ECRIT
Internet-Draft
Intended status: Experimental
Expires: March 25, 2011

B. Rosen
NeuStar, Inc.
H. Schulzrinne
Columbia U.
H. Tschofenig
Nokia Siemens Networks
September 21, 2010

Common Alerting Protocol (CAP) based Data-Only Emergency Alerts using the Session Initiation Protocol (SIP)
draft-ietf-ecrit-data-only-ea-00.txt

Abstract

The Common Alerting Protocol (CAP) 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 alerts allow to utilize the same 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 March 25, 2011.

Copyright Notice

Table of Contents

1. Introduction

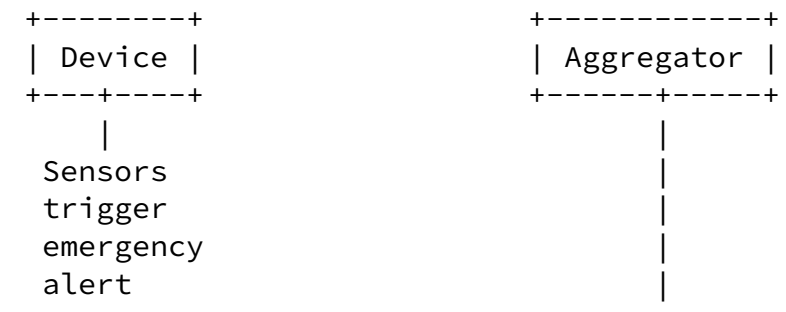
The Common Alerting Protocol (CAP) [cap] is an XML document format for exchanging emergency alerts and public warnings. CAP is mainly used for conveying alerts and warnings between authorities and from authorities to citizen/individuals. This document describes how data-only emergency calls are able to utilize the same CAP document format. Data-only emergency alerts may be similar to regular emergency calls in the sense that they have the same emergency call routing and location requirements; they do, however, not lead to the establishment of a voice channel. There are, however, data-only emergency alerts that are targeted directly to a dedicated entity responsible for evaluating the alerts and for taking the necessary steps, including triggering an emergency call towards a Public Safety Answering Point (PSAP).

2. 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 RFC 2119 [RFC2119].

3. Architectural Overview

This section illustrates two envisioned usage modes; targeted and location-based emergency alert routing. Figure 1 shows a deployment variant where a device is pre-configured (using techniques outside the scope of this document) to issue an alert to an aggregator that processes these messages and performs whatever steps are necessary to appropriately react on the alert. In many cases the device has the address of the aggregator pre-configured and corresponding security mechanisms are in place to ensure that only alert from authorized devices are processed.



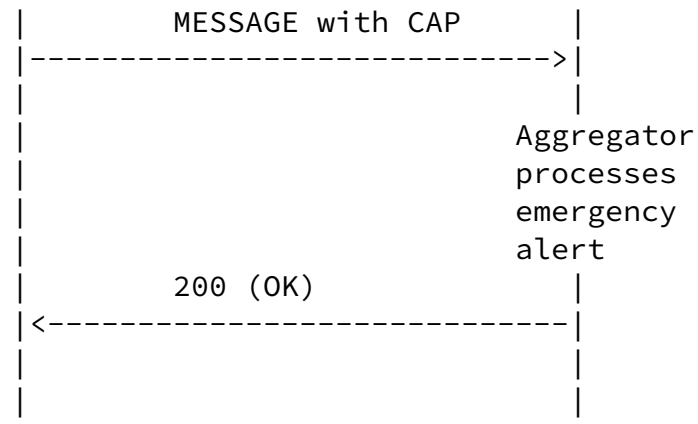
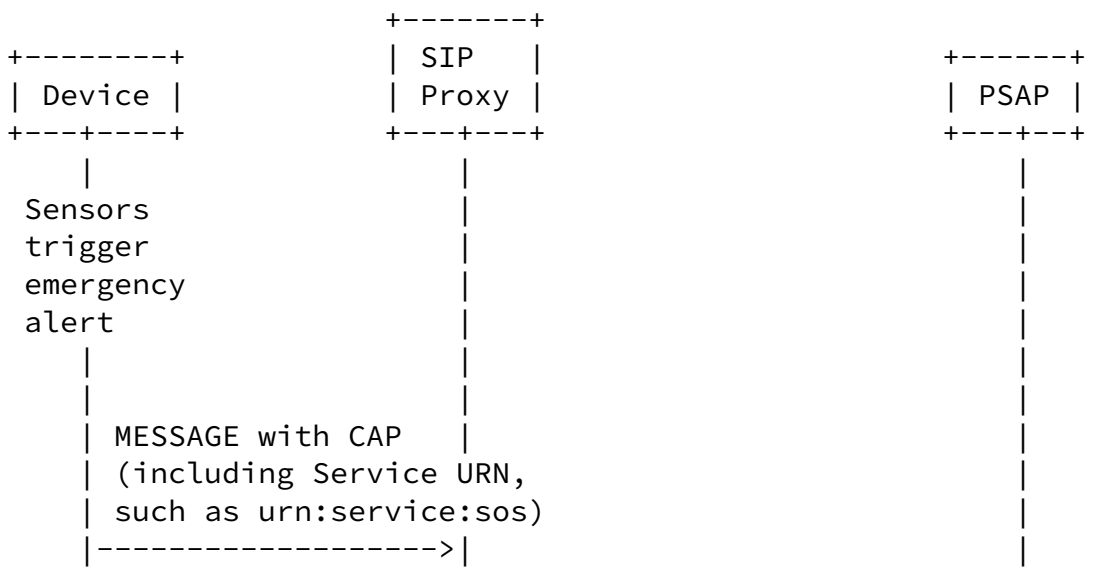


Figure 1: Targeted Emergency Alert Routing

In Figure 2 a scenario is shown whereby the alert is routed using location information and the Service URN. In this case the device issuing the alert may not know the message recipient (in case the LoST resolution is done at an emergency services routing proxy rather than at the end host). In any case, a trust relationship between the alert-issuing device and the PSAP cannot be assumed, i.e., the PSAP is likely to receive alerts from entities it cannot authorize. This scenario corresponds more to the classical emergency services classical and the description in [I-D.ietf-ecrit-phonebcp] is applicable.



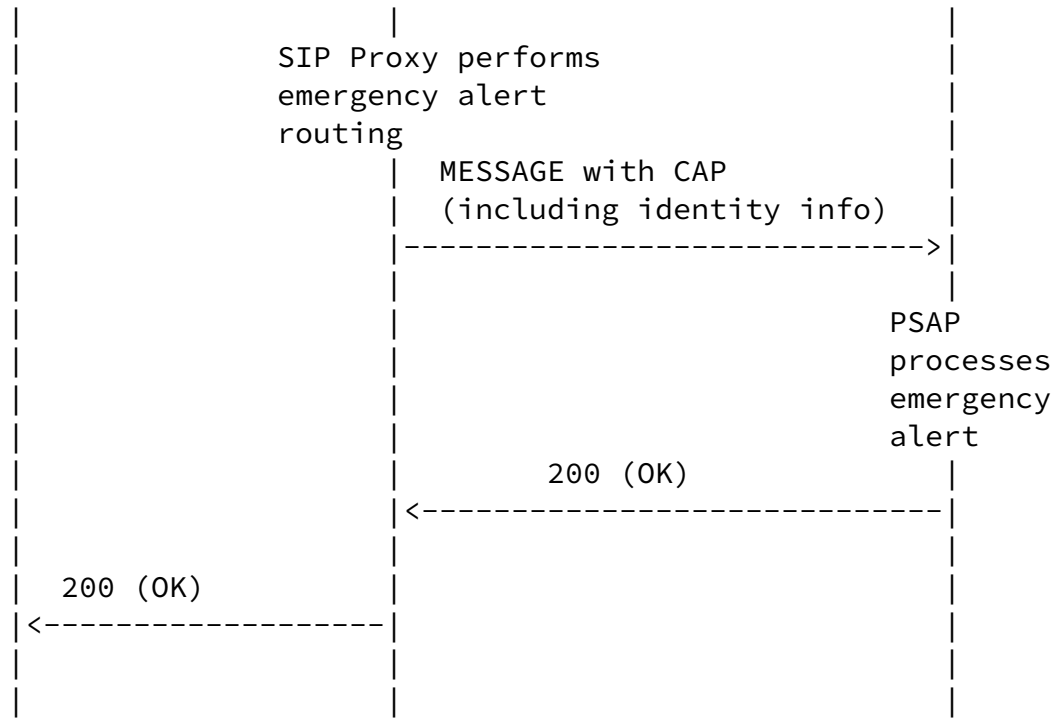


Figure 2: Location-Based Emergency Alert Routing

4. Protocol Specification

4.1. CAP Transport

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

The usage of CAP MUST conform to the specification provided with [cap]. 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 combination.

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 there. Populating address 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: For geodetic information the polygon and circle location shapes are available. The ability to conveying a structured format of civic location information is missing and hence civic information is encoded as a text string in the <areaDesc> element.

5. Example

Figure 3 shows a CAP document indicating a BURLARY alert issued by sensor1@example.com indicating that the alert was issued from the civic address NATURAL HISTORY MUSEUM, BURGRING 7, 1010 VIENNA, AUSTRIA. Additionally, the sensor provided some additional data long with the alert message using non-standardized information elements.

```
<?xml version="1.0" encoding="UTF-8"?>

<alert xmlns="urn:oasis:names:tc:emergency:cap:1.1">
    <identifier>S-1</identifier>
    <sender>sensor1@example.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>
        <area>
            <areaDesc>NATURAL HISTORY MUSEUM,
             BURGRING 7, 1010 VIENNA, AUSTRIA
            </areaDesc>
        </area>
        <parameter>
          <valueName>SENSOR-DATA-NAMESPACE1</valueName>
          <value>123</value>
        </parameter>
        <parameter>
          <valueName>SENSOR-DATA-NAMESPACE2</valueName>
          <value>TRUE</value>
        </parameter>
    </info>
</alert>
```

Figure 3: Example for an alert triggered by a sensor

6. Security Considerations

This section discusses security considerations when using SIP to make data-only emergency alerts utilizing CAP.

6.1. Forgery

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] specifies the signing of CAP documents. This does not protect against a legitimate sensor sending phrank alerts after being compromised.

6.2. Replay Attack

Threat:

Theft of CAP documents described in this document and replay of it 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, to tie the CAP message to the SIP message.

6.3. Injecting False Alerts

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.

Countermeasures:

For some types of data-only emergency calls the entity issuing the alert and the entity consuming the alert have a relationship with each other and hence it is possible (using cryptographic authentication) to verify whether a message was indeed issued by an authorized entity. There are, however, other types of data-only emergency calls where there is no such relationship between the sender and the consumer. In that case incoming alerts need to be treated more carefully, as the possibilities to place phrank calls are higher than with regular emergency calls that at least setup an audio channel.

7. IANA Considerations

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

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].

Encoding considerations: Uses XML, which can employ 8-bit characters, depending on the character encoding used. See RFC 3023 [RFC3023], 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], and many of the considerations described there also apply to application/common-alerting-protocol+xml.

8. Acknowledgments

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

9.1. Normative References

[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.

[RFC3903] Niemi, A., "Session Initiation Protocol (SIP) Extension for Event State Publication", RFC 3903, October 2004.

[RFC3023] Murata, M., St. Laurent, S., and D. Kohn, "XML Media Types", RFC 3023, January 2001.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

9.2. Informative References

[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.

Authors' Addresses

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