

GEOPRIV
Internet-Draft
Intended status: Informational
Expires: May 13, 2011

R. Barnes
BBN Technologies
M. Thomson
J. Winterbottom
Andrew Corporation
H. Tschofenig
Nokia Siemens Networks
November 9, 2010

Location Configuration Extensions for Policy Management
draft-barnes-geopriv-policy-uri-02

Abstract

Current location configuration protocols are capable of provisioning an Internet host with a location URI that refers to the host's location. These protocols lack a mechanism for the target host to inspect or set the privacy rules that are applied to the URIs they distribute. This document extends the current location configuration protocols to provide hosts with a reference to the rules that are applied to a URI, so that the host can view or set these rules.

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 May 13, 2011.

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 Simplified BSD License.

Table of Contents

1. Introduction	3
2. Definitions	4
3. Policy URIs	4
3.1. Policy URI Usage	4
3.2. Policy URI Allocation	5
4. Location Configuration Extensions	6
4.1. HELD	6
4.2. DHCP	7
5. Examples	8
5.1. HELD	8
5.2. DHCP	8
5.3. Basic access control policy	9
6. Acknowledgements	11
7. IANA Considerations	12
7.1. URN Sub-Namespace Registration for urn:ietf:params:xml:ns:geopriv:held:policy	12
7.2. XML Schema Registration	12
7.3. DHCP LuriType Registration	13
8. Operational Considerations	13
9. Security Considerations	14
9.1. Integrity and Confidentiality for Authorization Policy Data	14
9.2. Access Control for Authorization Policy	14
9.3. Location URI Allocation	15
10. References	16
10.1. Normative References	16
10.2. Informative References	17
Authors' Addresses	18

1. Introduction

A critical step in enabling Internet hosts to access location-based services is to provision those hosts with information about their own location. This is accomplished via a Location Configuration Protocol (LCP) [RFC5687], which allows a location provider (e.g., a local access network) to inform a host about its location.

There are two basic patterns for location configuration, namely configuration "by value" and "by reference" [RFC5808]. Configuration by value provisions a host directly with its location, by providing it location information that is directly usable (e.g., coordinates or a civic address). Configuration by reference provides a host with a URI that references the host's location, i.e., one that can be dereferenced to obtain the location (by value) of the host.

In some cases, location by reference offers a few benefits over location by value. From a privacy perspective, the required dereference transaction provides a policy enforcement point, so that the opaque URI itself can be safely conveyed over untrusted media (e.g., SIP through untrusted proxies [RFC5606]). If the target host is mobile, an application provider can use a single reference to obtain the location of the host multiple times, saving bandwidth to the host. For some configuration protocols, the location object referenced by a location URI provides a much more expressive syntax for location values than the configuration protocol itself (e.g., DHCP geodetic location [I-D.ietf-geopriv-rfc3825bis] versus GML in a PIDF-LO [RFC4119]).

From a privacy perspective, however, current LCPs are limited in their flexibility, in that they do not provide the Device (the client in an LCP) with a way to inform the Location Server with policy for how his location information should be handled. This document addresses this gap by defining a simple mechanism for referring to and manipulating policy, and by extending current LCPs to carry policy references. Using the mechanisms defined in this document, an LCP server (acting for the Location Server) can inform a client as to which policy document controls a given location resource, and the LCP client (in its Rule Maker role) can inspect this document and modify it as necessary.

The remainder of this document is structured as follows: After introducing a few relevant terms, we define policy URIs as a channel for referencing, inspecting, and updating policy documents. We then define extensions to the HELD protocol and the DHCP option for location by reference to allow these protocols to carry policy URIs. Examples are given that demonstrate how policy URIs are carried in these protocols and how they can be used by clients.

2. Definitions

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].

3. Policy URIs

A policy URI is an HTTP [RFC2616] URI that identifies a policy resource that contains the authorization policy for a linked location resource. Access to the location resource is governed by the contents of the authorization policy.

A policy URI identifies an HTTP resource that a Rule Maker can use to inspect and install policy documents that tell a Location Server how it should protect the associated location resource. A policy URI always identifies a resource that can be represented as a common-policy document [RFC4745] (possibly including some extensions; e.g., for geolocation policy [I-D.ietf-geopriv-policy]).

Note: RFC 3693 [RFC3693] identified the Rule Holder role as the one that stores policy information. In this document, the Location Server is also a Rule Holder.

3.1. Policy URI Usage

A Location Server that is the authority for policy URIs MUST support GET, PUT, and DELETE requests to these URIs, in order to allow clients to inspect, replace, and delete policy documents. Clients support the three request methods as they desire to perform these operations.

Knowledge of the policy URI can be considered adequate evidence of authorization. A Location Server SHOULD allow all requests, but it MAY deny certain requests based on local policy. For instance, a Location Server might allow clients to inspect policy (GET), but not to update it (PUT).

A GET request to a policy URI is a request for the referenced policy information. If the request is authorized, then the Location Server sends an HTTP 200 response containing the complete policy identified by the URI.

A PUT request to a policy URI is a request to replace the current policy. The entity-body of a PUT request includes a complete policy document. When a Location Server receives a PUT request, it MUST validate the policy document included in the body of the request. If

the request is valid and authorized, then the Location Server replaces the current policy with the policy provided in the request.

A DELETE request to a policy URI is a request to delete the referenced policy document and terminate access to the protected resource. If the request is authorized, then the Location Server deletes the policy referenced by the URI and disallows any further access to the location resource it governs.

The Location Server MUST support policy documents in the common-policy format [RFC4745], as identified by the MIME media type of "application/auth-policy+xml". The common-policy format MUST be provided as the default format in response to GET requests that do not include specific "Accept" headers, but content negotiation MAY be used to allow for other formats.

This usage of HTTP is generally compatible with the use of XCAP [RFC4825] or WebDAV [RFC4918] to manage policy documents, but this document does not define or require the use of these protocols.

3.2. Policy URI Allocation

A Location Server creates a policy URI for a specific location resource at the time that the location resource is created; that is, a policy URI is created at the same time as the location URI that it controls. The URI of the policy resource MUST be different to the location URI.

A policy URI is provided to a target device as part of the location configuration process. A policy URI MUST NOT be provided to an entity that is not authorized to view or set policy. A location server that provides a location configuration in addition to other location services (e.g., answering dereferencing requests [I-D.ietf-geopriv-deref-protocol] or requests from third parties [I-D.ietf-geopriv-held-identity-extensions]) MUST only include policy URIs in response to location configuration requests.

Each location URI has either one policy URI or no policy URI. A location server MUST NOT allocate multiple policy URIs controlling the same location URI. The initial policy that is referenced by a policy URI MUST be identical to the policy that would be applied in the absence of a policy URI. A client that does not support policy URIs can continue to use the location URI as they would have if no policy URI were provided.

Without a policy URI, clients have no way to know what this default policy is. The safest assumption for clients is that the default policy grants any request to dereference a location URI,

regardless of the requester's identity. With a policy URI, a client can ask the server to describe the default policy (with a GET request), or update the policy with a PUT request, prior to distributing the location URI.

A Location Server chooses whether or not to provide a policy URI based on local policy. A HELD-specific extension also allows a requester to specifically ask for a policy URI.

A policy URI is a shared secret between Location Server and its clients. Knowledge of a policy URI is all that is required to perform any operations allowed on the policy. Thus, a policy URI is constructed so that it is hard to predict (see Section 9).

4. Location Configuration Extensions

Location configuration protocols can provision hosts with location URIs that refer to the host's location. If the target host is to control policy on these URIs, it needs a way to access the policy that the Location Server uses to guide how it serves location URIs. This section defines extensions to LCPs to carry policy URIs that the target can use to control access to location resources.

4.1. HELD

The HELD protocol [I-D.ietf-geopriv-http-location-delivery] defines a "locationUriSet" element, which contain a set of one or more location URIs that reference the same resource and share a common access control policy. The schema in Figure 1 defines two extension elements for HELD: an empty "requestPolicyUri" element that is added to a location request to indicate that a Device desires that a policy URI be allocated; and a "policyUri" element that is included as a sub-element of the HELD "locationResponse" element.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:ietf:params:xml:ns:geopriv:held:policy"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:hp="urn:ietf:params:xml:ns:geopriv:held:policy"
  elementFormDefault="qualified" attributeFormDefault="unqualified">

  <xs:element name="requestPolicyUri">
    <xs:complexType name="empty"/>
  </xs:element>

  <xs:element name="policyUri" type="xs:anyURI"/>

</xs:schema>
```

Figure 1

The URI carried in a "policyUri" element refers to the common access control policy for requests for the target's location, including dereference requests for location URIs in the location response as well as third-party requests. The URI MUST be a policy URI as described in Section 3. A policy URI MUST use the "http:" or "https:" scheme, and the Location Server MUST support the specified operations on the URI.

A HELD request MAY contain an explicit request for a policy URI. The presence of the "requestPolicyUri" element in a location request indicates that a policy URI is desired. A location server may provide a policy URI regardless of the presence of this element.

4.2. DHCP

The DHCP location by reference option [I-D.ietf-geopriv-dhcp-lbyr-uri-option] provides location URIs in sub-options called LuriElements. This document defines a new LuriElement type for policy URIs.

LuriType=TBD Policy-URI - This is a policy URI that refers to the access control policy for the location URIs.

[NOTE TO IANA/RFC-EDITOR: Please replace TBD above with the assigned LuriType value and remove this note]

A Policy-URI LuriElement uses a UTF-8 character encoding.

A Policy-URI LuriElement identifies the policy resource for all location URIs included in the location URI option. The URI MUST be a policy URI as described in Section 3: It MUST use either the "http:"

or "https:" scheme, and the Location Server MUST support the specified operations on the URI.

5. Examples

In this section, we provide some brief illustrations of how policy URIs are delivered to target hosts and used by those hosts to manage policy.

5.1. HELD

A HELD request that explicitly requests the creation of a policy URI has the following form:

```
<locationRequest xmlns="urn:ietf:params:xml:ns:geopriv:held">
  <locationType exact="true">locationURI</locationType>
  <requestPolicyUri
    xmlns="urn:ietf:params:xml:ns:geopriv:held:policy"/>
</locationRequest>
```

A HELD response providing a single "locationUriSet", containing two URIs under a common policy, would have the following form:

```
<locationResponse xmlns="urn:ietf:params:xml:ns:geopriv:held">
  <locationUriSet expires="2011-01-01T13:00:00.0Z">
    <locationURI>
      https://ls.example.com:9768/357yc6s64ceyoiuy5ax3o
    </locationURI>
    <locationURI>
      sip:9769+357yc6s64ceyoiuy5ax3o@ls.example.com:
    </locationURI>
  </locationUriSet>
  <policyUri xmlns="urn:ietf:params:xml:ns:geopriv:held:policy">
    https://ls.example.com:9768/policy/357lp6f64prlbvhl5nk3b
  </policyUri>
</locationResponse>
```

5.2. DHCP

A DHCP option providing one of the location URIs and the corresponding policy URI from the previous example would have the following form:

0										1										2										3																			
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1																		
option-code										110																																							
1										0										1										49										'h'									
't'										't'										'p'										's'																			
':'										'/'										'/'										'l'																			
's'										'.'										...																													
TBD										56										'h'										't'																			
't'										'p'										's'										':'																			
'/'										'/'										...																													

[NOTE TO IANA/RFC-EDITOR: Please replace TBD above with the assigned LuriType value and remove this note]

5.3. Basic access control policy

Consider a user that gets the policy URI
 <https://ls.example.com:9768/policy/357lp6f64prlbvhl5nk3b>, as in the
 above LCP example. The first thing this allows the user to do is
 inspect the default policy that the LS has assigned to this URI:

```
GET /policy/357lp6f64prlbvhl5nk3b HTTP/1.1
Host: ls.example.com:9768
```

```
HTTP/1.1 200 OK
Content-type: application/auth-policy+xml
Content-length: 388
```

```
<?xml version="1.0" encoding="UTF-8"?>
<ruleset xmlns="urn:ietf:params:xml:ns:common-policy"
  xmlns:gp="urn:ietf:params:xml:ns:geolocation-policy">
  <rule id="AA56ia9">
    <conditions>
      <validity>
        <until>2011-01-01T13:00:00.0Z</until>
      </validity>
    </conditions>
    <actions/>
    <transformations>
      <gp:provide-location/>
      <gp:set-retransmission-allowed>
        false
      </gp:set-retransmission-allowed>
      <gp:set-retention-expiry>0</gp:set-retention-expiry>
    </transformations>
  </rule>
</ruleset>
```

This policy allows any requester to obtain location information, as long as they know the location URI. If the user disagrees with this policy, and prefers for example, to only provide location to one friend, at a city level of granularity, then he can install this policy on the Location Server:

```
PUT /policy/357lp6f64prlbvhl5nk3b HTTP/1.1
Host: ls.example.com:9768
Content-type: application/auth-policy+xml
Content-length: 462

<?xml version="1.0" encoding="UTF-8"?>
<ruleset xmlns="urn:ietf:params:xml:ns:common-policy">
  <rule id="f3g44r1">
    <conditions>
      <identity>
        <one id="sip:friend@example.com"/>
      </identity>
      <validity>
        <until>2011-01-01T13:00:00.0Z</until>
      </validity>
    </conditions>
    <actions/>
    <transformations>
      <gp:provide-location
        profile="civic-transformation">
        <lp:provide-civic>city</lp:provide-civic>
      </gp:provide-location>
    </transformations>
  </rule>
</ruleset>
```

HTTP/1.1 200 OK

Finally, after using the URI for a period, the user wishes to permanently invalidate the URI.

```
DELETE /policy/357lp6f64prlbvhl5nk3b HTTP/1.1
Host: ls.example.com:9768
```

HTTP/1.1 200 OK

6. Acknowledgements

Thanks to Mary Barnes, Alissa Cooper, and Hannes Tschofenig for providing critical commentary and input on the ideas described in this document.

7. IANA Considerations

This document requires several IANA registrations, detailed below.

7.1. URN Sub-Namespace Registration for urn:ietf:params:xml:ns:geopriv:held:policy

This section registers a new XML namespace,
"urn:ietf:params:xml:ns:geopriv:held:policy", per the guidelines in
[RFC3688].

URI: urn:ietf:params:xml:ns:grip

Registrant Contact: IETF, GEOPRIV working group,
(geopriv@ietf.org), Richard Barnes (rbarnes@bbn.com).

XML:

```
BEGIN
<?xml version="1.0"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">
  <head>
    <title>HELD Policy URI Extension</title>
  </head>
  <body>
    <h1>Namespace for HELD Policy URI Extension</h1>
    <h2>urn:ietf:params:xml:ns:geopriv:held:policy</h2>
    [NOTE TO IANA/RFC-EDITOR: Please replace XXXX
    with the RFC number for this specification.]
    <p>See RFCXXXX</p>
  </body>
</html>
END
```

7.2. XML Schema Registration

This section registers an XML schema as per the guidelines in
[RFC3688].

URI: urn:ietf:params:xml:ns:geopriv:held:policy

Registrant Contact: IETF, GEOPRIV working group (geopriv@ietf.org),
Richard Barnes (rbarnes@bbn.com)

Schema: The XML for this schema can be found in Section Section 4.1.

7.3. DHCP LuriType Registration

IANA is requested to add a value to the LuriTypes registry, as follows:

LuriType	Name	Reference
TBD*	Policy-URI	RFC XXXX**

* TBD is to be replaced with the assigned value

** RFC XXXX is to be replaced with this document's RFC number.

8. Operational Considerations

Associating a user's privacy preferences with a location URI can have a performance impact on the location configuration process, both in terms of protocol execution time and the state that a location server is required to store. There are additional protocol interactions (as described above), and the location server must store the user's privacy policies in addition to purely location-related state.

The mechanism that this document defines for installing policy conducts policy management actions through a separate set of interactions from the main location configuration transaction, rather than carrying policy-management messages in existing location configuration messages. This design decision imposes the cost of at least one an additional HTTP transaction on endpoints that wish to configure privacy policies. At the same time, however, it minimizes the changes that need to be made to a location configuration protocol, so that both HELD and DHCP can support policy management in basically the same fashion.

A server that supports this extension must store additional state for a location URI. By default, a location server only needs to keep location-related state for a location URI, so that it can compute location values to return in response to dereference requests. A server supporting this extension also has to store policy information. Such a server can mitigate the impact of this requirement by not storing policy information explicitly for each location URI. Until a user supplies his own policies, the server will apply a default policy, which doesn't need to be described separately for each location URI. So the amount of policy state that a server has to maintain scales as the number of users that actually

supply their own policy information. If policy URIs are constructed so that they can be associated with their corresponding location URIs algorithmically, then the server doesn't even need to maintain a table to store these associations.

Finally, a server that does not wish to be subject to any of these costs can opt not to support this extension at all. Such a server would simply never provide a "policyUri" element in a response, silently ignoring any "requestPolicyUri" element it might receive in a request.

9. Security Considerations

There are two main classes of risks associated with access control policy management: The risk of unauthorized disclosure of the protected resource via manipulation of the policy management process, and the risk of disclosure of policy information itself.

Protecting the policy management process from manipulation entails two primary requirements: First, the policy URI has to be faithfully and confidentially transmitted to the client, and second, the policy document has to be faithfully and confidentially transmitted to the Location Server. The mechanism also needs to ensure that only authorized entities are able to acquire or alter policy.

9.1. Integrity and Confidentiality for Authorization Policy Data

Each LCP ensures integrity and confidentiality through different means (see [I-D.ietf-geopriv-http-location-delivery] and [I-D.ietf-geopriv-dhcp-lbyr-uri-option]). These measures ensure that a policy URI is conveyed to the client without modification or interception.

To protect the integrity and confidentiality of policy data during management, the Location Server SHOULD provide policy URIs with the "https:" scheme and require the use of HTTP over TLS [RFC2818]. The cipher suites required by TLS [RFC5246] provide both integrity protection and confidentiality. If other means of protection are available, an "http:" URI MAY be used.

9.2. Access Control for Authorization Policy

Access control for the policy resource is based on knowledge of its URI. The URI of a policy resource operates under the same constraints as a possession model location URI [RFC5808] and is subject to the same constraints:

- o Knowledge of a policy URI MUST be restricted to authorized Rule Makers. Confidentiality is required for its conveyance in the location configuration protocol, and in the requests that are used to inspect, change or delete the policy resource.
- o The Location Server MUST ensure that the URI cannot be easily predicted. The policy URI MUST NOT be derived solely from information that might be public, including the Target identity or any location URI. The addition of random entropy increases the difficulty of guessing a policy URI.

Additional requestor authentication MAY be used for policy resources. For instance, in the particular case where the Device is identified to the Location Server by its IP address, the Location Server could use IP return routability as an additional authentication mechanism.

9.3. Location URI Allocation

A policy URI enables the authorization by access control lists model [RFC5808] for associated location URIs. Under this model, it might be possible to more widely distribute a location URI, relying on the authorization policy to constrain access to location information.

To allow for wider distribution, authorization by access control lists places additional constraints on the construction of location URIs.

If multiple Targets share a location URI, an unauthorized location recipient that acquires location URIs for the Targets can determine that the Targets are at the same location by comparing location URIs. With shared policy URIs, Targets are able to see and modify authorization policy for other Targets.

To allow for the creation of Target-specific authorization policies that are adequately privacy-protected, every location URI and policy URI that is issued to a different Target MUST be different. That is, no two client can receive the same location URI or policy URI.

In some deployments it is not always apparent to a LCP server that two clients are different. In particular, where a middlebox [RFC3234] exists two or more clients might appear as a single client. An example of a deployment scenario of this nature is described in [RFC5687]. An LCP server MUST create a different location URI and policy URI for every request, unless the requests can be reliably identified as being from the same client.

Conversely, if a location server chooses to provide the same location URI and policy URI to multiple endpoints, then it MUST use a

restricted profile of the above protocol for policy management. (A server might do this to mitigate problems with link-layer confidentiality, e.g., for multiple clients on a shared medium.) Such a server MAY allow GET requests to allow clients to know the default policy, but it MUST NOT allow PUT or DELETE requests to control policy unless it has an out-of-band mechanism to distinguish and separately authorize clients.

10. References

10.1. Normative References

- [I-D.ietf-geopriv-dhcp-lbyr-uri-option]
Polk, J., "Dynamic Host Configuration Protocol (DHCP) IPv4 and IPv6 Option for a Location Uniform Resource Identifier (URI)", draft-ietf-geopriv-dhcp-lbyr-uri-option-09 (work in progress), October 2010.
- [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.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.
- [RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.
- [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.
- [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

10.2. Informative References

- [I-D.ietf-geopriv-deref-protocol]
Winterbottom, J., Tschofenig, H., Schulzrinne, H., Thomson, M., and M. Dawson, "A Location Dereferencing Protocol Using HELD", draft-ietf-geopriv-deref-protocol-01 (work in progress), September 2010.
- [I-D.ietf-geopriv-held-identity-extensions]
Winterbottom, J., Thomson, M., Tschofenig, H., and R. Barnes, "Use of Device Identity in HTTP-Enabled Location Delivery (HELD)", draft-ietf-geopriv-held-identity-extensions-05 (work in progress), October 2010.
- [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-22 (work in progress), October 2010.
- [I-D.ietf-geopriv-rfc3825bis]
Polk, J., Schnizlein, J., Linsner, M., Thomson, M., and B. Aboba, "Dynamic Host Configuration Protocol Options for Coordinate-based Location Configuration Information", draft-ietf-geopriv-rfc3825bis-13 (work in progress), November 2010.
- [RFC3234] Carpenter, B. and S. Brim, "Middleboxes: Taxonomy and Issues", RFC 3234, February 2002.
- [RFC3693] Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements", RFC 3693, February 2004.
- [RFC4119] Peterson, J., "A Presence-based GEOPRIV Location Object Format", RFC 4119, December 2005.
- [RFC4825] Rosenberg, J., "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)", RFC 4825, May 2007.
- [RFC4918] Dusseault, L., "HTTP Extensions for Web Distributed Authoring and Versioning (WebDAV)", RFC 4918, June 2007.
- [RFC5606] Peterson, J., Hardie, T., and J. Morris, "Implications of 'retransmission-allowed' for SIP Location Conveyance", RFC 5606, August 2009.

- [RFC5687] Tschafenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol: Problem Statement and Requirements", RFC 5687, March 2010.
- [RFC5808] Marshall, R., "Requirements for a Location-by-Reference Mechanism", RFC 5808, May 2010.

Authors' Addresses

Richard Barnes
BBN Technologies
9861 Broken Land Parkway
Columbia, MD 21046
US

Phone: +1 410 290 6169
Email: rbarnes@bbn.com

Martin Thomson
Andrew Corporation
Andrew Building (39)
Wollongong University Campus
Northfields Avenue
Wollongong, NSW 2522
AU

Phone: +61 2 4221 2915
Email: martin.thomson@andrew.com

James Winterbottom
Andrew Corporation
Andrew Building (39)
Wollongong University Campus
Northfields Avenue
Wollongong, NSW 2522
AU

Phone: +61 242 212938
Email: james.winterbottom@andrew.com

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>

