# OASIS 🕅

# **Common Alerting Protocol Version 1.2**

# **OASIS Standard**

# 01 July 2010

#### **Specification URIs:**

#### This Version:

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

#### **Previous Version:**

http://docs.oasis-open.org/emergency/cap/v1.2/cs01/CAP-v1.2-cs01.html http://docs.oasis-open.org/emergency/cap/v1.2/cs01/CAP-v1.2-cs01.pdf http://docs.oasis-open.org/emergency/cap/v1.2/cs01/CAP-v1.2-cs01.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.oasisopen.org/committees/download.php/15135/emergency-CAPv1.1-Corrected\_DOM.pdf
- OASIS Standard CAP-V1.1, Approved Errata October 2007 http://docs.oasisopen.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.oasisopen.org/committees/emergency/.

# Notices

Copyright © OASIS® 2010. 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 <u>OASIS</u>, 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></alert>	7
	1.3.2 <info></info>	7
	1.3.3 <resource></resource>	7
	1.3.4 <area/>	7
	1.4 Applications of the CAP Alert Message	7
	1.5 Terminology	8
	1.6 Normative References	
2	Design Principles and Concepts (non-normative)	9
	2.1 Design Philosophy	
	2.2 Requirements for Design	
	2.3 Examples of Use Scenarios	
	2.3.1 Manual Origination	
	2.3.2 Automated Origination by Autonomous Sensor System	
	2.3.3 Aggregation and Correlation on Real-time Map	
	2.3.4 Integrated Public Alerting	
	2.3.5 Repudiating a False Alarm	
3	Alert Message Structure (normative)	
	3.1 Document Object Model	
	3.2 Data Dictionary	
	3.2.1 "alert" Element and Sub-elements	
	3.2.2 "info" Element and Sub-elements	
	3.2.3 "resource" Element and Sub-elements	
	3.2.4 "area" Element and Sub-elements	
	3.3 Implementation Notes	
	3.3.1 WGS 84 Note	
	3.3.2 DateTime Data Type	
	3.3.3 Character Entity References	
	3.3.4 Security Note	
	3.3.4.1 Digital Signatures	
	3.4 XML Schema	
	3.5 Use of ASN.1 to Specify and Encode the CAP Alert Message	
	3.5.1 General	
	3.5.2 Formal Mappings and Specification	
л	3.5.3 ASN.1 Schema Conformance (normative)	
4	4.1 Conformance (normative)	
	4.1 Conformance Targets	
	4.2 Conformance as a CAP V1.2 Message Producer	
	4.3 Conformance as a CAP V1.2 Message Producer	
	T.T OUTIOITIATIVE as a UAF VI.2 NESSAYE OUTSUITEL	50

Appendix A. CAP Alert Message Example	39
A.1. Homeland Security Advisory System Alert	
A.2. Severe Thunderstorm Warning	
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 1 Introduction

### 2 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;
- 12 Phased and delayed effective times and expirations;
- 13 Enhanced message update and cancellation features;
- Template support for framing complete and effective warning messages;
- Compatible with digital signature capability; and,
- 16 Facility for digital images and audio.
- 17 Key benefits of CAP will include reduction of costs and operational complexity by eliminating the need for
- 18 multiple custom software interfaces to the many warning sources and dissemination systems involved in
- 19 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
- 21 international "warning internet."

#### 22 **1.2 History**

23 The National Science and Technology Council report on "Effective Disaster Warnings" released in

24 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 actionally for input into a wide variety of discomination systems."
- 26 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)
- 32 during 2002 and 2003.
- 33 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
- 37 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.
- 40
- 41

### 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
- 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>
- 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>

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.

#### 63 1.3.4 <area>

- 64 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
- 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
- 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
- remergency 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
- 79 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.
- 82

#### 83 **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]**.

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 94	[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.
95	[dateTime]	N. Freed, XML Schema Part 2: Datatypes Second Edition,
95 96	[uaternine]	http://www.w3.org/TR/xmlschema-2/#dateTime, W3C REC-xmlschema-2,
90 97		October 2004.
98	[FIPS 180-2]	National Institute for Standards and Technology, Secure Hash Standard,
99	[111 0 100-2]	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	[RFC3066]	H. Alvestrand, Tags for the Identification of Languages,
106		http://www.ietf.org/rfc/rfc3066.txt, IETF RFC 3066, January 2001.
107	[WGS 84]	National Geospatial Intelligence Agency, Department of Defense World Geodetic
108		System 1984, http://earth-info.nga.mil/GandG/tr8350_2.html, NGA Technical
109		Report TR8350.2, January 2000.
110	[XML 1.0]	T. Bray, Extensible Markup Language (XML) 1.0 (Third Edition),
111		http://www.w3.org/TR/REC-xml/, W3C REC-XML-20040204, February 2004.
112	[XMLSIG]	Eastlake, D., Reagle, J. and Solo, D. (editors), XML-Signature Syntax and
113		Processing, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/, W3C
114		Recommendation, February 2002.
115	[ITU-T X.680]	ITU-T Recommendation X.680, Information technology – Abstract Syntax
116		Notation One (ASN.1): Specification of basic notation.
117	[ITU-T X.691]	ITU-T Recommendation X.691, Information technology – ASN.1 encoding rules:
118		Specification of Packed Encoding Rules (PER).
119	[ITU-T X.693]	ITU-T Recommendation X.693, Information technology – ASN.1 encoding rules:
120		Specification of XML Encoding Rules (XER).
121	[ITU-T X.694]	ITU-T Recommendation X.694, Information technology – ASN.1 encoding rules:
122		Mapping W3C XML schema definitions into ASN.1.
123		

# 124 2 Design Principles and Concepts (non-normative)

### 125 2.1 Design Philosophy

126	Among the principles	which guided the design of th	ne 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.

### 145 2.2 Requirements for Design

- 146Note: The following requirements were used as a basis for design and review of the CAP147Alert Message format. This list is non-normative and not intended to be exhaustive.
- 148 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 oneway "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:
- 158–Warnings159–Acknowledgements
- 160 Expirations and cancellations
- 161 Updates and amendments
- 162 Reports of results from dissemination systems
- 163 Administrative and system messages
- Provide for multiple message types, such as:

165		<ul> <li>Geographic targeting</li> </ul>
166		<ul> <li>Level of urgency</li> </ul>
167		<ul> <li>Level of certainty</li> </ul>
168		<ul> <li>Level of threat severity</li> </ul>
169 170	•	Provide a mechanism for referencing supplemental information (e.g., digital audio or image files, additional text);
171	•	Use an established open-standard data representation;
172	•	Be based on a program of real-world cross-platform testing and evaluation;
173	•	Provide a clear basis for certification and further protocol evaluation and improvement; and,
174 175	•	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.
470	2 2	Examples of Use Scenarios

#### 176 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.

#### 180 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-inplace 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 IncidentCommander issues the alert as a CAP message to a local alerting network.

### 188 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.

#### 196 2.3.3 Aggregation and Correlation on Real-time Map

197 At the State Operations Center a computerized map of the state depicts, in real time, all current and

198 recent warning activity throughout the state. All major warning systems in the state – the Emergency 199 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
- 202 center.)
- 203 Using this visualization tool, state officials can monitor for emerging patterns of local warning activity and
- 204 correlate it with other real time data (e.g., telephone central office traffic loads, 9-1-1 traffic volume, 205 seismic data, automatic vehicular crash notifications, etc.).
- 206

#### 207 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.

210 Each system converts the CAP message data into the form suitable for its technology (text captioning on

211 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.

214 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

216 acted upon.

#### 217 **2.3.5 Repudiating a False Alarm**

218 Inadvertently the integrated alerting network has been activated with an inaccurate warning message.

219 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

221 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

223 cancellation message. Other systems (e.g., highway signs) simply reset to their normal state.

# **3 Alert Message Structure (normative)**

#### 225 3.1 Document Object Model



#### 228

### 229 3.2 Data Dictionary

230 231 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 Su	b-elements	
alert	cap. alert. group	The container for all component parts of the alert message (REQUIRED)	<ul> <li>(1) Surrounds CAP alert message subelements.</li> <li>(2) MUST include the xmlns attribute referencing the CAP URN as the namespace, e.g.:         <cap:alert xmlns:cap="urn:oasis:names:tc:emerge         ncy:cap:1.2">             [sub-elements]         </cap:alert> </li> <li>(3) In addition to the specified subelements, MAY contain one or more         <info> blocks.</info></li> </ul>
identifier	cap. alert. identifier. identifier	The identifier of the alert message (REQUIRED)	<ol> <li>A number or string uniquely identifying this message, assigned by the sender.</li> <li>MUST NOT include spaces, commas or restricted characters (&lt; and &amp;).</li> </ol>
sender	cap. alert. sender. identifier	The identifier of the sender of the alert message (REQUIRED)	<ol> <li>Identifies the originator of this alert. Guaranteed by assigner to be unique globally; e.g., may be based on an Internet domain name.</li> <li>MUST NOT include spaces, commas or restricted characters (&lt; and &amp;).</li> </ol>
sent	cap. alert. sent. time	The time and date of the origination of the alert message (REQUIRED)	<ul> <li>(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).</li> <li>(2) Alphabetic timezone designators such as "Z" MUST NOT be used. The timezone for UTC MUST be represented as "-00:00".</li> </ul>

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</note>
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></note></references></references></references></references>
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)</addresses></restriction>

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".</scope>
addresses	cap. alert. addresses. group	The group listing of intended recipients of the alert message (CONDITIONAL)	<ol> <li>Required when <scope> is "Private", optional when <scope> is "Public" or "Restricted".</scope></scope></li> <li>Each recipient SHALL be identified by an identifier or an address.</li> <li>Multiple space-delimited addresses MAY be included. Addresses including whitespace MUST be enclosed in double-quotes.</li> </ol>
code	cap. alert. code. code	The code denoting the special handling of the alert message (OPTIONAL)	<ol> <li>Any user-defined flag or special code used to flag the alert message for special handling.</li> <li>Multiple instances MAY occur.</li> </ol>
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".</msgtype></status>
references	cap. alert. references. group	The group listing identifying earlier message(s) referenced by the alert message (OPTIONAL)	<ol> <li>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>If multiple messages are referenced, they SHALL be separated by whitespace.</li> </ol>

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)	<ol> <li>Used to collate multiple messages referring to different aspects of the same incident.</li> <li>If multiple incident identifiers are referenced, they SHALL be separated by whitespace. Incident names including whitespace SHALL be surrounded by double-quotes.</li> </ol>
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)	<ol> <li>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.</info></info></alert></li> <li>In addition to the specified sub- elements, MAY contain one or more <resource> blocks and/or one or more <area/> blocks.</resource></li> </ol>
language	cap. alertInfo. language. code	The code denoting the language of the info sub- element of the alert message (OPTIONAL)	<ol> <li>Code Values: Natural language identifier per [RFC 3066].</li> <li>If not present, an implicit default value of "en-US" SHALL be assumed.</li> <li>A null value in this element SHALL be considered equivalent to "en-US."</li> </ol>

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

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

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)	<ul> <li>(1) The <urgency>, <severity>, and</severity></urgency></li> <li><certainty> elements collectively distinguish less emphatic from more emphatic messages.</certainty></li> <li>(2) Code Values: <ul> <li>"Extreme" - Extraordinary threat to life or property</li> <li>"Severe" - Significant threat to life or property</li> <li>"Moderate" - Possible threat to life or property</li> <li>"Minor" – Minimal to no known threat to life or property</li> <li>"Unknown" - Severity unknown</li> </ul> </li> </ul>
certainty	cap. alertInfo. certainty. code	The code denoting the certainty of the subject event of the alert message (REQUIRED)	<ul> <li>(1) The <urgency>, <severity>, and</severity></urgency></li> <li><certainty> elements collectively distinguish</certainty></li> <li>less emphatic from more emphatic</li> <li>messages.</li> <li>(2) Code Values:</li> <li>"Observed" – Determined to have</li> <li>occurred or to be ongoing</li> <li>"Likely" - Likely (p &gt; ~50%)</li> <li>"Possible" - Possible but not likely (p &lt;= ~50%)</li> <li>"Unlikely" - Not expected to occur (p ~ 0)</li> <li>"Unknown" - Certainty unknown</li> <li>(3) For backward compatibility with CAP</li> <li>1.0, the deprecated value of "Very Likely"</li> <li>SHOULD be treated as equivalent to</li> <li>"Likely".</li> </ul>
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)	<ul> <li>(1) Any system-specific code for event typing, in the form:</li> <li><eventcode></eventcode></li> <li><valuename>valueName</valuename></li> <li><value>value</value></li> <li></li> <li>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").</li> <li>(2) Values of "valueName" that are acronyms SHOULD be represented in all capital letters without periods (e.g., SAME, FIPS, ZIP).</li> <li>(3) Multiple instances MAY occur within an <info> block.</info></li> </ul>
effective	cap. alertInfo. effective. time	The effective time of the information of the alert message (OPTIONAL)	<ul> <li>(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).</li> <li>(2) Alphabetic timezone designators such as "Z" MUST NOT be used. The timezone for UTC MUST be represented as "-00:00".</li> <li>(3) If this item is not included, the effective time SHALL be assumed to be the same as in <sent>.</sent></li> </ul>
onset	cap. alertInfo. onset. time	The expected time of the beginning of the subject event of the alert message (OPTIONAL)	<ul> <li>(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).</li> <li>(2) Alphabetic timezone designators such as "Z" MUST NOT be used. The timezone for UTC MUST be represented as "-00:00".</li> </ul>

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)	<ul> <li>(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).</li> <li>(2) Alphabetic timezone designators such as "Z" MUST NOT be used. The timezone for UTC MUST be represented as "-00:00".</li> <li>(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.</li> </ul>
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.</info>

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

Element Name	Context. Class. Attribute. Representation	Definition and (Optionality)	Notes or Value Domain			
3.2.3 "reso	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)	<ul> <li>(1) Refers to an additional file with supplemental information related to this <info> element; e.g., an image or audio file.</info></li> <li>(2) Multiple instances MAY occur within an <info> block.</info></li> </ul>			
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.			
тітеТуре	cap. alertInfoResource. mimeType. identifier	The identifier of the MIME content type and sub-type describing the resource file (REQUIRED)	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 http://www.iana.org/assignments/media- types/)			
size	cap. alertInfoResource. size. integer	The integer indicating the size of the resource file (OPTIONAL)	<ol> <li>(1) Approximate size of the resource file in bytes.</li> <li>(2) For <uri> based resources, <size> SHOULD be included if available.</size></uri></li> </ol>			
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.</derefuri>			

either with or instead of in messages transmitted g., broadcast) data links a resource via a URI is ed for use with one-way support this element. MUST NOT be used r is certain that all direct e of processing it. acluding this element are two-way network, the strip the <derefuri> DULD extract the file ride a <uri> link to a n of the file. ne-way data links MAY I restrictions on the use of ading message-size limits egarding file types.</uri></derefuri>
the Secure Hash ) per <b>[FIPS 180-2]</b> .

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)	<ol> <li>(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)</li> <li>(2) A minimum of 4 coordinate pairs MUST be present and the first and last pairs of coordinates MUST be the same.</li> <li>(3) Multiple instances MAY occur within an <area/> block.</li> </ol>
circle	cap. alertInfoArea. circle. group	The paired values of a point and radius delineating the affected area of the alert message (OPTIONAL)	<ul> <li>(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)</li> <li>(2) Multiple instances MAY occur within an <area/> block.</li> </ul>

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)	<ul> <li>(1) Any geographically-based code to describe a message target area, in the form:</li> <li><geocode></geocode></li> <li><valuename>valueName</valuename></li> <li><value>value</value></li> <li></li> <li>where the content of "valueName" is a userassigned 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").</li> <li>(2) Values of "valueName" that are acronyms SHOULD be represented in all capital letters without periods (e.g., SAME, FIPS, ZIP).</li> <li>(3) Multiple instances MAY occur within an <area/> block.</li> <li>(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.</circle></polygon></li> </ul>
altitude	cap. alertInfoArea. altitude. quantity	The specific or minimum altitude of the affected area of the alert message (OPTIONAL)	<ol> <li>(1) If used with the <ceiling> element this value is the lower limit of a range.</ceiling></li> <li>Otherwise, this value specifies a specific altitude.</li> <li>(2) The altitude measure is in feet above mean sea level per the <b>[WGS 84]</b> datum.</li> </ol>
ceiling	cap. alertInfoArea. ceiling. quantity	The maximum altitude of the affected area of the alert message (CONDITIONAL)	<ul> <li>(1) MUST NOT be used except in combination with the <altitude> element.</altitude></li> <li>(2) The ceiling measure is in feet above mean sea level per the <b>[WGS 84]</b> datum.</li> </ul>

#### 234 **3.3 Implementation Notes**

#### 235 **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.

#### 240 **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
- 255 zm indicates the minutes of offset from the preceding date and time to UTC, or "00" if the
   256 preceding time is in UTC
- 257 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".

#### 260 **3.3.3 Character Entity References**

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

#### 262 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.

#### 266 **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.

- 270 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 inform the user of their failure to
   validate the signature.

273 In other words, the presence of an element with the namespace URI [XMLSIG] and a local name of

274 < Signature> as a child of the <alert> element must not cause a processor to fail merely because of its 275 presence.

#### 3.4 XML Schema 276

277 278

281

282 283

284 285

286

287

288

289

290

291

292

293 294

295

296

297

298 299

300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316

317 318

319

324 325

326 327

328 329

330 331

332 333

334 335

336 337

338

339

340

```
<?xml version = "1.0" encoding = "UTF-8"?>
279
280
       <!-- 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">
                    </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"/>
                     <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>
```

```
342
                    <sequence>
343
                      <element name = "language" type = "xs:language" default = "en-US" minOccurs = "0"/>
344
                      <element name = "category" maxOccurs = "unbounded">
345
                        <simpleType>
346
                          <restriction base = "xs:string">
347
348
                            <enumeration value = "Geo"/>
                            <enumeration value = "Met"/>
349
350
351
352
                            <enumeration value = "Safety"/>
                            <enumeration value = "Security"/>
                            <enumeration value = "Rescue"/>
                            <enumeration value = "Fire"/>
353
                            <enumeration value = "Health"/>
354
                            <enumeration value = "Env"/>
355
                            <enumeration value = "Transport"/>
356
                            <enumeration value = "Infra"/>
357
358
                            <enumeration value = "CBRNE"/>
                            <enumeration value = "Other"/>
359
                          </restriction>
360
                        </simpleType>
361
                      </element>
362
                      <element name = "event" type = "xs:string"/>
363
                      <element name = "responseType" minOccurs = "0" maxOccurs = "unbounded">
364
                        <simpleType>
365
                          <restriction base = "xs:string">
366
                            <enumeration value = "Shelter"/>
367
                            <enumeration value = "Evacuate"/>
368
                            <enumeration value = "Prepare"/>
369
                            <enumeration value = "Execute"/>
370
371
372
373
                            <enumeration value = "Avoid"/>
                            <enumeration value = "Monitor"/>
                            <enumeration value = "Assess"/>
                            <enumeration value = "AllClear"/>
374
375
                            <enumeration value = "None"/>
                          </restriction>
376
377
378
379
380
                        </simpleType>
                      </element>
                      <element name = "urgency">
                        <simpleType>
                          <restriction base = "xs:string">
                            <enumeration value = "Immediate"/>
381
382
                            <enumeration value = "Expected"/>
383
                            <enumeration value = "Future"/>
384
                            <enumeration value = "Past"/>
385
                            <enumeration value = "Unknown"/>
386
387
                          </restriction>
                        </simpleType>
388
                      </element>
389
                      <element name = "severity">
390
                        <simpleType>
391
                          <restriction base = "xs:string">
392
                            <enumeration value = "Extreme"/>
393
                            <enumeration value = "Severe"/>
394
                            <enumeration value = "Moderate"/>
                            <enumeration value = "Minor"/>
395
396
                            <enumeration value = "Unknown"/>
397
                          </restriction>
398
                        </simpleType>
399
                      </element>
400
                      <element name = "certainty">
401
                        <simpleType>
402
                          <restriction base = "xs:string">
403
                            <enumeration value = "Observed"/>
404
                            <enumeration value = "Likely"/>
405
                            <enumeration value = "Possible"/>
                            <enumeration value = "Unlikely"/>
406
407
                            <enumeration value = "Unknown"/>
408
                          </restriction>
409
                        </simpleType>
410
                      </element>
411
                      <element name = "audience" type = "xs:string" minOccurs = "0"/>
412
                      <element name = "eventCode" minOccurs = "0" maxOccurs = "unbounded">
413
                        <complexType>
```

```
414
                           <sequence>
415
                             <element ref = "cap:valueName"/>
416
                             <element ref = "cap:value"/>
417
                           </sequence>
418
419
420
                        </complexType>
                      </element>
                      <element name = "effective" minOccurs = "0">
421
422
423
424
425
                       <simpleType>
                         <restriction base = "xs:dateTime">
                            <pattern value = "\d\d\d-\d\d-\d\dT\d\d:\d\d[-,+]\d\d:\d\d"/>
                          </restriction>
                       </simpleType>
426
                       </element>
427
428
429
430
431
                      <element name = "onset" minOccurs = "0">
                       <simpleType>
                         <restriction base = "xs:dateTime">
                            <pattern value = "\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,+]\d\d:\d\d"/>
                          </restriction>
432
                       </simpleType>
433
                       </element>
434
                      <element name = "expires" minOccurs = "0">
435
                        <simpleType>
436
                         <restriction base = "xs:dateTime">
437
438
                            <pattern value = "\d\d\d-\d\d-\d\dT\d\d:\d\d[-,+]\d\d:\d\d"/>
                          </restriction>
439
                       </simpleType>
440
                       </element>
441
                      <element name = "senderName" type = "xs:string" minOccurs = "0"/>
<element name = "headline" type = "xs:string" minOccurs = "0"/>
442
443
                      <element name = "description" type = "xs:string" minOccurs = "0"/>
444
                      <element name = "instruction" type = "xs:string" minOccurs = "0"/>
445
                      <element name = "web" type = "xs:anyURI" minOccurs = "0"/>
446
                      <element name = "contact" type = "xs:string" minOccurs = "0"/>
447
                      <element name = "parameter" minOccurs = "0" maxOccurs = "unbounded">
448
                        <complexType>
449
450
                           <sequence>
                             <element ref = "cap:valueName"/>
451
452
                             <element ref = "cap:value"/>
                           </sequence>
453
                        </complexType>
454
                      </element>
455
                      <element name = "resource" minOccurs = "0" maxOccurs = "unbounded">
4<u>56</u>
                         <complexType>
457
                          <sequence>
458
                             <element name = "resourceDesc" type = "xs:string"/>
459
                             <element name = "mimeType" type = "xs:string"/>
460
                             <element name = "size" type = "xs:integer" minOccurs = "0"/>
461
                             <element name = "uri" type = "xs:anyURI" minOccurs = "0"/>
462
                             <element name = "derefUri" type = "xs:string" minOccurs = "0"/>
463
                             <element name = "digest" type = "xs:string" minOccurs = "0"/>
464
                          </sequence>
465
                         </complexType>
466
                      </element>
467
                      <element name = "area" minOccurs = "0" maxOccurs = "unbounded">
468
                         <complexType>
469
470
                           <sequence>
                             <element name = "areaDesc" type = "xs:string"/>
471
472
473
                             <element name = "polygon" type = "xs:string" minOccurs = "0" maxOccurs =</pre>
        "unbounded"/>
                             <element name = "circle" type = "xs:string" minOccurs = "0" maxOccurs =</pre>
474
475
        "unbounded"/>
                             <element name = "geocode" minOccurs = "0" maxOccurs = "unbounded">
476
477
                               <complexType>
                                 <sequence>
478
                                   <element ref = "cap:valueName"/>
479
                                   <element ref = "cap:value"/>
480
                                 </sequence>
481
                               </complexType>
482
                             </element>
483
                             <element name = "altitude" type = "xs:decimal" minOccurs = "0"/>
484
                             <element name = "ceiling" type = "xs:decimal" minOccurs = "0"/>
485
                           </sequence>
```

486	
487	
488	
489	
490	
491	<any <="" maxoccurs="unbounded" minoccurs="0" namespace="http://www.w3.org/2000/09/xmldsig#" th=""></any>
492	processContents = "lax"/>
493	
494	
495	
496	
497	<pre><element name="valueName" type="xs:string"></element></pre>
498	<element name="value" type="xs:string"></element>
499	
500	
501	
501	

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

#### 504 **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.

#### 510 3.5.2 Formal Mappings and Specification

- 511 The normative specification of the compact binary encoding is in 3.5.3 with the application of the ASN.1 512 Unaligned Packed Encoding Rules (see ITU-T Rec. X.691).
- 513 The semantics of the fields in the ASN.1 specification are identical to those of the XSD specification, and 514 the mapping of the fields from the XSD specification to the ASN.1 specification is formally defined in ITU-515 T Rec. X.694.
- 516 Implementations can produce and process the CAP alert XML messages using either ASN.1-based or 517 XSD-based tools (or other ad hoc software).
- 518 Implementations can produce and process the CAP alert compact binary messages using ASN.1-based 519 tools (or by other ad hoc software).
- 520 Any XML encoded CAP alert messages can be converted to compact binary messages by decoding with
- 521 an ASN.1 tool configured for the Extended XML Encoding Rules and re-encoding the resulting abstract 522 values with an ASN.1 tool configured for Unaligned Packed Encoding Rules.
- 522 Values with an ASN. I tool configured for Onalighed 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.

#### 526 3.5.3 ASN.1 Schema

```
527
          CAP-1-2 {itu-t recommendation x cap(1303) version1-2(2)}
528
          DEFINITIONS XER INSTRUCTIONS AUTOMATIC TAGS ::=
529
          -- CAP Alert Message (version 1.2)
530
          BEGIN
531
532
          Alert ::= SEQUENCE {
533
             identifier IdentifierString,
534
                 -- Unambiguous identification of the message
535
                 -- from all messages from
536
                 -- this sender, in a format defined by the sender and
537
                 -- identified in the "sender" field below.
538
             sender
                       String,
                -- The globally unambiguous identification of the sender.
539
540
                 -- This specification does not define the root of
541
                 -- a global identification tree (there is no international
542
                 -- agreement on such a root), so it relies
543
                 -- on human-readable text to define globally and
544
                 -- unambiguously the sender.
545
                 -- An internet domain name or use of "iri:/ITU-T/..."
546
                 -- are possible, but
547
                -- the choice needs to be clearly stated in human-readable form.
548
                       DateTime (CONSTRAINED BY {/* XML representation of the XSD
             sent
549
          pattern "\d\d\d-\d\d-\d\dT\d\d:\d\d[-,+]\d\d:\d\d" */}),
550
            status AlertStatus,
551
                      AlertMessageType,
             msgType
552
             source
                        String OPTIONAL,
553
               -- Not standardised human-readable identification
```

```
554
                -- of the source of the alert.
555
                       AlertScope,
             scope
556
             restriction String OPTIONAL,
557
                 -- Not standardised human-readable restrictions
558
                 -- on the distribution of the alert message
559
             addresses
                        String OPTIONAL,
560
                 -- A space separated list of addressees for private messages
                 -- (see 3.2.1)
561
562
             code-list SEQUENCE SIZE((0..MAX)) OF code String,
563
                 -- A sequence codes for special handling
564
                 -- (see 3.2.1)
565
                 -- The format and semantics of the codes are not defined in this
566
                 -- specification.
567
             note
                        String OPTIONAL,
568
                 -- Not standardised human-readable clarifying text for the alert
569
                 -- (see 3.2.1)
570
             references String OPTIONAL,
571
                 -- Space-separated references to earlier messages
572
                 -- (see 3.2.1)
573
             incidents String OPTIONAL,
574
                 -- Space-separated references to related incidents
575
                 -- (see 3.2.1)
576
                        SEQUENCE SIZE((0..MAX)) OF info AlertInformation }
             info-list
577
578
          AlertStatus ::= ENUMERATED {
579
                  actual,
580
                  draft,
581
                  exercise,
582
                  system,
583
                  test }
584
585
          AlertMessageType ::= ENUMERATED {
586
                  ack,
587
                  alert,
588
                  cancel,
589
                  error,
590
                  update }
591
592
          AlertScope ::= ENUMERATED {
593
                  private,
594
                  public,
595
                  restricted }
596
597
          AlertInformation ::= SEQUENCE {
598
                              Language -- DEFAULT "en-US" --
             language
599
                 -- The language used in this value of the Info type
600
                 -- (see 3.2.2)
601
             category-list
                                SEQUENCE (SIZE(1..MAX)) OF
602
                                category InformationCategory,
603
             event
                                String,
604
                 -- Not standardised human-readable text describing the
605
                 -- type of the event (see 3.2.2)
606
             responseType-list SEQUENCE SIZE(((0..MAX)) OF
607
                               responseType InformationResponseType,
608
             urgency
                               HowUrgent,
609
             severity
                               HowSevere,
610
             certainty
                              HowCertain,
611
             audience
                               String OPTIONAL,
612
                 -- Not standardised human-readable text describing the
613
                 -- intended audience for the message (see 3.2.2)
614
             eventCode-list
                               SEQUENCE SIZE((0..MAX)) OF eventCode SEQUENCE {
615
                    valueName ValueName,
616
                    value
                              Value },
```

```
617
                              DateTime (CONSTRAINED BY {/* XML representation of the
             effective
618
          XSD pattern "\d\d\d-\d\d-\d\dT\d\d:\d\d[-,+]\d\d:\d\d" */}) OPTIONAL,
619
                              DateTime (CONSTRAINED BY {/* XML representation of the
             onset
620
          621
                              DateTime (CONSTRAINED BY {/* XML representation of the
             expires
622
          XSD pattern "\d\d\d\d-\d\dT\d\d:\d\d:\d\d[-,+]\d\d:\d\d" */}) OPTIONAL,
623
             senderName
                              String OPTIONAL,
624
                 -- Not standardised human-readable name of the authority
625
                -- issuing the message (see 3.2.2)
626
             headline
                              String (SIZE (1..160,...)) OPTIONAL,
627
                -- Not standardised human-readable short statement (headline)
628
                -- of the alert (see 3.2.2)
629
             description
                              String OPTIONAL,
630
                -- Not standardised human-readable extended description of
631
                -- the event (see 3.2.2)
632
             instruction
                              String OPTIONAL,
633
                -- Not standardised human-readable recommended action
634
                -- (see 3.2.2)
635
                              AnyURI OPTIONAL,
             web
636
                              String OPTIONAL,
             contact
637
                -- Not standardised human-readable contact details for
638
                 -- follow-up (see 3.2.2)
639
             parameter-list
                             SEQUENCE SIZE((0..MAX)) OF parameter SEQUENCE {
640
                -- System-specific parameters (see 3.2.2)
641
                valueName ValueName,
642
                value
                        Value },
643
             resource-list
                             SEQUENCE SIZE((0..MAX)) OF resource ResourceFile,
644
             area-list
                              SEQUENCE SIZE((0..MAX)) OF Area }
645
646
          InformationCategory ::= ENUMERATED {
647
                  CBRNE,
648
                  env,
649
                 fire,
650
                  geo,
651
                  health,
652
                 infra,
653
                 met,
654
                 other,
655
                 rescue,
656
                 safety,
657
                  security,
658
                  transport }
659
660
          InformationResponseType ::= ENUMERATED {
661
                 allClear,
662
                 assess,
663
                  avoid,
664
                  evacuate,
665
                  execute,
666
                  monitor,
667
                  none,
668
                  prepare,
669
                 shelter }
670
671
          HowUrgent ::= ENUMERATED {
672
                  expected,
673
                  future,
674
                 immediate,
675
                 past,
676
                 unknown }
677
678
          HowSevere ::= ENUMERATED {
679
                  extreme,
680
                 minor,
```

```
681
                  moderate,
682
                  severe.
683
                  unknown }
684
685
          HowCertain ::= ENUMERATED {
686
                  likely,
687
                  observed,
688
                  possible,
689
                  unknown,
690
                  unlikely }
691
692
          ResourceFile ::= SEQUENCE {
693
                 -- Information about an associated resource file
694
                 -- (see 3.2.3)
695
             resourceDesc String,
696
                 -- Not standardised human-readable description of the type
697
                 -- and content of
698
                 -- an associated resource file (for example a map or
699
                 -- photograph) (see 3.2.3)
700
             mimeType
                          String,
701
             size
                          INTEGER OPTIONAL, -- In bytes
702
             uri
                          AnyURI OPTIONAL,
703
                         String OPTIONAL,
             derefUri
704
                 -- An alternative to the URI giving the Base64-encoded
705
                 -- content of the resource file (see 3.2.3)
706
                          String OPTIONAL
             digest
707
                 -- SHA-1 hash of the resource file for error detection
708
                -- (see 3.2.3) -- }
709
710
          Area ::= SEQUENCE {
711
                 -- Identification of an affected area
712
             areaDesc
                          String,
713
                 -- Not standardised human-readable description of the area
714
             polygon-list SEQUENCE OF polygon String,
715
                 -- Each element is a space-separated list of coordinate pairs
716
                 -- The complete list starts and ends with the same point and
717
                 -- defines the polygon that defines the area
718
                 -- (see 3.2.4).
719
             circle-list SEQUENCE OF circle String,
720
                 -- A space-separated list of coordinates for a point and a radius
721
             geocode-list SEQUENCE SIZE((0..MAX)) OF geocode SEQUENCE {
722
                 -- A geographic code designating the alert target area
723
                 -- (see 3.2.4)
724
                      valueName ValueName,
725
                      value
                                Value },
726
             altitude
                       REAL OPTIONAL,
727
                 -- Specific or minimum altitude of the affected area
728
                      REAL OPTIONAL
             ceiling
729
                 -- Maximum altitude of the affected area -- }
730
731
          ValueName ::= String -- A not standardised name for
732
                 -- an information event code, a parameter or a geocode
733
734
          Value ::= String -- The value of the information event code,
735
                              -- parameter or geocode
736
737
          String ::= UTF8String (FROM (
738
                      {0,0,0,9} -- TAB
739
                    | {0,0,0,10} -- CR
740
                    | {0,0,0,13} -- LF
741
                    | \{0,0,0,32\}..\{0,0,215,255\} -- Space to the start of the S-zone
742
                    | {0,0,224,0}...{0,0,255,253} -- Rest of BMP after S-zone
743
                    | {0,1,0,0}..{0,16,255,253} -- Other planes -- ) )
744
```

```
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\} \dots \{0, 0, 215, 255\}
         |\{0, 0, 224, 0\} \dots \{0, 0, 255, 253\}
         |\{0,1,0,0\}..\{0,16,255,255\})\rangle
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
```

789

745

746 747

748

749

750 751

752

753 754

755

756 757

758

759

760

761 762

763

764

765

766 767

768

769 770

771

772

773

774

775

776

777

778

779

780

781

782

783

784

785

786

787

# 790 **4 Conformance**

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

793 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.
- 798

#### 799 **4.1 Conformance Targets**

- 800 The following conformance targets are defined in order to support the specification of conformance to this 801 standard:
- a) CAP V1.2 Message
- 803 b) CAP V1.2 Message Producer
- 804 c) CAP V1.2 Message Consumer

#### 805

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

- 807 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.oasisopen.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.
- 812

# 813 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(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;
- 829

### **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
- 838
- 839

# 840 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/

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

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

```
845
       <?xml version = "1.0" encoding = "UTF-8"?>
846
847
       <alert xmlns = "urn:oasis:names:tc:emergency:cap:1.2">
         <identifier>43b080713727</identifier>
848
849
         <sender>hsas@dhs.gov</sender>
         <sent>2003-04-02T14:39:01-05:00</sent>
850
         <status>Actual</status>
851
         <msgType>Alert</msgType>
852
         <scope>Public</scope>
853
854
         <info>
           <category>Security</category>
855
856
           <event>Homeland Security Advisory System Update</event>
           <urgency>Immediate</urgency>
857
           <severity>Severe</severity>
858
           <certainty>Likely</certainty>
859
           <senderName>U.S. Government, Department of Homeland Security</senderName>
860
           <headline>Homeland Security Sets Code ORANGE</headline>
861
           <description>The Department of Homeland Security has elevated the Homeland Security Advisory
862
       System threat level to ORANGE / High in response to intelligence which may indicate a heightened
863
       threat of terrorism.</description>
864
           <instruction> A High Condition is declared when there is a high risk of terrorist attacks. In
865
       addition to the Protective Measures taken in the previous Threat Conditions, Federal departments
866
       and agencies should consider agency-specific Protective Measures in accordance with their
867
       existing plans.</instruction>
868
           <web>http://www.dhs.gov/dhspublic/display?theme=29</web>
869
           <parameter>
870
             <valueName>HSAS</valueName>
871
872
             <value>ORANGE</value>
           </parameter>
873
           <resource>
874
875
             <resourceDesc>Image file (GIF)</resourceDesc>
             <mimeType>image/gif</mimeType>
876
877
             <uri>http://www.dhs.gov/dhspublic/getAdvisoryImage</uri>
           </resource>
878
879
           <area>
             <areaDesc>U.S. nationwide and interests worldwide</areaDesc>
880
           </area>
881
         </info>
882
       </alert>
```

### 884 A.2. Severe Thunderstorm Warning

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

```
886
       <?xml version = "1.0" encoding = "UTF-8"?>
887
       <alert xmlns = "urn:oasis:names:tc:emergency:cap:1.2">
888
         <identifier>KST01055887203</identifier>
889
         <sender>KSTO@NWS.NOAA.GOV</sender>
890
         <sent>2003-06-17T14:57:00-07:00</sent>
891
         <status>Actual</status>
892
         <msgType>Alert</msgType>
893
         <scope>Public</scope>
894
         <info>
895
           <category>Met</category>
896
           <event>SEVERE THUNDERSTORM</event>
897
           <responseType>Shelter</responseType>
898
           <urgency>Immediate</urgency>
899
           <severity>Severe</severity>
900
           <certainty>Observed</certainty>
901
           <eventCode>
902
             <valueName>SAME</valueName>
903
             <value>SVR</value>
904
           </eventCode>
905
           <expires>2003-06-17T16:00:00-07:00</expires>
906
           <senderName>NATIONAL WEATHER SERVICE SACRAMENTO CA</senderName>
907
           <headline>SEVERE THUNDERSTORM WARNING</headline>
908
           <description> AT 254 PM PDT...NATIONAL WEATHER SERVICE DOPPLER RADAR INDICATED A SEVERE
909
       THUNDERSTORM OVER SOUTH CENTRAL ALPINE COUNTY... OR ABOUT 18 MILES SOUTHEAST OF KIRKWOOD ... MOVING
910
       SOUTHWEST AT 5 MPH. HAIL...INTENSE RAIN AND STRONG DAMAGING WINDS ARE LIKELY WITH THIS
911
       STORM.</description>
912
           <instruction>TAKE COVER IN A SUBSTANTIAL SHELTER UNTIL THE STORM PASSES./instruction>
913
           <contact>BARUFFALDI/JUSKIE</contact>
914
915
916
           <area>
             <areaDesc>EXTREME NORTH CENTRAL TUOLUMNE COUNTY IN CALIFORNIA, EXTREME NORTHEASTERN
       CALAVERAS COUNTY IN CALIFORNIA, SOUTHWESTERN ALPINE COUNTY IN CALIFORNIA</areaDesc>
917
             <polygon>38.47,-120.14 38.34,-119.95 38.52,-119.74 38.62,-119.89 38.47,-120.14</polygon>
918
             <geocode>
919
               <valueName>SAME</valueName>
920
               <value>006109</value>
921
             </geocode>
922
923
             <geocode>
               <valueName>SAME</valueName>
924
               <value>006009</value>
925
926
             </geocode>
             <geocode>
927
                <valueName>SAME</valueName>
928
               <value>006003</value>
929
             </geocode>
930
           </area>
931
         </info>
932
       </alert>
```

## 934 A.3. Earthquake Report (Update Message)

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

```
936
       <?xml version = "1.0" encoding = "UTF-8"?>
937
       <alert xmlns = "urn:oasis:names:tc:emergency:cap:1.2">
938
         <identifier>TRI13970876.2</identifier>
939
         <sender>trinet@caltech.edu</sender>
940
         <sent>2003-06-11T20:56:00-07:00</sent>
941
         <status>Actual</status>
942
         <msgType>Update</msgType>
943
         <scope>Public</scope>
944
         <references>trinet@caltech.edu,TRI13970876.1,2003-06-11T20:30:00-07:00</references>
945
         <info>
946
           <category>Geo</category>
947
           <event>Earthquake</event>
948
           <urgency>Past</urgency>
949
950
           <severity>Minor</severity>
           <certainty>Observed</certainty>
951
952
           <senderName>Southern California Seismic Network (TriNet) operated by Caltech and
       USGS</senderName>
953
           <headline>EQ 3.4 Imperial County CA</headline>
954
            <description>A minor earthquake measuring 3.4 on the Richter scale occurred near Brawley,
955
       California at 8:30 PM Pacific Daylight Time on Wednesday, June 11, 2003. (This event has now been
956
       reviewed by a seismologist) </description>
957
           <web>http://www.trinet.org/scsn/scsn.html</web>
958
959
           <parameter>
             <valueName>EventID</valueName>
960
             <value>13970876</value>
961
           </parameter>
962
           <parameter>
963
              <valueName>Version</valueName>
964
             <value>1</value>
965
           </parameter>
966
           <parameter>
967
             <valueName>Magnitude</valueName>
968
             <value>3.4 Ml</value>
969
           </parameter>
970
            <parameter>
971
             <valueName>Depth</valueName>
971
972
973
974
975
976
976
             <value>11.8 mi.</value>
           </parameter>
           <parameter>
             <valueName>Quality</valueName>
             <value>Excellent</value>
           </parameter>
978
979
           <area>
             <areaDesc>1 mi. WSW of Brawley, CA; 11 mi. N of El Centro, CA; 30 mi. E of OCOTILLO
980
        (quarry); 1 mi. N of the Imperial Fault</areaDesc>
981
             <circle>32.9525,-115.5527 0</circle>
982
            </area>
983
         </info>
984
       </alert>
```

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

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

```
988
        <?xml version = "1.0" encoding = "UTF-8"?>
        <alert xmlns = "urn:oasis:names:tc:emergency:cap:1.2">
 989
 990
           <identifier>KAR0-0306112239-SW</identifier>
 991
           <sender>KARO@CLETS.DOJ.CA.GOV</sender>
 992
           <sent>2003-06-11T22:39:00-07:00</sent>
 993
           <status>Actual</status>
 994
           <msgType>Alert</msgType>
 995
           <source>SW</source>
 996
           <scope>Public</scope>
 997
           <info>
 998
              <language>en-US</language>
 999
              <category>Rescue</category>
1000
              <event>Child Abduction</event>
1001
              <urgency>Immediate</urgency>
1002
              <severity>Severe</severity>
1003
              <certainty>Likely</certainty>
1004
              <eventCode>
1005
                 <valueName>SAME</valueName>
1006
                 <value>CAE</value>
1007
              </eventCode>
1008
              <senderName>Los Angeles Police Dept - LAPD</senderName>
1009
              <headline>Amber Alert in Los Angeles County</headline>
1010
              <description>DATE/TIME: 06/11/03, 1915 HRS. VICTIM(S): KHAYRI DOE JR. M/B BLK/BRO 3'0", 40
1011
        LBS. LIGHT COMPLEXION. DOB 06/24/01. WEARING RED SHORTS, WHITE T-SHIRT, W/BLUE COLLAR.
1012
        LOCATION: 5721 DOE ST., LOS ANGELES, CA. SUSPECT(S): KHAYRI DOE SR. DOB 04/18/71 M/B, BLK HAIR,
1013
        BRO EYE. VEHICLE: 81' BUICK 2-DR, BLUE (4XXX000).</description>
1014
              <contact>DET. SMITH, 77TH DIV, LOS ANGELES POLICE DEPT-LAPD AT 213 485-2389</contact>
1015
              <area>
1016
                 <areaDesc>Los Angeles County</areaDesc>
1017
                 <geocode>
1018
                    <valueName>SAME</valueName>
1019
                    <value>006037</value>
1020
                 </geocode>
1021
              </area>
1022
1023
           </info>
           <info>
1024
              <language>es-US</language>
1025
              <category>Rescue</category>
1026
              <event>Abducción de Niño</event>
1027
1028
              <urgency>Immediate</urgency>
              <severity>Severe</severity>
1029
              <certainty>Likely</certainty>
1030
              <eventCode>
1031
                 <valueName>SAME</valueName>
1032
                 <value>CAE</value>
1033
              </event.Code>
1034
              <senderName>Departamento de Policía de Los Ángeles - LAPD</senderName>
1035
              <headline>Alerta Amber en el condado de Los Ángeles</headline>
1036
              <description>DATE/TIME: 06/11/03, 1915 HORAS. VÍCTIMAS: KHAYRI DOE JR. M/B BLK/BRO 3'0", 40
1037
        LIBRAS. TEZ LIGERA. DOB 06/24/01. CORTOCIRCUITOS ROJOS QUE USAN, CAMISETA BLANCA, COLLAR DE
1038
        W/BLUE. LOCALIZACIÓN: 5721 DOE ST., LOS ÁNGELES. SOSPECHOSO: KHAYRI DOE ST. DOB 04/18/71 M/B,
1039
        PELO DEL NEGRO, OJO DE BRO. VEHÍCULO: 81' BUICK 2-DR, AZUL (4XXX000)</description>
1040
              <contact>DET. SMITH, 77TH DIV, LOS ANGELES POLICE DEPT-LAPD AT 213 485-2389</contact>
1041
              <area>
1042
                 <areaDesc>condado de Los Ángeles</areaDesc>
1043
                 <geocode>
1044
                    <valueName>SAME</valueName>
1045
                    <value>006037</value>
1046
                 </geocode>
1047
              </area>
1048
           </info>
1049
        </alert>
```

# 1050 Appendix B. Acknowledgments

# 1051 OASIS Emergency Management Technical Committee

1052	Doug Allport, Canadian Association for Public Alerting and Notification (CAPAN)
1053	Patti Aymond, IEM
1054	Himadri Banerjee, Previstar Inc.
1055	Frank Bell, Individual
1056	Art Botterell, Contra Costa County Community Warning System
1057	John Bradley, Individual
1058	Rex Brooks, Individual
1059	Robert Bunge, NOAA's National Weather Service
1060	Toby Considine, University of North Carolina at Chapel Hill
1061	William Cox, Cox Software Architects LLC
1062	Olivier Dubuisson, France Telecom
1063	Sukumar Dwarkanath, SRA International
1064	David Ellis, Sandia National Laboratories
1065	Thomas Ferrentino, Individual
1066	Jack Fox, US Department of Homeland Security
1067	Patrick Gannon, Warning Systems, Inc.
1068	Timothy Gilmore, US Department of Homeland Security
1069	James Goodson, US Department of Homeland Security
1070	Tim Grapes, Evolution Technologies Inc.
1071	Gary Ham, Individual
1072	Harry Haury, NuParadigm Government Systems, Inc.
1072	Werner Joerg, IEM
1074	Elysa Jones, Warning Systems, Inc.
1075	Jeff Jortner, Sandia National Laboratories
1076	William Kalin, US Department of Homeland Security
1077	Ram Kumar, Individual
1078	Jeff Kyser, Warning Systems, Inc.
1079	Ron Lake, Galdos Systems Inc.
1080	David Lamendsdorf, Emergency Interoperability Consortium
1081	Mike McDougall, Individual
1082	Donald McGarry, Mitre Corporation
1083	Tom Merkle, Lockheed Martin
1084	Enoch Moses, ManTech Enterprise Integration Center (e-IC)
1085	Brian Nelson, Sandia National Laboratories
1086	Camille Osterloh, US Department of Homeland Security
1087	John Pitale, Edmond Scientific Company
1088	Mark Pleimann, Mitre Corporation
1089	Donald Ponikvar, US Department of Homeland Security
1090	Jacqueline Postell, US Department of Homeland Security
1091 1092	Carl Reed, Open Geospatial Consortium, Inc. (OGC) Dean Reese, ESI Acquisition, Inc.
	Kirby Rice, Eye Street Solutions
1093	
1094 1095	Howard Ryan, Desktop Alert Inc.
	Tracy Ryan, Emergency Interoperability Consortium
1096	Josh Shows, ESI Acquisition, Inc. Aviv Siegel, AtHoc, Inc.
1097	
1098	Andrew Sonner, Evolution Technologies Inc.
1099	Christopher Springer, US Department of Homeland Security
1100	Steve Streetman, US Department of Homeland Security
1101	Lee Tincher, Evolution Technologies Inc.

- 1102 James Trawick, viaRadio Corporation
- 1103
- Alessandro Triglia, OSS Nokalva Richard Vandame, US Department of Homeland Security 1104
- 1105 Matt Walton, Individual
- Jeff Waters, US Department of Defense (DoD) 1106
- 1107 David Webber, Individual
- 1108 Jacob Westfall, Individual
- David Yarbrough, Northrop Grumman 1109
- 1110 1111

# 1112 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	<ul> <li>Messaging Subcommittee approved changes based on initial public comment period:</li> <li>Expanded the scope of the <addresses> element</addresses></li> <li>Changed <mimetype> to be a required element and added note for <size></size></mimetype></li> <li>Qualified the base schema types in the schema</li> <li>Changed the schema typing for <altitude> and <ceiling> to be a decimal instead of a string</ceiling></altitude></li> <li>ASN.1 examples were added</li> <li>Various editorial corrections</li> </ul>
1.2	2009-04-28	Jacob Westfall	<ul> <li>Technical Committee approved the v. 1.2 draft with the following additional changes:</li> <li>DateTime Data Type moved to Implementation Notes</li> <li>Changes to <status> and <note> descriptions</note></status></li> <li>Wording change to <severity> "Minor"</severity></li> <li>Schema changed to allow only one <encrypteddata> element and changed Security Note section to allow multiple <signature> elements</signature></encrypteddata></li> <li>Various editorial corrections and clarifications</li> </ul>
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

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
			<ul> <li>New <responsetype> values of Avoid and AllClear</responsetype></li> </ul>
			<ul> <li>Clarification on acceptable <polygon> values and the use of character entity references</polygon></li> </ul>
			<ul> <li>Schemas were updated to reflect changes and to validate when XML signature/encryption elements are present</li> </ul>
			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:
			<ul> <li>Reordered items in object diagram and data dictionary to match sequence required by schema.</li> </ul>
			• Edited schema to make <scope> mandatory and to permit multiple instances of <responsetype> and <eventcode>, in accordance with the data dictionary.</eventcode></responsetype></scope>
1.1	2005-07-23	Art Botterell	Applied changes per recommendations of Messaging Subcommittee based on initial public comment period:
			<ul> <li>Modified XML syntax of <eventcode> ,</eventcode></li> <li><parameter> and <geocode></geocode></parameter></li> </ul>
			Added "Draft" value for <status></status>
			Changed CAP namespace to URN form
			• Tightened usage of dateTime formats in <sent>, <effective>, <onset> and <expiration></expiration></onset></effective></sent>
			<ul> <li>Corrected schema to correct value of "CBRNE" in <event></event></li> </ul>
			Conformed examples in Appendix A to new namespace.
1.1	2005-04-28	Elysa Jones	Technical Committee approved the v. 1.1 draft with the following additional changes:
			<ul> <li>Normative language added to specify uniqueness of <identifier></identifier></li> </ul>
			<ul> <li>Change [dateTime] format for <sent>, <effective>, <onset> and <expires> elements</expires></onset></effective></sent></li> </ul>
			<ul> <li>Change <language> element RFC from 1166 to 3066 and added null</language></li> </ul>
			<ul> <li>Changed the <minetype> element RFC 1521 to 2046</minetype></li> </ul>
			Added <derefuri> element</derefuri>
			Security Note updated and added Digital Signature and Encryption note paragraphs

1.1	2005-01-04	Art Botterell	Messaging Subcommittee approved v. 1.1 draft for submission to full Technical Committee:
			<ul> <li>Added <responsetype> element</responsetype></li> </ul>
			Made <category> element mandatory</category>
			<ul> <li>Amended enumerated values for the <certainty> element</certainty></li> </ul>
			Deleted the <password> element</password>
			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.)