SIP Working Group   James Polk
Internet Draft   Cisco Systems
Expires: September 9, 2009   Brian Rosen
Intended Status: Standards Track (PS)   NeuStar
                                                            March 9, 2009

Location Conveyance for the Session Initiation Protocol
draft-ietf-sip-location-conveyance-13.txt

Status of this Memo

Copyright Notice

Legal

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 servers make routing decisions based on the location of the user agent clients.

Table of Contents

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].

The following terms and acronyms used throughout this document are defined here:

"cid=" = content-ID URI. See Section 4.1 for more details.

Content-ID - Defined in RFC 2392 as a URL reference to find message body parts within the same message, to ease parsing.

LbyR = Location-by-Reference

LbyV = Location-by-Value

locationErrorValue - contains an actionable error code from a Location Recipient, identifying the location "inserter=", and optionally a test string describing the type of error. There can be one or more locationErrorValues within a Geolocation-Error header in a SIP response. See Section 4.3 for more details.

locationValue - contains a URI pointing to a Location Target's location (as a PIDF-LO), and one or more header parameters about that URI. There can be one or more locationValues within a Geolocation header in a SIP request. See Section 4.1 for more details.

Location Generator - the first IP enabled device that builds the IP packet that transmits the PIDF-LO containing the Target's location

Location Information Server (LIS) - a logical server that stores geolocation records, which correspond to LbyR URIs, which point to those records.

Location Object - Defined in RFC 4119 as the PIDF-LO (XML scheme) format which includes the geolocation of Location Target in either civic address or coordinate form.

Location Recipient - Defined in RFC3693 as any entity that understands geolocation (LbyR or LbyV) along a message path.

Does not include entities that process a message containing geolocation that do not understand geolocation (i.e., layer 3 routers).

Location Server - a logical IP server that transmits a PIDF-LO. This can be logically combined with the Location Generator, or could be an intermediary element - such as a LIS.

Location Target - The entity whose location is being sought, whether or not this entity is aware of this inquiry or is even an IP device.

Location-by-Reference (more than one meaning)

- a general purpose term meaning a message containing a URI that points to a PIDF-LO (geolocation of a Location Target) not within this same message

- a URI that logically locates a geolocation record of a Location Target. The URI does not point to location within the same message as the URI.

Location-by-Value - when a message contains the actual location of a Location Target, in the form of a PIDF-LO, within a part of the same message, usually pointed to by a "cid=" URI in a Geolocation header.

Using Protocol - as defined in [RFC3693], a protocol that is deemed to be in compliance with the security and privacy aspects of the Geopriv Requirements RFC [RFC3693], with good community verification.

Instead of using the terms Location-by-Reference (or just by-reference) and Location-by-Value (or just by-value), this document will herein use the acronyms LbyR and LbyV, respectively. The use of "cid=" implies LbyV, therefore, the use of a "cid=" Reference URL, which is *not* a Location-by-Reference (LbyR).

2. **Introduction**

This document describes how Location can be "conveyed" (that is, transmitted over the Internet) from one SIP user agent (UA), or in some circumstances, a proxy server acting in support of a UA, to another entity using SIP [RFC3261]. Here "Location" is a description of the physical geographical area where something currently exists. The phrase "location conveyance" describes scenarios in which a SIP user agent client (UAC) is informing a user agent server (UAS) or intermediate SIP server where the UAC is. A superset of this can also be true as well, in which one UA (UA-1) is telling another UA-2 where another Target is, meaning not necessarily where UA-1 is. The key to this is whether UA-1 has permission to retransmit that other Target's location. If yes, then this is valid. If no, then this is breaking a fundamental rule within this extension.

Location Conveyance is different from a UAC seeking the location the UAS. Location conveyance is a 'sending location out in the request' model, where 'asking that someone else's location be in a response' is not discussed here.

Geographic location in the IETF is discussed in RFC 3693 (Geopriv Requirements) [RFC3693]. It defines a "Target" as the entity whose location is being sought. In this case, this is the UA's (UA) location. A [RFC3693] "Using Protocol" defines how a "Location Server" transmits a "Location Object" to a "Location Recipient" while maintaining the contained privacy intentions of the Target intact. This document describes the extension to SIP for how it complies with the Using Protocol requirements, where the location server is a UA or Proxy Server and the Location Recipient is another UA or Proxy Server.

Location can be transmitted by-value or by-reference. The location "value" in this SIP extension is in the form of a Presence Information Data Format - Location Object, or PIDF-LO, as described in [RFC4119]. A PIDF-LO is an XML Scheme specifically for carrying geographic location of a Target. LbyV refers to a UA including a PIDF-LO as a body part of a SIP request, sending that Location Object to another SIP element. LbyR refers to a UA or proxy server including a URI in a SIP request header field which can be dereferenced by a Location Recipient for a Location Object, in the form of a PIDF-LO. Dereferencing can be by a SIP UA or a SIP server.

As recited in RFC 3693, location often must be kept private. The Location Object (PIDF-LO) contains rules which provides guidance to the Location Recipient and controls onward distribution and retention of the location. This document describes the security and privacy considerations that must be applied to location conveyed with SIP.

Another use for location is location-based routing of a SIP request, where the choice of the next hop (and usually, the outgoing Request-URI) is determined by the location of the UAC which is in the message by-value or by-reference. This document describes how location can be conveyed from the UAC, or a proxy acting on its behalf, to a routing proxy. How the location is actually used to determine the next hop or Request-URI is beyond the scope of this document.

We refer to the "emergency case". This refers to a specific, important use of SIP location conveyance where the location of the caller is used to determine which Public Safety Answering Point (PSAP) is expected to receive an emergency call request for help (e.g., a call to 1-1-2 or 9-1-1). This is an example of location-based routing. The location conveyed is also used by the PSAP to dispatch first responders to the caller's location. There are special security considerations, which make the emergency case unique, compared to a normal location conveyance within SIP.

Common terms are in Section 1. Section 3 provides an overview of SIP location conveyance. Section 4 details the modifications necessary to accomplish location conveyance. Section 5 gives decode examples of geolocation within SIP requests, both LbyV and LbyR. Section 6 articulates the SIP element type behaviors for location conveyance. Section 7 discusses Geopriv privacy considerations. Section 8 discusses security considerations. Section 9 IANA registers the modifications made to SIP by this document from section 4.

3. Overview of SIP Location Conveyance

This document defines a new SIP header: Geolocation. The Geolocation header field contains a URI which can either be a "cid:" URI (Content Identification), as defined in [RFC2392], or an LbyR -- to be dereferenced by a Location Recipient to retrieve the location of the Target UA.

Where the Geolocation header contains a "cid:", the URI points to a message body that is in the form of a PIDF [RFC3863], which was extended in [RFC4119] to include location, as a PIDF-LO. This is LbyV, the actual location information in the PIDF-LO is included in the body of the message.

If the URI in the Geolocation header field is a scheme other than "cid:", another protocol operation is needed by the SIP message recipient to obtain the location of the Target (UA). This is LbyR. This document describes how a SIP presence subscription [RFC3856] can be used as a dereference protocol.

The Geolocation header, either with the PIDF-LO in a body or as a LbyR URI, can be included by a UA in a SIP request. A SIP proxy server can assert location of the UA by inserting the header field, by adding an LbyR URI into the Geolocation header value, even if there is a locationValue already there. Since body parts cannot be inserted by a SIP proxy server, LbyV message body cannot be inserted by a proxy.

The Geolocation header can have parameters that are associated with a URI in the header field. The "inserted-by" parameter indicates the host-id of which specific element added this particular location to the request. This header parameter is included in every locationValue, and does not appear more than once per locationValue. The "inserted-by" parameter is especially useful for Location Recipients that receive more than one locationValue within a SIP request. Since implementations of a UA or SIP Server do not know they will be the last entity before a Location Recipient, this optional parameter is necessary within each locationValue.

Retargeting means the Request-URI of the request has changed to point at a new destination UAS. This is different than message routing, that all SIP proxies do. If a SIP request is retargeted based on the location contained or referenced within that message, the "used-for-routing" parameter is added as a header parameter within the appropriate locationValue.

There is no mechanism by which the veracity of these parameters can be verified. They are hints to downstream entities on how the location information in the message was originated and used. Transport Layer Security is expected when a request contains a user's location. Some implementations will choose to have S/MIME to encrypt message bodies from source to destination.

This document creates a new option tag: geolocation, to indicate support for this extension by UAs.

A new error response (424 Bad Location Information) is also defined in this document. Within this response is a new header indicating location-based errors, call the Geolocation-Error header. This header has various codes that provide additional information about the type of location error experienced by a Location Recipient.

The new headers, the header parameters, the new option tag, the new error response, and Geolocation-Error codes, which are defined in Section 4., are IANA registered by this document.

4. SIP Modifications for Geolocation Conveyance

The following are sections detail the standards track modifications to SIP for Location Conveyance.

4.1 The Geolocation Header

This document defines and IANA registers a new SIP header: Geolocation, with the following ABNF [RFC5234]:

```
Geolocation        =  "Geolocation" HCOLON (locationValue *(COMMA
                       locationValue)) (COMMA retrans-param)
locationValue      =  LAQUOT locationURI RAQUOT *(SEMI geoloc-param)
locationURI        =  sip-URI / sips-URI / pres-URI
                       / cid-url ; (from RFC 2392)
                       / absoluteURI ; (from RFC 3261)
geoloc-param       =  "inserted-by" EQUAL geoloc-inserter
                       / "used-for-routing"
```

```
                          / generic-param ; (from RFC 3261)
   geloc-inserter    =  DQUOTE hostport DQUOTE
```

```
                       / gen-value ; (from RFC 3261)
retrans-param      =  "routing-allowed" EQUAL "yes" / "no"
```

sip-URI, sips-URI and absoluteURI are defined according to RFC 3261. The pres-URI is defined in RFC 3859 [RFC3859].

The cid-url is defined in [RFC2392] to locate message body parts. This URI type MUST be present in a SIP request if location is transmitted LbyV only.

Other protocols used in the Location URI MUST be reviewed against the RFC 3693 criteria for a Using Protocol.

The Geolocation header MAY have one or more locationValues. SIP servers inserting a locationValue MUST add the new value as the last locationValue in the Geolocation header (i.e., the last locationValue in the header is the most recent one added to the message). Placement of the "routing-allowed" parameter, when present, MUST be the last header value in the Geolocation header.

A locationValue has the following independent header parameters,

- the "inserted-by=" parameter provides the hostport (alice.example.com -- which is the same as the "sent-by" parameter in a Via header, with or without a port number) of the SIP entity that inserted this locationValue into the request. If a Location Recipient has determined a supplied location is in error, as there can be more than one in any request, the "inserted-by=" parameter is copied into the locationErrorValue in the response indicating the location error, and to whom the error is for. Hence, this "inserted-by=" parameter MUST be present in each locationValue. If an entity receives an Geolocation-Error with a hostport not identifying this entity, the Geolocation-Error MUST be ignored.

- the "used-for-routing" parameter to inform recipients that the location in this locationValue was used to route the message towards the ultimate destination UAS. "used-for-routing" can occur more than once along the request's path. Because locationValues are inserted as last inserted is last in the header, the last locationValue is the most recent one added to the message. This also gives the "used-for-routing" header parameter added meaning - as the receiving SIP entity knows which locationURI the message was routed upon.

Each locationValue MUST contain exactly one "inserted-by" parameter, indicating which SIP entity added the locationValue to the SIP request.

There MUST NOT be more than one "inserted-by=" parameter or one "used-for-routing" parameter in the same locationValue. However, there can be more than one locationValue in the same Geolocation header.

The "routing-allowed" header parameter is a global parameter over any (and all/each) locationValues in the Geolocation header. This is the reason why the placement of the header parameter is outside any locationValue, and appears only once, and is always last in the header value.

This header parameter has values "=yes" or "=no" only. When this parameter "=yes", any locationValue can be used for routing decisions along the downstream signaling path by intermediaries. When this parameter "=no", this means no locationValue (inserted by the originating UAC or any (or subsequent) intermediary(ies) along the signaling path) can be used by any SIP intermediary to make routing decisions. This behavior MUST be adhered to.

The practical implication is that when the "routing-allowed" parameter is set to "no", if an LbyV is present in the SIP request, intermediaries SHOULD NOT view the location (because it is not for intermediaries to view), and if an LbyR is present, SHOULD NOT dereference it. UASs are allowed to view location in the SIP request even when the "routing-allowed" header parameter is set to "no".

The default behavior when this header parameter is not present in a message is to treat the SIP request as if the parameter were present and its value is set to "no".

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

```
INVITE [RFC3261],              REGISTER [RFC3261],
OPTIONS [RFC3261],             BYE [RFC3261],
UPDATE [RFC3311],              INFO [RFC2976],
MESSAGE [RFC3428],             REFER [RFC3515],
SUBSCRIBE [RFC3265],           NOTIFY [RFC3265],
PUBLISH [RFC3903] and          PRACK [RFC3262]
```

Discussing location using the PUBLISH request is out of scope for this document since it is part of Presence, therefore, for completeness, Table 1 shows PUBLISH is to support Location Conveyance via this extension, but is not discussed further.

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	R	ar	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

Table 1: Summary of the Geolocation Header

The Geolocation header field MAY be included in any one of the above requests by a UAC. A proxy MAY add the Geolocation header, but MUST NOT modify any pre-existing locationValue, including any associated header parameters within an existing Geolocation header value, unless one of the existing locationValues is used to retarget the request towards a new destination UAS. This is discussed in section 6.3.

[RFC3261] states message bodies cannot be added by proxies. Therefore, any Geolocation header field added by a proxy MUST be in the form of an LbyR URI, in its own locationValue header value.

A SIP proxy MAY add a Geolocation header if one is not present, and MAY add the "routing-allowed" parameter if not yet present in the SIP request. When a "routing-allowed" parameter is already present in the SIP request, a SIP server MUST NOT change the value of the parameter (i.e., from 'yes' to 'no', or from 'no' to 'yes'). This would override the policy set by an upstream SIP entity (i.e., likely the UAC).

Adding a new locationValue to an in-transit request SHOULD NOT occur for at least two reasons,

#1 - SIP Servers are not the best Sighters, as defined by [RFC3693], of geographically where a UAC can be; meaning the location information is not necessarily the greatest. There MAY be exceptions, but this SHOULD be the rule of thumb.

#2 - without appropriate caution to the fact that Location Recipients might not understand how to process more than one location, given this document's limited guidance as to what a Location Recipient should do when receiving more than one location (i.e., currently no priority instructions are given for which locationValue to use if there are more than one). A Location Recipient can easily be confused by too much location information, producing undesirable results. The <tuple id> element in the PIDF-LO XML indicates whose location is contained in the PIDF-LO.

Location Recipients receiving a location object, received directly or as the result of a dereference, MUST honor the usage element rules within that XML document, as defined in [RFC4119]. Such entities MUST NOT alter the rule set.

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 the location information was malformed or not satisfactory for the recipient's purpose, or could not be dereferenced.

Section 4.3 creates the Geolocation-Error header to provide more detail about what was wrong with the location information in the request. This header MUST be in the 424 response, containing a locationErrorValue for each invalid locationValue in the request (i.e., and one-for-one matching if all locationValues in the request were bad).

If more than one location is present in a request (LbyV or LbyR), and any of the locationValues is good for the Location Recipient to process, a 424 MUST NOT be sent. The 424 is only appropriate when the Location Recipient needs a locationValue and there are no locationValues included in a SIP request that are usable by a recipient.

A 424 (Bad Location Information) response is a final response within a transaction, and does not terminate a usage or a dialog.

The UAC can use whatever means it knows of to verify/refresh its location information before attempting a new request that includes location. There is no cross-transaction awareness expected by either the UAS or any SIP intermediary as a result of this error message.

The new 424 (Bad Location Information) error code is IANA registered in Section 8 of this document. An initial set of location error of IANA registered Geolocation-Error codes are in Section 4.3 of this document.

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 UAC is to know what was wrong within the original request. The Geolocation-Error header is created here for this purpose.

Geolocation-Error header is used to convey location specific errors within a response. Additions to this IANA registered header require an RFC be published. The Geolocation-Error header has the following ABNF [RFC5234]:

```
Geolocation-Error        = "Geolocation-Error" HCOLON
                             locationErrorValue
                            *(COMMA locationErrorValue)
locationErrorValue       = location-error-code *(SEMI
                            location-error-params)
location-error-code      = 1*3DIGIT
location-error-params    = location-error-node-id
                           / location-error-host-id
                           / location-error-code-text
                           / generic-param ; from RFC3261
location-error-node-id   = "node" EQUAL
                              DQOUTE hostport DQOUTE ; from RFC3261
location-error-host-id   = "inserter" EQUAL
                              DQOUTE hostport DQOUTE ; from RFC3261
location-error-code-text = "code" EQUAL quoted-string ; from RFC3261
```

The Geolocation-Error header MUST contain at least one locationErrorValue to indicate what was wrong with the original locationValue in the corresponding request. If a Location Recipient experienced more than one error a particular locationValue of the corresponding SIP request, there can be one locationErrorValue per problem with the locationValue in the request. Each locationErrorValue contains one 3-digit error code indicating what was wrong with the location in the request. Each error type has a corresponding quoted error text string that is human understandable. If there was something wrong with more than one locationValue in a request, a corresponding locationErrorValue would be sent, one per error, in the response.

Each locationErrorValue contains the Location Recipient identifier (the "node=" parameter) which experienced the location error, as well as an identifier of which SIP entity (the "inserter=" parameter) the Location Recipient is told (in the locationValue) added this problematic locationValue to the request. The "node=" and "inserter=" are the domain identifier of a SIP entity, with the ability to have the same host communicate on different ports - and have port specific identification. This is the same as is entered in the "sent-by" parameter of the Via header for that entity [RFC3261]. As stated in section 18 of RFC 3261, the usage of FQDN is RECOMMENDED. Here are examples of both locationErrorValue parameters

```
node="bob.example.com"
```

```
      inserter="alice.example.com"
```

Both the "node=" and "inserter=" parameters MUST be present in all locationErrorValues in a response, unless the "inserted-by=" parameter was not in the locationValue of a request (which is a violation of this document). The "inserter=" parameter value is copied from the "inserted-by=" parameter within the locationValue of the request. No manipulation or calculation is necessary to accomplish this.

Here's why this is necessary, a Location Recipient that experienced the location problem with the request needs to tell the specific SIP entity which added the locationValue in error into the original request. Since more than one SIP entity can insert location into a request in transit, all other SIP elements may be confused by receiving this error header, were it to remain generic to all entities in the response path. So, the header has to identify who it is for, so that all other SIP entities that read the header know to ignore it, since it is not for them. This is of particular use if the original UAC did not include a locationValue in the original SIP request, but a SIP server along the path did insert a locationValue. The locationErrorValue would travel to each SIP entity along the original path and tell both the server that included the locationValue what was wrong with the location and the UAC who did not know what the error meant. This will cause confusion if left without this indication.

A worse case is when both the original UAC and a SIP server along the path included a locationValue, but there was only something wrong with one of the locationValues. Without this identification of which locationValue was in error, both entities would react and one would do so incorrectly.

More than one locationErrorValue in a Geolocation-Error header is separated by a comma.

If more than one locationErrorValue is in a response, and intended for the same "inserter=", each error code MUST be unique to this "inserter=" entity, and the error codes SHOULD NOT conflict in meaning. In other words, two error codes (within separate locationErrorValues of the same response) SHOULD NOT give misleading or inconsistent indications to the location "inserter=".

Here is an example of a Geolocation-Error header

```
Geolocation-Error: 200; code="Retry Location Later";
                         node="bob.example.com";
                         inserter="alice.example.com";
```

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

The Geolocation-Error header field MAY be included in any response to one of the above SIP requests, so long as Geolocation was in the request part of the transaction. The choice of which SIP requests are in table 2 above come from which Methods can optionally have the Geolocation header (see section 4.1). That said, a UAC MUST ignore a Geolocation-Error header value if it did not include a Geolocation header value in the request part of the transaction.

Here is an example of a transaction that has a location error. In this case, Bob responds with a 424 (Bad Location Information) response, including a Geolocation-Error header, is in Figure 1.

```
   Alice                                                  Bob
     |                                                     |
     |       Request w/ Location                           |
     |---------------------------------------------------->|
     |                                                     |
     |                                                     |
     |  424 (Bad Location Information)                     |
     |  with Geolocation-Error containing                  |
     |  200 ("Retry Location Later" (with same data))      |
     |<----------------------------------------------------|
     |                                                     |
```

Figure 1. Basic Transaction with 424 and Geolocation-Error Header

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 5 categories, each based on receiver (of the response) actionable reactions to these errors.

- 100 "Cannot Process Location"

- 200 "Retry Location Later" (with same data)

- 300 "Retry Location Later" (with device updated location)

- 400 "Permission Necessary"

- 500 "Location Information Denial"

All 5 of the above error codes MUST be implemented to comply with this specification. Each of these actionable errors is given a 3 digit error code category, meaning any future 1XX, 2XX, 3XX, 4XX, and 5XX error codes defined will have the same action expected by X00 categories. If another action is expected to occur with a newly defined error code, it MUST outside the 100-599 range. 100 unit ranges are OPTIONAL for future error codes, but they apply here.

4.3.1 Location Error: 100 "Cannot Process Location"

The location error 100 "Cannot Process Location" indicates to a Geolocation-Error recipient that what they supplied in a request, as far as location is concerned, cannot be processed at this time. This only has to do with the location that the location "inserter=" added to the request, and not about the overall request that was sent.

Action(s) to be taken by Geolocation-Error receiver to a 1XX:
This error gives no guidance on what to do next. It is a general information indication to a SIP "inserter=" entity that there was an unspecific problem with the location supplied in the SIP request.

Implementations MAY choose to react in a way as if this "inserter=" entity received a 2XX or 3XX location error. A 4XX error MUST NOT be misunderstood here, as that error category involves human intervention to grant, or not, permission to reveal "inserter=" location when this is likely not desired.

The text string of "Cannot Process Location" is RECOMMENDED, but not mandatory for usage in this error. Implementations MAY use another text string.

An example of this location error is here:

```
Geolocation-Error: 100; code="Cannot Process Location";
                         node="bob.example.com";
                         inserter="alice.example.com";
```

This category covers location errors 1XX; meaning there MAY be more specific errors added to this category in future effort(s). The same basic actionable reaction is expected by a location "inserter=" entity to any 1XX location error.

4.3.2 Location Error: 200 "Retry Location Later" (same data)

The location error 200 "Retry Location Later" (same data) indicates to a Geolocation-Error recipient that what they supplied in a request, as far as location is concerned, cannot be processed at this time, but to retry this request, without changing the location information, at a later time - in a new SIP request. It is possible that the Location Recipient cannot process location at this time, or there was a timeout during dereferencing, if an LbyR were sent.

Action(s) to be taken by Geolocation-Error receiver to a 2XX:
Reactions to a 2XX location error are to try again, without having to update the location supplied originally. There is no constraints on how long this new try has to wait, unless there is a Retry-After header in a 424 response.

Implementations SHOULD choose to react by preparing, however this "inserter=" does or can, to queue another message with the same location information, provided the "inserter=" does not move between the time of the original request and the transmission time of the new request.

Implementations MAY choose whether or not to inform the user of this error. The text string of "Retry Location Later" is RECOMMENDED, but not mandatory for usage in this error. Implementations MAY use another text string to inform the user that location was not received by the UAS (i.e., the called party).

An example of this location error is here:

```
Geolocation-Error: 200; code="Retry Location Later";
                         node="bob.example.com";
                         inserter="alice.example.com";
```

This category covers location errors 2XX; meaning there MAY be more specific errors added to this category in future effort(s). The same basic actionable reaction is expected by a location "inserter=" entity to any 2XX location error.

If a SIP request has the "routing-allowed" header parameter set to "no", and the SIP server believes processing location within the request in order to service the request properly, a 2XX location error is sent towards the recipient. This error is the proper error even when there is no location in the SIP request, but the SIP request contains a policy statement that location is not to be viewed during transit towards the ultimate destination.

4.3.3 Location Error: 300 "Retry Location Later" (device updated location)

The location error 300 "Retry Location Later" (device updated location) indicates to a Geolocation-Error recipient that what they supplied in a request, as far as location is concerned, cannot be processed at this time, but to retry this request, once the location information has been updated, in a new SIP request.

Action(s) to be taken by Geolocation-Error receiver to a 3XX:

3XX location errors indicate the "inserter=" SIP entity needs to refresh its location, or make the location information supplied more complete, without notifying the user of this error. 3XX error are to be solved by without user intervention.

This document gives no guidance how this is accomplished, given the number of ways a UAC can learn its location, or a SIP intermediary can Sight a UAC, as defined in [RFC3693].

This 300 location error currently does not indicate what exactly was wrong with the location supplied, according to the Location Recipient. That is left for a future effort.

Implementations MAY choose whether or not to inform the user of this error. The text string of "Retry Location Later" is RECOMMENDED, but not mandatory for usage in this error. Implementation MAY use another text string to inform the user that location was not received by the UAS (i.e., the called party).

A 3XX location error would be used where the Location Recipient cannot find or cannot parse the location supplied, believing that a automated refresh and retry could fix the problem. Also, a 3XX location error would be used when a Location Recipient did not find any location in a SIP request, but was expecting it. Perhaps an emergency request was made that did not contain location. The retry in this case would be in the form of an UPDATE Method request, containing location (LbyV or LbyR).

An example of this location error is here:

```
Geolocation-Error: 300; code="Retry Location Later";
                         node="bob.example.com";
                         inserter="alice.example.com";
```

This category covers location errors 3XX; meaning there MAY be more specific errors added to this category in future effort(s). The same basic actionable reaction is expected by a location "inserter=" entity to any 3XX location error.

4.3.4 Location Error: 400 "Permission Necessary"

The location error 400 "Permission Necessary" indicates to a Geolocation-Error recipient that when they sent a particular SIP request, they included location in that request without giving permission in the request for a (or any) SIP server to look at that location information (i.e., the <retransmission-allowed> was set to "no") to route the message at the intended recipient (i.e., the UAS, or the called party).

Action(s) to be taken by Geolocation-Error receiver to a 4XX:

4XX location errors indicate to the UAC (i.e., the calling party) that they need to grant permission to a SIP intermediary server to look at the supplied location to complete the message routing. This indication MUST require human user intervention, as the rulemaker of the policy on whether or not their location is to be revealed.

The user of the location "inserter=" device can choose to grant permission to this SIP intermediary server to allow this request to be routed, or the user can deny this location revelation (request by the server). It is the user's choice as rulemaker.

Implementations MUST provide the user, as rulemaker, a clear indication that permission to consume their location is sought by an entity other than who that user is calling. The text string of "Permission Necessary" is RECOMMENDED, but not mandatory for usage in this error. Implementation MAY use another text string to inform the user that location is being sought by an intermediary (i.e., not the called party).

This document gives no guidance how this intervention is accomplished, given the number of ways a UAC can accomplish this (i.e., audio prompt or toggle or keystroke on their UA).

This 400 location error currently does not indicate exactly which SIP server indicates it needs the location revealed. That said, the "node=" FQDN address could be supplied, telling the user (via audio or video indication) which SIP entity wants this location. Perhaps the user can know in some circumstances whether this is an appropriate "node=" (domain). All of this is left for a future effort(s).

An example of this location error is here:

```
Geolocation-Error: 400; code="Permission Necessary";
                        node="bob.example.com";
                        inserter="alice.example.com";
```

This category covers location errors 4XX; meaning there MAY be more specific errors added to this category in future effort(s). The same actionable solution is expected to be afforded to the UAC user, as rulemaker, to any 4XX location error.

4.3.5 Location Error: 500 "Location Information Denial"

The location error 500 "Location Information Denial" indicates to a Geolocation-Error recipient that what they supplied in a request, as far as location is concerned, has been denied at this time.
This only has to do with the location that the location "inserter="

added to the request, and not about the overall request that was sent. If this were applied to the SIP request itself, this would equate to a 6XX Global error.

Action(s) to be taken by Geolocation-Error receiver to a 1XX:
      This error gives no guidance on what to do next, other than to
      not try again with this same location supplied.

If the Location Recipient believed that merely refreshing, or in some other way alter or augment the location supplied would work in a new request, then a 3XX location error SHOULD have been returned (to the "inserter="). An example of why this 5XX could have been returned is if location were sent as an LbyR, and the LIS denied the dereference request from the Location (reference) Recipient, this is the expected location error returned to the "inserter=" entity.

Implementations MUST NOT interpret anything else into this location error other than it is considered a location based denial error. This does not mean the SIP request was denied, or even had an error, unless the response was a 424. Otherwise, this only has to do with the location part of the request.

The difference between a 1XX and a 5XX location error is simple. A 1XX location error is a case of a Location Recipient either not knowing or not being able to tell the "inserter=" entity what was wrong with the location supplied in a SIP request. Whereas, a 5XX location error is where the location was purposely, and actively denied (or declined) from being received by the Location Recipient entity, or its user. This could occur in a UAS or SIP server.

If implementations choose to inform the UAC user of this error, the text string of "Location Information Denial" is RECOMMENDED, but not mandatory for usage in this error. Implementations MAY use another text string.

An example of this location error is here:

```
Geolocation-Error: 500; code="Location Information Denial";
                         node="bob.example.com";
                         inserter="alice.example.com";
```

This category covers location errors 5XX; meaning there MAY be more specific errors added to this category in future effort(s). The same basic actionable reaction is expected by a location "inserter=" entity to any 5XX location error.

4.3.6 Which Scenario Matches Which Error Code?

The following are some additional failure scenarios, with which error code SHOULD be used for consistency,

- Scheme (sip:, or sips:, or pres:, or another one) of the LbyR URI isn't supported (100)

- Format (geo or civic) isn't supported   (100)
- Cannot parse location (100)
- Can't find LIS (no access or no path (100) or denied access(500))
- Dereference failed (timeout)   (200)
- Insufficient location info supplied   (300)
- Cannot find location in message   (300)

4.4 The 'geolocation' Option Tag

This document creates and IANA registers one new option tag: "geolocation". This option tag is to be used, as defined in RFC 3261, in the Require, Supported and Unsupported headers. Whenever a UA wants to indicate support for this SIP extension, the geolocation option tag is included in a Supported header of the SIP request.

4.5 Using sip/sips/pres as a Dereference Scheme

If an LbyR URI is included in a SIP request, it MUST be a SIP, SIPS or PRES-URI. When PRES: is used, if the resulting resolution, as defined in [RFC3856], resolves to a SIP: or SIPS: URI, this section applies.

This document IANA registers 3 mandatory to implement URI schemes for LbyR:

- SIP:
- SIPS:
- PRES:

These 3 are IANA registered in Section 9.6.

These schemes MUST be implemented according to this document. absoluteURI is not mandatory to implement.

Dereferencing a Target's location using SIP or SIPS MUST be accomplished by treating the URI as a presence URI and generating a SUBSCRIBE request to a presence server as defined in [RFC3856] using the 'presence' event package. The resulting NOTIFY will contain a PIDF, which MUST contain a PIDF-LO. See Figure 2. for a basic message flow for a dereference.

When used in this manner, SIP is a Using Protocol as defined in [RFC3693] and elements receiving location MUST honor the 'usage-element' rules as defined in this extension.

```
     Alice                 Location Server                      Bob
       |                                                         |
       |                  INVITE w/ LbyR URI                     |
       |-------------------------------------------------------->|
       |                          |                              |
       |                       200 (OK)                          |
       |<--------------------------------------------------------|
       |                          |                              |
       |                          |  SUBSCRIBE to LbyR URI       |
       |                          |<-----------------------------|
       |                          |  200 (OK)                    |
       |                          |----------------------------->|
       |                          |                              |
       |                          |  NOTIFY   w/ PIDF-LO         |
       |                          |----------------------------->|
       |                          |  200 (OK)                    |
       |                          |<-----------------------------|
       |                          |                              |
```

Figure 2. Location-by-Reference and Dereferencing

In Figure 2., Alice sends Bob her location in an LbyR URI. Bob receives this LbyR URI in the INVITE and generates a new transaction (SUBSCRIBE) to retrieve the PIDF-LO of Alice. If accepted, the PIDF-LO will be in the NOTIFY request from the Location Server back to Bob's UA. This is the first instance between Alice and Bob that Alice's location is in any message, therefore it is sent only once, from the Location Server to Bob.

The SUBSCRIBE contains a geolocation option tag in either the Supported or Require header (depending on what strength of support the UAC wants to apply). The NOTIFY MUST match the subscribing UAC's option-tag strength for geolocation.

A dereference of an LbyR URI using SUBSCRIBE is not violating a PIDF-LO 'retransmission-allowed' element value set to 'no', as the NOTIFY is the only message in this multi-message set of transactions that contains the Target's location, with the location recipient being the only SIP element to receive this PIDF-LO. This is the purpose of this extension to SIP - to convey location to a specific destination.

5. Geolocation Examples

This section contains are two examples of messages providing location. One shows LbyV with coordinates, the other shows LbyR. The example for (Coordinate format) is taken from [RFC3825]. A civic format example of the same position on the earth as is in the coordinate format example is in appendix B, which is taken from [RFC4776]. The differences between the two formats are within the <gp:location-info> of the examples. Other than this portion of each

PIDF-LO, the rest is the same for both location formats.

The key to the provided samples is in the Geolocation header, which has a different type of URI, based on the different means of location conveyance. Section 5.1 shows a "cid:" URI, indicating this SIP request contains an LbyV message body - which is in the form of a PIDF-LO. Section 5.2 shows an LbyR URI indicating location is to be acquired via an indirection dereference mechanism, which is determined by the scheme of URI supplied.

5.1 Location-by-value (Coordinate Format)

This example shows an INVITE message with a coordinate, or coordinate location. In this example, the SIP request uses a sips-URI [RFC3261], meaning this message is TLS protected on a hop-by-hop basis all the way to Bob's domain.

```
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>
  ;inserted-by="alice@atlanta.example.com"
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: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="point2d">
         <timestamp>2007-12-02T14:00:00Z</timestamp>
         <status>
          <gp:geopriv>
            <gp:location-info>
              <gml:location>
                <gml:Point srsName="urn:ogc:def:crs:EPSG::4326">
                  <gml:pos>33.001111 -96.68142</gml:pos>
                </gml:Point>
               </gml:location>
            </gp:location-info>
            <gp:usage-rules>
              <gp:retransmission-allowed>no</gp:retransmission-allowed>
              <gp:retention-expiry>2007-12-07T18:00:00Z</gp:retention-
                            expiry>
            </gp:usage-rules>
            <gp:method>DHCP</gp:method>
            <gp:provided-by>www.example.com</gp:provided-by>
          </gp:geopriv>
         </status>
        </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, with SDP being the other message body part. The "cid:" eases parsing of message bodies.

If the Geolocation header field were this instead:

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

...the presence of something other than "cid:" indicates an LbyR is included in this message. It is expected that any node wanting to know where user target123 is would subscribe to server5 to dereference the sips-URI (see Figure 2. for this message flow, and Section 5.2 for this decoded example). The returning NOTIFY would contain Alice's location in a PIDF-LO, as if it were included in a message body (part) of the original INVITE here.

5.2 Location-by-reference

Below is an INVITE request with an LbyR URI instead of an LbyV PIDF-LO message body part shown in Section 5.1. It is up to the location recipient to dereference Alice's location at the Atlanta LIS server containing the location record. Dereferencing, if done with SIP, is accomplished by the Location Recipient sending a SUBSCRIBE request to the URI reference for Alice's location. The received NOTIFY is the first SIP request containing Alice's UA location, as a PIDF-LO message body (see Figure 2 for this message flow example). The NOTIFY, in this case, is the SIP request that is conveying location, and not the INVITE. There is no retransmission of location in this usage.

```
INVITE sips:bob@biloxi.example.com SIP/2.0
Via: SIP/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: <sips:3sdefrhy2jj7@lis.atlanta.example.com>
  ;inserted-by="bigbox3.atlanta.example.com"
Supported: geolocation
Accept: application/sdp, application/pidf+xml
CSeq: 31862 INVITE
Contact: <sips:alice@pc33.atlanta.example.com>

(...SDP goes here as the only message body)
```

A Location Recipient would need to dereference the sips-URI in the Geolocation header field to retrieve Alice's location. If the atlanta.example.com domain chooses to implement location conveyance and delivery in this fashion (i.e., LbyR), it is RECOMMENDED that entities outside this domain be able to reach the dereference server, otherwise this model of implementation is only viable within the atlanta.example.com domain.

6. SIP Element Behavior

Because a device's location is generally considered to be sensitive in nature, location information needs to be protected when transmitted. This can be addressed through securing the location information to prevent either viewing or changing the PIDF-LO.

Section 26 of [RFC3261] defines the security functionality SIPS by transporting SIP messages with either TLS or IPSec protection between SIP entities.

If a SIP entity wants to prevent all SIP entities in a request path from viewing or just changing the contents of the PIDF-LO, save those that possess decryption key, the message body needs to be secure by a means such as S/MIME. This would be the case in which a UAC wants to make sure only the destination UAS can read the PIDF-LO. S/MIME can be used for just signing, and not encrypting, a PIDF-LO message body to ensure the integrity of the PIDF-LO is maintained.

6.1 UAC Behavior

A UAC can send location in a SIP request, either because it is expected to facilitate location-based routing of the request, or spontaneously (i.e., a purpose not defined in this document but known to the UAC). Alice communicating her location to Bob in a SIP request is a simple example of this. If Alice wanted to include her location as a message body in an INVITE that also has an SDP message body, the Content-Type: Multipart MUST be supported by both UAC and UAS. Multipart comes in many forms (/mixed, /alternative, etc), and this document does not limit which type of Multipart is used, though future documents MAY specify or limit Multipart to a subset of all the choices for a given use.

A UAC conveying location MUST include a locationValue in a Geolocation header (see section 4.1) with either an LbyV indication (a cid-URL), or an LbyR. An LbyV message body sent without a Geolocation header field MUST NOT occur. The UAC supporting this extension MUST include a Supported header with the 'geolocation' option tag.

More than one location format (civic and coordinate) can be included in the same message body part, but all location parts of the same PIDF-LO MUST point at the same position on the earth, identifying the same target. The same location in multiple formats, for example, a partial or complete geodetic and a partial or complete civic, can allow the recipient to use the most convenient or preferable format for its use.

Multiple PIDF-LOs are allowed in the same request, with each allowed to point at separate positions - however, each PIDF-LO MUST identify a different Target. Therefore, there will be no confusion by a Location Recipient receiving more than one PIDF-LO (in a message body or when dereferenced, or a combination). It is RECOMMENDED there is only one locationValue in a single SIP request for the same Target. More than one will likely lead to confusion by a Location Recipient because this extension does not provide guidance on what a recipient is to do with more than one location, nor does it give any preference regarding which location is better or worse than another location in the same request.

The 'geolocation' option tag is inserted in a Supported header by a UAC to provide an indication of support for this extension. The presence of the 'geolocation' option tag in a Supported header without a Geolocation header field in the same message informs a SIP element receiving this request that the UAC understands this extension, but it does not know or wish to convey its location at this time. Certain scenarios exist (location-based retargeting) in which location is required in a SIP request in order to retarget the message properly. This affects how a UAS or SIP server processes such a request.

The 'geolocation' option tag SHOULD NOT be used in the Proxy-Require Header, because the UAC often will not know the underlying topology to know which proxy will do the retargeting, thus increasing the likelihood of a request failure by the first hop proxy that does not understand this extension, but is required to by inclusion of the option tag in this header.

A UAC inserting a locationValue MUST include an "inserted-by=" parameter to indicate its hostport. This is copied to the "inserter=" parameter of the Geolocation-Error header in a response if a Location Recipient determines there is something wrong with the locationValue in this request. Because more than one locationValue can be inserted along the path of the request, this indication is necessary to show which locationValue had the problem in the response, and who the locationErrorValue is for. For example:

```
Geolocation: <cid:alice123@atlanta.example.com>;
              inserted-by="alice@atlanta.example.com"
```

If a UAC does not learn and store its location locally (a GPS chip) or from the network (DHCP or LLDP-MED), the UAC MAY learn its LbyR URI (from DHCP for example). If the latter is the case, the UAC MAY SUBSCRIBE to this LbyR URI, using the 'presence' event package, to get and store its own location.

The act of dereferencing a Target's LbyR will be challenged by the LIS where this location record is - providing a good deal of protection, SHOULD still be treated as equivalent to possession of the location information itself and thus TLS SHOULD be used when transmitting LbyR hop-by-hop along the path to the Location Recipient, for protection reasons. This is not to be confused with a possession model, in which possessing the LbyR grants authorization to dereference the URI. Any entity dereferencing the LbyR MUST pass whatever authentication and authorization rules are on the LIS for this location record. The Ruleholder from [RFC3693] is still very much in control - for any entity possessing the LbyR.

If the Location Generator wishes to control whether any location included in the SIP request or added along the signaling path of this request can be viewed for routing decisions, the Location Generator adds a Geolocation header value including the "routing-allowed=no" parameter. This header parameter provides specific policy rules for each locationValue (if there is more than one inserted along the signaling path) within the SIP request. A UAC SHOULD include the "routing-allowed" header parameter, with or without a locationValue, to each SIP request supporting this specification to ensure the UAC's policy for intermediaries which might add a locationValue of the Target downstream. The UAC understands that the default behavior for SIP servers is to consider this value to be present, and that it is set to "no".

The UAC MUST understand there is no feedback mechanism to inform the

Target if a SIP server has included a locationValue downstream.

If a UAC has already conveyed location in the original request of a transaction, and wants to update its location information (for whatever reason) after the original request is sent, or after a dialog is created (regardless of how the UAC conveyed location previously, as an LbyV or LbyR) - this is done by a UAC sending an UPDATE request [RFC3311] containing the geolocation option tag and Geolocation header with the new locationValue (LbyV or LbyR) to the original destination UAS.

A PIDF includes identity information. It is possible for the identity in the PIDF to be anonymous. Implementations of this extension SHOULD consider the appropriateness of including an anonymous identity in the location information where a real identity is not required. When using LbyR, the LbyR MUST NOT contain any user identifying information. For example, use something unidentifiable like

3fg5t5yqw@example.atlanta.com

rather than

aliceishere@example.atlanta.com).

Use of self-signed certificates is inappropriate for use in protecting a PIDF, as the sender does not have a secure identity of the recipient.

6.1.1 UAC Receiving a Location Failure Indication

Location Recipients can be either, or both, destination UASs and intermediate servers that use the location information for location-based routing decisions. If a sent request fails based on the location information in the request, a 424 (Bad Location Information) response is sent back to the UAC. The 424 MUST have a Geolocation-Error header containing one or more locationErrorValues in the response message. A locationErrorValue has a header parameter indicating which entity inserted the locationValue correlated to this error, called the "inserter=" parameter. This "inserter=" parameter (in the locationErrorValue) is copied from the "inserted-by=" parameter (from the locationValue) by the Location Recipient (UAS or proxy) sending the error response. A UAC receiving a Geolocation-Error in any response type MUST review the "inserter=" parameter in the locationErrorValue to see if it indicates this UAC. If locationErrorValue does not match, the locationErrorValue MUST be ignored. If a locationErrorValue is in a 424, and the "inserter=" entity is not this UAC, the response SHOULD be treated as a 400 response. If locationErrorValue does indicate this UAC, this UAC MUST process the response, including the Geolocation-Error code (defined in section 4.3). Further, UAC MUST ignore a Geolocation-Error header value, even for this UAC, even in a 424 response if the UAC did not include a Geolocation header value (with locationValue) in the request part of the transaction.

A UAC MAY reattempt a new request if it believes it can correct the stated failure in the Geolocation-Error header, unless the location error is a 5XX level error - which clearly states in Section 4.3 not to do this. A UAC MUST follow all the guidance that pertains to UACs from Section 4.3 (Geolocation-Error header), heeding what to do in case it receives any of the error codes articulated in that section.

Any UAC that inserted location into a request SHOULD be prepared to receive the Geolocation-Error header in any response, looking to determine if a locationErrorValue is meant for the UAC, and to react accordingly.

If a UAC includes location in a request, and either the UAS does not determine errored location was critical to the transaction and accept the request, or the request failed for reason other than location, any response MAY contain a Geolocation-Error header containing a locationErrorValue with the details of the location error.

6.2 UAS Behavior

If the Geolocation header field is present in a received SIP request, the type of URI contained in the locationValue will indicate if location is an LbyV in a message body (part) or LbyR, requiring an additional dereference transaction. If the LbyR URI is sip:, sips: or pres:, and the UAS wants to learn the UAC's location, the UAS MUST initiate a SUBSCRIBE to the URI provided to retrieve the PIDF-LO being conveyed by the UAC as defined in [RFC3856]. If successful, the PIDF-LO will be returned in the NOTIFY request from the remote host. The UAS is not REQUIRED to dereference the LbyR if it does not want to (by configuration or user choice). It is RECOMMENDED the UAS render the location sent to it, however it is configured to do so.

A Require header with the 'geolocation' option tag indicates the UAC is requiring the UAS understand this extension or else send an error response. A 420 (Bad Extension) with a 'geolocation' option tag in an Unsupported header would be the appropriate response in this case.

It is possible, but undesirable, for a message to arrive with a body containing an LbyV, but with no Geolocation header field value pointing to it (potentially no Geolocation header field at all). In this case, the recipient MAY still read and use the message body. Unless stated otherwise by future standards-track publication(s), a LbyR URI only has meaning within the Geolocation header field and

MUST NOT appear in any other SIP header field.

There are 2 Geolocation header parameters,

- o "inserted-by="
- o "used-for-routing"

The "inserted-by=" parameter informs a Location Recipient which SIP element added this locationValue to the SIP request. This parameter is mandatory for each locationValue in the request. The value in the "inserted-by=" parameter is copied into the "inserter=" parameter in each locationErrorValue if there is an error in the location to be reported back to the location sender. See section 6.2.1.

The "used-for-routing" parameter is included in the locationValue if a SIP server used the location in the request to determine how to route or forward the message towards the ultimate destination. If there are more than one locationValues in the Geolocation header, and it is possible that different locationValues were used to route the message at different times of this request's journey. This is allowed, as it is consistent with the rule that anytime a message is routed based upon a locationValue, a "used-for-routing" parameter is added to the applicable locationValue. This parameter should be present in each locationValue used along the path. A "used-for-routing" parameter MUST NOT ever be removed from a locationValue in a request.

Additional locationValues inserted into a request SHOULD be placed the order they were generated, and not rearranged. This informs a Location Recipient which was the last locationValue in the message that was used to route the message. This is for troubleshooting and management reasons.

Individual header parameters in any received locationValue MUST NOT be modified or deleted in transit to the ultimate destination.

A UAS MUST NOT send location in a response message, as there can be any number of issues/problems with receiving location, and the UAC or proxy servers cannot error a response. Therefore, the UAS, if it wants to send a UAC its location, SHOULD do so in a new request in a separate transaction. This document gives no guidance which SIP request to use, but SIP MESSAGE is a viable choice.

A UAS MAY include a 'geolocation' option tag in the Supported header of a response, indicating it does understand this extension, even if location was not in a request to the UAS.

A UAS wishing to dereference an LbyR URI contained in a received request will use the 'presence' event package in a SUBSCRIBE request to the URI. If accepted, the PIDF-LO will return to the UAS in a NOTIFY request. If there are any errors during dereferencing, or in the PIDF-LO itself, the UAS will error the original request to the UAC with a locationErrorValue indicating what the UAS concluded was wrong with the location. This is to include any dereferencing problems encountered.

Section 4.5 of this document called for the IANA registration of 3 URI schemes (sip:, sips:, and pres:) that are mandatory to implement for dereferencing.

A UAS MUST be prepared to receive subsequent location updates from the UAC, either LbyV or LbyR (regardless of how the UAS received location previously from this UAC). The UAC will convey location using the UPDATE [RFC3311] method to the UAS.

If there is more than one location (any combination of LbyV and LbyR), this document does not give guidance what a Location Recipient does with each location. There are no priority or more-trusted indications given by this document. All this is considered application specific, and out-of-scope of this document. This document makes it clear that if when there are more than one location, each in the same PIDF-LO MUST be about the same Target (identifier) and point at the same position on the earth. If there is more than one PIDF-LO with different Target identifiers, then the UAC is merely telling the UAS where more than one Target is, and there should not be any conflict.

6.2.1 UAS Generating a Location Failure Indication

If a UAS receives location in a request, but determines there is a problem with the location in the request, it is the responsibility of the UAS to inform whomever inserted location into that request there was a problem experienced. The Geolocation header in the request has a locationValue, providing the UAS a URI indicating where the Target's location is. The Location Target identified in the PIDF-LO may or may not be the location inserter, or the generator of the request (the UAC or SIP server). Ultimately, location is in a PIDF-LO. This is either in the request as a message body (LbyV), or it has to be dereferenced from the LbyR in the locationValue in the request. LbyR records are typically kept on a LIS, which can challenge all dereference requests. All PIDF-LOs have a Location Target identifier. This is who the location is about. The "inserted-by=" parameter of the locationValue tells the UAS who inserted that locationValue. This "inserted-by=" parameter is copied into the "inserter=" parameter of the locationErrorValue generated by the Location Recipient (the UAS), in a response, when it wants to inform the location "inserter=" entity there was a problem with the location it received.

There can be more than one locationValues in a request. The "inserter=" parameter in the locationErrorValue will distinguish it from being misunderstood by entities that did not insert the errored location.

If there is one valid locationValue in a request, even if all the others have errors with them, a 424 (Bad Location Information) response MUST NOT be sent. The Location Recipient (the UAS) is RECOMMENDED to send a locationErrorValue for each errored locationValue, with unique "inserter=" parameters to make sure the right entities know which locations were in error.

As hinted at, a location "inserter=" can be a UAC or it can be an in-signaling-path SIP server, who is acting as a UAC Sighter, as defined in RFC3693. This means the SIP server is including its version of where it thinks the UAC is, geographically. This "inserter=" has to be in the form of an LbyR URI in a locationValue, because SIP servers are not allowed to insert message bodies, as of the time of this publication, from all the way back to RFC3261.

Each locationErrorValue has a error code, letting the location "inserter=" entity know what was wrong with the location supplied. See Section 4.3 for the 5 actionable responses a UAC can take from a locationErrorValue.

If the location "inserted-by=" entity, meaning either the UAC or proxy in the message path, chose to indicate that location was so important in the request to include a 'geolocation' option tag in a Require header, the response SHOULD be a 424 (Bad Location Information) back to the "inserter=" entity (knowing the response will ultimately go to the UAC regardless) if there needs to be a locationErrorValue sent because the location was bad. Only entities identified in a locationErrorValue as the "inserter=" entity will pay attention to this locationErrorValue. All other entities MUST ignore any locationErrorValue not directed towards them. See section 4.3 for more information on this, including all the location specific errors and Geolocation-Error header parameters.

In the above scenario ('geolocation' option tag in a Require header), the only other response can be a 420, but only if the UAS does not support this Geolocation extension to SIP, else the 424 is sent.
If the location "inserted-by=" entity placed the 'geolocation' option tag in a Supported header, the response can be a 424 if it chooses, but also can be any other SIP response, including a 200 OK. A locationErrorValue in a Geolocation-Error header that is not in a 424 (Bad Location Information) response is considered informational by the Location Recipient, and not considered important enough to reject the request based solely on bad location information.

For example, Alice INVITEs Bob to a dialog, and includes geolocation in the request. Bob can accept the INVITE with a 200 OK and still add a locationErrorValue in the 200 OK indicating "yes, I accept your request, and btw, something was wrong with the location you provided (in the INVITE)". What was wrong with the location is indicated by the Geolocation-Error code. Who this locationErrorValue is for is indicated by the "inserter=" parameter.

Each locationErrorValue is destined for one "inserter=" entity. This gives a Location Recipient one mechanism to tell each inserter what the Location Recipient concluded was wrong with what the "inserter=" included (as far as location is concerned). Therefore,

- o there MUST be a locationErrorValue for each locationValue that was considered bad by the UAS to ensure each upstream location inserter understands which error code(s) is intended for them (and which to ignore).
- o there MUST NOT be more than one locationErrorValue in the response per locationValue in the request.
- o there MUST NOT be more than one locationErrorValue to the same "inserter=" in the request.
- o there MUST NOT be a locationErrorValue in the response for a locationValue in the request that was not in error, according to the Location Recipient.

Here is an example of a Geolocation-Error header

```
Geolocation-Error: 400; code="Permission Necessary";
                        node="server42.example2.com";
                        inserter="alice.example.com";
```

The above example says that the Location Recipient is server42.example.com, and this entity believes it cannot route this message without knowing the "inserter="'s location. This location may be in the request, or it may need to be in the request and was not. If location is encrypted, server42 doesn't know it is in the request. server42.example.com sends a 424 (Bad Location Information) response with a locationErrorValue indicating a 400 location error, which means it requires permission to view Alice's location to proceed with processing her signaling. Section 4.3 highlights this example, stating the user, Alice, MUST be made aware of this location revelation request. This document does not give any guidance how Alice is to be informed (i.e., audio, visual, etc). Alice can grant permission or choose not to, knowing this SIP request attempt (to this destination, at this time) will fail. The problem could be corrected if a future SIP request were to travel through a different server than server42 (or it might not).

See Section 4.3 for further rules about the Geolocation-Error header and the locationErrorValue.

This document says nothing about what a Location Recipient does with more than one 'good' locationValue in a request (i.e., which to choose to use). This scenario MAY be addressed in a future effort.

Further, more than one error code is allowed in the locationErrorValue - each having one "inserter=" parameter. The error codes destined for the same inserter MUST NOT contradict the meaning of the problem the Location Recipient had with a particular locationValue.

6.3 Proxy Behavior

[RFC3261] states message bodies cannot be added by proxies. However, proxies are permitted to add a header to a request. This implies that a proxy can add a Geolocation locationValue with LbyR URI, but not LbyV message body.

It is allowed, but NOT RECOMMENDED, for more than one SIP element to insert location into a request along its path. As described earlier in this document, each insertion of location into a SIP request is accompanied by a new locationValue in a Geolocation header. Also described earlier, each locationValue MUST contain an "inserted-by=" value indicating to a Location Recipient which host inserted location into a particular request.

However, if location is already in a SIP request, a SIP server SHOULD NOT add another LbyR that identifies the same target in the PIDF-LO (in the <dm:device id> element) to the same request. This will likely cause confusion at the Location Recipient as to which to use.

A proxy is permitted to read any locationValue, and the associated body, if not S/MIME protected, in transit if present, and can use the contents of the header field to make location-based retargeting decisions, if retargeting requests based on location is a function of that proxy. Retargeting is defined in [RFC3261]. However, if the Geolocation header parameter "routing-allowed" is present and set to "no", or is not present (knowing the default behavior is "no" if not present, with or without a Geolocation header), SIP servers MUST NOT view the contents of the LbyV message body. Further, SIP servers MUST NOT attempt to dereference an LbyR. This is because the SIP request, likely from the originating UAC did not give the SIP server permission to view the location within the SIP request.

If the Geolocation header parameter "routing-allowed" is present in a SIP request, the value MUST NOT be changed during processing of the request. If the Geolocation header parameter "routing-allowed" is not present, SIP servers are to treat the location within the request as if the header parameter "routing-allowed" were present and set to "no".

In the spirit of informing implementers of B2BUAs and SBCs, each server type really should adhere to the above proxy guidance with respect to the "Routing-allowed" header parameter, understanding that there are no IETF police, and the specific behaviors of these types of SIP servers cannot presently be defined. In other words, if the particular type of SIP server mentioned here is not the ultimate destination of this SIP request and supports this SIP extension, each policy rule within the Geolocation header needs to remain intact and unchanged.

No type of SIP server can delete a "Routing-allowed" header parameter, but if one is not yet present, any SIP server MAY add a "Routing-allowed" header parameter with the value set to "no" only.

More than one Geolocation locationValue in a message is permitted, but can cause confusion at the recipient. If a proxy chooses to add a locationValue to a Geolocation header, which would be a local policy decision, the new locationValue MUST be added to the end of the header (after previous locationValue(s)). This is done to create an order of insertion of locationValues along the path. Proxies MUST NOT modify the order of locationValues in a geolocation header.

A proxy wishing to dereference an LbyR URI contained in a received request will use the 'presence' event package in a SUBSCRIBE request to the URI. If accepted, the PIDF-LO will return to the proxy in a NOTIFY request. If there are any errors during dereferencing, or in the PIDF-LO itself, the proxy will error the original request to the UAC with a locationErrorValue indicating what the proxy concluded was wrong with the location. This is to include any dereferencing problems encountered.

6.3.1 Proxy Behavior with Geolocation Header Parameters

SIP servers MUST NOT delete any existing Geolocation locationValue (URI or header parameter) from a request. An existing locationValue (URI or header parameter) MAY only be modified by adding a "used-for-routing" parameter to an existing locationValue, if the request was retargeted based on the location within that locationValue. Further modification of this Geolocation header field MUST NOT occur. For example, an existing Geolocation locationValue in a request of:

```
Geolocation: <cid:alice123@atlanta.example.com>;
              inserted-by="alice123@atlanta.example.com";
```

can be modified by a proxy to add the "used-for-routing" parameter, like this:

```
Geolocation: <cid:alice123@atlanta.example.com>;
```

```
                 inserted-by="alice123@atlanta.example.com";
                 used-for-routing
```

if this is the locationValue the proxy used to make a retargeting decision based upon, but make no other modification.

A SIP server MAY add a new Geolocation locationValue to a SIP request. The proxy SHOULD NOT insert a locationValue of a Location Target unless it is reasonably certain it knows the actual location of the Location Target, for example, if it thoroughly understands the topology of the underlying access network and it can identify the device reliably (in the presence of, for example, NAT or VPN). Routing errors are likely if the SIP server inserts an incorrect locationValue.

A server adding a locationValue to an existing Geolocation header would look like:

```
 Geolocation: <cid:alice123@atlanta.example.com>;
               inserted-by="alice123@atlanta.example.com",
              <sips:3sdefrhy2jj7@lis1.atlanta.example.com>;
               inserted-by="lis1.atlanta.example.com"
```

Notice the locationValue added by the proxy is last among locationValues. This practice MUST be done for all added locationValues.

If this request was then retargeted by an intermediary using the locationValue inserted by the server, the intermediary would add a "used-for-routing" parameter like this:

```
 Geolocation: <cid:alice123@atlanta.example.com>;
               inserted-by="alice123@atlanta.example.com",
              <sips:3sdefrhy2jj7@lis1.atlanta.example.com>;
               inserted-by="lis1.atlanta.example.com"; used-for-routing
```

It is conceivable that an initial routing decision is made on one locationValue, and subsequently another routing decision is made on a different locationValue further towards the ultimate destination. This retargeting decision can be made on a newly inserted locationValue. While unusual, it can occur. In such a case, proxies MUST NOT remove any existing "used-for-routing" header parameter. In this instance, the SIP server retargeting based on another locationValue MUST add the "used-for-routing" header parameter to the locationValue used for retargeting by this server. This will result in a Geolocation header looking as if it were retargeting more than once, which would be true - and is the desired outcome.

A Proxy that inserts or adds locationValue into a request MAY move a 'geolocation' option that is in a Supported header into a Require header if this proxy deems geolocation to be that important to

Location Recipient(s) of this request.

6.3.2 Proxy Error Behavior for Sending or Receiving locationErrorValues

For proxies that receive a SIP request that contains a location error, either in a contained message body or after the proxy does a dereference of the LbyR URI, all the rules applicable to a UAS apply here (see Section 6.2.1.), since in this case, the proxy is considered a Location Recipient. Therefore, there is no reason to restate them here, and potentially have the two sections be inconsistent. The one thing to add is that a proxy does not need to examine location contained in a request. Section 6.2.1. only applies to proxies that are needing, monitoring or policing location within requests (for whatever reason).

If a proxy inserted a locationValue into a request, it SHOULD be ready to examine the response to that request, in case there is one or more location errors in the response. To a great degree, this scenario has the proxy behaving as a UAC (see section 6.1.1.) that included a locationValue a request, which then receives an error to that locationValue.

This location inserting proxy SHOULD be transaction stateful for the response. If the proxy is configured as a stateless proxy, and it inserts location, it MUST process and monitor all SIP responses, looking for locationErrorValues that indicate it was the "inserter=" to learn that location it supplied was in error. It SHOULD react accordingly to the error code received. This document gives no guidance what the proxy should do to rectify the bad location information, but a future document MAY address this.

7. Geopriv Privacy Considerations

Location information is considered by most to be highly sensitive information, requiring protection from eavesdropping, and altering in transit. [RFC3693] articulates rules to be followed by any protocol wishing to be considered a "Using Protocol", specifying how a transport protocol meets those rules. This section describes how SIP as a Using Protocol meets those requirements.

Quoting requirement #4 of [RFC3693]:

> "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 that SIP entities sending or receiving location MUST obey such instructions.

Quoting requirement #5 of [RFC3693]:

"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."

[RFC3261] and the documents it references define the key establishment mechanisms.

Quoting requirement #6 of [RFC3693]:

"(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."

When used for tracking, a simple NOTIFY or UPDATE normally is relatively small, although the PIDF itself can get large. Normal RFC 3261 procedures of reverting to TCP when the MTU size is exceeded would be invoked.

8. Security Considerations

Conveyance of physical location of a UAC raises privacy concerns, and depending on use, there probably will be authentication and integrity concerns. This document calls for conveyance to normally be accomplished through secure mechanisms, like S/MIME protecting message bodies (but this is not widely deployed) or TLS protecting the overall signaling. In cases where a session set-up is retargeted based on the location of the UAC initiating the call or SIP MESSAGE, securing the LbyV location 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. Securing the location hop-by-hop, using TLS, protects the message from eavesdropping and modification, but exposes the information to all proxies on the path as well as the endpoint. In most cases, the UAC does not know the identity of the proxy or proxies providing location-based routing services, so that end-to-middle solutions might not be appropriate either.

These same issues exist for basic SIP signaling, but SIP normally does not carry information to physically track a user; making this extension especially sensitive.

When location is inserted by a UAC, which is RECOMMENDED, it can decide whether to reveal its location using hop-by-hop methods. UAC implementations MUST make such capabilities conditional on explicit user permission, and SHOULD alert a user that location is being conveyed. Proxies inserting location for location-based routing are unable to meet this requirement, and such use is NOT RECOMMENDED.

Proxies conveying location using this extension MUST have the permission of the Target to do so.

One facet within this extension is such that locations can be placed on a remote server, accessible with the possession of a URI. The concept of an LbyR URI has its own security considerations. It is tempting to assume that the dereference would have authentication, authorization and other security mechanisms that limit the access to information. Unfortunately, this might not be true. The access network the UAC is connected to can be the source of location reference, and it might not have any credentialing mechanism suitable for controlling access to location. Consider, specifically, a nomadic user connected to an access network in a hotel. The UAC has no way to provide a credential acceptable to the hotel Location Server (LS) to any of its intended Location Recipients. The recipient of a reference does not know if a reference has appropriate authorization policies or not. The LS should provide location to any requestor.

Accordingly, possession of the reference should be considered equivalent to possession of the value, and the reference should be treated with the same degree of care as the value. Specifically, TLS MUST be used to protect the security of the reference. Notice that this does not constrain the dereference protocol to use TLS. That specification is left entirely to the dereferencing protocol documents.

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

9. 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).

9.1 IANA Registration for the SIP Geolocation Header

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

Header Field	Parameter Name	Predefined Values	Reference
Geolocation	inserted-by=	no	[this doc]
Geolocation	used-for-routing	no	[this doc]

9.2 IANA Registration for New SIP 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 sip-parameters within IANA.

9.3 IANA Registration for Response Code 424

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.

9.4 IANA Registration of New Geolocation-Error Header

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

Header Field	Parameter Name	Predefined Values	Reference
Geolocation-Error	inserter=	no	[this doc]
Geolocation-Error	node=	no	[this doc]
Geolocation-Error	code=	no	[this doc]

9.5 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 at sip-parameters within IANA. 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 to be placed into SIP responses to inform the location

inserter of the error.

Code	Description	Reference
100	"Cannot Process Location" General location error, meaning location in the request cannot be processed at this time. No actionable guidance. Can be treated as a 200 or 300 error by error recipient.	[this doc]
200	"Retry Location Later" (with same data) Location cannot be processed at this time. Error recipient should try again with same data.	[this doc]
300	"Retry Location Later" (with device updated location) Location cannot be processed at this time. Error recipient should try again with same data.	[this doc]
400	"Permission Necessary" Permission from calling user to reveal location in request before request can be processed. This is a routing by location error. User MUST be informed of permission request.	[this doc]
500	"Location Information Denial" Request was actively denied because of the location in the request. Recipient should not try again.	

9.6 IANA Registration of LbyR 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. Below is an example of how it could look

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

Additions to this registry require an industry specification.

10. Acknowledgements

To Dave Oran for helping to shape this idea. To Jon Peterson and Dean Willis on 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, Paul Kyzivat, Shida Shubert, Umesh Sharma, Richard Barnes, Ted Hardie, Matt

Lepinski and Jacqueline Lee for constructive feedback and nits checking.

A special thanks to Paul Kyzivat for his help with the ABNF in this document, to Dan Wing for help with the S/MIME example, and to Robert Sparks for many helpful comments and the proper building of the Geolocation-Error header.

11. References

11.1 References - Normative

[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

[RFC3863] H. Sugano, S. Fujimoto, G. Klyne, A. Bateman, W. Carr, J. Peterson, "Presence Information Data Format (PIDF)", RFC 3863, August 2004

[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.

[IANA-civic] http://www.iana.org/assignments/civic-address-types-registry

11.2 References - Informative

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

[RFC3825] J. Polk, J. Schnizlein, M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information", RFC 3825, July 2004

[RFC4776] H. Schulzrinne, " Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information ", RFC 4776, October 2006

Author Information

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

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. There is a motivational statement below each requirements that is not obvious in intent

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: 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: in case a UAC has moved prior to the establishment of a dialog between UAs, the UAC must be able to send new location information. In the case of location having been conveyed, and the UA moves, it needs a means to update the conveyed to party of this location change.

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, whether included LbyV or LbyR.

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 be because the UAC does not implement this extension, or it can be that the UAC implements the extension, but does not know where it is. This may be, for example, due to the failure of the access network to provide a location acquisition mechanisms the UAC understands. 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 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 the capability of 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.

Appendix B. Example of INVITE with S/MIME encrypted Civic PIDF-LO

This appendix gives an *EXAMPLE* (meaning this might contain errors based on future review) of a SIP INVITE request that points to the same position on the earth as the coordinate based example that is in section 5.1 in the body of this document:

The INVITE request is TLS hop-by-hop encrypted, and the LbyV message body is S/MIME encrypted. This example shows the location message body in its unencrypted form for clarity. The message body lines below that have the '$' signs are S/MIME encrypted. In this example, the SDP is not S/MIME encrypted. A complete list of IANA registered CAtypes can be found at [IANA-civic].

```
INVITE sips:bob@biloxi.example.com SIP/2.0
Via: SIP/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>
  ;inserted-by="alice@atlanta.example.com"
Supported: geolocation
Accept: application/sdp, application/pidf+xml
CSeq: 31862 INVITE
Contact: <sips:alice@pc33.atlanta.example.com>
Content-Type: multipart/mixed; boundary=boundary1
Content-Length: ...

--boundary1

Content-Type: application/sdp

...SDP goes here

--boundary1

Content-Type: application/pkcs7-mime;
   smime-type=enveloped-data; name=smime.p7m
   Content-ID: <target123@atlanta.example.com>
```

```
$  Content-Type: application/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:cl="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
$         entity="pres:alice@atlanta.example.com">
$       <tuple id="sg89ae">
$        <timestamp>2007-07-09T14:00:00Z</timestamp>
$        <status>
$         <gp:geopriv>
$           <gp:location-info>
$             <cl:civicAddress>
$               <cl:country>US</cl:country>
$               <cl:A1>Texas</cl:A1>
$               <cl:A3>Colleyville</cl:A3>
$               <cl:HNO>3913</cl:HNO>
$               <cl:A6>Treemont</cl:A6>
$               <cl:STS>Circle</cl:STS>
$               <cl:PC>76034</cl:PC>
$               <cl:NAM>Haley's Place</cl:NAM>
$               <cl:FLR>1</cl:FLR>
$             <cl:civicAddress>
$           </gp:location-info>
$           <gp:usage-rules>
$             <gp:retransmission-allowed>no</gp:retransmission-allowed>
$             <gp:retention-expiry>2007-07-27T18:00:00Z</gp:retention-
$                            expiry>
$           </gp:usage-rules>
$           <gp:method>DHCP</gp:method>
$           <gp:provided-by>www.example.com</gp:provided-by>
$         </gp:geopriv>
$        </status>
$       </tuple>
$      </presence>
   --boundary1--
```