GEOPRIV	J. Winterbottom	
Internet-Draft	Andrew Corporation	
Intended status: Standards Track	H. Tschofenig	
Expires: July 31, 2010	Nokia Siemens Networks	
	H. Schulzrinne	
	Columbia University	
	M. Thomson	
	M. Dawson	
	Andrew Corporation	
	January 27, 2010	

TOC

A Location Dereferencing Protocol Using HELD
draft-winterbottom-geopriv-deref-protocol-05

Abstract

This document describes how to use the Hypertext Transfer Protocol (HTTP) over Transport Layer Security (TLS) as a dereferencing protocol to resolve a reference to a Presence Information Data Format Location Object (PIDF-LO). The document assumes that a Location Recipient possesses a secure HELD URI that can be used in conjunction with the HELD protocol to request the location of the Target.

Status of This Memo

Table of Contents

---

1. Introduction

TOC

Provision of location information by reference (Marshall, R., “Requirements for a Location-by-Reference Mechanism,” November 2009.) [I-D.ietf-geopriv-lbyr-requirements] involves the creation of a resource that is identified by a "location URI". A "location URI" identifies resource that contains the location of an entity. A location URI might be a temporary resource, created in response to a HTTP-Enabled Location Delivery (HELD) (Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, “HTTP Enabled Location Delivery (HELD),”

August 2009.) [I-D.ietf-geopriv-http-location-delivery] request. A location URI does not intrinsically include location information, instead the URI is "dereferenced" by a Location Recipient to acquire location information. This document specifies how a holder of a location URI uses that URI to retrieve location information.

The HELD protocol, as described in [I-D.ietf-geopriv-http-location-delivery] (Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, "HTTP Enabled Location Delivery (HELD)," August 2009.), defines a use of HTTP that enables location configuration - the process where a Device acquires location information about itself. A part of location configuration is the provision of a location URI. However, HELD does not describe how such a URI is used; this document provides that definition.

This document defines how HELD is used by a Location Recipient to dereference a location URI and acquire location information. The result of this process is location object in the form of a Presence Information Data Format - Location Object (PIDF-LO) document (Peterson, J., "A Presence-based GEOPRIV Location Object Format," December 2005.) [RFC4119]. A constrained set of HELD features are defined such that it is suitable for use as a location dereference protocol (Marshall, R., "Requirements for a Location-by-Reference Mechanism," November 2009.) [I-D.ietf-geopriv-lbyr-requirements]. Use as a location dereference protocol requires use of the Transport Layer Security (TLS) binding for HTTP (Rescorla, E., "HTTP Over TLS," May 2000.) [RFC2818] in order to provide confidentiality, authentication and protection from modification.

Use of HELD as a dereferencing protocol has the advantage that the Location Recipient can indicate the type of location information it would like to receive. This functionality is already available with the HELD base specification, described in [I-D.ietf-geopriv-http-location-delivery] (Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, "HTTP Enabled Location Delivery (HELD)," August 2009.). Furthermore, the HELD response from the LIS towards the Location Recipient not only provides the PIDF-LO but also encapsulates supplementary information, such as error messages, back to the Location Recipient.

Location URIs created for use with HELD dereferencing use the https: or http: scheme. The behaviour described in this document can be used by Location Recipients that are aware of the fact that the URI is a location URI.

An example scenario envisioned by this document is shown in Figure 1 (Example of Dereference Protocol Exchange). This diagram shows how a location dereference protocol fits with location configuration and conveyance. [I-D.ietf-geopriv-lbyr-requirements] (Marshall, R., "Requirements for a Location-by-Reference Mechanism," November 2009.) contains more information on this scenario and others like it.

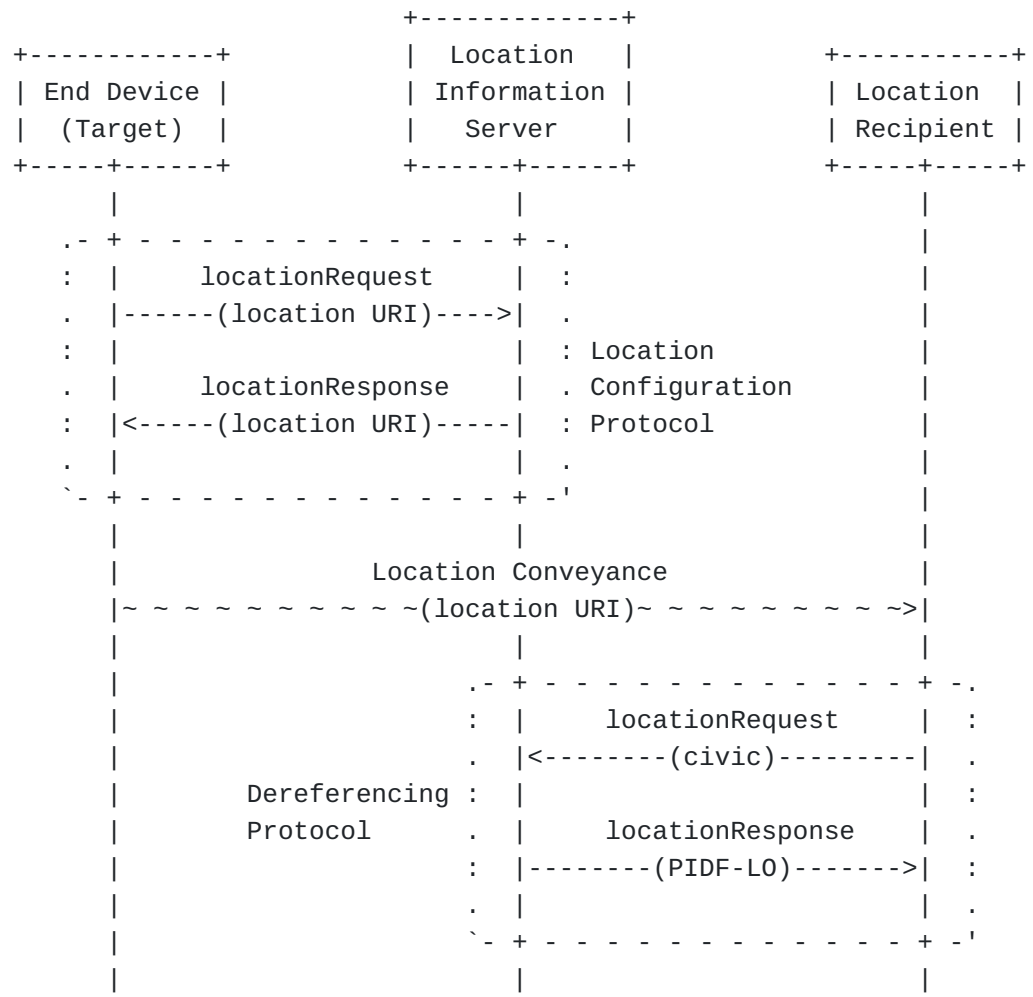

Figure 1: Example of Dereference Protocol Exchange

2. Terminology

TOC

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] (Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.).
This document uses key terminology from several sources:

*terms for the GEOPRIV reference model defined in [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," October 2009.);

*the term Location Information Server (LIS), from [I-D.ietf-geopriv-l7-lcp-ps] (Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol; Problem Statement and Requirements," July 2009.), is a node in the access network that provides location information to an end point; a LIS provides location URIs;

*the term Location Server (LS), from [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," October 2009.), is used to identify the role that responds to a location dereference request; this might be the same entity as the LIS, but the model in [I-D.ietf-geopriv-lbyr-requirements] (Marshall, R., "Requirements for a Location-by-Reference Mechanism," November 2009.) allows for the existence of separate - but related - entities; and

*the term location URI is coined in [I-D.ietf-geopriv-lbyr-requirements] (Marshall, R., "Requirements for a Location-by-Reference Mechanism," November 2009.).

---

3. Authorization Models

TOC

This section discusses two extreme types of authorization models for dereferencing with HELD URIs, namely "Authorization by Possession" and "Authorization by Access Control". In the subsequent subsections we discuss the properties of these two models. These two models can, however, be used in combination in a real deployment. Figure 2 (Communication Model), from [I-D.ietf-geopriv-lbyr-requirements] (Marshall, R., "Requirements for a Location-by-Reference Mechanism," November 2009.), shows the model applicable to location configuration, conveyance and dereference.

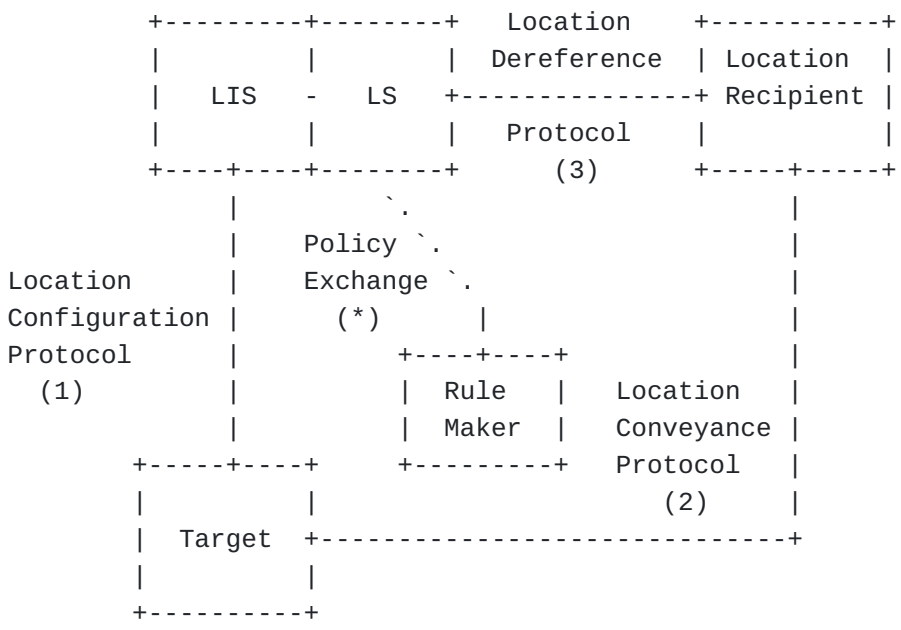

Figure 2: Communication Model

It is important to note that this document does not mandate a specific authorization model, nor does it constrain the usage with regard to these models in any way. Additionally, it is possible to combine certain parts of both models.
For either authorization model, the overall process is similar. The following steps are followed, with minor alterations:

1. The Target acquires a location URI from the LIS. This might use HELD as a location configuration protocol (LCP).

2. The Target then conveys the location URI to a third party, the Location Recipient (for example using SIP as described in [I-D.ietf-sipcore-location-conveyance] (Polk, J. and B. Rosen, "Location Conveyance for the Session Initiation Protocol," February 2010.)). This step is shown in (2) of Figure 2 (Communication Model).

3. The Location Recipient then needs to dereference the location URI in order to obtain the Location Object (3). Depending on the URI scheme of the location URI dereferencing might, as is the case for https: or http: URIs, be performed as described in this document.

In this final step, the Location Server (LS) or LIS makes an authorization decision. How this decision is reached depends on the authorization model.

3.1. Authorization by Possession

TOC

In this model, possession - or knowledge - of the location URI is used to control access to location information. A location URI is constructed such that it is hard to guess (see C9 of [I-D.ietf-geopriv-lbyr-requirements] (Marshall, R., "Requirements for a Location-by-Reference Mechanism," November 2009.)) and the set of entities that it is disclosed to is limited. The only authentication required by the LS is evidence of possession of the URI. The LS is able to immediately authorize any request that indicates this URI.

Authorization by possession uses a very simple policy that does not typically require direct interaction with a Rule Maker; it is assumed that the Rule Maker is able to exert control over the distribution of the location URI. Therefore, the LIS can operate with limited policy input from a Rule Maker.

Limited disclosure is an important aspect of this authorization model. The location URI is a secret; therefore, ensuring that adversaries are not able to acquire this information is paramount. Encryption, such as might be offered by TLS (Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," August 2008.) [RFC5246] or S/MIME (Ramsdell, B., "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification," July 2004.) [RFC3851], protects the information from eavesdroppers.

Use of authorization by possession location URIs in a hop-by-hop protocol such as SIP (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," June 2002.) [RFC3261] adds the possibility of on-path adversaries. Depending on the usage of the location URI for certain location based applications (e.g., emergency services, location based routing) specific treatment is important, as discussed in [I-D.ietf-sipcore-location-conveyance] (Polk, J. and B. Rosen, "Location Conveyance for the Session Initiation Protocol," February 2010.).

Using possession as a basis for authorization means that, once granted, authorization cannot be easily revoked. Cancellation of a location URI ensures that legitimate users are also affected; application of additional policy is theoretically possible, but could be technically infeasible. Therefore, other measures are provided to prevent an adversary from gaining access to location information indefinitely.

A very simple policy is established at the time that the location URI is created. This policy specifies that the location URI expires after a certain time, which limits any inadvertent exposure of location information to adversaries. The expiration time of the location URI might be negotiated at the time of its creation, or it might be unilaterally set by the LIS.

3.2. Authorization via Access Control

TOC

Use of explicit access control provides a Rule Maker greater control over the behaviour of an LS. In contrast to authorization by possession, possession of a this form of location URI does not imply authorization. Since an explicit policy is used to authorize access to location information, the location URI can be distributed to many potential Location Recipients.

Either before creation or dissemination of the location URI, the Rule Maker establishes an authorization policy with the LS. In reference to Figure 2 (Communication Model), authorization policies might be established at creation (Step 1), and need to be established before before the location URI is published (Step 2) to ensure that the policy grants access to the desired Location Recipients. Depending on the mechanism used, it might also be possible to change authorization policies at any time.

A possible format for these authorization policies is available with GEOPRIV Common Policy [RFC4745] (Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J., and J. Rosenberg, “Common Policy: A Document Format for Expressing Privacy Preferences,” February 2007.) and Geolocation Policy [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,” January 2010.). Additional constraints might be established by other means.

The LS enforces the authorization policy when a Location Recipient dereferences the URI. Explicit authorization policies allow a Rule Maker to specify the identity of Location Recipients, constrain the accuracy and form of location information, and to control other aspects of the authorization process.

---

4. HELD Dereference Protocol

TOC

This section describes how HELD can be used to dereference a location URI. This process can be applied when a Location Recipient is in possession of a location URI with a https: or http: URI scheme.

A Location Recipient that wishes to dereference an https: or http: URI performs a HELD request on HTTP to the identified resource.

> **Note:** In many cases, an http: URI does not provide sufficient security for location URIs. The absence of the security mechanisms provided by TLS means that the Rule Maker has no control over who receives location information and the Location Recipient has no assurance that the information is correct.

The Location Recipient establishes a connection to the LS, as described in [RFC2818] (Rescorla, E., "HTTP Over TLS," May 2000.). The TLS ciphersuite TLS_NULL_WITH_NULL_NULL MUST NOT be used. The LS MUST be authenticated to ensure that the correct server is contacted. Given that a location URI does not indicate the authorization model used, the Location Recipient MUST be prepared to provide authentication information unless it has external information on the authorization model used by the URI. This document does not specify how the LS authenticates the Location Recipient; however, a Location Recipient MUST support provision of a client certificate during TLS session creation and HTTP digest authentication (Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication," June 1999.) [RFC2617], unless these authentication methods are known to be inapplicable.

4.1. HELD Usage Profile

TOC

Use of HELD as a location dereference protocol is largely the same as its use as a location configuration protocol. Aside from the restrictions noted in this document, HELD semantics do not differ from those established in [I-D.ietf-geopriv-http-location-delivery] (Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, "HTTP Enabled Location Delivery (HELD)," August 2009.).

The HELD locationRequest is the only request permitted by this specification. Similarly, request parameters other than the following MUST NOT be accepted by the LS: responseTime, locationType (including the associated exact attribute). Other specifications MUST explicitly describe whether other requests or parameters apply to dereference requests and how they are to be interpreted if they are permitted. The LS MUST ignore any parameters that it does not understand unless it knows the parameters to be invalid, such as those defined in [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)," February 2010.). If parameters are known to be invalid, the LS MAY generate a HELD error response.

The LS MUST NOT generate any location URIs or provide a locationUriSet in response to a dereference request. If the location request contains a locationType element that includes locationURI, this parameter is either ignored or rejected as appropriate, based on the associated exact attribute.

This document requires additional HTTP features from Location Recipients that are not required of Devices in HELD. HTTP digest authentication (Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication," June 1999.) [RFC2617] MUST be

supported by Location Recipients, unless there is no means to provide such authentication information.

5. Examples

TOC

The example in Figure 3 (Minimal Dereferencing Request) shows the simplest form of dereferencing request using HELD to the location URI https://ls.example.com:49152/uri/w3g61nf5n66p0. The only way that this differs from the example in Section 10.1 of [I-D.ietf-geopriv-http-location-delivery] (Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, "HTTP Enabled Location Delivery (HELD)," August 2009.) is in the request URI and the source of the URI.

```
POST /uri/w3g61nf5n66p0 HTTP/1.1
Host: ls.example.com:49152
Content-Type: application/held+xml
Content-Length: 87

<?xml version="1.0"?>
<locationRequest xmlns="urn:ietf:params:xml:ns:geopriv:held"/>
```

Figure 3: Minimal Dereferencing Request

Figure 4 (Response with Location Information) shows the response to the previous request listing both civic and geodetic location information of the Target's location. If this looks similar to the response in Section 10.1 of [I-D.ietf-geopriv-http-location-delivery] (Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, "HTTP Enabled Location Delivery (HELD)," August 2009.), that is no coincidence - unless policy specfies otherwise, the Location Recipient receives the same information as the Device.

```
HTTP/1.1 200 OK
Server: Example LIS
Date: Tue, 10 Jan 2009 03:42:29 GMT
Expires: Tue, 10 Jan 2009 03:42:29 GMT
Cache-control: private
Content-Type: application/held+xml
Content-Length: 594

<?xml version="1.0"?>
<locationResponse xmlns="urn:ietf:params:xml:ns:geopriv:held">
<presence xmlns="urn:ietf:params:xml:ns:pidf"
          entity="pres:3650n87934c@ls.example.com">
  <tuple id="b650sf789nd">
  <status>
   <geopriv xmlns="urn:ietf:params:xml:ns:pidf:geopriv10">
    <location-info>
       <Point xmlns="http://www.opengis.net/gml"
              srsName="urn:ogc:def:crs:EPSG::4326">
         <pos>-34.407 150.88001</pos>
       </Point>
     </location-info>
     <usage-rules>
       <retention-expiry>
         2006-01-11T03:42:28+00:00</retention-expiry>
     </usage-rules>
     <method>Wiremap</method>
   </geopriv>
  </status>
  <timestamp>2006-01-10T03:42:28+00:00</timestamp>
  </tuple>
</presence>
</locationResponse>
```

Figure 4: Response with Location Information

6. Security Considerations

TOC

Privacy of location information is the most important security consideration for this document. Two measures in particular are used to protect privacy: TLS and authorization policies. TLS provides a means of ensuring confidentiality of location information through encryption and mutual authentication. An authorization policy allows a Rule Maker to explicitly control how location information is provided to Location

Recipients. The process by which a Rule Maker establishes an authorization policy is not covered by this document; several methods are possible, for instance: [I-D.winterbottom-geopriv-held-context] (Winterbottom, J., Tschofenig, H., and M. Thomson, "Location URI Contexts in HTTP-Enabled Location Delivery (HELD)," October 2009.), [RFC4825] (Rosenberg, J., "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)," May 2007.).

Use of TLS for the dereferencing of location URIs is strongly RECOMMENDED, as discussed in Section 4.1 (HELD Usage Profile). Location Recipients MUST authenticate the host identity using the domain name included in the location URI, using the procedure described in Section 3.1 of [RFC2818] (Rescorla, E., "HTTP Over TLS," May 2000.). Local policy determines what a Location Recipient does is authentication fails, or is not attempted.

The authorization by possession model (Authorization by Possession) further relies on TLS when transmitting the location URI to protect the secrecy of the URI. Possession of such a URI implies the same privacy considerations as possession of the PIDF-LO document that the URI references. This is necessary, since the policy attached to such a location URI permits any who have the URI to view it. This aspect of security is covered in more detail in the specification of location conveyance protocols, such as [I-D.ietf-sipcore-location-conveyance] (Polk, J. and B. Rosen, "Location Conveyance for the Session Initiation Protocol," February 2010.).

The Location Recipient MUST be prepared to provide authentication credentials when making a dereference request.

To comply with identity protection requirements in [I-D.ietf-geopriv-lbyr-requirements] (Marshall, R., "Requirements for a Location-by-Reference Mechanism," November 2009.), the LS MUST NOT include any information that could be used to identify a Target, unless policy is provided that allows this. To this end, an unlinked pseudonym MUST be provided in the entity attribute of the PIDF-LO document.

Further security considerations and requirements relating to the use of location URIs are described in [I-D.ietf-geopriv-lbyr-requirements] (Marshall, R., "Requirements for a Location-by-Reference Mechanism," November 2009.).

---

7. IANA Considerations

TOC

This document makes no request of IANA.

[[IANA/RFC-EDITOR: Please remove this section before publication.]]

TOC

8. Acknowledgements

Thanks to Barbara Stark and Guy Caron for providing early comments. Thanks to Rohan Mahy for constructive comments on the scope and format of the document. Thanks to Ted Hardie for his strawman proposal that provided assistance with the security section of this document.
The authors would like to thank the participants of the GEOPRIV interim meeting 2008 for their feedback.
James Polk provided comments on a security aspects in June 2008.

---

9. References

TOC

9.1. Normative References

TOC

[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 (TXT).
[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[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 (TXT, PS, PDF, HTML, XML).
[RFC2617]	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 (TXT, HTML, XML).
[RFC2818]	Rescorla, E., “HTTP Over TLS,” RFC 2818, May 2000 (TXT).
[RFC3986]	Berners-Lee, T., Fielding, R., and L. Masinter, “Uniform Resource Identifier (URI): Generic Syntax,” STD 66, RFC 3986, January 2005 (TXT, HTML, XML).
[RFC4119]	Peterson, J., “A Presence-based GEOPRIV Location Object Format,” RFC 4119, December 2005 (TXT).
[RFC4395]	Hansen, T., Hardie, T., and L. Masinter, “Guidelines and Registration Procedures for New URI Schemes,” BCP 35, RFC 4395, February 2006 (TXT).
[RFC5234]	Crocker, D. and P. Overell, “Augmented BNF for Syntax Specifications: ABNF,” STD 68, RFC 5234, January 2008 (TXT).

[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 (TXT).

9.2. Informative references

TOC

[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 (TXT).
[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-03 (work in progress), February 2010 (TXT).
[I-D.ietf-geopriv-l7-lcp-ps]	Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol; Problem Statement and Requirements," draft-ietf-geopriv-l7-lcp-ps-10 (work in progress), July 2009 (TXT).
[I-D.ietf-geopriv-lbyr-requirements]	Marshall, R., "Requirements for a Location-by-Reference Mechanism," draft-ietf-geopriv-lbyr-requirements-09 (work in progress), November 2009 (TXT).
[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 (TXT).
[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 (TXT).
[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 (TXT).
[RFC3261]	Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," RFC 3261, June 2002 (TXT).

[RFC3693]	Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements," RFC 3693, February 2004 (TXT).
[RFC3851]	Ramsdell, B., "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification," RFC 3851, July 2004 (TXT).
[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 (TXT).
[RFC4825]	Rosenberg, J., "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)," RFC 4825, May 2007 (TXT).
[RFC5246]	Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246, August 2008 (TXT).

Appendix A. GEOPRIV Using Protocol Compliance

TOC

This section describes how use of HELD as a location dereference protocol complies with the GEOPRIV requirements described in [RFC3693] (Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements," February 2004.).

Req. 1. (Location Object generalities):
This section relates to the PIDF-LO (Peterson, J., "A Presence-based GEOPRIV Location Object Format," December 2005.) [RFC4119] document, which is used by HELD. These requirements are addressed by [RFC4119] (Peterson, J., "A Presence-based GEOPRIV Location Object Format," December 2005.) and [RFC5491] (Winterbottom, J., Thomson, M., and H. Tschofenig, "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations," March 2009.).

Req. 2. (Location Object fields):
This section relates to the PIDF-LO (Peterson, J., "A Presence-based GEOPRIV Location Object Format," December 2005.) [RFC4119] document, which is used by HELD. These requirements are addressed by [RFC4119] (Peterson, J., "A Presence-based GEOPRIV Location Object Format," December 2005.) and [RFC5491] (Winterbottom, J., Thomson, M., and H. Tschofenig, "GEOPRIV Presence Information

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

Req. 3. (Location Data Types):
This section relates to the PIDF-LO (Peterson, J., "A Presence-based GEOPRIV Location Object Format," December 2005.) [RFC4119] document, which is used by HELD. These requirements are addressed by [RFC4119] (Peterson, J., "A Presence-based GEOPRIV Location Object Format," December 2005.) and [RFC5491] (Winterbottom, J., Thomson, M., and H. Tschofenig, "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations," March 2009.).

Section 7.2 of [RFC3693] (Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements," February 2004.) details the requirements of a "Using Protocol". These requirements are repeated here for reference, followed by a statement of compliance:

Req. 4. "The using protocol has to obey the privacy and security instructions coded in the Location Object and in the corresponding Rules regarding the transmission and storage of the LO."
Compliant: This document carries the PIDF-LO as is via HTTPS from the LIS 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."
Compliant: This document specifies that authentication of the LS uses the established public key infrastructure used by HTTP over TLS (Rescorla, E., "HTTP Over TLS," May 2000.) [RFC2818].
Location Recipient is accomplished using certificates exchanged using TLS, or through HTTP digest authentication (Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication," June 1999.) [RFC2617].
Authentication of Location Recipients as specified in this document requires pre-arrangement; further key establishment methods are left to later work.

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."
Not Compliant: The XML encoding specified in [RFC4119] (Peterson, J., "A Presence-based GEOPRIV Location Object Format," December 2005.) is not suited to single packet transfers. It is

not the goal of this document to define a new Location Object format.

Section 7.3 of [RFC3693] (Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, “Geopriv Requirements,” February 2004.) details the requirements of a "Rule based Location Data Transfer". These requirements are repeated where they are applicable to this document:

Req. 7. "(LS Rules) The decision of a Location Server to provide a Location Recipient access to Location Information MUST be based on Rule Maker-defined Privacy Rules."
Compliance or Not Applicable: This document describes two alternative methods by which a Rule Maker is able to control access to location information. Rule Maker policy is enforced by the LS when a location URI is dereferenced. However, this document does not describe how a location URI is created, or how a Rule Maker associates policy with a location URI. These are outside the scope of this document.

Req. 8. (LG Rules) Not Applicable: This relationship between LS and the source of its information (be that Location Generator (LG) or LIS) is out of scope for this document.

Req. 9. "(Viewer Rules) A Viewer does not need to be aware of the full Rules defined by the Rule Maker (because a Viewer SHOULD NOT retransmit Location Information), and thus a Viewer SHOULD receive only the subset of Privacy Rules necessary for the Viewer to handle the LO in compliance with the full Privacy Rules (such as, instruction on the time period for which the LO can be retained)."
Compliant: The Rule Maker might define (via mechanisms outside the scope of this document) which policy rules are disclosed to other entities. For instance, if [RFC4745] (Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J., and J. Rosenberg, “Common Policy: A Document Format for Expressing Privacy Preferences,” February 2007.) is used to convey authorization policies from Rule Maker to LS, this is possible using the parameters specified in [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,” January 2010.).

Req. 10. (Full Rule language) Not Applicable: Note however that Geopriv has defined a rule language capable of expressing a wide range of privacy rules (see [RFC4745] (Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J., and J. Rosenberg, “Common Policy: A Document Format for Expressing Privacy Preferences,” February 2007.) and

[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," January 2010.).

Req. 11. (Limited Rule language) Not Applicable: This requirement applies to (and is addressed by) PIDF-LO (Peterson, J., "A Presence-based GEOPRIV Location Object Format," December 2005.) [RFC4119].

Section 7.4 of [RFC3693] (Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements," February 2004.) details the requirements of "Location Object Privacy and Security". These requirements are repeated where they are applicable to this document:

Req. 12. (Identity Protection) Potentially Compliant: Identity protection of the Target is provided as long as both of the following conditions are true:

(a) the location URI is not associated with the identity of the Target in any context, and

(b) if the PIDF-LO does not contain information about the identity about the Target.

For instance, this requirement is complied with if the protocol that conveys the location URI does not link the identity of the Target to the location URI and the LS doesn't include meaningful identification information in the PIDF-LO document. Section 6 (Security Considerations) recommends that an unlinked pseudonym is used by the LS.

Req. 13. (Credential Requirements) Compliant: The primary 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) Compliant: 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) Compliant: The mandatory to implement ciphersuite is provided in the TLS layer security specification.

Appendix B. Compliance to Location Reference Requirements

TOC

This section describes how HELD complies to the location reference requirements stipulated in [I-D.ietf-geopriv-lbyr-requirements] (Marshall, R., “Requirements for a Location-by-Reference Mechanism,” November 2009.). Compliance to the Location Configuration Protocol are included in this document.

> Note that use of HELD as a location dereference protocol does not necessarily imply that HELD is the corresponding LCP. This document is still applicable to held: location URIs that are acquired by other means.

B.1. Requirements for a Location Configuration Protocol

TOC

C1. "location URI support: The configuration protocol MUST support a location reference in URI form."
Compliant: HELD only provides location references in URI form.

C2. "location URI expiration: When a location URI has a limited validity interval, its lifetime MUST be indicated."
Compliant: HELD indicates the expiry time of location URIs using the expires attribute. HELD contexts (Winterbottom, J., Tschofenig, H., and M. Thomson, “Location URI Contexts in HTTP-Enabled Location Delivery (HELD),” October 2009.) [I-D.winterbottom-geopriv-held-context] also expire, and an explicit indication is included in the context response; a Device is able to specify limits on the life time of a HELD context.

C3. "location URI cancellation: The location configuration protocol MUST support the ability to request a cancellation of a specific location URI."
Compliant conditional on on the source of the location URI: HELD contexts (Winterbottom, J., Tschofenig, H., and M. Thomson, “Location URI Contexts in HTTP-Enabled Location Delivery (HELD),” October 2009.) [I-D.winterbottom-geopriv-held-context] can be explicitly removed. HELD does not provide a method for cancelling location URIs.

C4. "Location Information Masking: The location URI form MUST, through randomization and uniqueness, ensure that any location specific information embedded within the location URI itself is kept obscure during location configuration."
Compliant: The HELD specification explicitly references this

requirement in providing guidance on the format of the location URI.

C5. "User Identity Protection: The location URI MUST NOT contain any user identifying information that identifies the user, device or address of record, (e.g., which includes phone extensions, badge numbers, first or last names, etc.), within the URI form."
Compliant: The HELD specification provides specific guidance on the anonymity of the Target with regards to the generation of location URIs. Section 6 (Security Considerations) expands on this guidance.

C6. "Reuse indicator: There SHOULD be a way to allow a client to control whether a location URI can be resolved once only, or multiple times."
Compliant: The default semantics of location URIs in HELD place no limits on the number of times that a location URI can be dereferenced.

C7. "Validity Interval Indication: A location configuration protocol MUST provide an indication of the location URI validity interval (i.e., expiry time) when present."
Duplicate Requirement: As above.

C8. "Location only: The location URI MUST NOT point to any information about the Target other than it's location."
Compliance depends on implementation: A PIDF-LO document can contain information other than location, but no protocol semantics exist that allow for or encourage inclusion of other information.

C9. "Location URI Not guessable: Where location URIs are used publicly, any location URI MUST be constructed using properties of uniqueness and cryptographically random sequences so that it is not guessable."
Compliant: HELD specifies that location URIs conform to this requirement.

C10. "Location URI Optional: In the case of user-provided authorization policies, where anonymous or non-guessable location URIs are not warranted, the location configuration protocol MAY support optional location URI forms."
Not Compliant: HELD does not support Device-specified location URI forms.

C11. "Location URI Authorization Model: The location configuration protocol SHOULD indicate whether the requested location URI conforms to the access control authorization model or the possession authorization model."

Compliant: HELD explicitly indicates that the possession model applies to all URIs.

C12. "Location URI Lifetime: A location URI SHOULD have an associated expiration lifetime (i.e., validity interval), and MUST have an validity interval if used with the possession authorization model."
Duplicate Requirement: As above.

B.2. Requirements for a Location Dereference Protocol

TOC

D1. "Location URI support: The location dereference protocol MUST support a location reference in URI form."
Compliant: HELD only provides location references in URI form.

D2. "Validity Interval Indication: A location dereference protocol MUST provide an indication of the location URI validity interval (i.e., expiry time) when present."
Invalid Requirement: not applicable to location dereference protocols.

D3. "Authentication: The location dereference protocol MUST include mechanisms to authenticate both the client and the server."
Compliant: TLS provides means for mutual authentication. This document only specifies the required mechanism for server authentication.

D4. "Dereferenced Location Form: The value returned by the dereference protocol MUST contain a well-formed PIDF-LO document."
Compliant: HELD requires that location objects are in the form of a PIDF-LO that complies with [RFC5491] (Winterbottom, J., Thomson, M., and H. Tschofenig, "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations," March 2009.).

D5. "Location URI Repeated Use: The location dereference protocol MUST support the ability for the same location URI to be resolved more than once, based on dereference server configuration."
Compliant: A Location Recipient may access and use a location URI as many times as desired until URI expiration results in the URI being invalidated. Authorization policies might include rules that modify this behavior.

D6. "Validity Interval Indication: A dereference protocol MUST provide an indication of the location URI validity interval

(i.e., expiry time) when present."
Not Compliant: This document does not provide this indication - this information is arguably useful to a Location Recipient, but it also reveals something about the policy associated with the location URI. Without also providing a mechanism to suppress this capability and hide the expiry time, this might reveal more information than a Rule Maker is willing to share.

D7. "Location URI anonymized: Any location URI whose dereference will not be subject to authentication and access control MUST be anonymized."
Not applicable to location dereference protocols - applies to the creation of the URI.

D8. "Location Information Masking: The location URI form MUST, through randomization and uniqueness, ensure that any location specific information embedded within the location URI itself is kept obscure during location URI dereferencing."
Not applicable to location dereference protocols - applies to the creation of the URI.

D9. "Location Privacy: The location dereference protocol MUST support the application of privacy rules to the dissemination of a requested location object."
Compliant: Authorization policy must be applied by the LS for all attempts at dereferencing. Note that in the case of authorization by possession, this authorization policy grants access to location information based on proof of knowledge of the location URI.

D10. "Location Confidentiality: The dereference protocol MUST support encryption of messages sent between the location dereference client and the location dereference server, and MAY alternatively provide messaging unencrypted."
Compliant: This document strongly recommends the use of TLS for confidentiality. Unsecured HTTP is permitted, and some of the associated risks are described in Section 4.1 (HELD Usage Profile).

D11. "Location URI Authorization Model: The location dereference protocol SHOULD indicate whether the requested location URI conforms to the access control authorization model or the possession authorization model."
Not Compliant: The basis of an authorization decision is potentially private information; this document does not provide this indication. Note that the recipient of a location URI is expected to respect the confidentiality of a location URI as if it were secret, even if it is not.

Authors' Addresses

TOC

	James Winterbottom
	Andrew Corporation
	PO Box U40
	University of Wollongong, NSW 2500
	AU
Phone:	+61 242 212938
EMail:	james.winterbottom@andrew.com
URI:	http://www.andrew.com/products/geometrix
	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
	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
	Martin Thomson
	Andrew Corporation
	PO Box U40
	University of Wollongong, NSW 2500
	AU
EMail:	martin.thomson@andrew.com
	Martin Dawson
	Andrew Corporation
	PO Box U40
	University of Wollongong, NSW 2500
	AU
EMail:	martin.dawson@andrew.com