SIP Working Group
Internet Draft
Expiration: Dec 26th, 2006

James Polk
Cisco Systems
Brian Rosen
NeuStar

Session Initiation Protocol Location Conveyance

draft-ietf-sip-location-conveyance-03.txt

June 26th, 2006

Status of this Memo

Copyright Notice

Abstract

This document defines how the Session Initiation Protocol (SIP) conveys, or pushes, geographic location information from one SIP entity to another SIP entity. SIP Location Conveyance is always end to end, but sometimes the embedded location information can be acted upon by SIP Servers to direct where the message goes, based on where

the user agent client is.

Table of Contents

1. Introduction

There are several situations in which it is desired or necessary for a Session Initiation Protocol (SIP) [RFC3261] user agent to convey, or push its geographic Location Information (LI) from one SIP entity to another. This document discusses the rules for such conveyance, and includes the requirements to be met when a SIP UAC wants or needs to convey its location to another SIP entity. A concept of inheritance exists in which the conveyance of the location of a user agent means conveying the location of a user of that user agent.

This is not an absolute in SIP, but applies for the pushing of location using SIP. The privacy concerns of this topic are also discussed, and need to meet the requirements laid out in RFC 3693 [RFC3693]. This document does not discuss the pulling of location information from a remote element to learn that element's location. This is left for a future effort.

Why would a SIP user agent (UA) push its location to another SIP UA?

There are 3 reasonable scenarios why location can be, or needs to be

conveyed to a remote SIP element:

1) to include location in a request message seeking the nearest instance of destination, where there could be more than one choice; (hey, here I am, I want to talk to the nearest instance of you? i.e. where's the nearest Pizza Hut relative to where I am now).

2) to push the user agent's location to a server such that it can either deal with all the inquiries, leaving the UA to do other tasks (Presence Server), or allow the server to return information to that UAC according to what the UAC is at this time.

3) to inform the user of another UA where the sending user is; (dude, he is where I am) or (I need help, here I am)

Scenario #1 revolves around the idea of a user wanting to find the nearest instances of something else. For example, where is the nearest pizza parlor. A chain of pizza parlors may be contacted through a single well known URI (sip:pizzaparlor.example.com). This by itself does not solve enough to the sending UA. The server at this well known URI needs to know where the nearest one is to the requester. In SIP, this could be accomplished in the initial message by including the location of the UAC in the Request message. This allows the SIP message to be forwarded to the closest physical site by the pizzaparlor.com proxy server. Additionally, the receiving site's UAS uses the UAC's location to determine the location your delivery. A more immediate example may be: where's the nearest (car) garage repair shop, because the user of the UAC has a flat tire.

Scenario #2 revolves around pushing the user's location information

to an external server to deal with all location requests in the future. This leaves a buffer layer between the user and the seeker of the user's location. This server would typically handle all security checks and challenges of those seeking the user's location, as well as handling all the processing of the location target's profile rules entered into that server. This external server c/would be a Presence server. This scenario will not be addressed in this document because of the prevailing Presence solutions for conveying location information.

Alternatively, a user agent pushing location to a server can allow that server to provide back information pertinent to that UA's location. Perhaps replying with certain information unique to the country or region a mobile UA resides. This would not be possible without the server knowing where the UA is.

Scenario #3 actually has a part A and a part B to it. Both involve the UAC including its location in the request to the UAS within a SIP transaction. Part A simply has the user, Alice, informing

another user, Bob, where she is. This could be the loan purpose for this SIP message, or it could be part of another transaction - in which location were merely included, such as within a call set-up.

Part B of scenario #3 has a user, Alice, calling for help and including location to inform who she's calling where she is. This is where the called party needs to come bring help to. Within this scenario, the UAC will need to know this is a special SIP request message to include the UAC's location in this message. It is envisioned that SIP elements along the path of the SIP request will need to know where Alice's UA is for proper routing purposes. An example of this special SIP request is an emergency call set-up.

While scenarios 1, 2 and 3A should use some form of SIP security, typically at the wishes of the user, scenario 3B may or may not involve SIP security measures. This is because including any security measures may cause the SIP request to fail, and that is likely not a good result. It is also conceivable that a first attempt with the user's security measures enabled is tried, and if there are any failures, the subsequent attempt or attempts do not involve security measures. Most believe that completing the emergency call is more important than protecting the information in the SIP message. Obviously this is up to local and jurisdictional

policies, but is mentioned here as a hint of a rationale of a later section of this document.

This document does not discuss how the UAC discovers or is configured with its location. This document however will specify how it meets the requirements for SIP qualifying as a "using protocol" as defined in [RFC3693], in section 7.

Section 3 lists the requirements for SIP location conveyance. Section 4 defines how SIP conveys location. Section 5 illustrates specifics about location conveyance in certain SIP request messages. Section 6 briefly discusses pertinent behaviors with respect to the unique nature of emergency calling. Section 9 provides the security considerations and Section 9 IANA registers one new SIP header, two new option tags and one new 4XX Response codes.

The "changes from prior versions" section (the old Section 1.2) has been moved to the lone appendix, as its size is getting too large for efficient reading of this document.

1.1 Conventions used in this document

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

2. Location In the Body or in a Header

In determining where "location" is placed in a SIP message, consideration is taken as to where the trust model is based on the architecture involved.

If the user agent has the location stored within it, and this user agent wants to inform another user agent where it is, it seems reasonable to have this accomplished by placing the location information (coordinate or civic) in a message body (part), sending it as part of a SIP request or response. This is location by-value.

No routing of the request based on the location contents is required in this case, therefore no SIP Proxies between these two UAs need to view the location information contained in the SIP message(s). The

UAC should know certain types of messages will be routed based on the UA's location when creating a message.

RFC 3261 does not permit SIP intermediaries to modify or delete a message body [RFC3261]. There is, however, no restriction on intermediaries viewing message bodies. S/MIME protected message bodies, implemented on bodies for end-to-end communications only (i.e. between user agents), would render the location object opaque to a proxy server from any viewing of the message body.

The location format is defined in [RFC4119] as a "Presence Information Data Format - Location Object", or PIDF-LO. The amount of information that is necessary to appropriately transmit location information in a format that is understandable is larger than a SIP header could realistically include. However, there must be a means for both a UAC to include a reference point to where location can be retrieved from a remote server, and in some cases, for a SIP server to add a UAC's location to a SIP message as it is processed by that element. This must be in a SIP header for the above stated reason, and should therefore be in a compact form. A URI satisfies this description. This is location-by-reference.

The idea of Location-by-Reference is to allow a UA to store its location on a remote node, to be retrieved by who has this URI. This concept allows the remote node to use its processing power to handle all policy rule operations the user wants performed per request, and all security challenges done as well.

Since location in a message body may be opaque to a routing element, message needing to be routed based on the UAC's location should not have said location in the message body where it may not be seen. A UAC's Location in these cases should be in the Location header where it can be dereferenced by a (SIP) routing element.

[RFC3693] prefers S/MIME for confidentiality and integrity of Location Information on an end-to-end basis, and indeed S/MIME is preferable in SIP [RFC3261] for protecting a message body.

Accordingly, this document specifies location be carried in a body when it is known to/stored in a user agent for end-to-end conveyance of location. The use of SIPS [RFC3261] is orthogonal to this discussion and should always be used.

It is conceivable that an initial attempt to communicate with

location included may fail due to the security measures used. Subsequent requests ought to use less security. For example, if an initial request used S/MIME and failed. A subsequent request could downgrade the security measures used to that of TLS. A message may be important enough, say an emergency call attempt, where TLS is not used. This should not be a default configuration, but a fallback usage. This is always a matter for local and jurisdictional policy.

3. 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.

3.1 Requirements for a UAC Conveying Location

The following are the requirements for location conveyance by a user agent client. There is a motivational statement below each requirements that is not obvious in intent.

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. See Section 7 for analysis.

UAC-8 The PIDF-LO [RFC4119] is a mandatory to implement format for location conveyance within SIP, whether included by-value or by-reference.

If location is within the message, it is a PIDF-LO by-value in a message body (part). If location is stored on an external node, it is dereferenced as a PIDF-LO.

Motivation: interoperability

UAC-9 A UAC MUST be capable of transmitting a SIP request without protecting the PIDF-LO message body. It is RECOMMENDED this not be the default configuration of any UA. This requirement is orthogonal to the use of TLS or IPSec hop-by-hop between SIP elements.

Motivation: If a SIP request is part of an emergency call, therefore includes the UAC's location, the UAC may understand through local policy or configuration that a proxy server will need to learn the UAC's location to route the message correctly. Using S/MIME on the PIDF-LO defeats this capability in proxies.

UAC-10 A UAC MUST allow its user to be able to disable providing location within any SIP request message. It is RECOMMENDED this not is the default configuration of any UA.

Motivation: local laws may give this right to all users within a jurisdiction, even when the request is initiating an emergency call.

UAC-11 A UAC SHOULD NOT use the Proxy-Require header indicating a SIP intermediary is required to act upon location within a SIP message.

Motivation: This is because it is not expected that all SIP elements will understand location, therefore the chances of a message failure is high if proxies are required to support location before forwarding a message. This will lead to unnecessary message failures.

3.2 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 one, mandatory to implement means of receiving location confidentially.

Motivation: interoperability

UAS-3 The PIDF-LO [RFC4119] is a mandatory to implement format for location conveyance within SIP, whether included by-value or by-reference.

If location is within the message, it is a PIDF-LO by-value in a message body (part). If location is stored on an external node, it is dereferenced as a PIDF-LO.

Motivation: interoperability

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

UAS-5 UASs MUST be prepared to receive location without privacy mechanisms enabled. It is RECOMMENDED this not be the default configuration of any UA, however, this MUST be possible for local laws that require this function.

Motivation: Because a SIP request can fail in transit for security reasons, UACs are allowed to transmit, or retransmit requests including location without any security mechanisms utilized, even when this SIP transaction is an emergency call. UAs must be prepared to receive the messages without confidential location.

UAS-6 There MUST be a unique 4XX error response code informing the UAC it did not provide applicable location information.

3.3 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 NOT modify or remove a location message body part, and SHOULD NOT modify or remove a location header or location header value.

Motivation: [RFC3261] forbids the removal of a message body part, and the proxy may not have all the relevant information as to why location was included in this message (meaning it might need to be there), and should not remove this critical piece of information.

Proxy-2 Proxy servers MUST be capable of adding a Location header during processing of SIP requests.

Motivation: If the proxy determines a message needs to have the location of the UAC in the message, and knows the UAC's location by-reference, it must be able to add this header and URI to the message during processing. This SHOULD NOT violate requirement Proxy-3 below.

Proxy-3 If a Proxy server detects "location" already exists within a SIP message, it SHOULD NOT add another location header or location body to the message.

Motivation: This may lead to confusion downstream. Section 4.1 explains this more.

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

4. Location Conveyance Using SIP

RFC 4119 defines the PIDF-LO location object to be inside a RFC 3693 defined "using protocol" message from one entity to another entity. For SIP location conveyance, using the PIDF-LO body satisfies the entire format and message-handling requirements as stated in the baseline Geopriv Requirements [RFC3693].

Although a PIDF-LO is to be used to indicate location of a UA, the actual PIDF-LO does not need to be contained in the message itself, it can be as a by-reference URI in a SIP header or message body part, pointing to the PIDF-LO of that UA on a remote node.

The basic operation of location conveyance is as easy as this in Figure 1., showing a user agent conveying its location to another user agent:

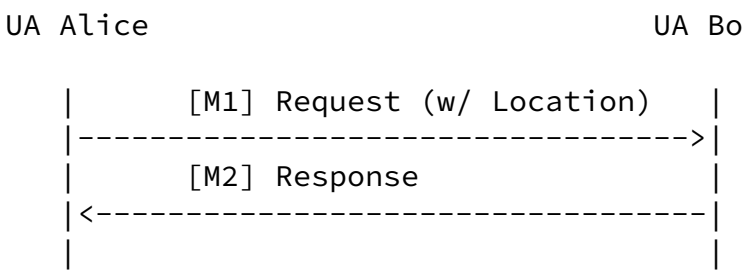

Figure 1. Basic SIP Location Conveyance

Alice wants to inform Bob where she is. She includes location by-value (in a message body) or by-reference (in a new Location header) in her request message towards Bob. Bob MAY choose to include his location in a response back to Alice.

Another usage of location conveyance is for a SIP Server route the SIP request message based on included location information, by-value or by-reference, to an appropriate destination. Figure 2 shows this

message flow to UAS-B, because that is determined to be the appropriate destination for this message, based on the location of Alice.

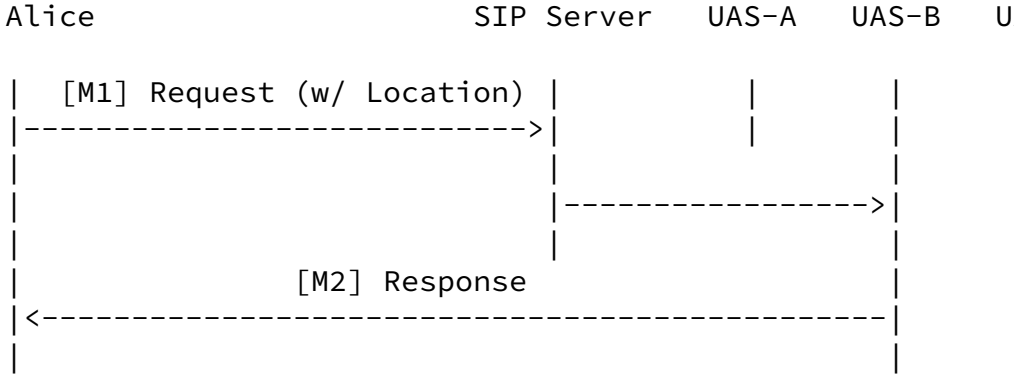

Figure 2. Message Routing based on Location Information

How a SIP Server would route a message based on the location in a SIP message is out of scope for this document. But in Figure 2, Alice's message could go to one of three destinations, with the SIP server choosing destination B based on Alice's location.

A use-case for Figure 2 could be one in which Alice wants a pizza delivered to her location, wherever she is. She calls her favorite pizza store chain's main address, perhaps this is a single, national URI, with her included location determining which specific store this SIP request is routed to. In such a use-case, Alice can use the same URI wherever she is to contact the same store chain she prefers; never needing to look up the specifics of which store is closest in a unfamiliar city.

Another use-case is emergency calling, in which the location of the caller is the key trigger as to which emergency response center receives this SIP request.

Because a person's location is generally considered to be sensitive in nature, certain security measures need to be taken into account 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. 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.

The entities sending and receiving location MUST obey the privacy and security rules in the PIDF-LO, regarding retransmission and retention, to be compliant with this specification.

Self-signed certificates SHOULD NOT be used for protecting PIDF-LO,

as the sender does not have a secure identity of the recipient.

More than one location representation or format MAY be included in the same message body part, but all MUST point at the same position on the earth (altitude not withstanding), as this would confuse the recipient by pointing at more than one position within the same message body part. There MAY be a case in which part or parts of one location format and part or parts of another format exist in the same message body part. These complementary pieces of information MUST point at the same position on the earth, yet are incomplete within their own format. For example, there maybe be a latitude and longitude in coordinate format and a civic altitude value to

complete a 3-dimensional position of a thing (i.e. which floor of a building the UA is on in a building at a particular lat/long coordinates pair).

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 (altitude not withstanding). If the message length exceeds the maximum message length of a single packet (1300 bytes), TCP MUST to be used for proper message fragmentation and reassembly.

Several push-based SIP Request Methods are capable (and applicable) of carrying location, including:

INVITE,
REGISTER,
UPDATE, and
MESSAGE,

While the authors do not yet see a reason to have location conveyed in the ACK, PRACK, BYE, REFER and CANCEL Methods, we do not see a reason to prevent carrying a PIDF-LO within these Method Requests as long as the SIP message meets the requirements stated within this document. Discussing Location in the PUBLISH Request Method will be for another document.

SIP Methods such as SUBSCRIBE and NOTIFY are considered a pull-based location retrieval mechanism, and are therefore not part of this document.

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

4.1 A New Option Tag and SIP Header

This document creates and IANA registers one new option tag:

"location". 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 location option tag is included in a Supported header of the SIP message.

This option tag SHOULD NOT be used in the Proxy-Require header.

This document also creates and IANA registers a new SIP header: Location. The Location header, if present, will have one of two header values defined by this document:

o a Location-by-reference URI

o a Content-ID indicating where location is within the message body

A location-by-reference URI is a pointer to a record on a remote node containing the PIDF-LO of a UA.

If the PIDF-LO of a UA is contained in a SIP message, a Location header will be present in the message with a content-ID (cid-url) [RFC2392] indicating which message body part contains location for this UA. This is to aid a node in not having to parse the whole message body or body parts looking for this body type.

The purpose of the Location option-tag is to indicate support for this document in the Require, Supported and Unsupported headers. It gives a UAS the proper means to indicate it does not support the concept of location in an Unsupported header in a response message that might otherwise not be clear that the lack of support for location is the problem with the request message.

The presence of the Location option tag in a Supported header without a Location 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.

The new "Location" header has the following BNF syntax:

```
Location           =  "Location" HCOLON (locationURI *(COMMA
                       locationURI))
locationURI        =  absoluteURI / cidURI
cidURI             =  "cid:" content-id

content-id         =  addr-spec ; URL encoding of RFC3261 addr-spec
```

The content-ID (cid:) is defined in [RFC2392] to locate message body parts. This MUST be present if location is by-value in a message.

It is envisioned that HTTP, through the http_URL in [RFC216], and

HTTPS [RFC2818] MAY be used to dereference a location-by-reference PIDF-LO.

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

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

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

The Location header MAY be added to, or read if present in, a request message listed above. A proxy MAY add the Location header in transit if one is not present. [RFC3261] states message bodies cannot be added by proxies. A proxy MAY read the location header in transit if present, and MAY use the contents of the location header to make message routing decisions.

It is RECOMMENDED that only one Location header be in the same message, but this is not mandatory. That said, there MUST NOT be more than one cid-url pointing to the same location message body (part) in a SIP message, regardless of how many Location headers there are in that message.

As of the writing of this document, there is no means in a PIDF-LO to indicate which element generated that PIDF-LO. There is a means of indicating what the subject of the location information is within a PIDF-LO. Meaning, if more than one location, by-value and/or by-reference is included in a message, the recipient, whether intermediary or destination, will not know which location entry was inserted by which element. This can lead to confusion in some cases. Therefore, it is RECOMMENDED that there be a single location representation referring to the same target/subject in a SIP message. This PIDF-LO generation indication may be fixed in the future, resolving this limitation, but that is not part of the scope of this document.

Here is an example INVITE request message that includes the proper Location and Supported headers:

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
Location: cid:alice123@atlanta.example.com
Supported: location
```



```
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/pidf+xml
Content-ID: alice123@atlanta.example.com

...PIDF-LO here

--boundary1--
```

The Location header from the above INVITE:

```
Location: cid:alice123@atlanta.example.com
```

indicates the Content-ID location [RFC2392] within the multipart message body of were location information is.

If the Location header were this instead:

```
Location: <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 fetch (dereference) the PIDF-LO from the server

URI.

4.2 424 (Bad Location Information) Response Code

In the case that 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 this is the problem with the request message. This document creates the new error code:

424 (Bad Location Information)

The 424 (Bad Location Information) response code is a rejection of the location contents, whether by-value or by-reference of the original SIP Request. The server function of the recipient (UAS or intermediary) has deemed this location by-reference or location by-

value to be bad. No further action by the UAC is required. 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.

This new error code will be IANA registered in Section 9.

4.3 Example PIDF-LO in Geo Format

This subsection will show a sample of what just the PIDF-LO can look like, as defined in [RFC4119]. Having this here will first offer a look at a location by-value message body, and secondly, give readers an appreciation for how large a location message body is. This section shows a coordinate position based PIDF-LO. Section 4.4 shows this same position in a civic address format. Full example message flows will be left for another document.

Whether this PIDF-LO message body is S/MIME encrypted in the SIP message or not, the PIDF-LO stays exactly the same. There is no change to its format, text or characteristics. Whether TLS or IPSec is used to encrypt this overall SIP message or not, the PIDF-LO stays exactly the same. There is no change to its format, text or characteristics. The examples in section 4.3 (Geo format) taken from [RFC3825] and 4.4 (Civic format) taken from [ID-CIVIC] are for

the exact same position on the Earth. The differences between the two formats is within the <gp:location-info> are of the examples. Other than this portion, of each PIDF-LO, the rest the same for both location formats.

```
<?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>2006-03-20T14:00:00Z</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>2006-03-24T18:00:00Z</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>
```

4.4 Example PIDF-LO in Civic Format

This subsection will show a sample of what just the PIDF-LO can look like, as defined in [RFC4119]. Having this here will first offer a look at a location by-value message body, and secondly, give readers an appreciation for how large a location message body. This section shows a civic address based PIDF-LO. Section 4.3 shows this same

position in a coordinate format. Full example message flows will be left for another document.

Whether this PIDF-LO message body is S/MIME encrypted in the SIP message or not, the PIDF-LO stays exactly the same. There is no change to its format, text or characteristics. Whether TLS or IPSec is used to encrypt this overall SIP message or not, the PIDF-LO stays exactly the same. There is no change to its format, text or characteristics. The examples in section 4.3 (Geo format) taken from [RFC3825] and 4.4 (Civic format) taken from [ID-CIVIC] are for the exact same position on the Earth. The differences between the two formats is within the <gp:location-info> are of the examples. Other than this portion, of each PIDF-LO, the rest the same for both location formats.

```
<?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>2006-03-20T14:00:00Z</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:LMK>Polk Place</cl:LMK>
```



```
             <cl:FLR>1</cl:FLR>
           <cl:civilAddress>
         </gp:location-info>
         <gp:usage-rules>
           <gp:retransmission-allowed>no</gp:retransmission-allowed>
           <gp:retention-expiry>2006-03-24T18:00:00Z</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>
```

5. SIP Element Behavior When Conveying Location

This specification includes requirements for the conveyance of location information in the INVITE, REGISTER, UPDATE, and MESSAGE request methods. The mechanisms within this specification could presumably be used in other SIP requests types. However, since there currently are no agreed upon requirement(s) for conveying location in other request types, this specification only describes location conveyance in the four request methods mentioned here.

The message flows in this document will be example messages containing only the key headers to convey the point being made that do not include all the requisite SIP headers. All well formed SIP message flows are to be in a separate document for brevity here.

5.1 Location Conveyance Using the INVITE Method

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

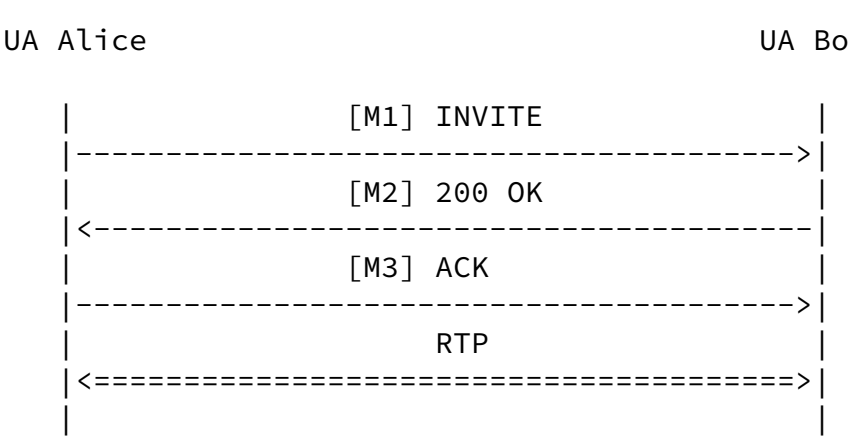

Figure 3. Location Conveyance in INVITE Requests

User agent Alice invites user agent Bob to a session [M1 of Figure

1].

```
INVITE sips:bob@biloxi.example.com SIP/2.0
To: Bob <sips:bob@biloxi.example.com>
From: Alice <sips:alice@atlanta.example.com>;tag=1928301774
Supported: Location
Location: cid:alice123@atlanta.example.com
```

If the message were S/MIME encrypted, this would be the Content-type header:

```
Content-Type: application/pkcs7-mime;
   smime-type=enveloped-data; name=smime.p7m
```

If this INVITE were not S/MIME encrypted, this would be the Content-Type header:

```
Content-Type: multipart/mixed; boundary=boundary1
```

The obvious reason this for a multipart/mixed Content-Type is that this is an INVITE message and there is an SDP message body part included. This is not mandatory, but highly likely. The cid-url in the Location header points a parsing entity that can view the message body to where the PIDF-LO is in the message.

Within the non-S/MIME message body is this:

```
--boundary1

Content-Type: application/sdp

v=0
...

--boundary1

Content-type: application/pidf+xml

PIDF-LO

--boundary1--
```

In the INVITE, Alice's UAC included the Supported header with the location option tag, and the Location header with the cid:url pointing at the by-value PIDF-LO. These two headers MAY be hidden in the S/MIME encrypted message body next to the topmost Content-Type header to hide the fact that this message is carrying location in transit. Bob's UAS, the destination UA of Alice's message, will read these headers when deciphering the overall message body.

- If Bob's UA wants to join the call, his UA responses with a 200 OK

[M2]. Bob can include his location in the 200 OK response, but this shouldn't be expected to due to user timing.

A 424 (Bad Location Information) Response is the proper response if Bob's UA understands this SIP extension (location), but somehow determines the supplied location information is bad.

[Alternative M2(1) of Figure 3]
SIP/2.0 424 Bad Location Information
To: Bob <sips:bob@biloxi.example.com>
From: Alice <sips:alice@atlanta.example.com>;tag=1928301774

The 424 is expected to be more commonly sent by SIP intermediaries along the path between Alice and Bob, than from Bob's UA.

- If Bob's UA accepts with a 200 OK message, Alice's UA replies with an ACK and the session is set up.

- If Bob's UA does not accept the INVITE for reasons other than location included, a 488 (Not Acceptable Here) may be the response.

Figure 3 does not include any Proxies because in it assumed they would not affect the session set-up with respect to whether or not Alice's location is in a message body part, and Proxies do not react to S/MIME encrypted bodies, making their inclusion more or less moot and asking for more complex message flows than necessary here.

If Alice included a Require header such as this:

Require: Location

and Bob did not understand this SIP extension, Bob's appropriate response would be a 420 (Bad Extension) with an Unsupported header containing the Location option tag. This is shown below as an alternative (2) to M2 in Figure 3.

[Alternative M2(2) of Figure 3]
SIP/2.0 420 Bad Extension
To: Bob <sips:bob@biloxi.example.com>
From: Alice <sips:alice@atlanta.example.com>;tag=1928301774

Unsupported: location

5.2 Location Conveyance Using the MESSAGE Method

There are no additional rules regarding conveying location in a MESSAGE request verses an INVITE request.

5.3 Location Conveyance Using the UPDATE Method

The UPDATE Method [RFC3311] is to be used any time location information is to be updated between UAs setting up a dialog or after the dialog has been established, no matter how long that dialog has been operational. reINVITE is inappropriate here, and the MESSAGE Method is for non-dialog location conveyance between UAs only. The same security properties used in the INVITE MUST be applied in the UPDATE message.

There are 3 conditions UPDATE is used to convey location between UAs:

1) During dialog establishment, but before the final 200 OK

2) After dialog establishment, but no prior location information has been convey, and

3) After dialog establishment, when a UA has determined it has moved (not specified here)

There are no additional rules regarding conveying location in a UPDATE request verses an INVITE request.

5.4 Location Conveyance Using the REGISTER Method

Alice's user agent MAY choose to communicate its location during registration, the REGISTER Method is used here. This MAY be done to inform the Registrar server where this UA is to provide it a customized response based on the particulars of UAs in that jurisdiction. To indicate to a Registrar Server a UAC supports this

SIP extension, but does not include location in the message, including a Supported header with a location option tag does this. Either transaction SHOULD an appropriate confidentiality mechanism.

6. Special Considerations for Emergency Calls

Emergency calling, such as 911, 112 and 999 calling today, necessitates a UAC to understand the type of call it is about to initiate with an INVITE message to a PSAP. First of all, the purpose of calling for emergency help is to get someone to respond to the UAC's location, therefore, location MUST be included in the INVITE, if known by the UAC. If the UAC understands this, but does not know its location at this time, it MUST include the location option tag in the Supported header, and MUST NOT include the Location header, as it would not have anything to put as a header value.

The emergency services community strongly prefers that message routing occur in the network with the freshest available Public

Safety Answering Point (PSAP) information. Message routing, in this context, means choosing which SIP(S)-URI to place in the Request-URI field of the status line.

If a UAC knows it is generating an emergency request towards a PSAP, there MAY be unique message handling characteristics that diminish the level of confidentiality of the location information within the SIP message(s). This is because emergency call routing requires proxies to know the location of the message originating UAC in order to make a decision on where to route the message. This is because emergency calls are directed to the PSAP local to the caller's location. A proxy performing this function requires that proxy to learn the location of the UAC during message processing.

How a message is routed based on the location of the UAC, and if and by how much the level of confidentiality of location information is diminished when calling for emergency help are both out of scope of this document.

Hop-by-hop confidentiality mechanisms, as defined in [RFC3261] MUST be initially attempted by a UAC that includes location. Local configuration MAY allow a subsequent retry, after a security related failure, to be without hop-by-hop confidentiality. SIP elements

MUST obey the rules set forth in [RFC3261] regarding maintaining hop-by-hop confidentiality when a message using a SIPS-URI. If a UAC retries an emergency request as the result of a 424 (Bad Location) response, that new request MUST NOT include message body encryption. Further details of emergency request messages are left to future work to define.

While many jurisdictions force a user to reveal their location during an emergency call set-up, there is 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. Meeting RFC3693 Requirements

Section 7.2 of [RFC3693] details the requirements of a "using protocol". They are:

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

This document requires, in Section 3, that SIP entities sending or receiving location MUST obey such instructions.

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

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

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

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

single message, which may be fragmented via TCP, but is still not a streaming delivery.

8. Security Considerations

Conveyance of physical location of a UAC is problematic for many reasons. This document calls for that conveyance to normally be accomplished through secure message body means (like S/MIME or TLS). In cases where a session set-up is routed based on the location of the UAC initiating the session or SIP MESSAGE, securing the location with an end-to-end mechanism such as S/MIME is problematic, due to the probability of a proxy from requiring the ability to read that information to route the message appropriately. This means the use of S/MIME may not be possible. This leaves location information of the caller available in each proxy through to the PSAP. This may not be a perfect solution, but may be a pill we need to swallow to enable this functionality.

A bad implementation of SIP location conveyance would have a UAC send location in cleartext, without hop-by-hop confidentiality, or have any SIP element along the path towards the PSAP alter the transport of any message carrying location to be without hop-by-hop confidentiality between elements. The latter would be in clear violation of RFC3261 rules surrounding the use of a SIPS-URI.

9. IANA Considerations

This section defines one new SIP header, one new option tag, and one new 4XX error response code within the sip-parameters section of IANA. [NOTE: RFC XXXX denotes this document].

9.1 IANA Registration for the SIP Location Header

The SIP Location header is created by this document, with its definition and rules in Section 4 of this document.

9.2 IANA Registration for New SIP Option Tag

The SIP option tag "Location" is created by this document, with the definition and rule in Section 4 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 4.2 of this document.

10. Acknowledgements

To Dave Oran for helping to shape this idea. To Jon Peterson and Dean Willis on guidance of the effort. To Henning Schulzrinne, Jonathan Rosenberg, Dick Knight, Mike Hammer, Paul Kyzivat, Jean-Francois Mule, Hannes Tschofenig, Marc Linsner, Jeroen van Bemmel and Keith Drage for constructive feedback.

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

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

[RFC4119] J. Peterson, "draft-ietf-geopriv-pidf-lo-03", Internet Draft, Sept 2004, work in progress

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

[RFC2392] E. Levinson, " Content-ID and Message-ID Uniform Resource Locators", RFC 2393, August 1998

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

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

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

11.2 References - Informative

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

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

Appendix A. Changes from Prior Versions

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

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

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

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