ECRIT	J. Kim	
Internet-Draft	W. Song	
Intended status: BCP	H. Schulzrinne	
Expires: May 21, 2010	Columbia University	
	P. Boni	
	M. Armstrong	
	Verizon	
	November 17, 2009	

TOC

Emergency Text Messaging using SIP MESSAGE
draft-kim-ecrit-text-00

Abstract

This memo describes best current practices on how to use the SIP MESSAGE method for emergency text messaging from citizen and visitors to authorities.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.
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.”
The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.
The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.
This Internet-Draft will expire on May 21, 2010.

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 BSD License.

Table of Contents

1. Terminology
2. Introduction
3. Overview of operation
4. Caller UAC Processing
5. Proxy Processing
6. Conversion to SIP MESSAGE
7. Security Considerations
8. IANA Considerations
9. Normative References
§ Authors' Addresses

---

1. Terminology

TOC

This document uses terms from [I-D.ietf-ecrit-framework] (Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, “Framework for Emergency Calling using Internet Multimedia,” July 2009.) and [RFC3428] (Campbell, B., Ed., Rosenberg, J., Schulzrinne, H., Huitema, C., and D. Gurle, “Session Initiation Protocol (SIP) Extension for Instant Messaging,” December 2002.).
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 (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.) [RFC2119].

---

2. Introduction

TOC

The SIP MESSAGE method [RFC3428] (Campbell, B., Ed., Rosenberg, J., Schulzrinne, H., Huitema, C., and D. Gurle, “Session Initiation Protocol (SIP) Extension for Instant Messaging,” December 2002.) is used for page-mode messaging. In page mode, each individual message is sent independently and not as part of any session. On the other hand, there are session-mode text messaging standards such as the Message Session Relay Protocol (MSRP) [RFC4975] (Campbell, B., Ed., Mahy, R., Ed., and C. Jennings, Ed., “The Message Session Relay Protocol (MSRP),”

September 2007.) and Real Time Text (RTT) [RFC5194] (van Wijk, A., Ed. and G. Gybels, Ed., "Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP)," June 2008.) where every message is part of a session with a definite start and end. Which mode to use in an emergency depends on what the endpoint is capable of.

This document describes how the SIP MESSAGE method is used to support emergency text messaging within the framework described in [I-D.ietf-ecrit-framework] (Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling using Internet Multimedia," July 2009.). The existing framework does not consider methods that do not create a session or are not a part of it. The main difference between the existing framework and the MESSAGE approach is in the way the proxies handle SIP MESSAGE methods.

This document assumes that the Emergency Services network (ESInet) and PSAPs are SIP-based infrastructures. However, the caller-facing access network may or may not be IP based. Emergency messages may be sent end-to-end using the SIP MESSAGE method, or it may be in a different format and protocol in the caller side and have to be converted to SIP MESSAGE somewhere along the path towards the call taker. Therefore, we also describe recommendations on how a SIP MESSAGE is formed from non-SIP text protocols.

Presence is beyond the scope of this document.

3. Overview of operation

TOC

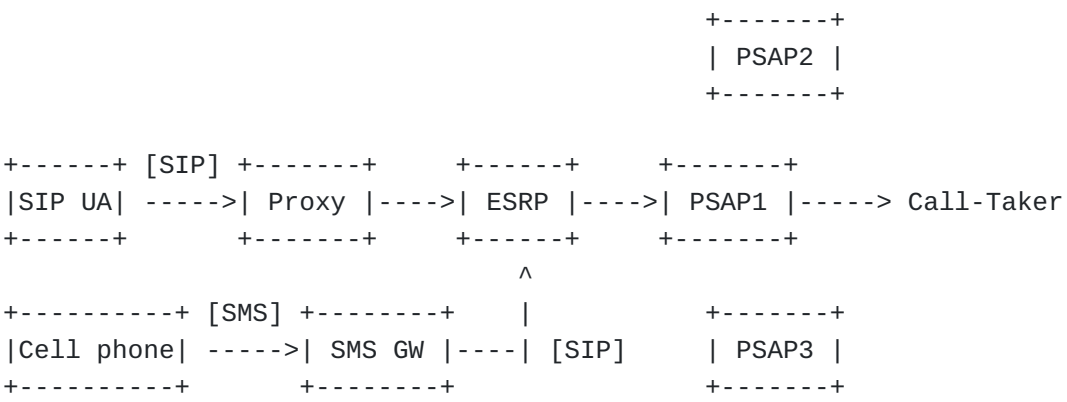

Figure 1: Emergency Text Flow

Emergency text communication may utilize SIP MESSAGE end-to-end from the caller's end device or application to the call taker, or may start

as another form of text messaging scheme such as SMS but ultimately be converted to a SIP MESSAGE. Text handling after the conversion is the same. In any case, the MESSAGE request is constructed as described in [RFC3428] (Campbell, B., Ed., Rosenberg, J., Schulzrinne, H., Huitema, C., and D. Gurle, "Session Initiation Protocol (SIP) Extension for Instant Messaging," December 2002.). The body of the request contains the message to be delivered. Then the values for various emergency header fields are filled as stated in [I-D.ietf-ecrit-framework] (Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling using Internet Multimedia," July 2009.). If the location information is appended to the body of the request, the caller's message and the location information must be inserted into the body of the request as multiple MIME attachments. These are explained in more detail in Section 4 (Caller UAC Processing).

The main difference of this approach from both the traditional SIP MESSAGE routing and the emergency framework is in the way the MESSAGE is handled along the path. In emergency handling, the path that the first MESSAGE request takes is important. Subsequent MESSAGE requests from the same person or device must follow the same path as the first one so that they are delivered correctly to the same call taker. Otherwise, if subsequent MESSAGE requests are delievered to another call taker or another PSAP, there will be considerable confusion for both the sender and the receiver. Therefore, the path of the first MESSAGE request is determined by location and/or local policy, but all subsequent MESSAGE requests must follow the path of the first request regardless of location or local policy.

This means that entities within the path that determine the next hop based on location or local policy need to keep track of MESSAGE requests that it forwards. Emergency Service Routing Proxy [I-D.ietf-ecrit-framework] (Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling using Internet Multimedia," July 2009.) is an example of such entity. How such proxy behaves is described in Section 5 (Proxy Processing). However, this behavior is not confined to proxies. SIP UAs and call distributing entities within the PSAPs are also affected. If the SIP UA does not keep track of MESSAGE requests, then it would query LoST [RFC5222] (Hardie, T., Newton , A., Schulzrinne , H., and H. Tschofenig , "LoST: A Location-to-Service Translation Protocol," August 2008.) everytime a MESSAGE is sent. This is a big problem if the caller is moving while sending messages. The SIP UA may send the MESSAGE requests to different PSAPs. Call distributing entities need to keep track of MESSAGE requests so that requests from one caller is forwarded consistently to one call taker. For these entities, the same state-keeping mechanisms described in Section 5 (Proxy Processing) can be used.

When the call taker sends a reply to the caller, the application constructs a SIP MESSAGE request without location or other special header fields used in emergency and sends it towards the caller. The reply follows the normal SIP routing path. If the caller's original message was not SIP, then the replies from call taker must also be

converted from SIP MESSAGE request to the original message format and tranport protocol. As an example, if the caller's original message was an SMS message, then the call taker's reply may have to be converted to an SMS message so that the caller can receive it on his/her cell phone. There may be other protocols, such as proprietary IM protocols, that may need conversion. Gateways, such as the SMS gateway shown in Figure 1 (Emergency Text Flow), handles these conversions. Conversion is described in Section 6 (Conversion to SIP MESSAGE).

---

4. Caller UAC Processing

TOC

Caller UAC follows the rules of SIP MESSAGE [RFC3428] (Campbell, B., Ed., Rosenberg, J., Schulzrinne, H., Huitema, C., and D. Gurle, "Session Initiation Protocol (SIP) Extension for Instant Messaging," December 2002.) and those of [I-D.ietf-ecrit-framework] (Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling using Internet Multimedia," July 2009.). The following description of caller UAC processing is derived from the union of the two documents mentioned earlier.
The UAC may include location information in the body as type "xml/pidf-lo" with a corresponding Geolocation header field, or include a reference to the location information in the Geolocation header field as specified in [I-D.ietf-sip-location-conveyance] (Polk, J. and B. Rosen, "Location Conveyance for the Session Initiation Protocol," July 2009.). In the former case, the UAC needs to include both the sender's message and the location information in one body. To do so, the UAC must use multipart MIME. Here is an example:

```
----- =_RjhENkI3RjQ4NUE0QjI2Q0VEODdGNjIwMkMwNjZC
MIME-Version: 1.0
Content-ID: <3252.1224700600.5@NG911_Desktop1>
Content-Type: text/plain
Content-Transfer-Encoding: 8bit

Hello, I need help.

----- =_RjhENkI3RjQ4NUE0QjI2Q0VEODdGNjIwMkMwNjZC
MIME-Version: 1.0
Content-ID: caller@x.y
Content-Type: application/pidf+xml
Content-Transfer-Encoding: UTF-8

<?xml version="1.0" encoding="ISO-8859-1"?>
<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:civicLoc"
  entity="sip:caller@x.y">
  <tuple id="id94954">
    <status>
      <gp:geopriv>
        <gp:location-info>
          <cl:civicAddress>
            <cl:country>us</cl:country>
            <cl:A1>ny</cl:A1>
            <cl:A3>new york</cl:A3>
            <cl:A6>amsterdam</cl:A6>
            <cl:HNO>1214</cl:HNO>
            <cl:PC>10027</cl:PC>
          </cl:civicAddress>
        </gp:location-info>
        <gp:method>Manual</gp:method>
      </gp:geopriv>
    </status>
    <contact priority="1.0">sip:caller@x.y</contact>
    <timestamp>2008-11-14T19:43:43Z</timestamp>
  </tuple>
</presence>
----- =_RjhENkI3RjQ4NUE0QjI2Q0VEODdGNjIwMkMwNjZC
```

The UAC should resolve the location to a URI by querying LoST [RFC5222] (Hardie, T., Newton , A., Schulzrinne , H., and H. Tschofenig , “LoST: A Location-to-Service Translation Protocol,” August 2008.) and should include the URI in the Route header field. This should be done only once in the beginning of conversation to make sure all subsequent MESSAGE requests follow the same next-hop as the first request. If the

UAC is not able to resolve the location, then it should not include a Route header field.
It is out of the scope of this document to decide when the conversation begins or ends. The UAC may use a user-interface-based approach for this, i.e., start a new conversation when the user opens a new chat window, and then terminate the conversation when the user closes that window. However, this is only an example.
If the UAC receives a non-200 response, it should notify the sender of the response and give the sender the option of dialing the emergency number instead of sending another MESSAGE request.

---

5. Proxy Processing

TOC

As described in Section 3 (Overview of operation), proxies that determine the next hop of an emergency request based on location or local policy need to keep track of MESSAGE requests it handles. On the other hand, proxies that foward MESSAGE requests based on the To header field or the Route header field do not need to keep track since the MESSAGE requests will be delivered consistently.
The proxies that need to track MESSAGE requests, e.g., the Emergency Services Routing Proxy [I-D.ietf-ecrit-framework] (Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, "Framework for Emergency Calling using Internet Multimedia," July 2009.), MUST perform additional record keeping for MESSAGE requests if all of the following conditions are met.

1. The destination (obtained from the To header field) is urn:service:sos.

2. This is the first MESSAGE from a particular source (obtained from the From header field). In other words, the proxy has no record of the source sending a MESSAGE to urn:service:sos.

The record is a (source, next-hop, expiration timer) triplet. The source is obtained from the From header field of the request. The next-hop is determined by a LoST query [RFC5222] (Hardie, T., Newton , A., Schulzrinne , H., and H. Tschofenig , "LoST: A Location-to-Service Translation Protocol," August 2008.) based on the location information or a reference to the location information within the first request. Location information in subsequent requests do not affect the next-hop value. The expiration timer is a value in seconds that will keep the record from expiring. Each subsequent request resets the expiration timer. For example, if the configured value of the expiration timer is 30 seconds, then the countdown begins after the first request is processed. When the second request comes in, the expiration timer is reset to 30 seconds and the countdown starts again. If the timer falls to zero, the record is no longer valid.

Proxies route all subsequent MESSAGE request from the same source to the same next-hop while the expiration timer is greater than zero. Each subsequent MESSAGE request resets the expiration timer to its maximum value. This is to ensure that a 'conversation' between the caller and the call taker is consistent.

---

6. Conversion to SIP MESSAGE

TOC

The original message may not be SIP. It may be an SMS message or an IM message in a proprietary format and protocol. In these cases, the original format and protocol must be converted to a SIP MESSAGE.
The following is the minimum information needed to convert a non-SIP message to a valid SIP MESSAGE.

Type of Information	**Correspoding SIP MESSAGE element**
Origination address or number	From header field
User message	In the body as type "text/plain"
Location information	Geolocation header field and in the body as type "xml/pidf-lo" (Geolocation header field only if conveying location by reference)

The SIP URI for the From header field must be created by merging the origination address or number and the IP address and port of the converting entity. For example, let's say the origination address or number is 123-456-7890 and the IP address and port number of the converting entity is 128.59.19.184:5060. Then the SIP URI should be sip:1234567890@128.59.19.184:5060.
The To header field must contain an emergency string such as "urn:service:sos". The destination address or number, e.g., 9-1-1, in the original non-SIP message is retained and carried along with the SIP message in the History-Info header [RFC4244] (Barnes, M., Ed., “An Extension to the Session Initiation Protocol (SIP) for Request History Information,” November 2005.). The destination address could be useful in post incident call analysis for PSAP personnel to identify network issues such as mis-routed text messages allowing more efficient trouble clearing with the appropriate network provider.
The next hop entity should be determined by quering LoST with the provided location information and it should be included in the Route header field.
If the converter receives a 200 OK response, it should send a success indicator to the original sender. There may not be a one-to-one match between SIP responses and the original protocol, especially when

non-200 responses are received. In this case, the converter must indicate failure and may send the reason text as a message to the sender.
The call taker's reply, which is another SIP MESSAGE request in the reverse direction, should be sent to the origination address or number in its original format. The origination address or number can be extracted from the To header field. The From header field may contain "urn:service:sos", in which case it must be replaced with the original emergency number or string.
If the sender protocol allows provisional and final responses, the converter should make use of them to indicate the status of the call taker. For example, the converter should send a 202 Accepted response upon receiving the call taker's MESSAGE, and then a 200 OK upon receiving the final success indication from the sender. If the sender protocol does not allow such elaborate responses, the converter must send a 200 OK upon receiving the call taker's MESSAGE.

---

7. Security Considerations

TOC

TBD

---

8. IANA Considerations

TOC

This memo includes no request to IANA.

---

9. Normative References

TOC

[I-D.ietf-ecrit-framework]	Rosen, B., Schulzrinne, H., Polk, J., and A. Newton, “Framework for Emergency Calling using Internet Multimedia,” July 2009.
[I-D.ietf-sip-location-conveyance]	Polk, J. and B. Rosen, “Location Conveyance for the Session Initiation Protocol,” July 2009.
[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC3428]	Campbell, B., Ed., Rosenberg, J., Schulzrinne, H., Huitema, C., and D. Gurle, “Session Initiation Protocol (SIP) Extension for Instant Messaging,” December 2002.
[RFC4244]	

	Barnes, M., Ed., “An Extension to the Session Initiation Protocol (SIP) for Request History Information,” November 2005.
[RFC4975]	Campbell, B., Ed., Mahy, R., Ed., and C. Jennings, Ed., “The Message Session Relay Protocol (MSRP),” September 2007.
[RFC5194]	van Wijk, A., Ed. and G. Gybels, Ed., “Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP),” June 2008.
[RFC5222]	Hardie, T., Newton , A., Schulzrinne , H., and H. Tschofenig , “LoST: A Location-to-Service Translation Protocol,” August 2008.

Authors' Addresses

TOC

	Jong Yul Kim
	Columbia University
	New York, NY
	USA
Email:	jyk@cs.columbia.edu
	Wonsang Song
	Columbia University
	New York, NY
	USA
Email:	wonsang@cs.columbia.edu
	Henning Schulzrinne
	Columbia University
	New York, NY
	USA
Email:	hgs@cs.columbia.edu
	Piotr Boni
	Verizon
Email:	p.boni@verizon.com
	Michael Armstrong
	Verizon
Email:	michael.g.armstrong@verizon.com