Common Alerting Protocol, v. 0.9

Draft for Public Comment, 20 June 2003

Document identifier:

emergency-CAP-0.9

Location:

http://www.oasis-open.org/committees/emergency/

Editor:

Art Botterell, Partnership for Public Warning <acb@incident.com>

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 is a draft for discussion by the Emergency Management Technical Committee and for public comment. This document is updated periodically. Send comments about this document to the editor.

Committee members should send comments on this specification to the emergency@lists.oasis-open.org list. Others should subscribe to and send comments to the emergency-comment@lists.oasis-open.org list. To subscribe, send an email message to emergency-comment-request@lists.oasis-open.org with the word "subscribe" as the body of the message.

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 Emergency Management TC web page (http://www.oasis-open.org/committees/emergency/).

Table of Contents

1. Introduction

1.1. Purpose

The Common Alerting Protocol (CAP) provides an open, non-proprietary digital message format for all types of alerts and notifications. 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 NOAA Weather Radio and the Emergency Alert System, while offering enhanced capabilities that include:

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

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

1.2. History

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

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

In 2002 the CAP initiative was endorsed by the national non-profit Partnership for Public Warning, which sponsored its contribution in 2003 to the OASIS standards process.

1.3. Structure of the CAP Alert Message

Each CAP Alert Message consists of an <alert> segment, which may contain one or more <info> segments, each of which may include one or more <area> segments. (See the document object model diagram in section 3.1, below.)

1.3.1. <alert>

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

1.3.2. <info>

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

1.3.3. <area>

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

1.4. Applications of the CAP Alert Message

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

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

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

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

1.5. Terminology

Within this document 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]**.

1.6. Normative References

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

2. Design Principles and Concepts (non-normative)

2.1. Design Philosophy

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

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

2.2. Requirements for Design

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

The Common Alerting Protocol SHOULD:

1. Provide a specification for a simple, extensible format for digital representation of warning messages and notifications;
2. Enable integration of diverse sensor, threat-evaluation and dissemination systems;
3. Be usable over multiple transmission systems, including both TCP/IP-based networks and one-way "broadcast" channels;
4. Support credible end-to-end authentication and validation of all messages;
5. Provide a unique identifier (e.g., an ID number) for each warning message and for each message originator;
6. Provide for multiple message types, such as:

    a. Warnings
    b. Acknowledgements
    c. Expirations and cancellations
    d. Updates and amendments
    e. Reports of results from dissemination systems
    f. Administrative and system messages
7. Provide for flexible description of each warning's:
    a. Geographic targeting
    b. Level of urgency
    c. Level of certainty
    d. Level of threat severity
8. Provide a mechanism for referencing supplemental information (e.g., digital audio or image files, additional text);
9. Use an established open-standard data representation;
10. Be based on a program of real-world cross-platform testing and evaluation;
11. Provide a clear basis for certification and further protocol evaluation and improvement; and,
12. Provide a clear logical structure that is relevant and clearly applicable to the needs of emergency response and public safety users and warning system operators.

2.3. Examples of Use Scenarios

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

2.3.1. Manual Origination

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

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

2.3.2. Automated Origination by Autonomous Sensor System

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

2.3.3. Aggregation and Correlation on Real-time Map

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

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

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 by authorized authority of a single CAP message.

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

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

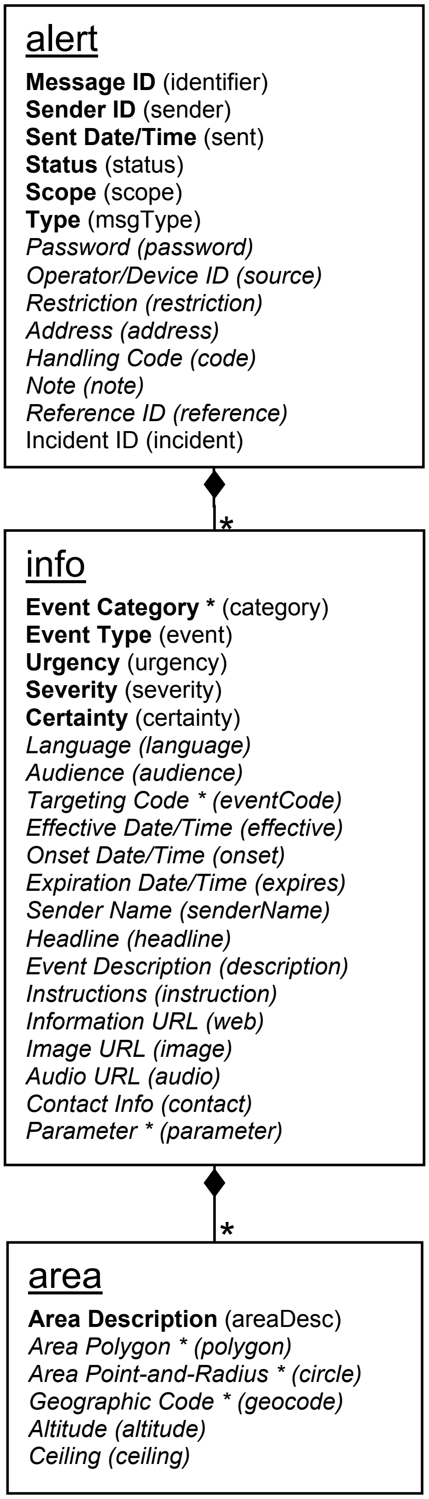
2.3.5. Repudiating A False Alarm

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

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

3. Alert Message Structure (normative)

3.1. Document Object Model


alert
Message ID (identifier)
Sender ID (sender)
Sent Date/Time (sent)
Status (status)
Scope (scope)
Type (msgType)
Password (password)
Operator/Device ID (source)
Restriction (restriction)
Address (address)
Handling Code (code)
Note (note)
Reference ID (reference)
Incident ID (incident)
*
info
Event Category * (category)
Event Type (event)
Urgency (urgency)
Severity (severity)
Certainty (certainty)
Language (language)
Audience (audience)
*Targeting Code * (eventCode)*
Effective Date/Time (effective)
Onset Date/Time (onset)
Expiration Date/Time (expires)
Sender Name (senderName)
Headline (headline)
Event Description (description)
Instructions (instruction)
Information URL (web)
Image URL (image)
Audio URL (audio)
Contact Info (contact)
*Parameter * (parameter)*
*
area
Area Description (areaDesc)
*Area Polygon * (polygon)*
*Area Point-and-Radius * (circle)*
*Geographic Code * (geocode)*
Altitude (altitude)
Ceiling (ceiling)

Elements in **bold** are mandatory; those in *italics* are optional; asterisk (*) indicates multiple instances permitted

3.2. Data Dictionary

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

cap: alert	**message. alert. group**	**The container for all component parts of the alert message (mandatory)**	(1) Surrounds CAP alert message sub-elements.
			(2) Must include the xmlns attribute referencing the CAP URI as the namespace, e.g.:
			`<cap:alert xmlns:cap="http://www.incident.com/cap">`
			[sub-elements]
			`</cap:alert>`
			(3) In addition to the specified sub-elements, may contain one or more <info> blocks.

cap: identifier	**message. identifier**	**The identifier of the alert message (mandatory)**	(1) A number or string uniquely identifying this message, assigned by the sender (2) No spaces or restricted characters (< and &)
cap: sender	**message. sender. identifier**	**The identifier of the sender of the alert message (mandatory)**	(1) Identifies the originator of this alert. Guaranteed by assigner to be unique globally; e.g., may be based on an Internet domain name (2) No spaces or restricted characters (< and &)
cap: password	message. password. string	The string representing the password of the alert message (optional)	The string password is used for authenticating the sender. (Note that this element should only be used on secure channels, and that simple password authentication schemes have numerous well-known weaknesses.)
cap: source	message. source. identifier	The text identifying the source of the alert message (optional)	The source may be an operator or a device.
cap: sent	**message. sent. time**	**The time and date of the origination of the alert message (mandatory)**	The date and time is represented in ISO 8601 format (e. g., "`2002-05-24T16:49:00-07:00`" for 24 May 2002 at 16: 49 PDT).

cap: status	**message. status. code**	**The code denoting the appropriate handling of the alert message (mandatory)**	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
cap: scope	**message. scope. code**	**The code denoting the intended distribution of the alert message (mandatory)**	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 <address>, below)
cap: restriction	message. restriction. text	The text describing the rule for limiting distribution of the restricted alert message (conditional)	Used when <scope> value is "Restricted"
cap: address	message. address. group	The group listing of intended recipients of the private alert message (conditional)	(1) Used when <scope> value is "Private" (2) Each recipient may be identified by an identifier or an address
cap: code	message. control. code	The code denoting the special handling of the alert message (optional)	Any user-defined flag or special code used to flag the alert message for special handling.

cap: msgType	**message. type. code**	**The code denoting the nature of the alert message (mandatory)**	Code Values: • “Alert” - Initial information requiring attention by targeted recipients • “Update” - Updates and supercedes the earlier message(s) identified in <reference> • “Cancel” - Cancels the earlier message(s) identified in <reference> • “Ack” - Acknowledges receipt and acceptance of the message(s)) identified in <reference> • “Error” indicates rejection of the message(s) identified in <reference>; explanation should appear in <note>
cap: note	message. note. text	The text describing the purpose or significance of the alert message (optional)	The message note is primarily intended for use with Cancel and Error alert message types.
cap: reference	message. reference. group	The group listing identifying earlier messages referenced by the alert message (optional)	(1) The extended message identifier (in the form *identifier/ sender)* of an earlier message or messages referenced by this one. (2) If multiple messages are referenced, they are separated by whitespace.
cap: incident	message. incident. name	The name of the referent incident of the alert message (optional)	Used to collate multiple messages referring to different aspects of the same incident

3.2.2. "info" Element and Sub-elements

cap: info	message. info. group	The container for all component parts of the info sub-element of the alert message (optional)	(1) Multiple occurrences are permitted within a single <alert>. If targeting of multiple "info" blocks in the same language overlaps, information in later blocks may expand but may not override the corresponding values in earlier ones. Each set of "info" blocks containing the same language identifier is to be treated as a separate sequence. (2) In addition to the specified sub-elements, may contain one or more <area> blocks.

cap: language	message. language. code	The code denoting the language of the info sub-element of the alert message (optional)	(1) Code Values: Natural language identifier per RFC 1766. (2) If not present, assumed value is "en-US".
cap: category	**message. category. code**	**The code denoting the category of the subject event of the alert message (mandatory)**	(1) Code Values: • “Geo” - Geophysical (inc. landslide) • “Met” - Meteorological (inc. flood) • “Safety” - General emergency and public safety • “Security” - Law enforcement, military, homeland and local/private security • “Rescue” - Rescue and recovery • “Fire” - Fire suppression and rescue • “Health” - Medical and public health • “Env” - Pollution and other environmental • “Transport” - Public and private transportation • “Infra” - Utility, telecommunication, other non-transport infrastructure • “Other” - Other events (2) Multiple instances may occur within a single "info" block.
cap: event	**message. event. text**	**The text denoting the type of the subject event of the alert message (mandatory)**	The text may use a specified nomenclature if available.

cap: urgency	**message. urgency. code**	**The code denoting the urgency of the subject event of the alert message (mandatory)**	(1) The “urgency”, “severity”, and “certainty” elements collectively may distinguish less emphatic from more emphatic messages. (2) Code Values: • “Immediate” - Responsive action should be taken immediately • “Expected” - Responsive action should be taken soon (within next hour) • “Future” - Responsive action should be taken in the near future • “Past” - Responsive action is no longer required • “Unknown” - Urgency not known
cap: severity	**message. severity. code**	**The code denoting the severity of the subject event of the alert message (mandatory)**	(1) The “urgency”, “severity”, and “certainty” elements collectively may distinguish less emphatic from more emphatic messages. (2) Code Values: • “Extreme” - Extraordinary threat to life or property • “Severe” - Significant threat to life or property • “Moderate” - Possible threat to life or property • “Minor” - Minimal threat to life or property • “Unknown” - Severity unknown
cap: certainty	**message. certainty. code**	**The code denoting the certainty of the subject event of the alert message (mandatory)**	(1) The “urgency”, “severity”, and “certainty” elements collectively may distinguish less emphatic from more emphatic messages. (2) Code Values: • “Very Likely” - Highly likely (p > ~ 85%) or certain • “Likely” - Likely (p > ~50%) • “Possible” - Possible but not likely (p <= ~50%) • “Unlikely” - Not expected to occur (p ~ 0) • “Unknown” - Certainty unknown
cap: audience	message. audience. text	The text describing the intended audience of the alert message (optional)	

cap: eventCode	message. target. code	The system-specific code identifying the event type	(1) Code Values: Any system-specific code for event typing, in the form "code_type= code" where "code_type" is a user-assigned designator for the target system (e. g,, "SAME=CEM"). Designators may not include spaces or XML-restricted characters (<, >, &, ',"). (2) Multiple instances may occur within a single "info" block.
cap: effective	message. effective. time	The effective time of the information of the alert message (optional)	(1) The date and time is represented in ISO 8601 format (e. g., “2002-05-24T16:49:00-07:00” for 24 May 2002 at 16: 49 PDT). (2) If this item is not included, it is assumed the same as in <sent>.
cap: onset	message. onset. time	The expected time of the beginning of the subject event of the alert message (optional)	(1) The date and time is represented in ISO 8601 format (e. g., “2002-05-24T16:49:00-07:00” for 24 May 2002 at 16: 49 PDT). (2) If this item is not included, it is assumed the same as in <sent>.
cap: expires	message. expires. time	The expiry time of the information of the alert message (optional)	(1) The date and time is represented in ISO 8601 format (e. g., “2002-05-24T16:49:00-07:00” for 24 May 2002 at 16: 49 PDT). (2) If this item is not provided, each recipient is free to set its own policy as to when the message is not longer in effect.
cap: senderName	message. sender. name	The text naming the originator of the alert message (optional)	The human-readable name of the agency or authority issuing this alert.
cap: headline	message. headline. text	The text headline of the alert message (optional)	A brief human-readable headline. Note that some displays 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.
cap: description	message. description. text	The text describing the subject event of the alert message (optional)	

cap: instruction	message. instruction. text	The text describing the recommended action to be taken by recipients of the alert message (optional)	
cap: web	message. information. 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
cap: image	message. image. identifier	The identifier of the hyperlink associating the image with the alert message (optional)	A full, absolute URI of an online image file
cap: audio	message. audio. identifier	The identifier of the hyperlink associating the audio with the alert message (optional)	A full, absolute URI of an online audio file.
cap: contact	message. contact. text	The text describing the contact for follow-up and confirmation of the alert message (optional)	

cap: parameter	message. parameter. group	The group listing of additional parameters associated with the alert message (optional)	(1) Code Values: Parameter label / value pair(s) in the form "label=value". (2) Multiple instances may occur within a single "info" block.

3.2.3. "area" Element and Sub-elements

cap: area	message. area. group	The container for all component parts of the area sub-element of the info sub-element of the alert message (optional)	(1) Multiple occurrences permitted, in which case the target area for the "info" block is the union of all the included "area" blocks. (2) May contain one or multiple instances of <polygon>, <circle> or <geocode>. If multiple <polygon>, <circle> or <geocode> elements are included, the area described by this <area> is the union of those represented by the included elements.
cap: areaDesc	**message. area. text**	**The text describing the affected area of the alert message (mandatory)**	A text description of the affected area.
cap: polygon	message. polygon. group	The group listing of the polygons delineating the affected area of the alert message (conditional)	(1) Code Values: The geographic polygon is represented by a whitespace-delimited list of WGS-84 coordinate values [see WGS-84 Note]. (2) Multiple instances may occur within an <area>.
cap: circle	message. circle. group	The paired values of a point and radius delineating the affected area of the alert message (conditional)	(1) Code Values: The circular area is represented by a central point given as a WGS-84 coordinate value [see WGS-84 Note], followed by a space character and a radius value in kilometers. (2) Multiple instances may occur within an <area>.

cap: geocode	message. geocode. code	The geographic code delineating the affected area of the alert message (conditional)	(1) Code Values: Any geographically-based code to describe message target area, in the form "code_type=code" where "code_type" is a user-assigned abbreviation for the target system (e. g,, "fips6=06003"). Code-types may not include spaces or XML-restricted characters (<, >, &, ',"). (2) Multiple instances may occur within an <area>. (3) 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 the equivalent and more universally understood <polygon> and <circle> representations whenever possible.
cap: altitude	message. altitude. quantity	The specific or minimum altitude of the affected area of the alert message (optional)	(1) If used with the <ceiling> element this value is the lower limit of a range. Otherwise, this value specifies a specific altitude. (2) The altitude measure is in feet above mean sea level (per WGS-84 datum).
cap: ceiling	message. ceiling. quantity	The maximum altitude of the affected area of the alert message (conditional)	(1) May only be used in combination with the <altitude> element (2) The altitude measure is in feet above mean sea level (per WGS-84 datum).

3.3. Implementation Notes

3.3.1. WGS-84 Note

Geographic locations in CAP are defined using WGS 84 (World Geodetic System 1984), equivalent to EPSG (European Petroleum Survey Group) code 4326 (2 dimensions). CAP does not assign responsibilities for coordinate transformations from and to other Spatial Reference Systems. A WGS-84 coordinate value is here represented as a comma-delimited latitude/longitude pair, measured in decimal degrees (un-projected). Latitudes range from -90 to 90 and longitudes range from -180 to 180. Coordinates in the Southern and Western hemispheres are signed negative with a leading dash.

3.3.2. Security Note

The OASIS WS-Security framework is recommended as the basis for ensuring message authenticity, integrity and (where applicable) confidentiality.

3.4. XML Schema

```
<?xml version = "1.0" encoding = "UTF-8"?>
<!-- Conforms to w3c http://www.w3.org/2001/XMLSchema-->
<schema xmlns = "http://www.w3.org/2001/XMLSchema"
   targetNamespace = "http://www.incident.com/cap/0.9"
   elementFormDefault = "qualified">
  <element name = "alert">
   <annotation>
     <documentation>CAP Alert Message (draft version 0.9)</documentation>
   </annotation>
   <complexType>
     <sequence>
      <element name = "identifier" type = "string"/>
      <element name = "sender" type = "string"/>
      <element name = "sent" type = "dateTime"/>
      <element name = "status">
        <simpleType>
         <restriction base = "string">
           <enumeration value = "Actual"/>
           <enumeration value = "Exercise"/>
           <enumeration value = "System"/>
           <enumeration value = "Test"/>
         </restriction>
        </simpleType>
      </element>
      <element name = "msgType">
        <simpleType>
         <restriction base = "string">
           <enumeration value = "Alert"/>
           <enumeration value = "Update"/>
           <enumeration value = "Cancel"/>
           <enumeration value = "Ack"/>
           <enumeration value = "Error"/>
         </restriction>
        </simpleType>
      </element>
      <element name = "password" type = "string" minOccurs = "0"/>
      <element name = "source" type = "string" minOccurs = "0"/>
      <element name = "scope" minOccurs = "0">
        <simpleType>
         <restriction base = "string">
           <enumeration value = "Public"/>
           <enumeration value = "Restricted"/>
           <enumeration value = "Private"/>
         </restriction>
        </simpleType>
      </element>
      <element name = "restriction" type = "string" minOccurs = "0"/>
      <element name = "address" type = "string" minOccurs = "0"/>
      <element name = "code" type = "string" minOccurs = "0" maxOccurs =
"unbounded"/>
      <element name = "note" type = "string" minOccurs = "0"/>
      <element name = "reference" minOccurs = "0">
        <simpleType>
         <list itemType = "string"/>
        </simpleType>
      </element>
      <element name = "incident" minOccurs = "0">
        <simpleType>
         <list itemType = "string"/>
        </simpleType>
      </element>
      <element name = "info" minOccurs = "0" maxOccurs = "unbounded">
        <complexType>
         <sequence>
           <element name = "language" type = "language" default = "en-US"
minOccurs = "0"/>
           <element name = "category" maxOccurs = "unbounded">
```

```
            <simpleType>
              <restriction base = "string">
                <enumeration value = "Geo"/>
                <enumeration value = "Met"/>
                <enumeration value = "Safety"/>
                <enumeration value = "Security"/>
                <enumeration value = "Rescue"/>
                <enumeration value = "Fire"/>
                <enumeration value = "Health"/>
                <enumeration value = "Env"/>
                <enumeration value = "Transport"/>
                <enumeration value = "Infra"/>
                <enumeration value = "Other"/>
              </restriction>
            </simpleType>
          </element>
          <element name = "event" type = "string"/>
          <element name = "urgency">
            <simpleType>
              <restriction base = "string">
                <enumeration value = "Immediate"/>
                <enumeration value = "Expected"/>
                <enumeration value = "Future"/>
                <enumeration value = "Past"/>
                <enumeration value = "Unknown"/>
              </restriction>
            </simpleType>
          </element>
          <element name = "severity">
            <simpleType>
              <restriction base = "string">
                <enumeration value = "Extreme"/>
                <enumeration value = "Severe"/>
                <enumeration value = "Moderate"/>
                <enumeration value = "Minor"/>
                <enumeration value = "Unknown"/>
              </restriction>
            </simpleType>
          </element>
          <element name = "certainty">
            <simpleType>
              <restriction base = "string">
                <enumeration value = "Very Likely"/>
                <enumeration value = "Likely"/>
                <enumeration value = "Possible"/>
                <enumeration value = "Unlikely"/>
                <enumeration value = "Unknown"/>
              </restriction>
            </simpleType>
          </element>
          <element name = "audience" type = "string" minOccurs = "0"/>
          <element name = "eventCode" type = "string" minOccurs = "0" maxOccurs
= "unbounded"/>
          <element name = "effective" type = "dateTime" minOccurs = "0"/>
          <element name = "onset" type = "dateTime" minOccurs = "0"/>
          <element name = "expires" type = "dateTime" minOccurs = "0"/>
          <element name = "senderName" type = "string" minOccurs = "0"/>
          <element name = "headline" type = "string" minOccurs = "0"/>
          <element name = "description" type = "string" minOccurs = "0"/>
          <element name = "instruction" type = "string" minOccurs = "0"/>
          <element name = "web" type = "anyURI" minOccurs = "0"/>
          <element name = "image" type = "anyURI" minOccurs = "0"/>
          <element name = "audio" type = "anyURI" minOccurs = "0"/>
          <element name = "contact" type = "string" minOccurs = "0"/>
          <element name = "parameter" type = "string" minOccurs = "0" maxOccurs
= "unbounded"/>
          <element name = "area" minOccurs = "0" maxOccurs = "unbounded">
            <complexType>
              <sequence>
                <element name = "areaDesc" type = "string"/>
```

```
                    <element name = "polygon" minOccurs = "0" maxOccurs =
"unbounded">
                      <simpleType>
                        <list itemType = "string"/>
                      </simpleType>
                    </element>
                    <element name = "circle" minOccurs = "0" maxOccurs = "unbounded">
                      <simpleType>
                        <list itemType = "string"/>
                      </simpleType>
                    </element>
                    <element name = "geocode" type = "string" minOccurs = "0"
maxOccurs = "unbounded"/>
                    <element name = "altitude" type = "string" minOccurs = "0"/>
                    <element name = "ceiling" type = "string" minOccurs = "0"/>
                  </sequence>
                </complexType>
              </element>
            </sequence>
          </complexType>
        </element>
      </sequence>
    </complexType>
  </element>
</schema>
```

Appendix A. CAP Alert Message Example

A.1. Homeland Security Advisory System Alert

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

```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns = "http://www.incident.com/cap/0.9”>
  <identifier>43b08071-3727</identifier>
  <sender>hsas@dhs.gov</sender>
  <sent>2003-04-02T14:39:01-05:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <info>
    <category>Security</category>
    <event>Homeland Security Advisory System Update</event>
    <urgency>Immediate</urgency>
    <severity>Severe</severity>
    <certainty>Likely</certainty>
    <senderName>U.S. Government, Department of Homeland Security</senderName>
    <headline>Homeland Security Sets Code ORANGE</headline>
    <description>The Department of Homeland Security has elevated the Homeland
Security Advisory System threat level to ORANGE / High in response to
intelligence which may indicate a heightened threat of terrorism.</description>
    <instruction> A High Condition is declared when there is a high risk of
terrorist attacks. In addition to the Protective Measures taken in the previous
Threat Conditions, Federal departments and agencies should consider agency-
specific Protective Measures in accordance with their existing
plans.</instruction>
    <web>http://www.dhs.gov/dhspublic/display?theme=29</web>
    <image>http://www.dhs.gov/dhspublic/getAdvisoryImage</image>
    <parameter>HSAS=ORANGE</parameter>
    <area>
      <areaDesc>U.S. nationwide and interests worldwide</areaDesc>
    </area>
  </info>
</alert>
```

A.2. Severe Thunderstorm Warning

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

```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns = "http://www.incident.com/cap/0.9”>
  <identifier>KSTO1055887203</identifier>
  <sender>KSTO@NWS.NOAA.GOV</sender>
  <sent>2003-06-17T14:57:00-07:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <info>
    <category>Met</category>
    <event>SEVERE THUNDERSTORM</event>
    <urgency>Immediate</urgency>
    <severity>Severe</severity>
    <certainty>Likely</certainty>
    <eventCode>SVRSTO</eventCode>
    <expires>2003-06-17T16:00:00-07:00</expires>
    <senderName>NATIONAL WEATHER SERVICE SACRAMENTO CA</senderName>
    <headline>SEVERE THUNDERSTORM WARNING</headline>
    <description> AT 254 PM PDT...NATIONAL WEATHER SERVICE DOPPLER RADAR
INDICATED A SEVERE THUNDERSTORM OVER SOUTH CENTRAL ALPINE COUNTY...OR ABOUT 18
MILES SOUTHEAST OF KIRKWOOD...MOVING SOUTHWEST AT 5 MPH. HAIL...INTENSE RAIN AND
STRONG DAMAGING WINDS ARE LIKELY WITH THIS STORM.</description>
    <instruction>TAKE COVER IN A SUBSTANTIAL SHELTER UNTIL THE STORM
PASSES.</instruction>
    <contact> BARUFFALDI/JUSKIE</contact>
    <area>
      <areaDesc>EXTREME NORTH CENTRAL TUOLUMNE COUNTY IN CALIFORNIA, EXTREME
NORTHEASTERN CALAVERAS COUNTY IN CALIFORNIA, SOUTHWESTERN ALPINE COUNTY IN
CALIFORNIA</areaDesc>
      <polygon>38.47,-120.14 38.34,-119.95 38.52,-119.74 38.62,-119.89</polygon>
    </area>
  </info>
</alert>
```

A.3. Earthquake Report

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

```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns = "http://www.incident.com/cap/0.9”>
  <identifier>TRI13970876.1</identifier>
  <sender>trinet@caltech.edu</sender>
  <sent>2003-06-11T20:56:00-07:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <incident>13970876</incident>
  <info>
    <category>Geo</category>
    <event>Earthquake</event>
    <urgency>Past</urgency>
    <severity>Minor</severity>
    <certainty>Highly Likely</certainty>
    <senderName>Southern California Seismic Network (TriNet) operated by Caltech
and USGS</senderName>
    <headline>EQ 3.4 Imperial County CA - PRELIMINARY REPORT</headline>
    <description>A minor earthquake measuring 3.4 on the Richter scale occurred
near Brawley, California at 8:53 PM Pacific Daylight Time on Wednesday, June 11,
2003. (This is a computer-generated solution and has not yet been reviewed by a
human.)</description>
    <web>http://www.trinet.org/scsn/scsn.html</web>
    <parameter>EventID=13970876</parameter>
    <parameter>Version=1</parameter>
    <parameter>Magnitude=3.4 Ml</parameter>
    <parameter>Depth=11.8 mi.</parameter>
    <parameter>Quality=Excellent</parameter>
    <area>
      <areaDesc>1 mi. WSW of Brawley, CA; 11 mi. N of El Centro, CA; 30 mi. E of
OCOTILLO (quarry); 1 mi. N of the Imperial Fault</areaDesc>
      <circle>32.9525,-115.5527 0</circle>
    </area>
  </info>
</alert>
```

A.4. AMBER Alert

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

```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns = "http://www.incident.com/cap/0.9”>
  <identifier>KAR0-0306112239-SW</identifier>
  <sender>KARO@CLETS.DOJ.CA.GOV</sender>
  <source>SW</source>
  <sent>2003-06-11T22:39:00-07:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <info>
    <category>Rescue</category>
    <event>Child Abduction</event>
    <urgency>Immediate</urgency>
    <severity>Severe</severity>
    <certainty>Likely</certainty>
    <senderName>LOS ANGELES POLICE DEPT - LAPD</senderName>
    <headline>AMBER ALERT</headline>
    <description>DATE/TIME: 06/11/03, 1915 HRS.  VICTIM(S): KHAYRI DOE JR. M/B
BLK/BRO 3'0", 40 LBS. LIGHT COMPLEXION.  DOB 06/24/01. WEARING RED SHORTS, WHITE
T-SHIRT, W/BLUE COLLAR.  LOCATION: 5721 DOE ST., LOS ANGELES, CA.  SUSPECT(S):
KHAYRI DOE SR. DOB 04/18/71 M/B, BLK HAIR, BRO EYE. VEHICLE: 81' BUICK 2-DR,
BLUE (4XXX000).</description>
    <contact>DET. SMITH, 77TH DIV, LOS ANGELES POLICE DEPT-LAPD AT 213 485-
2389</contact>
  </info>
</alert>
```

Appendix B. Acknowledgments

B.1. OASIS Emergency Management Technical Committee, Notification Methods and Messages Subcommittee

John Aerts, LA County Information Systems
Art Botterell, Partnership for Public Warning
Thomas Bui, The Boeing Company
Rick Carlton, e-Team
Eliot Christian, US Department of the Interior
Nasseam Elkarra
Jason Gilliam, Blue292
David Hall
Joyce Kern, Sungard Availability Services
Gary Ham, Disaster Management Interoperability Services
Bona Nasution, MTG Management Consultants
Brian Pattinson, Unisys
Walid Ramadan, Blue292
Dr. John Silva
Cathy Subatch,e-Team
Jerry Weltman, IEM
Allen Wyke, Blue292

B.2. Partnership for Public Warning

The Common Alerting Protocol was sponsored into the OASIS standards process by the Trustees of the Partnership for Public Warning, a national non-profit institute devoted to the enhancement and expansion of effective public warning systems in the U.S, and internationally. Their support is gratefully acknowledged.

B.3. Common Alerting Protocol Working Group

The initial design and demonstration of the Common Alerting Protocol Alert Message was performed by the Common Alerting Protocol Working Group, an ad-hoc committee of more than 130 emergency management and technology practitioners, including:

Rex Buddenberg, Naval Postgraduate School
Bill Butler, Los Angeles County Office of Emergency Management
Neil Briscombe, QinetiQ (Great Britain)
Kim Carsell, David Ford Consulting Engineers
Phillip S. Cogan, Bernstein Communications
Denis DesRosiers, CARIS-Universal Systems (Canada)
Brian Dopp, Phoenix Disaster Services
Darrell Ernst, The MITRE Corporation
John Fleming, Florida Emergency Management Agency
Kevin Farrell, Aberdeen Proving Ground
Lawrence C. Freudinger, NASA Dryden Flight Research Center
David Gillen, mobileFOUNDATIONS
Ben Green, California Office of Emergency Services
Patrick Halley, The ComCARE Alliance
Al Kenyon, Clear Channel Communications
Elizabeth Klute, Contra Costa County (CA) Community Warning System
Elden P. Laffoon, Sr., Midwest Computer Technical
Dave Luneau, Classco
Lois Clark McCoy, National Institute for Urban Search and Rescue
Michael McGuire, Oregon Department of Human Services
Peter B. Olinger, Lockheed Martin Space & Strategic Missiles
David Oppenheimer, United States Geological Survey
Rick Paige, Mendocino County (CA) Emergency Services Authority
Darryl Parker, TFT
Efraim Petel, HormannAmerica,
David E. Price, Lawrence Livermore National Laboratory
Valerie Quigley, Laurence Berkeley Laboratory
Bob Robinson, Business Recovery Managers Association
Don Root, California Office of Emergency Services
Ben Rotholtz, Real Networks
Richard Rudman, EAS Consultant
Van H. Schallenberg, Professional Engineer
Craig Schmidt, National Weather Service
Ingo Simonis, University of Muenster (Germany)
John Sokich, National Weather Service
Chris Warner, Earth911
Gram Wheeler, Microsoft
Kon Wilms, NDS Amerca

B.4. Additional Contributors

Kenneth Allen, Partnership for Public Warning
Peter Anderson, Simon Fraser University (Canada)
David Aylward, The ComCARE Alliance
Alan Beiagi, GeoDecisions
Ray Chadwick, Classco
Cliff Dice, Dice Corporation

Gary DuBrueler, Shenandoah County (VA) Emergency Management
Rich Eisner, California Office of Emergency Services
David Fowler, City and County of San Francisco
Daniel Gast, Orillion
Gan Wei Boon, Ministry of Home Affairs (Singapore)
Sol Glassner, The MITRE Corporation
Alan Jones, USGS
Joe Jumayao, Qualcomm
John Laye, Contingency Management Consultants
Dave Liebersbach, Alaska Emergency Management
Roland Lussier, ComLabs
Don Miller, Washington (state) Emergency Management
Kent Paxton, San Francisco Office of Emergency Services
Dr. Jack Potter, Winchester (VA) Medical Center
Tim Pozar, CSI Telecommunications
Tim Putprush, Federal Emergency Management Agency
Randy Schulley, California Office of Emergency Services
Alan Shoemaker, The MITRE Corporation
Dr. Peter Ward, Partnership for Public Warning
Herbert White, National Weather Service
George Whitney, California Office of Emergency Services
Tom Worden, California Office of Emergency Services

Appendix C. Revision History

Rev	Date	By Whom	What
0.9	2003-06-20	Art Botterell	Draft for Comment

Appendix D. Notices

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's procedures with respect to rights in OASIS specifications can be found at 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 implementors or users of this specification, can be obtained from the OASIS Executive Director.

OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to implement this specification. Please address the information to the OASIS Executive Director.

Based in part on prior work contributed by the Common Alerting Protocol Working group, copyright 2002-2003 Art Botterell for the Common Alerting Protocol Working Group.