Session Initiation Protocol Location Conveyance

October 27th, 2003

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

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.

Abstract

This document presents the framework and requirements for an extension to the Session Initiation Protocol (SIP) [1] for conveyance of user location information from a Session Initiation Protocol (SIP) user agent to another SIP entity. We consider cases where location information is conveyed from end to end, as well as cases where message routing by intermediaries is influenced by the location of the session initiator.
1. Introduction

This document presents the framework and requirements for an extension to the Session Initiation Protocol (SIP) [1] for conveyance of user location information object described by [7] from a SIP User Agent to another SIP entity.

There are several situations in which it is appropriate for SIP to be used to convey Location Information (LI) from one SIP entity to another. This document specifies requirements when a SIP UAC knows its location by some means not specified herein, and needs to inform another SIP entity. One example is to reach your nearest pizza parlor. A chain of pizza parlors may have a single well known uri (sip:pizzaparlor.com), that is forwarded to the closest franchise by the pizzaparlor.com proxy server. The receiving franchise UAS uses the location information of the UAC to schedule your delivery.

Another important example is emergency calling. A call to sip:sos@example.com is an emergency call as in [3]. The example.com proxy server must route the call to the correct emergency response center (ERC) determined by the location of the caller. At the ERC, the UAS must determine the correct police/fire/ambulance/... service, which is also based on your location. In many jurisdictions, accurate location information is a required component of a call to an emergency center.

A third example is a direction service, which might give you verbal directions to a venue from your present position. This is a case where only the destination UAS needs to receive the location information.

This document does not discuss how the UAC discovers or is
configured with its location (either coordinate based or civil based). It also does not discuss the contents of the Location Object (LO). It does specify the requirements for the "using protocol" in [7].

1.1 Conventions used in this document

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 [2].

1.2 Changes from -00 Version

This is a list of the changes that have been made from the -00 version of this ID:

- Brian Rosen was brought on as a co-author
- Requirements that a location header were negatively received in the previous version of this document. AD and chair advice was to move all location information into a message body (and stay away from headers)
- Added a section of "emergency call" specific requirements
- Added an Open Issues section to mention what hasn’t been resolved yet in this effort

2. In the Body or in a Header

When one user agent wants to inform another user agent where they are, it seems reasonable to have this accomplished by placing the location information (coordinate or civil) in an S/Mime registered and encoded message body, and sending it as part of a SIP request or response. No routing of the request based on the location information is required in this case; therefore no SIP Proxies between these two UAs need to view the location information contained in the SIP messages.

Although SIP [1] does not permit a proxy server to modify or delete a body, there is no restriction on viewing bodies. However, S/MIME protection implemented on bodies is only specified between UAS and UAC and if engaged, would render the location object opaque to a proxy server. This problem is similar to that raised in Session Policy [8], where an intermediary may need information in a body, such as IP address of media streams or codec choices to route a call properly. Requirements in [8] are applicable to routing based on
location, and are incorporated in these requirements by reference.

It is conceivable to create a new header for location information. However, [7] prefers S/MIME for security of Location Information, and indeed S/MIME is preferable in SIP for protecting one part of a message. Accordingly, these requirements specify location be carried in a body.

It is the use of S/MIME however, that limits routing based on location. Therefore, it seems appropriate to require that, where routing is dependent on location, protection of the location information object be accomplished by other mechanisms, probably TLS ("sips:" from [1]). It is envisioned that S/MIME SHOULD be used when location information is not required by proxy servers, and TLS SHOULD be used when it is.

This document does not address the behavior or configuration of SIP Proxy Servers in these cases in order to accomplish location-sensitive routing. That is out of scope, and left for further (complementary) efforts.

3. Scope of Location in a Message Body

If the location information is to be contained within a message body, and either another body (SDP for example) is also to be sent in the message, or the LO is to be protected with S/MIME, the rules stated in section 7 of [1] regarding multipart MIME bodies MUST be followed. The format and privacy/security rules of the location information SHOULD be defined within the Geopriv WG.

4. Requirements for UA-to-UA Location Conveyance

The following are the requirements for UA-to-UA Location Conveyance situations:

U-U1 - MUST work with dialog-initiating SIP Requests and responses, as well as the SIP MESSAGE method[4], and SHOULD work with most SIP messages.

U-U2 - UAC Location information SHOULD remain confidential in route to the destination UA

U-U3 - The privacy and security rules established within the Geopriv Working Group that would categorize SIP as a ‘using protocol’ MUST be met [7]
5. Requirements for UA-to-Proxy Server Location Conveyance

The following are the requirements for UA-to-Proxy Server Location Conveyance situations:

U-PS1 - MUST work with dialog-initiating SIP Requests and responses, as well as the SIP MESSAGE method[4], and SHOULD work with most SIP messages.

U-PS2 - UAC location information SHOULD remain confidential in route to the destination, but MUST be useable by intermediary proxy servers.

U-PS3 - The privacy and security rules established within the Geopriv Working Group which would categorize SIP as a 'using protocol' MUST be met [7]

U-PS4 - Modification or removal of the LO by proxy servers MUST NOT be required

U-PS5 - any mechanism used to prevent unwanted observation of this Location Header(s) CANNOT fail the SIP Request if not understood by intermediary SIP entities or the destination UAS

U-PS6 - It MUST be possible for a proxy server to assert the validity of the location information provided by the UA. Alternatively, it is acceptable for there to be a mechanism for a proxy server to assert a location object itself.

6. Additional Requirements for Emergency Calls

Emergency calls have requirements that are not generally important to other uses for location in SIP:

Emergency calls presently have between 2 and 8-second call setup times. There is ample evidence that the longer call setup end of the range causes an unacceptable number of callers to abandon the call before it is completed. Two-second call completion time is a goal of many existing emergency call centers. Allocating 25% of the call set up for processing privacy concerns seems reasonable; 1 second would be 50% of the goal, which seems unacceptable; less than 0.5 second seems unachievable, therefore:

E-1 - Privacy mechanisms MUST add no more than 0.5 second of call setup time when implemented in present technology UAs and Proxy Servers.

It may be acceptable for full privacy mechanisms related to the location of the UAC (and it's user) to be tried on an initial
attempt to place a call, as long as the call attempt may be retried without the mechanism if the first attempt fails. Abandoning privacy in cases of failure of the privacy mechanism might be subject to user preference, although such a feature would be within the domain of a UA implementation and thus not subject to standardization. It should be noted that some jurisdictions have laws that explicitly deny any expectation of location privacy when making an emergency call.

E-2 Â Privacy mechanisms MUST NOT be mandatory for successful conveyance of location during an (sos-type) emergency call.

E-3 Â The retention and retransmission policy of the ERC must be able to be made available to the user, and override the user’s normal policy when local regulation governs such retention and retransmission. As in E-2 above, requiring the use of the ERC’s retention and/or retransmission policy may be subject to user preference although in most jurisdictions, local laws specify such policies and may not be overridden by user preference.

7. Current Known Open issues

This is a list of open issues that have not yet been addressed to conclusion:

- Whether self signed S/MIME bodies can work in both directions in the emergency call scenario (to and from an ERC) as in [9]. It appears that document covers self-signed certs from the UA to ERC direction, but it is not clear it solves communications in the reverse direction.

- If S/MIME is chosen as a SHOULD (in general, vs. TLS), this doc might consider stipulating a special purpose Proxy (an "emergency services" proxy) that can process location information (a Geopriv LO) and route the message directly to the appropriate ERC.

At Issue: plain "vanilla" proxies probably won’t have the capabilities to route based on location information in the near future, but should that timing be considered here?

8. Security Considerations

Conveyance of geo-location of a UAC is problematic for many reasons. This document calls for that conveyance to normally be accomplished through secure message body means (like S/MIME or TLS). In cases where a session set-up is routed based on the location of the UAC initiating the session or SIP MESSAGE, securing the location with an end-to-end mechanism such as S/MIME is problematic.
9. IANA Considerations

There are no IANA considerations within this document at this time.

10. Acknowledgements

To Dave Oran for helping to shape this idea. To Jon Peterson and Dean Willis on guidance of the effort.

11. References - Normative


12. Author Information

James M. Polk  
Cisco Systems  
2200 East President George Bush Turnpike  
Richardson, Texas 75082 USA  
jmpolk@cisco.com

Brian Rosen  
Marconi Communications, Inc.  
2000 Marconi Drive  
Warrendale, PA 15086  
Brian.rosen@marconi.com

"Copyright (C) The Internet Society (February 23rd, 2001).  
All Rights Reserved.

This document and translations of it may be copied and furnished to  
others, and derivative works that comment on or otherwise explain it  
or assist in its implementation may be prepared, copied, published  
and distributed, in whole or in part, without restriction of any  
kind, provided that the above copyright notice and this paragraph  
are included on all such copies and derivative works. However, this  
document itself may not be modified in any way, such as by removing  
the copyright notice or references to the Internet Society or other  
Internet organizations, except as needed for the purpose of  
developing Internet standards in which case the procedures for  
copyrights defined in the Internet Standards process must be  
followed, or as required to translate it into languages other than  
English.

The limited permissions granted above are perpetual and will not be  
revoked by the Internet Society or its successors or assigns.

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

The Expiration date for this Internet Draft is:

April 27th, 2004