SIP Working Group   James Polk
Internet Draft   Cisco Systems
Expiration: July 2nd, 2007   Brian Rosen
                                                     NeuStar

                Session Initiation Protocol Location Conveyance
                  draft-ietf-sip-location-conveyance-06.txt
                              Jan 2nd, 2007

Status of this Memo

Copyright Notice

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 proxy servers
   make routing decisions based on the location of the UAC.

Table of Contents

1. Introduction

This document describes how Location can be "conveyed" (that is,
sent on the Internet) from a SIP user agent, or in some
circumstances a proxy server acting on behalf of a user agent, to
another entity using the SIP [RFC3261] protocol. Here "Location" is
a description of the physical geographical area where a User Agent
currently exists. We use the term "conveyance" to distinguish other
circumstances when a location is used such as how the entity
conveying location using this extension determined where the
location was (using, for example, an Assisted GPS mechanism) or a
protocol by which the entity acquired the location it is conveying

from another entity.

   Geographic location in the IETF is discussed in RFC 3693 (Geopriv

Requirements) [RFC3693]. It defines a "target" as the entity whose
location is being transmitted, in this case, it is the user agent'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 User Agent or Proxy Server and the location recipient is
another User Agent or Proxy Server.

Location can be transmitted by-value or by-reference. The "value"
used in this document is a location object as described in
[RFC4119], that is, a PIDF-LO. Location-by-value refers to a user
agent including a PIDF-LO as a body part of a SIP message, sending
that location object to another SIP element. Location-by-reference
refers to a user agent or proxy server including a URI in a SIP
message which can be exchanged by a location recipient for a
location object, in the form of a PIDF-LO.

As recited in RFC3693, location often must be kept private. The
location object (PIDF-LO) contains rules which are binding on 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.

Often, location is sent from the User Agent Client to the User Agent
Server, or vice versa for purposes that are beyond the scope of this
document. 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 may 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.

The Geolocation header is introduced to signify that location is
included in a SIP message to provide either a content identifier
(cid:) pointer to the body part containing the UAs PIDF-LO, or a
location-by-reference URI that may subsequently be "dereferenced" by
a using protocol (which may be SIP or another protocol).

In this document, we frequently 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) should 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.

This document is intended to become a standards track RFC.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL
NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and
"OPTIONAL" in this document are to be interpreted as described
in [RFC2119].

3. Mechanisms

3.1 Overview of SIP Location Conveyance

This document creates a new SIP header: Geolocation. The
Geolocation header contains either a URI which may be a "cid:" URI
(Content Identification, per [RFC2392], or a location-by-reference
URI to be dereferenced by a location recipient to retrieve the
location of the UAC.

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
location-by-value, the actual location information in the PIDF-LO is
included in the body of the message.

If the URI in the Geolocation header is a scheme other than "cid:",
another protocol operation is needed by the message recipient to
obtain the location of the target (UA). This is
location-by-reference. 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
location-by-reference URI, may be included by a User Agent in a
message. A proxy server may assert location of the UA by inserting
the header, which must specify a location-by-reference URI. Since
body parts may not be inserted by a proxy server, location-by-value
cannot be inserted by a proxy.

The Geolocation header may have parameters that are associated
with a URI in the header. The "inserted-by" parameter has values of
"endpoint" or "server", indicative of which entry added location to
the message. This header parameter MAY be added every time a new
location is added into a message.

If a SIP message is routed within the network based on the location
contained within that message, the "message-routed-on-this-uri"
parameter MUST be added as a header parameter of the URI used to
route the message. Once a header parameter is added to a
Geolocation header, it SHOULD NOT be deleted in transit to the

ultimate destination.

Polk & Rosen

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.

This document describes an extension to PIDF-LO, the
"routing-query-allowed" element, defined in the 'usage-rules'
element. When set, this allows an element receiving location to
transmit the location to another element to obtain routing
information. When used in conjunction with the
"retransmission-allowed" element, the rule maker can control
distribution of the location information for location-based routing.

This document also creates a new option tag: Geolocation, to
indicate support for the Geolocation extension. A new error message
(424 Bad Location Information) is also defined in this document.

3.2 The Geolocation Header

This document creates and IANA registers a new SIP header:
Geolocation. The Geolocation header MUST contain one of two types
of URIs:

o a location-by-reference URI, or

o a content-ID indicating where location is within the message body
   of this message

A location-by-reference URI is a pointer to a record on a remote
node containing location of the location target, typically the
UA in this transaction.

A location-by-value content-ID (cid-url) [RFC2392] indicates which
message body part contains location for this UA.

The Geolocation header has the following BNF syntax:

```
Geolocation        =  "Geolocation" HCOLON (locationValue *(COMMA
                        locationValue))
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
                        / "message-routed-on-this-uri"
                        / generic-param ; (from RFC 3261)
geoloc-inserter    =  "endpoint" / "server"
                        / gen-value ; (from RFC 3261)
```

The cid-url is defined in [RFC2392] to locate message body
parts. This URI MUST be present if location is by-value in a

message.

sip-URI, sips-URI and absoluteURI are defined according to RFC3261.
The pres-URI is defined in RFC 3859 [RFC3859].

Other protocols used in the Location URI MUST be reviewed against
the RFC3693 criteria for a using protocol.

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

    INVITE [RFC3261],
    REGISTER [RFC3261],
    OPTIONS [RFC3261],
    UPDATE [RFC3311],
    MESSAGE [RFC3428],
    SUBSCRIBE [RFC3265], and
    NOTIFY [RFC3265]

Use of the header in BYE, INFO and REFER Methods are allowed,
although no purpose is known. Conveying location in a CANCEL, BYE,
ACK or PRACK is not defined. Discussing location using the PUBLISH
Request Method out of scope for this document.

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

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

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

Table 1: Summary of the Geolocation Header

The Geolocation header MAY be included in one of the above messages
by a User Agent. A proxy MAY add the Geolocation header, but MUST
NOT modify the contents of an existing Geolocation header.
[RFC3261] states message bodies cannot be added by proxies.
Therefore, a Geolocation header added by a proxy MUST specify
location-by-reference.

Entities receiving location information MUST honor the usage element
rules per RFC4119. Such entities MUST NOT alter the rule set.

3.3 424 (Bad Location Information) Response Code

If a UAS or SIP intermediary detects an error in a request message

specific to the location information supplied by-value or
by-reference, a new 4XX level error is created here to indicate a

problem with the location in the request message. This document
creates and IANA registers the new error code:

    424 (Bad Location Information)

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

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 SIP intermediary as a result of this error message.

More resolution of the error for which the 424 was generated MAY be
included in a Warning header [RFC3261] with new, IANA registered,
location specific warning values (see Section 3.4).

The new 424 (Bad Location Information) error code is IANA registered
in Section 9 of this document. An initial set of location error
codes are in [ID-ERROR].

3.4 New Warning Codes for Location Error Granularity

As discussed in Section 3.3, more granular error codes, specific to
location errors within a received message, are required if the UAC
is to know what was wrong with the original request. The Warning
header will be used to convey such error conditions within the 424
(Bad Location Information) response. Rather than depleting the
remaining available 3XX codes, codes 700 through 740 will be
designated for Location warnings. Additions to this
IANA registration range for location codes require an RFC.

Warning has the advantage of including the node ID in the header,
meaning the ID of the entity that sent this response. This can
useful for troubleshooting.

The Warning header allows for multiple warning codes be returned in
the same response. If a location-by-reference is sent and the
supplied scheme is not desired or cannot be processed, but more than
one other scheme can be, the 424 response can list more than one
code from the 720-724 range in the response. The UAC may
subsequently retry the operation with one of the schemes supported
or desired by the recipient.

To illustrate this, here is an example of Alice including
location-by-reference using an HTTP schema. Bob cannot dereference
using HTTP, but can dereference using SIP, SIPS, and PRES:

```
        Alice                                Bob
          |                                   |
          |          Request w/ Location      |
          |          using http schema        |
          |---------------------------------->|
          |                                   |
          |                                   |
          |   424 (Bad Location Information)  |
          |   with Warning header containing  |
          |   720 (SIP), 721 (SIPS), 722 (PRES) |
          |<----------------------------------|
          |                                   |
```
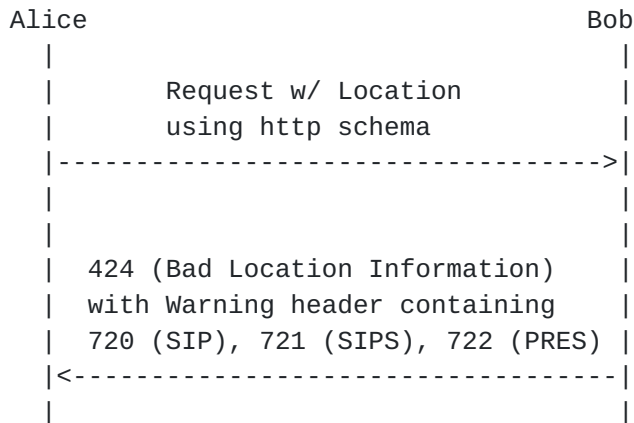
3.4.1 Warning code 701 Location Format Not Supported

A Warning header with the code 701 "Location Format not supported"
means the location format supplied in the request, by-value or
by-reference, was not supported. This cause means the recipient
understood that location was included in the message, but the format
is not supported. Perhaps the format was a freeform text format or
data-URL and the recipient only understood location in RFC4119
PIDF-LO format (civic or geo). If a more specific Warning code is
available, it MUST be used. For example, if the format is
understood, but not desired, a 702 or 703 Warning header SHOULD be
returned. The same applies to a location recipient that only
understands one format and did not receive that format. For example,
if a message containing geo formatted location arrives but the
recipient only can process civic formatted location a 703 Warning
header should be returned in a 424 response.

Recommended warn-text: Location format not supported

An example usage in a SIP 424 response:

Warning: 701 alice.example.com "Location Format not supported"

3.4.2 Warning code 702 Geo-location Format Desired Instead

A Warning header with the code 702 "Geo-location Format Desired"
means the location format supplied in the request (probably
formatted in civic), by-value or by-reference, was understood and
supported, but that the recipient, or an application on the
recipient prefers, or can only process location in the geo-location
format.

A typical reaction to receiving this Warning code is to resend the
original message with location formatted in geo instead.

Recommended warn-text: Geo-location Format Desired

An example usage in a SIP 424 response:

Warning: 702 node_alice.example.com "Geo-location Format Desired"

3.4.3 Warning code 703 Civic-location Format Desired Instead

A Warning header with the code 703 "Civic-location Format Desired"
means the location format supplied in the request (probably
formatted in geo), by-value or by-reference, was understood and
supported, but that the recipient, or an application on the
recipient prefers, or can only process location in the
civic-location format.

A typical reaction to receiving this Warning code is to resend the
original message with location formatted in civic instead.

Recommended warn-text: Civic-location Format Desired

An example usage in a SIP 424 response:

Warning: 703 alice.example.com "Civic-location Format Desired"

3.4.4 Warning code 704 Cannot Parse Location Supplied

A Warning header with the code 704 "Cannot parse location supplied"
means the location provided, whether by-value or by-reference in a
request is not well formed.

Recommended warn-text: Cannot parse location supplied

An example usage in a SIP 424 response:

Warning: 704 alice.example.com "Cannot parse location supplied"

3.4.5 Warning code 705 Cannot Find Location

A Warning header with the code 705 "Cannot find location" means
location should have been in the message received, but the recipient
cannot find it, either because it is not in the message, or it is
encrypted/opaque to the recipient.

A typical reaction to receiving this error would be for the location
sender to verify it has indeed included location in the new request
and send the message again.

Recommended warn-text: Cannot find location

An example usage in a SIP 424 response:

Warning: 705 alice.example.com "Cannot find location"

[3.4.6](#) Warning code 706 Conflicting Locations Supplied

A Warning header with the code 706 "Conflicting Locations Supplied"
means a location recipient received more than one location
describing where the target is, and is either unsure which whole
location is true or which parts of multiple locations make up where
the target is. This is generally a case of either too much
information, and the information is conflicting.

A typical reaction to receiving this error is to reduce the number
of different locations supplied in the request, and send another
message to the location recipient.

Recommended warn-text: Conflicting Locations Supplied

An example usage in a SIP 424 response:

Warning: 706 alice.example.com "conflicting locations supplied"

[3.4.7](#) Warning code 707 Incomplete Location Supplied

A Warning header with the code 707 "Incomplete Location Supplied"
means there is not enough location information, by-value or
by-reference, to determine where the location target is.

A typical reaction to receiving this message is for the sender to
Convey more information if it is willing to do so.

Recommended warn-text: Incomplete location supplied

An example usage in a SIP 424 response:

Warning: 707 alice.example.com "Incomplete location supplied"

[3.4.8](#) Warning code 708 Cannot Dereference

A Warning header with the code 708 "Cannot dereference" means the
act of dereferencing failed to return the target's location. This
generally means the supplied URI is bad.

Recommended warn-text: Cannot dereference

An example usage in a SIP 424 response:

Warning: 708 alice.example.com "Cannot dereference"

[3.4.9](#) Warning code 709 Dereference Denied

A Warning header with the code 709 "Dereference Denied" means there

was insufficient authorization to dereference the target's location
at, or before the LIS. This is a application layer error, so it is
not to be confused with lacking permission through a lower layer
firewall.

Recommended warn-text: Dereference Denied

An example usage in a SIP 424 response:

Warning: 709 alice.example.com "Dereference Denied"

3.4.10 Warning code 710 Dereference Timeout

A Warning header with the code 710 "Dereference Timeout" means that
the dereferencing node has not received the target's location within
a reasonable timeframe.

Recommended warn-text: Dereference Timeout

An example usage in a SIP 424 response:

Warning: 710 alice.example.com "Dereference Timeout"

3.4.11 Warning code 711 Cannot Process Dereference

A Warning header with the code 711 "Cannot process Dereference"
means the dereference protocol has received an overload condition
error, indicating the location cannot be accessed at this time. If
a sip or sips schema were used to dereference the target's location,
and a 503 (Service Unavailable) were the response to the dereference
query, this 711 Warning code would be placed in the 424 (Bad
Location Information) response to the location sender.

Recommended warn-text: Cannot process Dereference

An example usage in a SIP 424 response:

Warning: 711 alice.example.com "Cannot process Dereference"

3.4.12 Warning code 720 Unsupported Schema - sip desired

A Warning header with the code 720 "Unsupported Schema - sip
desired" means the location dereferencer cannot dereference using
the location-by-reference URI schema supplied because it does not
support the necessary protocol to do this. This Warning code means
the location recipient can dereference the target's location using a
sip-URI schema. There can be more than one Warning code in a

Warning header, indicated in this context the recipient can
   dereference using each schema protocol included in the Warning

header.

A typical reaction to receiving this error would be for the location sender to send a URI with the sip schema.

Recommended warn-text: unsupported schema

An example usage in a SIP 424 response:

Warning: 720 alice.example.com "unsupported schema - sip desired"

3.4.12 Warning code 721 Unsupported Schema - sips desired

A Warning header with the code 721 "Unsupported Schema - sips desired" means the location dereferencer cannot dereference using the location-by-reference URI schema supplied because it does not support the necessary protocol to do this. This Warning code means the location recipient can dereference the target's location using a sips-URI schema. There can be more than one Warning code in a Warning header, indicated in this context the recipient can dereference using each schema protocol included in the Warning header.

Recommended warn-text: unsupported schema

An example usage in a SIP 424 response:

Warning: 721 alice.example.com "unsupported schema - sips desired"

3.4.13 Warning code 722 Unsupported Schema - pres desired

A Warning header with the code 722 "Unsupported Schema - pres desired" means the location dereferencer cannot dereference using the location-by-reference URI schema supplied because it does not support the necessary protocol to do this. This Warning code means the location recipient can dereference the target's location using a pres-URI schema. There can be more than one Warning code in a Warning header, indicated in this context the recipient can dereference using each schema protocol included in the Warning header.

Recommended warn-text: unsupported schema

An example usage in a SIP 424 response:

Warning: 722 alice.example.com "unsupported schema - pres desired"

3.5 The Geolocation Option Tag

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

The purpose of the geolocation option-tag is to indicate support for
this extension in the Supported and Unsupported headers. Appearance
of the option tag in the Require header is a request for location to
be conveyed.

A UAC SHOULD NOT include this option tag in a Proxy-Require header,
since is not likely to understand the topology of the
infrastructure, and therefore would not understand which proxy will
do the location-based routing function, if any.

3.6 Using sip/sips/pres as a Dereference Protocol

A sip, sips or pres URI SHOULD be included in a Geolocation header
for the location-by-reference URI. When pres: is used, if the
resulting resolution, per [RFC3851], resolves to a sip: or sips:
URI, this section applies. Use of other protocols for dereferencing
of a pres: URI is not defined, and such use is subject to review
against RFC3693 using protocol criteria.

Dereferencing using sip or sips MUST be accomplished by treating the
URI as a presence URI and dereferencing is accomplished by a
SUBSCRIBE to a presence service per [RFC3856]. The resulting NOTIFY
will contain a PIDF, which MUST contain a PIDF-LO.

When used in this manner, SIP is a using protocol per [RFC3693] and
elements receiving location MUST honor the 'usage-element' rules as
defined in Section 3.4 above.

A dereference of a location-by-reference 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 series
of transactions that contains the UAC's location, with the location
recipient being the only SIP element to receive location - which the
purpose of this extension: to convey location to a specific
destination.

4. Examples

Three examples of messages providing location are provided. One
shows location-by-value with geo-coordinates, one shows

location-by-value with civic location and the third shows
location-by-reference. The examples for (Geo format) are taken

from [RFC3825] and (Civic format) are taken from [ID-CIVIC] and are
for the exact same position on the Earth. The differences between
the two formats is 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.

4.1 Location-by-value (Coordinate Format)

This example shows an INVITE message with a coordinate, or geo
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: 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:alice123@atlanta.example.com>
  ;inserted-by=endpoint
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 here

--boundary1

Content-Type: application/pidf+xml
Content-ID: alice123@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:gs="urn:ietf:params:xml:ns:pidf:geopriv10:geoShape"
       entity="pres:alice@atlanta.example.com">
     <tuple id="sg89ae">
      <timestamp>2007-03-20T14:00:00Z</timestamp>
      <status>
       <gp:geopriv>
         <gp:location-info>
```

```
        <gml:location>
          <gml:Point gml:id="point96" srsName="epsg:4326">
```

```
                   <gml:coordinates>33.001111N
                                  96.68142W</gml:coordinates>
               </gml:Point>
             </gml:location>
          </gp:location-info>
          <gp:usage-rules>
            <gp:retransmission-allowed>no</gp:retransmission-allowed>
            <gp:retention-expiry>2007-03-24T18:00:00Z</gp:retention-
                        expiry>
            <gp:method>DHCP</gp:method>
            <gp:provided-by>www.cisco.com</gp:provided-by>
          </gp:usage-rules>
        </gp:geopriv>
      </status>
    </tuple>
   </presence>
--boundary1--
```

The Geolocation header from the above INVITE...

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

...indicates the content-ID location [RFC2392] within the multipart
message body of were location information is, with SDP being the
other message body part.

If the Geolocation header were this instead:

```
   Geolocation: <sips:server5.atlanta.example.com/alice123>
```

...this would indicate location by-reference was included in this
message. It is expected that any node wanting to know where user
alice123 is would subscribe to server5 to dereference the sips-URI.
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.

4.2 Location-by-value (Civic Format)

This example shows an INVITE message with a civic location. The
headers are shown as if the location was S/MIME encrypted, but the
unencrypted location information is shown for clarity. The lines
below that have the '$' signs are encrypted.

```
INVITE sip:bob@biloxi.example.com SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.example.com
   ;branch=z9hG4bK74bf9
Max-Forwards: 70
```

```
   To: Bob <sip:bob@biloxi.example.com>
   From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
```

```
    Call-ID: 3848276298220188511@atlanta.example.com
    Geolocation: <cid:alice123@atlanta.example.com>
      ;inserted-by=endpoint
    Supported: geolocation
    Accept: application/sdp, application/pidf+xml
    CSeq: 31862 INVITE
    Contact: <sip:alice@atlanta.example.com>
    Content-Type: multipart/mixed; boundary=boundary1
    Content-Length: ...

    --boundary1

    Content-Type: application/sdp

    ...SDP here

    --boundary1

    Content-Type: application/pkcs7-mime;
        smime-type=enveloped-data; name=smime.p7m
    Content-ID: alice123@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"
$           xmlns:gs="urn:ietf:params:xml:ns:pidf:geopriv10:geoShape"
$           entity="pres:alice@atlanta.example.com">
$         <tuple id="sg89ae">
$          <timestamp>2007-03-20T14:00:00Z</timestamp>
$          <status>
$           <gp:geopriv>
$             <gp:location-info>
$               <cl:civilAddress>
$                 <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:civilAddress>
$             </gp:location-info>
$             <gp:usage-rules>
$                <gp:retransmission-allowed>no</gp:retransmission-allowed>
```

```
$              <gp:retention-expiry>2007-03-24T18:00:00Z</gp:retention-
$                            expiry>
$              <gp:method>DHCP</gp:method>
```

```
$              <gp:provided-by>www.cisco.com</gp:provided-by>
$            </gp:usage-rules>
$          </gp:geopriv>
$        </status>
$      </tuple>
$    </presence>
   --boundary1--
```

4.3 Location-by-reference

   Here is an example of an INVITE with a location-by-reference URI,
   sips: in this case, instead of a location-by-value PIDF-LO message
   body part shown in Sections 4.1 and 4.2. It is up to the location
   recipient to dereference Alice's location at the Atlanta LIS.

```
   INVITE sip:bob@biloxi.example.com SIP/2.0
   Via: SIP/2.0/TCP pc33.atlanta.example.com
     ;branch=z9hG4bK74bf9
   Max-Forwards: 70
   To: Bob <sip:bob@biloxi.example.com>
   From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
   Call-ID: 3848276298220188511@atlanta.example.com
   Geolocation: <sips:3sdefrhy2jj7@lis.atlanta.example.com>
     ;inserted-by=server
   Supported: geolocation
   Accept: application/sdp, application/pidf+xml
   CSeq: 31862 INVITE
   Contact: <sip:alice@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 to retrieve Alice's location. If the
   atlanta.example.com domain chooses to implement location conveyance
   and delivery in this way (i.e. location-by-reference), it is
   RECOMMENDED that entities outside this domain be able to reach the
   dereferencing LIS server, otherwise this model of implementation is
   only viable within the atlanta.example.com domain. This will likely
   not suit some services already being considered in the IETF at the
   time of this writing, such as emergency calling.

5. SIP Element Behavior

   Because a person's location is generally considered to be sensitive
   in nature, privacy of the location information must be protected
   when transmitting such information. Section 26 of [RFC3261] defines
   the security functionality SIPS for transporting SIP messages with
   either TLS or IPSec, and S/MIME for encrypting message bodies from

SIP intermediaries that would otherwise have access to reading the
clear-text bodies. SIP endpoints SHOULD implement S/MIME to encrypt

the PIDF-LO message body (part) end-to-end when the intended
recipient is the opposite UA. The SIPS-URI from [RFC3261] MUST be
implemented for message protection (message integrity and
confidentiality) and SHOULD be used when S/MIME is not used.
Possession of a dereferenceable location URI may be equivalent to
possession of the location information itself and thus TLS SHOULD be
used when sending location-by-reference.

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 location-by-reference, it is
RECOMMENDED that the URI not contain any identifying information
(for example use 3fg5t5yqw@example.com rather than
alice@example.com)

The entities receiving location MUST obey the privacy
and security rules in the PIDF-LO as described in RFC4119, regarding
retransmission and retention.

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

More than one location representation or format, for example: civic
and geo, MAY be included in the same message body part, but all MUST
point at the same position on the earth. Multiple representations
allow the recipient to use the most convenient representation of
location.

There MAY be more than one PIDF-LO in the same SIP message, but each
in separate message body parts. Each location body part MAY point at
different positions on the earth. The meaning of such a
construction is not defined, and may cause confusion at the
recipient

5.1 UAC Behavior

A UAC may send location because it was requested to, to facilitate
location-based routing, or spontaneously (i.e. a purpose not defined
in this document but known to the UAC). A UAC MAY receive location
from the UAS spontaneously.

A UAC conveying location MUST include a Geolocation header with
either a location by-value indication (a cid-URL), or a location
by-reference indication (a dereferenceable URI). A location body
sent without a Geolocation header MUST NOT occur. The UAC
supporting this extension MUST include a Supported header with the
geolocation option tag.

The presence of the geolocation option tag in a Supported header

without a Geolocation header in the same message informs a receiving
SIP element the UAC understands the concept of location, but it does
not know its location at this time. Certain scenarios exist
(location-based routing) in which location is required in a message
in order to route the message properly. This affects how a UAS or
SIP server reacts to such a message.

The geolocation option tag SHOULD NOT be used in the Proxy-Require
Header.

If the UAC inserts a geolocation header, it SHOULD include a
"inserted-by=endpoint" parameter. For example:

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

UACs receiving a 424 (Bad Location Information) response MAY find a
more granular cause for the location based error in a Warning
header. Section 3.4 extends the list of IANA registered Warning
codes, specifically for location errors within the request. The
UAC SHOULD learn from the Warning code in the response and take
appropriate steps based on that error given before attempting to
convey location again. See Section 3.4. for the list of new
location specific Warning codes.

There MAY be future work defining additional error information, say
in an XML body, indicating exactly what the error was, if any of the
new Warning codes are ambiguous.

The behavior of the UAC receiving location is the same as the UAS,
as below, except a UAC cannot send a Warning code indicating
something was wrong with the location supplied by the UAS. In this
case, the location information SHOULD just be ignored in this
transaction. A subscription is a better means of getting a UAS's
location.

5.2 UAS Behavior

If the Geolocation header is present, the URI contained in as a
header field will indicate if location has been conveyed by-value in
a message body (part) or by-reference, requiring an additional
dereference transaction. If the by-reference URI is sip:, sips: or
pres:, the UAS will initiate a SUBSCRIBE to the URI provided to
retrieve the PIDF-LO of the UAC per [RFC3856]. If successful, the
PIDF-LO of the UAC will be returned in the NOTIFY request from the
server.

A Require header with the geolocation option tag indicates the
UAC is requiring the UAS understand this extension or error the

message. A 420 (Bad Extension) with a geolocation option tag in a
Unsupported header would be the appropriate response.

If the UAC conveys location in a request, but the UAS has one or
more problems with the location in the request (or while attempting
to dereference the UAC's location), a 424 (Bad Location Information)
response would be an appropriate response. If the UAS can indicate
what the problem is with the location in the request, in the form of
one of the new Warning codes specifically about location errors, the
Warning header SHOULD be included along with the most applicable
Warning code(s). Zero or more Warning codes are allowed in a
response.

For example, if a UAC conveyed location-by-reference and chose a
pres schema for the UAS to dereference, and the UAS cannot or will
not dereference using pres (for whatever reason), the UAS can
include more than one Warning code in the 424 response to indicate
what will be acceptable to the UAS in this case. This scenario would
like something like this:

Warning: 720 UAS-ID Unsupported Schema - sip desired,
         721 UAS-ID Unsupported Schema - sips desired,

The UAS behavior for sending location is the same as the UAC as
above.

5.3 Proxy Behavior

[RFC3261] states message bodies cannot be added by proxies.
However, a proxy may add a header to a message. This implies that a
proxy MAY add a geolocation header with location-by-reference, but
not location-by-value.

A proxy MAY read the Geolocation header, and the associated body, if
not S/MIME protected, in transit if present, and MAY use the
contents of the header to make location-based routing decisions.

More than one Geolocation header or header value in a message is
permitted. The meaning of such a construction is not defined, and
may cause confusion at the recipient.

Proxies receiving location where the proxy performs location-based
routing may need to consult external databases or systems to
determine the route. Transmission of the location information
(which SHOULD NOT reveal identity, even if the proxy knows the
identity) is governed by the 'retransmission-allowed' and
'routing-query-allowed':

Retransmission-allowed Routing-query-allowed Transmission for Query
---------------------- -------------------- ----------------------
"no" or not present   "no" or not present   Not Allowed

```
"no" or not present     "yes"             Allowed
"yes"                   not present       Allowed
```

```
  "yes"                  "no"                  Not Allowed
  "yes"                  "yes"                 Allowed
```

   If transmission is not allowed per the above, the proxy SHOULD
   provide a suitable error response. The 424 (Bad Location) is the
   appropriate response here.

5.3.1 Proxy Behavior with Geolocation Header Parameters

   When a message traverses a SIP intermediary, any existing header
   value URI and header parameter MUST NOT be modified or deleted,
   but MAY be augmented to indicate if the message was routed based on
   a specific geolocation URI. For example:

```
   Geolocation: <cid:alice123@atlanta.example.com>;
                inserted-by=endpoint; message-routed-on-this-uri
```

   A SIP intermediary MAY add a new Geolocation URI value to a message.
   The proxy SHOULD NOT insert a location unless it is reasonably
   certain it knows the actual location of the endpoint, 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).

   B2BUAs normally set the "inserted-by" parameter to "server".

   A server adding a geolocation value to an existing endpoint inserted
   location would look like:

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

   If this message was then routed by an intermediary using the URI
   inserted by the server, the intermediary would note this as:

```
 Geolocation: <cid:alice123@atlanta.example.com>; inserted-by=endpoint,
              <sips:3sdefrhy2jj7@lis.atlanta.example.com>;
               inserted-by=server; message-routed-on-this-uri
```

   It is conceivable that an initial routing decision is made on an
   existing header, and subsequently another routing decision is made
   on a different header, perhaps even subsequently added by another
   proxy on the path. While unusual, it could occur. In such a case,
   the later routing proxy MUST remove the incoming
   "message-routed-on-this-uri" and replace it with another on the URI
   it uses for routing. Downstream entities will not be able to
   determine that two routing decisions were made on different location
   values. Such a circumstance is considered unlikely to happen, and
   the inability to detect it is not considered harmful.

5.3.2 Proxy Error Behavior with Warning Codes

If a SIP intermediary detects a location specific problem with a SIP
request, if SHOULD reply with a 424 (Bad Location Information)
response and include the appropriate Warning code defined in Section
3.4 so the UAC can take whatever corrective action it needs to take
to send a new message with good location information.

6. Special Considerations for Emergency Calls

Emergency calls (1-1-2, 9-1-1, etc.) need location for two reasons:

1. Location is needed to route the call to the correct Public Safety
   Answering Point (PSAP), and

2. Location is needed by the PSAP to send responders to the location
   of the caller when the caller cannot accurately describe where
   s/he is

While all of the privacy concerns for location apply to emergency
calls, it is not acceptable for a security mechanism in place to
support confidentiality of the location to cause an emergency call
to be misrouted, or not supply location when it is needed.
Therefore, some of the behaviors of elements in the path are
different when used with an emergency call.

Recognizing which calls are emergency calls is beyond the scope of
this document. When an emergency call is placed, location is
normally provided by the UAC. Since emergency calls must be routed
based on location (and indeed, in some jurisdictions, there may be
several steps to such routing), the location must be visible to
proxies along the path. Thus S/MIME protection of location MUST NOT
be used. TLS protection of location SHOULD be used, however, if
establishment of the TLS connection fails, the call set-up
operation, including location conveyance, MUST be retried without
TLS.

The entity inserting the geolocation header MUST specify the
"inserted-by" parameter, with values of "endpoint" or "server" as
appropriate.

Both the "retransmission-allowed" and "routing-query-allowed" SHOULD
be set to "yes". Querying for routing may be performed by proxies
providing a routing service for emergency calls even if
retransmission-allowed or routing-query-allowed is set to "no" or is
not present. Proxies routing on the location MUST set the
"message-routed-on-this-uri" parameter.

While many jurisdictions force a user to reveal their location

during an emergency call set-up, there are a small, but real, number
of jurisdictions that allow a user to configure their calling device

to disable providing location, even during emergency calling. This
capability MUST be configurable, but is NOT RECOMMENDED as the
default configuration of any UA. Local policies will dictate this
ability.

7. Geopriv Privacy Considerations

Transmitting location information is considered by most to be highly
sensitive information, requiring protection from eavesdropping,
tracking, and altering in transit. [RFC3693] articulates rules to
be followed by any protocol wishing to be considered a Geopriv
"using protocol", specifying how a transport protocol meetings
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
RFC3261 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 may be authentication and integrity
concerns. This document calls for conveyance to normally be
accomplished through secure mechanisms (like S/MIME or TLS). In
cases where a session set-up is routed based on the location of the
UAC initiating the session or SIP MESSAGE, securing the by-value
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
information to route the message appropriately. 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 may
not be appropriate either.

When the UAC is the source of the location information, 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. Emergency calls have their own
rules in this regard, as detailed in Section 6. 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.

9. IANA Considerations

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 3.2 of this document.

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 3.5 of this document.

9.3 IANA Registration for Response Code 4XX

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

This SIP Response code is defined in section 3.3 of this document.

9.4 IANA Registration of New Warning Codes for Location

New location specific Warning codes are created by this document,

with the definitions in Section 3.4 of this document.

```
701 Location Format Not Supported
702 Geo-location Format Desired Instead
703 Civic-location Format Desired Instead
704 Cannot Parse Location Supplied
705 Cannot Find Location
706 Conflicting Locations Supplied
707 Incomplete Location Supplied
708 Cannot Dereference
709 Dereference Denied
710 Dereference Timeout
711 Cannot Process Dereference
720 Unsupported Schema - sip desired
721 Unsupported Schema - sips desired
722 Unsupported Schema - pres desired
```

Adding new location specific Warning codes, or modifying to existing location specific Warning codes requires an RFC and community review.

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 and Paul Kyzivat for constructive feedback. Thanks to Dan Wing for help with the S/MIME example.

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.

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

 [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 2393, 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.

11.2 **References - Informative**

   [ID-ERROR] J. Polk, "A Geopriv Registry for Location-based Error
             Response Codes",
             draft-polk-geopriv-location-based-error-registry-00, "work
             in progress", October 2006

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

   [ID-CIVIC] H. Schulzrinne, " Dynamic Host Configuration Protocol
             (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration
             Information ", draft-ietf-geopriv-dhcp-civil-09, "work in
             progress", January 2006

      Author Information

      James Polk
      Cisco Systems
      3913 Treemont Circle   33.00111N
      Colleyville, Texas 76034   96.68142W

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

Brian Rosen
NeuStar, Inc.

     470 Conrad Dr.   40.70497N
     Mars, PA 16046   80.01252W
     US

     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
   user agent client, the user agent server, 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 by-value or
          by-reference.

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-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 user
agent server:

UAS-1   SIP Responses must support location conveyance.

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
         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. Changes from Prior Versions

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

   This is a list of the changes that have been made from the SIP WG
   version -05 to this version -06:

   - cleaned up some inconsistencies wrt the S/MIME example in Section
     4.2

   - changed the ABNF to include the ability to indicate which SIP
     element inserted a particular location URI, and how a message
     routing server indicates which location the message was routed
     upon (based on the location in the message)

   - changed the granular error code from a Reason header indication to
     a Warning code indication (section 3.4), and IANA registered 14
     new Warning codes in this document

   - As a consequence of the above bullet, changed the specific SIP
     element behaviors of each SIP element regarding sending or
     receiving a 424 response with a Warning header

   - Added rules about indicating which SIP element inserted a
     particular location into a message (a new Geolocation header
     parameter), as well as when a server adds another new header
     parameter indicating the request was routed based on a particular
     location included in the message

   This is a list of the changes that have been made from the SIP WG
   version -04 to this version -05:

   - altered the meaning of use of OPTIONS to not be for retrieving the
     location of a UAS, but for cases in which location is a required
     element of information by a SIP entity.

   - added a comment/warning for usage of location-by-reference to a
     model in which a domain's LIS be reachable if location is deployed
     in this fashion (Section 4.3)

   - added a Informative reference to a new ID that is an IANA registry

of location specific error codes to be used in, for example, a
Reason header, to give more granular reasons why a 424 (Bad

Location Information) was sent.

This is a list of the changes that have been made from the SIP WG
version -03 to this version -04:

- removed the inappropriate 2119 language from the Requirements
  section.

- removed the old Section 2., which was a Location in a header vs.
  in a body artifact from the original versions of the document.

- Added a new Geopriv (or Privacy) Considerations

- Changed the ABNF to reflect discussion on how restrictive the
  location-by-reference schemes should be, with an added "Editor's
  Note" discussing the issues being faced on this point.

- Changed the "Location" header and option-tag to "Geolocation"
  header and option-tag, due to it being pointed out that there is a
  conflicting HTTP header called "Location".

- Added new element to PIDF-LO 'routing-query-allowed'

- Stipulated the Reason Header can be used in the 424 Response
  Message

- added SUBSCRIBE and NOTIFY as Methods for location conveyance when
  used to dereference a sip:, sips: or pres: location-by-reference
  URI

- Added OPTIONS Method for a UAC to request the location of a UAS
  with a Require header geolocation option-tag.

This is a list of the changes that have been made from the SIP WG
version -02 to this version -03:

- general clean-up of some of the sections

- removed the message examples from the UPDATE, MESSAGE and REGISTER
  sections, as these seemed to be making the doc less readable, and
  not more readable

- removed the "unknown" option tag, as it was not needed with a
  certain combination of the Supported and Location headers

- clarified the location option tag usage in Supported, Require,
  Unsupported, and that it shouldn't be used in Proxy-Require, and
  why not.

- Added a basic message flow to the basic operation section (Section

[4](#)) to aid in understanding of this SIP extension.

- Added a message routing flow, which is based on the location of
  the requestor to show how a SIP server can make a routing decision
  to a destination based on where the UAC is.

- Articulated how a UAS concludes a UAC understands this extension,
  yet does not know its location to provide to the UAS. This is
  helpful in those times where an intermediary will act differently
  based on whether or not a UAC understands this extension, and
  whether or not the UAC includes its location in the request.

- Corrected the erroneous text regarding an Unsupported header being
  in a 424 response. It belongs in a 420 response. (Section 5.1)

- Corrected the BNF (I hope)

- Corrected some text in Section 5 that read like this document was
  an update to RFC 3261.

This is a list of the changes that have been made from the SIP WG
version -01 to this version -02:

- streamlined the doc by removing text (ultimately removing 42 pages
  of text).

- Limited the scope of this document to SIP conveyance, meaning only
  how SIP can push location information.

- reduced emergency calling text to just a few paragraphs now that
  the ECRIT WG is taking most of that topic on.

- greatly reduced the number of requirements in this version.

- changed the requirements groups from "UA-to-UA", "UA-to-Proxy",
  etc to "UAC Reqs", "UAS-Reqs" and "Proxy-Reqs" to focus on what is
  being asked of each SIP element.

- Removed the full SIP message examples.

- completed the ABNF for the Location header, including a cid-url to
  point at a message body part to help in parsing for location.

- Deleted the call for a new 425 (Retry Location) response code, as
  it appears this can easily be used to spoof a UA into providing
  where it is inadvertently, even if the intent is legitimate by the
  UAC.

This is a list of the changes that have been made from the SIP WG
version -00 to this version -01:

- cleaned up a lot of loose ends in the text

- created a new Location header to convey many means (location is in

the body - even if not viewable, which location format is present,
which format is requested in a query, how to request more than one
location format in a query, whether the UAC understands location
at all, if the UA knows its location, how to push location from
one UA to through a second to a third UA, etc).

- added the ability to convey location by-reference, but only under
  certain conditions.

- Added support for the OPTIONS Request to query a server for the
  UAC's location, through the use of the new Location header.

- moved both new Response code sections forward in the document for
  their meaning to be clearer, earlier for necessary discussion.

- Changed the message flows to only have the pertinent message
  headers shown for brevity.

- Added text to the SUB/NOT section showing how and why the location
  of a UA can be refreshed or updated with an interval, or by a
  trigger.

This is a list of the changes that have been made from the SIPPING
WG version -02 to this SIP WG item document version -00:

- Changed which WG this document is in from SIPPING to SIP due to
  the extension of the protocol with new Response codes (424 and
  425) for when there is an error involving the LO message body.

- Moved most of the well formed SIP messages out of the main body of
  this document and into separate appendixes. This should clean up
  the document from a readability point of view, yet still provide
  the intended decode examples to readers of this document who wish
  that level of detail per flow. The first few flows still have the
  decoded SIP messages (unencrypted and encrypted).

- Removed some flow examples which no longer made sense

- Changed all references of "ERC" (Emergency Response Center) to
  "PSAP" (Public Safety Answering Point) as a result of discussion
  within the new ECRIT WG to define a single term

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

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

- added "Bad Location Information" as section 8.6

- added "Retry Location Body " as section 9.3

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

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

- added SUBSCRIBE and NOTIFY as [section 8.5](#)

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

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

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

- removed use of reINVITE to convey location

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

- updated list of open issues

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

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

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

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

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

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

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

- Brian Rosen was brought on as a co-author

- Requirements that a location header were negatively received in

the previous version of this document. AD and chair advice was to
move all location information into a message body (and stay away

   from headers)

   - Added a section of "emergency call" specific requirements

   - Added an Open Issues section to mention what hasn't been resolved
     yet in this effort

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

   - Added the IPR Statement section

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

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

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

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

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

   - added a few names to the acknowledgements section

Intellectual Property Statement

   The IETF takes no position regarding the validity or scope of any
   Intellectual Property Rights or other rights that might be claimed
   to pertain to the implementation or use of the technology described
   in this document or the extent to which any license under such
   rights might or might not be available; nor does it represent that
   it has made any independent effort to identify any such rights.
   Information on the procedures with respect to rights in RFC
   documents can be found in BCP 78 and BCP 79.

   Copies of IPR disclosures made to the IETF Secretariat and any
   assurances of licenses to be made available, or the result of an
   attempt made to obtain a general license or permission for the use

of such proprietary rights by implementers or users of this
specification can be obtained from the IETF on-line IPR repository

at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any
copyrights, patents or patent applications, or other proprietary
rights that may cover technology that may be required to implement
this standard. Please address the information to the IETF at
ietf-ipr@ietf.org.

Disclaimer of Validity

Copyright Statement

Acknowledgment