Internet Engineering Task Force
Internet Draft
Expiration: April 25th, 2005
File: draft-ietf-sipping-location-requirements-02.txt

James M. Polk
Cisco Systems
Brian Rosen
Emergicom

Requirements for Session Initiation Protocol Location Conveyance

October 25th, 2004

Status of this Memo

Copyright Notice

Abstract

This document presents the framework and requirements for usage of the Session Initiation Protocol (SIP) to convey user location information from one Session Initiation Protocol (SIP) entity 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. We offer a set of solutions to the requirements, based on the scenario(s) being addressed.

Table of Contents

1. Introduction

This document presents the framework and requirements for the usage of the Session Initiation Protocol (SIP) [1] for conveyance of user location information described by [7] from a SIP entity 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 one user agent informing another user agent where it is (you want to tell your friend where you are).

Another 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, precise location information of the caller in distress is a required component of a call to an emergency center.

A forth 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 or civic based). It also does not discuss the contents of the Location Object (LO). It does specify the requirements for the "using protocol" as defined by Geopriv in [7].

Sections 7, 8 and 9 give specific examples (in well-formed SIP messages) of SIP UA and Proxy behavior for location conveyance, the last of which is a section devoted to the unique circumstances regarding emergency calling. Section 10 addresses how this document adheres to the requirements specified in [7] (Geopriv Requirements). Sections 11 and 12 list the current open issues with location conveyance in SIP, and the new open issues recently discovered as a result of the added effort to this revision.

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 Prior Versions

[NOTE TO RFC-EDITOR: If this document is to be published as an RFC, this section is to be removed prior to that event.]

This is a list of the changes that have been made from the -01 working group version of this effort to this -02 version:

- added requirements for 2 new 4XX error responses (Bad Location Information) and (Retry Location Body)

- added "Bad Location Information" as section 8.6

- added "Retry Location Body " as section 9.3

- added support for session mode to cover packet sizes larger than the single packet limit of 1300 bytes in the message body

- added requirement for a SIP entity to SUBSCRIBE to another for location information

- added SUBSCRIBE and NOTIFY as section 8.5

- added requirement to have user turn off any tracking created by subscription

- removed doubt about which method to use for updating location after a INVITE is sent (update)

- cleaned up which method is to be used if there is no dialog existing (message)

- removed use of reINVITE to convey location

- clarified that UAs include <provided-by> element of PIDF-LO when placing an emergency call (to inform ERC who supplied Location information)

- updated list of open issues

- added to IANA Considerations section for the two new 4XX level error responses requested in the last meeting

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

- Added the offered solution in detail (with message flows, appropriate SIP Methods for location conveyance, and

- Synchronized the requirements here with those from the Geopriv Working Group's (attempting to eliminate overlap)

- Took on the task of making this effort the SIP "using protocol" specification from Geopriv's POV

- Refined the Open Issues section to reflect the progress we've made here, and to indicate what we have discovered needs addressing, but has not been to date.

This is a list of the changes that have been made from the -01 individual submission version to the WG -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

This is a list of the changes that have been made from the individual submission version -00 to the -01 version

- Added the IPR Statement section

- Adjusted a few requirements based on suggestions from the Minneapolis meeting

- Added requirements that the UAC is to include from where it learned its location in any transmission of its LI

- Distinguished the facts (known to date) that certain jurisdictions relieve persons of their right to privacy when they call an ERC, while other jurisdictions maintain a person's right to privacy, while still others maintain a person's right to privacy - but only if they ask that their service be set up that way.

- Made the decision that TLS is the security mechanism for location conveyance in emergency communications (vs. S/MIME, which is still the mechanism for UA-to-UA non-emergency location conveyance cases).

- Added the Open Issue of whether a Proxy can insert location information into an emergency SIP INVITE message, and some of the open questions surrounding the implications of that action

- added a few names to the acknowledgements section

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 civic) 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 UAC and UAS, and if engaged, would render the location object opaque to a proxy server for any desired modification if it is not correct or precise enough from that proxy's point of view (were it to be able to view it). 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: here TLS ("sips:" from [1]). It is envisioned that S/MIME SHOULD be used when location information is not required by proxy servers, and TLS MUST be used when it is. The UAC will need to know the difference in the call's intent as to which security mechanism to engage for LI conveyance.

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

As concluded from the previous section, location information is to be contained within a message body. If either another body (SDP for example) is also to be sent in the message, or the LI 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.

User agents providing location can perform this function incorrectly. Therefore, there needs to be a UAC error response code created to inform the UAC by a UAS or Proxy of this incorrect request message containing location information.

There will be times in which the UAC does not know its location information, or another SIP entity knows the UAC's location better than the UAC itself. How this is determined is out of scope of this document. In these times, a Proxy servers that knows the location of the UAC needs inform the UAC of its location information and have that UAC include that message body in its next SIP message to the same destination UA. This error code needs to be unique with respect to the error code for merely incorrect location information from the UAC.

4. Requirements for UA-to-UA Location Conveyance

The following are the requirements for UA-to-UA Location Conveyance Situations where routing is not based on the LI of either UA:

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].

U-U4 - Location information MUST be contained in the location Object as defined in [13], which will satisfy all format requirements for interoperability.

U-U5 - SHOULD be able to communicate location between user agents with as many packets as is necessary.

U-U6 - There MUST be a unique UAC error response code informing the UAC is did not provide valid location information.

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 with respect to entities to which the location information is not addressed, 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 (as [1] currently forbids this).

U-PS5 - any mechanism used to prevent unwanted observation of this Location Information MUST NOT fail the SIP Request if not understood by intermediary SIP entities or the destination UAS.

U-PS6 - Proxy Servers that do not or cannot understand the Location Information in the message body for routing purposes MUST NOT fail the SIP Request.

U-PS7 ¡ 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.

U-PS8 - There MUST be a unique UAC error response code informing the UAC is did not provide valid location information.

U-PS9 - There MUST be a unique UAC error response code informing the UAC it did not provide valid location information, and to include the location information contained in the message body of the error message in its next attempt to the same UAS of the original message.

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, while others grant the user the ability to remain anonymous even when calling an ERC. So far, this has been offered in some jurisdictions, but the user within that jurisdiction must state this preference, as it is not the default configuration.

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

E-3 - It MUST be possible to provide a privacy mechanism (that does not violate the other requirements within this document) to a user within a jurisdiction that gives that user the right to choose not to reveal their location even when contacting an ERC.

E-4 ¡ 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 (but does not violate requirement E-3). 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.

Location information is considered so important during emergency calls, that it is to be transmitted even when it is not considered reliable, or might even be wrong. For example, some application might know that the DHCP reply with location information was overwritten recently (or exactly) when a VPN connection was activated. This could, and likely will, provide any new location information to the UA from somewhere far away from the UA (perhaps the user's corporate facility).

E-5 Location information MUST be transmitted, if known to the UAC, in all calls to an ERC, even in the case it is not considered reliable.

With that in mind, it is important to distinguish the location information learned locally from LI learned over a VPN; which in itself is useful additional information to that ERC operator.

E-7 THE UA must provide the actual LI of the endpoint, and not location which might have been erroneously given to it by, e.g. a VPN tunnel DHCP server.

E-8 An ERC MAY wish to SUBSCRIBE to the UAC that initiated a session. If this is supported by the UAC, all NOTIFY messages MUST contain the UAC's location information.

This is a means for the emergency response centers to maintain a location the callers in distress.

E-9 It MUST be possible that any UAC supporting E-8 be informed of this subscription, as this will provide a means of alert to the user who does not wish this capability to remain enabled.

7. Location Conveyance using SIP

Geopriv is the IETF working group assigned to define a Location Object for carrying within another protocol to convey geographic location of an endpoint to another entity. This Location Object will be supplied within SIP to convey location of a UA (or user of a UA). The Location Object (LO) is defined in [13]. Section 26 of [1] defines the security functionality SIPS for transporting SIP messages with either TLS or IPsec, and S/MIME for encrypting message bodies from SIP intermediaries that would otherwise have access to reading the clear-text bodies. For UA-to-UA location conveyance, using the PIDF-LO body satisfies the entire format and message-handling requirements as stated in the baseline Geopriv requirements [7]. SIP entities that will carry an LO MUST implement S/MIME for encrypting on an end-to-end basis the location of a user agent, satisfying [7]'s security requirements. The SIPS-URI from [1] SHOULD also be used for further message protection (message integrity, authentication and message confidentiality) and MUST be used when S/MIME is not used. The entities sending and receiving the LO MUST obey the privacy and security instructions in the LO to be compliant with this specification.

Self-signed certificates SHOULD NOT be used for protecting LI, as the sender does not have a secure identity of the recipient.

Several LOs MAY be included in a body. If the message length exceeds the maximum message length of a single packet, session mode is to be used.

Several SIP Methods are capable (and applicable) to carry the LO. The Methods are divided into two groups, one for those applicable for UA-to-UA location conveyance, and the other group for UA-to-Proxy Location conveyance for routing the message.

The list of applicable Methods for UA-to-UA location conveyance is:

INVITE,
UPDATE,
MESSAGE, and
PUBLISH.

The list of applicable Methods for UA-to-Proxy location conveyance is:

INVITE,
UPDATE,
MESSAGE, and
SUBSCRIBE/NOTIFY

While the authors do not yet see a reason to have location conveyed in the OPTIONS, ACK, PRACK, BYE, REFER and CANCEL Methods, we do not see a reason to prevent carrying a LO within these Method Requests as long as the SIP message meets the requirements stated within this document.

A 200 OK to an INVITE MAY carry the UAS's LO back to the UAC that provided its location in the INVITE, but this is not something that can be required due to the timing of the INVITE to 200 OK messages, with potential local/user policy requiring the called user to get involved in determining if the caller is someone they wish to give location to (and at what precision).

There is an open question as to whether there needs to be a new event package created for a SUBSCRIBE such that one SIP entity (perhaps a service using SIP) can request the ability to have a remote UA's location refreshed at some interval. This idea is not explored further in this version of the document. The capability to have location information refreshed between devices is out of scope within the Geopriv working group at this time, but could easily become part of the "using protocol's" capabilities without violating any of the Geopriv Requirements in [7]. The authors want feedback on incorporating this into this document, or a separate document.

For UA-to-Proxy location conveyance, there are two cases: one in which all proxies on the path from the UA to the proxy that requires location can be trusted with the LI, and one in which intermediate proxies may not be trusted. The former may be implemented with "hop-by-hop" security as specified in [1] using sips: (i.e. TLS security). In particular, emergency call routing requires routing proxies to know location, and sips: protection is appropriate. The latter case is under study by the SIPPING working group under the subject "End to Middle" security [12].

Regardless which scenario (UA-to-UA or UA-to-Proxy) is used to convey location, SIP entities MUST adhere to the rules of [7], specifically the retention and distribution (privacy) attributes of a UA's location. When Alice is deciding how to transmit her location, she should be keenly aware of the parameters in which she wants her location to be stored and distributed. However, once she sends that location information to Bob, he MUST also now obey Alice's wishes regarding these privacy attributes if he is deciding to inform another party about Alice. This is a fundamental principle of the Geopriv Working Group, i.e. "PRIVACY".

8. User Agent-to-User Agent Location Conveyance

The offered solution here for the User-to-User solution for location conveyance between UAs is used with the INVITE, UPDATE, MESSAGE, and PUBLISH Methods in the following subsections.

8.1 UA-to-UA using INVITE Method

Below is a common SIP session set-up sequence between two user agents. In this example, Alice will provide Bob with her geographic location in the INVITE message.

```
   UA Alice                                  UA Bob

      |                INVITE [M1]               |
      |----------------------------------------->|
      |                                          |
      |                200 OK [M2]               |
      |<-----------------------------------------|
      |                                          |
      |                  ACK [M3]                |
      |----------------------------------------->|
      |                                          |
      |                   RTP                    |
      |<========================================>|
      |                                          |
```

Figure 1. UA-UA with Location in INVITE

User agent Alice invites user agent Bob to a session [M1 of Figure 1]. Within this INVITE is a multipart body indication that it is S/MIME encrypted [according to the rules of 1] by Alice for Bob. One body part contains the SDP offered by Alice to Bob. Alice's location (here coordinate based) is the other body part contained in this INVITE. Bob responses with a 200 OK [M2] (choosing a codec as specified by the Offer/Answer Model [14]). Bob can include his location in the 200 OK response, but this shouldn't be expected due to user timing. If Bob wants to provide his location to Alice after the 200 OK, but before a BYE, the UPDATE Method [9] should be used. Alice's UA replies with an ACK and the session is set up.

Figure 1. does not include any Proxies because in it assumed they would not affect the session set-up with respect to whether or not Alice's location is in a message body part, and Proxies don't react to S/MIME bodies, making their inclusion more or less moot and more complex than necessary.

The most relevant message in Figure 1 having to do with location is (obviously) the message with the location object in it [M1]. So to cut down on length of this document, only the INVITE message in this example will be shown. Section 8.1.1 will give an example of this well formed INVITE message using a Coordinate location format. Section 8.1.2 will give an example of this well formed INVITE message using the civic location format.

8.1.1 UA-to-UA INVITE with Coordinate Location Using S/MIME

Below is a well-formed SIP INVITE Method message to the example in Figure 1 in section 8.1.

[Message 1 in Figure 1]

```
INVITE sips:bob@biloxi.example.com SIP/2.0
Via: SIP/2.0/TLS pc33.atlanta.example.com
 ;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sips:bob@biloxi.example.com>
From: Alice <sips:alice@atlanta.example.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.example.com
CSeq: 314159 INVITE
Contact: <sips:alice@pc33.atlanta.example.com>
Content-Type: application/pkcs7-mime;
   smime-type=enveloped-data; name=smime.p7m
Content-Disposition: attachment;
   filename=smime.p7m  handling=required


Content-Type: multipart/mixed; boundary=boundary1


--boundary1


Content-Type: application/sdp
v=0
o=alice 2890844526 2890844526 IN IP4 atlanta.example.com
c=IN IP4 10.1.3.33
t=0 0
m=audio 49172 RTP/AVP 0 4 8
a=rtpmap:0 PCMU/8000


--boundary1
```

```
   Content-type: application/cpim-pidf+xml
   <?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:gml="urn:opengis:specification:gml:schema-
                    xsd:feature:v3.0"
          entity="pres:alice@atlanta.example.com">
        <tuple id="sg89ae">
         <timestamp>2004-11-11T08:57:29Z</timestamp>
         <status>
          <gp:geopriv>
            <gp:location-info>
              <gml:location>
                <gml:Point gml:id="point96" srsName="epsg:4326">
                  <gml:coordinates>41.87891N
                                   87.63649W</gml:coordinates>
                </gml:Point>
               </gml:location>
              <method>dhcp</method>
            </gp:location-info>
            <gp:usage-rules>
              <gp:retransmission-allowed>no</gp:retransmission-allowed>
              <gp:retention-expiry>2004-11-13T14:57:29Z</gp:retention-
                            expiry>
             </gp:usage-rules>
          </gp:geopriv>
         </status>
        </tuple>
       </presence>


   --boundary1--
```

8.1.1.1 UA-to-UA INVITE with Coordinate Location Not Using S/MIME

Below is a well-formed SIP INVITE Method message to the example in Figure 1 in section 8.1. This message is here to show that although the requirements are mandatory to implement proper security, it is not mandatory to use. This message below is show for those cases where hop-by-hop security is deployed.

[Message 1 in Figure 1]

```
INVITE sip:bob@biloxi.example.com SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.example.com
  ;branch=z9hG4bK74bf9
Max-Forwards: 70
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.example.com>
Call-ID: 3848276298220188511@atlanta.example.com
CSeq: 31862 INVITE
Contact: <sip:alice@atlanta.example.com>
Content-Type: multipart/mixed; boundary=boundary1
Content-Length: ...
```

```
   --boundary1


   Content-Type: application/sdp
   v=0
   o=alice 2890844526 2890844526 IN IP4 atlanta.example.com
   c=IN IP4 10.1.3.33
   t=0 0
   m=audio 49172 RTP/AVP 0 4 8
   a=rtpmap:0 PCMU/8000

   --broundary1

   Content-Type: application/cpim-pidf+xml
   <?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:gml="urn:opengis:specification:gml:schema-
          xsd:feature:v3.0"
          entity="pres:alice@atlanta.example.com">
        <tuple id="sg89ae">
         <timestamp>2004-11-11T08:57:29Z</timestamp>
         <status>
          <gp:geopriv>
            <gp:location-info>
              <gml:location>
                <gml:Point gml:id="point96" srsName="epsg:4326">
                  <gml:coordinates>41.87891N
                                   87.63649W</gml:coordinates>
                </gml:Point>
               </gml:location>
              <method>dhcp</method>
            </gp:location-info>
            <gp:usage-rules>
              <gp:retransmission-allowed>no</gp:retransmission-allowed>
              <gp:retention-expiry>2004-11-13T14:57:29Z</gp:retention-
                     expiry>
            </gp:usage-rules>
          </gp:geopriv>
         </status>
        </tuple>
       </presence>

   --boundary1--
```

8.1.2 UA-to-UA INVITE with Civic Location Using S/MIME

Below is a well-formed SIP INVITE Method message to the example in Figure 1 in section 8.1 using the civic location format.

[Message 1 in Figure 1]

```
INVITE sips:bob@biloxi.example.com SIP/2.0
Via: SIP/2.0/TLS pc33.atlanta.example.com
 ;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sips:bob@biloxi.example.com>
From: Alice <sips:alice@atlanta.example.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.example.com
```

```
   CSeq: 314159 INVITE
   Contact: <sips:alice@pc33.atlanta.example.com>
   Content-Type: application/pkcs7-mime;
      smime-type=enveloped-data; name=smime.p7m
   Content-Disposition: attachment;
      filename=smime.p7m  handling=required


   Content-Type: multipart/mixed; boundary=boundary1


   --boundary1


   Content-Type: application/sdp
   v=0
   o=alice 2890844526 2890844526 IN IP4 atlanta.example.com
   c=IN IP4 10.1.3.33
   t=0 0
   m=audio 49172 RTP/AVP 0 4 8
   a=rtpmap:0 PCMU/8000


   --boundary1


   Content-type: application/cpim-pidf+xml
   <?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:gml="urn:opengis:specification:gml:schema-
                     xsd:feature:v3.0"
          entity="pres:alice@atlanta.example.com">
        <tuple id="sg89ae">
         <timestamp>2004-11-11T08:57:29Z</timestamp>
         <status>
          <gp:geopriv>
            <gp:location-info>
              <cl:civilAddress>
                <cl:country>US</cl:country>
                <cl:A1>Illinois</cl:A1>
                <cl:A3>Chicago</cl:A3>
                <cl:HNO>233</cl:HNO>
                <cl:PRD>South</cl:PRD>
                <cl:A6>Wacker</cl:A6>
                <cl:STS>Drive</cl:STS>
                <cl:PC>60606</cl:PC>
                <cl:LMK>Sears Tower</cl:LMK>
                <cl:FLR>1</cl:FLR>
              <cl:civilAddress>
              <method>dhcp</method>
              <provided-by><nena>www.cisco.com</nena></provided-by/>
            </gp:location-info>
            <gp:usage-rules>
              <gp:retransmission-allowed>no</gp:retransmission-allowed>
              <gp:retention-expiry>2004-11-13T14:57:29Z</gp:retention-
                            expiry>
            </gp:usage-rules>
          </gp:geopriv>
         </status>
        </tuple>
       </presence>

--boundary1--
```

8.1.2.1 UA-to-UA INVITE with Civic Location Not Using S/MIME

Below is a well-formed SIP INVITE Method message to the example in Figure 1 in section 8.1. This message is here to show that although the requirements are mandatory to implement proper security, it is not mandatory to use. This message below is show for those cases where the sending user does not wish to use security mechanisms in transmitting their coordinate location.

[Message 1 in Figure 1]

```
INVITE sip:bob@biloxi.example.com SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.example.com
  ;branch=z9hG4bK74bf9
Max-Forwards: 70
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.example.com>
Call-ID: 3848276298220188511@atlanta.example.com
CSeq: 31862 INVITE
Contact: <sip:alice@atlanta.example.com>
Content-Type: multipart/mixed; boundary=boundary1
Content-Length: ...

--boundary1

Content-Type: application/sdp
v=0
o=alice 2890844526 2890844526 IN IP4 atlanta.example.com
c=IN IP4 10.1.3.33
t=0 0
m=audio 49172 RTP/AVP 0 4 8
a=rtpmap:0 PCMU/8000
```

```
   --broundary1


   Content-type: application/cpim-pidf+xml
   <?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:gml="urn:opengis:specification:gml:schema-
                     xsd:feature:v3.0"
          entity="pres:alice@atlanta.example.com">
```

```
        <tuple id="sg89ae">
         <timestamp>2004-11-11T08:57:29Z</timestamp>
         <status>
          <gp:geopriv>
            <gp:location-info>
              <cl:civilAddress>
                <cl:country>US</cl:country>
                <cl:A1>Illinois</cl:A1>
                <cl:A3>Chicago</cl:A3>
                <cl:HNO>233</cl:HNO>
                <cl:PRD>South</cl:PRD>
                <cl:A6>Wacker</cl:A6>
                <cl:STS>Drive</cl:STS>
                <cl:PC>60606</cl:PC>
                <cl:LMK>Sears Tower</cl:LMK>
                <cl:FLR>1</cl:FLR>
              <cl:civilAddress>
              <method>dhcp</method>
              <provided-by><nena>www.cisco.com</nena></provided-by/>
            </gp:location-info>
            <gp:usage-rules>
              <gp:retransmission-allowed>no</gp:retransmission-allowed>
              <gp:retention-expiry>2004-11-13T14:57:29Z</gp:retention-
                            expiry>
            </gp:usage-rules>
          </gp:geopriv>
         </status>
        </tuple>
       </presence>


--boundary1--
```

8.1.3 UA-to-UA Location Conveyance Involving 3 Users

In the following example, Alice presents her location in the INVITE to Bob, which Bob 200 OKs with his location as well. Bob then directs Alice to contact Carol. The REFER Method [15] is used in the message sequence, but it does not carry anyone's location within the REFER message. This example is here to show a 3-way communication of location, coupled with how a UA can include someone else's location. This has security implications due to neither primary party in the last location transfer being the owner of the location information. Alice (in this case) MUST adhere to the retention and distribution privacy requirements within Bob's location object regarding his location information prior to considering its inclusion in the INVITE to Carol.

```
   UA Alice                        Bob          Carol


      |           INVITE [M1]       |             |
      |---------------------------->|             |
      |           200 OK [M2]       |             |
      |<----------------------------|             |
      |            ACK [M3]         |             |
      |---------------------------->|             |
      |              RTP            |             |
      |<===========================>|             |
      |     reINVITE (hold) [M4]    |             |
      |<----------------------------|             |
      |          200 OK [M5]        |             |
      |---------------------------->|             |
      | REFER (Refer-to:Carol) [M6] |             |
      |<----------------------------|             |
      |                 INVITE [M7]               |
      |------------------------------------------>|
      |                 200 OK [M8]               |
      |------------------------------------------>|
      |                     RTP                   |
      |<=========================================>|
      |          NOTIFY [M9]        |             |
      |---------------------------->|             |
      |          200 OK [M10]       |             |
      |<----------------------------|             |
      |           BYE [M11]         |             |
      |<----------------------------|             |
      |          200 OK [M12]       |             |
      |---------------------------->|             |
      |                                           |
```

Figure 1a. UA-to-UA with Location in REFER

8.1.3.1 UA-to-UA REFER with Civic Location Using S/MIME

In Figure 1a., we have an example message flow involving the REFER Method. The REFER itself does not carry location objects.

We are not including all the messages for space reasons. M1 is a well-formed SIP message that contains Alice's location. M2 is Bob's 200 OK in response to Alice's INVITE, and it contains Bob's Location.

[M1 of Figure 1a] - Alice at Sears Tower

```
   INVITE sips:bob@biloxi.example.com SIP/2.0
   Via: SIP/2.0/TLS pc33.atlanta.example.com
    ;branch=z9hG4bK776asdhds
   Max-Forwards: 70
   To: Bob <sips:bob@biloxi.example.com>
   From: Alice <sips:alice@atlanta.example.com>;tag=1928301774
   Call-ID: a84b4c76e66710@pc33.atlanta.example.com
   CSeq: 314159 INVITE
   Contact: <sips:alice@pc33.atlanta.example.com>
   Content-Type: application/pkcs7-mime;
      smime-type=enveloped-data; name=smime.p7m
   Content-Disposition: attachment;
      filename=smime.p7m  handling=required


   Content-Type: multipart/mixed; boundary=boundary1


   --boundary1


   Content-Type: application/sdp
   v=0
   o=alice 2890844526 2890844526 IN IP4 atlanta.example.com
   c=IN IP4 10.1.3.33
   t=0 0
   m=audio 49172 RTP/AVP 0 4 8
   a=rtpmap:0 PCMU/8000


   --boundary1


   Content-type: application/cpim-pidf+xml
   <?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:gml="urn:opengis:specification:gml:schema-
                     xsd:feature:v3.0"
          entity="pres:alice@atlanta.example.com">
        <tuple id="sg89ae">
         <timestamp>2004-11-11T08:57:29Z</timestamp>
         <status>
          <gp:geopriv>
            <gp:location-info>
              <cl:civilAddress>
                <cl:country>US</cl:country>
                <cl:A1>Illinois</cl:A1>
                <cl:A3>Chicago</cl:A3>
                <cl:HNO>233</cl:HNO>
                <cl:PRD>South</cl:PRD>
                <cl:A6>Wacker</cl:A6>
                <cl:STS>Drive</cl:STS>
                <cl:PC>60606</cl:PC>
                <cl:LMK>Sears Tower</cl:LMK>
                <cl:FLR>1</cl:FLR>
              <cl:civilAddress>
              <method>dhcp</method>
              <provided-by><nena>www.cisco.com</nena></provided-by/>
            </gp:location-info>
            <gp:usage-rules>
              <gp:retransmission-allowed>no</gp:retransmission-allowed>
              <gp:retention-expiry>2004-11-13T14:57:29Z</gp:retention-
                            expiry>
            </gp:usage-rules>
          </gp:geopriv>
```

```
         </status>
        </tuple>
       </presence>

   --boundary1--
```

Bob replies to Alice's INVITE with a 200 OK and includes his location.

[M2 of Figure 4] - Bob watching Cubs Game at Wrigley Field

```
   SIP/2.0 200 OK
   Via: SIP/2.0/TCP pc33.atlanta.example.com
     ;branch=z9hG4bKnashds8 ;received=10.1.3.33
   To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
   From: Alice <sip:alice@atlanta.example.com>;tag=1928301774
   Call-ID: a84b4c76e66710
   CSeq: 314159 INVITE
   Contact: <sip:bob@192.168.10.20>
   Content-Type: application/pkcs7-mime;
      smime-type=enveloped-data; name=smime.p7m
   Content-Disposition: attachment;
      filename=smime.p7m  handling=required

   Content-Type: multipart/mixed; boundary=boundary1

   --boundary1

   Content-Type: application/sdp
   v=0
   o=bob 2890844530 2890844530 IN IP4 biloxi.example.com
   c=IN IP4 192.168.10.20
   t=0 0
   m=audio 3456 RTP/AVP 0
   a=rtpmap:0 PCMU/8000

   --boundary1

   Content-type: application/cpim-pidf+xml
   <?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:gml="urn:opengis:specification:gml:schema-
                     xsd:feature:v3.0"
          entity="pres:bob@biloxi.example.com">
        <tuple id="sg89ae">
         <timestamp>2004-11-6T02:30:29Z</timestamp>
         <status>
          <gp:geopriv>
            <gp:location-info>
              <cl:civilAddress>
```

```
                <cl:country>US</cl:country>
                <cl:A1>Illinois</cl:A1>
                <cl:A3>Chicago</cl:A3>
                <cl:A6>Addison</cl:A6>
                <cl:HNO>1060</cl:HNO>
                <cl:PRD>W</cl:PRD>
                <cl:STS>street</cl:STS>
                <cl:LMK>Wrigley Field</cl:LMK>
                <cl:PC>60613</cl:PC>
              <cl:civilAddress>
              <method>dhcp</method>
              <provided-by>www.cisco.com</provided-by/>
            </gp:location-info>
            <gp:usage-rules>
              <gp:retransmission-allowed>no</gp:retransmission-allowed>
              <gp:retention-expiry>2004-11-6T18:30:29Z</gp:retention-
                            expiry>
            </gp:usage-rules>
          </gp:geopriv>
         </status>
        </tuple>
       </presence>


   --boundary1--
```

Bob REFERs Alice to Carol, and in M7, Alice includes both locations in a single SIP message. This is possible because Bob set his retention value to "yes", thus allowing Alice to pass his location on to Carol.

[M7 of Figure 1a] - Alice tells Carol where she and Bob are

```
   INVITE sips:carol@chicago.example.com SIP/2.0
   Via: SIP/2.0/TLS pc33.atlanta.example.com
    ;branch=z9hG4bK776asdhdt
   Max-Forwards: 70
   To: Carol <sips:carol@chicago.example.com>
   From: Alice <sips:alice@atlanta.example.com>;tag=1928301775
   Call-ID: a84b4c76e66711@pc33.atlanta.example.com
   CSeq: 314160 INVITE
   Contact: <sips:alice@pc33.atlanta.example.com>
   Content-Type: application/pkcs7-mime;
      smime-type=enveloped-data; name=smime.p7m
   Content-Disposition: attachment;
      filename=smime.p7m  handling=required
   Content-Type: multipart/mixed; boundary=boundary1


   --boundary1


   Content-Type: application/sdp
   v=0
   o=alice 2890844531 2890844531 IN IP4 atlanta.example.com
   c=IN IP4 10.1.3.33
   t=0 0
   m=audio 49173 RTP/AVP 0 4 8
   a=rtpmap:0 PCMU/8000


   --boundary1


   Content-type: application/cpim-pidf+xml
   <?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:gml="urn:opengis:specification:gml:schema-
                     xsd:feature:v3.0"
          entity="pres:bob@biloxi.example.com">
        <tuple id="sg89af">
         <timestamp>2004-11-5T02:30:29Z</timestamp>
         <status>
          <gp:geopriv>
            <gp:location-info>
              <cl:civilAddress>
                <cl:country>US</cl:country>
                <cl:A1>Illinois</cl:A1>
                <cl:A3>Chicago</cl:A3>
                <cl:A6>Addison</cl:A6>
                <cl:HNO>1060</cl:HNO>
                <cl:PRD>W</cl:PRD>
                <cl:STS>street</cl:STS>
                <cl:LMK>Wrigley Field</cl:LMK>
                <cl:PC>60613</cl:PC>
              <cl:civilAddress>
              <method>dhcp</method>
              <method>802.11</method>
              <provided-by>www.cisco.com</provided-by/>
            </gp:location-info>
            <gp:usage-rules>
              <gp:retransmission-allowed>yes</gp:retransmission-
                                                             allowed>
              <gp:retention-expiry>2004-11-6T18:30:29Z</gp:retention-
                                    expiry>
            </gp:usage-rules>
          </gp:geopriv>
         </status>
        </tuple>
       </presence>
   --boundary1


   Content-type: application/cpim-pidf+xml
   <?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:gml="urn:opengis:specification:gml:schema-
                     xsd:feature:v3.0"
          entity="pres:alice@atlanta.example.com">
        <tuple id="sg89ae">
         <timestamp>2004-11-6T02:30:29Z</timestamp>
         <status>
          <gp:geopriv>
            <gp:location-info>
              <cl:civilAddress>
                <cl:country>US</cl:country>
                <cl:A1>Illinois</cl:A1>
                <cl:A3>Chicago</cl:A3>
                <cl:HNO>233</cl:HNO>
                <cl:PRD>South</cl:PRD>
                <cl:A6>Wacker</cl:A6>
                <cl:STS>Drive</cl:STS>
                <cl:PC>60606</cl:PC>
                <cl:LMK>Sears Tower</cl:LMK>
                <cl:FLR>1</cl:FLR>
              <cl:civilAddress>
              <method>dhcp</method>
              <method>802.11</method>
              <provided-by>www.marconi.com</provided-by/>
            </gp:location-info>
            <gp:usage-rules>
              <gp:retransmission-allowed>no</gp:retransmission-allowed>
              <gp:retention-expiry>2004-11-6T18:30:29Z</gp:retention-
                            expiry>
            </gp:usage-rules>
          </gp:geopriv>
         </status>
        </tuple>
       </presence>


   --boundary1--
```

It is an open question of whether there should be a mechanism to request or require the transmission of an LO. The LO is contained in a body, so the available sip mechanisms do not apply.

8.2 UA-to-UA Using MESSAGE Method

Anytime a user transmits location information outside a dialog, the

MESSAGE Method is to be used. The logic here is as follows:

- UPDATE isn't appropriate because it is for the updating of session capabilities and parameters of a dialog (after the INVITE included location information).

- reINVITE isn't appropriate because it is only used (or only supposed to be used) for changing the parameters of an existing dialog, and one might not exist in all cases of location conveyance.

This leaves MESSAGE as the only viable Request Method for location conveyance outside of a dialog between two users (Alice and Bob in this case). The following is an example of this communication.

```
   UA Alice                                  UA Bob

      |               MESSAGE [M1]               |
      |----------------------------------------->|
      |                                          |
      |                200 OK [M2]               |
      |<-----------------------------------------|
      |                                          |
```

Figure 2. UA-UA with Location in MESSAGE

Section 8.2.1 will give the well formed MESSAGE Method containing a well formed Geopriv Location Object using the Coordinate location format that fully complies with all security requirements - SIPS for hop-by-hop security, and S/MIME for message body confidentiality end-to-end, as well as adhering to the retention and distribution concerns from [7]. Section 8.2.2 will show the Civic Location format alternative to the same location, as conveyed from Alice to Bob. This section does not adhere to confidentiality or integrity concerns of [7], but does convey retention and distribution indicators from Alice.

8.2.1 UA-to-UA MESSAGE with Coordinate Location Using S/MIME

Below is M1 from Figure 2 in section 8.2. that is fully secure and in compliance with Geopriv requirements in [7] for security concerns.

[Message 1 in Figure 2]

```
   MESSAGE sips:bob@biloxi.example.com SIP/2.0
   Via: SIP/2.0/TLS pc33.atlanta.example.com
    ;branch=z9hG4bK776asegma
   Max-Forwards: 70
   To: Bob <sips:bob@biloxi.example.com>
   From: Alice <sips:alice@atlanta.example.com>;tag=1928301774
   Call-ID: a84b4c76e66710@pc33.atlanta.example.com
   CSeq: 22756 MESSAGE
   Content-Type: application/pkcs7-mime;
      smime-type=enveloped-data; name=smime.p7m
   Content-Disposition: attachment;
```

```
      filename=smime.p7m  handling=required

   Content-Type: multipart/mixed; boundary=boundary1


   --boundary1


   Content-Type: text/plain
   Here's my location, Bob?


   --broundary1


   Content-Type: application/cpim-pidf+xml
   Content-Disposition: render
   Content-Description: my location
   <?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:gml="urn:opengis:specification:gml:schema-
          xsd:feature:v3.0"
          entity="pres:alice@atlanta.example.com">
        <tuple id="sg89ae">
         <timestamp>2004-11-11T08:57:29Z</timestamp>
         <status>
          <gp:geopriv>
            <gp:location-info>
              <gml:location>
                <gml:Point gml:id="point96" srsName="epsg:4326">
                  <gml:coordinates>41.87891N
                                   87.63649W</gml:coordinates>
                </gml:Point>
               </gml:location>
              <method>dhcp</method>
            </gp:location-info>
            <gp:usage-rules>
              <gp:retransmission-allowed>no</gp:retransmission-allowed>
              <gp:retention-expiry>2004-11-13T14:57:29Z</gp:retention-
                     expiry>
            </gp:usage-rules>
          </gp:geopriv>
         </status>
        </tuple>
       </presence>


   --boundary1--
```

8.2.2 UA-to-UA MESSAGE with Civic Location Not Using S/MIME

Below is a well-formed SIP MESSAGE Method message to the example in Figure 2 in section 8.2 when hop-by-hop security mechanisms are deployed.

[Message 1 in Figure 2]

```
MESSAGE sip:bob@biloxi.example.com SIP/2.0
From: <sip:alice@atlanta.example.com>;tag=34589882
To: <sip:bob@biloxi.example.com>
Call-ID: 9242892442211117@atlanta.example.com
CSeq: 6187 MESSAGE
Content-Type: application/cpim-pidf+xml
Content-ID: <766534765937@atlanta.example.com>
Content-Disposition: render
Content-Description: my location


<?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:gml="urn:opengis:specification:gml:schema-
       xsd:feature:v3.0"
       entity="pres:alice@atlanta.example.com">
     <tuple id="sg89ae">
      <timestamp>2004-11-11T08:57:29Z</timestamp>
      <status>
       <gp:geopriv>
         <gp:location-info>
           <cl:civilAddress>
             <cl:country>US</cl:country>
             <cl:A1>Illinois</cl:A1>
             <cl:A3>Chicago</cl:A3>
             <cl:HNO>233</cl:HNO>
             <cl:PRD>South</cl:PRD>
             <cl:A6>Wacker</cl:A6>
             <cl:STS>Drive</cl:STS>
             <cl:PC>60606</cl:PC>
             <cl:LMK>Sears Tower</cl:LMK>
             <cl:FLR>1</cl:FLR>
           <cl:civilAddress>
           <method>dhcp</method>
         </gp:location-info>
         <gp:usage-rules>
           <gp:retransmission-allowed>no</gp:retransmission-allowed>
           <gp:retention-expiry>2004-11-13T14:57:29Z</gp:retention-
                   expiry>
         </gp:usage-rules>
       </gp:geopriv>
      </status>
     </tuple>
```

```
       </presence>
```

8.3 UA-to-UA Location Conveyance Using UPDATE

UPDATE MUST NOT be used to send location information from UA-to-UA unless location has already been sent in an INVITE or corresponding 200 OK that was the first message exchange in the same dialog set-up. The same security properties used in the INVITE MUST be used in the UPDATE message.

The UPDATE Method is to be used any time location information is to be updated between UAs setting up a dialog or after the dialog has been established, no matter how long that dialog has been operational. reINVITE is out of scope here, and the MESSAGE Method is for non-dialog location conveyance between UAs only.

One reason for this message being generated is if either UA that sent its location information to the other UA (say in the INVITE and corresponding 200 OK) is if either UA determines that is has moved while the dialog has remained operational. How this movement is determined is outside the scope of this document, but ultimately should be configurable by local administration or the user of the UA. By how much Alice has moved to trigger the "sense of movement" (i.e. the need to send new location) to Bob is also outside the scope of this specification, but ultimately should be configurable by local administration or the user of the UA.

In Figure 3., we have an example message flow involving the UPDATE Method. We are not including all the messages for space reasons. M1 is a well formed SIP message that contains Alice's location. During the session set-up, Alice's UA knows it has moved while knowing too the session has not been formally accepted by Bob. Alice's UA decides to update Bob with her new location with an UPDATE Method message. Messages M2, M3 and M4 have nothing to do with location conveyance, therefore will not be shown in detail. Only M1 and M5 will be shown.

NOTE: A similar use for UPDATE is within the UA-to-Proxy Location
      Conveyance section of this document.

```
UA Alice                                  UA Bob

   |                INVITE [M1]              |
   |---------------------------------------->|
   |                                         |
   |        183 (session Progress) [M2]      |
   |<----------------------------------------|
   |                                         |
   |                 PRACK [M3]              |
   |---------------------------------------->|
   |                                         |
   |              ACK (PRACK) [M4]           |
   |<----------------------------------------|
   |                                         |
   |                 UPDATE [M5]             |
   |---------------------------------------->|
   |                                         |
   |              ACK (UPDATE) [M6]          |
   |<----------------------------------------|
   |                                         |
   |            200 OK (INVITE) [M7]         |
   |<----------------------------------------|
   |                                         |
   |                   RTP                   |
   |<=======================================>|
   |                                         |
```

Figure 3. UA-UA with Location in UPDATE

The following section will include the M1 and M5 messages in detail, but only in the civic format.

8.3.1 UA-to-UA UPDATE with Civic Location Not Using S/MIME

Here is the initial INVITE from Alice to Bob.

[M1 INVITE to Bob]

```
INVITE sips:bob@biloxi.example.com SIP/2.0
Via: SIP/2.0/TLS pc33.atlanta.example.com
 ;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sips:bob@biloxi.example.com>
From: Alice <sips:alice@atlanta.example.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.example.com
CSeq: 314159 INVITE
Contact: <sips:alice@pc33.atlanta.example.com>
Content-Type: application/pkcs7-mime;
   smime-type=enveloped-data; name=smime.p7m
Content-Disposition: attachment;
   filename=smime.p7m  handling=required


Content-Type: multipart/mixed; boundary=boundary1


--boundary1
```

```
   Content-Type: application/sdp
   v=0
   o=alice 2890844526 2890844526 IN IP4 atlanta.example.com
   c=IN IP4 10.1.3.33
   t=0 0
   m=audio 49172 RTP/AVP 0 4 8
   a=rtpmap:0 PCMU/8000


   --boundary1
   Content-type: application/cpim-pidf+xml
   <?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:gml="urn:opengis:specification:gml:schema-
                     xsd:feature:v3.0"
          entity="pres:alice@atlanta.example.com">
        <tuple id="sg89ae">
         <timestamp>2004-11-11T08:57:29Z</timestamp>
         <status>
          <gp:geopriv>
            <gp:location-info>
              <cl:civilAddress>
                <cl:country>US</cl:country>
                <cl:A1>Illinois</cl:A1>
                <cl:A3>Chicago</cl:A3>
                <cl:HNO>233</cl:HNO>
                <cl:PRD>South</cl:PRD>
                <cl:A6>Wacker</cl:A6>
                <cl:STS>Drive</cl:STS>
                <cl:PC>60606</cl:PC>
                <cl:LMK>Sears Tower</cl:LMK>
                <cl:FLR>1</cl:FLR>
              <cl:civilAddress>
              <method>dhcp</method>
              <method>802.11</method>
             <provided-by>www.cisco.com</provided-by/>
            </gp:location-info>
            <gp:usage-rules>
              <gp:retransmission-allowed>no</gp:retransmission-allowed>
              <gp:retention-expiry>2004-11-13T14:57:29Z</gp:retention-
                            expiry>
            </gp:usage-rules>
          </gp:geopriv>
         </status>
        </tuple>
       </presence>


--boundary1--
```

Alice moves locations (with her UA detecting the movement), causing her UA to generate an UPDATE message ([M5] of Figure 3) prior to her UA receiving a final response from Bob. Here is that message:

M5 UPDATE to Bob

```
   UPDATE sips:bob@biloxi.example.com/TCP SIP/2.0
   Via: SIP/2.0/TLS pc33.atlanta.example.com
    ;branch=z9hG4bK776asdhds
   Max-Forwards: 70
   To: Bob <sips:bob@biloxi.example.com>
   From: Alice <sips:alice@atlanta.example.com>;tag=1928
   Call-ID: a84b4c76e66710@pc33.atlanta.example.com
   CSeq: 10197 UPDATE
   Contact: <sips:alice@pc33.atlanta.example.com>
   Content-Type: application/pkcs7-mime;
      smime-type=enveloped-data; name=smime.p7m
   Content-Disposition: attachment;
      filename=smime.p7m  handling=required


   Content-Type: multipart/mixed; boundary=boundary1


   --boundary1


   Content-Type: application/sdp
   v=0
   o=alice 2890844526 2890844526 IN IP4 atlanta.example.com
   c=IN IP4 10.1.3.33
   t=0 0
   m=audio 49172 RTP/AVP 0 4 8
   a=rtpmap:0 PCMU/8000


   --boundary1


   Content-type: application/cpim-pidf+xml
   <?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:gml="urn:opengis:specification:gml:schema-
                     xsd:feature:v3.0"
          entity="pres:alice@atlanta.example.com">
        <tuple id="sg89ae">
         <timestamp>2004-11-11T08:57:29Z</timestamp>
         <status>
          <gp:geopriv>
            <gp:location-info>
              <cl:civilAddress>
                <cl:country>US</cl:country>
                <cl:A1>Illinois</cl:A1>
                <cl:A3>Chicago</cl:A3>
                <cl:HNO>250</cl:HNO>
                <cl:PRD>South Upper</cl:PRD>
                <cl:A6>Wacker</cl:A6>
                <cl:STS>Drive</cl:STS>
                <cl:PC>60606</cl:PC>
                <cl:NAM>Venice Cafe</cl:NAM>
                <cl:FLR>1</cl:FLR>
              <cl:civilAddress>
              <method>dhcp</method>
              <method>802.11</method>
              <provided-by>www.t-mobile.com</provided-by/>
            </gp:location-info>
            <gp:usage-rules>
              <gp:retransmission-allowed>no</gp:retransmission-allowed>
              <gp:retention-expiry>2004-11-13T14:57:29Z</gp:retention-
                            expiry>
            </gp:usage-rules>
          </gp:geopriv>
         </status>
        </tuple>
       </presence>

--boundary1--
```

8.4 UA-to-UA Location Conveyance Using PUBLISH

** This section could not be completed before submission time and will be completed shortly after IETF61. A thousand and one pardons.

8.5 UA-to-UA Location Conveyance Using SUBSCRIBE and NOTIFY

This section was not completed in time for the ID cut-off, thus all text was removed until it can be completed. The authors apologize.

8.6 424 "Bad Location Information" Error Response

In the case that a user agent server or SIP Proxy detects an error in a message containing location information specific to that message body, a new 4XX level error needs to be sent. This document creates the new error code:

   424 (Bad Location Information)

This will provide the UAC with directed feedback about the status of location information it sent to that UAS or Proxy. The UAC MAY attempt to retry sending the message providing its location.

This new error code will be IANA registered.

An example flow of this scenario will be included in the next version of this internet draft.

9. Special Considerations for Emergency Calls

When a Proxy Server knows to look for a location message body to route an emergency call as in [11].

Emergency calls, which might be detected as detailed in [3], have special rules for conveyance of location:

1. An emergency call MUST have all LI available to the UA, if any, sent with the INVITE, and subsequent UPDATE or reINVITE messages

as a PIDF-LO in a body

2. The LO must be protected with sips: unless the attempt to establish hop-by-hop TLS connection fails and cannot reasonably be established in a very short (less than a second) time. In such a case, the LO SHOULD be sent without TLS ONLY for those hops that failed to support TLS establishment.

3. User Agents MUST NOT use S/MIME

4. User Agents MUST include the <provided-by> element in the PIDF-LO (if known) to give the ERC an indication as to who is responsible for providing the UA with its location information.

Proxies MUST NOT remove a location message body at any time. In the case where the Proxy knows the location of the UAC and does not detect the UAC's location information message body in the message (or determines the LO is bad), the Proxy generates a new 4XX (Retry Location Body) error message that includes a location information message body for that UAC to include in the subsequent message. The user agent MUST include this message body in the subsequent emergency message.

In the <provided-by> element of the PIDF-LO, the Proxy MUST identify itself as the source of this location information. The user agent MUST NOT alter this field's value if received from a Proxy server.

If the UAS of the ERC receives a SIP request with multiple location objects, it must determine which to use, since more than one may be present. This specification does not limit the number of LOs in a message, even in session mode.

9.1 UA-to-Proxy Routing the Message with INVITE (secure)

When Alice signifies "sos@" [per 3], her UA must understand this message MUST NOT use S/MIME for the message body, because this is an emergency call - otherwise the message will not properly route to the correct destination. Two definite possibilities will exist for how this message flow will occur [note: the message flows are not being defined here, they are defined in [11], but two are shown here to show the messages themselves]. The first possibility has Alice sending her INVITE to her first hop Proxy, which recognizes the message as an emergency message. The Proxy knows to look into the message bodies for the location body; determine where Alice is and route the call to the appropriate ERC. This is shown in Figure 4A.

```
   UA Alice             Proxy                  ERC


      |    INVITE [M1]    |                      |
      |------------------>|                      |
      |                   |      INVITE [M2]    |
      |                   |-------------------->|
      |                   |      200 OK [M3]    |
      |                   |<--------------------|
      |   200 OK [M4]     |                     |
      |<------------------|                     |
      |     ACK [M5]                            |
      |---------------------------------------->|
      |                   RTP                   |
      |<=======================================>|
      |                                         |
```

Figure 4A. UA-PROXY with Location in INVITE

[M1 of Figure 4A]

```
   INVITE sips:sos@atlanta.example.com SIP/2.0
   Via: SIP/2.0/TLS pc33.atlanta.example.com
     ;branch=z9hG4bK74bf9
   Max-Forwards: 70
   From: Alice <sips:alice@atlanta.example.com>;tag=9fxced76sl
   To: <sips:sos@atlanta.example.com>
   Call-ID: 3848276298220188511@atlanta.example.com
   CSeq: 31862 INVITE
   Contact: <sips:alice@atlanta.example.com>
   Content-Type: multipart/mixed; boundary=boundary1
   Content-Length: ...


   --boundary1


   Content-Type: application/sdp
   v=0
   o=alice 2890844526 2890844526 IN IP4 atlanta.example.com
   c=IN IP4 10.1.3.33
   t=0 0
   m=audio 49172 RTP/AVP 0 4 8
   a=rtpmap:0 PCMU/8000


   --boundary1
```

Once the Proxy receives M1 and recognizes it as an emergency INVITE Request, this proxy knows to look into the message body for a location body part to determine the location of the UAC in order to match the location to an ERC. Once this look-up occurs, the message is sent directly to the ERC (in message [M2]).

[M2 of Figure 4A] - Proxy has determined when to send message

```
INVITE sips:sos@192.168.10.20 SIP/2.0
Via: SIP/2.0/TLS pc33.atlanta.example.com
```

```
     ;branch=z9hG4bK74bf9
   Max-Forwards: 69
   From: Alice <sips:alice@atlanta.example.com>;tag=9fxced76sl
   To: <sips:sos@atlanta.example.com>
   Call-ID: 3848276298220188511@atlanta.example.com
   CSeq: 31862 INVITE
   Contact: <sips:alice@atlanta.example.com>
   Content-Type: multipart/mixed; boundary=boundary1
   Content-Length: ...


   --boundary1


   Content-Type: application/sdp
   v=0
   o=alice 2890844526 2890844526 IN IP4 atlanta.example.com
   c=IN IP4 10.1.3.33
   t=0 0
   m=audio 49172 RTP/AVP 0 4 8
   a=rtpmap:0 PCMU/8000


   --boundary1


   Content-type: application/cpim-pidf+xml
   <?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:gml="urn:opengis:specification:gml:schema-
                     xsd:feature:v3.0"
          entity="pres:alice@atlanta.example.com">
        <tuple id="sg89ae">
         <timestamp>2004-11-11T08:57:29Z</timestamp>
         <status>
          <gp:geopriv>
            <gp:location-info>
              <cl:civilAddress>
                <cl:country>US</cl:country>
                <cl:A1>Illinois</cl:A1>
                <cl:A3>Chicago</cl:A3>
                <cl:HNO>233</cl:HNO>
                <cl:PRD>South</cl:PRD>
                <cl:A6>Wacker</cl:A6>
                <cl:STS>Drive</cl:STS>
                <cl:PC>60606</cl:PC>
                <cl:LMK>Sears Tower</cl:LMK>
                <cl:FLR>1</cl:FLR>
              <cl:civilAddress>
              <method>dhcp</method>
              <method>802.11</method>
              <provided-by>www.t-mobile.com</provided-by/>
            </gp:location-info>
            <gp:usage-rules>
              <gp:retransmission-allowed>no</gp:retransmission-allowed>
              <gp:retention-expiry>2004-11-13T14:57:29Z</gp:retention-
                            expiry>
            </gp:usage-rules>
          </gp:geopriv>
         </status>
        </tuple>
       </presence>


--boundary1--
```

The second probability in message flows is in Figure 4B. in which the first hop Proxy does not either: understand location, or does not know where the appropriate ERC is to route the message to. In either case, that Proxy forwards the message to another Proxy for proper message routing ([11] talks to how this occurs).

```
   UA Alice       Proxy         Proxy          ERC

      | INVITE [M1] |             |             |
      |------------>|             |             |
      |             | INVITE [M2] |             |
      |             |------------>|             |
      |             |             | INVITE [M3] |
      |             |             |------------>|
      |             |             | 200 OK [M4] |
      |             |             |<------------|
      |             | 200 OK [M5] |             |
      |             |<------------|             |
      | 200 OK [M6] |             |             |
      |<------------|             |             |
      |   ACK [M7]                              |
      |---------------------------------------->|
      |                   RTP                   |
      |<=======================================>|
      |                                         |
```

Figure 4B. UA-PROXY with Location in INVITE

In message flows similar to 4A and/or 4B, the Record-Route header could be added by the proxies, this is OPTIONAL in usage and left to other documents to refine.

In the case of an identifiable emergency call, something that cannot happen is for any Proxy to Challenge [per 1] the INVITE message. In fact, while usage of the SIPS URI is encouraged and SHOULD be used, it MUST NOT be mandatory for successful message routing. If the first SIPS INVITE fails for security property reasons, the second attempt by Alice (in these examples) MUST be allowed to be in the clear, not challenged, and routed properly. Security mechanisms MUST NOT fail any call attempt, and if they do once, they MUST NOT be mandatory for the subsequent attempt for a successful session set-up to an ERC. The results of this are that the Proxy that failed the first attempt for security reasons MUST be aware of this failed attempt for the subsequent attempt that MUST process without failure a second time.   It must be assumed that the INVITE in any instance is considered "well formed".

The remaining messages in both 4A and 4B are not included at this time. If the working groups wants these added, they will be in the next revision of this document.

9.1.1 UA-to-Proxy Routing the Message with INVITE (unsecure)

Below can be considered the initial unsecure INVITE M1 from Figures 4A and 4A, or the second attempt message to an initial message that was failed by a Proxy. This version of M1 is not using any security measures and is using the civic format message body that is the identical location to the previous example.

```
[Message M1 from Figure 4A]

INVITE sip:sos@atlanta.example.com SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.example.com
  ;branch=z9hG4bK74bf9
Max-Forwards: 70
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
To: <sip:sos@atlanta.example.com>
Call-ID: 3848276298220188511@atlanta.example.com
CSeq: 31862 INVITE
Contact: <sip:alice@atlanta.example.com>
Content-Type: multipart/mixed; boundary=boundary1
Contact-Length: ...

--boundary1

Content-Type: application/sdp
v=0
o=alice 2890844526 2890844526 IN IP4 atlanta.example.com
c=IN IP4 10.1.3.33
t=0 0
```

```
m=audio 49172 RTP/AVP 0 4 8
a=rtpmap:0 PCMU/8000


--boundary1


Content-type: application/cpim-pidf+xml
<?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:gml="urn:opengis:specification:gml:schema-
```

```
                     xsd:feature:v3.0"
          entity="pres:alice@atlanta.example.com">
        <tuple id="sg89ae">
         <timestamp>2004-11-11T08:57:29Z</timestamp>
         <status>
          <gp:geopriv>
            <gp:location-info>
              <cl:civilAddress>
                <cl:country>US</cl:country>
                <cl:A1>Illinois</cl:A1>
                <cl:A3>Chicago</cl:A3>
                <cl:HNO>233</cl:HNO>
                <cl:PRD>South</cl:PRD>
                <cl:A6>Wacker</cl:A6>
                <cl:STS>Drive</cl:STS>
                <cl:PC>60606</cl:PC>
                <cl:LMK>Sears Tower</cl:LMK>
                <cl:FLR>1</cl:FLR>
              <cl:civilAddress>
              <method>dhcp</method>
              <method>802.11</method>
              <provided-by>www.t-mobile.com</provided-by/>
            </gp:location-info>
            <gp:usage-rules>
              <gp:retransmission-allowed>no</gp:retransmission-allowed>
              <gp:retention-expiry>2004-11-13T14:57:29Z</gp:retention-
                            expiry>
            </gp:usage-rules>
          </gp:geopriv>
         </status>
        </tuple>
       </presence>


--boundary1--
```

9.2 UA-to-Proxy Routing with UPDATE

If the previous example of the location contained in the INVITE were to account for the movement of Alice (and her UA) before the ERC responded with a 200 OK, the UPDATE method is the appropriate SIP Request Method to use to update the proxies and ERC personnel that Alice has moved locations from where she initially made her set-up request.

In this scenario (shown in the call flow of Figure 5A), Alice sending the UPDATE message here may cause the Proxy to CANCEL an existing pending INVITE Request, and retransmit INVITE to a NEW ERC(2), for example, if she walked across a street into a new ERC coverage area. The Proxy MUST remain transaction stateful in order to be aware of the 200 OK Response from ERC1. Upon receiving the UPDATE from Alice and analyzing the location provided by the message looking for a location change, either forwarding that message to ERC1 if the change is still within ERC1's coverage area, or deciding to forward a message to another ERC covering where Alice is now (ERC2 in this case) with her new location. If the latter change in destinations is required, the Proxy MUST CANCEL the pending INVITE to ERC1 (with a 487 "terminated request" being the specified response).

SIPS SHOULD be used by Alice initially. Upon any failure of the initial Request, Alice's UA MUST decide to send the new message without SIPS.

```
   UA Alice           Proxy         ERC1          ERC2

      |   INVITE [M1]   |             |             |
      |---------------->|             |             |
      |                 | INVITE [M2] |             |
      |                 |------------>|             |
      |   183 SP [M3]   |             |             |
      |<----------------|             |             |
      |    PRACK [M4]   |             |             |
      |---------------->|             |             |
      | 200 OK (PR)[M5] |             |             |
      |<----------------|             |             |
      |   UPDATE [M6]   |             |             |
      |---------------->|             |             |
      | 200 OK (UP)[M7] |             |             |
      |<----------------|             |             |
      |                 | CANCEL [M8] |             |
      |                 |------------>|             |
      |                 | 487 [M9]    |             |
      |                 |<------------|             |
      |                 | INVITE [M10]              |
      |                 |-------------------------->|
      |                 |        200 OK (INV) [M11] |
      |                 |<--------------------------|
      |200 OK (INV)[M12]|                           |
      |<----------------|                           |
      |   ACK [M13]                                 |
      |-------------------------------------------->|
      |                        RTP                  |
      |<==========================================>|
      |                                             |
```

Figure 5A. UA-PROXY with Location in UPDATE

** see new open issue #9 for the problems with messages 8 through 10
** of the above flow.

9.2.1 UA-to-Proxy Routing the Message with UPDATE (secure)

```
   INVITE sip:sos@atlanta.example.com SIP/2.0
   Via: SIP/2.0/TCP pc33.atlanta.example.com
     ;branch=z9hG4bK74bf9
   Max-Forwards: 70
   From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
   To: <sip:sos@atlanta.example.com>
   Call-ID: 3848276298220188511@atlanta.example.com
   CSeq: 31862 INVITE
   Contact: <sip:alice@atlanta.example.com>
   Content-Type: multipart/mixed; boundary=boundary1
   Contact-Length: ...


   --boundary1


   Content-Type: application/sdp
   v=0
   o=alice 2890844526 2890844526 IN IP4 atlanta.example.com
   c=IN IP4 10.1.3.33
   t=0 0
   m=audio 49172 RTP/AVP 0 4 8
   a=rtpmap:0 PCMU/8000


   --boundary1


   Content-type: application/cpim-pidf+xml
   <?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:gml="urn:opengis:specification:gml:schema-
                     xsd:feature:v3.0"
          entity="pres:alice@atlanta.example.com">
        <tuple id="sg89ae">
         <timestamp>2004-11-11T08:57:29Z</timestamp>
         <status>
          <gp:geopriv>
            <gp:location-info>
              <cl:civilAddress>
                <cl:country>US</cl:country>
                <cl:A1>Illinois</cl:A1>
                <cl:A3>Chicago</cl:A3>
                <cl:HNO>233</cl:HNO>
                <cl:PRD>South</cl:PRD>
                <cl:A6>Wacker</cl:A6>
                <cl:STS>Drive</cl:STS>
                <cl:PC>60606</cl:PC>
                <cl:LMK>Sears Tower</cl:LMK>
                <cl:FLR>1</cl:FLR>
              <cl:civilAddress>
              <method>dhcp</method>
              <method>802.11</method>
```

```
             <provided-by>www.cisco.com</provided-by/>
            </gp:location-info>
            <gp:usage-rules>
              <gp:retransmission-allowed>no</gp:retransmission-allowed>
              <gp:retention-expiry>2004-11-13T14:57:29Z</gp:retention-
                            expiry>
            </gp:usage-rules>
          </gp:geopriv>
         </status>
        </tuple>
       </presence>

--boundary1--
```

Alice moves locations (with her UA detecting the movement), causing her UA to generate an UPDATE message ([M5] of Figure 3) prior to her UA receiving a final response from the ERC. In this case, Alice has walked across the South Wacker Drive to another building. Here is that message:

[M5 UPDATE to ERC]

```
UPDATE sips:bob@biloxi.example.com/TCP SIP/2.0
Via: SIP/2.0/TLS pc33.atlanta.example.com
 ;branch=z9hG4bK776asdhds
Max-Forwards: 70
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
To: <sip:sos@atlanta.example.com>
Call-ID: 3848276298220188511@atlanta.example.com
CSeq: 10187 UPDATE
Contact: <sip:alice@atlanta.example.com>
Content-Type: multipart/mixed; boundary=boundary1
Contact-Length: ...

--boundary1

Content-Type: application/sdp
v=0
o=alice 2890844526 2890844526 IN IP4 atlanta.example.com
c=IN IP4 10.1.3.33
t=0 0
m=audio 49172 RTP/AVP 0 4 8
a=rtpmap:0 PCMU/8000
```

```
   --boundary1


   Content-type: application/cpim-pidf+xml
   <?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:gml="urn:opengis:specification:gml:schema-
                     xsd:feature:v3.0"
          entity="pres:alice@atlanta.example.com">
        <tuple id="sg89ae">
         <timestamp>2004-11-11T08:57:29Z</timestamp>
         <status>
          <gp:geopriv>
            <gp:location-info>
              <cl:civilAddress>
                <cl:country>US</cl:country>
                <cl:A1>Illinois</cl:A1>
                <cl:A3>Chicago</cl:A3>
                <cl:HNO>250</cl:HNO>
                <cl:PRD>South Upper</cl:PRD>
                <cl:A6>Wacker</cl:A6>
                <cl:STS>Drive</cl:STS>
                <cl:PC>60606</cl:PC>
                <cl:NAM>Venice Cafe</cl:NAM>
                <cl:FLR>1</cl:FLR>
              <cl:civilAddress>
              <method>dhcp</method>
              <method>802.11</method>
              <provided-by>www.t-mobile.com</provided-by/>
            </gp:location-info>
            <gp:usage-rules>
              <gp:retransmission-allowed>no</gp:retransmission-allowed>
              <gp:retention-expiry>2004-11-13T14:57:29Z</gp:retention-
                            expiry>
            </gp:usage-rules>
          </gp:geopriv>
         </status>
        </tuple>
       </presence>


--boundary1--
```

9.2.2 UA-to-Proxy Routing the Message with UPDATE (unsecure)

left blank for now

9.3 425 "Retry Location Body" Error Response

In the case that a SIP Proxy detects an error in a message containing location information specific to that message body and has the location of that UAC locally, a new 400 level error needs to be sent back to the UAC to instruct the UAC to include the included location information message body in a subsequent message. This document creates the new error code:

425 (Retry Location Body)

The UAC MUST]retransmission of the failed message including this new location information. User agents may conclude they have already supplied a proper LO in the failed request. That LO can be resent, but the Proxy supplied LO MUST be included as well.

This new error code will be IANA registered.

An example flow of this scenario will be included in the next version of this internet draft.

10. Meeting RFC3693 Requirements

Section 7.2 of [7] details the requirements of a "using protocol". They are:

Req. 4. The using protocol has to obey the privacy and security instructions coded in the Location Object and in the corresponding Rules regarding the transmission and storage of the LO.

This document requires, in Section 7, that SIP entities sending or receiving location MUST obey such instructions.

Req. 5. The using protocol will typically facilitate that the keys associated with the credentials are transported to the respective parties, that is, key establishment is the responsibility of the using protocol.

[1] and the documents it references define the key establish mechanisms.

Req. 6. (Single Message Transfer) In particular, for tracking of small target devices, the design should allow a single message/packet transmission of location as a complete transaction.

This document specifies that the LO be contained in the body of a single message.

11. Current Known Open issues

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

1) Should a Proxy somehow label its location information in the 4XX (Retry Location Body) message?

2) Still have not determined how a SIP entity can request location to be delivered in a certain format (civil vs. coordinate).

3) Still have not determined how a UAC can request the UAS return

its location in a 1XX or 2XX response

4) Still have not determined if a Redirect model should be accounted for (if the 3XX response includes LI, does that get included in the new Request by the UAC?)

5) This document needs to be renamed within SIPPING to remove the "requirements" portion

6) From section 9.2 (Emergency call with an updated location), if Alice does venture into another coverage area, how does her new UPDATE with new location get sent to a second (and now appropriate) ERC(2)?

The pending INVITE needs to be cancelled or able to be sequentially forked (which not all Proxies will be able to do). Without that occurring, the new UPDATE will not cause a new INVITE to be originated from the Proxy towards ERC2... and what happens to the UPDATE message (which cannot be an original request into ERC2)?

12. New Open Issues

These are new open issues to be addressed within this document or the topics/areas dropped from consideration:

1) May add a section for end-to-middle in a services model

2) Is there a need to create a new events package for a subscription to a UA to get it's location either at periodic time intervals or when the UA has determined it has moved?

13. 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.

14. IANA Considerations

This section defines two new 4XX error response codes within the sip-parameters section of IANA. [NOTE: RFC XXXX denotes this document.

14.1 IANA Registration for Response Code 4XX

RFC number: XXXX
Response code: 424
Default reason phrase: Bad Location Information

14.2 IANA Registration for Response Code 4XX

RFC number: XXXX
Response code: 425
Default reason phrase: Retry Location Body

15. Acknowledgements

To Dave Oran for helping to shape this idea. To Jon Peterson and Dean Willis on guidance of the effort. To Henning Schulzrinne, Jonathan Rosenberg, Dick Knight, and Keith Drage for constructive feedback.

16. References

16.1 References - Normative

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, "SIP: Session Initiation Protocol ", RFC 3261, June 2002

[2] S. Bradner, "Key words for use in RFCs to indicate requirement levels," RFC 2119, Mar. 1997.

[3] H. Schulzrinne, "draft-ietf-sipping-sos-00.txt", Internet Draft, Feb 2004, Work in progress

[4] B. Campbell, Ed., J. Rosenberg, H. Schulzrinne, C. Huitema, D. Gurle, "Session Initiation Protocol (SIP) Extension for Instant Messaging" , RFC 3428, December 2002

[5] J. Polk, J. Schnizlein, M. Linsner, " DHCP Option for Location Configuration Information", RFC 3825, July 2004

[6] H. Schulzrinne, "draft-ietf-geopriv-dhcp-civic-03.txt", Internet Draft, July 04, Work in progress

[7] J. Cuellar, J. Morris, D. Mulligan, J. Peterson. J. Polk, "Geopriv Requirements", RFC 3693, February 2004

[8] J. Rosenberg, "Requirements for Session Policy for the Session Initiation Protocolö, draft-ietf-sipping-session-policy-req-00", Internet Draft, June, 2003, "work in progress"

[9] J. Rosenberg, "The Session Initiation Protocol (SIP) UPDATE Method", RFC 3311, October 2002

[10] A. Niemi, Ed., "draft-ietf-sip-publish-04", Internet Draft, May 2004, work in progress

[11] H. Schulzrinne, B. Rosen, "draft-schulzrinne-sipping-emergency-arch", Internet Draft, Feb 2004, work in progress

[12] "Requirements for End to Middle Security in SIP", draft-ietf-sipping-e2m-sec-reqs-03.txt, Internet Draft, June 2004, work in progress,

[13] J. Peterson, "draft-ietf-geopriv-pidf-lo-02", Internet Draft, May 2004, work in progress

[14] J. Rosenberg, H. Schulzrinne, "The Offer/Answer Model with Session Description Protocol", RFC 3264, June 2002

[15] R. Sparks, "The Session Initiation Protocol (SIP) Refer Method", RFC 3515, April 2003

17. Author Information

James M. Polk
Cisco Systems
2200 East President George Bush Turnpike 33.00111N
Richardson, Texas 75082 USA 96.68142W
jmpolk@cisco.com

Brian Rosen 40.4N
br@brianrosen.net 80.0W

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

The Expiration date for this Internet Draft is:

April 25th, 2005