

Network WG
Internet-Draft
Intended status: Proposed Standard
Expires: Aug 25, 2013

James Polk
Cisco Systems
Feb 25, 2013

Dynamic Host Configuration Protocol (DHCP) IPv4 and IPv6
Option for a Location Uniform Resource Identifier (URI)
draft-ietf-geopriv-dhcp-lbyr-uri-option-19

Abstract

This document creates a Dynamic Host Configuration Protocol (DHCP) Option for transmitting a client's geolocation Uniform Resource Identifier (URI). This Location URI can then be dereferenced in a separate transaction by the client or sent to another entity and dereferenced to learn physically where the client is located, but only while valid.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 25, 2013.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. DHCP LocationURI Option Format and Rules	4
2.1. Overall Format of LocationURI Option in IPv4	4
2.2. Overall Format of LocationURI Option in IPv6	5
2.3. Rules for both LocationURI and Valid-For Options	6
3. DHCP Option Operation	7
4. Architectural Assumptions	8
4.1 Harmful URIs and URLs	8
4.2 Valid Location URI Schemes or Types	9
5. IANA Considerations	9
6. Security Considerations	10
7. Acknowledgements	11
8. References	12
8.1. Normative References	12
8.2. Informative References	13
Author's Address	13

1. Introduction

This document creates a Dynamic Host Configuration Protocol (DHCP) Option for transmitting a client's geolocation Uniform Resource Identifier (URI) [RFC3986]. In this scenario, the DHCP client is a Geopriv Target (i.e., the entity whose geolocation is associated with the location URI). The DHCP implementation of the client can then make this location information available to other applications for their usage. This location URI points to a Location Server [RFC5808] which has the geolocation of the client (e.g., previously uploaded into a wiremap database then the client attaches to a known wall-jack, or by means of 802.11 geolocation mechanisms).

Applications within the Target can then choose to dereference this location URI and/or transmit the URI to another entity as a means of conveying where the Target is located. Both Conveying and Dereferencing a location URI is described in [RFC6442]. Session Initiation Protocol (SIP) [RFC3261] is not the only protocol that can dereference a location URI; there is also HTTP-Enabled Location Delivery (HELD) [RFC6753] and HTTP [RFC2616].

A Location Server (LS) stores the Target's location as a presence document, called a Presence Information Data Format - Location Object (PIDF-LO), defined in RFC 4119 [RFC4119]. The Location Server is the entity contacted during the act of dereferencing a Target's location. If the dereferencing entity has permission, defined in [RFC6772], the location of the target will be received. The LS will grant permission to location inquiries based on the rules established by a Rule Holder [RFC3693]. The LS has the ability to challenge any request for a target's location, thereby providing additive security properties before location revelation.

Possessing a location URI has advantages over having a PIDF-LO, especially when a target's location changes. With a location URI, when a target moves, the location URI does not change (at least within the same domain). The location URI can still be given out as the reference to the Target's current location. The opposite is true if the location is conveyed by value in a message. Once the Target moves, the previously given location is no longer valid, and if the Target wants to inform another entity about its location, it has to send the PIDF-LO to the location recipient (again).

A problem exists within existing RFCs that provide location to the UA ([RFC6225] and [RFC4776]). Those DHCP Options for geolocation values require an update of the entire location information (LI) every time a client moves. Not all clients will move frequently, but some will. Refreshing location values every time a client moves does not scale in certain networks/environments, such as IP-based cellular networks, enterprise networks or service provider networks with mobile endpoints. An 802.11 based access network is one example of this. Constantly updating Location Configuration Information (LCI) to endpoints might not scale in mobile (residential or enterprise or municipal) networks in which the client is moving through more than one network attachment point, perhaps as a person walks or drives with their client down a neighborhood street or apartment complex or a shopping center or through a municipality (that has IP connectivity as a service).

If the client was provided a location URI reference to retain and hand out when it wants or needs to convey its location (in a protocol other than DHCP), a location URI that would not change as the client's location changes (within a domain). Scaling issues would be significantly reduced to needing an update of the location URI only when a client changes administrative domains - which is much less often. This delivery of an indirect location has the added benefit of not using up valuable or limited bandwidth to the client with the constant updates. It also relieves the client from having to determine when it has moved far enough to consider asking for a refresh of its location.

In enterprise networks, if a known location is assigned to each individual Ethernet port in the network, a device that attaches to the network, such as a wall-jack (directly associated with a specific Ethernet Switch port) will be associated with a known location via a unique circuit-ID that's used by the Relay Agent Information Option (RAIO) defined in RFC 3046 [RFC3046]. This assumes wall-jacks have an updated wiremap database. RFC 6225 [RFC6225] and RFC 4776 [RFC4776] would return an LCI value of location for either IPv4 or IPv6. This document specifies how a location URI is returned using DHCP. The location URI points to a PIDF-LO contained on an LS. Performing a dereferencing transaction, that Target's PIDF-LO will be returned. If local configuration has the requirement of only assigning unique location URIs to each client at the same attachment point to the network (i.e., same RJ-45

jack or same 802.11 Access Point - except when triangulation is used), then unique location URIs will be given out. They will all have the same location at the record, relieving the backend Sighter or LS from individually maintaining each location independently.

The location URI Option can be useful in IEEE 802.16e connected endpoints or IP cellular endpoints. The location URI Option can be configured on a router, such as a residential home gateway, such that the router receives this Location URI Option as a client with the ability to communicate to downstream endpoints as a server.

How an LS responds to a dereference request can vary, and a policy established by a Ruleholder [RFC3693] for a Location Target as to what type of challenge(s) is to be used, how strong a challenge is used or how precise the location information is given to a Location Recipient (LR). This document does not provide mechanisms for the LS to tell the client about policies or for the client to specify a policy for the LS. While an LS should apply an appropriate access-control policy, clients must assume that the LS will provide location in response to any request (following the possession model [RFC5808]). For further discussion of privacy, see the Security Considerations.

This document IANA-registers the new IPv4 and IPv6 DHCP Options for a location URI and Valid-For.

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. Format of the DHCP LocationURI Option

2.1 Overall Format of LocationURI Option in IPv4

The LocationURI Option format for IPv4 is as follows:

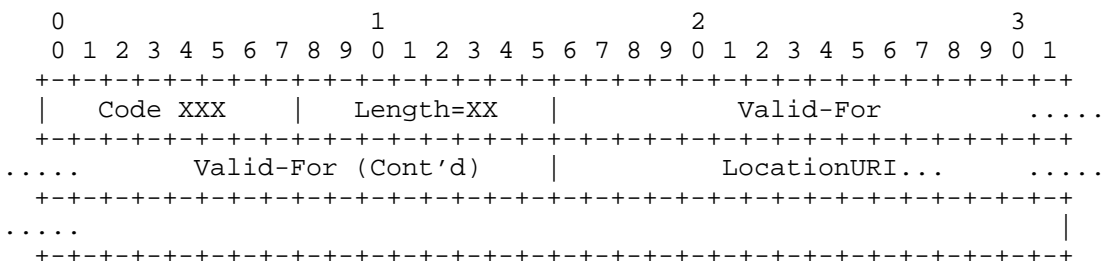


Figure 1. IPv4 Fields for this LocationURI Option

Code XXX: The code for this DHCPv4 option (IANA assigned).

Length=XX: The length of this option, counted in bytes - not counting the Code and Length bytes. This is a variable length Option, therefore the length value will change based on the length of the URI within the Option.

Valid-For: The time, in seconds, the LocationURI is to be considered valid for dereferencing. The Valid-For is always represented as a four-byte unsigned integer.

LocationURI: Location URI - This field, in bytes, is the URI pointing at the location record where the PIDF-LO for the Location Target resides. The LocationURI is always represented in ASCII.

2.2 Overall Format of LocationURI Option in IPv6

The LocationURI Option format for IPv6 is as follows:

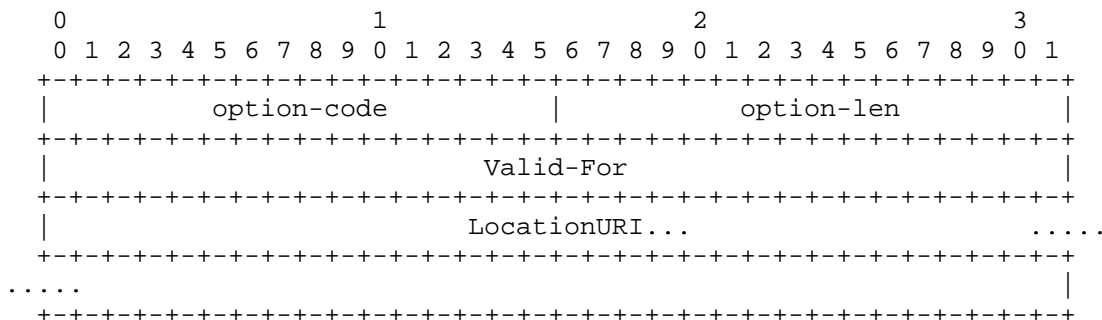


Figure 2. IPv6 fields of this LocationURI Option

option-code: The code for this DHCPv6 option (IANA assigned).

option-len: The length of this option, counted in bytes - not counting the option-code and option-len bytes. This is a variable length Option, therefore the length value will change based on the length of the URI within the Option.

Valid-For: see Section 2.1

LocationURI: see Section 2.1

2.3 Rules for the LocationURI Option

The LocationURI Option has the following rules:

- o Implementation of the Location URI Option is REQUIRED on the DHCP server and client.

- o Clients SHOULD be expected to have to request the Location URI Option from servers. Although local policy can have servers perform an unsolicited push of a Location URI Option to a client.

Applications on a client can use the Location URI (value) until the Valid-For value reaches zero. If there is no Valid-For Option value, then the counter did not ever start (a null value), and applications on a client continue to use the Location URI value until given a new Location URI Option (with or without a Valid-For value) which overwrites any previous Location URI and Valid-For Option values.

- o A Location URI Option with a non-zero Valid-For field MUST NOT transmit the Location URI once the Valid-For field counts down to zero.
- o A received Location URI Option containing all zeros in the Valid-For field means that Location URI has no lifetime, and not "no lifetime left". All zeros in the Valid-For field equates to a null value.
- o Receipt of the Location URI Option containing all zeros in the Valid-For field MUST NOT cause any error in handling the Location URI.
- o When the Valid-For timer reaches zero, the client MUST purge any location URI received via DHCP from its memory.

The choice of the Valid-For value is a policy decision for the operator of the DHCP server. Like location URIs themselves, it can be statically configured on the DHCP server or provisioned dynamically (via an out-of-band exchange with a Location Information Server) as requests for location URIs are received.

- o Clients receiving a Location URI Option start the Valid-For timer upon receipt of the DHCP message containing the Option.
- o Clients MUST NOT trigger an automatic DHCP refresh on expiry of the Valid-For timer; rather, they MUST follow normal DHCP mechanics.

If the Valid-For timer is set to expire before the lease refresh, the client will not have the ability to hand out its location until the lease refresh, inadvertently allowing a gap of coverage. If the Valid-For timer is set to expire after the lease refresh, some wayward application on the client can divulge that location URI after it is no longer valid, meaning the location could be stale or just plain wrong.

- o Servers SHOULD set the Valid-For timer to that of the lease refresh, or bad things can happen.

3. DHCP Option Operation

The [RFC3046] RAI0 can be utilized to provide the appropriate indication to the DHCP Server where this DISCOVER or REQUEST message came from, in order to supply the correct response.

Caution SHOULD always be used involving the creation of large Options, meaning that this Option may need to be in its own INFORM, OPTION or ACK message. DHCP messages are limited in size, and long URIs will require the use of multiple messages and concatenation [RFC3396]. It is, therefore, best to limit the total length of a URI, including any parameters, to 220 bytes.

Location URIs MUST NOT reveal identity information of the user of the device, since DHCP is a cleartext delivery protocol. For example, creating a location URI such as

sips:34LKJH534663J54@example.com

is better than a location URI such as

sips:aliceisatl23mainstatlantageorgiaus@example.com

The username portion of the first example URI provides no direct identity information (in which 34LKJH534663J54 is considered to be a random number in this example).

In the <presence> element of a PIDF-LO document, there is an 'entity' attribute that identifies what entity *this* presence document (including the associated location) refers to. It is up to the PIDF-LO generator, either Location Server or an application in the endpoint, to insert the identity in the 'entity' attribute. This can be seen in [RFC4119]. The considerations for populating the entity attribute value in a PIDF-LO document are independent from the considerations for avoiding exposing identification information in the username part of a location URI.

This Option is used only for communications between a DHCP client and a DHCP server. It can be solicited (requested) by the client, or it can be pushed by the server without a request for it. DHCP Options not understood MUST be ignored [RFC2131]. A DHCP server supporting this Option might or might not have the location of a client. If a server does not have a client's location, but needs to provide this Location URI Option to a client (for whatever reason), an LS is contacted. This server-to-LS transaction is not DHCP, therefore it is out of scope of this document. Note that this server-to-LS transaction could delay the DHCP messaging to the client. If the server fails to have location before it transmits its message to the client, location will not be part of that DHCP message. Any timers involved here are a matter of local configuration.

The dereference of a target's location URI would not involve DHCP, but an application layer protocol, such as SIP or HTTP, therefore dereferencing is out of scope of this document.

In the case of residential gateways being DHCP servers, they usually perform as DHCP clients in a hierarchical fashion up into a service provider's network DHCP server(s), or learn what information to provide via DHCP to residential clients through a protocol, such as PPP. In these cases, the location URI would likely indicate the residence's civic address to all wired or wireless clients within that residence.

4. Architectural Assumptions

The following assumptions are made once the client has obtained a location URI, and not about DHCP operation specifics (in no particular order):

- o Any user control (what [RFC3693] calls a 'Ruleholder') for access to the dereferencing step is assumed to be out of scope of this document. An example authorization policy is in [RFC6772].
- o The authorization security model vs. possession security model discussion can be found in [RFC5606], describing what is expected in each model of operation. It should be assumed that a location URI attained using DHCP will operate under a possession model by default. An authorization model can be instituted as a matter of local policy. An authorization model means possessing the location URI does not give that entity the right to view the PIDF-LO of the target whose location is indicated in a presence document. The dereference transaction will be challenged by the Location Server only in an authorization model. The nature of this challenge is out of scope of this document.
- o This document does not prevent some environments from operating in an authorization model, for example - in less tightly controlled networks. The costs associated with authorization vs. possession models are discussed in Section 3.3.2 of [RFC5606].

4.1 Harmful URIs and URLs

There are, in fact, some types of URIs that are not good to receive, due to security concerns. For example, any URLs that can have scripts, such as "data:" URLs, and some "HTTP:" URLs that go to web pages that have scripts. Therefore,

- o URIs received via this Option SHOULD NOT be automatically sent to a general-browser to connect to a web page, because they could have harmful scripts, unless

- o the browser has been set up to defend against harmful scripts,
- or
- o the browser does not run scripts automatically.
- o This Option MUST NOT contain "data:" URLs [RFC2397], because they could contain harmful scripts.

4.2 Valid Location URI Schemes or Types

URIs carried by this DHCP Option MUST have one of the following URI schemes:

1. sip:
2. sips:
3. pres:
4. http:
5. https:

URIs using the "pres" scheme are dereferenced using the presence event package for SIP [RFC3856], so they will reference a PIDF-LO document when location is available. Responses to requests for URIs with other schemes ("sip", "sips", "http", and "https") MUST have media type 'application/pidf+xml' [RFC4119]. Alternatively, HTTP and HTTPS URIs MAY refer to information with media type 'application/held+xml', in order to support HELD dereferencing [RFC6753]. Clients can indicate which media types they support using the "Accept" header field in SIP [RFC3261] or HTTP [RFC2616].

See RFC 3922 [RFC3922] for using the "pres:" URI with XMPP.

It is RECOMMENDED that implementers follow Section 4.6 of RFC 6442 [RFC6442] as guidance regarding which Location URI schemes to provide in DHCP. That document discusses what a receiving entity does when receiving a URI scheme that is not understood. Awareness to the two URI types there is important for conveying location, if SIP is used to convey a Location URI provided by DHCP.

5. IANA Considerations

5.1 The IPv4 Option number for the Location URI Option

This document IANA registers the DHCP Location URI Option Number in the BOOTP Vendor Extensions and DHCP Options subregistry of the Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) Parameters registry located.

Tag	Name	Data Length	Meaning	Reference
----	-----	-----	-----	-----
XXX	LocationURI	N	GeoLocation URI	[this document]

The authors have no preference at this time on what number IANA chooses.

5.2 The IPv6 Option-Code for the Location URI Option

This document IANA registers the DHCPv6 Option Code in the DHCP Option Codes subregistry of the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) registry.

Value	Description	Reference
----	-----	-----
XX	OPTION_GEOLOCATION_URI	[this document]

The authors have no preference at this time on what number IANA chooses.

5.3 Valid Location URI Schemes

This document creates a new IANA registry (Valid Location URI Schemes) of acceptable location URI schemes (or types) for this DHCP Location URI Option of the Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) Parameters registry.

Initial values are given below; new assignments are to be made following the "IETF Review" policies [RFC5226].

"Valid Location URI Schemes"

Location URI Scheme	Reference
-----	-----
sip:	[this document]
sips:	[this document]
pres:	[this document]
http:	[this document]
https:	[this document]

6. Security Considerations

Where critical decisions might be based on the value of this location URI option, DHCP authentication as defined in "Authentication for DHCP Messages" [RFC3118] and "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)" [RFC3315] SHOULD be used to protect the integrity of the DHCP options.

A real concern with RFC 3118 or RFC 3315 is that neither is widely deployed because each requires pre-shared keys to successfully work (i.e., in the client and in the server). Most implementations do not accommodate this.

DHCP, initially, is a broadcast request (a client looking for a server), and a unicast response (answer from a server) type of protocol. There is no privacy protection for DHCP messages, an eavesdropper who can monitor the link between the DHCP server and requesting client can discover the Location URI.

Once a client has a Location URI, it needs information on how the location server will control access to dereference requests. A client might treat a tightly access-controlled URI differently from one that can be dereferenced by anyone on the Internet (i.e., one following the "possession model"). Since the client does not know what policy will be applied during this validity interval, clients MUST handle location URIs as if they could be dereferenced by anybody until they expire. For example, such open location URIs should only be transmitted in encrypted channels. Nonetheless, location servers SHOULD apply appropriate access control policies, for example by limiting the number of queries that any given client can make, or limiting access to users within an enterprise.

Extensions to this option, such as [ID-POLICY-URI] can provide mechanisms for accessing and provisioning policy. Giving users access to policy information will allow them to make more informed decisions about how to use their location URIs. Allowing users to provide policy information to the LS will enable them to tailor access control policies to their needs (within the bounds of policy that the LS will accept).

As to the concerns about the location URI itself, as stated in the document (see Section 3), it MUST NOT have any user identifying information in the URI user-part/string itself. The location URI also needs to be hard to guess that it belongs to a specific user.

In some cases a DHCP server may be implemented across an uncontrolled network. In those cases, it would be appropriate for a network administrator to perform a threat analysis (see RFC 3552) and take precautions as needed.

Link-layer confidentiality and integrity protection may also be employed to reduce the risk of location disclosure and tampering.

7. Acknowledgements

Thanks to James Winterbottom, Marc Linsner, Roger Marshall and Robert Sparks for their useful comments. And to Lisa Dusseault for her concerns about the types of URIs that can cause harm. To

Richard Barnes for inspiring a more robust Security Considerations section, and for offering the text to incorporate HTTP URIs. To Hannes Tschofenig and Ted Hardie for riding me to comply with their concerns, including a good scrubbing of the nearly final doc.

8. References

8.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.
- [RFC3046] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, January 2001.
- [RFC3118] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 2001.
- [RFC3315] R. Droms, Ed., J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003
- [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.
- [RFC3396] T. Lemon, S. Cheshire, "Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)", RFC 3396, November 2002
- [RFC3856] J. Rosenberg, "A Presence Event Package for the Session Initiation Protocol (SIP)", RFC 3856, August 2004
- [RFC3922] P. Saint-Andre, " Mapping the Extensible Messaging and Presence Protocol (XMPP) to Common Presence and Instant Messaging (CPIM)", RFC 3922, October 2004
- [RFC3986] T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", RFC 3986, January 2005
- [RFC4119] J. Peterson, "A Presence-based GEOPRIV Location Object Format", RFC 4119, December 2005
- [RFC5226] T. Narten, H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 5226, May 2008
- [RFC6442] Polk, J., Rosen, B., and J. Peterson, "Location Conveyance

for the Session Initiation Protocol", RFC 6442, December 2011.

- [RFC6753] J. Winterbottom, H. Tschofenig, H. Schulzrinne, M. Thomson, M. Dawson, "A Location Dereferencing Protocol Using HELD", October 2012

8.2. Informative References

- [RFC2397] L. Masinter, "The "data" URL scheme", RFC 2397, 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
- [RFC3693] J. Cuellar, J. Morris, D. Mulligan, J. Peterson. J. Polk, "Geopriv Requirements", RFC 3693, February 2004
- [RFC6225] Polk, J., Linsner, M., Thomson, M., and B. Aboba, "Dynamic Host Configuration Protocol Options for Coordinate-Based Location Configuration Information", RFC 6225, July 2011.
- [RFC4776] H. Schulzrinne, "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information ", RFC 4776, November 2006
- [RFC5606] J. Peterson, T. Hardie, J. Morris, "Implications of 'retransmission-allowed' for SIP Location Conveyance", August 2009
- [RFC5808] R. Marshall, "Requirements for a Location-by-Reference Mechanism", RFC 5808, May 2010
- [RFC6772] H. Schulzrinne, H. Tschofenig, J. Morris, J. Cuellar, J. Polk, "Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information", January 2013
- [ID-POLICY-URI] R. Barnes, M. Thomson, J. Winterbottom, "Location Configuration Extensions for Policy Management", "work in progress", November 2011

Authors' Address

James Polk
3913 Treemont Circle
Colleyville, Texas 76034
USA

Email: jmpolk@cisco.com

GEOPRIV
Internet-Draft
Intended status: Standards Track
Expires: September 28, 2010

R. Mahy
Individual
B. Rosen
NeuStar
H. Tschofenig
Nokia Siemens Networks
March 27, 2010

Filtering Location Notifications in the Session Initiation Protocol
(SIP)
draft-ietf-geopriv-loc-filters-11.txt

Abstract

This document describes filters that limit asynchronous location notifications to compelling events, designed as an extension to RFC 4661, an XML-based format for event notification filtering, and based on RFC 3856, the SIP presence event package. The resulting location information is conveyed in existing location formats wrapped in the Presence Information Data Format Location Object (PIDF-LO).

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on September 28, 2010.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the

document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the BSD License.

Table of Contents

1. Introduction	3
2. Terminology	5
3. Filter Definitions	6
3.1. Movement	6
3.2. Speed Changes	6
3.3. Element Value Changes	7
3.4. Entering or Exiting a Region	10
3.5. Location Type	12
3.6. Rate Control	14
4. XML Schema	16
5. Security Considerations	18
6. IANA Considerations	19
6.1. URN Sub-Namespace Registration for urn:ietf:params:xml:ns:location-filter	19
6.2. Schema Registration For location-filter	19
7. Contributors	21
8. Acknowledgments	22
9. References	23
9.1. Normative References	23
9.2. Informational References	24
Authors' Addresses	25

1. Introduction

Conveying location information encapsulated with a Presence Information Data Format Location Object (PIDF-LO) [RFC4119] document within SIP is described in [I-D.ietf-sipcore-location-conveyance]. An alternative signaling approach to location conveyance, which uses asynchronous communication, is available with the SIP event notification mechanisms (see RFC 3265 [RFC3265]). This document focuses on the event notification paradigm. Event notifications are technically more complex since location may be measured as a continuous gradient and unlike notifications using discrete-valued quantities, it is difficult to know when a change in location is large enough to warrant a notification. Event notifications [RFC3265] can be used with filters (see RFC 4661 [RFC4661]) that allow the number of notifications to be reduced. The mechanism described in this document defines an extension to RFC 4661 [RFC4661], which limits location notification to events that are of relevance to the subscriber. These filters persist until they are changed with a replacement filter or when the subscription itself is terminated.

The frequency of notifications necessary for various geographic location applications varies dramatically. The subscriber should be able to get asynchronous notifications with appropriate frequency and granularity, without being flooded with a large number of notifications that are not important to the application.

This document defines a new event filters and describes others using existing mechanisms that may be relevant to a subscriber in the context of location filtering. Based on the functionality defined in this document notifications can be provided in the following cases:

1. the Device moves more than a specified distance since the last notification (see Section 3.1).
2. the Device exceeds a specified speed (see Section 3.2).
3. the Device enters or exits a region, described by a circle or a polygon (see Section 3.4).
4. one or more of the values of the specified address labels have changed for the location of the Device (see Section 3.3). For example, the value of the <Al> civic address element has changed from 'California' to 'Nevada'.
5. the type of location information being requested (see Section 3.5).

6. a certain amount of time passes (see Section 3.6).

This document builds on the presence event package [RFC3856], i. e. an existing event package for communicating location information inside the PIDF-LO.

2. Terminology

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 RFC 2119 [RFC2119].

This document reuses terminology from [I-D.ietf-geopriv-arch].

3. Filter Definitions

This specification builds on top of a number of other specifications, as noted in Section 1. In order to reduce the number of options (and thereby decrease the chance of interoperability problems), the functionality of [RFC4661] listed in the sub-sections below MUST be implemented, namely the <ns-bindings> (see Section 3.3 of [RFC4661]), the <filter> (Section 3.4 of [RFC4661]), and the <trigger> (Section 3.6 of [RFC4661] excluding the functionality of the <added> and <removed> element).

3.1. Movement

The <moved> element MUST contain a value in meters indicates the minimum distance that the resource must have moved from the location of the resource since the last notification was sent in order to trigger this event. The distance MUST be measured in meters absolutely from the point of last notification, and must include vertical movement. The <moved> element MUST NOT appear more than once as a child element of the <filter> element.

```
<?xml version="1.0" encoding="UTF-8"?>
<filter-set
  xmlns="urn:ietf:params:xml:ns:simple-filter"
  xmlns:lf="urn:ietf:params:xml:ns:location-filter">
  <filter id="123" uri="sip:presentity@example.com">
    <trigger>
      <lf:moved>300</lf:moved>
    </trigger>
  </filter>
</filter-set>
```

Figure 1: Movement Filter Example

3.2. Speed Changes

Speed changes can be filtered by combining functionality from RFC 4661 with the PIDF-LO extensions for spatial orientation, speed, heading, and acceleration defined in [I-D.singh-geopriv-pidf-lo-dynamic]. The value of the <speed> element from [I-D.singh-geopriv-pidf-lo-dynamic] MUST be defined in meters per second. Note that the condition could be met by a change in any axis including altitude.

Figure 2 shows an example for a trigger that fires when the speed of the Target changes by 3 meters per second.

```
<?xml version="1.0" encoding="UTF-8"?>
<filter-set xmlns="urn:ietf:params:xml:ns:simple-filter">
  <ns-bindings>
    <ns-binding prefix="dyn"
      urn="urn:ietf:params:xml:schema:pidf:dynamic"/>
  </ns-bindings>
  <filter id="123" uri="sip:presentity@example.com">
    <trigger>
      <changed by="3">
        //dyn:speed
      </changed>
    </trigger>
  </filter>
</filter-set>
```

Figure 2: Speed Change Example

An implementation MUST support `<ns-bindings>` to replace the namespace prefix. The XPath expression MUST start with a `'//'` followed by a single element. No other form of XPath expression is supported. The `<changed>` element comes with a few attributes but only the `'by'` attribute MUST be implemented by this specification.

3.3. Element Value Changes

Changes in values, for example related to civic location information, is provided by the base functionality offered with RFC 4661 utilizing the `<changed>` element.

Figure 3 shows an example where a notification is sent when the civic address tokens A1, A2, A3, and PC change (all four must change in order to let the `<trigger>` element evaluate to TRUE).

(A change in ALL four tokens triggers an event.)

```
<?xml version="1.0" encoding="UTF-8"?>
<filter-set xmlns="urn:ietf:params:xml:ns:simple-filter">
  <ns-bindings>
    <ns-binding prefix="ca"
      urn="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"/>
  </ns-bindings>
  <filter id="123" uri="sip:presentity@example.com">
    <trigger>
      <changed>//ca:country</changed>
      <changed>//ca:A1</changed>
      <changed>//ca:A2</changed>
      <changed>//ca:A3</changed>
      <changed>//ca:PC</changed>
    </trigger>
  </filter>
</filter-set>
```

Figure 3: Element Value Change Example

Note: The civic address tokens country, A1, A2, ..., A6 are hierarchical. It is likely that a change in one civic address token therefore leads to changes of tokens lower in the hierarchy, e.g., a change in A3 ('city or town') may cause a change in A4, A5, and A6.

In times where it is desirable to know if any one element of a list of CAtypes changes, then they have to be put into separate <changes> filters to ensure you are notified when any of the element values change. Figure 4 shows such an example that illustrates the difference.

(A change in value of ANY of the four tokens triggers an event.)

```
<?xml version="1.0" encoding="UTF-8"?>
<filter-set xmlns="urn:ietf:params:xml:ns:simple-filter">
  <ns-bindings>
    <ns-binding prefix="ca"
      urn="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"/>
  </ns-bindings>
  <filter id="123" uri="sip:presentity@example.com">
    <trigger>
      <changed>//ca:country</changed>
    </trigger>
    <trigger>
      <changed>//ca:A1</changed>
    </trigger>
    <trigger>
      <changed>//ca:A2</changed>
    </trigger>
    <trigger>
      <changed>//ca:A3</changed>
    </trigger>
    <trigger>
      <changed>//ca:PC</changed>
    </trigger>
  </filter>
</filter-set>
```

Figure 4: Element Value Change Example

The following example illustrates a filter that triggers when the Target's location changes from 'FR' (France) to some other country.

```
<?xml version="1.0" encoding="UTF-8"?>
<filter-set xmlns="urn:ietf:params:xml:ns:simple-filter">
  <ns-bindings>
    <ns-binding prefix="ca"
      urn="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"/>
  </ns-bindings>
  <filter id="123" uri="sip:presentity@example.com">
    <trigger>
      <changed from="FR">//ca:country</changed>
    </trigger>
  </filter>
</filter-set>
```

Figure 5: Element Value Change Example (Country Change)

An implementation MUST support <ns-bindings> to replace the namespace prefix. The XPath expression MUST start with a '/' followed by a single element. No other form of XPath expression is supported. No other variant is supported. The <changed> element comes with a few attributes and the 'by', 'to' and 'from' attribute MUST be implemented to support this specification.

3.4. Entering or Exiting a Region

The <enterOrExit> condition is satisfied when the Target enters or exits a named 2-dimensional region described by a polygon (as defined in Section 5.2.2 of [RFC5491]), or a circle (as defined in Section 5.2.3 of [RFC5491]). The <enterOrExit> element MUST contain either a polygon or a circle as a child element. The <enterOrExit> element MUST NOT have more than one polygon and/or circle.

If the Target was previously outside the region, the notifier sends a notification when the Target's location is within the region with at least 50% confidence. Similarly, when a Target starts within the region, a notification is sent when the Target's location moves outside the region with at least 50% confidence.

Note that having 50% confidence that the Target is inside the area does not correspond to 50% outside. The confidence that the location is within the region, plus the confidence that the location is outside the region is limited to the confidence of the location. The total confidence depends on the confidence in the location, which is always less than 100% (95% is recommended in [RFC5491]). The benefit of this is that notifications are naturally limited: small movements (relative to the uncertainty of the location) at the borders of the region do not trigger notifications.

Figure 6 shows filter examples whereby a notification is sent when the Target enters or exits an area described by a circle and Figure 7 describes an area using a polygon.

```
<?xml version="1.0" encoding="UTF-8"?>
<filter-set
  xmlns="urn:ietf:params:xml:ns:simple-filter"
  xmlns:lf="urn:ietf:params:xml:ns:location-filter"
  xmlns:gml="http://www.opengis.net/gml"
  xmlns:gs="http://www.opengis.net/pidflo/1.0">

  <filter id="123" uri="sip:presentity@example.com">
    <trigger>
      <lf:enterOrExit>
        <gs:Circle
          srsName="urn:ogc:def:crs:EPSG::4326">
            <gml:pos>42.5463 -73.2512</gml:pos>
            <gs:radius
              uom="urn:ogc:def:uom:EPSG::9001">
                850.24
            </gs:radius>
          </gs:Circle>
        </lf:enterOrExit>
      </trigger>
    </filter>
  </filter-set>
```

Figure 6: <enterOrExit> Circle Filter Example


```

<?xml version="1.0" encoding="UTF-8"?>
<filter-set
  xmlns="urn:ietf:params:xml:ns:simple-filter"
  xmlns:lf="urn:ietf:params:xml:ns:location-filter"
  xmlns:gml="http://www.opengis.net/gml">

  <filter id="123" uri="sip:presentity@example.com">
    <trigger>
      <lf:enterOrExit>
        <gml:Polygon srsName="urn:ogc:def:crs:EPSG::4326">
          <gml:exterior>
            <gml:LinearRing>
              <gml:pos>43.311 -73.422</gml:pos>
              <!--A-->
              <gml:pos>43.111 -73.322</gml:pos>
              <!--F-->
              <gml:pos>43.111 -73.222</gml:pos>
              <!--E-->
              <gml:pos>43.311 -73.122</gml:pos>
              <!--D-->
              <gml:pos>43.411 -73.222</gml:pos>
              <!--C-->
              <gml:pos>43.411 -73.322</gml:pos>
              <!--B-->
              <gml:pos>43.311 -73.422</gml:pos>
              <!--A-->
            </gml:LinearRing>
          </gml:exterior>
        </gml:Polygon>
      </lf:enterOrExit>
    </trigger>
  </filter>
</filter-set>

```

Figure 7: <enterOrExit> Polygon Filter Example

3.5. Location Type

The <locationType> element MAY be included as a child element of the <what> element and it contains a list of location information types that are requested by the subscriber. The following list describes the possible values:

any: The Notifier SHOULD attempt to provide LI in all forms available to it.

geodetic: The Notifier SHOULD return a location by value in the form of a geodetic location.

civic: The Notifier SHOULD return a location by value in the form of a civic address.

The Notifier SHOULD return the requested location type or types. The location types the Notifier returns also depends on the setting of the optional 'exact' attribute. If the 'exact' attribute is set to "true" then the Notifier MUST return either the requested location type or no location information. The 'exact' attribute does not apply (is ignored) for a request for a location type of "any".

In the case of a request for specific locationType(s) and the 'exact' attribute is "false", the Notifier MAY provide additional location types, or it MAY provide alternative types if the request cannot be satisfied for a requested location type.

If the <locationType> element is absent, a value of "any" MUST be assumed as the default.

The Notifier SHOULD provide location in the response in the same order in which they were included in the "locationType" element in the request. Indeed, the primary advantage of including specific location types in a request when the 'exact' attribute is set to "false" is to ensure that one receives the available locations in a specific order. For example, a subscription for "civic" (with the 'exact' attribute set to "false") could yield any of the following location types in the response:

- o civic
- o civic, geodetic
- o geodetic (only if civic is not available)

The default value of "false" for the 'exact' attribute allows the Notifier the option of returning something beyond what is specified, such as a set of location URIs when only a civic location was requested.

An example is shown in Figure 8 that utilizes the <locationType> element with the 'exact' and the 'responseTime' attribute.

```
<?xml version="1.0" encoding="UTF-8"?>
<filter-set
  xmlns="urn:ietf:params:xml:ns:simple-filter"
  xmlns:lf="urn:ietf:params:xml:ns:location-filter">
  <filter id="123" uri="sip:presentity@example.com">
    <what>
      <lf:locationType exact="true">
        geodetic
      </lf:locationType>
    </what>
  </filter>
</filter-set>
```

Figure 8: <locationType> Filter Example

3.6. Rate Control

[I-D.ietf-sipcore-event-rate-control] extends the SIP events framework by defining the following three "Event" header field parameters that allow a subscriber to set a minimum, a maximum and an average rate of event notifications generated by the notifier. This allows a subscriber to have overall control over the stream of notifications, for example to avoid being flooded. Two of the parameters, namely "min-interval" (which specifies a minimum notification time period between two notifications, in seconds) and "max-interval" (which specifies a maximum notification time period between two notifications, in seconds.) are used by this document. Only the implementation of these two attributes is required from the attributes defined in [I-D.ietf-sipcore-event-rate-control]. Whenever the time since the most recent notification exceeds the value in the "max-interval" parameter, the current state would be sent in its entirety, just like after a subscription refresh.

A notifier is required to send a NOTIFY request immediately after creation of a subscription. If state is not available at that time, then the NOTIFY request may be sent with no content. A separate NOTIFY containing location is subsequently generated some time between the time included in 'min-interval' and the time in 'max-interval'. An important use case for location based applications focuses on the behavior of the initial NOTIFY message(s) and the information it returns, for example in case of emergency call routing. When an initial NOTIFY is transmitted it might not include complete state.

Subscriber	Notifier
---SUBSCRIBE(1)--->	Create subscription (w/small value
<-----200-----	for min-interval and max-interval)
<-----NOTIFY(2)----	Return initial notify with no state
-----200----->	
<-----NOTIFY(3)----	Return full state (between min-interval
-----200----->	and max-interval)
---SUBSCRIBE(4)--->	Update subscription (to update
<-----200-----	min-interval and max-interval)

Figure 9: SUBSCRIBE/NOTIFY with Rate Control

Figure 9 shows a SUBSCRIBE/NOTIFY exchange. The initial SUBSCRIBE message (1) has filters attached and contains a 'max-interval' rate control parameter. In certain situations it is important to obtain some amount of location information within a relatively short and pre-defined period of time even if the obtained location information contains a high amount of uncertainty and location information with less uncertainty at a later point in time. An example is emergency call routing where a emergency services routing proxy may need to obtain location information suitable for routing rather quickly and subsequently a Public Safety Answering Point requests location information for dispatch.

To obtain location information in a timely fashion using the SUBSCRIBE/NOTIFY mechanism, it is RECOMMENDED that the initial SUBSCRIBE contains a 'max-interval' rate control parameter (with a small value) that is in a later message updated to a more sensible value. This provides equivalent functionality to the 'responseTime' attribute in Section 6.1 of

[I-D.ietf-geopriv-http-location-delivery]. The 'max-interval' for this first request is therefore much lower than thereafter. Updating the 'max-interval' for the subscription can be performed in the 200 response (see message 3) to the NOTIFY that contains state. Depending on the value in the 'max-interval' parameter the Notifier may create a NOTIFY message (see message 2) immediately in response to the SUBSCRIBE that might be empty in case no location information is available at this point in time. The desired location information may then arrive in the subsequent NOTIFY message (see message 4).

4. XML Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:ietf:params:xml:ns:location-filter"
  xmlns:filter="urn:ietf:params:xml:ns:location-filter"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:gml="http://www.opengis.net/gml">

  <xs:element name="enterOrExit" type="gml:GeometryPropertyType"/>

  <xs:element name="moved" type="filter:movedType"/>

  <xs:complexType name="movedType">
    <xs:simpleContent>
      <xs:extension base="xs:double">
        <xs:anyAttribute namespace="##any" processContents="lax"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>

  <xs:element name="locationType" type="filter:locationTypeType"/>

  <xs:simpleType name="locationTypeBase">
    <xs:union>
      <xs:simpleType>
        <xs:restriction base="xs:token">
          <xs:enumeration value="any"/>
        </xs:restriction>
      </xs:simpleType>
      <xs:simpleType>
        <xs:restriction base="filter:locationTypeList">
          <xs:minLength value="1"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:union>
  </xs:simpleType>

  <xs:simpleType name="locationTypeList">
    <xs:list>
      <xs:simpleType>
        <xs:restriction base="xs:token">
          <xs:enumeration value="civic"/>
          <xs:enumeration value="geodetic"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:list>
  </xs:simpleType>
</xs:schema>
```

```
</xs:simpleType>

<xs:complexType name="locationTypeType">
  <xs:simpleContent>
    <xs:extension base="filter:locationTypeBase">
      <xs:attribute name="exact" type="xs:boolean"
        use="optional" default="false"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
</xs:schema>
```

Figure 10: XML Schema

5. Security Considerations

This document specifies one piece, namely filters, utilized in larger system. As such, this document builds on a number of specifications for the security of the complete solution, namely

- o the SIP event notification mechanism, described in RFC 3265 [RFC3265], defining the SUBSCRIBE/NOTIFY messages.
- o the presence event package, described in RFC 3856 [RFC3856], which is a concrete instantiation of the general event notification framework.
- o the filter framework, described in RFC 4661 [RFC4661], to offer the ability to reduce the amount of notifications being sent.

Finally, this document indirectly (via the SIP presence event package) relies on PIDF-LO, described in RFC 4119 [RFC4119], as the XML container that carries location information.

Each of these documents listed above comes with a security consideration section but the security and privacy aspects are best covered by the SIP presence event package, see Section 9 of [RFC3856], and with the GEOPRIV architectural description found in [I-D.ietf-geopriv-arch].

The functionality offered by authorization policies to limit access to location information are provided by other protocols, such Common Policy [RFC4745], Geolocation Policy [I-D.ietf-geopriv-policy] or more recent work around HELD context [I-D.winterbottom-geopriv-held-context]. Although [I-D.ietf-geopriv-policy] defines a standardized format for geolocation authorization policies it does not define specific policies for controlling filters.

The functionality described in this document extends the filter framework with location specific filters. Local policies might be associated with the usage of certain filter constructs and with the amount of notifications specific filter settings might cause. Uploading filters have a significant effect on the ways in which the request is handled at a server. As a result, it is especially important that messages containing this extension be authenticated and authorised. RFC 4661 [RFC4661] discusses this security threat and proposed authentication and authorization solutions applicable by this specification.

6. IANA Considerations

6.1. URN Sub-Namespace Registration for urn:ietf:params:xml:ns:location-filter

This section registers a new XML namespace, as per the guidelines in [RFC3688].

URI: urn:ietf:params:xml:ns:location-filter

Registrant Contact: IETF, GEOPRIV working group, <geopriv@ietf.org>, as delegated by the IESG <iesg@ietf.org>.

XML:

```
BEGIN
<?xml version="1.0"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
    "http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
  <meta http-equiv="content-type"
    content="text/html; charset=iso-8859-1"/>
  <title>Location Filter Namespace</title>
</head>
<body>
  <h1>Namespace for PIDF-LO Location Filters</h1>
  <h2>urn:ietf:params:xml:ns:location-filter</h2>
  <p>See <a href="[[URL of published RFC]]">RFCXXXX</a>.</p>
</body>
</html>
END
```

6.2. Schema Registration For location-filter

This specification registers a schema, as per the guidelines in [RFC3688].

URI: urn:ietf:params:xml:ns:location-filter

Registrant Contact: IETF, GEOPRIV Working Group
(geopriv@ietf.org), as delegated by the IESG (iesg@ietf.org).

XML: The XML can be found as the sole content of Section 4.

7. Contributors

We would like to thank Martin Thomson and James Polk for their contributions to this document.

8. Acknowledgments

Thanks to Richard Barnes and Alissa Cooper, Randall Gellens, Carl Reed, Ben Campbell, Adam Roach, Allan Thomson, James Winterbottom for their comments.

Furthermore, we would like to thank Alexey Melnikov for his IESG review comments.

9. References

9.1. Normative References

- [GML] OpenGIS, "Open Geography Markup Language (GML) Implementation Specification", OpenGIS OGC 02-023r4, January 2003, <<http://www.opengis.org/techno/implementation.htm>>.
- [I-D.ietf-geopriv-arch] Barnes, R., Lepinski, M., Cooper, A., Morris, J., Tschofenig, H., and H. Schulzrinne, "An Architecture for Location and Location Privacy in Internet Applications", draft-ietf-geopriv-arch-01 (work in progress), October 2009.
- [I-D.ietf-sipcore-event-rate-control] Niemi, A., Kiss, K., and S. Loreto, "Session Initiation Protocol (SIP) Event Notification Extension for Notification Rate Control", draft-ietf-sipcore-event-rate-control-03 (work in progress), February 2010.
- [I-D.singh-geopriv-pidf-lo-dynamic] Schulzrinne, H., Singh, V., Tschofenig, H., and M. Thomson, "Dynamic Extensions to the Presence Information Data Format Location Object (PIDF-LO)", draft-singh-geopriv-pidf-lo-dynamic-09 (work in progress), March 2010.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC3265] Roach, A., "Session Initiation Protocol (SIP)-Specific Event Notification", RFC 3265, June 2002.
- [RFC3856] Rosenberg, J., "A Presence Event Package for the Session Initiation Protocol (SIP)", RFC 3856, August 2004.
- [RFC4119] Peterson, J., "A Presence-based GEOPRIV Location Object Format", RFC 4119, December 2005.
- [RFC4661] Khartabil, H., Leppanen, E., Lonnfors, M., and J. Costa-Requena, "An Extensible Markup Language (XML)-Based Format for Event Notification Filtering", RFC 4661, September 2006.
- [RFC5491] Winterbottom, J., Thomson, M., and H. Tschofenig, "GEOPRIV

Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations", RFC 5491, March 2009.

9.2. Informational References

- [I-D.ietf-geopriv-http-location-delivery]
Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, "HTTP Enabled Location Delivery (HELD)", draft-ietf-geopriv-http-location-delivery-16 (work in progress), August 2009.
- [I-D.ietf-geopriv-policy]
Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., and J. Polk, "Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information", draft-ietf-geopriv-policy-21 (work in progress), January 2010.
- [I-D.ietf-sipcore-location-conveyance]
Polk, J. and B. Rosen, "Location Conveyance for the Session Initiation Protocol", draft-ietf-sipcore-location-conveyance-02 (work in progress), February 2010.
- [I-D.winterbottom-geopriv-held-context]
Winterbottom, J., Tschofenig, H., and M. Thomson, "Location URI Contexts in HTTP-Enabled Location Delivery (HELD)", draft-winterbottom-geopriv-held-context-05 (work in progress), October 2009.
- [RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, January 2004.
- [RFC4745] Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J., and J. Rosenberg, "Common Policy: A Document Format for Expressing Privacy Preferences", RFC 4745, February 2007.

Authors' Addresses

Rohan Mahy
Individual

Email: rohan@ekabal.com

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

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

Hannes Tschofenig
Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

Phone: +358 (50) 4871445
Email: Hannes.Tschofenig@gmx.net
URI: <http://www.tschofenig.priv.at>

