Internet Engineering Task Force (IETF)
Request for Comments: 6753
Category: Standards Track
ISSN: 2070-1721

J. Winterbottom
Commscope
H. Tschofenig
Nokia Siemens Networks
H. Schulzrinne
Columbia University
M. Thomson
Microsoft

October 2012

A Location Dereference Protocol Using HTTP-Enabled Location Delivery (HELD)

Abstract

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

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6753.

Table of Contents

1. Introduction

A location URI [RFC5808] identifies a resource that contains the location of an entity. This document specifies how a holder of an "http:" or "https:" location URI uses that URI to retrieve location information using a subset of HELD functionality or an HTTP GET request.

A location URI can be acquired using a location configuration protocol, such as HTTP-Enabled Location Delivery (HELD) [RFC5985] or the Dynamic Host Configuration Protocol (DHCP) location URI option [DHCP-URI-OPT].

A Location Recipient that dereferences a location URI acquires location information in the form of a Presence Information Data Format - Location Object (PIDF-LO) document [RFC4119]. HELD parameters allow for specifying the type of location information, though some constraints are placed on allowable parameters.

Location URIs compatible with HELD dereferencing use the "https:" or "http:" scheme. HELD can be used by Location Recipients that are aware of the fact that the URI is a location URI. Mandatory support for an HTTP GET request ensures that the URI can be used even if it is not recognized as a location URI.

2. Terminology

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

This document uses key terminology from several sources:

- The terms for the GEOPRIV reference model defined are in [RFC6280].
- The term "Location Information Server (LIS)", from [RFC5687], is a node in the access network that provides location information to an endpoint. A LIS provides location URIs.
- The term "Location Server (LS)", from [RFC6280], is used to identify the role that responds to a location dereference request. A Location Server might be the same entity as the LIS, but the model in [RFC5808] allows for the existence of separate -- but related -- entities.
- The term "location URI" is coined in [RFC5808].

3. HELD Dereference Protocol

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 an "https:" or "http:" URI scheme.

This document does not describe a specific authentication mechanism. This means that authorization policies are unable to specifically identify authorized Location Recipients.

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].

The scheme of a location URI determines whether or not TLS is used on a given dereference transaction. Location Servers MUST be configured to issue only HTTPS URIs and respond to only to HTTPS dereference requests, unless confidentiality and integrity protection are provided by some other mechanism. For example, the server might only accept requests from clients within a trusted network or via an IPsec-protected channel. When TLS is used, the TLS ciphersuite TLS_NULL_WITH_NULL_NULL MUST NOT be used, and the LS MUST be authenticated [RFC6125] to ensure that the correct server is contacted.

A Location Server MAY reject a request and ask that a Location Recipient provide authentication credentials if authorization is dependent on the Location Recipient identity. Future specifications could define an authentication mechanism and a means by which Location Recipients are identified in authorization policies. This document does not provide definitions for either item.

3.1. HELD Usage Profile

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 [RFC5985].

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" and "locationType" (including the associated "exact" attribute).

Parameters and requests that do not have known behavior for dereference requests MUST NOT be used. The LS MUST ignore any parameters that it does not understand unless it knows the parameters to be invalid. If parameters are understood by the LS and known to be invalid, the LS MAY generate a HELD error response. For instance, those defined in [RFC6155] are always invalid and can be rejected.

The LS MUST NOT generate 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.

3.2. HTTP GET Behavior

GET is the method assumed by generic HTTP user agents; therefore, unless context identifies an "https:" URI as a HELD URI, such a user agent might simply send an HTTP GET. Rather than providing an HTTP 405 (Method Not Allowed) response indicating that POST is the only permitted method, a LIS MUST provide a HELD location response if it receives an HTTP GET request.

An HTTP GET request to a HELD URI produces a HELD response as if the following HELD request had been sent using HTTP POST:

```
<locationRequest xmlns="urn:ietf:params:xml:ns:geopriv:held">
  <locationType exact="false">
    geodetic civic
  </locationType>
</locationRequest>
```

Figure 1: GET Request Equivalent Location Request

HTTP GET requests MUST be safe and idempotent [RFC2616] -- that is, there are no side effects of making the request, and a repeated request has no more effect than a single request. Repeating a HELD request might result in a different location, but only as a result of a change in the state of the resource: the location of the Target.

Only the creation of a location URI as a result of receiving a request causes a HELD request to have side effects. A request to a location URI can be both safe and idempotent, since a location URI cannot be produced in response to a request to a location URI. A

Location Recipient MAY infer from a response containing the HELD content type "application/held+xml" that a URI references a resource that supports HELD.

Content negotiation MAY be supported to produce a presence document in place of a HELD location response. Where the presence document would otherwise be included in a "locationResponse" document, it can be included in the body of the HTTP response directly by including an "Accept" header that includes "application/pidf+xml".

4. Authorization Models

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. Figure 2, from [RFC5808], shows the model applicable to location configuration, conveyance, and dereference.

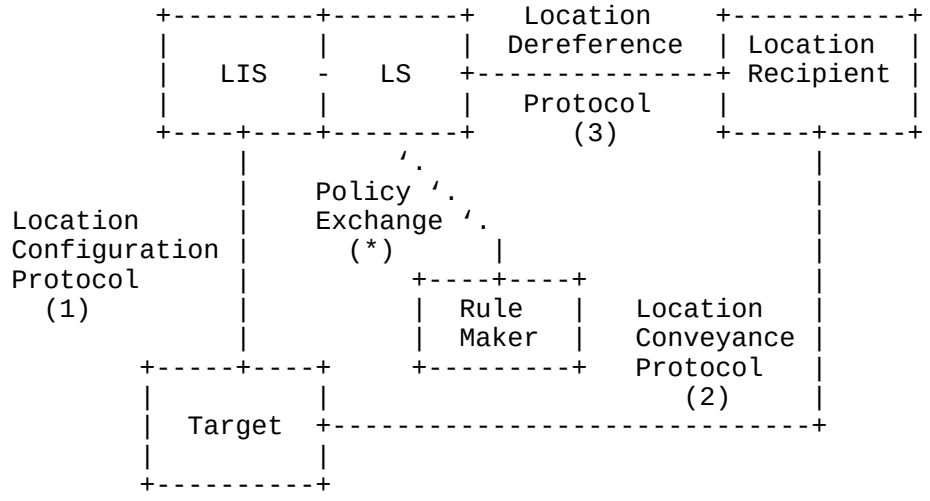

Figure 2: Communication Model

It is important to note that this document does not mandate a specific authorization model. It is possible to combine aspects of both models. However, no authentication framework is provided, which limits the policy options available when the "Authorization by Access Control" model is used.

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 uses a location configuration protocol (LCP), such as HELD or DHCP.

2. The Target then conveys the location URI to a third party, the Location Recipient (for example, using SIP as described in [RFC6442]). This step is shown in (2) of Figure 2.

3. The Location Recipient then needs to dereference the location URI in order to obtain the Location Object (3). An "https:" or "http:" URI is dereferenced as described in this document; other URI schemes might be dereferenced using another method.

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

4.1. Authorization by Possession

In this model, possession -- or knowledge -- of the location URI is used to control access to location information. A location URI might be constructed such that it is hard to guess (see C8 of [RFC5808]), and the set of entities that it is disclosed to can be limited. The only authentication this would require by the LS is evidence of possession of the URI. The LS could immediately authorize any request that indicates this URI.

Authorization by possession does not 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 [RFC5246] or S/MIME [RFC5751], protects the information from eavesdroppers.

Use of authorization by possession location URIs in a hop-by-hop protocol such as SIP [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 and location-based routing), specific treatment is important, as discussed in [RFC6442].

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. Expiration of location URIs limits the usable time for a location URI, requiring that an attacker continue to learn new location URIs to retain access to current location information.

A very simple policy might be established at the time that a 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.

4.2. Authorization via Access Control

Use of explicit access control provides a Rule Maker greater control over the behavior of an LS. In contrast to authorization by possession, possession of 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, authorization policies might be established at creation (Step 1) and need to be established 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] and Geolocation Policy [GEOPRIV-POLICY]. 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 how location information is provided to Location Recipients.

4.3. Access Control with HELD Dereference

This document does not describe a specific authentication mechanism; therefore, the authorization by access control model is not an option. Instead, this document assumes the authorization by possession model.

Other policy mechanisms, such as those described in [GEOPRIV-POLICY], can be applied for different Location Recipients if each recipient is given a different location URI. Each location URI can be assigned a different authorization policy. Selective disclosure used in this fashion can be used in place of identity-based authorization.

How policy is associated with a location URI is not defined by this document. [GEOPRIV-POLICY-URI] describes one possible mechanism.

Use of an identity-based authorization policy is not precluded. A Location Server MAY support an authentication mechanism that enables identity-based authorization policies to be used. Future specifications might define means of identifying recipients.

> Note: Policy frameworks like [RFC4745] degrade in a way that protects privacy if features are not supported. If a policy specifies a rule that is conditional on the identity of a recipient and the protocol does not (or cannot) provide an assertion identity of the recipient, the rule has no effect, and the policy defaults to providing less information.

5. Examples

An example scenario envisioned by this document is shown in Figure 3. This diagram shows how a location dereference protocol fits with location configuration and conveyance. [RFC5808] contains more information on this scenario and others like it.

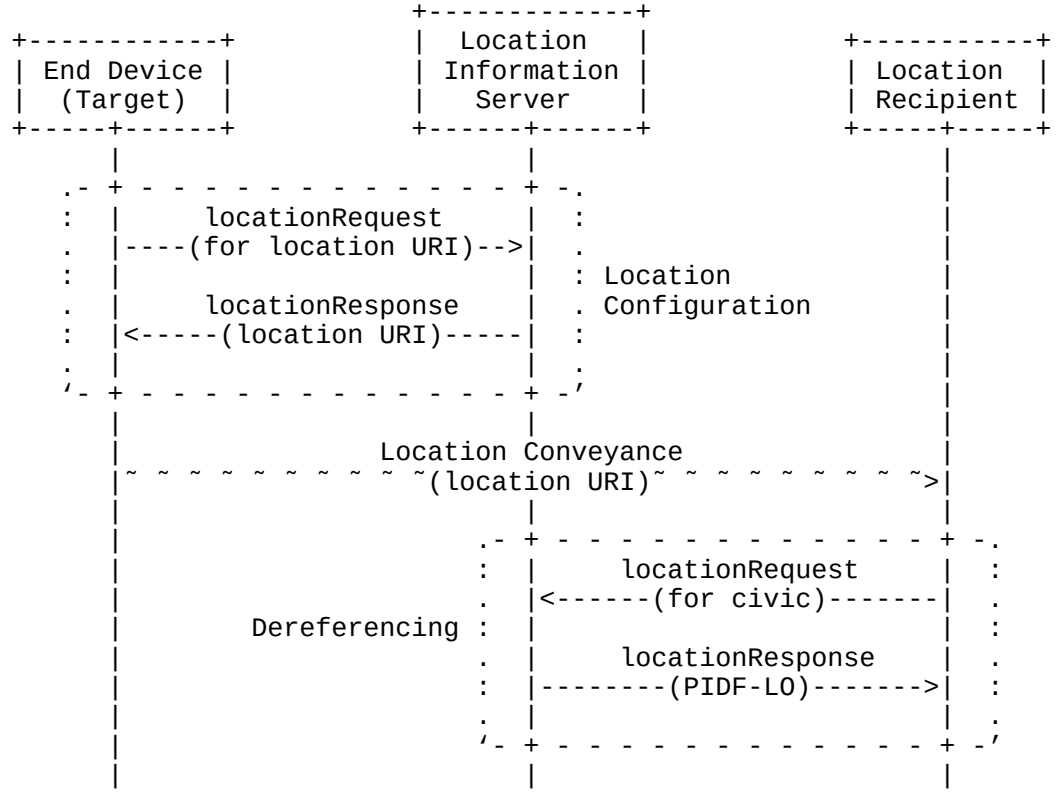

Figure 3: Example of Dereference Protocol Exchange

The example in Figure 4 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 [RFC5985] 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 4: Minimal Dereferencing Request

Figure 5 shows the response to the previous request listing both civic and geodetic location information of the Target's location. Again, this is identical to the response in Section 10.1 of [RFC5985] -- unless policy specifies otherwise, the Location Recipient receives the same information as the Device.

```
HTTP/1.1 200 OK
Server: Example LIS
Date: Mon, 10 Jan 2011 03:42:29 GMT
Expires: Tue, 11 Jan 2011 03:42:29 GMT
Cache-control: private
Content-Type: application/held+xml
Content-Length: 676

<?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"
     xmlns:gbp="urn:ietf:params:xml:ns:pidf:geopriv10:basic-policy">
    <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>
       <gbp:retransmission-allowed>
         false</gbp:retransmission-allowed>
       <gbp:retention-expiry>
         2011-01-11T03:42:29+00:00</gbp:retention-expiry>
     </usage-rules>
     <method>Wiremap</method>
   </geopriv>
  </status>
  <timestamp>2006-01-10T03:42:28+00:00</timestamp>
  </tuple>
</presence>
</locationResponse>
```

Figure 5: Response with Location Information

The following GET request is treated in an equivalent fashion. The LS treats this request as though it were a location request of the form shown in Figure 1. The same response might be provided.

```
GET /uri/w3g61nf5n66p0 HTTP/1.1
Host: ls.example.com:49152
Accept: application/held+xml
```

Figure 6: GET Request

The following GET request uses content negotiation to indicate a preference for a presence document.

```
GET /uri/w3g61nf5n66p0 HTTP/1.1
Host: ls.example.com:49152
Accept: application/pidf+xml,application/held+xml;q=0.5
```

Figure 7: GET Request with Content Negotiation

The response only differs from a normal HELD location response to a POST request in that the "locationResponse" element is omitted and the "Content-Type" header reflects the changed content.

```
HTTP/1.1 200 OK
Server: Example LIS
Date: Mon, 10 Jan 2011 03:42:29 GMT
Expires: Tue, 11 Jan 2011 03:42:29 GMT
Cache-control: private
Content-Type: application/pidf+xml
Content-Length: 591

<?xml version="1.0"?>
<presence xmlns="urn:ietf:params:xml:ns:pidf"
          entity="pres:3650n87934c@ls.example.com">
  <!-- PIDF contents are identical to the previous example -->
</presence>
```

Figure 8: GET Response with PIDF-LO

6. Security Considerations

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, [GEOPRIV-POLICY-URI] and [RFC4825].

TLS MUST be used for dereferencing location URIs unless confidentiality and integrity are provided by some other mechanism, as discussed in Section 3. 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]. Local policy determines what a Location Recipient does if authentication fails or cannot be attempted.

The authorization by possession model (Section 4.1) 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.

Location URIs MUST only be disclosed to authorized Location Recipients. The GEOPRIV architecture [RFC6280] designates the Rule Maker to authorize disclosure of the URI.

Protection of the location URI is necessary, since the policy attached to such a location URI permits anyone who has the URI to view the associated location information. This aspect of security is covered in more detail in the specification of location conveyance protocols, such as [RFC6442].

According to the requirements in [RFC5808] the LS MUST NOT provide any information about the Target except its location, unless policy from a Rule Maker allows otherwise. Thus, the Location Server MUST only provide an unlinked pseudonym in the "entity" attribute of the PIDF-LO document unless the Rule Maker policy allows for identity disclosure.

Further security considerations and requirements relating to the use of location URIs are described in [RFC5808].

7. 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. Richard Barnes made helpful observations on the application of authorization policy. Bernard Aboba and Julian Reschke contributed constructive reviews.

The participants of the GEOPRIV interim meeting 2008 provided significant feedback on this document.

James Polk provided input on security in June 2008.

Martin Dawson was an original author of this document. Sadly, he passed away prior to its publication.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[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.

[RFC4119] Peterson, J., "A Presence-based GEOPRIV Location Object Format", RFC 4119, December 2005.

[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.

[RFC5985] Barnes, M., "HTTP-Enabled Location Delivery (HELD)", RFC 5985, September 2010.

[RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, March 2011.

8.2. Informative References

[DHCP-URI-OPT] Polk, J., "Dynamic Host Configuration Protocol (DHCP) IPv4 and IPv6 Option for a Location Uniform Resource Identifier (URI)", Work in Progress, May 2012.

[GEOPRIV-POLICY]
Schulzrinne, H., Tschofenig, H., Cuellar, J., Polk, J., Morris, J., and M. Thomson, "Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information", Work in Progress, August 2012.

[GEOPRIV-POLICY-URI]
Barnes, R., Thomson, M., Winterbottom, J., and H. Tschofenig, "Location Configuration Extensions for Policy Management", Work in Progress, November 2011.

[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.

[RFC3693] Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements", RFC 3693, February 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.

[RFC4825] Rosenberg, J., "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)", RFC 4825, May 2007.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5687] Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol: Problem Statement and Requirements", RFC 5687, March 2010.

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, January 2010.

[RFC5808] Marshall, R., "Requirements for a Location-by-Reference Mechanism", RFC 5808, May 2010.

[RFC6155] Winterbottom, J., Thomson, M., Tschofenig, H., and R. Barnes, "Use of Device Identity in HTTP-Enabled Location Delivery (HELD)", RFC 6155, March 2011.

[RFC6280] Barnes, R., Lepinski, M., Cooper, A., Morris, J., Tschofenig, H., and H. Schulzrinne, "An Architecture for Location and Location Privacy in Internet Applications", BCP 160, RFC 6280, July 2011.

[RFC6442] Polk, J., Rosen, B., and J. Peterson, "Location Conveyance for the Session Initiation Protocol", RFC 6442, December 2011.

Appendix A. GEOPRIV Using Protocol Compliance

This section describes how use of HELD as a location dereference protocol complies with the GEOPRIV requirements described in [RFC3693].

Req. 1. (Location Object generalities):

This requirement relates to the PIDF-LO [RFC4119] document, which is used by HELD. These requirements are addressed by [RFC4119] and [RFC5491].

Req. 2. (Location Object fields):

This requirement relates to the PIDF-LO [RFC4119] document, which is used by HELD. These requirements are addressed by [RFC4119] and [RFC5491].

Req. 3. (Location Data Types):

This requirement relates to the PIDF-LO [RFC4119] document, which is used by HELD. These requirements are addressed by [RFC4119] and [RFC5491].

Section 7.2 of [RFC3693] details the requirements of a "Using Protocol". These requirements are restated, 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 specification describes the use of HTTP over TLS for carrying the PIDF-LO from the LS to the Location Recipient. The sending and receiving parties are expected to comply with the instructions carried inside the object.

Though discouraged, using unsecured "http:" URIs is permitted. Using unsecured HTTP is likely to result in non-compliance with this requirement.

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 [RFC2818]. Authentication of Location Recipients is based on distribution of a secret (the location URI) using a conveyance protocol (for instance, [RFC6442]), allowances are made for later work to define alternative methods.

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] is not suited to single packet transfers. Use of compressed content encoding [RFC2616] might allow this condition to be met.

Section 7.3 of [RFC3693] details the requirements of a "Rule based Location Data Transfer". These requirements are restated 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".

Compliant: 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 covered by other specifications.

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 the scope of 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] is used to convey authorization policies from Rule Maker to LS, this is possible using the parameters specified in [GEOPRIV-POLICY].

In order to comply with these rules, a Location Recipient MUST NOT redistribute a location URI without express permission. Depending on the access control model, the location URI might be secret (see Section 3.3 of [RFC5808]).

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] and [GEOPRIV-POLICY].

Req. 11. (Limited Rule language) Not Applicable: This requirement applies to (and is addressed by) PIDF-LO [RFC4119].

Section 7.4 of [RFC3693] details the requirements of "Location Object Privacy and Security". These requirements are restated where they are applicable to this document:

Req. 12. (Identity Protection) 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) the PIDF-LO does not contain information about the identity of 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 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, 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 endpoint authentication, data object integrity, data object confidentiality, and replay protection. The ability to use Transport Layer Security fulfills most of these requirements. Authentication of Location Recipients in this document relies on proof of a shared secret -- the location URI. This does not preclude the addition of more robust authentication procedures.

Req. 15. (Minimal Crypto) Compliant: The mandatory-to-implement ciphersuite is provided in the TLS layer security specification [RFC5246].

Appendix B. Compliance to Location Reference Requirements

This section describes how HELD complies to the location reference requirements stipulated in [RFC5808]. Compliance of [RFC5985] to the Location Configuration Protocol is included.

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

B.1. Requirements for a Location Configuration Protocol

C1. "Location URI support: The location 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. [GEOPRIV-POLICY-URI] provides a way to control expiration of a location URI.

C3. "Location URI cancellation: The location configuration protocol MUST support the ability to request a cancellation of a specific location URI".

Compliant with Extension: [GEOPRIV-POLICY-URI] describes how a location URI can be canceled through the application of policy. Without extensions, HELD does not provide a method for canceling location URIs.

C4. "Location Information Masking: The location URI MUST ensure, by default, through randomization and uniqueness, that the location URI does not contain location information specific components".

Compliant: The HELD specification [RFC5985] explicitly references this requirement in providing guidance on the format of the location URI.

C5. "Target Identity Protection: The location URI MUST NOT contain information that identifies the Target (e.g., user or device)".

Compliant: The HELD specification [RFC5985] provides specific guidance on the anonymity of the Target with regards to the generation of location URIs. Section 6 expands on this guidance.

C6. "Reuse indicator: There SHOULD be a way to allow a Target to control whether a location URI can be resolved once only, or multiple times".

Not Compliant: Specific extensions to the protocol or authorization policy formats are needed to alter the default behavior, which allows unlimited resolution of the location URI.

C7. "Selective disclosure: The location configuration protocol MUST provide a mechanism that allows the Rule Maker to control what information is being disclosed about the Target".

Compliant with Extension: Use of policy mechanisms and [GEOPRIV-POLICY-URI] enable this capability. Note that this document recommends that only location information be provided.

C8. "Location URI Not guessable: As a default, the location configuration protocol MUST return location URIs that are random and unique throughout the indicated lifetime. A location URI with 128-bits of randomness is RECOMMENDED".

Compliant: HELD specifies that location URIs conform to this requirement. The amount of randomness is not specifically identified since it depends on a number of factors that change over time, such as the number of valid location URIs, the validity period of those URIs, and the rate that guesses can be made.

C9. "Location URI Options: In the case of user-provided authorization policies, where anonymous or non-guessable location URIs are not warranted, the location configuration protocol MAY support a variety of optional location URI conventions, as requested by a Target to a location configuration server, (e.g., embedded location information within the location URI)".

Not Compliant: HELD does not support Device-specified location URI forms.

B.2. Requirements for a Location Dereference Protocol

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. "Authentication: The location dereference protocol MUST include mechanisms to authenticate both the client and the server".

Partially Compliant: TLS provides means for mutual authentication. This document only specifies the required mechanism for server authentication. Client authentication is not precluded.

D3. "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].

D4. "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.

D5. "The location dereference protocol MUST support confidentiality protection of messages sent between the Location Recipient and the location server".

Compliant: This document strongly recommends the use of TLS for confidentiality, and HELD mandates its implementation. Unsecured HTTP is permitted: the associated risks are described in Section 3.

Authors' Addresses

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

Phone: +61 242 212938
EMail: james.winterbottom@commscope.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

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

Phone: +1 212 939 7042
EMail: hgs@cs.columbia.edu
URI: http://www.cs.columbia.edu

Martin Thomson
Microsoft
3210 Porter Drive
Palo Alto, CA 94304
USA

Phone: +1 650-353-1925
EMail: martin.thomson@skype.net