Common Alerting Protocol Version 1.1

USA Integrated Public Alert and Warning System Profile Version 1.0

Public Review Draft 01

26 February 2009

Specification URIs:
This Version:

http://docs.oasis-open.org/emergency/cap/v1.1/ipaws-profile/v1.0/pr01/cap-v1.1-ipaws-profile-v1.0-pr01.html
http://docs.oasis-open.org/emergency/cap/v1.1/ipaws-profile/v1.0/pr01/cap-v1.1-ipaws-profile-v1.0-pr01.doc (Authoritative)
http://docs.oasis-open.org/emergency/cap/v1.1/ipaws-profile/v1.0/pr01/cap-v1.1-ipaws-profile-v1.0-pr01.pdf

Previous Version:

N/A

Latest Version:

http://docs.oasis-open.org/emergency/cap/v1.1/ipaws-profile/v1.0/cap-v1.1-ipaws-profile-v1.0.html
http://docs.oasis-open.org/emergency/cap/v1.1/ipaws-profile/v1.0/cap-v1.1-ipaws-profile-v1.0.doc
http://docs.oasis-open.org/emergency/cap/v1.1/ipaws-profile/v1.0/cap-v1.1-ipaws-profile-v1.0.pdf

Technical Committee:

OASIS Emergency Management TC

Chair(s):

Elysa Jones, Warning Systems, Inc.

Editor(s):

Rex Brooks, Individual
Sukumar Dwarkanath, SRA International

Related work:

This specification is related to:

- OASIS Standard Common Alerting Protocol Version 1.1, October 2005
- OASIS Standard Common Alerting Protocol Version 1.1 Approved Errata 2 October 2007

Declared XML Namespace(s):

urn:oasis:names:tc:emergency:cap:1.1

Abstract:

This profile of the XML-based Common Alerting Protocol (CAP) describes an interpretation of the OASIS CAP v1.1 standard necessary to meet the needs of the Integrated Public Alert and Warning System (IPAWS), a public alerting "system of systems" created by the U.S. Federal Emergency Management Agency.

Status:

This document was last revised or approved by the Emergency Management Technical Committee on the above date. The level of approval is also listed above. Check the “Latest Version” or “Latest Approved Version” location noted above for possible later revisions of this document.

Technical Committee members should send comments on this specification to the Technical Committee’s email list. Others should send comments to the Technical Committee by using the “Send A Comment” button on the Technical Committee’s web page at http://www.oasis-open.org/committees/emergency/.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Technical Committee web page (http://www.oasis-open.org/committees/emergency/ipr.php.

The non-normative errata page for this specification is located at http://www.oasis-open.org/committees/emergency/.

Notices

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The names "OASIS", “CAP”, “Common Alerting Protocol”, and “Emergency Data Exchange Language” are trademarks of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see http://www.oasis-open.org/who/trademark.php for above guidance.

Table of Contents

1 Introduction

1.1 Purpose

In order to meet the needs of the devices intended to receive alerts from the United States Integrated Public Alert and Warning System (IPAWS) System of Systems (SoS), this CAP v1.1 IPAWS Profile constrains the CAP v1.1 standard for receipt and translation with and among IPAWS exchange partners.

The use of this profile is not necessarily limited to the initial IPAWS Exchange Partners. It is available to all who might want to use the particular concepts defined in this specification.

The Common Alerting Protocol (CAP) provides an open, non-proprietary digital message format for all types of alerts and notifications. It does not address any particular application or telecommunications method. The CAP format is compatible with emerging techniques, such as Web services, as well as existing formats including the Specific Area Message Encoding (SAME) used for the United States' National Oceanic and Atmospheric Administration (NOAA) Weather Radio and the Emergency Alert System (EAS), while offering enhanced capabilities that include:

- Flexible geographic targeting using latitude/longitude shapes and other geospatial representations in three dimensions;
- Multilingual and multi-audience messaging;
- 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.

The Common Alerting Protocol (CAP) v1.0 and v1.1 were approved as OASIS standards before the Emergency Data Exchange Language (EDXL) project was developed. However, this profile specification shares the goal of the EDXL project to facilitate emergency information sharing and data exchange across the local, state, tribal, national and non-governmental organizations of different professions that provide emergency response and management services. Several exchange partner alerting systems of the IPAWS SoS are identified by this profile for specific accommodation. However, the CAP v1.1-IPAWS Profile is not limited to systems. It is structured to allow inclusion of other alerting systems as deemed appropriate or necessary.

In addition to the definition of the term Profile in Section 1.2 Terminology, this profile is responsive to the requirements articulated by the FEMA IPAWS Program Management Office as cited in Section 1.5 Non-Normative References.

1.2 Process

This Profile was developed primarily by integrating requirements related to three federal warning-delivery systems:

- the broadcast Emergency Alert System (EAS) as recommended by the EAS-CAP Industry Working Group;
- the NOAA Non-Weather Emergency Message (NWEM) "HazCollect" program for weather radio and other delivery systems as derived from technical documentation; and,
- the Commercial Mobile Alerting Service (CMAS) for cellular telephones as described in the recommendations of the Commercial Mobile Service Alert Advisory Committee (CMSAAC).

Additional guidance was drawn from subject matter experts familiar with the design and implementation of those and other public warning systems.

1.3 Terminology

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in **[RFC2119]**.

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

The term **coordinate pair** is used in this document 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.

CMAS – Commercial Mobile Alert System – System recommended by FCC-established Commercial Mobile Service Alert Advisory Committee (CMSAAC) CMSAAC's mission was to develop recommendations on technical standards and protocols to facilitate the ability of commercial mobile service (CMS) providers to voluntarily transmit emergency alerts to their subscribers. The committee was established pursuant to Section 603 of the Warning, Alert and Response Network Act (WARN Act), which was enacted on October 13, 2006.

DateTime Data Type - All CAP 1.1 dateTime elements (sent, effective, onset and expires) SHALL be specified in the form "YYYY-MM-DDThh:mm:ssXzh:zm" where:

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

DHS – USA Department of Homeland Security – Federal Executive Branch Cabinet Department

EAS – USA Emergency Alert System, specifically mandated by the FCC is a national public warning system that requires broadcasters, cable television systems, wireless cable systems, satellite digital audio radio service (SDARS) providers and, direct broadcast satellite (DBS) service providers to provide the communications capability to the President to address the American public during a National emergency. The system also may be used by state and local authorities to deliver important emergency information such as AMBER alerts and weather information targeted to a specific area.

FCC – USA Federal Communication Commission.

FEMA – USA Federal Emergency Management Agency

HazCollect – USA National Oceanic and Atmospheric Administration, National Weather Service All Hazards Emergency Message Collection System (HazCollect) provides an automated capability to streamline the creation, authentication, collection, and dissemination of non-weather emergency messages in a quick and secure fashion. The HazCollect system is a comprehensive solution for the centralized collection and efficient distribution of Non-Weather Emergency Messages (NWEMs) to the NWS dissemination infrastructure, the Emergency Alert System (EAS), and other national systems.

IPAWS – USA Integrated Public Alert and Warning System was established by Executive Order 13407 in June 2006. The Department of Homeland Security, the Federal Emergency Management Agency (DHS/FEMA) and the IPAWS Program Management Office (PMO) work with public and private sectors to integrate warning systems to allow the President and authorized officials to effectively address and warn the public and State and local emergency operations centers via phone, cell phone, pagers, computers and other personal communications devices

IPAWS Exchange Partner –The EAS, HazCollect and CMAS exchange partners are specifically addressed by this specification document. Other systems may also use this profile.

Profile – As used in this document, a profile consists of an agreed-upon subset and interpretation of the. OASIS CAP-v1.1 Specification. An XML Profile is applied to an existing XML Schema (in this case the OASIS Standard CAP v1.1 Schema) in order to constrain or enforce aspects of it to accomplish a specific purpose according to the definition and criteria set forth for an XML Profile. Any message that is in compliance with the Profile must validate against the original XML Schema as well as the resulting XML Schema of the Profile.

1.4 Normative References

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

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

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

[namespaces] T. Bray, Namespaces in XML, W3C REC-xml-names-19990114, January 1999.
http://www.w3.org/TR/REC-xml-names/

[RFC2046] N. Freed, Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types, IETF RFC 2046, November 1996.
http://www.ietf.org/rfc/rfc2046.txt

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

[RFC3066] H. Alvestrand, Tags for the Identification of Languages, IETF RFC 3066, January 2001.
http://www.ietf.org/rfc/rfc3066.txt

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

[XML 1.0] T. Bray, Extensible Markup Language (XML) 1.0 (Third Edition), W3C REC-XML-20040204, February 2004.
http://www.w3.org/TR/REC-xml/

[XMLSIG] Eastlake, D., Reagle, J. and Solo, D. (editors), *XML-Signature Syntax and Processing*, W3C Recommendation, February 2002.
http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

[XMLENC] Eastlake, D. and Reagle, J. (editors), *XML Encryption Syntax and Processing*,
W3C Recommendation, December 2002.
http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

[CFR Title 47 Pt 11] Office of the Federal Register, National Archives and Records Administration, Government Printing Office, *XML Code of Federal Regulations, Federal Communications Commission*, Title 47 Telecommunication Part 11 Emergency Alert System, October 1998.
http://www.access.gpo.gov/nara/cfr/waisidx_98/47cfr11_98.html

1.5 Non-Normative References

[FEMA IPAWS CAP PROFILE REQUIREMENTS] FEMA IPAWS Program Management Office *FEMA IPAWS CAP v1.1 Profile Requirements v2.4 - Public*, December 2008
http://www.oasis-open.org/committees/download.php/31084/FEMA_IPAWS_CAP%20v1.1_Profile_Requirements_v2.4_-_Public.doc

[EAS-CAP PROFILE] EAS-CAP Industry Group *EAS-CAP Profile Recommendation EAS-CAP-01*, September 2008.
http://www.eas-cap.org/Recommendation%20EAS-CAP-0.1.pdf

[**NOAA HazCollect]** Disaster Management Open Platform for Emergency Networks Program *Instructions for Using the NOAA HazCollect Interface on the Open Platform for Emergency Networks (OPEN)* November 2008

. http://www.oasis-open.org/committees/download.php/31085/using_hazcollect_on_open20081106.pdf

1.6 Requirements

The FEMA IPAWS Program Management Office submitted the *FEMA IPAWS CAP v1.1Profile Requirements v2.4 – Public* document referenced above and available at the URL cited above as the basis for developing the CAP v1.1 IPAWS Profile v1.0. It should be noted that not all requirements found in the FEMA IPAWS Program Management Office Requirements document are included in this specification. For example, the proposal for multiple info blocks for different delivery systems was found unnecessary.

2 CAP v1.1 IPAWS Profile

The following table specifies the REQUIRED constraints placed by the CAP v1.1 IPAWS Profile on a CAP v1.1 message in order for the message to be a valid CAP IPAWS Profile message. This table contains only those elements of CAP v1.1 for which there is a Profile Specification or Profile Note. CAP v1.1 elements not included here simply means there is no specific constraint or condition in the use of those elements for the Profile.

Table 1: CAP v1.1 IPAWS Profile Specification and Profile Note

CAP Element	Profile Specification (Normative)	Profile Note (Non-Normative)
	(Subcommittee)	(Subcommittee)
sent	(1) The XML dateTime value SHALL include the timezone offset	
status	(1) A value of "Actual" SHALL be used for messages intended for dissemination to the public, including test messages intended for delivery to the public.	messages of status “Actual” based on those messages” eventCode values. For example, CMAS may not carry EAS required weekly test messages.
source		(1) Implementers should be aware that the <source> value may be publicly presented as a "signature" line in some delivery systems.
code*	(1) REQUIRED. Value SHALL include the string "IPAWSv1.0" to indicate the profile version in use.	
references	(1) All messages that have not yet expired should be referenced for messages of type “update” or “cancel”.	
info*	(2) All info blocks in a single alert MUST relate to a single incident or update, with the same category and eventCode values. (3) All info blocks SHALL be appropriate for immediate public release.	(1) Multiple info blocks may be used for the same message in different languages. (2) If additional info blocks are present, IPAWS System Partners MAY process only the first info block.
responseType *		(1) Use of the non-standard value "Avoid" is a recognized exception to the CAP 1.1 specification. (2) Use of this value will not validate against the CAP v1.1 schema.

CAP Element	Profile Specification (Normative)	Profile Note (Non-Normative)
eventCode *	(1) Messages intended for EAS, CMAS and HazCollect dissemination MUST include an instance of this with a valueName of "SAME" and using a SAME-standard three-letter value. (2) Other eventCode elements may also be present. (3) All values for EAS Event Code SHALL be passed through by EAS CAP Profile devices, even if the Event Code is not shown in FCC Part 11.31, as long as the value is a three-letter code and is approved by the FCC.	
effective	(1) Ignored if present. Alerts SHALL be effective upon issuance. (2) However, the description and/or instruction may refer to future events or actions.	
onset	(1) Ignored if present. Alerts SHALL be effective upon issuance. (2) However, the description and/or instruction may refer to future events or actions.	
expires	(1) REQUIRED. The XML dateTime value MUST include the timezone offset.	
parameter*	(1) Message intended for EAS and/or HazCollect dissemination MUST include a parameter with a valueName of "EAS-ORG" with a value of SAME ORG code. (2) Messages invoking the "Gubernatorial Must-Carry" rule SHALL also include a parameter with valueName of "EAS-Must-Carry" and value of "TRUE" for gubernatorial alerts. (3) OPTIONAL free-form text for CMAS MAY be included in a parameter with valueName of "CMAMtext". (4) There is a 90 English character limit in the free form text. (5) Other parameter elements may also be present.	The handling of free form CMAS text messages is still TBD.

CAP Element	Profile Specification (Normative)	Profile Note (Non-Normative)
resourceDesc	(1) A value of "EAS Broadcast Content" SHALL be used to indicate that the audio, video or image content of the current <resource> is intended for EAS broadcast.	
mimeType	(1) Recorded audio for delivery to the public SHALL be identified and encoded in one of the following formats: a. As “audio/x-ipaws-audio-mpeg”, encoded as MPEG Layer 3 (MP3) audio, 64kbps, 22.05 or 44.1 kHz sampling; or, b. As “audio/x-ipaws-audio-wav”, encoded as WAV PCM, mono, 16-bit, 22.05 kHz sampling. (2) Streaming audio for delivery to the public SHALL be identified as “audio/x-ipaws-streaming-audio-mpeg” and SHALL be MP3 audio, 64kbps, 22.05 or 44.1 kHz sampling, and transported via HTTP or Shoutcast/Icecast service. (3) Additional MIME types and encodings for other media formats such as video may be specified by the United States Department of Homeland Security using the “x-ipaws-“ prefix in the parameter portion of the MIME designator type.	
area*	(1) At least one <area> element MUST be present. (2) All <area> elements SHALL be considered in message distribution.	
geocode*	(1) At least one instance REQUIRED with a valueName of "SAME" and value of a SAME 6-digit location code (extended FIPS). (2) A SAME value of “000000” refers to ALL United States territoriy.	(1) The 5-digit form, if needed, can be derived by removing the first digit from the 6 digit form.

*May have multiple occurrences in a message under CAP 1.1 spec

3 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.

3.1 Conformance Targets

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

a) CAP V1.1 IPAWS PROFILE Message
b) CAP V1.1 IPAWS PROFILE Message Producer
c) CAP V1.1 IPAWS PROFILE Message Consumer

A CAP V1.1 IPAWS PROFILE Message is an XML 1.0 document whose syntax and semantics are specified in this standard.

A CAP V1.1 IPAWS PROFILE Message Producer is a software entity that produces CAP V1.1 IPAWS PROFILE Messages.

3.2 Conformance as an CAP V1.1 IPAWS Profile Message

An XML 1.0 document is a conforming CAP V1.1 IPAWS PROFILE Message if and only if:

a) it is valid according to the schema in Section 3.4 of the specification located at http://www.oasis-open.org/committees/download.php/15135/emergency-CAPv1.1-Corrected_DOM.pdf and
b) the content of its elements and the values of its attributes meet all the additional mandatory requirements specified in Section 2.

3.3 Conformance as an CAP V1.1 IPAWS Profile Message Producer

A software entity is a conforming CAP V1.1 IPAWS PROFILE Message Producer if and only if:

(1) it is constructed in such a way that any XML document produced by it and present in a place in which a conforming CAP V1.1 IPAWS PROFILE Message is expected (based on contextual information) is indeed a conforming CAP V1.1 IPAWS PROFILE Message according to this standard.

The condition in (1) above can be satisfied in many different ways. Here are some examples of possible scenarios:

– a standard protocol (for example, EDXL-DE) transfers messages carrying CAP V1.1 IPAWS PROFILE Messages; a client has sent a request for an CAP V1.1 IPAWS PROFILE Message to a server which claims to be a conforming CAP V1.1 IPAWS PROFILE Message Producer, and has received a response which is therefore expected to carry a conforming CAP V1.1 IPAWS PROFILE Message;

– a local test environment has been set up, and the application under test (which claims to be a conforming CAP V1.1 IPAWS PROFILE Message Producer) has the ability to produce a CAP V1.1 IPAWS PROFILE Message and write it to a file in a directory in response to a request coming from the testing tool; the testing tool has sent many requests to the application under test and is now verifying all the files present in the directory, which is expected to contain only conforming CAP V1.1 IPAWS PROFILE Messages;

3.4 Conformance as an CAP V1.1 IPAWS Profile Message Consumer

A software entity is a conforming CAP V1.1 IPAWS PROFILE Message Consumer if and only if:

(1) it is constructed in such a way that it is able to successfully validate and ingest a CAP V1.1 IPAWS PROFILE Message, as defined in Sec 3.2

The condition in (1) above can be satisfied in many different ways. Here is one example of a possible scenario:

- a client receives and processes a CAP V1.1 IPAWS PROFILE Message from a server which claims to be a conforming CAP V1.1 IPAWS PROFILE Message Producer

A. CAP v1.1 IPAWS Exchange Partner System Requirements – Non-Normative

The following table specifies the REQUIRED constraints placed by the CAP v1.1 IPAWS Profile Exchange Partner Alert Systems on a CAP v1.1 message in order for the message to be processed by the EAS, the CMAS and the NOAA NWS HazCollect System. This table contains only those elements of CAP v1.1 for which there is IPAWS Exchange Partner Alerting System-specific annotation of interest. CAP v1.1 elements not included here simply means there is no specific constraint or condition in the use of those elements for any of these IPAWS Exchange Partner Alert Systems.

Appendix A Table: CAP v1.1 IPAWS Profile Exchange Partner System-specific Requirements (Non-Normative)

CAP Element	EAS	CMAS	Hazcollect NWEM
	(EAS-CAP Industry Group Recommendation 9/23/08)	(CMAS Architecture and Requirements, CMSAAC 2007)	(Instructions for Using the NOAA HazCollect Interface, v 0.3, 6 Nov 2008)
identifier			Must be unique throughout HazCollect universe
sent	Time zone mandatory.	Time zone mandatory. Note: CMAS C-Interface requires UTC plus offset and must be consistent with any associated update or cancel messages	
status	Must be "Actual" to be aired even for EAS test messages	"Draft" will be rejected by CMAS Federal Alert gateway.	
msgType		"Ack" will be rejected by CMAS Federal Alert Gateway.	
source			Sender signature (name/initials).
scope		Any value but "Public" will be rejected by CMAS Federal Alert Gateway.	Must be "Public" or system will reject.
restriction		If present CMAS Federal Alert Gateway will reject message.	
addresses		If present CMAS Federal Alert Gateway will reject message.	

CAP Element	EAS	CMAS	Hazcollect NWEM
note	If msgType is "Ack", should include "Ignored:", "Accepted:" or "Aired on:" plus station callsign		
info *			Only one permitted.
language		English only	REQUIRED: May only be en-US or sp-US.
event			REQUIRED. String must match NWEM name for corresponding eventCode
responseType *		Value of "Assess" will result in rejection by CMAS Federal Alert Gateway. Additional value of "Avoid" recommended.	
urgency	Should be "Unknown" if the eventCode is DMO, NMN, NPT, RMT and RWT.	Only messages with urgency of "Immediate" and "Expected" will be passed to the CMSPs	
severity	Should be "Minor" if the eventCode is DMO, NMN, NPT, RMT and RWT.	Only message with a severity of "Extreme" or "Severe" will the passed to CMSPs	
certainty	Should be "Unknown" if the eventCode is DMO, NMN, NPT, RMT and RWT.	Only message with a certainty of "Observed" or "Likely" will the passed to CMSPs	

CAP Element	EAS	CMAS	Hazcollect NWEM
eventCode*	REQUIRED. The valueName must be "SAME", the value must be SAME three-letter event code.	If value is "EAN" CMAS Federal Alert Gateway will process as Presidential. 1. If value is "CAE" CMAS Federal Alert Gateway will process as Child Abduction. 2. CMAS Federal Alert Gateway will ignore messages marked "NIC" or "EAT". 3. The CMAS specifications recommends that an eventCode also be present to assist in the generation of the alert text.	REQUIRED: The valueName must be "SAME", the value must be SAME three-letter event code.
expires	REQUIRED: Time zone mandatory.	If already expired CMAS Federal Alert Gateway will reject. 4. If expires is missing, the Federal Alert Gateway will calculate a default expiration date and time. 5. UTC plus offset is mandatory. Note: the CMAS C-Interface limits alerts to a maximum of 24 hours	REQUIRED: Must conform to EAS expiration intervals (15 minute increments up to 120 minutes, 30 minute intervals up to 360, 360 max.)
senderName			REQUIRED: String must match DMIS COG id used for login.
parameter*	Two REQUIRED for EAS transmission: First valueName of "EAS-ORG" with value of SAME ORG code: Second valueName of "EAS-STN-ID" with SAME station ID: Third OPTIONAL with valueName of "EAS-Must-Carry": and, value of "TRUE" for gubernatorial alerts.	OPTIONAL parameter with valueName of "CMAMtext" provides free text as alternative to the automatically constructed CMAS message. There is a 90 English character limit in the free form text. Any free form text must comply with the FCC rules & CMSAAC recommendations.	

CAP Element	EAS	CMAS	Hazcollect NWEM
resourceDesc	If <resource> is used, value must be "EAS Audio" or "EAS Streaming Audio" as appropriate.	Initial version the CMAS C-Interface is text only. Multimedia formats such as audio and video are not pushed to the CMSPs on the C-Interface.	
mimeType	Recorded audio must be MP3 64kbps 22.05 or 44.1 kHz samping, or WAV PCM, mono, 16-bit, 22.05 kHz sampling. Streaming audio must be MP3 via HTTP or Shoutcast/Icecast service.		
area*	Only the first <area> block will be processed.		
geocode*	REQUIRED: valueName of "SAME" and value of 6-digit location code (extended FIPS).	CMAS specification currently uses a 5-digit FIPS code as well as codes for states and regions.	REQUIRED: May have valueName of "fips" with 5-digit FIPS code, or "state" with two-letter state code, or "zone" with NOAA zone designator.

232

233 *May have multiple occurrences in a message under CAP 1.1 spec

B. Acknowledgements

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Participants:

Aviv Siegel, AtHoc, Inc.
Art Botterell, Conta Costa County Community Warning System
Tim Grapes, Evolution Technologies, Inc.
Lee Tincher, Evolution Technologies, Inc.
Rex Brooks, Individual Member
Gary Ham, Inidividual Member
Jacob Westfall, Individual Member
Thomas Ferrentino, Individual Member
Robert Bunge, NOAA's National Weather Service
Sukumar Dwarkanath, SRA International
William Kalin, U.S. Department of Homeland Security
Richard Vandame, U.S. Department of Homeland Security
Patrick Gannon, Warning Systems, Inc.
Elysa Jones, Warning Systems, Inc.

C. Revision History

Revision	Date	Editor	Changes Made
‘WD.01	1-26-2009	Rex Brooks	First Draft.
WD.02	1-27-2009	Rex Brooks	Updated Table of Contents; Added Text to Section 1.1; Added Revision History
WD.03	1-29/2009	Rex Brooks	Full Subcommittee Revision of Section 1,
WD.04	2-3-2009	Rex Brooks	Multiple updates per CAP Profiles Subcommittee decisions.
WD.041	2-5-209	Rex Brooks	Multiple updates per CAP Profiles Subcommittee decisions.
WD.042	2-10-2009	Rex Brooks	Move Sections 3 to an Appendix; Insert FEMA CAPv1.1 Profile Requirements v2.4 Public as Appendix; Delete Section 4; Prepare Document for vote to submit to Emergency Management Technical Committee per CAP Profiles Subcommittee decisions.
WD.05	2-12-2009	Rex Brooks	Final prep for report out to the TC.
CD 01	2-24-2009	Rex Brooks	First Committee Draft version.
PR 02	2-26-2009	Rex Brooks	First Public Review Draft