International Telecommunication Union

ITU-T X.1303 *bis*

(03/2014)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services – Emergency communications

Common alerting protocol (CAP 1.2)

Recommendation ITU-T X.1303 *bis*

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	**X.1300–X.1309**
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

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

Recommendation ITU-T X.1303 *bis*

Common alerting protocol (CAP 1.2)

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 an undetected hazard or hostile act might indicate. CAP also provides a template for effective warning messages based on best practices identified in academic research and real-world experience.

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

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1303 bis	2014-03-01	17	11.1002/1000/12150

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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/.

Table of Contents

Introduction

A brief introduction to the common alerting protocol (the current specification is identified as CAP 1.2) is provided below.

Purpose

The common alerting protocol (CAP) provides an open, non-proprietary digital message format for all types of alerts and notifications. It does not address any particular application or telecommunications method. The CAP format is compatible with emerging techniques, such as web services 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 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 (NSTC) report on "Effective Disaster Warnings" released in November 2000 recommended that "a standard method should be developed to collect and relay instantaneously and automatically all types of hazard warnings and reports locally, regionally and nationally for input into a wide variety of dissemination systems."

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

In 2002, the CAP initiative was endorsed by the national non-profit Partnership for Public Warning, which sponsored its contribution in 2003 to the OASIS standards process. In 2004, CAP version 1.0 was adopted as an OASIS standard. In 2005, changes based on user feedback were incorporated into CAP and version 1.1 was released. As part of the International Telecommunication Union (ITU-T) adoption of CAP, a CAP 1.1 Errata was released in 2007 to support ASN.1 encoding. Version 1.2 is a minor release to resolve issues identified by the EM-TC CAP Call for Comments initiated in April 2008 and also incorporates feedback from CAP profile development efforts.

NOTE – There are incompatible changes in the XML schema between CAP 1.1 and 1.2. Consequently, the ASN.1 module for CAP 1.2 as described in clause 8.3 is not compatible with that of CAP 1.1 – Recommendation ITU-T X.1303 (2007).

Structure of the CAP alert message

Each CAP alert message consists of an <alert> segment, which may contain one or more <info> segments, each of which may include one or more <area> and/or <resource> segments. Under most circumstances, CAP messages with a <msgType> value of "Alert" should include at least one <info> element. (See the document object model diagram in 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 appropriate response by message recipients and various other details (hazard duration, technical parameters, contact information, links to additional information sources, etc.). Multiple <info> segments may be used to describe differing parameters (e.g., for different probability or intensity "bands") or to provide the information in multiple languages.

- **<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 the CAP alert message 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.

Recommendation ITU-T X.1303 *bis*

Common alerting protocol (CAP 1.2)

1 Scope

This Recommendation defines the common alerting protocol (CAP) – version 1.2 – 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 those that 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.

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 XML schema definition (XSD) schema and an abstract syntax notation one (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.1.2.

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] Recommendation ITU-T X.680 (2008) | ISO/IEC 8824-1:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

[ITU-T X.691] Recommendation ITU-T X.691 (2008) | ISO/IEC 8825-2:2008, *Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER).*

[ITU-T X.693] Recommendation ITU-T X.693 (2008) | ISO/IEC 8825-4:2008, *Information technology – ASN.1 encoding rules: XML Encoding Rules (XER).*

[ITU-T X.694] Recommendation ITU-T X.694 (2008) | ISO/IEC 8825-5, *Information technology – ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1*.

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

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

[IETF RFC 3066] IETF RFC 3066 (2001), *Tags for the Identification of Languages*.
http://www.ietf.org/rfc/rfc3066.txt

[W3C Namespaces] W3C, *Namespaces in XML 1.0 (Third Edition)*, W3C Recommendation, December 2009.
http://www.w3.org/TR/REC-xml-names/

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

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

[W3C Signature] W3C, *XML-Signature Syntax and Processing*, W3C Recommendation, February 2002.
http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ASN.1 Abstract Syntax Notation One

CAP Common Alerting Protocol

EAS Emergency Alert System

EPSG European Petroleum Survey Group

HTML Hypertext Markup Language

ID Identification

MIME	Multipurpose Internet Mail Extensions
NOAA	National Oceanic and Atmospheric Administration
NSTC	National Science and Technology Council
SAME	Specific Area Message Encoding
URI	Uniform Resource Identifier
TCP/IP	Transmission Control Protocol/Internet Protocol
UTC	Coordinated Universal Time
WGS	World Geodetic System
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, unprojected, in the form "[latitude],[longitude]". Latitudes in the Southern Hemisphere and longitudes in the Western Hemisphere are signed negative by means of a leading dash.

6 Design principles and concepts

This clause is non-normative.

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 1.0], [W3C Namespaces]) and portable structure: Although the primary anticipated use of the CAP alert message is as an XML document, the format should remain sufficiently abstract to be adaptable to other coding schemes.
- Multi-use format: One message schema supports multiple message types (e.g., alert / update / cancellations / acknowledgements / error messages) in various applications (actual / exercise / test / system message).
- Familiarity: The data elements and code values should be meaningful to warning originators and non-expert recipients alike.
- Interdisciplinary and international utility: The design should allow a broad range of applications in public safety and emergency management and allied applications and should be applicable worldwide.

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.

CAP should:

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

1) an evacuation of the area within half a mile of the fire;
2) 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;

3) a request for all media and civilian aircraft to remain above 2'500 feet above ground level when within a half mile radius of the fire."

"Using a portable computer and a webpage (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 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)."

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, from an authorized authority, of a single CAP message."

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

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

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., clause 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 dialling systems) stop doing so. Broadcast systems deliver a cancellation message. Other systems (e.g., highway signs) simply reset to their normal state."

7 Alert message structure

This clause discusses the 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.

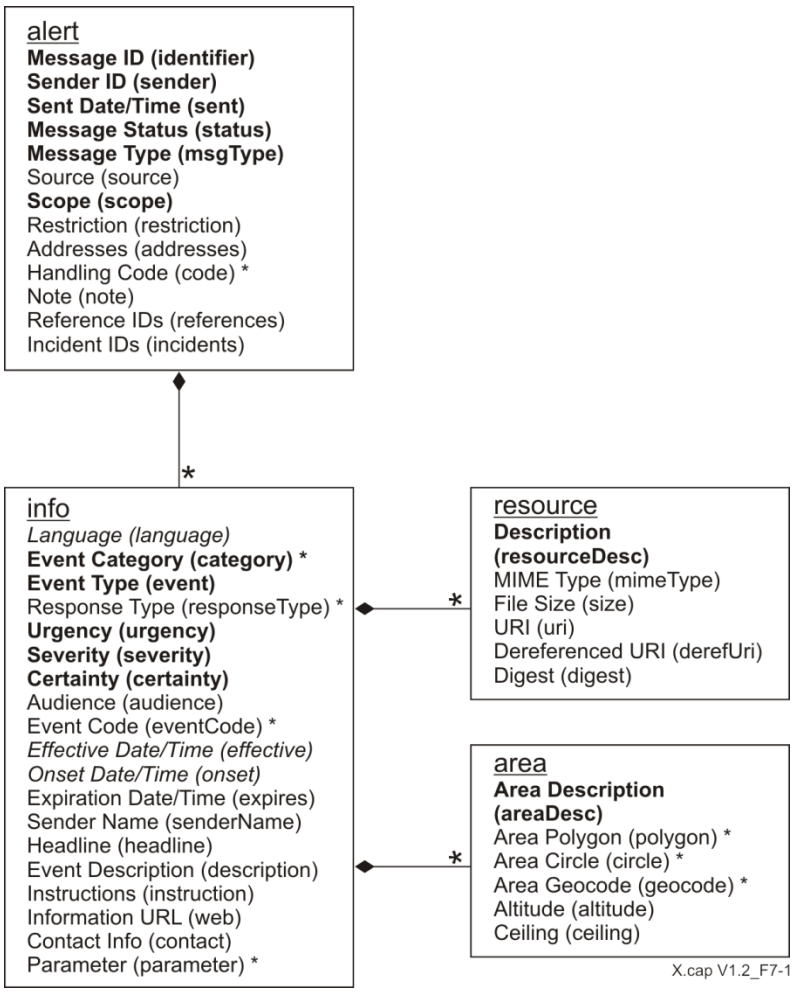

Figure 7-1 – Document object model

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 (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	Context.class.attribute. representation	Definition and (Optionality)	Notes or value domain

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

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

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

Element name	Context.class.attribute. representation	Definition and (Optionality)	Notes or value domain
status	cap.alert.status.code	The code denoting the appropriate handling of the alert message (REQUIRED)	Code Values: "Actual" – Actionable by all targeted recipients "Exercise" – Actionable only by designated exercise participants; exercise identifier should appear in <note> "System" – For messages that support alert network internal functions "Test" – Technical testing only, all recipients disregard "Draft" – A preliminary template or draft, not actionable in its current form
msgType	cap.alert.msgType.code	The code denoting the nature of the alert message (REQUIRED)	Code Values: "Alert" – Initial information requiring attention by targeted recipients "Update" – Updates and 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>
source	cap.alert.source.identifier	The text identifying the source of the alert message (OPTIONAL)	The particular source of this alert; e.g., an operator or a specific device.
scope	cap.alert.scope.code	The code denoting the intended distribution of the alert message (REQUIRED)	Code Values: "Public" – For general dissemination to unrestricted audiences "Restricted" – For dissemination only to users with a known operational requirement (see <restriction>, below) "Private" – For dissemination only to specified addresses (see <addresses>, below)

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

Element name	Context.class.attribute. representation	Definition and (Optionality)	Notes or value domain
restriction	cap.alert.restriction.text	The text describing the rule for limiting distribution of the restricted alert message (CONDITIONAL)	Used when <scope> value is "Restricted".
addresses	cap.alert.addresses.group	The group listing of intended recipients of the alert message (CONDITIONAL)	(1) Required when <scope> is "Private", optional when <scope> is "Public" or "Restricted". (2) Each recipient shall be identified by an identifier or an address. (3) Multiple space-delimited addresses may be included. Addresses including whitespace must be enclosed in double-quotes.
code	cap.alert.code.code	The code denoting the special handling of the alert message (OPTIONAL)	(1) Any user-defined flag or special code used to flag the alert message for special handling. (2) Multiple instances may occur.
note	cap.alert.note.text	The text describing the purpose or significance of the alert message (OPTIONAL)	The message note is primarily intended for use with <status> "Exercise" and <msgType> "Error".
references	cap.alert.references.group	The group listing identifying earlier message(s) referenced by the alert message (OPTIONAL)	(1) The extended message identifier(s) (in the form *sender,identifier,sent)* of an earlier CAP message or messages referenced by this one. (2) If multiple messages are referenced, they shall be separated by whitespace.
incidents	cap.alert.incidents.group	The group listing naming the referent incident(s) of the alert message (OPTIONAL)	(1) Used to collate multiple messages referring to different aspects of the same incident. (2) If multiple incident identifiers are referenced, they shall be separated by whitespace. Incident names including whitespace shall be surrounded by double-quotes.

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	Context.class.attribute. representation	Definition and (Optionality)	Notes or value domain
info	cap.alertInfo.info.group	The container for all component parts of the info sub-element of the alert message (OPTIONAL)	(1) Multiple occurrences are permitted within a single <alert>. If targeting of multiple <info> blocks in the same language overlaps, information in later blocks may expand but may not override the corresponding values in earlier ones. Each set of <info> blocks containing the same language identifier shall be treated as a separate sequence. (2) In addition to the specified sub-elements, may contain one or more <resource> blocks and/or one or more <area> blocks.
language	cap.alertInfo.language.code	The code denoting the language of the info sub-element of the alert message (OPTIONAL)	(1) Code Values: Natural language identifier per [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."
category	cap.alertInfo.category.code	The code denoting the category of the subject event of the alert message (REQUIRED)	(1) Code Values: "Geo" – Geophysical (inc. landslide) "Met" – Meteorological (inc. flood) "Safety" – General emergency and public safety "Security" – Law enforcement, military, homeland and local/private security "Rescue" – Rescue and recovery "Fire" – Fire suppression and rescue "Health" – Medical and public health "Env" – Pollution and other environmental "Transport" – Public and private transportation "Infra" – Utility, telecommunication, other non-transport infrastructure "CBRNE" – Chemical, Biological, Radiological, Nuclear or High-Yield Explosive threat or attack "Other" – Other events (2) Multiple instances may occur within an <info> block.

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

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

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

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

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

Element name	Context.class.attribute. representation	Definition and (Optionality)	Notes or value domain

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

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

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

Element name	Context.class.attribute. representation	Definition and (Optionality)	Notes or value domain
expires	cap.alertInfo.expires.time	The expiry time of the information of the alert message (OPTIONAL)	(1) The date and time shall be represented in the DateTime Data Type (See Implementation Notes) format (e.g., "2002-05-24T16:49:00-07:00" for 24 May 2002 at 16:49 PDT). (2) Alphabetic timezone designators such as "Z" must not be used. The timezone for UTC must be represented as "-00:00". (3) If this item is not provided, each recipient is free to set its own policy as to when the message is no longer in effect.
senderName	cap.alertInfo.senderName. text	The text naming the originator of the alert message (OPTIONAL)	The human-readable name of the agency or authority issuing this alert.
headline	cap.alertInfo.headline.text	The text headline of the alert message (OPTIONAL)	A brief human-readable headline. Note that some displays (for example, short messaging service devices) may only present this headline; it should be made as direct and actionable as possible while remaining short. 160 characters may be a useful target limit for headline length.
description	cap.alertInfo.description. text	The text describing the subject event of the alert message (OPTIONAL)	An extended human readable description of the hazard or event that occasioned this message.
instruction	cap.alertInfo.instruction.text	The text describing the recommended action to be taken by recipients of the alert message (OPTIONAL)	An extended human readable instruction to targeted recipients. If different instructions are intended for different recipients, they should be represented by use of multiple <info> blocks.
web	cap.alertInfo.web.identifier	The identifier of the hyperlink associating additional information with the alert message (OPTIONAL)	A full, absolute URI for an HTML page or other text resource with additional or reference information regarding this alert.

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

Element name	Context.class.attribute. representation	Definition and (Optionality)	Notes or value domain
contact	cap.alertInfo.contact.text	The text describing the contact for follow-up and confirmation of the alert message (OPTIONAL)	

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

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	Context.class.attribute. representation	Definition and (Optionality)	Notes or value domain
resource	cap.alertInfoResource. resource.group	The container for all component parts of the resource sub-element of the info sub-element of the alert element (OPTIONAL)	(1) Refers to an additional file with supplemental information related to this <info> element; e.g., an image or audio file. (2) Multiple instances may occur within an <info> block.
resource Desc	cap.alertInfoResource. resourceDesc.text	The text describing the type and content of the resource file (REQUIRED)	The human-readable text describing the type and content, such as "map" or "photo", of the resource file.

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

Element name	Context.class.attribute. representation	Definition and (Optionality)	Notes or value domain
mimeType	cap.alertInfoResource. mimeType.identifier	The identifier of the MIME content type and sub-type describing the resource file (REQUIRED)	MIME content type and sub-type as described in [IETF RFC 2046]. (As of this document, the current IANA registered MIME types are listed at http://www.iana.org/assignments/ media-types/)
size	cap.alertInfoResource.size. integer	The integer indicating the size of the resource file (OPTIONAL)	(1) Approximate size of the resource file in bytes. (2) For <uri> based resources, <size> should be included if available.
uri	cap.alertInfoResource.uri.id entifier	The identifier of the hyperlink for the resource file (OPTIONAL)	A full absolute URI, typically a Uniform Resource Locator that can be used to retrieve the resource over the Internet OR a relative URI to name the content of a <derefUri> element if one is present in this resource block.
derefUri	cap.alertInfoResource. derefUri.data	The base-64 encoded data content of the resource file (CONDITIONAL)	(1) May be used either with or instead of the <uri> element in messages transmitted over one-way (e.g., broadcast) data links where retrieval of a resource via a URI is not feasible. (2) Clients intended for use with one-way data links must support this element. (3) This element must not be used unless the sender is certain that all direct clients are capable of processing it. (4) If messages including this element are forwarded onto a two-way network, the forwarder must strip the <derefUri> element and should extract the file contents and provide a <uri> link to a retrievable version of the file. (5) Providers of one-way data links may enforce additional restrictions on the use of this element, including message-size limits and restrictions regarding file types.

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

Element name	Context.class.attribute. representation	Definition and (Optionality)	Notes or value domain
digest	cap.alertInfoResource. digest.code	The code representing the digital digest ("hash") computed from the resource file (OPTIONAL)	Calculated using the Secure Hash Algorithm (SHA-1) per [NIST FIPS 180-2].

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	Context.class.attribute. representation	Definition and (Optionality)	Notes or value domain
area	cap.alertInfoArea.area. group	The container for all component parts of the area sub-element of the info sub-element of the alert message (OPTIONAL)	(1) Multiple occurrences permitted, in which case the target area for the <info> block is the union of all the included <area> blocks. (2) May contain one or multiple instances of <polygon>, <circle> or <geocode>. If multiple <polygon>, <circle> or <geocode> elements are included, the area described by this <area> block is represented by the union of all the included elements.
areaDesc	cap.alertInfoArea.areaDesc. text	The text describing the affected area of the alert message (REQUIRED)	A text description of the affected area.
polygon	cap.alertInfoArea.polygon. group	The paired values of points defining a polygon that delineates the affected area of the alert message (OPTIONAL)	(1) Code Values: The geographic polygon is represented by a whitespace-delimited list of [b-WGS 84] coordinate pairs. (See WGS 84 note in clause 7.3.1) (2) A minimum of four coordinate pairs must be present and the first and last pairs of coordinates must be the same. (3) Multiple instances may occur within an <area> block.
circle	cap.alertInfoArea.circle. group	The paired values of a point and radius delineating the affected area of the alert message (OPTIONAL)	(1) Code Values: The circular area is represented by a central point given as a [b-WGS 84] coordinate pair followed by a space character and a radius value in kilometers. (See WGS 84 note in clause 7.3.1) (2) Multiple instances may occur within an <area> block.

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

Element name	Context.class.attribute. representation	Definition and (Optionality)	Notes or value domain
geocode	cap.alertInfoArea.geocode. code	The geographic code delineating the affected area of the alert message (OPTIONAL)	(1) Any geographically-based code to describe a message target area, in the form: <geocode> <valueName>*valueName*</valueName> <value>*value*</value> </geocode> where the content of "valueName" is a user-assigned string designating the domain of the code, and the content of "value" is a string (which may represent a number) denoting the value itself (e.g., valueName ="SAME" and value="006113"). (2) Values of "valueName" that are acronyms should be represented in all capital letters without periods (e.g., SAME, FIPS, ZIP). (3) Multiple instances may occur within an <area> block. (4) This element is primarily for compatibility with other systems. Use of this element presumes knowledge of the coding system on the part of recipients; therefore, for interoperability, it should be used in concert with an equivalent description in the more universally understood <polygon> and <circle> forms whenever possible.
altitude	cap.alertInfoArea.altitude. quantity	The specific or minimum altitude of the affected area of the alert message (OPTIONAL)	(1) If used with the <ceiling> element this value is the lower limit of a range. Otherwise, this value specifies a specific altitude. (2) The altitude measure is in feet above mean sea level per the [b-WGS 84] datum.
ceiling	cap.alertInfoArea.ceiling. quantity	The maximum altitude of the affected area of the alert message (CONDITIONAL)	(1) Must not be used except in combination with the <altitude> element. (2) The ceiling measure is in feet above mean sea level per the [b-WGS 84] datum.

7.3 Implementation considerations

7.3.1 WGS 84

Geographic locations in CAP are defined using [b-WGS 84] (World Geodetic System 1984), equivalent to European Petroleum Survey Group (EPSG) code 4326 (2 dimensions). CAP does not assign responsibilities for coordinate transformations from and to other spatial reference systems. See clause 5 of that document for the format of coordinate pairs within CAP elements.

7.3.2 DateTime data type

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

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

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

7.3.3 Character entity references

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

7.3.4 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.

7.3.4.1 Digital signatures

The <alert> element of a CAP alert message may have an Enveloped Signature, as described by XML-Signature and Syntax Processing [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 should inform the user of their failure to validate the signature.

In other words, the presence of an element with the namespace URI [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.

7.4 XML schema

```
<?xml version = "1.0" encoding = "UTF-8"?>
<!-- Copyright OASIS Open 2010 All Rights Reserved -->
<schema xmlns = "http://www.w3.org/2001/XMLSchema"
   targetNamespace = "urn:oasis:names:tc:emergency:cap:1.2"
   xmlns:cap = "urn:oasis:names:tc:emergency:cap:1.2"
   xmlns:xs = "http://www.w3.org/2001/XMLSchema"
   elementFormDefault = "qualified"
   attributeFormDefault = "unqualified"
   version = "1.2">
  <element name = "alert">
    <annotation>
      <documentation>CAP Alert Message (version 1.2)</documentation>
    </annotation>
    <complexType>
      <sequence>
        <element name = "identifier" type = "xs:string"/>
        <element name = "sender" type = "xs:string"/>
        <element name = "sent">
          <simpleType>
            <restriction base = "xs:dateTime">
              <pattern value = "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,+]\d\d:\d\d"/>
            </restriction>
          </simpleType>
        </element>
        <element name = "status">
          <simpleType>
            <restriction base = "xs:string">
              <enumeration value = "Actual"/>
              <enumeration value = "Exercise"/>
              <enumeration value = "System"/>
              <enumeration value = "Test"/>
              <enumeration value = "Draft"/>
            </restriction>
          </simpleType>
        </element>
        <element name = "msgType">
          <simpleType>
            <restriction base = "xs:string">
              <enumeration value = "Alert"/>
              <enumeration value = "Update"/>
              <enumeration value = "Cancel"/>
              <enumeration value = "Ack"/>
              <enumeration value = "Error"/>
            </restriction>
          </simpleType>
        </element>
        <element name = "source" type = "xs:string" minOccurs = "0"/>
        <element name = "scope">
          <simpleType>
            <restriction base = "xs:string">
              <enumeration value = "Public"/>
              <enumeration value = "Restricted"/>
              <enumeration value = "Private"/>
            </restriction>
          </simpleType>
        </element>
        <element name = "restriction" type = "xs:string" minOccurs = "0"/>
        <element name = "addresses" type = "xs:string" minOccurs = "0"/>
        <element name = "code" type = "xs:string" minOccurs = "0" maxOccurs = "unbounded"/>
        <element name = "note" type = "xs:string" minOccurs = "0"/>
        <element name = "references" type = "xs:string" minOccurs = "0"/>
        <element name = "incidents" type = "xs:string" minOccurs = "0"/>
        <element name = "info" minOccurs = "0" maxOccurs = "unbounded">
          <complexType>
            <sequence>
              <element name = "language" type = "xs:language" default = "en-US" minOccurs = "0"/>
              <element name = "category" maxOccurs = "unbounded">
                <simpleType>
                  <restriction base = "xs:string">
                    <enumeration value = "Geo"/>
                    <enumeration value = "Met"/>
                    <enumeration value = "Safety"/>
                    <enumeration value = "Security"/>
                    <enumeration value = "Rescue"/>
                    <enumeration value = "Fire"/>
                    <enumeration value = "Health"/>
                    <enumeration value = "Env"/>
                    <enumeration value = "Transport"/>
                    <enumeration value = "Infra"/>
                    <enumeration value = "CBRNE"/>
                    <enumeration value = "Other"/>
                  </restriction>
                </simpleType>
              </element>
              <element name = "event" type = "xs:string"/>
              <element name = "responseType" minOccurs = "0" maxOccurs = "unbounded">
                <simpleType>
```

```
      <restriction base = "xs:string">
        <enumeration value = "Shelter"/>
        <enumeration value = "Evacuate"/>
        <enumeration value = "Prepare"/>
        <enumeration value = "Execute"/>
        <enumeration value = "Avoid"/>
        <enumeration value = "Monitor"/>
        <enumeration value = "Assess"/>
        <enumeration value = "AllClear"/>
        <enumeration value = "None"/>
      </restriction>
    </simpleType>
  </element>
  <element name = "urgency">
    <simpleType>
      <restriction base = "xs:string">
        <enumeration value = "Immediate"/>
        <enumeration value = "Expected"/>
        <enumeration value = "Future"/>
        <enumeration value = "Past"/>
        <enumeration value = "Unknown"/>
      </restriction>
    </simpleType>
  </element>
  <element name = "severity">
    <simpleType>
      <restriction base = "xs:string">
        <enumeration value = "Extreme"/>
        <enumeration value = "Severe"/>
        <enumeration value = "Moderate"/>
        <enumeration value = "Minor"/>
        <enumeration value = "Unknown"/>
      </restriction>
    </simpleType>
  </element>
  <element name = "certainty">
    <simpleType>
      <restriction base = "xs:string">
        <enumeration value = "Observed"/>
        <enumeration value = "Likely"/>
        <enumeration value = "Possible"/>
        <enumeration value = "Unlikely"/>
        <enumeration value = "Unknown"/>
      </restriction>
    </simpleType>
  </element>
  <element name = "audience" type = "xs:string" minOccurs = "0"/>
  <element name = "eventCode" minOccurs = "0" maxOccurs = "unbounded">
    <complexType>
      <sequence>
        <element ref = "cap:valueName"/>
        <element ref = "cap:value"/>
      </sequence>
    </complexType>
  </element>
  <element name = "effective" minOccurs = "0">
   <simpleType>
     <restriction base = "xs:dateTime">
       <pattern value = "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,+]\d\d:\d\d"/>
     </restriction>
   </simpleType>
  </element>
  <element name = "onset"  minOccurs = "0">
   <simpleType>
     <restriction base = "xs:dateTime">
       <pattern value = "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,+]\d\d:\d\d"/>
     </restriction>
   </simpleType>
  </element>
  <element name = "expires"  minOccurs = "0">
   <simpleType>
     <restriction base = "xs:dateTime">
       <pattern value = "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,+]\d\d:\d\d"/>
     </restriction>
   </simpleType>
  </element>
  <element name = "senderName" type = "xs:string" minOccurs = "0"/>
  <element name = "headline" type = "xs:string" minOccurs = "0"/>
  <element name = "description" type = "xs:string" minOccurs = "0"/>
  <element name = "instruction" type = "xs:string" minOccurs = "0"/>
  <element name = "web" type = "xs:anyURI" minOccurs = "0"/>
  <element name = "contact" type = "xs:string" minOccurs = "0"/>
  <element name = "parameter" minOccurs = "0" maxOccurs = "unbounded">
    <complexType>
      <sequence>
        <element ref = "cap:valueName"/>
        <element ref = "cap:value"/>
      </sequence>
    </complexType>
  </element>
```

```
              <element name = "resource" minOccurs = "0" maxOccurs = "unbounded">
                <complexType>
                  <sequence>
                    <element name = "resourceDesc" type = "xs:string"/>
                    <element name = "mimeType" type = "xs:string"/>
                    <element name = "size" type = "xs:integer" minOccurs = "0"/>
                    <element name = "uri" type = "xs:anyURI" minOccurs = "0"/>
                    <element name = "derefUri" type = "xs:string" minOccurs = "0"/>
                    <element name = "digest" type = "xs:string" minOccurs = "0"/>
                  </sequence>
                </complexType>
              </element>
              <element name = "area" minOccurs = "0" maxOccurs = "unbounded">
                <complexType>
                  <sequence>
                    <element name = "areaDesc" type = "xs:string"/>
                    <element name = "polygon" type = "xs:string" minOccurs = "0" maxOccurs = "unbounded"/>
                    <element name = "circle" type = "xs:string" minOccurs = "0" maxOccurs = "unbounded"/>
                    <element name = "geocode" minOccurs = "0" maxOccurs = "unbounded">
                      <complexType>
                        <sequence>
                          <element ref = "cap:valueName"/>
                          <element ref = "cap:value"/>
                        </sequence>
                      </complexType>
                    </element>
                    <element name = "altitude" type = "xs:decimal" minOccurs = "0"/>
                    <element name = "ceiling" type = "xs:decimal" minOccurs = "0"/>
                  </sequence>
                </complexType>
              </element>
            </sequence>
          </complexType>
        </element>
        <any minOccurs = "0" maxOccurs = "unbounded" namespace = "http://www.w3.org/2000/09/xmldsig#"
processContents = "lax"/>

      </sequence>
    </complexType>
  </element>
  <element name = "valueName" type = "xs:string"/>
  <element name = "value" type = "xs: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 (see [ITU-T X.680]) schema 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 are identical to those of the XML schema definition (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.

NOTE – Due to the way the XML schema has been changed in CAP 1.2, the ASN.1 module as described in clause 8.3 is not compatible with that of CAP 1.1. The ASN.1 module identifier indicates a version number, although the module identifier may not be communicated through a wire protocol. Implementers of this Recommendation should consider incorporating another mechanism that identifies the version of CAP, e.g., through prior handshake mechanism.

8.3 ASN.1 module

```
/* xml version = "1.0" encoding = "UTF-8" */
/* Copyright OASIS Open 2010 All Rights Reserved */
CAP-1-2 {itu-t recommendation x(24) cap(1303) version1-2(2)}
DEFINITIONS AUTOMATIC TAGS ::=
BEGIN
IMPORTS
    -- from Rec. ITU-T X.694 | ISO/IEC  8825-5
    String, DateTime, Language, AnyURI, Decimal
    FROM XSD {joint-iso-itu-t asn1(1) specification(0) modules(0) xsd-module(2)
version2(2)};

/* CAP Alert Message (version 1.2) */
Alert ::= SEQUENCE {
    identifier  XSD.String,
    sender      XSD.String,
    sent        XSD.DateTime (CONSTRAINED BY
                {/* XML representation of the XSD pattern "\d\d\d\d-\d\d-\d\dT
                \d\d:\d\d:\d\d[-,+]\d\d:\d\d" */}),
    status      ENUMERATED {
        actual,
        draft,
        exercise,
        system,
        test
    },
    msgType     ENUMERATED {
        ack,
        alert,
        cancel,
        error,
        update
    },
    source      XSD.String OPTIONAL,
    scope       ENUMERATED {
        private,
        public,
        restricted
    },
    restriction XSD.String OPTIONAL,
    addresses   XSD.String OPTIONAL,
    code-list   SEQUENCE OF code XSD.String,
    note        XSD.String OPTIONAL,
    references  XSD.String OPTIONAL,
    incidents   XSD.String OPTIONAL,
    info-list   SEQUENCE OF info SEQUENCE {
        language          XSD.Language OPTIONAL,
        category-list     SEQUENCE (SIZE(1..MAX)) OF category ENUMERATED {
            cBRNE,
            env,
            fire,
            geo,
            health,
```

```
        infra,
        met,
        other,
        rescue,
        safety,
        security,
        transport
    },
    event             XSD.String,
    responseType-list SEQUENCE OF responseType ENUMERATED {
        allClear,
        assess,
        avoid,
        evacuate,
        execute,
        monitor,
        none,
        prepare,
        shelter
    },
    urgency           ENUMERATED {
        expected,
        future,
        immediate,
        past,
        unknown
    },
    severity          ENUMERATED {
        extreme,
        minor,
        moderate,
        severe,
        unknown
    },
    certainty         ENUMERATED {
        likely,
        observed,
        possible,
        unknown,
        unlikely
    },
    audience          XSD.String OPTIONAL,
    eventCode-list    SEQUENCE OF eventCode SEQUENCE {
        valueName ValueName,
        value     Value
    },
    effective         XSD.DateTime (CONSTRAINED BY
                      {/* XML representation of the XSD pattern "\d\d\d\d-
                      \d\d-\d\dT\d\d:\d\d:\d\d[-,+]\d\d:\d\d" */})
                      OPTIONAL,
    onset             XSD.DateTime (CONSTRAINED BY
                      {/* XML representation of the XSD pattern "\d\d\d\d-
                      \d\d-\d\dT\d\d:\d\d:\d\d[-,+]\d\d:\d\d" */})
                      OPTIONAL,
    expires           XSD.DateTime (CONSTRAINED BY
                      {/* XML representation of the XSD pattern "\d\d\d\d-
                      \d\d-\d\dT\d\d:\d\d:\d\d[-,+]\d\d:\d\d" */})
                      OPTIONAL,
    senderName        XSD.String OPTIONAL,
    headline          XSD.String OPTIONAL,
    description       XSD.String OPTIONAL,
    instruction       XSD.String OPTIONAL,
    web               XSD.AnyURI OPTIONAL,
    contact           XSD.String OPTIONAL,
    parameter-list    SEQUENCE OF parameter SEQUENCE {
        valueName ValueName,
        value     Value
    },
    resource-list     SEQUENCE OF resource SEQUENCE {
        resourceDesc XSD.String,
        mimeType     XSD.String,
```

```
            size         INTEGER OPTIONAL,
            uri          XSD.AnyURI OPTIONAL,
            derefUri     XSD.String OPTIONAL,
            digest       XSD.String OPTIONAL
        },
        area-list         SEQUENCE OF area SEQUENCE {
            areaDesc     XSD.String,
            polygon-list SEQUENCE OF polygon XSD.String,
            circle-list  SEQUENCE OF circle XSD.String,
            geocode-list SEQUENCE OF geocode SEQUENCE {
                valueName ValueName,
                value     Value
            },
            altitude     XSD.Decimal OPTIONAL,
            ceiling      XSD.Decimal OPTIONAL
        }
    },
    elem-list   SEQUENCE OF elem XSD.String (CONSTRAINED BY
                {/* Shall conform to the "AnyElementFormat" specified
                in ITU-T Rec. X.693 | ISO/IEC 8825-4, clause 19 */})
}

ValueName ::= XSD.String

Value ::= XSD.String

ENCODING-CONTROL XER
    GLOBAL-DEFAULTS MODIFIED-ENCODINGS
    GLOBAL-DEFAULTS CONTROL-NAMESPACE
        "http://www.w3.org/2001/XMLSchema-instance" PREFIX "xsi"
    NAMESPACE ALL, ALL IN ALL AS "urn:oasis:names:tc:emergency:cap:1.2"
        PREFIX "cap"
    NAME Alert, ValueName, Value AS UNCAPITALIZED
    UNTAGGED SEQUENCE OF
    ANY-ELEMENT Alert.elem-list.elem FROM "http://www.w3.org/2000/09/xmldsig#"
    DEFAULT-FOR-EMPTY Alert.info-list.info.language AS "en-US"
    TEXT Alert.status:ALL, Alert.msgType:ALL, Alert.scope:ALL,
        Alert.info-list.info.category-list.category:ALL,
        Alert.info-list.info.responseType-list.responseType:ALL,
        Alert.info-list.info.urgency:ALL, Alert.info-list.info.severity:ALL,
        Alert.info-list.info.certainty:ALL AS CAPITALIZED
END
```

9 Conformance

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

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

9.1 Conformance targets

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

a) CAP version 1.2 message

b) CAP version 1.2 message producer

c) CAP version 1.2 message consumer

9.2 Conformance as a CAP version 1.2 message

An XML 1.0 document is a conforming CAP version 1.2 message if and only if:

a) it is valid according to the schema located at http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.xsd and

b) the content of its elements and the values of its attributes meet all the additional mandatory requirements specified in clause 7.

9.3 Conformance as a CAP version 1.2 message producer

A software entity is a conforming CAP version 1.2 message producer if and only if:

a) it is constructed in such a way that any XML document produced by it and present in a place in which a conforming CAP version 1.2 message is expected (based on contextual information) is indeed a conforming CAP version 1.2 message according to this standard.

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

– a distribution element (for example, EDXL-DE) transfers messages carrying CAP version 1.2 messages; a client has sent a request for a CAP version 1.2 message to a server which claims to be a conforming CAP version 1.2 message producer, and has received a response which is therefore expected to carry a conforming CAP version 1.2 message;

– a local test environment has been set up, and the application under test (which claims to be a conforming CAP version 1.2 message producer) has the ability to produce a CAP version 1.2 message and write it to a file in a directory in response to a request coming from the testing tool; the testing tool has sent many requests to the application under test and is now verifying all the files present in the directory, which is expected to contain only conforming CAP version 1.2 messages;

9.4 Conformance as a CAP version 1.2 message consumer

A software entity is a conforming CAP version 1.2 message consumer if and only if:

a) it is constructed in such a way that it is able to successfully validate and ingest a conforming CAP version 1.2 message according to this standard.

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

– a client receives and processes a CAP version 1.2 message from a server which claims to be a conforming CAP version 1.2 message producer.

Appendix I

CAP alert message examples

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

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

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

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:1.2">
  <identifier>KSTO1055887203</identifier>
  <sender>KSTO@NWS.NOAA.GOV</sender>
  <sent>2003-06-17T14:57:00-07:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Public</scope>
  <info>
    <category>Met</category>
    <event>SEVERE THUNDERSTORM</event>
    <responseType>Shelter</responseType>
    <urgency>Immediate</urgency>
    <severity>Severe</severity>
    <certainty>Observed</certainty>
    <eventCode>
      <valueName>SAME</valueName>
      <value>SVR</value>
    </eventCode>
    <expires>2003-06-17T16:00:00-07:00</expires>
    <senderName>NATIONAL WEATHER SERVICE SACRAMENTO CA</senderName>
    <headline>SEVERE THUNDERSTORM WARNING</headline>
    <description> AT 254 PM PDT...NATIONAL WEATHER SERVICE DOPPLER RADAR INDICATED A SEVERE
THUNDERSTORM OVER SOUTH CENTRAL ALPINE COUNTY...OR ABOUT 18 MILES SOUTHEAST OF KIRKWOOD...MOVING
```

```
SOUTHWEST AT 5 MPH. HAIL...INTENSE RAIN AND STRONG DAMAGING WINDS ARE LIKELY WITH THIS
STORM.</description>
    <instruction>TAKE COVER IN A SUBSTANTIAL SHELTER UNTIL THE STORM PASSES.</instruction>
    <contact>BARUFFALDI/JUSKIE</contact>
    <area>
      <areaDesc>EXTREME NORTH CENTRAL TUOLUMNE COUNTY IN CALIFORNIA, EXTREME NORTHEASTERN CALAVERAS
COUNTY IN CALIFORNIA, SOUTHWESTERN ALPINE COUNTY IN CALIFORNIA</areaDesc>
      <polygon>38.47,-120.14 38.34,-119.95 38.52,-119.74 38.62,-119.89 38.47,-120.14</polygon>
      <geocode>
        <valueName>SAME</valueName>
        <value>006109</value>
      </geocode>
      <geocode>
        <valueName>SAME</valueName>
        <value>006009</value>
      </geocode>
      <geocode>
        <valueName>SAME</valueName>
        <value>006003</value>
      </geocode>
    </area>
  </info>
</alert>
```

I.3 Earthquake report (Update message)

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

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

I.4 AMBER alert (Multilingual message)

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

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

Bibliography

[b-WGS 84] National Geospatial Intelligence Agency, Department of Defense World Geodetic System (1984), *Its Definition and Relationships with Local Geodetic Systems*, http://earth-info.nga.mil/GandG/publications/tr8350.2/wgs84fin.pdf, NIMA Technical Report TR8350.2, June 2004, Third Edition Amendment 1.

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	Terminals and subjective and objective assessment methods
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, 2014