

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



International
Telecommunication
Union

Documents
Document Sharing Hub

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/>.

© ITU 2008

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

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 Institute 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/xmlsigcore/>.
- [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