Network Working Group
Internet Draft
Expires: April 25, 2011
Intended Status: Standards Track (PS)

James Polk
Cisco Systems
Brian Rosen
Jon Peterson
NeuStar

Oct 25, 2010

Location Conveyance for the Session Initiation Protocol
draft-ietf-sipcore-location-conveyance-04.txt

Abstract

This document defines an extension to the Session Initiation Protocol (SIP) to convey geographic location information from one SIP entity to another SIP entity. The extension covers end-to-end conveyance as well as location-based routing, where SIP intermediaries make routing decisions based upon the location of the user agent client.

Status of this Memo

Copyright Notice

Table of Contents

1. Conventions and Terminology used in this document 3
2. Introduction 3
3. Overview of SIP Location Conveyance 4
   3.1 Location Conveyed by Value 4
   3.2 Location Conveyed as a Location URI 4
   3.3 Location Conveyed though a SIP Intermediary 5
   3.4 SIP Intermediary Replacing Bad Location 6
4. SIP Modifications for Geolocation Conveyance 8
   4.1 The Geolocation Header 8
   4.2 424 (Bad Location Information) Response Code 10
   4.3 The Geolocation-Error Header 11
   4.4 The 'geolocation' Option Tag 14
   4.5 Location URIs in Message Bodies 14
   4.6 Location URIs Allowed 14
5. Geolocation Examples 14
   5.1 Location-by-value (Coordinate Format) 14
   5.2 Two Locations Composed in Same Location Object Example . 16
6. Geopriv Privacy Considerations 18
7. Security Considerations 18
8. IANA Considerations 19
   8.1 IANA Registration for New SIP Geolocation Header 20
   8.2 IANA Registration for New SIP 'geolocation' Option Tag . 20
   8.3 IANA Registration for New 424 Response Code 20
   8.4 IANA Registration for New SIP Geolocation-Error Header . 20
   8.5 IANA Registration for New SIP Geolocation-Error Codes . . 20
   8.6 IANA Registration of Location URI Schemes 21
9. Acknowledgements 21

10. References 22
10.1 Normative References 22
10.2 Informative References 23

Author Information 24
Appendix A. Requirements for SIP Location Conveyance 24

1. Conventions and Terminology 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 [RFC2119]. This document furthermore uses numerous terms defined in RFC 3693 [RFC3693], including Location Objection, Location Recipient, Location Server, Target, and Using Protocol.

2. Introduction

Session Initiation Protocol (SIP) [RFC3261] creates, modifies and terminates multimedia sessions. SIP carries certain information related to a session while establishing or maintaining calls. This document defines how SIP conveys geographic location information of a Target (Target) to a Location Recipient (LR). SIP acts as a Using Protocol of location information, as defined in RFC 3693.

In order to convey location information, this document specifies a new SIP header, the Geolocation header, which carries a reference to a Location Object. That Location Object may appear in a MIME body attached to the SIP request, or it may be a remote resource in the network.

Note that per RFC 3693, a Target is an entity whose location is being conveyed. Thus, a Target could be a SIP user agent (UA), some other IP device (a router or a PC) that does not have a SIP stack, a non-IP device (a person or a black phone) or even a non-communications device (a building or store front). In no way does this document assume that the SIP user agent client which sends a request containing a location object is necessarily the Target. The location of a Target conveyed within SIP typically corresponds to that of a device controlled by the Target, for example, a mobile phone, but such devices can be separated from their owners, and moreover, in some cases the user agent may not know its own location.

In the SIP context, a location recipient will most likely be a SIP UA, but due to the mediated nature of SIP architectures, location information conveyed by a single SIP request may have multiple recipients, as any SIP proxy server in the signaling path that inspects the location of the Target must also be considered a Location Recipient. In presence-like architectures, an intermediary that receives publications of location information and distributes them to watchers acts as a Location Server per RFC 3693. This location conveyance mechanism can also be used to deliver URIs point to such Location Servers where prospective Location Recipients can request Location Objects.

3. Overview of SIP Location Conveyance

An operational overview of SIP location conveyance can be shown in 4 basic diagrams, with most applications falling under one of the following basic use cases. Each is separated into its own subsection here in section 3.

Each diagram has Alice and Bob as UAs. Alice is the Target, and Bob is an LR. A SIP intermediary appears in some of the diagrams. Any SIP entity that receives and inspects location information is an LR, therefore any of the diagrams the SIP intermediary receives the SIP request is potentially an LR - though that does not mean such an intermediary necessarily has to route the SIP request based on the location information. In some use cases, location information passes through the LS on the right of each diagram.

3.1 Location Conveyed by Value

We start with the simplest diagram of Location Conveyance, Alice to Bob, where no other layer 7 entities are involved.

```
      Alice          SIP Intermediary       Bob               LS
        |                |                   |                 |
        |       Request w/Location           |                 |
        |----------------------------------->|                 |
        |                                    |                 |
        |             Response               |                 |
        |<-----------------------------------|                 |
        |                |                   |                 |
```

Figure 1. Location Conveyed by Value

In Figure 1, Alice is both the Target and the LS that is conveying her location directly to Bob, who acts as an LR. This conveyance is point-to-point - it does not pass through any SIP-layer intermediary. A Location Object appears by-value in the initial SIP request as a MIME body, and Bob responds to that SIP request as appropriate. There is a 'Bad Location Information' response code introduced within this document to specifically inform Alice if she conveys bad location to Bob (e.g., Bob "cannot parse the location provided", or "there is not enough location information to determine where Alice is").

3.2 Location Conveyed as a Location URI

Here we make Figure 1 a little more complicated by showing a diagram of indirect Location Conveyance from Alice to Bob, where

Bob's entity has to retrieve the location object from a 3rd party server.

```
      Alice          SIP Intermediary       Bob               LS
        |                |                    |                 |
        |      Request w/Location URI         |                 |
        |----------------------------------->|                 |
        |                                    |    Dereference  |
        |                                    |        Request  |
        |                                   (To: Location URI) |
        |                                    |---------------->|
        |                                    |                 |
        |                                    |    Dereference  |
        |                                    |       Response  |
        |                                  (includes location) |
        |                                    |<----------------|
        |             Response               |                 |
        |<-----------------------------------|                 |
        |                |                    |                 |
```

Figure 2. Location Conveyed as a Location URI

In Figure 2, location is conveyed indirectly, via a Location URI carried in the SIP message (more of those details later). If Alice sends Bob this Location URI, Bob will need to dereference the URI - analogous to Content Indirection [RFC4483] - in order to request the location information. In general, the LS provides the location value to Bob instead of Alice directly. From a user interface perspective, Bob the user won't know that this information was gathered from an LS indirectly rather than culled from the SIP request, and practically this does not impact the operation of location-based applications.

3.3 Location Conveyed though a SIP Intermediary

In Figure 3, we introduce the idea of a SIP intermediary into the example to illustrate the role of proxying in the location architecture. This intermediary could be a SIP proxy or it could be a back-to-back-user-agent (B2BUA). In this message flow, the SIP intermediary could act as a LR, in addition to Bob. The primary use case for intermediaries consuming location information is location-based routing. In this case, the intermediary chooses a next hop for the SIP request by consulting a specialized location service which selects forwarding destinations based on geographical location. In this case, the intermediary acts as a Location Recipient.

```
      Alice          SIP Intermediary       Bob               LS
        |                |                    |                 |
        |   Request      |                   |                 |
        |    w/Location  |                   |                 |
        |--------------->|                   |                 |
        |                |  Request         |                 |
        |                |   w/Location     |                 |
        |                |------------------>|                 |
        |                |                  |                 |
        |                |   Response       |                 |
        |                |<------------------|                 |
        |     Response   |                  |                 |
        |<---------------|                  |                 |
        |                |                  |                 |
```

Figure 3. Location Conveyed though a SIP Intermediary

However, the most common case will be one in which the SIP intermediary receives a request with location information (conveyed either by-value or by-reference) and does not know or care about Alice's location, or support this extension, and merely passes it on to Bob. In this case, the intermediary does not act as a Location Recipient.

Note that an intermediary does not have to perform location-based routing in order to be location recipient. It could be the case that a SIP intermediary which does not perform location-based routing but does care when Alice includes her location; for example, it could care that the location information is complete or that it correctly identifies where Alice is. The best example of this is intermediaries that verify location information for emergency calling, but it could also be for any location based routing - e.g., contacting Pizza Hut, making sure that organization has Alice's proper location in the initial SIP request.

There is another scenario in which the SIP intermediary cares about location and is not an LR, one in which the intermediary inserts another location of the Target, Alice in this case, into the request, and forwards it. This secondary insertion is generally not advisable because downstream SIP entities will not be given any guidance about which location to believe is better, more reliable, less prone to error, more granular, worse than the other location or just plain wrong.

The only conceivable way forward, when a second location is placed into the same SIP request by a SIP intermediary is to take a "you break it, you bought it" philosophy with respect to the inserting SIP intermediary. That entity becomes completely responsible for all location within that SIP request (more on this in Section 4).

3.4 SIP Intermediary Replacing Bad Location

If the SIP intermediary rejects the message due to unsuitable location information (we are not going to discuss any other reasons in this document, and there are many), the SIP response will indicate there was 'Bad Location Information' in the SIP request, and provide a location specific error code indicating what Alice needs to do to send an acceptable request (see Figure 4 for this scenario).

```
      Alice          SIP Intermediary       Bob               LS
        |                |                   |                 |
        |   Request      |                   |                 |
        |    w/Location  |                   |                 |
        |--------------->|                   |                 |
        |                |                   |                 |
        |   Rejected     |                   |                 |
        | w/New Location |                   |                 |
        |<---------------|                   |                 |
        |                |                   |                 |
        |   Request      |                   |                 |
        | w/New Location |                   |                 |
        |--------------->|                   |                 |
        |                |    Request        |                 |
        |                |  w/New Location   |                 |
        |                |------------------>|                 |
        |                |                   |                 |
```

Figure 4. SIP Intermediary Replacing Bad Location

In this last use case, the SIP intermediary wishes to include a Location Object indicating where it understands Alice to be. Thus, it must inform her user agent what location she should include in any subsequent SIP request that contains her location. In these cases, the intermediary can reject Alice's request, through the SIP response, convey to her the best way to repair the request in order for the intermediary to accept it.

Overriding location information provided by the user requires a deployment where an intermediary necessarily knows better than an end user - after all, it could be that Alice has an on-board GPS, and the SIP intermediary only knows her nearest cell tower. Which is more accurate location information? Currently, there is no way to tell which entity is more accurate, or which is wrong - for that matter. This document will not specify how to indicate which location is more accurate than another. If desired, intermediaries may furthermore allow both Alice's internally generated location, as well as the SIP intermediary's determination of where Alice, to appear in the same SIP request (the resubmitted one), and permit that to be forwarded to Bob. This case is discussed in more detail in section 4.2 of this document.

As an aside, it is not envisioned that any SIP-based emergency services request (i.e., IP-911, or 112 type of call attempt) will receive a corrective 'Bad Location Information' response from an intermediary. Most likely, the SIP intermediary would in that scenario act a B2BUA and insert into the request by-value any appropriate location information for the benefit of Public Safety Answering Point (PSAP) call centers to expedite call reception by the emergency services personnel; thereby, minimizing any delay in call establishment time. The implementation of these specialized deployments is, however, outside the scope of this document.

4. SIP Modifications for Geolocation Conveyance

The following sections detail the modifications to SIP for location conveyance.

4.1 The Geolocation Header

This document defines "Geolocation" as a new SIP header field registered by IANA, with the following ABNF [RFC5234]:

```
Geolocation-header = "Geolocation" HCOLON Geolocation-value
Geolocation-value  = ( locationValue [ COMMA locationValue ] )
                     / routing-param
locationValue      =  LAQUOT locationURI RAQUOT
                       *(SEMI geoloc-param)
locationURI        =  sip-URI / sips-URI / pres-URI
                       / http-URI / HTTPS-URI
                       / cid-url ; (from RFC 2392)
                       / absoluteURI ; (from RFC 3261)
geoloc-param       =  generic-param;  (from RFC 3261)
routing-param      =  "routing-allowed" EQUAL "yes" / "no"
```

sip-URI, sips-URI and absoluteURI are defined according to [RFC3261].

The pres-URI is defined in [RFC3859].

HTTP-URI and HTTPS-URI are defined according to [RFC2616] and [RFC2818], respectively.

The cid-url is defined in [RFC2392] to locate message body parts. This URI type is present in a SIP request when location is conveyed as a MIME body in the SIP message.

GEO-URIs [RFC5870] are not appropriate for usage the SIP Geolocation header.

Other URI schemas used in the location URI MUST be reviewed against the RFC 3693 [RFC3693] criteria for a Using Protocol.

The Geolocation header field has zero, one or two locationValues, but MUST NOT contain more than two locationValue. A SIP intermediary SHOULD NOT add location to a SIP request that already contains location. This will quite often lead to confusion within LRs.

However, if a SIP intermediary were to add location, even if location was not previously present in a SIP request, that SIP intermediary is fully responsible for addressing the concerns of any 424 (Bad Location Information) SIP response it receives about this location addition, and MUST NOT pass on (upstream) the 424 response.

The placement of the "routing-allowed" header field parameter, strongly encouraged by [RFC5606], is outside the locationValue, and MUST always be last in the header field value. The routing-allowed parameter MUST be present, even when no locationValue is present. This scenario sets the routing-allowed policy downstream along the request's signaling path. This header field parameter only has the values "=yes" or "=no". When this parameter is "=yes", the locationValue can be used for routing decisions along the downstream signaling path by intermediaries. If no routing-allowed parameter is present in a SIP request, a SIP intermediary MAY insert this value with a RECOMMENDED value of "no" by default.

When this parameter is "=no", this means no locationValue (inserted by the originating UAC or any intermediary along the signaling path can be used by any SIP intermediary to make routing decisions. Intermediaries that attempt to use the location information for routing purposes in spite of this counter indication may end up routing the request improperly as a result. Sections 4.3 describes the details on what a routing intermediary does if it determines it needs to use the location in the SIP request in order to process the message further.

The practical implication is that when the "routing-allowed" parameter is set to "no", if a cid:url is present in the SIP request, intermediaries MUST NOT view the location (because it is not for intermediaries to view), and if a location URI is present, intermediaries MUST NOT dereference it. UAs are allowed to view location in the SIP request even when the "routing-allowed" parameter is set to "no". An LR MUST by default consider the "routing-allowed" header parameter as set to "no", with no exceptions, unless the header field value is set to "yes".

If a routing-allowed parameter is parsed as set to "=yes", an implementation MUST parse the rest of the SIP headers for another instance of the Geolocation header value to determine if there is another instance of the routing-allowed parameter set to "=no". If this is the case, the behavior MUST be to process the "=no" indication only, and ignore the "=yes".

This document defines the Geolocation header field as valid in the following SIP requests:

INVITE [RFC3261],
OPTIONS [RFC3261],
UPDATE [RFC3311],
REGISTER [RFC3261],
BYE [RFC3261],
INFO [RFC2976],

MESSAGE [RFC3428],
SUBSCRIBE [RFC3265],
PUBLISH [RFC3903],
REFER [RFC3515],
NOTIFY [RFC3265],
PRACK [RFC3262]

The following table extends the values in Tables 2 and 3 of RFC 3261 [RFC3261].

Header field	where	proxy	INV	ACK	CAN	BYE	REG	OPT	PRA
Geolocation	R	ar	o	-	-	o	o	o	o
Geolocation	424	r	o	-	-	o	o	o	o

Header field	where	proxy	SUB	NOT	UPD	MSG	REF	INF	PUB
Geolocation	R	ar	o	o	o	o	o	o	o
Geolocation	424	r	o	o	o	o	o	o	o

Table 1: Summary of the Geolocation Header Field

The Geolocation header field MAY be included in any one of the optional requests by a UA. A proxy MAY add the Geolocation header field, but MUST NOT modify any pre-existing locationValue, including the "routing-allowed" header field value.

A SIP intermediary MAY add a Geolocation header field if one is not present - for example, when a user agent does not support the Geolocation mechanism but their outbound proxy does and knows their location, or any of a number of other use cases (see Section 3). When adding a Geolocation header, a SIP intermediary MAY supply the "routing-allowed" parameter if not yet present in the SIP request, but MUST NOT add a "routing-allowed" parameter if one is already present in this SIP request.

SIP implementations are advised to pay special attention to the policy elements for location retransmission and retention described in RFC 4119.

4.2 424 (Bad Location Information) Response Code

This SIP extension creates a new location-specific response code, defined as follows,

424 (Bad Location Information)

The 424 (Bad Location Information) response code is a rejection of the request due to its location contents, indicating location information that was malformed or not satisfactory for the recipient's purpose, or could not be dereferenced.

A SIP intermediary can also reject a location it receives from a Target when it understands the Target to be in a different location. The proper handling of this scenario, described in Section 3.4, is for the SIP intermediary to include the proper location in the 424 Response. This SHOULD be included in the response as a MIME message body (i.e., a location value), rather than as a URI; however, in cases where the intermediary is willing to share location with recipients but not with a user agent, a reference might be necessary.

As mentioned in Section 3.4, it might be the case that the intermediary does not want to chance providing less accurate location information than the user agent; thus it will compose its understanding of where the user agent is in a separate <geopriv> element of the same PIDF-LO message body in the SIP response (which also contains the Target's version of where it is). Therefore, both locations are included - each with different <method> elements. The proper reaction of the user agent is to generate a new SIP request that includes this composed location object, and send it towards the original LR. SIP intermediaries can verify that subsequent requests properly insert the suggested location information before forwarding said requests.

SIP intermediaries MUST NOT add, modify or delete the location in a 424 response. This specifically applies to intermediaries that are between the 424 response generator and the original UAC. All respects of the Geolocation and Geolocation-Error headers and PIDF-LO(s) MUST remain unchanged, never added to or deleted.

Section 4.3 describes a Geolocation-Error header field to provide more detail about what was wrong with the location information in the request. This header field MUST be included in the 424 response.

It is only appropriate to generate a 424 response when the responding entity needs a locationValue and there are no locationValues included in the SIP request that are usable by that recipient, or as shown in Figure 4 of section 3.4. In this scenario, a SIP intermediary is informing the upstream UA which location to include in the next SIP request.

A 424 MUST NOT be sent in response to a request that lacks a Geolocation header entirely, as the user agent in that case may not support this extension at all. If a SIP intermediary inserted a locationValue into a SIP request where one was not previously present, it MUST take any and all responsibility for the corrective action if it receives a 424 to a SIP request it sent.

A 424 (Bad Location Information) response is a final response within a transaction, and MUST NOT terminate an existing dialog.

4.3 The Geolocation-Error Header

As discussed in Section 4.2, more granular error notifications specific to location errors within a received request are required if the UA is to know what was wrong within the original request. The Geolocation-Error header field is used for this purpose.

The Geolocation-Error header field is used to convey location-specific errors within a response. The Geolocation-Error header field has the following ABNF [RFC5234]:

```
Geolocation-Error        = "Geolocation-Error" HCOLON
                             locationErrorValue
locationErrorValue       = location-error-arg
location-error-arg       = location-error-code
                            *(SEMI location-error-params)
location-error-code      = 1*3DIGIT
location-error-params    = location-error-code-text
                           / generic-param ; from RFC3261
location-error-code-text = "code" EQUAL quoted-string ; from RFC3261
```

The Geolocation-Error header field MUST contain only one locationErrorValue to indicate what was wrong with the locationValue the Location Recipient determined was bad. The locationErrorValue contains a 3-digit error code indicating what was wrong with the location in the request. Each error code has a corresponding quoted error text string that is human understandable. This text string is OPTIONAL, but RECOMMENDED for human readability.

The following table extends the values in Table 2&3 of RFC 3261 [RFC3261].

Header field	where	proxy	INV	ACK	CAN	BYE	REG	OPT	PRA
Geolocation-Error	r	ar	o	-	-	o	o	o	o

Header field	where	proxy	SUB	NOT	UPD	MSG	REF	INF	PUB
Geolocation-Error	r	ar	o	o	o	o	o	o	o

Table 2: Summary of the Geolocation-Error Header Field

The Geolocation-Error header field MAY be included in any response to one of the above SIP requests, so long as a Geolocation locationValue was in the request part of the transaction. For example, Alice includes her location in an INVITE to Bob. Bob can accept this INVITE, thus creating a dialog, even though his UA determined the location contained in the INVITE was bad. Bob merely includes a Geolocation-Error header value in the 200 OK to the INVITE informing Alice the INVITE was accepted but the location provided was bad. The SIP requests included in table 2 above are the ones allowed to optionally contain the Geolocation header field (see section 4.1).

If, on the other hand, Bob cannot accept Alice's INVITE without a suitable location, a 424 (Bad Location Information) is sent. This message flow is shown in Figures 1, 2 or 3 in Section 3.

The following subsections provide an initial list of location based errors for any SIP non-100 response, including the new 424 (Bad Location Information) response. These error codes are divided into 4 categories, based on how the response receiver should react to these errors.

- 1XX errors mean the LR cannot process the location within the request.

- 2XX errors mean the LR wants the LS to send new or updated location information, perhaps with a delay associated with when to send the request.

- 3XX errors mean some specific permission is necessary to process the included location information.

- 4XX errors mean there was trouble dereferencing the Location URI sent.

Within these 4 number ranges, there is a top level error as follows:

```
Geolocation-Error: 100 "Cannot Process Location"

Geolocation-Error: 200 "Retry Location Later with device updated
                        location"

Geolocation-Error: 300 "Permission To Use Location Information"

Geolocation-Error: 400 "Dereference Failure"
```

There are two specific Geolocation-Error codes necessary to include in this document, both have to do with permissions necessary to process the SIP request; they are

```
Geolocation-Error: 301 "Permission To Retransmit Location
                     Information to a Third Party"
```

This location error is specific to having the Presence Information Data Format (PIDF-LO) [RFC4119] <retransmission-allowed> element set to "=no". This location error is stating it requires permission (i.e., PIDF-LO <retransmission-allowed> element set to "=yes") to process this SIP request further. If the LS sending the location information does not want to give this permission, it will not reset this permission in a new request. If the LS wants this message processed without this permission reset, it MUST choose another logical path (if one exists).

```
Geolocation-Error: 302 "Permission to Route based on Location
```

Information"

This location error is specific to having the locationValue header parameter <routing-allowed> set to "=no". This location error is stating it requires permission (i.e., a <routing-allowed> set to "=yes") to process this SIP request further. If the LS sending the location information does not want to give this permission, it will not reset this permission in a new request. If the LS wants this message processed without this permission reset, it MUST choose another logical path (if one exists).

4.4 The 'geolocation' Option Tag

This document creates and registers with the IANA one new option tag: "geolocation". This option tag is to be used, as defined in [RFC3261], in the Require, Supported and Unsupported header fields.

4.5 Location URIs in Message Bodies

In the case where a location recipient sends a 424 response and wishes to communicate suitable location by reference rather than by value, the 424 MUST include a content-indirection body per RFC 4483.

4.6 Location URIs Allowed

The following is part of the discussion started in Section 3, Figure 2, which introduced the concept of sending location indirectly.

If a location URI is included in a SIP request, it SHOULD be a SIP-, SIPS- or PRES-URI. When PRES: is used, as defined in [RFC3856], if the resulting resolution resolves to a SIP: or SIPS: URI, this section applies. These schemes MUST be implemented according to this document.

See [ID-GEO-FILTERS] for more details on dereferencing location.

An HTTP: [RFC2616] or HTTPS: URI [RFC2818] are also allowed, and SHOULD be dereferenced according to [ID-HELD-DEREF].

5. Geolocation Examples

5.1 Location-by-value (in Coordinate Format)

This example shows an INVITE message with a coordinate location. In this example, the SIP request uses a sips-URI [RFC3261], meaning this message is protected using TLS on a hop-by-hop basis.

```
INVITE sips:bob@biloxi.example.com SIP/2.0
Via: SIPS/2.0/TLS pc33.atlanta.example.com;branch=z9hG4bK74bf9
```

```
   Max-Forwards: 70
   To: Bob <sips:bob@biloxi.example.com>
```

```
From: Alice <sips:alice@atlanta.example.com>;tag=9fxced76sl
Call-ID: 3848276298220188511@atlanta.example.com
Geolocation: <cid:target123@atlanta.example.com>
  ;routing-allowed=no
Supported: geolocation
Accept: application/sdp, application/pidf+xml
CSeq: 31862 INVITE
Contact: <sips:alice@atlanta.example.com>
Content-Type: multipart/mixed; boundary=boundary1
Content-Length: ...

--boundary1

Content-Type: application/sdp

...SDP goes here

--boundary1

Content-Type: application/pidf+xml
Content-ID: <target123@atlanta.example.com>
<?xml version="1.0" encoding="UTF-8"?>
    <presence
       xmlns="urn:ietf:params:xml:ns:pidf"
       xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
       xmlns:gbp="urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy"
       xmlns:cl="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
       xmlns:gml="http://www.opengis.net/gml"
       xmlns:dm="urn:ietf:params:xml:ns:pidf:data-model"
       entity="pres:alice@atlanta.example.com">
     <dm:device id="target123-1">
       <gp:geopriv>
         <gp:location-info>
           <gml:location>
             <gml:Point srsName="urn:ogc:def:crs:EPSG::4326">
               <gml:pos>32.86726 -97.16054</gml:pos>
             </gml:Point>
          </gml:location>
         </gp:location-info>
         <gp:usage-rules>
           <gbp:retransmission-allowed>false
           </gbp:retransmission-allowed>
           <gbp:retention-expiry>2010-11-14T20:00:00Z
           </gbp:retention-expiry>
         </gp:usage-rules>
         <gp:method>802.11</gp:method>
       </gp:geopriv>
       <dm:deviceID>mac:1234567890ab</dm:deviceID>
       <dm:timestamp>2010-11-04T20:57:29Z</dm:timestamp>
```

```
        </dm:device>
      </presence>
   --boundary1--
```

The Geolocation header field from the above INVITE:

```
Geolocation: <cid:target123@atlanta.example.com>
```

... indicates the content-ID location [RFC2392] within the multipart message body of where location information is. An assumption can be made that SDP is the other message body part. The "cid:" eases message body parsing by disambiguating the MIME body that contains the location information associated with this request.

If the Geolocation header field did not contain a "cid:" scheme, for example, it could look like this location URI:

```
Geolocation: <sips:target123@server5.atlanta.example.com>
```

... the existence of a non-"cid:" scheme indicates this is a location URI, to be dereferenced to learn the Target's location. Any node wanting to know where user "target123" is would subscribe to that user at server5 to dereference the sips-URI (see Figure 3 in section 3 for this message flow).

5.2 Two Locations Composed in Same Location Object Example

This example shows the INVITE message after a SIP intermediary rejected the original INVITE (say, the one in section 5.1). This INVITE contains the composed LO sent by the SIP intermediary which includes where the intermediary understands Alice to be. The rules of RFC 5491 [RFC5491] are followed in this construction.

This example is here, but should not be taken as occurring very often. In fact, this is believed to be a corner case of location conveyance applicability.

```
INVITE sips:bob@biloxi.example.com SIP/2.0
Via: SIPS/2.0/TLS pc33.atlanta.example.com;branch=z9hG4bK74bf0
Max-Forwards: 70
To: Bob <sips:bob@biloxi.example.com>
From: Alice <sips:alice@atlanta.example.com>;tag=9fxced76sl
Call-ID: 3848276298220188512@atlanta.example.com
Geolocation: <cid:target123@atlanta.example.com>
  ;routing-allowed=no
Supported: geolocation
Accept: application/sdp, application/pidf+xml
CSeq: 31863 INVITE
Contact: <sips:alice@atlanta.example.com>
Content-Type: multipart/mixed; boundary=boundary1
Content-Length: ...

--boundary1
```

```
   Content-Type: application/sdp
   ...SDP goes here

   --boundary1

   Content-Type: application/pidf+xml
   Content-ID: <target123@atlanta.example.com>
   <?xml version="1.0" encoding="UTF-8"?>
       <presence
          xmlns="urn:ietf:params:xml:ns:pidf"
          xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
          xmlns:gbp="urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy"
          xmlns:dm="urn:ietf:params:xml:ns:pidf:data-model"
          xmlns:cl="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
          xmlns:gml="http://www.opengis.net/gml"
          entity="pres:alice@atlanta.example.com">
        <dm:device id="target123-1">
          <gp:geopriv>
            <gp:location-info>
              <gml:location>
                <gml:Point srsName="urn:ogc:def:crs:EPSG::4326">
                  <gml:pos>32.86726 -97.16054</gml:pos>
                </gml:Point>
              </gml:location>
            </gp:location-info>
            <gp:usage-rules>
              <gbp:retransmission-allowed>false
              </gbp:retransmission-allowed>
              <gbp:retention-expiry>2010-11-14T20:00:00Z
              </gbp:retention-expiry>
            </gp:usage-rules>
            <gp:method>802.11</gp:method>
          </gp:geopriv>
          <dm:deviceID>mac:1234567890ab</dm:deviceID>
          <dm:timestamp>2010-11-04T20:57:29Z</dm:timestamp>
        </dm:device>
        <dm:person id="target123">
          <gp:geopriv>
            <gp:location-info>
              <cl:civicAddress>
                <cl:country>US</cl:country>
                <cl:A1>Texas</cl:A1>
                <cl:A3>Colleyville</cl:A3>
                <cl:RD>Treemont</cl:RD>
                <cl:STS>Circle</cl:STS>
                <cl:HNO>3913</cl:HNO>
                <cl:FLR>1</cl:FLR>
                <cl:NAM>Haley's Place</cl:NAM>
                <cl:PC>76034</cl:PC>
              </cl:civicAddress>
            </gp:location-info>
            <gp:usage-rules>
```

```
              <gbp:retransmission-allowed>false
              </gbp:retransmission-allowed>
              <gbp:retention-expiry>2010-11-14T20:00:00Z
              </gbp:retention-expiry>
            </gp:usage-rules>
            <gp:method>triangulation</gp:method>
          </gp:geopriv>
          <dm:timestamp>2010-11-04T12:28:04Z</dm:timestamp>
        </dm:person>
      </presence>
   --boundary1--
```

6. Geopriv Privacy Considerations

Location information is considered by most to be highly sensitive information, requiring protection from eavesdropping and altering in transit. [RFC3693] originally articulated rules to be followed by any protocol wishing to be considered a "Using Protocol", specifying how a transport protocol meets those rules. [ID-GEOPRIV-ARCH] updates the guidance in RFC3693 to include subsequently-introduced entities and concepts in the geolocation architecture. Implementations of this SIP location conveyance mechanism MUST adhere to the guidance given in RFC3693 and its successors, including (but not limited to) the handling of rules for retention and retransmission.

7. Security Considerations

Conveyance of physical location of a UA raises privacy concerns, and depending on use, there probably will be authentication and integrity concerns. This document calls for conveyance to be accomplished through secure mechanisms, like S/MIME encrypting message bodies (although this is not widely deployed), TLS protecting the overall signaling or conveyance location by-reference and requiring all entities that dereference location to authenticate themselves. In location-based routing cases, encrypting the location payload with an end-to-end mechanism such as S/MIME is problematic, because one or more proxies on the path need the ability to read the location information to retarget the message to the appropriate new destination UAS. Data can only be encrypted to a particular, anticipated target, and thus if multiple recipients need to inspect a piece of data, and those recipients cannot be predicted by the sender of data, encryption is not a very feasible choice. Securing the location hop-by-hop, using TLS, protects the message from eavesdropping and modification in transit, but exposes the information to all proxies on the path as well as the endpoint. In most cases, the UA has no trust relationship with the proxy or proxies providing location-based routing services, so such end-to-middle solutions might not be appropriate either.

When location information is conveyed by reference, however, one can properly authenticate and authorize each entity that wishes to inspect location information. This does not require that the sender of data anticipate who will receive data, and it does permit multiple entities to receive it securely, but it does not however obviate the need for pre-association between the sender of data and any prospective recipients. Obviously, in some contexts this pre-association cannot be presumed; when it is not, effectively unauthenticated access to location information must be permitted. In this case, choosing pseudo-random URIs for location by-reference, coupled with path encryption like SIPS, can help to ensure that only entities on the SIP signaling path learn the URI, and thus restores rough parity with sending location by-value.

Location information is especially sensitive when the identity of its Target is obvious. Note that there is the ability, according to [RFC3693] to have an anonymous identity for the Target's location. This is accomplished by use of an unlinkable pseudonym in the "entity=" attribute of the <presence> element [RFC4479]. Though, this can be problematic for routing messages based on location (covered in the document above). Moreover, anyone fishing for information would correlate the identity at the SIP layer with that of the location information referenced by SIP signaling.

When a UA inserts location, the UA sets the policy on whether to reveal its location along the signaling path - as discussed in Section 4, as well as flags in the PIDF-LO [RFC4119]. UAC implementations MUST make such capabilities conditional on explicit user permission, and MUST alert the user that location is being conveyed.

This SIP extension offers the default ability to require permission to view location while the SIP request is in transit. The default for this is set to "no". There is an error explicitly describing how an intermediary asks for permission to view the Target's location, plus a rule stating the user has to be made aware of this permission request.

There is no end-to-end integrity on any locationValue or locationErrorValue header field parameter (or middle-to-end if the value was inserted by a intermediary), so recipients of either header field need to implicitly trust the header field contents, and take whatever precautions each entity deems appropriate given this situation.

8. IANA Considerations

The following are the IANA considerations made by this SIP extension. Modifications and additions to these registrations require a standards track RFC (Standards Action).

[Editor's Note: RFC-Editor - within the IANA section, please

replace "this doc" with the assigned RFC number,
if this document reaches publication.]

8.1 IANA Registration for the SIP Geolocation Header Field

The SIP Geolocation Header Field is created by this document, with its definition and rules in Section 4.1 of this document, and should be added to the IANA sip-parameters registry, in the portion titled "Header Field Parameters and Parameter Values".

Header Field	Parameter Name	Predefined Values	Reference
Geolocation	routing-allowed	yes	[this doc]

8.2 IANA Registration for New SIP 'geolocation' Option Tag

The SIP option tag "geolocation" is created by this document, with the definition and rule in Section 4.4 of this document, to be added to the IANA sip-parameters registry.

8.3 IANA Registration for 424 Response Code

Reference: RFC-XXXX (i.e., this document)
Response code: 424 (recommended number to assign)
Default reason phrase: Bad Location Information

This SIP Response code is defined in section 4.2 of this document.

8.4 IANA Registration of New Geolocation-Error Header Field

The SIP Geolocation-error header field is created by this document, with its definition and rules in Section 4.3 of this document, to be added to the IANA sip-parameters registry, in the portion titled "Header Field Parameters and Parameter Values".

Header Field	Parameter Name	Predefined Values	Reference
Geolocation-Error	code=	yes*	[this doc]

* see section 8.5 for the newly created values.

8.5 IANA Registration for the SIP Geolocation-Error Codes

New location specific Geolocation-Error codes are created by this document, and registered in a new table in the IANA sip-parameters registry. Details of these error codes are in Section 4.3 of this document.

Geolocation-Error codes

Geolocation-Error codes provide reason for the error discovered by Location Recipients, categorized by action to be taken by error recipient.

Code	Description	Reference
100	"Cannot Process Location"	[this doc]
200	"Retry Location Later with device updated location"	[this doc]
300	"Permission To Use Location Information"	[this doc]
301	"Permission To Retransmit Location Information to a Third Party"	[this doc]
302	"Permission to Route based on Location Information"	[this doc]
400	"Dereference Failure"	[this doc]

8.6 IANA Registration of Location URI Schemes

This document directs IANA to create a new set of parameters in a separate location from SIP and Geopriv, called the "Location Reference URI" registry, containing the URI scheme, the Content-Type, and the reference, as follows:

URI Scheme	Content-Type	Reference
SIP:		[this doc]
SIPS:		[this doc]
PRES:		[this doc]
HTTP:		[this doc]
HTTPS:		[this doc]

Additions to this registry must be defined in a permanent and readily available specification (this is the "Specification Required" IANA policy defined in [RFC5226]).

9. Acknowledgements

To Dave Oran for helping to shape this idea.

To Dean Willis for guidance of the effort.

To Allison Mankin, Dick Knight, Hannes Tschofenig, Henning

Schulzrinne, James Winterbottom, Jeroen van Bemmel, Jean-Francois Mule, Jonathan Rosenberg, Keith Drage, Marc Linsner, Martin Thomson, Mike Hammer, Ted Hardie, Shida Shubert, Umesh Sharma, Richard Barnes, Dan Wing, Matt Lepinski, John Elwell and Jacqueline Lee for constructive feedback and nits checking.

Special thanks to Paul Kyzivat for his help with the ABNF in this document and to Robert Sparks for many helpful comments and the proper construction of the Geolocation-Error header field.

And finally, to Spencer Dawkins for giving this doc a good scrubbing to make it more readable.

10. References

10.1 Normative References

[RFC3261] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, May 2002.

[RFC4119] J. Peterson, "A Presence-based GEOPRIV Location Object Format", RFC 4119, December 2005

[RFC2119] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997

[RFC2392] E. Levinson, " Content-ID and Message-ID Uniform Resource Locators", RFC 2392, August 1998

[RFC3856] J. Rosenberg, " A Presence Event Package for the Session Initiation Protocol (SIP)", RFC 3856, August 2004

[RFC3859] J. Peterson, "Common Profile for Presence (CPP)", RFC 3859, August 2004

[RFC3428] B. Campbell, Ed., J. Rosenberg, H. Schulzrinne, C. Huitema, D. Gurle, "Session Initiation Protocol (SIP) Extension for Instant Messaging" , RFC 3428, December 2002

[RFC3311] J. Rosenberg, "The Session Initiation Protocol (SIP) UPDATE Method", RFC 3311, October 2002

[RFC3265] Roach, A, "Session Initiation Protocol (SIP)-Specific Event Notification", RFC 3265, June 2002.

[RFC3262] Rosenberg, J. and H. Schulzrinne, "Reliability of Provisional Responses in Session Initiation Protocol (SIP)", RFC 3262, June 2002.

[RFC2976] S. Donovan, "The SIP INFO Method", RFC 2976, Oct 2000

[RFC3515] R. Sparks, "The Session Initiation Protocol (SIP) Refer Method", RFC 3515, April 2003

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

[RFC5234] Crocker, D., Ed., and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

[RFC5226] T. Narten, H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 5226, May 2008

[RFC4479] J. Rosenberg, "A Data Model for Presence", RFC 4479, July 2006

[RFC3264] J. Rosenberg, H. Schulzrinne, "The Offer/Answer Model with Session Description Protocol", RFC 3264, June 2002

[RFC4483] E. Berger, "A Mechanism for Content Indirection in SIP", RFC 4483, May 2006

[RFC5491] J. Winterbottom, M. Thomson, H. Tschofenig, "GEOPRIV PIDF-LO Usage Clarification, Considerations, and Recommendations ", RFC 5491, March 2009

[RFC5870] A. Mayrhofer, C. Spanring, "A Uniform Resource Identifier for Geographic Locations ('geo' URI)", RFC 5870, June 2010

[RFC5606] J. Peterson, T. Hardie, J. Morris, "Implications of 'retransmission-allowed' for SIP Location Conveyance", RFC5606, Oct 2008

[RFC2616] R. Fielding, J. Gettys, J., Mogul, H. Frystyk, L., Masinter, P. Leach, T. Berners-Lee, "Hypertext Transfer Protocol - HTTP/1.1", RFC 2616, June 1999

10.2 Informative References

[RFC3693] J. Cuellar, J. Morris, D. Mulligan, J. Peterson. J. Polk, "Geopriv Requirements", RFC 3693, February 2004

[RFC2818] E. Rescorla, "HTTP Over TLS", RFC 2818, May 2000

[ID-GEO-FILTERS] R. Mahy, B. Rosen, H. Tschofenig, "Filtering Location Notifications in SIP", draft-ietf-geopriv-loc-filters, "work in progress", March 2010

[ID-HELD-DEREF] J. Winterbottom, H. Tschofenig, H. Schulzrinne, M.

Thomson, M. Dawson, "A Location Dereferencing Protocol Using HELD", "work in progress", September 2010

[ID-GEO-ARCH] R. Barnes, M. Lepinski, A. Cooper, J, Morris, H. Tschofenig, H. Schulzrinne, "An Architecture for Location and Location Privacy in Internet Applications", draft-ietf-geopriv-arch, "work in progress", October 2010

Author Addresses

James Polk
Cisco Systems
3913 Treemont Circle
Colleyville, Texas 76034

33.00111N
96.68142W

Phone: +1-817-271-3552
Email: jmpolk@cisco.com

Brian Rosen
NeuStar, Inc.
470 Conrad Dr.
Mars, PA 16046

40.70497N
80.01252W

Phone: +1 724 382 1051
Email: br@brianrosen.net

Jon Peterson
NeuStar, Inc.

Email: jon.peterson@neustar.biz

Appendix A. Requirements for SIP Location Conveyance

The following subsections address the requirements placed on the UAC, the UAS, as well as SIP proxies when conveying location. If a requirement is not obvious in intent, a motivational statement is included below it.

A.1 Requirements for a UAC Conveying Location

UAC-1 The SIP INVITE Method [RFC3261] must support location conveyance.

UAC-2 The SIP MESSAGE method [RFC3428] must support location conveyance.

UAC-3 SIP Requests within a dialog should support location conveyance.

UAC-4 Other SIP Requests may support location conveyance.

UAC-5 There must be one, mandatory to implement means of transmitting location confidentially.

Motivation: to guarantee interoperability.

UAC-6 It must be possible for a UAC to update location conveyed at any time in a dialog, including during dialog establishment.

Motivation: if a UAC has moved prior to the establishment of a dialog between UAs, the UAC must be able to send location information. If location has been conveyed, and the UA moves, the UAC must be able to update the location previously conveyed to other parties.

UAC-7 The privacy and security rules established within [RFC3693] that would categorize SIP as a 'Using Protocol' must be met.

UAC-8 The PIDF-LO [RFC4119] is a mandatory to implement format for location conveyance within SIP.

Motivation: interoperability with other IETF location protocols and Mechanisms.

UAC-9 There must be a mechanism for the UAC to request the UAS send its location.

UAC-9 has been DEPRECATED by the SIP WG, due to the many problems this requirement would have caused if implemented. The solution is for the above UAS to send a new request to the original UAC with the UAS's location.

UAC-10 There must be a mechanism to differentiate the ability of the UAC to convey location from the UACs lack of knowledge of its location

Motivation: Failure to receive location when it is expected can happen because the UAC does not implement this extension, or because the UAC implements the extension, but does not know where the Target is. This may be, for example, due to the failure of the access network to provide a location acquisition mechanism the UAC supports. These cases must be differentiated.

UAC-11 It must be possible to convey location to proxy servers along the path.

Motivation: Location-based routing.

A.2 Requirements for a UAS Receiving Location

The following are the requirements for location conveyance by a UAS:

UAS-1 SIP Responses must support location conveyance.

Just as with UAC-9, UAS-1 has been DEPRECATED by the SIP WG, due to the many problems this requirement would have caused if implemented. The solution is for the above UAS to send a new request to the original UAC with the UAS's location.

UAS-2 There must be a unique 4XX response informing the UAC it did not provide applicable location information.

In addition, requirements UAC-5, 6, 7 and 8 also apply to the UAS.

A.3 Requirements for SIP Proxies and Intermediaries

The following are the requirements for location conveyance by a SIP proxies and intermediaries:

Proxy-1 Proxy servers must be capable of adding a Location header field during processing of SIP requests.

Motivation: Provide network assertion of location when UACs are unable to do so, or when network assertion is more reliable than UAC assertion of location

Note: Because UACs connected to SIP signaling networks may have widely varying access network arrangements, including VPN tunnels and roaming mechanisms, it may be difficult for a network to reliably know the location of the endpoint. Proxy assertion of location is NOT RECOMMENDED unless the SIP signaling network has reliable knowledge of the actual location of the Targets.

Proxy-2 There must be a unique 4XX response informing the UAC it did not provide applicable location information.