Geopriv
Internet-Draft
Intended status: Standards Track
Expires: January 6, 2009

J. Winterbottom
Andrew Corporation
H. Tschofenig
Nokia Siemens Networks
H. Schulzrinne
Columbia University
M. Thomson
M. Dawson
Andrew Corporation
July 5, 2008

An HTTPS Location Dereferencing Protocol Using HELD
draft-winterbottom-geopriv-deref-protocol-01.txt

Status of this Memo

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 into 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.

Table of Contents

1. Introduction

This document describes how to transport Presence Information Data Format Location Object (PIDF-LO) when dereferencing a location URI in the form of a secure HELD URI (held: URI scheme) [1]. This held: URI indicates that the XML-based HELD messages are carried on top of the Hypertext Transfer Protocol (HTTP), which is secured using Transport Layer Security (TLS) ([2] and [3]).

The document describes how HELD [1] is used to request and to receive location information in a way that also satisfies the requirements laid out in [7]. HELD provides location information in the form of a PIDF-LO (see [4]) which, as part of its definition, complies with the requirements of a location object as described in [8].

To use 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 [1]. 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.

The general usage scenario envisioned by this document is shown in Figure 1. While the figure shows a typical HELD location request being made to initially obtain the location URI. As Figure 1 indicates, an alternative Location Configuration Protocol (LCP) that can provide a HELD URI can be used.

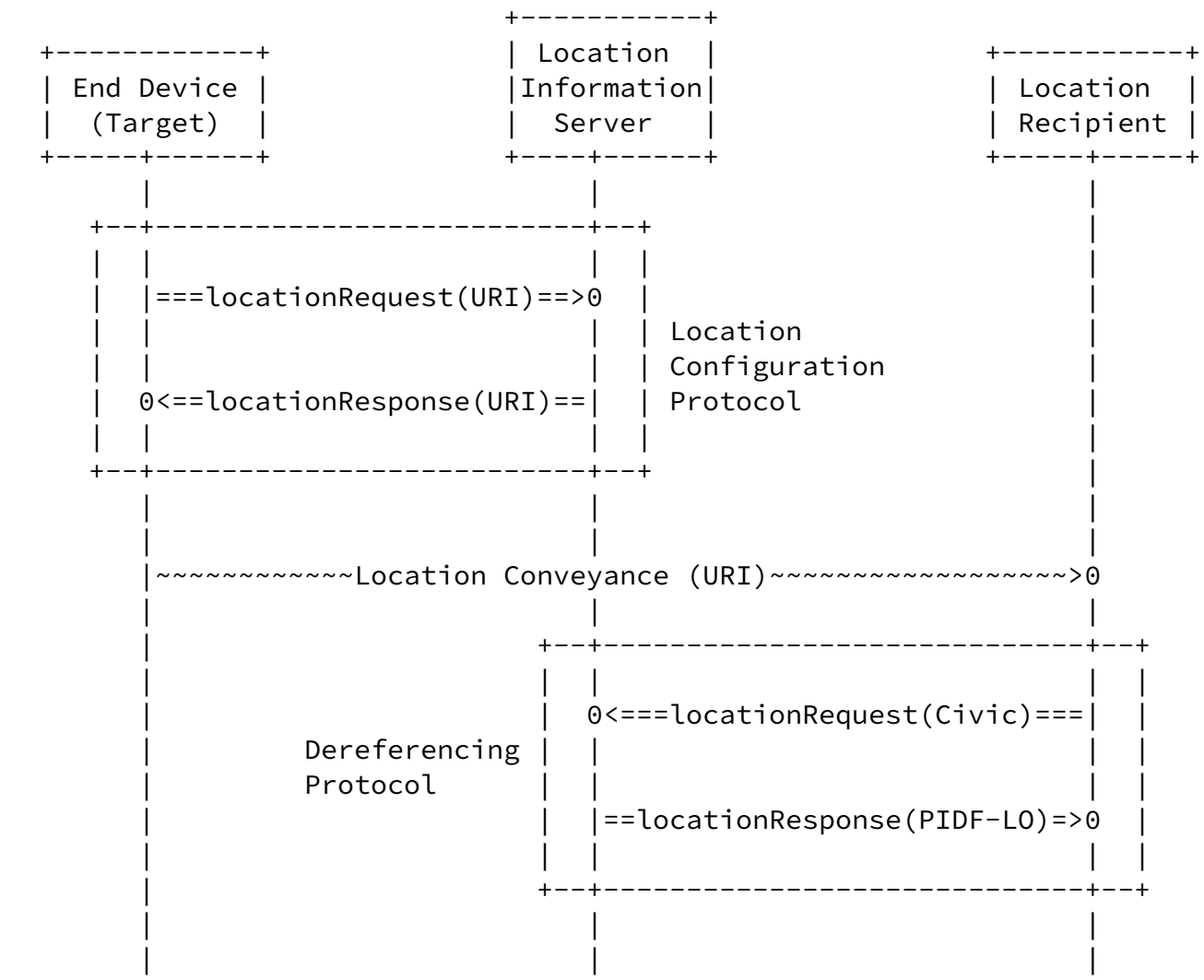

End Device (Target)
Location Information Server
Location Recipient
===locationRequest(URI)==>
<==locationResponse(URI)==
Location Configuration Protocol
~~~~~~~~~~~~~Location Conveyance (URI)~~~~~~~~~~~~~~~~~~>
<===locationRequest(Civic)===
==locationResponse(PIDF-LO)=>
Dereferencing Protocol
~~~~~~~~~~~~~

Figure 1: Example of Dereference Protocol Exchange

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 [5].

The key conventions and terminology used in this document are defined as follows:

This document reuses the term Target, as defined in [8].

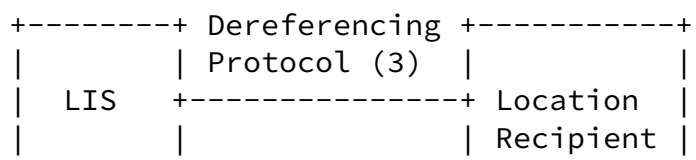
This document uses the term Location Information Server, LIS, as the node in the access network providing location information to an end point, or to the node dereferencing a location URI. This term is also used in [9].

The Location Recipient acts as a HELD client and the LIS as a HELD server in the context of this document.

Many architectural descriptions related to the updated terminology of RFC 3693 can be found in [10].

3. Authorization Models

This section discusses two extreme types of authorization models for dereferencing with HELD URIs, namely "Authorization by Possession" and "Authorization via Access Control Lists". 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 shows the communication model relevant for this discussion. It is a simplified version of Figure 1 from [7].



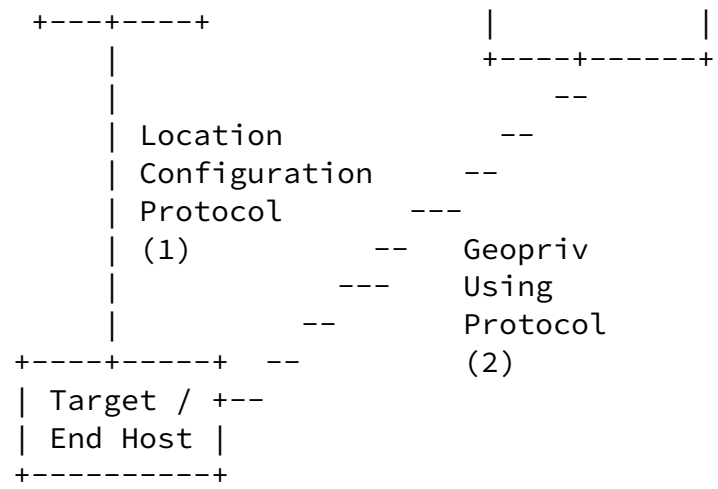


Figure 2: Communication Model

3.1. Authorization by Possession

With this type of authorization model the communication steps with respect to Figure 2 are as follows. We focus on the description of the case where the Location URI is dereferenced by an entity other than the Target.

1. The Target discovers the LIS.

2. The Target sends a request to the LIS asking for a location-by-reference, as shown in (1) of Figure 2.

3. The LIS responds to the request and returns a Location URI. This reference fullfills the requirements indicated in [7], in particular it must be non-guessable (see requirement C9 of [7]).

4. The Target then conveys the Location URI to a third party, the Location Recipient (for example using SIP as described in [11]). This step is shown in (2) of Figure 2.

5. The Location Recipient then needs to dereference the Location URI in order to obtain the Location Object. Depending on the URI scheme of the Location URI this might, for example in case of a HELD URI, be done as described in this document.

The last step where the LIS has to decide whether to resolve the reference and to return the Location Object to the entity asking for it is important. With this authorization model there is the assumption that the possession of the Location URI by the Location Recipient alone is sufficient, from an authorization point of view, to grant access to the Location Object that is being referenced by the Location URI. As such, the Location Recipient authenticates the LIS using TLS server-side authentication but no authentication from the Location Recipient point of view is demanded.

A few aspects are worth further discussion when the Target would like to avoid unrestricted disclosure of it's location information. First, the Target is able to control the disclosure of location information by making the Location URI available only to trusted entities. Second, in order to deal with adversary along the signaling path between the Target and the Location Recipient the properties of the using protocol need to be taken advantage of. For example, the Location URI may be encrypted end-to-end using S/MIME and consequently only the entity that is able to decrypt the protected object can resolve the reference. 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 [11].

3.2. Authorization via Access Control Lists

In this model the communication steps are slightly different, as shown below.

1. The procedure again starts with the Target performing the LIS discovery procedure.

2. The Target sends a request to the LIS asking for a location-by-reference, as shown in (1) of Figure 2.

3. Before handing out the reference the Target uploads authorization policies to the LIS that aim to control access to the dereferencing step. A possible format for these authorization policies is available with GEOPRIV Common Policy [12] and

Geolocation Policy [13]. Additional policies are described in

[14] that allow constraints to be placed on the dereferencing procedure to limit the location information being exposed to Location Recipients.

4. The LIS responds to the request and returns a Location URI. With the uploaded authorization policies in place there are no requirements for the Location URI to be non-guessable.

5. The Target then conveys the Location URI to a third party, the Location Recipient (for example using SIP as described in [11]). This step is shown in (2) of Figure 2.

6. The Location Recipient then needs to dereference the Location URI in order to obtain the Location Object. Depending on the specific content of the authorization policies (such as identity-based conditions in the policy rule set) the Location Recipient has to be authenticated in order to allow the authorization check to continue.

It is important to note that this document does not mandate a specific authorization model nor does it constraint the usage with regard to these models in any way. Additionally, it is possible to combine certain parts of both models.

4. Steps for Retrieval

When a Location Recipient obtains a Location URI with the "held:" URI scheme then the following steps for dereferencing the Location URI are being executed:

1. The Location Recipient, acting as a HELD client, determines the IP address of the LIS based on the obtained Location URI following the procedure described in Section 3 of [15].

2. The HELD client establishes a TLS connection to the LIS, as described in [3]. The TLS ciphersuite TLS_NULL_WITH_NULL_NULL MUST NOT be used.

3. When certificate based authentication is used the client authenticates the server and compares the domain part of the Location URI with the identity information in the certificate.

4. The server MAY require the client to be authenticated. This could, for example, be useful in deployment environments where certain Location Recipients are granted access to location information only or where access control rules have to be executed as part of the authorization procedure. Various authentication mechanisms for HTTP exist and this document does not restrict them in any way since the preferred mechanism may be deployment specific.

5. The client retrieves the PIDF-LO document encapsulated into the HELD locationResponse or an error message conveyed in a HELD error message.

The subsequent text describes how HELD protected by TLS can be used to qualify location requests to the LIS. Only a subset of HELD functionality is required and is described in the following paragraphs. The HELD based dereferencing step provides ways to tell the LIS what information is desired and allows the LIS to communicate additional information back to the client.

The <locationType> element allows location to be requested in a specific form, such as civic or geodetic location information. The Location Recipient SHOULD NOT request location as a locationURI. The LIS MUST respond with a "requestError" if it receives a request for a locationURI where HELD is being used as a dereference protocol. Location information provided by the LIS MUST correspond to the rules and guidelines in [6]. If the requested form of location violates any authorization policies known to the LIS, then the LIS MUST

respond with a "cannotProvideLiType" error.

The LIS will provide location information on request even if the location information does not fit the form requested. This stems from the premise that some location is better than no location. HELD provides a means for the requestor to modify this behaviour and instruct the LIS to return an error if location information is not available in the form requested. This is done using the "exact" attribute.

Location systems often have more than one location determination mechanism at their disposal. Differing determination techniques provide different degrees of accuracy over differing periods of time. Generally, more accurate determination techniques require more time. HELD addresses this trade-off by allowing the requestor to specify how long they are prepared to wait for a location result. This allows the LIS to select the most accurate determination technique at its disposal that can return a result in the specified time. The HELD attribute for specifying this value is the "responseTime" attribute and MAY be used by a Location Recipient to specify their preference for the accuracy-time trade-off.

The LIS MUST support the HELD locationRequest semantic using an HTTP GET as described in [1]. The usage of HTTP POST is optional.

Where the LIS is unable to process the Location Recipient's request, it MUST return the appropriate error from the existing HELD error set defined in [1].

5. Examples

This example in Figure 3 shows the most basic rereferencing request for a LO. This uses the GET feature described by the HTTP binding from Section 9 of [1]. This example assumes that the LO is available for retrieval at the URL "https://lis.example.com/357yc6s64ceyoiuy5ax3o".

```
GET /357yc6s64ceyoiuy5ax3o HTTP/1.1
Host: lis.example.com
Accept:application/held+xml,
       application/xml;q=0.8,
       text/xml;q=0.7
Accept-Charset: UTF-8,*
```

Figure 3: Minimal GET Dereferencing Request

The GET request is exactly identical to a minimal POST request that includes an empty "locationRequest" element.

```
POST /357yc6s64ceyoiuy5ax3o HTTP/1.1
Host: lis.example.com
Accept: application/held+xml,
        application/xml;q=0.8,
        text/xml;q=0.7
Accept-Charset: UTF-8,*
Content-Type: application/held+xml
Content-Length: 87

<?xml version="1.0"?>
```

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

Figure 4: Minimal POST Dereferencing Request

Figure 5 shows a request indicating that both civic and geodetic location information has to be returned. If it cannot be provided, the request fails.


```
POST /357yc6s64ceyoiuy5ax3o HTTP/1.1
Host: lis.example.com
Accept: application/held+xml,
    application/xml;q=0.8,
    text/xml;q=0.7
Accept-Charset: UTF-8,*
Content-Type: application/held+xml
Content-Length: 87

<?xml version="1.0"?>
<locationRequest xmlns="urn:ietf:params:xml:ns:geopriv:held">
  <locationType exact="true">
    civic
    geodetic
  </locationType>
</locationRequest>
```

Figure 5: Dereferencing POST Request for Civic and Geodetic Location Information

Figure 6 shows the response to the previous request listing both civic and geodetic location information of the Target's location.

```
HTTP/1.x 200 OK
```

```
Server: Example LIS
Date: Tue, 10 Jan 2006 03:42:29 GMT
Expires: Tue, 10 Jan 2006 03:49:20 GMT
Content-Type: application/held+xml
Content-Length: XYZ

<?xml version="1.0"?>
<locationResponse xmlns="urn:ietf:params:xml:ns:geopriv:held">
  <presence xmlns="urn:ietf:params:xml:ns:pidf:geopriv10"
    entity="pres:ae3be8585902e2253ce2@10.102.23.9">
    <tuple id="lisLocation">
      <status>
        <geopriv>
          <location-info>
            <gs:Circle
              xmlns:gs="http://www.opengis.net/pidflo/1.0"
              xmlns:gml="http://www.opengis.net/gml"
              srsName="urn:ogc:def:crs:EPSG::4326">
              <gml:pos>-34.407242 150.882518</gml:pos>
              <gs:radius uom="urn:ogc:def:uom:EPSG::9001">30
              </gs:radius>
            </gs:Circle>
            <ca:civicAddress
```



```
              ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
              xml:lang="en-au">
              <ca:country>AU</ca:country>
              <ca:A1>NSW</ca:A1>
              <ca:A3>Wollongong</ca:A3>
              <ca:A4>Gwynneville</ca:A4>
              <ca:STS>Northfield Avenue</ca:STS>
              <ca:LMK>University of Wollongong</ca:LMK>
              <ca:FLR>2</ca:FLR>
              <ca:NAM>Andrew Corporation</ca:NAM>
              <ca:PC>2500</ca:PC>
              <ca:BLD>39</ca:BLD>
              <ca:SEAT>WS-183</ca:SEAT>
              <ca:POBOX>U40</ca:POBOX>
            </ca:civicAddress>
          </location-info>
          <usage-rules>
            <retransmission-allowed>false</retransmission-allowed>
```

```
            <retention-expiry>2007-05-25T12:35:02+10:00
            </retention-expiry>
          </usage-rules>
          <method>Wiremap</method>
        </geopriv>
      </status>
      <timestamp>2007-05-24T12:35:02+10:00</timestamp>
    </tuple>
  </presence>
</locationResponse>
```

Figure 6: Response with Civic and Geodetic Location Information

Figure 7 shows an error message returned in response to a request.

```
HTTP/1.x 200 OK
Server: Example LIS
Expires: Tue, 10 Jan 2006 03:49:20 GMT
Content-Type: application/held+xml
Content-Length: XYZ

<error xmlns="urn:ietf:params:xml:ns:geopriv:held"
 code="cannotProvideLiType"
message="Authorization policies do not permit
         location information to be disclosed."/>
```

Figure 7: Error Message

6. Security Considerations

This document assumes that the use of TLS to protect HTTP is sufficient to protect the privacy of the PIDF-LO content while in flight. When access control at the LIS is not applied, as described in Section 3.1, then the possession of the location URI is equal to the possession of location information. When the requirements for creating a location URI, as described in [7], are met, then the reference provides sufficiently high security guarantees for most location-based applications. Furthermore, the ability of the Rule Maker to put constraints on the dereferencing step, as described in

[14], provides the ability to restrict how often location can be accessed through a location URI, how long the URI is valid for, and the type of location information returned when a location URI is accessed. If this is still not sufficient then the Target is able to put authorization policies either to the LIS or uploads the Location URI to a presence server that hosts authorization policies, as described in [16].

Connection establishment from the Location Recipient to the LIS will be made using HTTP over TLS, and the location URI being dereferenced by the Location Recipient will contain the hostname of the LIS. The Location Recipient MUST check the FQDN of the LIS in the reference with the identity presented in the server's certificate. A discrepancy may indicate a possible man-in-the-middle-attack, and the Location Recipient should take appropriate action based on application dependent semantics. Actions may include but are not limited to; proceeding anyway, flagging the result as suspect, or giving up.

In some applications the Location Recipient has a pre-established relationship with one or several Location Information Servers and hence the LIS might authorize only certain Location Recipients might be allowed to resolve a reference.

7. IANA Considerations

There are no specific IANA considerations for this document.

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

9.1. Normative References

[1] Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, "HTTP Enabled Location Delivery (HELD)", draft-ietf-geopriv-http-location-delivery-07 (work in progress), April 2008.

[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] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

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

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

[6] Winterbottom, J., Thomson, M., and H. Tschofenig, "GEOPRIV PIDF-LO Usage Clarification, Considerations and Recommendations", draft-ietf-geopriv-pdif-lo-profile-11 (work in progress), February 2008.

9.2. Informative references

[7] Marshall, R., "Requirements for a Location-by-Reference Mechanism", draft-ietf-geopriv-lbyr-requirements-02 (work in progress), February 2008.

[8] Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements", RFC 3693, February 2004.

[9] Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol; Problem Statement and Requirements", draft-ietf-geopriv-l7-lcp-ps-08 (work in progress), June 2008.

[10] Barnes, R., Lepinski, M., Tschofenig, H., and H. Schulzrinne,

"Security Requirements for the Geopriv Location System", draft-barnes-geopriv-lo-sec-02 (work in progress), February 2008.

[11] Polk, J. and B. Rosen, "Location Conveyance for the Session Initiation Protocol", draft-ietf-sip-location-conveyance-10 (work in progress), February 2008.

[12] 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.

[13] 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-17 (work in progress), June 2008.

[14] Winterbottom, J., Tschofenig, H., and M. Thomson, "HELD Protocol Context Management Extensions", draft-winterbottom-geopriv-held-context-02 (work in progress), February 2008.

[15] Thomson, M. and J. Winterbottom, "Discovering the Local Location Information Server (LIS)", draft-ietf-geopriv-lis-discovery-01 (work in progress), June 2008.

[16] Garcia-Martin, M., Tschofenig, H., and H. Schulzrinne, "Indirect Presence Publication with the Session Initiation Protocol(SIP)", draft-garcia-simple-indirect-presence-publish-00 (work in progress), February 2008.

Appendix A. GEOPRIV Using Protocol Compliance

This section compares the GEOPRIV requirements described in [8] with the approach outlined in this document.

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 [4] allows both civic and geospatial location information to be expressed. Combining this with [6] ensures that location can be constructed and interpreted in a consistent manner.

- 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 [4]) 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 LIS 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.

- 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 used 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 and to indicate which location format has to be returned.

- Regarding requirement 2.7, the PIDF-LO relevant elements and attributes are available.

- Regarding requirement 2.8, provision exists for a reference to an external (more detailed rule set) within the PIDF-LO to be made. This is the <external-ruleset> element.

- 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, [4] defines geospatial location information as the mandatory to implement location format. [6] describes in more detail the acceptable forms of geolocation and its interaction with civic notations.

- With the support of civic and geodedic location information in [4] the requirement 3.2 is fulfilled.

- Regarding requirement 3.3, rules described in [13] apply to an absolute geodetic point. Geodetic information expressed in a PIDF-LO that complies with [6] may express an area or volume there-by "fuzzing" the location of the Target.

- Regarding requirement 3.4, since the PIDF-LO format is designed to be extensible it allows further location information types to be defined in the future.

Section 7.2 of [8] 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 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. 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 [8] details the requirements of a "Rule based Location Data Transfer". These requirements are listed below:

Req. 7. (LS Rules): Access to location information is controlled by allowing the Target (or by an entity on behalf of the Target) to indicate to which Location Recipients the short-lived location URI that contains a unguessable random component. Additionally, constraints can be put on the dereferencing step by the Target.

Req. 8. (LG Rules): In context of location URI it is not possible that there is no relationship between the Location Generator and the Location Information Server. As such, the statement made in Requirement 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 [13]. These rules are, however, best used when the location URI is not directly provided to Location Recipients

but rather to an intermediary that stores these authorization policies, such as a location-based presence server.

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 [12] and [13]. These rules may be used in a larger context but this document does not define their usage.

Req. 11. (Limited Rule language): A limited (or basic) ruleset was introduced with PIDF-LO [4]).

Section 7.4 of [8] details the requirements of "Location Object Privacy and Security". These requirements are listed below:

Req. 12. (Identity Protection): Identity protection of the Target can be provided if both the following conditions are true:

(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 LIS which identity information to include 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: The mandatory to implement ciphersuite is provided in the TLS layer security specification.

Appendix B. HELD Compliance to IETF Location Reference Requirements

This section describes how HELD complies to the location reference requirements stipulated in [7].

High-level requirements for a location configuration protocol.

C1. "Location URI support - LCP: The configuration protocol MUST support a location reference in URI form."

COMPLY. HELD only provides location references in URI form.

C2. "Location URI expiration: The LCP MUST support the ability to specify to the server, the length of time that a location URI will be valid."

COMPLY. basic HELD supports the LIS informing the Target of the location URI expiry time. HELD context management extension [14] provides the Target the ability to specify exipry times for location URIs.

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

COMPLY. HELD context management extension [14] provides the Target the ability to void location URIs when required.

C4. "Random Generated: The location URI MUST be hard to guess, i.e., it MUST contain a cryptographically random component."

COMPLY. The HELD specification provides specific guidance on the security surrounding location URI generation.

C5. "Identity Protection - LCP: The location URI MUST NOT contain

any information that identifies the user, device or address of record within the URI form."

COMPLY. The HELD specification provides specific guidance on the anonymity of the Target with regards to the generation of

location URIs.

C6. "Reuse flag default: The LCP MUST support the default condition of a requested location URI being repeatedly reused."

COMPLY. The default semantics of location URIs in HELD place no limits on the number of times that a location URI can be dereferenced.

C7. "One-time-use: The LCP MUST support the ability for the client to request a 'one-time-use' location URI (e.g., via a reuse flag setting)."

COMPLY. HELD context management extension [14] provides the Target the ability to set the number of times that a location URI may yield the Target's location.

High-level requirements for a location dereference protocol.

D1. "Location URI support - LDP: The LDP MUST support a location reference in URI form."

COMPLY. HELD only provides location references in URI form.

D2. "Location URI expiration status: The LDP MUST support a message indicating that for a location URI which is no longer valid, that the location URI has expired."

COMPLY. HELD indicates to the requestor that location for the URI cannot be provided by returning a locationUnknown error when a location URI is found to have expired.

D3. "Authentication: The LDP MUST support either client-side and server-side authentication between client and server."

COMPLY. Client authentication may be provided using a variety of techniques. However, this document does not mandate a specific procedure nor does it specify the format of

authorization policies that may be in place to control access at the LIS. The server authenticates itself using the methods described in HTTP on TLS [3].

D4. "Dereferenced Location Form: Location URI dereferencing MUST result in a well-formed PIDF-LO."

COMPLY. HELD when used as a dereference protocol MUST provide location information as a PIDF-LO that complies with [6] as described in Section 4.

D5. "Repeated use: The LDP MUST support the ability for the same location URI to be resolved more than once, based on server settings and LCP parameters."

COMPLY. A Location Recipient may access and use a location URI as many times as desired until such time as the URI expires due to age, or is made invalid by other Target policies on the LIS.

D6. "Updated location: The LDP MUST support the ability for the same location URI to be resolved into a continuum of location values (e.g., location updates)."

COMPLY. Using base-HELD the location of the Target is determined each time that URI is accessed.

D7. "Location form: The LDP MUST support dereferenced location in both coordinate and civic forms."

COMPLY. HELD provide the locationType parameter allowing the Location Recipient the ability to specify the form of location they require.

Authors' Addresses

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

Full Copyright Statement

Intellectual Property