

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 3, 2008

H. Tschofenig
Nokia Siemens Networks
H. Schulzrinne
Columbia University
July 2, 2007

A GEOPRIV HTTPS Using Protocol
draft-tschofenig-geopriv-http-using-protocol-00.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of 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 January 3, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Internet-Draft

GEOPRIV HTTPS Using Protocol

July 2007

Abstract

This document describes an approach to to use Hypertext Transfer Protocol (HTTP) over Transport Layer Protocol (TLS) to transport Presence Information Data Format Location Objects (PIDF-LO) (see [RFC 4119](#)). It is a GEOPRIV using protocol as described in [Section 5.2](#) or [RFC 3693](#) to resolve an identifier, which denotes a reference, to a PIDF-LO. The document assumes that the HTTP client possesses the reference that is obtained using a mechanism that are outside the scope of this document and conveys it to the HTTP server in order to retrieve a PIDF-LO in a response.

Table of Contents

1.	Introduction	3
2.	Requirements Notation	5
3.	Threat Models	6
4.	Steps for Retrieval	8
5.	Structure of Authorization Documents	9
5.1.	Conditions	9
5.1.1.	Identity	9
5.1.2.	Sphere	10
5.2.	Matching with GEOPRIV Using Protocol Requirements	11
6.	IANA Considerations	16
7.	Security Considerations	17
8.	Acknowledgments	18
9.	Open Issues	19
9.1.	Steps for publication	19
9.1.1.	The client uses HTTPS to connect to the server	19
9.1.2.	The client authenticates to the server	19
9.1.3.	The client publishes the resource	19
10.	References	20
10.1.	Normative References	20
10.2.	Informative References	20
	Authors' Addresses	22
	Intellectual Property and Copyright Statements	23

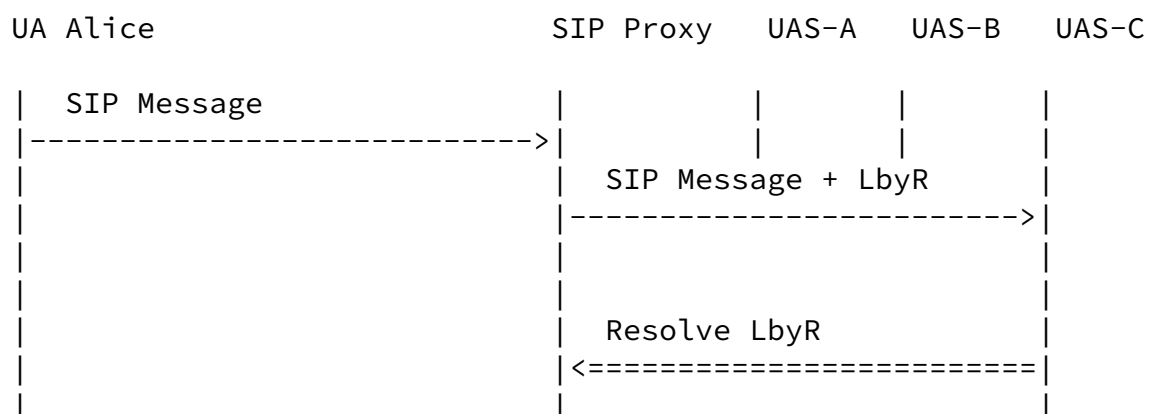
1. Introduction

This document describes a strawman approach for HTTP [2] to transport PIDF-LO objects [3]. RFC 3693 [4], Section 5.2 says the following about Geopriv transport protocols:

"A protocol that just transports the LO as a string of bits, without looking at them (like an IP storage protocol could do), is not a using protocol, but only a transport protocol. Nevertheless, the entity or protocol that caused the transport protocol to move the LO is responsible for the appropriate distribution, protection, usage, retention, and storage of the LO based on the rules that apply to that LO."

While it might be possible to describe HTTP as a transport protocol and punt all of the requirements to the layer above HTTP, this document describes a layering of HTTP over TLS in use between client and server, so that a common set of mechanisms for privacy and authentication are established.

A usage scenario envisioned by this document is described in Figure 1.



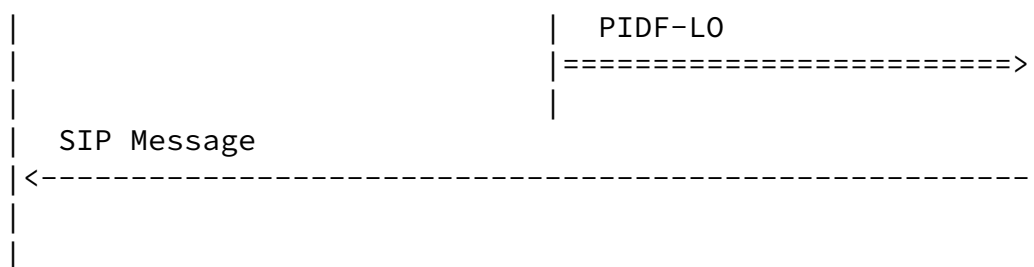


Figure 1: Usage Scenario: Proxy adding Reference

Another usage scenario addressed by this document is described in Figure 2.

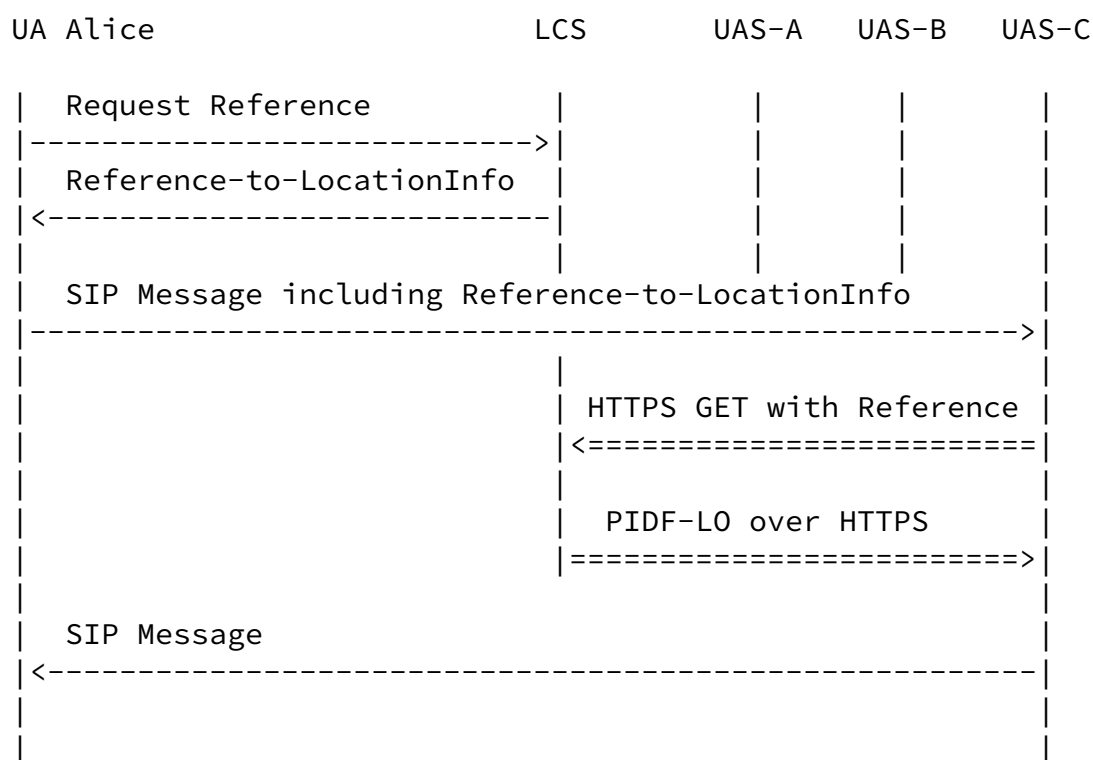


Figure 2: Usage Scenario: End Host adding Reference

The scenario presented in Figure 2 describes a SIP User Agent Alice using a reference to location information obtained using the Location Configuration Protocol (LC), such as HELD [11], RELO [13] or LocationRef [12]. This reference is then added to the SIP message to a SIP message (as described in [14]). The SIP message travels from the Alice via the SIP proxy to UAS-C whereby the reference might be

protected using S/MIME.

When UAS-C receives a SIP message with an included reference then it resolves the reference to a PIDF-LO using the HTTPS mechanism specified in this document.

[2.](#) Requirements Notation

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 [\[1\]](#).

This document furthermore uses the terminology defined in [\[4\]](#).

[3.](#) Threat Models

HTTP can be used as a substrate to a number of different applications, and defining a set of guidelines for conveying a PIDF-LO for any application which might use HTTP would be difficult or impossible. This document does not attempt that task. Instead, it is limited in applicability to the case where a client uses an HTTP GET request to retrieve a PIDF-LO object from a server. No other functionality is covered. This document does not describe how you would determine the URI of the PIDF-LO document or the appropriate server to query.

This document assumes that the reference contains a random component and does not contain identity information as outlined in [\[16\]](#).

There are three threat models that need to be described:

Authorization Policy Threat Model:

The assumption here is that the HTTP server also has some authorization policies and is therefore able to control access to these policies. Consequently, when the reference is conveyed to the potential Location Recipient (e.g., via SIP [[14](#)]), then it does not need to be protected (neither hop-by-hop nor end-to-end). Authentication by the Location Recipient is needed (e.g., TLS client authentication, HTTP Digest authentication, etc.) to disclose location information only to authorized entities.

End-to-End Threat Model:

In this threat model we assume that the reference is encrypted end-to-end, for example using S/MIME and an adversary is not able to eavesdrop, modify or replay a reference. Storing authorization policies at the Location Server is not necessary since the end host is able to control the disclosure of the PIDF-LO by making it available only to trusted entities. Consequently, only the entity that is able to decrypt the end-to-end protected object (in our case the S/MIME encrypted object) can use the reference to resolve it to a PIDF-LO.

Hop-by-Hop Threat Model:

This threat model assumes the reference can either be directly communication between the Target and the Location Recipient or that involved proxies are trusted. In some cases this threat model is also applicable the reference is conveyed to multiple

Location Recipients (such as intermediaries and the final communication end point as it is true for location-based routing). The party that sees the reference has to be able to resolve it into a PIDF-LO.

The first threat model requires client authentication and therefore we describe a mechanism to apply the Geopriv authorization policy framework (see [[5](#)] and [[10](#)]) to HTTP.

[4.](#) Steps for Retrieval

1. The client uses HTTPS [[6](#)] to connect to the server.
2. The client establishes an HTTPS connection to the server, as described in [RFC 2818](#). At the TLS layer, the use of TLS_NULL_WITH_NULL_NULL MUST NOT be used as the CipherSuite.
3. The client authenticates to the server.
4. The client retrieves the resource. The client retrieves the PIDF-L0 resource using an HTTP GET request.

[5.](#) Structure of Authorization Documents

An authorization document is an XML document, formatted according to the schema defined in [\[5\]](#). The authorization documents used by this document inherit the MIME type of common policy documents, application/auth-policy+xml. As described in [\[5\]](#), an authorization document is composed of rules which contain three parts - conditions, actions, and transformations. Each action or transformation, which is also called a permission, has the property of being a positive grant of information to a Location Recipient. As a result, there is a well-defined mechanism for combining actions and transformations obtained from several sources. This mechanism is privacy safe, since the lack of any action or transformation can only result in less information being presented to a watcher.

This section describes how the identity and sphere elements are instantiated. No new conditions, actions and transformations are defined.

[5.1.](#) Conditions

[5.1.1.](#) Identity

Although the <identity> element is defined in [\[5\]](#), that specification indicates that the specific usages of the framework document need to define details that are protocol and usage specific. In particular, it is necessary for a usage of the Common Policy framework to:

- o Define acceptable means of authentication.
- o Define the procedure for representing the identity of the WR (Watcher/Requestor) as a URI or a IRI [\[8\]](#).

[5.1.1.1.](#) Acceptable Forms of Authentication

A request is considered authenticated if one of the following techniques is used:

HTTP Digest:

The presence agent has authenticated the Location Recipient using HTTP digest authentication [\[9\]](#).

TLS Authentication:

[[Editor's Note: More complex description since the different identities used for TLS authentication need to be mapped to a URI

or a IRI.]]

Identity Condition within a SAML Assertion:

TBD

Since HTTP Basic authentication is not recommended it is not described above.

[5.1.1.2](#). Computing a URI for the Location Recipient

For requests that are authenticated using HTTP Digest, the identity of the Location Recipient is set equal to the concatenation of the following case-sensitive items in the given order:

1. the scheme https to 'https:'
2. the content of the username parameter (i.e., username-value) of the as carried in the Authorization Request Header as defined in Section 3.2.2 of [\[9\]](#)
3. '@' token
4. The content of the realm parameter. Note that the realm parameter MUST be chosen in such a way that it does not contain '@' token. [[Editor's note: Alternatively, we could relax this restriction and determine whether it would be OK to use ':' instead of '@' for concatenation. As an example, this would lead to examples like Mufasa:myhost@testrealm.com]]

The concatenated parameters are always a URI since the username parameter is a URI as specified in and the realm parameter is also a URI with the above-mentioned constraint. Consider the following example and the respective result-URI.

```
digest username: alice
digest realm: example.com
```

URI: <https://alice@example.com>

[5.1.2.](#) Sphere

The <sphere> element is defined in [\[5\]](#). However, each application making use of the common policy specification needs to determine how the presence server computes the value of the sphere to be used in the evaluation of the condition.

Tschofenig & Schulzrinne Expires January 3, 2008

[Page 10]

Internet-Draft

GEOPRIV HTTPS Using Protocol

July 2007

This document does not provide an instantiation of the <sphere> element. Hence, the <sphere> element is not present in an authorization policy document defined in this document.

[5.2.](#) Matching with GEOPRIV Using Protocol Requirements

This section compares the GEOPRIV requirements described in [\[4\]](#) with the approach outlined in this document.

Section 7.1 of [\[4\]](#) details the requirements of a "Location Object". We discuss these requirements in the subsequent list.

Req. 1. (Location Object generalities):

- * Regarding requirement 1.1, the Location Object has to be understood by the Location Recipient and the Location Server, the two communication end points. The PIDF-LO [\[3\]](#) allows both civic and geospatial location information to be used.
- * Regarding requirement 1.2, a number of fields in the civic location information format are optional.
- * Regarding requirement 1.3, the civic location information is defined in an extensible way.
- * Regarding requirement 1.4, the location information itself is not defined in this document.
- * Regarding requirement 1.5, the protocol described in this document allows the Location Recipient to resolve a reference to a PIDF-LO only.

- * Regarding requirement 1.6, the Location Object contains both location information and privacy rules. Depending on the deployment scenario, which is outside the scope of this document, the privacy rules might have stronger or a weaker semantic.
- * Regarding requirement 1.7, the Location Object is usable in a variety of protocols.
- * Regarding requirement 1.8, no change regarding with respect to the encoding of the Location Object (see [RFC 4119](#) [3]) was made by this document.

Req. 2. (Location Object fields):

- * Regarding requirement 2.1, depending on the deployment scenario an identifier pointing to the Target may be carried inside the PIDF-LO since the PIDF object provides the ability to carry this identifier. In some circumstances it might be desirable not to carry information about the Target's identity in the PIDF-LO.
- * Regarding requirement 2.2, depending on the deployment scenario the Location Server might require that the Location Recipient performs an authentication step. The security mechanisms for client and server authentication are outside the scope of this document and defined already for HTTPS itself. This document, however, outlines how the authenticated identity is instantiated for usage with the authorization policy framework.
- * Regarding requirement 2.3, proof of possession of the Location Recipient credentials is provided outside the scope of this document. The security mechanisms defined for HTTPS are utilized by this document.
- * Regarding requirement 2.5, [RFC 4119](#) defines the basis for carrying location information in a PIDF document. The ability to extend [RFC 4119](#) to convey motion specific information is

work in progress.

- * Regarding requirement 2.6, this document as specified only allows the Location Recipient to resolve the reference but it does not provide the capability to indicate which location format or granularity has to be returned.
- * Regarding requirement 2.7, the PIDF-LO relevant elements and attributes are available. [[Editor's Note: I need to lookup whether the PIDF-LO contains 'sighting time' and 'TTL']]
- * Regarding requirement 2.8, a reference to an external (more detailed rule set) is provided within the PIDF-LO.
- * Regarding requirement 2.9, security headers and trailers are provided Transport Layer Security.
- * Regarding requirement 2.10, extensibility within the PIDF-LO is provided regarding the definition of namespaces.

Req. 3. (Location Data Types):

- * Regarding requirement 3.1, [RFC 4119](#) [3] defines geospatial location information as the mandatory to implement location format.
- * With the support of civic and geospatial location information in [RFC 4119](#) [3] the requirement 3.2 is fulfilled.
- * Regarding requirement 3.3, the geospatial location information used by this document only refers to absolute coordinates. However, the granularity of the location information can be reduced with the help of the AltRes, LoRes, LaRes fields described in [7].
- * Regarding requirement 3.4, since the PIDF-LO format is designed to be extensible it allows further location information to be defined in the future.

Section 7.2 of [4] details the requirements of a "Using Protocol". These requirements are listed below:

Req. 4.: The using protocol has to obey the privacy and security instructions coded in the Location Object regarding the transmission and storage of the LO. This document carries the PIDF-LO as is via HTTPS from the Location Server to the Location Recipient. The sending and receiving parties must obey the instructions carried inside the object.

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. This document does not define additional security mechanisms beyond HTTPS.

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. The encoding of the [RFC 4119](#)-defined Location Object format is not changed. Because of the verbose XML encoding it is not tailored towards inclusion into a single message.

Section 7.3 of [4] details the requirements of a "Rule based Location Data Transfer". These requirements are listed below:

Req. 7. (LS Rules): Depending on the deployment environment access to location information might be controlled by authorization rules created by the Rule Maker or by a short-lived reference that contains a unguessable random component provided by the Target (or by an entity on behalf of the Target).

Req. 8. (LG Rules): In context of Location-by-Reference it is not possible that there is no relationship between the LG and the LS. As such, the statement made in Req. 7 applies.

Req. 9. (Viewer Rules): The Rule Maker might define (via mechanisms outside the scope of this document) which policy rules are disclosed to other entities. These mechanisms are available with [\[10\]](#).

Req. 10. (Full Rule language): Geopriv has defined a rule language capable of expressing a wide range of privacy rules which is applicable in the area of the distribution of Location Objects. The format of these rules are described in [\[5\]](#) and [\[10\]](#).

Req. 11. (Limited Rule language): A limited (or basic) ruleset was introduced with PIDF-LO [\[3\]](#).

Section 7.4 of [\[4\]](#) details the requirements of a "Location Object Privacy and Security". These requirements are listed below:

Req. 12 (Identity Protection): Identity protection of the Target can be provided if (a) the protocol used to convey the reference does not disclose the identity of the Target and (b) if the PIDF-LO does not contain information about the identity about the Target. Currently, there is no mechanism available that allows the Target to tell the LS not to include identity information in the PIDF-LO.

Req. 13. (Credential Requirements): The security mechanism specified in this document is Transport Layer Security. TLS offers the ability to use different types of credentials, including symmetric, asymmetric credentials or a combination of them.

Req. 14. (Security Features): Geopriv defines a few security requirements for the protection of Location Objects such as mutual end-point authentication, data object integrity, data object confidentiality and replay protection. The ability to use

Transport Layer security fulfills these requirements.

Req. 15. (Minimal Crypto): [[Editor's Note: A mandatory to implement ciphersuite has to be specified in this document.]]

6. IANA Considerations

This document does not imply any actions for IANA.

[7.](#) Security Considerations

This document assumes that the use of TLS as substrate to HTTP is sufficient to protect the privacy of the PIDF-LO content while in flight. When access control has to be applied prior to conveying the PIDF-LO towards the Location Recipient then the content of [Section 5.1](#) is applicable. The description about instantiating the identity element allows the Common Policy authorization framework to be used. In order to make reasonable authorization decisions the Location Recipient needs to be authenticated (e.g., using HTTP Digest Authentication or client-side TLS authentication) or to present authorization information in the form of a SAML assertion. There is ongoing work to update Digest Authentication, and those may eventually require an update to the recommended authentication method. If access control is not applied as described in the threat models in [Section 3](#) then the possession of the reference to location information that must fulfill certain characteristics (such as containing a random component) is sufficient to obtain be authorized to resolve the reference to a PIDF-LO.

Internet-Draft

GEOPRIV HTTPS Using Protocol

July 2007

8. Acknowledgments

The authors would like to thank the GEOPRIV working group for discussions in relationship to a Geopriv Layer 7 Location Configuration Protocol and SIP Location Conveyance that motivate this document.

The authors would like to thank Ted Hardie for the work with [draft-hardie-geopriv-https-strawman-00](#) document that served as a basis for this document.

[9.](#) Open Issues

This document contains a couple of open issues and is primarily meant to stimulate some discussions around dereferencing of HTTPS URIs to PIDF-LOs. A further open issue is whether a GEOPRIV using protocol should also define steps for publication of PIDF-LOs, as described below.

[9.1.](#) Steps for publication

[9.1.1.](#) The client uses HTTPS to connect to the server

The client establishes an HTTPS connection to the server, as described in [RFC 2818](#). At the TLS layer, the use of TLS_NULL_WITH_NULL_NULL MUST NOT be used as the CipherSuite.

[9.1.2.](#) The client authenticates to the server

The client authenticates to the server using HTTP's digest authentication mechanism as described in [RFC 2617](#) and updated by the errata.

[9.1.3.](#) The client publishes the resource

The client publishes the PIDF-LO resource using an HTTP PUT request.

[10.](#) References

[10.1.](#) Normative References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [2] 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.
- [3] Peterson, J., "A Presence-based GEOPRIV Location Object Format", [RFC 4119](#), December 2005.
- [4] Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements", [RFC 3693](#), February 2004.
- [5] 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.

- [6] Rescorla, E., "HTTP Over TLS", [RFC 2818](#), May 2000.
- [7] Polk, J., Schnizlein, J., and M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information", [RFC 3825](#), July 2004.
- [8] Duerst, M. and M. Suignard, "Internationalized Resource Identifiers (IRIs)", [RFC 3987](#), January 2005.
- [9] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", [RFC 2617](#), June 1999.

[10.2](#). Informative References

- [10] Schulzrinne, H., "Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information", [draft-ietf-geopriv-policy-12](#) (work in progress), May 2007.
- [11] Barnes, M., "HTTP Enabled Location Delivery (HELD)", [draft-ietf-geopriv-http-location-delivery-00](#) (work in progress), June 2007.
- [12] Schulzrinne, H., "A Location Reference Event Package for the Session Initiation Protocol (SIP)", [draft-schulzrinne-geopriv-locationref-00](#) (work in progress), October 2006.

- [13] Schulzrinne, H., "RELO: Retrieving End System Location Information", [draft-schulzrinne-geopriv-relo-03](#) (work in progress), March 2007.
- [14] Polk, J. and B. Rosen, "Session Initiation Protocol Location Conveyance", [draft-ietf-sip-location-conveyance-07](#) (work in progress), February 2007.
- [15] Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol; Problem Statement and Requirements", [draft-ietf-geopriv-l7-lcp-ps-02](#) (work in progress), April 2007.

- [16] Marshall, R., "Requirements for a Location-by-Reference Mechanism used in Location Configuration and Conveyance", [draft-marshall-geopriv-lbyr-requirements-01](#) (work in progress), March 2007.

Authors' Addresses

Hannes Tschofenig
Nokia Siemens Networks
Otto-Hahn-Ring 6

Munich, Bavaria 81739
Germany

Phone: +49 89 636 40390
Email: Hannes.Tschofenig@nsn.com
URI: <http://www.tschofenig.com>

Henning Schulzrinne
Columbia University
Department of Computer Science
450 Computer Science Building
New York, NY 10027
US

Phone: +1 212 939 7004
Email: hgs@cs.columbia.edu
URI: <http://www.cs.columbia.edu>

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

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

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

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

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).

