International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1303

(09/2007)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

Common alerting protocol (CAP 1.1)

ITU-T Recommendation X.1303

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	**X.1000–**

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation X.1303

Common alerting protocol (CAP 1.1)

Summary

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. CAP also provides a template for effective warning messages based on best practices identified in academic research and real-world experience.

ITU-T Recommendation X.1303 also provides both an XSD specification and an equivalent ASN.1 specification (that permits a compact binary encoding) and allows the use of ASN.1 as well as XSD tools for the generation and processing of CAP messages. This Recommendation enables existing systems, such as H.323 systems, to more readily encode, transport and decode CAP messages.

Source

ITU-T Recommendation X.1303 was approved on 13 September 2007 by ITU-T Study Group 17 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

		Page
1	Scope	1
2	References	2
3	Definitions	3
4	Abbreviations and acronyms	3
5	Conventions	3
6	Design principles and concepts	3
	6.1 Design philosophy	3
	6.2 Examples of requirements for design	4
	6.3 Examples of use scenarios	4
7	Alert message structure	6
	7.1 Document object model	6
	7.2 Data dictionary	6
	7.3 Implementation considerations	17
	7.4 XML schema	18
8	Use of ASN.1 to specify and encode the CAP alert message	21
	8.1 General	21
	8.2 Formal mappings and specification	21
Appendix I – CAP alert message examples		27
	I.1 Homeland security advisory system alert	27
	I.2 Severe thunderstorm warning	28
	I.3 Earthquake report	29
	I.4 AMBER alert (Including EAS activation)	30
Bibliography		31

Introduction

Provides a brief introduction to the common alerting protocol (the current specification is identified as CAP 1.1).

Purpose

The common alerting protocol (CAP) provides an open, non-proprietary 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 and the ITU-T fast web services, as well as existing formats including the specific area message encoding (SAME) used for the United States' National Oceanic and Atmospheric Administration (NOAA) weather radio and the emergency alert system (EAS), while offering enhanced capabilities that include:

- flexible geographic targeting using latitude/longitude shapes and other geospatial representations in three dimensions;
- multilingual and multi-audience messaging;
- phased and delayed effective times and expirations;
- enhanced message update and cancellation features;
- template support for framing complete and effective warning messages;
- compatible with digital encryption and signature capability; and
- facility for digital images and audio.

CAP provides 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".

CAP 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 National Science and Technology Council (NSTC) report as a point of departure for the design of a common alerting protocol (CAP). Their draft went through several revisions and was tested in demonstrations and field trials in Virginia (supported by the ComCARE Alliance) and in California (in cooperation with the California Office of Emergency Services) during 2002 and 2003.

Geographic locations in CAP are defined using [b-WGS 84] (World Geodetic System 1984). CAP does not assign responsibilities for coordinate transformations from and to other Spatial Reference Systems. See clause 5, below, for the format of coordinate pairs within CAP elements.

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.

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. Under most circumstances, CAP messages with a <msgType> value of "Alert" should include at least one <info> element. (See the document object model diagram in clause 7.1, below.)

- **<alert>**

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

- **<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 an 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 or to provide the information in multiple languages.

- **<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.

- **<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.

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.

ITU-T Recommendation X.1303

Common alerting protocol (CAP 1.1)

1 Scope

This Recommendation defines the common alerting protocol (CAP) – version 1.1 – which 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 facilitates the detection of emerging patterns in local warnings of various kinds, such as might indicate an undetected hazard or hostile act. CAP provides a template for effective warning messages based on best practices identified in academic research and real-world experience.

The common alerting protocol (CAP) provides an open, non-proprietary digital message format for various types of alerts and notifications. CAP provides the following capabilities:

- flexible geographic targeting using latitude/longitude shapes and other geospatial representations in three dimensions;
- multilingual and multi-audience messaging;
- phased and delayed effective times and expirations;
- enhanced message update and cancellation features;
- template support for framing complete and effective warning messages;
- compatible with digital encryption and signature capability; and
- facility for digital images and audio.

CAP provides 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".

This Recommendation also provides both an XSD schema and an ASN.1 specification for the common alerting protocol.

NOTE – The ASN.1 specification defines the same message information content and XML encoding as that defined by the XSD schema, but permits a compact binary encoding and the use of ASN.1 as well as XSD tools for the generation and processing of CAP messages.

This Recommendation is technically equivalent to the OASIS Common Alerting Protocol v.1.1 with the Errata approved on 2 October 2007. This Recommendation defines the following:

1) structure of the CAP alert message;
2) design principles and concepts of CAP;
3) alert message structure;
4) XML and compact binary encodings of the message (using XSD for the XML encoding and the ASN.1 specification and its Encoding Rules for the XML – identical to the XSD specification – and the binary encodings);
5) conversion between compact binary and XML encodings of the message using ASN.1 Recommendations.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.680] ITU-T Recommendation X.680 (2002), *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

[ITU-T X.691] ITU-T Recommendation X.691 (2002), *Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)*.

[ITU-T X.693] ITU-T Recommendation X.693 (2001), *Information technology – ASN.1 encoding rules: XML Encoding Rules (XER)*.

[ITU-T X.694] ITU-T Recommendation X.694 (2004), *Information technology – ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1*.

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

[IETF RFC 2046] IETF RFC 2046 (1996), *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types*.

[IETF RFC 3066] IETF RFC 3066 (2001), *Tags for the Identification of Languages*.

[W3C Datatypes] *XML Schema Part 2: Data types Second Edition*, W3C Recommendation, Copyright © [28 October 2004] World Wide Web Consortium, (Massachusetts Institute of Technology, *Institut National de Recherche en Informatique et en Automatique*, Keio University), http://www.w3.org/TR/xmlschema-2/#dateTime.

[W3C Encryption] *XML Encryption Syntax and Processing*, W3C Recommendation, Copyright © [10 December 2002] World Wide Web Consortium, (Massachusetts Institute of Technology, *Institut National de Recherche en Informatique et en Automatique*, Keio University), http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/.

[W3C Namespaces] *Namespaces in XML*, W3C Recommendation, Copyright © [14 January 1999] World Wide Web Consortium (Massachusetts *Institut of Technology, Institut National de Recherche en Informatique et en Automatique*, Keio University), http://www.w3.org/TR/REC-xml-names/.

[W3C Signature] *XML-Signature Syntax and Processing*, W3C Recommendation, Copyright © [12 February 2002] World Wide Web Consortium, (Massachusetts Institute of Technology, *Institut National de Recherche en Informatique et en Automatique*, Keio University), http://www.w3.org/TR/xmldsigcore/.

[W3C XML] *Extensible Markup Language (XML) 1.0 (Third Edition)*, W3C Recommendation, Copyright © [4 February 2004] World Wide Web Consortium, (Massachusetts Institute of Technology, *Institut National de Recherche en Informatique et en Automatique*, Keio University), http://www.w3.org/TR/REC-xml/.

3 Definitions

This clause is intentionally left blank.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

ASN.1 Abstract Syntax Notation One

CAP Common Alerting Protocol

EAS Weather radio and the Emergency Alert System

MIME Multipurpose Internet Mail Extensions

SAME Specific Area Message Encoding

URI Uniform Resource Identifier

XML eXtensible Markup Language

XSD XML Schema Definition

5 Conventions

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

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

References to XML elements within the body of this Recommendation are in bold font.

6 Design principles and concepts

This clause is non-normative.

This clause provides a brief review of the design concepts and principles behind CAP.

6.1 Design philosophy

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

- Interoperability: First and foremost, the CAP Alert Message should provide a means for interoperable exchange of alerts and notifications among all kinds of emergency information systems.
- Completeness: The CAP Alert Message format should provide for all the elements of an effective public warning message.
- Simple implementation: The design should not place undue burdens of complexity on technical implementers.
- Simple XML (see [W3C XML], [W3C Namespaces], [W3C Datatypes]) and portable structure: Although the primary anticipated use of the CAP Alert Message is as an XML document or its binary equivalent, 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.

6.2 Examples of requirements for design

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

The common alerting protocol should:

- Provide a specification for a simple, extensible format for digital representation of warning messages and notifications;
- Enable integration of diverse sensor and dissemination systems;
- Be usable over multiple transmission systems, including TCP/IP-based networks and one-way "broadcast" channels and low-bandwidth communication;
- Support credible end-to-end authentication and validation of all messages;
- Provide a unique identifier (e.g., an ID number) for each warning message and for each message originator;
- Provide for multiple message types, such as:
  - warnings;
  - acknowledgements;
  - expirations and cancellations;
  - updates and amendments;
  - reports of results from dissemination systems;
  - administrative and system messages.
- Provide for multiple message types, such as:
  - geographic targeting;
  - level of urgency;
  - level of certainty;
  - level of threat severity.
- Provide a mechanism for referencing supplemental information (e.g., digital audio or image files, additional text);
- Use an established open-standard data representation;
- Be based on a program of real-world cross-platform testing and evaluation;
- Provide a clear basis for certification and further protocol evaluation and improvement; and
- Provide a clear logical structure that is relevant and clearly applicable to the needs of emergency response and public safety users and warning system operators.

6.3 Examples of use scenarios

This clause provides examples of use scenarios that were used as a basis for the design and review of the CAP Alert Message format.

NOTE – These scenarios are non-normative and not intended to be exhaustive or to reflect actual practices.

6.3.1 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."

6.3.2 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."

6.3.3 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.)."

6.3.4 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."

6.3.5 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., 6.3.3 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."

7 Alert message structure

This clause discusses CAP alert message structure.

7.1 Document object model

The CAP document object model is provided in Figure 7-1 below.

NOTE – In the figure below, elements in boldface are mandatory; elements in italics have default values that will be assumed if the element is not present; asterisks (*) indicate that multiple instances are permitted.

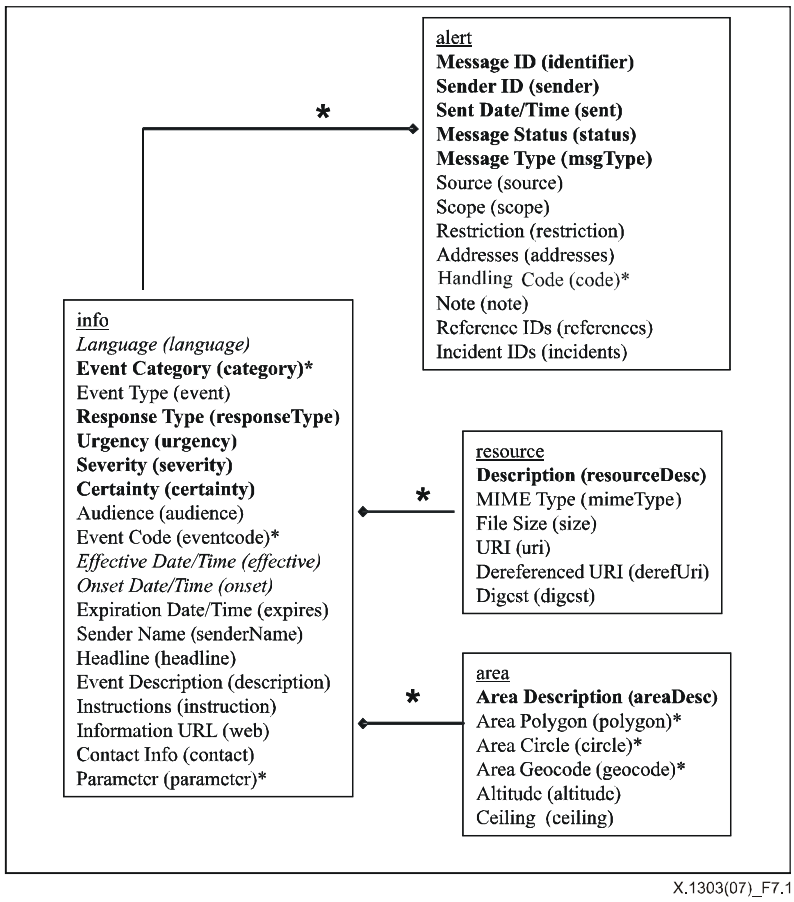

Figure 7-1 – Document object model

7.2 Data dictionary

This clause provides a description of the CAP data dictionary.

NOTE – Unless explicitly constrained within this Data Dictionary or the XML Schema (see [W3C XML] and clause 7.4), CAP elements may have null values. Implementers must check for this condition wherever it might affect application performance.

7.2.1 "alert" element and sub-elements

Table 7-1 provides a description of the "alert" element and sub-elements.

Table 7-1 – "alert" element and sub-elements

Element name	alert	**context.class.attribute.representation**	cap.alert.group
Definition	The container for all Component parts of the alert message		
Optionality	REQUIRED		
Notes	1) Surrounds CAP alert message sub-elements 2) Must include the xmlns attribute referencing the CAP URN as the namespace, e.g.: <cap:alert xmlns:cap="urn:oasis:names:tc:emerge ncy:cap:1.1"> [*sub-elements*] </cap:alert> 3) In addition to the specified sub-elements, may contain one or more <info> blocks.		

Element name	identifier	**context.class.attribute.representation**	cap.alert.identifier
Definition	The identifier of the alert message		
Optionality	REQUIRED		
Notes	1) A number or string uniquely identifying this message, assigned by the sender 2) Must not include spaces, commas or restricted characters (< and &)		

Element name	sender	**context.class.attribute.representation**	cap.alert.sender.identifier
Definition	The identifier of the sender of the alert message		
Optionality	REQUIRED		
Notes	1) Identifies the originator of this alert. Guaranteed by assigner to be unique globally; e.g., may be based on an Internet domain name 2) Must not include spaces, commas or restricted characters (< and &)		

Element name	sent	**context.class.attribute.representation**	cap.alert.sent.time
Definition	The time and date of the origination of the alert message		
Optionality	REQUIRED		
Notes	1) The date and time is represented in [dateTime] format (e.g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT). 2) Alphabetic timezone designators such as "Z" must not be used. The timezone for UTC must be represented as "–00:00" or "+00:00".		

Element name	status	**context.class.attribute.representation**	cap.alert.status.code
Definition	The code denoting the appropriate handling of the alert message		
Optionality	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.		

Table 7-1 – "alert" element and sub-elements

Element name	msgType	**context.class.attribute.representation**	cap.alert.type.code
Definition	The code denoting the nature of the alert message		
Optionality	REQUIRED		
Code Values	"Alert" – Initial information requiring attention by targeted recipients "Update" – Updates and supersedes 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>		

Element name	source	**context.class.attribute.representation**	cap.alert.source.identifier
Definition	The text identifying the source of the alert message		
Optionality	OPTIONAL		
Notes	The particular source of this alert; e.g., an operator or a specific device.		

Element name	scope	**context.class.attribute.representation**	cap.alert.scope.code
Definition	The code denoting the Intended distribution of the alert message		
Optionality	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 <address>, below)		

Element name	restriction	**context.class.attribute.representation**	cap.alert.restriction.text
Definition	The text describing the rule for limiting distribution of the restricted alert message		
Optionality	CONDITIONAL		
Notes	Used when <scope> value is "Restricted"		

Element name	addresses	**context.class.attribute.representation**	cap.alert.addresses.group
Definition	The group listing of Intended recipients of the private alert message		
Optionality	CONDITIONAL		
Notes	1) Used when <scope> value is "Private" 2) Each recipient shall be identified by an identifier or an address 3) Multiple space-delimited addresses may be included. Addresses including whitespace must be enclosed in double-quotes.		

Element name	code	**context.class.attribute.representation**	cap.alert.code
Definition	The code denoting the Special handling of the alert message		
Optionality	OPTIONAL		
Notes	1) Any user-defined flag or special code used to flag the alert message for special handling. 2) Multiple instances may occur within a single <info> block.		

Table 7-1 – "alert" element and sub-elements

Element name	note	**context.class.attribute.representation**	cap.alert.note.text
Definition	The text describing the purpose or significance of the alert message		
Optionality	OPTIONAL		
Notes	The message note is primarily intended for use with Cancel and Error alert message types.		

Element name	references	**context.class.attribute.representation**	cap.alert.references.group
Definition	The group listing Identifying earlier message(s) referenced by the alert message		
Optionality	OPTIONAL		
Notes	1) The extended message identifier(s) (in the form *sender, identifier, sent*) of an earlier CAP message or messages referenced by this one. 2) If multiple messages are referenced, they shall be separated by whitespace.		

Element name	incidents	**context.class.attribute.representation**	cap.alert.incidents.group
Definition	The group listing naming the referent incident(s) of the alert message		
Optionality	OPTIONAL		
Notes	1) Used to collate multiple messages referring to different aspects of the same incident 2) If multiple incident identifiers are referenced, they shall be separated by whitespace. Incident names including whitespace shall be surrounded by double-quotes		

7.2.2 "info" element and sub-elements

Table 7-2 provides a description of the "info" element and sub-elements.

Table 7-2 – "info" element and sub-elements

Element name	info	**context.class.attribute.representation**	cap.alertInfo.info.group
Definition	The container for all component parts of the info sub-element of the alert message		
Optionality	OPTIONAL		
Notes	1) Multiple occurrences are permitted within a single <alert>. If targeting of multiple "info" blocks in the same language overlaps, information in later blocks may expand but may not override the corresponding values in earlier ones. Each set of "info" blocks containing the same language identifier shall be treated as a separate sequence. 2) In addition to the specified sub-elements, may contain one or more <resource> blocks and/or one or more <area> blocks.		

Element name	language	**context.class.attribute.representation**	cap.alertInfo.language.code
Definition	The code denoting the language of the info sub-element of the alert message		
Optionality	OPTIONAL		
Notes	1) Code Values: Natural language identifier per [IETF RFC 3066]. 2) If not present, an implicit default value of "en-US" shall be assumed. 3) A null value in this element shall be considered equivalent to "en-US."		

Table 7-2 – "info" element and sub-elements

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

Element name	event	**context.class.attribute.representation**	cap.alertInfo.event.text
Definition	The text denoting the type of the subject event of the alert message		
Optionality	REQUIRED		

Element name	responseType	**context.class.attribute.representation**	cap.alertInfo.responseType.code
Definition	The code denoting the type of action recommended for the target audience		
Optionality	OPTIONAL		
Notes	1) Code Values: "Shelter" – Take shelter in place or per <instruction> "Evacuate" – Relocate as instructed in the <instruction> "Prepare" – Make preparations per the <instruction> "Execute" – Execute a pre-planned activity identified in <instruction> "Monitor" – Attend to information sources as described in <instruction> "Assess" – Evaluate the information in this message. (This value should NOT be used in public warning applications.) "None" – No action recommended 2) Multiple instances may occur within a single <info> block.		

Table 7-2 – "info" element and sub-elements

Element name	urgency	**context.class.attribute.representation**	cap.alertInfo.urgency.code
Definition	The code denoting the urgency of the subject event of the alert message		
Optionality	REQUIRED		
Notes	1) The "urgency", "severity", and "certainty" elements collectively distinguish less emphatic from more emphatic messages. 2) Code Values: "Immediate" – Responsive action should be taken immediately "Expected" – Responsive action should be taken soon (within next hour) "Future" – Responsive action should be taken in the near future "Past" – Responsive action is no longer required "Unknown" – Urgency not known		

Element name	severity	**context.class.attribute.representation**	cap.alertInfo.severity.code
Definition	The code denoting the severity of the subject event of the alert message		
Optionality	REQUIRED		
Notes	1) The "urgency", "severity", and "certainty" elements collectively distinguish less emphatic from more emphatic messages. 2) Code Values: "Extreme" – Extraordinary threat to life or property "Severe" – Significant threat to life or property "Moderate" – Possible threat to life or property "Minor" – Minimal threat to life or property "Unknown" – Severity unknown		

Element name	certainty	**context.class.attribute.representation**	cap.alertInfo.certainty.code
Definition	The code denoting the certainty of the subject event of the alert message		
Optionality	REQUIRED		
Notes	1) The "urgency", "severity", and "certainty" elements collectively distinguish less emphatic from more emphatic messages. 2) Code Values: "Observed" – Determined to have occurred or to be ongoing. "Likely" – Likely ($p > \sim 50\%$) "Possible" – Possible but not likely ($p \leq \sim 50\%$) "Unlikely" – Not expected to occur ($p \sim 0$) "Unknown" – Certainty unknown 3) For backward compatibility with CAP 1.0, the deprecated value of "Very Likely" should be treated as equivalent to "Likely".		

Table 7-2 – "info" element and sub-elements

Element name	audience	**context.class.attribute.representation**	cap.alertInfo.audience.text
Definition	The text describing the intended audience of the alert message		
Optionality	OPTIONAL		
Notes			

Element name	eventCode	**context.class.attribute.representation**	cap.alertInfo.event.code
Definition	A system-specific code identifying the event type of the alert message		
Optionality	OPTIONAL		
Notes	1) Any system-specific code for event typing, in the form: <eventCode> <valueName>valueName</valueName> <value>value</value> </eventCode> where the content of "valueName" is a user-assigned string designating the domain of the code, and the content of "value" is a string (which may represent a number) denoting the value itself (e.g., valueName ="SAME" and value="CEM"). 2) Values of "valueName" that are acronyms should be represented in all capital letters without periods (e.g., SAME, FIPS, ZIP). 3) Multiple instances may occur within a single <info> block.		

Element name	effective	**context.class.attribute.representation**	cap.alertInfo.effective.time
Definition	The effective time of the information of the alert message		
Optionality	OPTIONAL		
Notes	1) The date and time is represented in [dateTime] format (e.g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT). 2) Alphabetic timezone designators such as "Z" must not be used. The timezone for UTC must be represented as "–00:00" or "+00:00". 3) If this item is not included, the effective time shall be assumed to be the same as in <sent>.		

Element name	onset	**context.class.attribute.representation**	cap.alertInfo.onset.time
Definition	The expected time of the beginning of the subject event of the alert message		
Optionality	OPTIONAL		
Notes	1) The date and time is represented in [dateTime] format (e.g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT). 2) Alphabetic timezone designators such as "Z" must not be used. The timezone for UTC must be represented as "–00:00" or "+00:00".		

Table 7-2 – "info" element and sub-elements

Element name	expires	**context.class.attribute.representation**	cap.alertInfo.expires.time
Definition	The expiry time of the information of the alert message		
Optionality	OPTIONAL		
Notes	1) The date and time is represented in [dateTime] format (e.g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT). 2) Alphabetic timezone designators such as "Z" must not be used. The timezone for UTC must be represented as "–00:00" or "+00:00". 3) If this item is not provided, each recipient is free to set its own policy as to when the message is no longer in effect.		

Element name	senderName	**context.class.attribute.representation**	cap.alertInfo.sender.name
Definition	The text naming the originator of the alert message		
Optionality	OPTIONAL		
Notes	The human-readable name of the agency or authority issuing this alert.		

Element name	headline	**context.class.attribute.representation**	cap.alertInfo.headline.text
Definition	The text headline of the alert message		
Optionality	OPTIONAL		
Notes	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.		

Element name	description	**context.class.attribute.representation**	cap.alertInfo.description.text
Definition	The text describing the subject event of the alert message		
Optionality	OPTIONAL		
Notes	An extended human readable description of the hazard or event that occasioned this message.		

Element name	instruction	**context.class.attribute.representation**	cap.alertInfo.instruction.text
Definition	The text describing the recommended action to be taken by recipients of the alert message		
Optionality	OPTIONAL		
Notes	An extended human readable instruction to targeted recipients. (If different instructions are intended for different recipients, they should be represented by use of multiple <info> blocks.)		

Element name	web	**context.class.attribute.representation**	cap.alertInfo.information.identifier
Definition	The identifier of the hyperlink associating additional information with the alert message		
Optionality	OPTIONAL		
Notes	A full, absolute URI for an HTML page or other text resource with additional or reference information regarding this alert.		

Table 7-2 – "info" element and sub-elements

Element name	contact	**context.class.attribute.representation**	cap.alertInfo.contact.text
Definition	The text describing the contact for follow-up and confirmation of the alert message		
Optionality	OPTIONAL		
Notes			

Element name	parameter	**context.class.attribute.representation**	cap.alertInfo.parameter. group
Definition	A system-specific additional parameter associated with the alert message		
Optionality	OPTIONAL		
Notes	1) Any system-specific datum, in the form: <parameter> <valueName>*valueName*</valueName> <value>*value*</value> </parameter> where the content of "valueName" is a user-assigned string designating the domain of the code, and the content of "value" is a string (which may represent a number) denoting the value itself (e.g., valueName="SAME" and value="CIV".) 2) Values of "valueName" that are acronyms should be represented in all capital letters without periods (e.g., SAME, FIPS, ZIP). 3) Multiple instances may occur within a single <info> block.		

7.2.3 "resource" element and sub-elements

Table 7-3 provides a description of the "resource" element and sub-elements.

Table 7-3 – "resource" element and sub-elements

Element name	resource	**context.class.attribute.representation**	cap.alertInfoResource. resource.group
Definition	The container for all Component parts of the resource sub-element of the info sub-element of the alert element		
Optionality	OPTIONAL		
Notes	1) Refers to an additional file with supplemental information related to this <info> element; e.g., an image or audio file 2) Multiple occurrences may occur within a single <info> block		

Element name	resourceDesc	**context.class.attribute.representation**	cap.alertInfoResource. resourceDesc.text
Definition	The text describing the type and content of the resource file		
Optionality	REQUIRED		
Notes	The human-readable text describing the content and kind, such as "map" or "photo", of the resource file.		

Table 7-3 – "resource" element and sub-elements

Element name	mimeType	**context.class.attribute.representation**	cap.alertInfoResource.mimeType.identifier
Definition	The identifier of the MIME content type and sub-type describing the resource file		
Optionality	OPTIONAL		
Notes	MIME content type and sub-type as described in [IETF RFC 2046]. (As of the publication of this Recommendation the current IANA registered MIME types are listed at: http://www.iana.org/assignments/mediatypes/)		

Element name	size	**context.class.attribute.representation**	cap.alertInfoResource.size.integer
Definition	The integer indicating the size of the resource file		
Optionality	OPTIONAL		
Notes	Approximate size of the resource file in bytes.		

Element name	uri	**context.class.attribute.representation**	cap.alertInfoResource.uri.identifier
Definition	The identifier of the hyperlink for the resource file		
Optionality	OPTIONAL		
Notes	A full absolute URI, typically a Uniform Resource Locator that can be used to retrieve the resource over the Internet OR a relative URI to name the content of a <derefUri> element if one is present in this resource block.		

Element name	derefUri	**context.class.attribute.representation**	cap.alertInfoResource.derefUri.data
Definition	The base-64 encoded data content of the resource file		
Optionality	CONDITIONAL		
Notes	1) May be used either with or instead of the <uri> element in messages transmitted over one-way (e.g., broadcast) data links where retrieval of a resource via a URI is not feasible. 2) Clients intended for use with one-way data links must support this element. 3) This element must not be used unless the sender is certain that all direct clients are capable of processing it. 4) If messages including this element are forwarded onto a two-way network, the forwarder must strip the <derefUri> element and should extract the file contents and provide a <uri> link to a retrievable version of the file. 5) Providers of one-way data links may enforce additional restrictions on the use of this element, including message-size limits and restrictions regarding file types.		

Table 7-3 – "resource" element and sub-elements

Element name	digest	**context.class.attribute.representation**	cap.alertInfoResource. digest.code
Definition	The code representing the digital digest ("hash") computed from the resource file		
Optionality	OPTIONAL		
Notes	Calculated using the secure hash algorithm (SHA-1) per [FIPS 180-2] NOTE – It should be noted that NIST is encouraging the use of SHA-256 as a more secure alternative to SHA-1.		

7.2.4 "area" element and sub-elements

Table 7-4 provides a description of the "area" element and sub-elements.

Table 7-4 – "area" element and sub-elements

Element name	area	**context.class.attribute.representation**	cap.alertInfoArea.area. group
Definition	The container for all component parts of the area sub-element of the info sub-element of the alert message		
Optionality	OPTIONAL		
Notes			

Element name	areaDesc	**context.class.attribute.representation**	cap.alertInfoArea.area.text
Definition	The text describing the affected area of the alert message		
Optionality	REQUIRED		
Notes	A text description of the affected area.		

Element name	polygon	**context.class.attribute.representation**	cap.alertInfoArea.polygon. group
Definition	The paired values of points defining a polygon that delineates the affected area of the alert message		
Optionality	OPTIONAL		
Notes	1) Code Values: The geographic polygon is represented by a whitespace-delimited list of coordinate pairs. 2) The first and last pairs of coordinates must be the same. 3) Multiple instances may occur within an <area>.		

Element name	circle	**context.class.attribute.representation**	cap.alertInfoArea.circle. group
Definition	The paired values of a point and radius delineating the affected area of the alert message		
Optionality	OPTIONAL		
Notes	1) Code Values: The circular area is represented by a central point given as a coordinates pair followed by a space character and a radius value in kilometres. NOTE – Per the [b-WGS 84] datum. 2) Multiple instances may occur within an <area>.		

Table 7-4 – "area" element and sub-elements

Element name	geocode	**context.class.attribute.representation**	cap.alertInfoArea.geocode.code
Definition	The geographic code delineating the affected area of the alert message		
Optionality	OPTIONAL		
Notes	1) Any geographically-based code to describe message target area: <parameter> <valueName>valueName</valueName> <value>value</value> </parameter> where the content of "valueName" is a user-assigned string designating the domain of the code, and the content of "value" is a string (which may represent a number) denoting the value itself (e.g., valueName ="SAME" and value="006113"). 2) Values of "valueName" that are acronyms should be represented in all capital letters without periods (e.g., SAME, FIPS, ZIP). 3) Multiple instances may occur within a single <info> block. 4) This element is primarily for compatibility with other systems. Use of this element presumes knowledge of the coding system on the part of recipients; therefore, for interoperability, it should be used in concert with an equivalent description in the more universally understood <polygon> and <circle> forms whenever possible.		

Element name	altitude	**context.class.attribute.representation**	cap.alertInfoArea.altitude.quantity
Definition	The specific or minimum altitude of the affected area of the alert message		
Optionality	OPTIONAL		
Notes	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. NOTE – Per the [b-WGS 84] datum.		

Element name	ceiling	**context.class.attribute.representation**	cap.alertInfoArea.ceiling.quantity
Definition	The maximum altitude of the affected area of the alert message		
Optionality	CONDITIONAL		
Notes	1) Must not be used except in combination with the <altitude> element 2) The ceiling measure is in feet above mean sea level. NOTE – Per the [b-WGS 84] datum.		

7.3 Implementation considerations

This clause defines some insights into CAP implementations.

7.3.1 Security

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.

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

7.3.2 Digital signatures

The alert element of a CAP Alert Message may have an Enveloped Signature, as described by XML-Signature and Syntax Processing (see [W3C Signature]). Other XML signature mechanisms must not be used in CAP Alert Messages.

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

In other words, the presence of an element with the namespace URI (see [W3C Signature]) and a local name of "Signature" as a child of the alert element must not cause a processor to fail merely because of its presence.

7.3.3 Encryption

The alert element of a CAP Alert Message may be encrypted, using the mechanisms described by XML Encryption Syntax and Processing (see [W3C Encryption]). Other XML encryption mechanisms must not be used in CAP Alert Messages; however, transport-layer encryption mechanisms may be used independently of this requirement.

7.4 XML schema

```
<?xml version = "1.0" encoding = "UTF-8"?>
<schema xmlns = "http://www.w3.org/2001/XMLSchema"
   targetNamespace = "urn:oasis:names:tc:emergency:cap:1.1"
   xmlns:cap = "urn:oasis:names:tc:emergency:cap:1.1"
   xmlns:xs = "http://www.w3.org/2001/XMLSchema"
   elementFormDefault = "qualified"
   attributeFormDefault = "unqualified">
  <element name = "alert">
    <annotation>
      <documentation>CAP Alert Message (version 1.1)</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"/>
              <enumeration value = "Draft"/>
            </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 = "source" type = "string" minOccurs = "0"/>
<element name = "scope">
  <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 = "addresses" type = "string" minOccurs = "0"/>
<element name = "code" type = "string" minOccurs = "0"
        maxOccurs = "unbounded"/>
<element name = "note" type = "string" minOccurs = "0"/>
<element name = "references" type = "string" minOccurs = "0"/>
<element name = "incidents" type = "string" minOccurs = "0"/>
<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 = "CBRNE"/>
            <enumeration value = "Other"/>
          </restriction>
        </simpleType>
      </element>
      <element name = "event" type = "string"/>
      <element name = "responseType" minOccurs = "0"
           maxOccurs = "unbounded">
        <simpleType>
          <restriction base = "string">
            <enumeration value = "Shelter"/>
            <enumeration value = "Evacuate"/>
            <enumeration value = "Prepare"/>
            <enumeration value = "Execute"/>
            <enumeration value = "Monitor"/>
            <enumeration value = "Assess"/>
            <enumeration value = "None"/>
          </restriction>
        </simpleType>
      </element>
      <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 = "Observed"/>
      <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" minOccurs = "0"
          maxOccurs = "unbounded">
  <complexType>
    <sequence>
      <element ref = "cap:valueName"/>
      <element ref = "cap:value"/>
    </sequence>
  </complexType>
</element>
<element name = "effective" type = "dateTime" form = "qualified"
     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 = "contact" type = "string" minOccurs = "0"/>
<element name = "parameter" minOccurs = "0"
          maxOccurs = "unbounded">
  <complexType>
    <sequence>
      <element ref = "cap:valueName"/>
      <element ref = "cap:value"/>
    </sequence>
  </complexType>
</element>
<element name = "resource" minOccurs = "0"
          maxOccurs = "unbounded">
  <complexType>
    <sequence>
```

```
                    <element name = "resourceDesc" type = "string"/>
                    <element name = "mimeType" type = "string" minOccurs = "0"/>
                    <element name = "size" type = "integer" minOccurs = "0"/>
                    <element name = "uri" type = "anyURI" minOccurs = "0"/>
                    <element name = "derefUri" type = "string" minOccurs = "0"/>
                    <element name = "digest" type = "string" minOccurs = "0"/>
                  </sequence>
                </complexType>
              </element>
              <element name = "area" minOccurs = "0" maxOccurs = "unbounded">
                <complexType>
                  <sequence>
                    <element name = "areaDesc" type = "string"/>
                    <element name = "polygon" type = "string" minOccurs = "0"
maxOccurs = "unbounded"/>
                    <element name = "circle" type = "string" minOccurs = "0"
maxOccurs = "unbounded"/>
                    <element name = "geocode" minOccurs = "0"
                        maxOccurs = "unbounded">
                      <complexType>
                        <sequence>
                          <element ref = "cap:valueName"/>
                          <element ref = "cap:value"/>
                        </sequence>
                      </complexType>
                    </element>
                    <element name = "altitude" type = "string" minOccurs = "0"/>
                    <element name = "ceiling" type = "string" minOccurs = "0"/>
                  </sequence>
                </complexType>
              </element>
            </sequence>
          </complexType>
        </element>
      </sequence>
    </complexType>
  </element>
  <element name = "valueName" type = "string"/>
  <element name = "value" type = "string"/>
</schema>
```

8 Use of ASN.1 to specify and encode the CAP alert message

This clause provides the ASN.1 specification of the CAP alert message.

8.1 General

The ASN.1 specification (see [ITU-T X.680]) in clause 8.3 provides an alternative formulation of the XML schema defined in clause 7.4. If the ASN.1 Extended XML Encoding Rules (see [ITU-T X.693]) are applied to this ASN.1 schema, the permitted XML is identical to that supported by the XML schema in clause 7.4. If the ASN.1 Unaligned Packed Encoding Rules (see [ITU-T X.691]) are applied to it, the resulting binary encodings are more compact than the corresponding XML encodings.

8.2 Formal mappings and specification

The normative specification of the compact binary encoding is in clause 8.3 with the application of the ASN.1 Unaligned Packed Encoding Rules (see [ITU-T X.691]).

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

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

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

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

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

8.3 ASN.1 module

```
CAP-1-1 {itu-t recommendation x cap(1303) version1-1(1)}
DEFINITIONS XER INSTRUCTIONS AUTOMATIC TAGS ::=
-- CAP Alert Message (version 1.1)
BEGIN
-- References in comments to clauses outside this module refer to
-- ITU-T Recommendation X.1303 (09/2007).
-- This ASN.1 module is also included in OASIS CAP v1.1 Errata
-- (approved on 2 October 2007), and the references there are to
-- clauses 3.2.x as in OASIS CAP v1.1 and not clauses 7.2.x as
-- in ITU-T X.1303
Alert ::= SEQUENCE {
   identifier IdentifierString,
         -- Unambiguous identification of the message
       -- from all messages from
         -- this sender, in a format defined by the sender and
       -- identified in the "sender" field below.
   sender     String,
         -- The globally unambiguous identification of the sender.
         -- This specification does not define the root of
       -- a global identification tree (there is no international
       -- agreement on such a root), so it relies
         -- on human-readable text to define globally and
       -- unambiguously the sender.
         -- An internet domain name or use of "iri:/ITU-T/..."
       -- is possible, but
         -- the choice needs to be clearly stated in human-readable form.
   sent       DateTime,
   status     AlertStatus,
   msgType    AlertMessageType,
   source     String OPTIONAL,
         -- Not standardized human-readable identification
      -- of the source of the alert.
   scope      AlertScope,
   restriction String OPTIONAL,
         -- Not standardized human-readable restrictions
       -- on the distribution of the alert message
   addresses   String OPTIONAL,
         -- A space separated list of addresses for private messages
         -- (see 7.2.1)
   code-list   SEQUENCE SIZE((0..MAX)) OF code String,
         -- A sequence codes for special handling
      -- (see 7.2.1)
         -- The format and semantics of the codes are not defined in this
         -- specification.
   note        String OPTIONAL,
         -- Not standardized human-readable clarifying text for the alert
         -- (see 7.2.1)
```

```
   references  String OPTIONAL,
         -- Space-separated references to earlier messages
     -- (see 7.2.1)
   incidents   String OPTIONAL,
         -- Space-separated references to related incidents
     -- (see 7.2.1)
   info-list   SEQUENCE SIZE((0..MAX)) OF info AlertInformation  }

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

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

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

AlertInformation ::= SEQUENCE {
   language          Language -- DEFAULT "en-US" -- ,
         -- The language used in this value of the Info type
     -- (see 7.2.2)
   category-list     SEQUENCE (SIZE(1..MAX)) OF
                     category InformationCategory,
   event             String,
         -- Not standardized human-readable text describing the
       -- type of the event (see 7.2.2)
   responseType-list SEQUENCE SIZE((0..MAX)) OF
                     responseType InformationResponseType,
   urgency           HowUrgent,
   severity          HowSevere,
   certainty         HowCertain,
   audience          String OPTIONAL,
         -- Not standardized human-readable text describing the
       -- intended audience for the message (see 7.2.2)
   eventCode-list    SEQUENCE SIZE((0..MAX)) OF eventCode SEQUENCE {
          valueName ValueName,
          value     Value },
   effective         DateTime OPTIONAL,
   onset             DateTime OPTIONAL,
   expires           DateTime OPTIONAL,
   senderName        String OPTIONAL,
         -- Not standardized human-readable name of the authority
       -- issuing the message (see 7.2.2)
   headline          String (SIZE (1..160,...)) OPTIONAL,
         -- Not standardized human-readable short statement (headline)
       -- of the alert (see 7.2.2)
   description       String OPTIONAL,
         -- Not standardized human-readable extended description of
       -- the event (see 7.2.2)
   instruction       String OPTIONAL,
         -- Not standardized human-readable recommended action
     -- (see 7.2.2)
   web               AnyURI OPTIONAL,
   contact           String OPTIONAL,
```

```
        -- Not standardized human-readable contact details for
       -- follow-up (see 7.2.2)
   parameter-list    SEQUENCE SIZE((0..MAX)) OF parameter SEQUENCE {
         -- System-specific parameters (see 7.2.2)
         valueName ValueName,
         value     Value },
   resource-list     SEQUENCE SIZE((0..MAX)) OF resource ResourceFile,
   area-list         SEQUENCE SIZE((0..MAX)) OF Area }

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

InformationResponseType ::= ENUMERATED {
        assess,
        evacuate,
        execute,
        monitor,
        none,
        prepare,
        shelter }

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

HowSevere ::= ENUMERATED {
        extreme,
        minor,
        moderate,
        severe,
        unknown }

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

ResourceFile ::= SEQUENCE {
         -- Information about an associated resource file
     -- (see 7.2.3)
   resourceDesc String,
         -- Not standardized human-readable description of the type
       -- and content of
         -- an associated resource file (for example a map or
       -- photograph)(see 7.2.3)
   mimeType     String OPTIONAL,
   size         INTEGER OPTIONAL, -- In bytes
   uri          AnyURI OPTIONAL,
```

```
   derefUri     String OPTIONAL,
         -- An alternative to the URI giving the Base64-encoded
        -- content of the resource file (see 7.2.3)
   digest       String OPTIONAL
         -- SHA-1 hash of the resource file for error detection
      -- (see 7.2.3) -- }

Area ::= SEQUENCE {
         -- Identification of an affected area
   areaDesc     String,
         -- Not standardized human-readable description of the area
   polygon-list SEQUENCE OF polygon String,
         -- Each element is a space-separated list of coordinate pairs
         -- The complete list starts and ends with the same point and
         -- defines the polygon that defines the area
         -- (see 7.2.4).
   circle-list  SEQUENCE OF circle String,
         -- A space-separated list of coordinates for a point and a radius
   geocode-list SEQUENCE SIZE((0..MAX)) OF geocode SEQUENCE {
         -- A geographic code designating the alert target area
         -- (see 7.2.4)
             valueName ValueName,
             value     Value },
   altitude     String OPTIONAL,
         -- Specific or minimum altitude of the affected area
   ceiling      String OPTIONAL
         -- Maximum altitude of the affected area -- }

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

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

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

StringChar ::= String (SIZE(1))

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

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

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

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

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

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

ENCODING-CONTROL XER
    GLOBAL-DEFAULTS MODIFIED-ENCODINGS
    GLOBAL-DEFAULTS CONTROL-NAMESPACE
        "http://www.w3.org/2001/XMLSchema-instance" PREFIX "xsi"
    NAMESPACE ALL, ALL IN ALL AS "urn:oasis:names:tc:emergency:cap:1.1"
              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
```

Appendix I

CAP alert message examples

(This appendix does not form an integral part of this Recommendation)

I.1 Homeland security advisory system alert

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

```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns = "urn:oasis:names:tc:emergency:cap:1.1">
<identifier>43b080713727</identifier>
<sender>hsas@dhs.gov</sender>
<sent>2003-04-02T14:39:01-05:00</sent>
<status>Actual</status>
<msgType>Alert</msgType>
<scope>Public</scope>
     <info>
          <category>Security</category>
          <event>Homeland Security Advisory System Update</event>
          <urgency>Immediate</urgency>
          <severity>Severe</severity>
          <certainty>Likely</certainty>
          <senderName>U.S. Government, Department of Homeland
Security</senderName>
          <headline>Homeland Security Sets Code ORANGE</headline>
          <description>The Department of Homeland Security has elevated the
          Homeland Security Advisory
          System threat level to ORANGE / High in response to intelligence which
          may indicate a heightened
          threat of terrorism.</description>
          <instruction> A High Condition is declared when there is a high risk
          of terrorist attacks. In
          addition to the Protective Measures taken in the previous Threat
          Conditions, Federal departments
          and agencies should consider agency-specific Protective Measures in
          accordance with their
          existing plans.</instruction>
          <web>http://www.dhs.gov/dhspublic/display?theme=29</web>
               <parameter>
                    <valueName>HSAS</valueName>
                    <value>ORANGE</value>
               </parameter>
     <resource>
          <resourceDesc>Image file (GIF)</resourceDesc>
          <uri>http://www.dhs.gov/dhspublic/getAdvisoryImage</uri>
     </resource>
     <area>
          <areaDesc>U.S. nationwide and interests worldwide</areaDesc>
     </area>
</info>
</alert>
```

I.2 Severe thunderstorm warning

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

```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns = "urn:oasis:names:tc:emergency:cap:1.1">
<identifier>KSTO1055887203</identifier>
<sender>KSTO@NWS.NOAA.GOV</sender>
<sent>2003-06-17T14:57:00-07:00</sent>
<status>Actual</status>
<msgType>Alert</msgType>
<scope>Public</scope>
<info>
     <category>Met</category>
     <event>SEVERE THUNDERSTORM</event>
     <responseType>Shelter</responseType>
     <urgency>Immediate</urgency>
     <severity>Severe</severity>
     <certainty>Observed</certainty>
     <eventCode>
          <valueName>same</valueName>
          <value>SVR</value>
     </eventCode>
     <expires>2003-06-17T16:00:00-07:00</expires>
     <senderName>NATIONAL WEATHER SERVICE SACRAMENTO CA</senderName>
     <headline>SEVERE THUNDERSTORM WARNING</headline>
<description> AT 254 PM PDT...NATIONAL WEATHER SERVICE DOPPLER RADAR INDICATED
A SEVERE THUNDERSTORM OVER SOUTH CENTRAL ALPINE COUNTY...OR ABOUT 18 MILES
SOUTHEAST OF KIRKWOOD...MOVING
SOUTHWEST AT 5 MPH. HAIL...INTENSE RAIN AND STRONG DAMAGING WINDS ARE LIKELY
WITH THIS STORM.</description>
     <instruction>TAKE COVER IN A SUBSTANTIAL SHELTER UNTIL THE STORM
PASSES.</instruction>
     <contact>BARUFFALDI/JUSKIE</contact>
     <area>
     <areaDesc>EXTREME NORTH CENTRAL TUOLUMNE COUNTY IN CALIFORNIA, EXTREME
NORTHEASTERN CALAVERAS COUNTY IN CALIFORNIA, SOUTHWESTERN ALPINE COUNTY IN
CALIFORNIA</areaDesc>
     <polygon>38.47,-120.14 38.34,-119.95 38.52,-119.74 38.62,-119.89 38.47,-
120.14</polygon>
     <geocode>
          <valueName>FIPS6</valueName>
          <value>006109</value>
     </geocode>
     <geocode>
          <valueName>FIPS6</valueName>
          <value>006009</value>
     </geocode>
     <geocode>
          <valueName>FIPS6</valueName>
          <value>006003</value>
     </geocode>
     </area>
</info>
</alert>
```

I.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 = "urn:oasis:names:tc:emergency:cap:1.1">
<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>
<incidents>13970876</incidents>
     <info>
          <category>Geo</category>
          <event>Earthquake</event>
          <urgency>Past</urgency>
          <severity>Minor</severity>
          <certainty>Observed</certainty>
          <senderName>Southern California Seismic Network (TriNet) operated by
               Caltech and
          USGS</senderName>
          <headline>EQ 3.4 Imperial County CA - 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>
                    <valueName>EventID</valueName>
                    <value>13970876</value>
               </parameter>
          <parameter>
               <valueName>Version</valueName>
               <value>1</value>
          </parameter>
     <parameter>
          <valueName>Magnitude</valueName>
          <value>3.4 Ml</value>
     </parameter>
     <parameter>
          <valueName>Depth</valueName>
          <value>11.8 mi.</value>
     </parameter>
     <parameter>
          <valueName>Quality</valueName>
          <value>Excellent</value>
     </parameter>
     <area>
          <areaDesc>1 mi. WSW of Brawley, CA; 11 mi. N of El Centro, CA; 30 mi.
               E of OCOTILLO
          (quarry); 1 mi. N of the Imperial Fault</areaDesc>
          <circle>32.9525,-115.5527 0</circle>
     </area>
     </info>
</alert>
```

I.4 AMBER alert (Including EAS activation)

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

```
<?xml version = "1.0" encoding = "UTF-8"?>
<alert xmlns = "urn:oasis:names:tc:emergency:cap:1.1">
<identifier>KAR0-0306112239-SW</identifier>
<sender>KARO@CLETS.DOJ.CA.GOV</sender>
<sent>2003-06-11T22:39:00-07:00</sent>
<status>Actual</status>
<msgType>Alert</msgType>
<source>SW</source>
<scope>Public</scope>
     <info>
          <category>Rescue</category>
          <event>Child Abduction</event>
          <urgency>Immediate</urgency>
          <severity>Severe</severity>
          <certainty>Likely</certainty>
          <eventCode>
               <valueName>SAME</valueName>
               <value>CAE</value>
          </eventCode>
     <senderName>LOS ANGELES POLICE DEPT - LAPD</senderName>
     <headline>AMBER ALERT</headline>
     <description>DATE/TIME: 06/11/03, 1915 HRS. VICTIM(S): KHAYRI DOE
     JR. M/B BLK/BRO 3'0", 40
LBS. LIGHT COMPLEXION. DOB 06/24/01. WEARING RED SHORTS, WHITE T-SHIRT,
W/BLUE COLLAR. LOCATION: 5721 DOE ST., LOS ANGELES, CA. SUSPECT(S):
KHAYRI DOE SR. DOB 04/18/71 M/B, BLK HAIR,
     BRO EYE. VEHICLE: 81' BUICK 2-DR, BLUE (4XXX000).</description>
     <contact>DET. SMITH, 77TH DIV, LOS ANGELES POLICE DEPT-LAPD
     AT 213  485-2389</contact>
     <area>
     <areaDesc>Los Angeles County</areaDesc>
          <geocode>
               <valueName>SAME</valueName>
               <value>006037</value>
          </geocode>
     </area>
     </info>
</alert>
```

Bibliography

[b-WGS 84] National Geospatial Intelligence Agency, Department of Defense World Geodetic System 1984, http://earth-info.nga.mil/GandG/publications/tr8350.2/tr8350_2.html, NGA Technical, Report TR8350.2, January 2000.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2008