ECRIT	B. Rosen	
Internet-Draft	NeuStar, Inc.	
Intended status: Experimental	H. Schulzrinne	
Expires: April 28, 2011	Columbia U.	
	H. Tschofenig	
	Nokia Siemens Networks	
	October 25, 2010	

TOC

Common Alerting Protocol (CAP) based Data-Only Emergency Alerts using the Session Initiation Protocol (SIP)
draft-ietf-ecrit-data-only-ea-01.txt

Abstract

The Common Alerting Protocol (CAP) is a document format for exchanging emergency alerts and public warnings. CAP is mainly used for conveying alerts and warnings between authorities and from authorities to citizen/individuals. This document describes how data-only emergency alerts allow devices to issue alerts using the CAP document format.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.
Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as “work in progress.”
This Internet-Draft will expire on April 28, 2011.

Copyright Notice

from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

---

1. Introduction

TOC

The Common Alerting Protocol (CAP) [cap] (Jones, E. and A. Botterell, “Common Alerting Protocol v. 1.1,” October 2005.) is an XML document format for exchanging emergency alerts and public warnings. CAP is mainly used for conveying alerts and warnings between authorities and from authorities to citizen/individuals. This document describes how data-only emergency calls are able to utilize the same CAP document format.

Data-only emergency alerts are similar to regular emergency calls in the sense that they require emergency call routing functionality and may even have the same location requirements. On the other hand, the initial communication interaction will not lead to the establishment of a voice or video channel.

Based on the deployment experience with non-IP based systems we distinguish between two types of environments, namely (1) data-only emergency alerts that are targeted directly to a recipient responsible for evaluating the alerts and for taking the necessary steps, including

triggering an emergency call towards a Public Safety Answering Point (PSAP) and (2) alerts that are targeted to a Service URN as used for regular IP-based emergency calls where the recipient is not known to the originator. We describe these two cases in more detail in Section 3 (Architectural Overview).

---

2. Terminology

TOC

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 RFC 2119 [RFC2119] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).
This document utilizes terminology introduced in [I-D.ietf-atoca-requirements] (Schulzrinne, H., Norreys, S., Rosen, B., and H. Tschofenig, “Requirements, Terminology and Framework for Exigent Communications,” September 2010.).

---

3. Architectural Overview

TOC

This section illustrates two envisioned usage modes; targeted and location-based emergency alert routing. Figure 1 (Targeted Emergency Alert Routing) shows a deployment variant where a sensor, as the author and originator of the alert, is pre-configured (using techniques outside the scope of this document) to issue an alert to a receiver or an aggregator, a special form of mediator, that processes these messages and performs whatever steps are necessary to appropriately react on the alert. For example, a security firm may use different sensor inputs to dispatch their security staff to a building they protect.

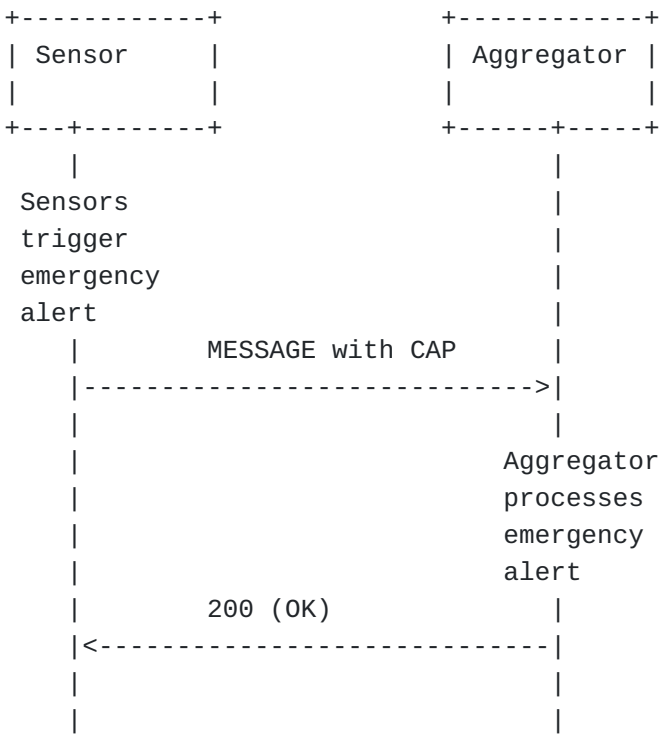

Figure 1: Targeted Emergency Alert Routing

In Figure 2 (Location-Based Emergency Alert Routing) a scenario is shown whereby the alert is routed using location information and the Service URN. In case the LoST resolution is done at an emergency services routing proxy rather than at the entity issuing the alert since it may not know the address of the receiver. A possible receiver is a PSAP and the recipient of the alert may be call taker. In the generic case, there is very likely no prior relationship between the originator and the receiver, e.g. PSAP. A PSAP, for example, is likely to receive and accept alerts from entities it cannot authorize. This scenario corresponds more to the classical emergency services use case and the description in [I-D.ietf-ecrit-phonebcp] (Rosen, B. and J. Polk, “Best Current Practice for Communications Services in support of Emergency Calling,” July 2010.) is applicable.

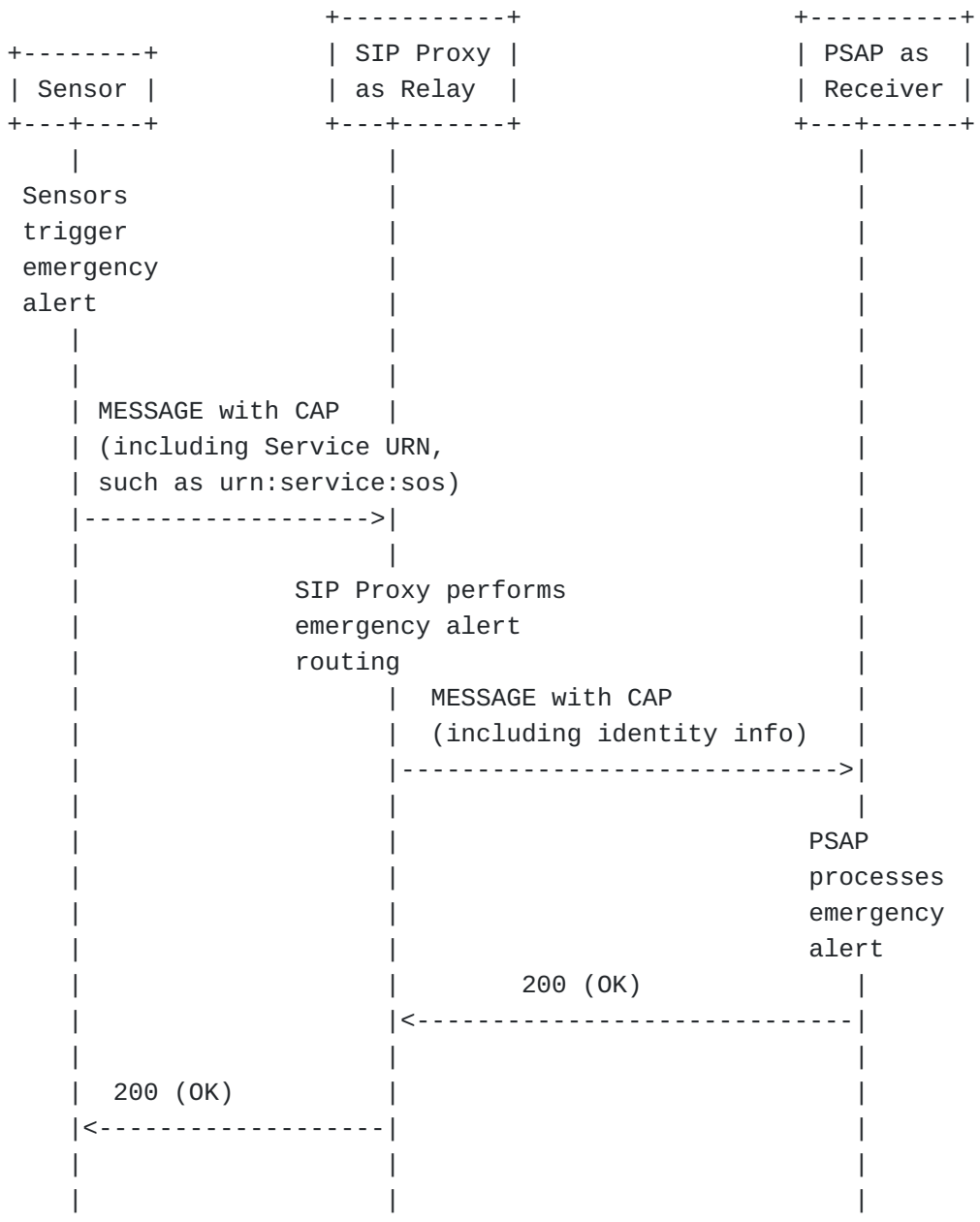

Figure 2: Location-Based Emergency Alert Routing

4. Protocol Specification

TOC

4.1. CAP Transport

TOC

Since alerts structured via CAP require a "push" medium, they SHOULD be sent via the SIP MESSAGE. The MIME type is set to 'application/common-alerting-protocol+xml'.

> Alternatively, the SIP PUBLISH mechanism or other SIP messages could be used. However, the usage of SIP MESSAGE is a simple enough approach from an implementation point of view.

4.2. Profiling of the CAP Document Content

TOC

The usage of CAP MUST conform to the specification provided with [cap] (Jones, E. and A. Botterell, "Common Alerting Protocol v. 1.1," October 2005.). For the usage with SIP the following additional requirements are imposed:

> **sender:** When the CAP was created by a SIP-based entity then the element MUST be populated with the SIP URI of that entity.
>
> **incidents:** The <incidents> element MUST be present whenever there is a possibility that alert information needs to be updated. The initial message will then contain an incident identifier carried in the <incidents> element. This incident identifier MUST be chosen in such a way that it is unique for a given <sender, expires, incidents> combination. Note that the <expires> element is optional and may not be present.
>
> **scope:** The value of the <scope> element MUST be set to "private" as the alert is not meant for public consumption. The <addresses> element is, however, not used by this specification since the message routing is performed by SIP and the respective address information is already available in the geolocation header. Populating location information twice into different parts of the message can quickly lead to inconsistency.
>
> **parameter:** The <parameter> element MAY contain additional information specific to the sensor.
>
> **area:** It is RECOMMENDED to omit this element when constructing a message. In case that the CAP message already contained an <area> element then the specified location information MUST be copied into the PIDF-LO structure of the geolocation header element.

5. Example

TOC

Figure 3 (Example Message conveying an Alert) shows a CAP document indicating a BURLARY alert issued by a sensor with the identity 'sensor1@domain.com'. The location of the sensor can be obtained from the attached geolocation information provided via the geolocation header contained in the SIP MESSAGE structure. Additionally, the sensor provided some data long with the alert message using proprietary information elements only to be processed by the receiver, a SIP entity acting as an aggregator. This example reflects the description in Figure 1 (Targeted Emergency Alert Routing).

```
 MESSAGE sip:aggregator@domain.com SIP/2.0
 Via: SIP/2.0/TCP sensor1.domain.com;branch=z9hG4bK776sgdkse
 Max-Forwards: 70
 From: sip:sensor1@domain.com;tag=49583
 To: sip:aggregator@domain.com
 Call-ID: asd88asd77a@1.2.3.4
 Geolocation: <cid:abcdef@domain.com>
   ;routing-allowed=yes
 Supported: geolocation
 Accept: application/pidf+xml, application/common-alerting-protocol+xml
 CSeq: 1 MESSAGE
 Content-Type: multipart/mixed; boundary=boundary1
 Content-Length: ...

 --boundary1

 Content-Type: common-alerting-protocol+xml
 Content-ID: <abcdef2@domain.com>
<?xml version="1.0" encoding="UTF-8"?>

<alert xmlns="urn:oasis:names:tc:emergency:cap:1.1">
  <identifier>S-1</identifier>
  <sender>sip:sensor1@domain.com</sender>
  <sent>2008-11-19T14:57:00-07:00</sent>
  <status>Actual</status>
  <msgType>Alert</msgType>
  <scope>Private</scope>
  <incidents>abc1234</incidents>
  <info>
      <category>Security</category>
      <event>BURGLARY</event>
      <urgency>Expected</urgency>
      <certainty>Likely</certainty>
      <severity>Moderate</severity>
      <senderName>SENSOR 1</senderName>
      <parameter>
        <valueName>SENSOR-DATA-NAMESPACE1</valueName>
        <value>123</value>
      </parameter>
      <parameter>
        <valueName>SENSOR-DATA-NAMESPACE2</valueName>
        <value>TRUE</value>
      </parameter>
  </info>
 </alert>

 --boundary1
```

```
Content-Type: application/pidf+xml
Content-ID: <abcdef2@domain.com>
<?xml version="1.0" encoding="UTF-8"?>
   <presence xmlns="urn:ietf:params:xml:ns:pidf"
       xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
       xmlns:cl="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
       xmlns:gml="http://www.opengis.net/gml"
       entity="pres:sensor1@domain.com">
     <tuple id="12345">
      <dm:device id="sensor1">
       <gp:geopriv>
         <gp:location-info>
           <gml:location>
             <gml:Point srsName="urn:ogc:def:crs:EPSG::4326">
               <gml:pos>32.86726 -97.16054</gml:pos>
             </gml:Point>
            </gml:location>
         </gp:location-info>
         <gp:usage-rules>
           <gp:retransmission-allowed>yes
           </gp:retransmission-allowed>
           <gp:retention-expiry>2010-07-30T20:00:00Z
           </gp:retention-expiry>
         </gp:usage-rules>
         <gp:method>802.11</gp:method>
        </gp:geopriv>
       <dm:deviceID>mac:1234567890ab</dm:deviceID>
       <dm:timestamp>2010-07-28T20:57:29Z</dm:timestamp>
      </dm:device>
     </tuple>
   </presence>

--boundary1--
```

Figure 3: Example Message conveying an Alert

---

6. Security Considerations

TOC

This section discusses security considerations when using SIP to make data-only emergency alerts utilizing CAP. Location specific threats are not unique to this document and the discussion in [I-D.ietf-ecrit-trustworthy-location] (Tschofenig, H., Schulzrinne, H., and B. Aboba, “Trustworthy Location Information,” October 2010.).

6.1. Forgery

TOC

Threat:

An adversary could forge or alter a CAP document to report false emergency alarms.

Countermeasures:

To avoid this kind of attack, the entities must assure that proper mechanisms for protecting the CAP documents are employed, e.g., signing the CAP document itself. Section 3.3.2.1 of [cap] (Jones, E. and A. Botterell, “Common Alerting Protocol v. 1.1,” October 2005.) specifies the signing of CAP documents. This does not protect against a legitimate sensor sending phrank alerts after being compromised.

6.2. Replay Attack

TOC

Threat:

An adversary could eavesdrop alerts and reply them at a later time.

Countermeasures:

A CAP document contains the mandatory <identifier>, <sender>, <sent> elements and an optional <expire> element. These attributes make the CAP document unique for a specific sender and provide time restrictions. An entity that has received a CAP message already within the indicated timeframe is able to detect a replayed message and, if the content of that message is unchanged, then no additional security vulnerability is created. Additionally, it is RECOMMENDED to make use of SIP security mechanisms, such as SIP Identity [RFC4474] (Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” August 2006.), to tie the CAP message to the SIP message.

6.3. Injecting False Alerts

TOC

Threat:

When an entity receives a CAP message it has to determine whether the entity distributing the CAP messages is genuine to avoid accepting messages that are injected by adversaries. In scenario

Countermeasures:

For some types of data-only emergency calls author/originator and the receiver/recipient have a relationship with each other and hence it is possible (using cryptographic techniques) to verify whether a message was indeed issued by an authorized entity. Figure 1 (Targeted Emergency Alert Routing) is such an environment. Standard SIP security mechanisms can be re-used for this purpose. For example, identity based access control is a viable approach utilizing the asserted identity of the alert originator using P-Asserted-Identity [RFC3325] (Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks," November 2002.) or SIP Identity [RFC4474] (Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)," August 2006.).

There are, however, other types of data-only emergency calls where there is no such relationship between the author/originator and the receiver/recipient. Incoming alerts need to be treated more carefully than multi-media emergency calls that contain additional information, such as audio, to allow a call taker to sort out phrank calls.

---

7. IANA Considerations

TOC

7.1. Registration of the 'application/common-alerting-protocol+xml' MIME type

TOC

To: ietf-types@iana.org

Subject: Registration of MIME media type application/ common-alerting-protocol+xml

MIME media type name: application

MIME subtype name:
common-alerting-protocol+xml

Required parameters: (none)

Optional parameters: charset; Indicates the character encoding of enclosed XML. Default is UTF-8 [RFC3629] (Yergeau, F., "UTF-8, a transformation format of ISO 10646," November 2003.).

Encoding considerations: Uses XML, which can employ 8-bit characters, depending on the character encoding used. See RFC 3023 [RFC3023] (Murata, M., St. Laurent, S., and D. Kohn, "XML Media Types," January 2001.), Section 3.2.

Security considerations: This content type is designed to carry payloads of the Common Alerting Protocol (CAP).

Interoperability considerations: This content type provides a way to convey CAP payloads.

Published specification: RFC XXX [Replace by the RFC number of this specification].

Applications which use this media type: Applications that convey alerts and warnings according to the CAP standard.

Additional information: OASIS has published the Common Alerting Protocol at http://www.oasis-open.org/committees/documents.php&wg_abbrev=emergency

Person & email address to contact for further information: Hannes Tschofenig, Hannes.Tschofenig@nsn.com

Intended usage: Limited use

Author/Change controller: IETF SIPPING working group

Other information: This media type is a specialization of application/xml RFC 3023 [RFC3023] (Murata, M., St. Laurent, S., and D. Kohn, "XML Media Types," January 2001.), and many of the considerations described there also apply to application/common-alerting-protocol+xml.

---

8. Acknowledgments

TOC

The authors would like to thank the participants of the Early Warning adhoc meeting at IETF#69 for their feedback. Additionally, we would

like to thank the members of the NENA Long Term Direction Working Group for their feedback.

9. References

TOC

9.1. Normative References

TOC

[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.
[cap]	Jones, E. and A. Botterell, “Common Alerting Protocol v. 1.1,” October 2005.
[RFC3265]	Roach, A., “Session Initiation Protocol (SIP)-Specific Event Notification,” RFC 3265, June 2002 (TXT).
[RFC3903]	Niemi, A., “Session Initiation Protocol (SIP) Extension for Event State Publication,” RFC 3903, October 2004 (TXT).
[RFC3023]	Murata, M., St. Laurent, S., and D. Kohn, “XML Media Types,” RFC 3023, January 2001 (TXT).
[RFC3629]	Yergeau, F., “UTF-8, a transformation format of ISO 10646,” STD 63, RFC 3629, November 2003 (TXT).
[I-D.ietf-ecrit-trustworthy-location]	Tschofenig, H., Schulzrinne, H., and B. Aboba, “Trustworthy Location Information,” draft-ietf-ecrit-trustworthy-location-01 (work in progress), October 2010 (TXT).

9.2. Informative References

TOC

[I-D.ietf-ecrit-phonebcp]	Rosen, B. and J. Polk, “Best Current Practice for Communications Services in support of Emergency Calling,” draft-ietf-ecrit-phonebcp-15 (work in progress), July 2010 (TXT).
[I-D.ietf-atoca-requirements]	Schulzrinne, H., Norreys, S., Rosen, B., and H. Tschofenig, “Requirements, Terminology and Framework for Exigent Communications,” draft-ietf-atoca-requirements-00 (work in progress), September 2010 (TXT).
[RFC4474]	Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” RFC 4474, August 2006 (TXT).
[RFC3325]	Jennings, C., Peterson, J., and M. Watson, “Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks,” RFC 3325, November 2002 (TXT).

Authors' Addresses

TOC

	Brian Rosen
	NeuStar, Inc.
	470 Conrad Dr
	Mars, PA 16046
	US
Phone:	
Email:	br@brianrosen.net
	Henning Schulzrinne
	Columbia University
	Department of Computer Science
	450 Computer Science Building
	New York, NY 10027
	US
Phone:	+1 212 939 7004
Email:	hgs+ecrit@cs.columbia.edu
URI:	http://www.cs.columbia.edu
	Hannes Tschofenig
	Nokia Siemens Networks
	Linnoitustie 6
	Espoo 02600
	Finland

Phone:	+358 (50) 4871445
Email:	Hannes.Tschofenig@gmx.net
URI:	http://www.tschofenig.priv.at