2000/09/xmldsig#"
processContents = "lax"/>
```


Copyright © OASIS Open 2010. All Rights Reserved.

```
        <any minOccurs = "0" namespace = "http://www.w3.org/2000/09/xmlenc#" processContents = "lax"/>
      </sequence>
    </complexType>
  </element>
  <element name = "valueName" type = "xs:string"/>
  <element name = "value" type = "xs:string"/>
</schema>
```


Copyright © OASIS Open 2010. All Rights Reserved.

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

3.5.1 General

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

3.5.2 Formal Mappings and Specification

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

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

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

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

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

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

3.5.3 ASN.1 Schema

```
CAP-1-2 {itu-t recommendation x cap(1303) version1-2(2)}
DEFINITIONS XER INSTRUCTIONS AUTOMATIC TAGS ::=
-- CAP Alert Message (version 1.2)
BEGIN

Alert ::= SEQUENCE {
   identifier IdentifierString,
       -- Unambiguous identification of the message
       -- from all messages from
       -- this sender, in a format defined by the sender and
       -- identified in the "sender" field below.
   sender     String,
       -- The globally unambiguous identification of the sender.
       -- This specification does not define the root of
       -- a global identification tree (there is no international
       -- agreement on such a root), so it relies
       -- on human-readable text to define globally and
       -- unambiguously the sender.
       -- An internet domain name or use of "iri:/ITU-T/..."
       -- are possible, but
       -- the choice needs to be clearly stated in human-readable form.
   sent       DateTime (CONSTRAINED BY {/* XML representation of the XSD
pattern "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,+]\d\d:\d\d" */}),
   status     AlertStatus,
   msgType    AlertMessageType,
   source     String OPTIONAL,
       -- Not standardised human-readable identification
```


Copyright © OASIS Open 2010. All Rights Reserved.

```
      -- of the source of the alert.
   scope      AlertScope,
   restriction String OPTIONAL,
       -- Not standardised human-readable restrictions
       -- on the distribution of the alert message
   addresses   String OPTIONAL,
       -- A space separated list of addressees for private messages
       -- (see 3.2.1)
   code-list   SEQUENCE SIZE((0..MAX)) OF code String,
       -- A sequence codes for special handling
       -- (see 3.2.1)
       -- The format and semantics of the codes are not defined in this
       -- specification.
   note        String OPTIONAL,
       -- Not standardised human-readable clarifying text for the alert
       -- (see 3.2.1)
   references  String OPTIONAL,
       -- Space-separated references to earlier messages
      -- (see 3.2.1)
   incidents   String OPTIONAL,
       -- Space-separated references to related incidents
      -- (see 3.2.1)
   info-list   SEQUENCE SIZE((0..MAX)) OF info AlertInformation  }

AlertStatus ::= ENUMERATED {
        actual,
        draft,
        exercise,
        system,
        test }

AlertMessageType ::= ENUMERATED {
        ack,
        alert,
        cancel,
        error,
        update }

AlertScope ::= ENUMERATED {
        private,
        public,
        restricted }

AlertInformation ::= SEQUENCE {
   language          Language -- DEFAULT "en-US" -- ,
       -- The language used in this value of the Info type
      -- (see 3.2.2)
   category-list     SEQUENCE (SIZE(1..MAX)) OF
                     category InformationCategory,
   event             String,
       -- Not standardised human-readable text describing the
       -- type of the event (see 3.2.2)
   responseType-list SEQUENCE SIZE((0..MAX)) OF
                     responseType InformationResponseType,
   urgency           HowUrgent,
   severity          HowSevere,
   certainty         HowCertain,
   audience          String OPTIONAL,
       -- Not standardised human-readable text describing the
       -- intended audience for the message (see 3.2.2)
   eventCode-list    SEQUENCE SIZE((0..MAX)) OF eventCode SEQUENCE {
         valueName ValueName,
         value     Value },
```


Copyright © OASIS Open 2010. All Rights Reserved.

```
   effective         DateTime (CONSTRAINED BY {/* XML representation of the
XSD pattern "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,+]\d\d:\d\d" */}) OPTIONAL,
   onset             DateTime (CONSTRAINED BY {/* XML representation of the
XSD pattern "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,+]\d\d:\d\d" */}) OPTIONAL,
   expires           DateTime (CONSTRAINED BY {/* XML representation of the
XSD pattern "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,+]\d\d:\d\d" */}) OPTIONAL,
   senderName        String OPTIONAL,
       -- Not standardised human-readable name of the authority
       -- issuing the message (see 3.2.2)
   headline          String (SIZE (1..160,...)) OPTIONAL,
       -- Not standardised human-readable short statement (headline)
       -- of the alert (see 3.2.2)
   description       String OPTIONAL,
       -- Not standardised human-readable extended description of
       -- the event (see 3.2.2)
   instruction       String OPTIONAL,
       -- Not standardised human-readable recommended action
      -- (see 3.2.2)
   web               AnyURI OPTIONAL,
   contact           String OPTIONAL,
       -- Not standardised human-readable contact details for
       -- follow-up (see 3.2.2)
   parameter-list    SEQUENCE SIZE((0..MAX)) OF parameter SEQUENCE {
       -- System-specific parameters (see 3.2.2)
       valueName ValueName,
       value     Value },
   resource-list     SEQUENCE SIZE((0..MAX)) OF resource ResourceFile,
   area-list         SEQUENCE SIZE((0..MAX)) OF Area }

InformationCategory ::=  ENUMERATED {
        cBRNE,
        env,
        fire,
        geo,
        health,
        infra,
        met,
        other,
        rescue,
        safety,
        security,
        transport }

InformationResponseType ::= ENUMERATED {
        allClear(7),
        assess(0),
        avoid(8),
        evacuate(1),
        execute(2),
        monitor(3),
        none(4),
        prepare(5),
        shelter(6) }

HowUrgent ::= ENUMERATED {
        expected,
        future,
        immediate,
        past,
        unknown }

HowSevere ::= ENUMERATED {
        extreme,
        minor,
```


Copyright © OASIS Open 2010. All Rights Reserved.

```
        moderate,
        severe,
        unknown }

HowCertain ::= ENUMERATED {
        likely,
        observed,
        possible,
        unknown,
        unlikely }

ResourceFile ::= SEQUENCE {
       -- Information about an associated resource file
       -- (see 3.2.3)
   resourceDesc String,
       -- Not standardised human-readable description of the type
       -- and content of
       -- an associated resource file (for example a map or
       -- photograph)(see 3.2.3)
   mimeType     String~~ OPTIONAL~~,
   size         INTEGER OPTIONAL, -- In bytes
   uri          AnyURI OPTIONAL,
   derefUri     String OPTIONAL,
       -- An alternative to the URI giving the Base64-encoded
       -- content of the resource file (see 3.2.3)
   digest       String OPTIONAL
       -- SHA-1 hash of the resource file for error detection
      -- (see 3.2.3) -- }

Area ::= SEQUENCE {
       -- Identification of an affected area
   areaDesc     String,
       -- Not standardised human-readable description of the area
   polygon-list SEQUENCE OF polygon String,
       -- Each element is a space-separated list of coordinate pairs
       -- The complete list starts and ends with the same point and
       -- defines the polygon that defines the area
      -- (see 3.2.4).
   circle-list  SEQUENCE OF circle String,
       -- A space-separated list of coordinates for a point and a radius
   geocode-list SEQUENCE SIZE((0..MAX)) OF geocode SEQUENCE {
       -- A geographic code designating the alert target area
      -- (see 3.2.4)
            valueName ValueName,
            value     Value },
   altitude     REAL~~String~~ OPTIONAL,
       -- Specific or minimum altitude of the affected area
   ceiling      REAL~~String~~ OPTIONAL
       -- Maximum altitude of the affected area -- }

ValueName ::=  String  -- A not standardised name for
       -- an information event code, a parameter or a geocode

Value ::=  String  -- The value of the information event code,
                   -- parameter or geocode

String ::=  UTF8String (FROM (
          {0,0,0,9} -- TAB
        | {0,0,0,10} -- CR
        | {0,0,0,13} -- LF
        | {0,0,0,32}..{0,0,215,255} -- Space to the start of the S-zone
        | {0,0,224,0}..{0,0,255,253} -- Rest of BMP after S-zone
        | {0,1,0,0}..{0,16,255,253}  -- Other planes -- ) )
```


Copyright © OASIS Open 2010. All Rights Reserved.

```
StringChar ::= String (SIZE(1))

SpaceAndComma ::= UTF8String (FROM (
            {0,0,0,32} -- SPACE
          | {0,0,0,44} -- COMMA -- ) )

IdentifierString ::= String (FROM (StringChar EXCEPT SpaceAndComma))

Language ::= VisibleString(FROM ("a".."z" | "A".."Z" | "-" | "0".."9"))
               (PATTERN "[a-zA-Z]#(1,8)(-[a-zA-Z0-9]#(1,8))*")
      -- The semantics of Language is specified in IETF RFC 3066

DateTime ::= TIME (SETTINGS "Basic=Date-Time Date=YMD
          Year=Basic Time=HMS Local-or-UTC=LD")
       -- This is the ISO 8601 format using local time and a
       -- time difference

StringWithNoCRLFHT ::= UTF8String (FROM (
         {0,0,0,32}..{0,0,215,255}
         |{0,0,224,0}..{0,0,255,253}
         |{0,1,0,0}..{0,16,255,255}))

AnyURI ::= StringWithNoCRLFHT (CONSTRAINED BY {
          /* Shall be a valid URI as defined in IETF RFC 2396 */})

ENCODING-CONTROL XER
    GLOBAL-DEFAULTS MODIFIED-ENCODINGS
    GLOBAL-DEFAULTS CONTROL-NAMESPACE
        "http://www.w3.org/2001/XMLSchema-instance" PREFIX "xsi"
    NAMESPACE ALL, ALL IN ALL AS "urn:oasis:names:tc:emergency:cap:1.2"
              PREFIX "cap"
    NAME Alert, Area AS UNCAPITALIZED
    UNTAGGED SEQUENCE OF
    DEFAULT-FOR-EMPTY AlertInformation.language AS "en-US"
    TEXT AlertStatus:ALL,
         AlertMessageType:ALL,
         AlertScope:ALL,
         InformationCategory:ALL,
         InformationResponseType:ALL,
         HowUrgent:ALL,
         HowSevere:ALL,
         HowCertain:ALL AS CAPITALIZED
    WHITESPACE Language, AnyURI COLLAPSE
END
```


Copyright © OASIS Open 2010. All Rights Reserved.

4 Conformance

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

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

4.1 Conformance Targets

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

a) CAP V1.2 Message
b) CAP V1.2 Message Producer
c) CAP V1.2 Message Consumer

4.2 Conformance as a CAP V1.2 Message

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

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

4.3 Conformance as a CAP V1.2 Message Producer

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

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

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

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

Copyright © OASIS Open 2010. All Rights Reserved.

4.4 Conformance as a CAP V1.2 Message Consumer

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

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

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

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

Copyright © OASIS Open 2010. All Rights Reserved.

Appendix A. CAP Alert Message Example

XML examples are included below and are also available as separate files, along with ASN.1 binary encoded examples, in the CAP 1.2 document repository http://docs.oasis-open.org/emergency/cap/v1.2/

A.1. Homeland Security Advisory System Alert

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

```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns = "urn:oasis:names:tc:emergency:cap:1.2">
  <identifier>43b080713727</identifier>
  <sender>hsas@dhs.gov</sender>
  <sent>2003-04-02T14:39:01-05:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <info>
    <category>Security</category>
    <event>Homeland Security Advisory System Update</event>
    <urgency>Immediate</urgency>
    <severity>Severe</severity>
    <certainty>Likely</certainty>
    <senderName>U.S. Government, Department of Homeland Security</senderName>
    <headline>Homeland Security Sets Code ORANGE</headline>
    <description>The Department of Homeland Security has elevated the Homeland Security Advisory
System threat level to ORANGE / High in response to intelligence which may indicate a heightened
threat of terrorism.</description>
    <instruction> A High Condition is declared when there is a high risk of terrorist attacks. In
addition to the Protective Measures taken in the previous Threat Conditions, Federal departments
and agencies should consider agency-specific Protective Measures in accordance with their
existing plans.</instruction>
    <web>http://www.dhs.gov/dhspublic/display?theme=29</web>
    <parameter>
      <valueName>HSAS</valueName>
      <value>ORANGE</value>
    </parameter>
    <resource>
      <resourceDesc>Image file (GIF)</resourceDesc>
      <mimeType>image/gif</mimeType>
      <uri>http://www.dhs.gov/dhspublic/getAdvisoryImage</uri>
    </resource>
    <area>
      <areaDesc>U.S. nationwide and interests worldwide</areaDesc>
    </area>
  </info>
</alert>
```


Copyright © OASIS Open 2010. All Rights Reserved.

A.2. Severe Thunderstorm Warning

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

```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns = "urn:oasis:names:tc:emergency:cap:1.2">
  <identifier>KSTO1055887203</identifier>
  <sender>KSTO@NWS.NOAA.GOV</sender>
  <sent>2003-06-17T14:57:00-07:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <info>
    <category>Met</category>
    <event>SEVERE THUNDERSTORM</event>
    <responseType>Shelter</responseType>
    <urgency>Immediate</urgency>
    <severity>Severe</severity>
    <certainty>Observed</certainty>
    <eventCode>
      <valueName>SAME</valueName>
      <value>SVR</value>
    </eventCode>
    <expires>2003-06-17T16:00:00-07:00</expires>
    <senderName>NATIONAL WEATHER SERVICE SACRAMENTO CA</senderName>
    <headline>SEVERE THUNDERSTORM WARNING</headline>
    <description> AT 254 PM PDT...NATIONAL WEATHER SERVICE DOPPLER RADAR INDICATED A SEVERE
THUNDERSTORM OVER SOUTH CENTRAL ALPINE COUNTY...OR ABOUT 18 MILES SOUTHEAST OF KIRKWOOD...MOVING
SOUTHWEST AT 5 MPH. HAIL...INTENSE RAIN AND STRONG DAMAGING WINDS ARE LIKELY WITH THIS
STORM.</description>
    <instruction>TAKE COVER IN A SUBSTANTIAL SHELTER UNTIL THE STORM PASSES.</instruction>
    <contact>BARUFFALDI/JUSKIE</contact>
    <area>
      <areaDesc>EXTREME NORTH CENTRAL TUOLUMNE COUNTY IN CALIFORNIA, EXTREME NORTHEASTERN
CALAVERAS COUNTY IN CALIFORNIA, SOUTHWESTERN ALPINE COUNTY IN CALIFORNIA</areaDesc>
      <polygon>38.47,-120.14 38.34,-119.95 38.52,-119.74 38.62,-119.89 38.47,-120.14</polygon>
      <geocode>
        <valueName>SAME</valueName>
        <value>006109</value>
      </geocode>
      <geocode>
        <valueName>SAME</valueName>
        <value>006009</value>
      </geocode>
      <geocode>
        <valueName>SAME</valueName>
        <value>006003</value>
      </geocode>
    </area>
  </info>
</alert>
```


Copyright © OASIS Open 2010. All Rights Reserved.

A.3. Earthquake Report (Update Message)

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

```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns = "urn:oasis:names:tc:emergency:cap:1.2">
  <identifier>TRI13970876.2</identifier>
  <sender>trinet@caltech.edu</sender>
  <sent>2003-06-11T20:56:00-07:00</sent>
  <status>Actual</status>
  <msgType>Update</msgType>
  <scope>Public</scope>
  <references>trinet@caltech.edu,TRI13970876.1,2003-06-11T20:30:00-07:00</references>
  <info>
    <category>Geo</category>
    <event>Earthquake</event>
    <urgency>Past</urgency>
    <severity>Minor</severity>
    <certainty>Observed</certainty>
    <senderName>Southern California Seismic Network (TriNet) operated by Caltech and
USGS</senderName>
    <headline>EQ 3.4 Imperial County CA</headline>
    <description>A minor earthquake measuring 3.4 on the Richter scale occurred near Brawley,
California at 8:3053 PM Pacific Daylight Time on Wednesday, June 11, 2003. (This event has now
been reviewed by a seismologist)</description>
    <web>http://www.trinet.org/scsn/scsn.html</web>
    <parameter>
      <valueName>EventID</valueName>
      <value>13970876</value>
    </parameter>
    <parameter>
      <valueName>Version</valueName>
      <value>1</value>
    </parameter>
    <parameter>
      <valueName>Magnitude</valueName>
      <value>3.4 Ml</value>
    </parameter>
    <parameter>
      <valueName>Depth</valueName>
      <value>11.8 mi.</value>
    </parameter>
    <parameter>
      <valueName>Quality</valueName>
      <value>Excellent</value>
    </parameter>
    <area>
      <areaDesc>1 mi. WSW of Brawley, CA; 11 mi. N of El Centro, CA; 30 mi. E of OCOTILLO
(quarry); 1 mi. N of the Imperial Fault</areaDesc>
      <circle>32.9525,-115.5527 0</circle>
    </area>
  </info>
</alert>
```


Copyright © OASIS Open 2010. All Rights Reserved.

A.4. AMBER Alert (Multilingual Message)

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

```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns = "urn:oasis:names:tc:emergency:cap:1.2">
   <identifier>KAR0-0306112239-SW</identifier>
   <sender>KARO@CLETS.DOJ.CA.GOV</sender>
   <sent>2003-06-11T22:39:00-07:00</sent>
   <status>Actual</status>
   <msgType>Alert</msgType>
   <source>SW</source>
   <scope>Public</scope>
   <info>
      <language>en-US</language>
      <category>Rescue</category>
      <event>Child Abduction</event>
      <urgency>Immediate</urgency>
      <severity>Severe</severity>
      <certainty>Likely</certainty>
      <eventCode>
         <valueName>SAME</valueName>
         <value>CAE</value>
      </eventCode>
      <senderName>Los Angeles Police Dept - LAPD</senderName>
      <headline>Amber Alert in Los Angeles County</headline>
      <description>DATE/TIME: 06/11/03, 1915 HRS.  VICTIM(S): KHAYRI DOE JR. M/B BLK/BRO 3'0", 40
LBS. LIGHT COMPLEXION.  DOB 06/24/01. WEARING RED SHORTS, WHITE T-SHIRT, W/BLUE COLLAR.
LOCATION: 5721 DOE ST., LOS ANGELES, CA.  SUSPECT(S): KHAYRI DOE SR. DOB 04/18/71 M/B, BLK HAIR,
BRO EYE. VEHICLE: 81' BUICK 2-DR, BLUE (4XXX000).</description>
      <contact>DET. SMITH, 77TH DIV, LOS ANGELES POLICE DEPT-LAPD AT 213 485-2389</contact>
      <area>
         <areaDesc>Los Angeles County</areaDesc>
         <geocode>
            <valueName>SAME</valueName>
            <value>006037</value>
         </geocode>
      </area>
   </info>
   <info>
      <language>es-US</language>
      <category>Rescue</category>
      <event>Abducción de Niño</event>
      <urgency>Immediate</urgency>
      <severity>Severe</severity>
      <certainty>Likely</certainty>
      <eventCode>
         <valueName>SAME</valueName>
         <value>CAE</value>
      </eventCode>
      <senderName>Departamento de Policía de Los Ángeles - LAPD</senderName>
      <headline>Alerta Amber en el condado de Los Ángeles</headline>
      <description>DATE/TIME: 06/11/03, 1915 HORAS. VÍCTIMAS: KHAYRI DOE JR. M/B BLK/BRO 3'0", 40
LIBRAS. TEZ LIGERA. DOB 06/24/01. CORTOCIRCUITOS ROJOS QUE USAN, CAMISETA BLANCA, COLLAR DE
W/BLUE. LOCALIZACIÓN: 5721 DOE ST., LOS ÁNGELES. SOSPECHOSO: KHAYRI DOE ST. DOB 04/18/71 M/B,
PELO DEL NEGRO, OJO DE BRO. VEHÍCULO: 81' BUICK 2-DR, AZUL (4XXX000)</description>
      <contact>DET. SMITH, 77TH DIV, LOS ANGELES POLICE DEPT-LAPD AT 213 485-2389</contact>
      <area>
         <areaDesc>condado de Los Ángeles</areaDesc>
         <geocode>
            <valueName>SAME</valueName>
            <value>006037</value>
         </geocode>
      </area>
   </info>
</alert>
```


Copyright © OASIS Open 2010. All Rights Reserved.

Appendix B. Acknowledgments

OASIS Emergency Management Technical Committee

Doug Allport, Canadian Association for Public Alerting and Notification (CAPAN)
Patti Aymond, IEM
Himadri Banerjee, Previstar Inc.
Frank Bell, Individual
Art Botterell, Contra Costa County Community Warning System
John Bradley, Individual
Rex Brooks, Individual
Robert Bunge, NOAA's National Weather Service
Toby Considine, University of North Carolina at Chapel Hill
William Cox, Cox Software Architects LLC
Olivier Dubuisson, France Telecom
Sukumar Dwarkanath, SRA International
David Ellis, Sandia National Laboratories
Thomas Ferrentino, Individual
Jack Fox, US Department of Homeland Security
Patrick Gannon, Warning Systems, Inc.
Timothy Gilmore, US Department of Homeland Security
James Goodson, US Department of Homeland Security
Tim Grapes, Evolution Technologies Inc.
Gary Ham, Individual
Harry Haury, NuParadigm Government Systems, Inc.
Werner Joerg, IEM
Elysa Jones, Warning Systems, Inc.
Jeff Jortner, Sandia National Laboratories
William Kalin, US Department of Homeland Security
Ram Kumar, Individual
Jeff Kyser, Warning Systems, Inc.
Ron Lake, Galdos Systems Inc.
David Lamendsdorf, Emergency Interoperability Consortium
Mike McDougall, Individual
Donald McGarry, Mitre Corporation
Tom Merkle, Lockheed Martin
Enoch Moses, ManTech Enterprise Integration Center (e-IC)
Brian Nelson, Sandia National Laboratories
Camille Osterloh, US Department of Homeland Security
John Pitale, Edmond Scientific Company
Mark Pleimann, Mitre Corporation

Copyright © OASIS Open 2010. All Rights Reserved.

Donald Ponikvar, US Department of Homeland Security
Jacqueline Postell, US Department of Homeland Security
Carl Reed, Open Geospatial Consortium, Inc. (OGC)
Dean Reese, ESI Acquisition, Inc.
Kirby Rice, Eye Street Solutions
Howard Ryan, Desktop Alert Inc.
Tracy Ryan, Emergency Interoperability Consortium
Josh Shows, ESI Acquisition, Inc.
Aviv Siegel, AtHoc, Inc.
Andrew Sonner, Evolution Technologies Inc.
Christopher Springer, US Department of Homeland Security
Steve Streetman, US Department of Homeland Security
Lee Tincher, Evolution Technologies Inc.
James Trawick, viaRadio Corporation
Alessandro Triglia, OSS Nokalva
Richard Vandame, US Department of Homeland Security
Matt Walton, Individual
Jeff Waters, US Department of Defense (DoD)
David Webber, Individual
Jacob Westfall, Individual
David Yarbrough, Northrop Grumman

Copyright © OASIS Open 2010. All Rights Reserved.

1123 # Appendix C. Revision History

Rev	Date	By Whom	What
1.2	2010-03-02	Jacob Westfall	Technical Committee approved changes that removed XML Digital Encryption within CAP messages.
1.2	2009-12-22	Jacob Westfall	Technical Committee approved the v. 1.2 draft submitted by the Messaging Subcommittee with a duplicate Normative Reference entry removed.
1.2	2009-09-29	Jacob Westfall	Technical Committee approved the v. 1.2 draft submitted by the Messaging Subcommittee with a change made to responseType in the ASN.1 schema.
1.2	2009-09-17	Jacob Westfall	Messaging Subcommittee approved changes based on initial public comment period: • Expanded the scope of the <addresses> element • Changed <mimeType> to be a required element and added note for <size> • Qualified the base schema types in the schema • Changed the schema typing for <altitude> and <ceiling> to be a decimal instead of a string • ASN.1 examples were added Various editorial corrections
1.2	2009-04-28	Jacob Westfall	Technical Committee approved the v. 1.2 draft with the following additional changes: • DateTime Data Type moved to Implementation Notes • Changes to <status> and <note> descriptions • Wording change to <severity> “Minor” • Schema changed to allow only one <EncryptedData> element and changed Security Note section to allow multiple <Signature> elements Various editorial corrections and clarifications
1.2	2009-04-14	Jacob Westfall	Messaging Subcommittee approved v. 1.2 draft for submission to full Technical Committee: • Multiple XML signature/encryption elements • Editorial changes to History and Character Entity References sections • DateTime Data Type examples • Fixed DOM display

Copyright © OASIS Open 2010. All Rights Reserved.

1.2	2009-03-31	Jacob Westfall	Applied changes per recommendations identified by CAP comments process and profile development: • Includes CAP 1.1 Errata and ASN.1 Schema • DateTime Data Type to further define the acceptable date and time values • New <responseType> values of Avoid and AllClear • Clarification on acceptable <polygon> values and the use of character entity references • Schemas were updated to reflect changes and to validate when XML signature/encryption elements are present • Conformance section added • Updated CAP Alert Message Examples Various editorial corrections and clarifications
1.1 Errata	2007-10-02		CAP 1.1 Errata approved (see CAP 1.1 Errata document for prior change history)
1.1	2005-09-30		CAP 1.1 adopted as OASIS Standard (see CAP 1.1 specification document for prior change history)
1.1	2005-07-27	Art Botterell	Edits to conform object model, data dictionary and schema: • Reordered items in object diagram and data dictionary to match sequence required by schema. • Edited schema to make <scope> mandatory and to permit multiple instances of <responseType> and <eventCode>, in accordance with the data dictionary.
1.1	2005-07-23	Art Botterell	Applied changes per recommendations of Messaging Subcommittee based on initial public comment period: • Modified XML syntax of <eventCode> , <parameter> and <geocode> • Added “Draft” value for <status> • Changed CAP namespace to URN form • Tightened usage of dateTime formats in <sent>, <effective>, <onset> and <expiration> • Corrected schema to correct value of “CBRNE” in <event> • Conformed examples in Appendix A to new namespace.
1.1	2005-04-28	Elysa Jones	Technical Committee approved the v. 1.1 draft with the following additional changes: • Normative language added to specify uniqueness of <identifier> • Change [dateTime] format for <sent>, <effective>, <onset> and <expires> elements • Change <language> element RFC from 1166 to 3066 and added null • Changed the <mineType> element RFC 1521 to 2046 • Added <derefURI> element • Security Note updated and added Digital Signature and Encryption note paragraphs

Copyright © OASIS Open 2010. All Rights Reserved.

1.1	2005-01-04	Art Botterell	Messaging Subcommittee approved v. 1.1 draft for submission to full Technical Committee: • Added <responseType> element • Made <category> element mandatory • Amended enumerated values for the <certainty> element • Deleted the <password> element • Various editorial corrections and clarifications
1.0	2004-04-01	Art Botterell	CAP 1.0 adopted as OASIS Standard (see CAP 1.0 specification document for prior change history.)

1124

Copyright © OASIS Open 2010. All Rights Reserved.