GEOPRIV WG
Internet-Draft
Intended status: Standards Track
Expires: August 25, 2008

M. Barnes, Ed.
Nortel

February 22, 2008

HTTP Enabled Location Delivery (HELD)
draft-ietf-geopriv-http-location-delivery-05.txt

Status of this Memo

Copyright Notice

Abstract

A Layer 7 Location Configuration Protocol (L7 LCP) is described that is used for retrieving location information from a server within an access network. The protocol includes options for retrieving location information in two forms: by value and by reference. The protocol is an extensible application-layer protocol that is independent of session-layer. This document describes the use of

Hypertext Transfer Protocol (HTTP) as a transport for the protocol.

Table of Contents

1. Introduction

The location of a Device is information that is useful for a number of applications. The L7 Location Configuration Protocol (LCP) problem statement and requirements document [13] provides some scenarios in which the Device might rely on its access network to provide location information. The LIS service applies to access networks employing both wired technology (e.g. DSL, Cable) and wireless technology (e.g. WiMAX) with varying degrees of Device mobility. This document describes a protocol that can be used to acquire Location Information (LI) from a Location Information Server (LIS) within an access network.

This specification identifies two types of location information that may be retrieved from the LIS. Location may be retrieved from the LIS by value, that is, the Device may acquire a literal location object describing the location of the Device. The Device may also request that the LIS provide a location reference in the form of a location URI or set of location URIs, allowing the Device to distribute its LI by reference. Both of these methods can be provided concurrently from the same LIS to accommodate application requirements for different types of location information.

This specification defines an extensible XML-based protocol that enables the retrieval of LI from a LIS by a Device. This protocol can be bound to any session-layer protocol, particularly those capable of MIME transport. This document describes the use of Hypertext Transfer Protocol (HTTP) as a transport for the protocol.

2. Conventions & 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 [1].

This document uses the terms (and their acronym forms) Access Provider (AP), Location Information (LI), Location Object (LO), Device, Target, Location Generator (LG), Location Recipient (LR), Rule Maker (RM) and Rule Holder (RH) as defined in RFC 3693, GEOPRIV Requirements [8] . The terms Location Information Server (LIS), Access Network, Access Provider (AP) and Access Network Provider are used in the same context as defined in the L7 LCP Problem statement and Requirements document [13]. The usage of the terms, Civic Location/Address and Geodetic Location follows the usage in many of the referenced documents.

In describing the protocol, the terms "attribute" and "element" are

used according to their context in XML. The term "parameter" is used in a more general protocol context and can refer to either an XML "attribute" or "element".

3. Overview and Scope

This document describes an interface between a Device and a Location Information Server (LIS). This document assumes that the LIS is present within the same administrative domain as the Device (e.g., the access network). An Access Provider (AP) operates the LIS so that Devices (and Targets) can retrieve their LI. The LIS exists because not all Devices are capable of determining LI, and because, even if a device is able to determine its own LI, it may be more efficient with assistance. This document does not specify how LI is determined.

This document is based on the attribution of the LI to a Device and not specifically a person (end user) or Target, based on the premise that location determination technologies are generally designed to locate a device and not a person. It is expected that, for most applications, LI for the device can be used as an adequate substitute for the end user's LI. Since revealing the location of the device almost invariably reveals some information about the location of the user of the device, the same level of privacy protection demanded by a user is required for the device. This approach may require either some additional assurances about the link between device and target, or an acceptance of the limitation that unless the device requires active user authentication, there is no guarantee that any particular individual is using the device at that instant.

The following diagram shows the logical configuration of some of the functional elements identified in [8] and the LIS defined in [13] and where this protocol applies, with the Rule Maker and Target represented by the role of the Device.

```
                     +---------------------------------------------+
                     | Access Network Provider                     |
                     |                                             |
                     |   +--------------------------------------+  |
                     |   | Location Information Server          |  |
                     |   |                                      |  |
                     |   |                                      |  |
                     |   |                                      |  |
                     |   |                                      |  |
                     |   +------|---------------------'---------+  |
                     +----------|---------------------'------------+
                                |                     '
                                |                     '
                               HELD                  APP
                                |                     '
     Rule Maker   - _     +-----------+         +-----------+
           o          - - | Device    |         | Location  |
          <U\             |           | - - - - | Recipient |
          / \       _ - - |           |   APP   |           |
         Target - -       +-----------+         +-----------+
```

Figure 1: Significant Roles

The interface between the Location Recipient (LR) and the Device and/or LIS is application specific, as indicated by the APP annotation in the diagram and it is outside the scope of the document. An example of an APP interface between a device and LR can be found in the SIP Location Conveyance document [25].

4. Protocol Overview

The HELD protocol facilitates retrieval of location directly in the form of a PIDF-LO document (by value) and indirectly as a Location URI (by reference). The policy that describes to whom, and how, LI is granted is outside the scope of this document and may be specified in separate specifications as required.

As described in the L7 LCP problem statement and requirements [13], the Device must first discover the URI for the LIS for sending the HELD protocol requests. The discovery methods are specified in [16].

For the HELD protocol requests, the LIS uses the source IP address of the request sent from the Device as the identifier in determining the location of the device. The use of additional identifiers for the HELD protocol is outside the scope of this document.

4.1. Location by Value

Where a Device requires LI directly, it can request that the LIS create a PIDF-LO document. This approach fits well with a configuration whereby the device directly makes use of the provided PIDF-LO document. The details on the information that may be included in the PIDF-LO MUST follow the subset of those rules relating to the construction of the "location-info" element in the PIDF-LO Usage Clarification, Considerations and Recommendations document [12]. Further detail is included in the detailed protocol section of this document Section 6

4.2. Location by Reference

Requesting location directly does not always address the requirements of an application. A Device can request a location URI instead of literal location. A Location URI is a URI [22] of any scheme, which a Location Recipient (LR) can use to retrieve LI. A location URI provided by a LIS can be assumed to be globally-addressable; that is, anyone in possession of the URI can access the LIS. However, this does not in any way suggest that the LIS is bound to reveal the location associated with the location URI. This issue is deemed out of scope for this document. The merits and drawbacks of using a Location URI approach are discussed in [17].

4.3. Device Identifiers, NAT and VPNs

Use of the HELD protocol is subject to the viability of the identifier used by the LIS to determine location. This document describes the use of the source IP address sent from the Device as the identifier used by the LIS. When Network Address Translation (NAT), a Virtual Private Network (VPN) or other forms of address modification occur between the Device and the LIS the location returned could be inaccurate.

Not all cases of NATs introduce inaccuracies in the returned location. For example, a NAT used in a residential Local Area Network (LAN) is typically not a problem. The external IP address used on the Wide Area Network (WAN) side of the NAT is an acceptable identifier for all of the devices in the residence, on the LAN side of the NAT, since the covered geographical area is small.

On the other hand, if there is a VPN between the Device and the LIS,

for example for a teleworker, then the IP address seen by a LIS inside the enterprise network might not be the right address to identify the location of the Device. Section 4.3.2 provides recommendations to address this issue.

4.3.1. Devices and VPNs

To minimize the impact of VPNs, Devices should perform their HELD query prior to establishing a VPN tunnel. It is RECOMMENDED that discovery [16] and an initial query are performed before establishing the VPN. If a Device performs the HELD query after establishing the VPN tunnel the Device may receive inaccurate location information.

Devices that establish VPN connections for use by other devices inside a LAN or other closed network could serve as a LIS, that implements the HELD protocol, for those other Devices. Devices within the closed network are not necessarily able to detect the presence of the VPN and rely on the VPN device. To this end, a VPN device should provide the address of the LIS server it provides, in response to discovery queries, rather than passing such queries through the VPN tunnel.

It could also be useful for a VPN device to serve as a LIS for other location configuration options such as Dynamic Host Configuration Protocol (DHCP)[23] or Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) [27]. VPN devices that serve as a LIS may acquire their own location using HELD.

4.3.2. LIS Handling of NATs and VPNs

In the cases where the Device connects to the LIS through a VPN or a NAT that serves a large geographic area or multiple geographic locations (for example, a NAT used by an enterprise to connect their private network to the Internet), the LIS might not be able to return an accurate LI. If the LIS cannot determine an accurate LI, it should not provide location information to the requesting device. The LIS needs to be configured to recognize identifiers that represent these conditions.

LIS operators have a large role in ensuring the best possible environment for location determination. The LIS operator needs to ensure that the LIS is properly configured with identifiers that fall within NATs and VPNs. In order to serve a Device on a remote side of a NAT or VPN a LIS needs to have a presence on the side of the NAT or VPN nearest the Device.

5. Protocol Description

As discussed in Section 4, this protocol provides for the retrieval of the device's location in the form of a PIDF-LO document and/or Location URI(s) from a LIS. Three messages are defined to support the location retrieval: locationRequest, locationResponse and error. Messages are defined as XML documents.

The Location Request (locationRequest) message is described in Section 5.2. A Location Request message from a Device indicates whether location in the form of a PIDF-LO document (with specific type(s) of location) and/or Location URI(s) should be returned. The LIS replies with a locationResponse message, including a PIDF-LO document and/or one or more Location URIs in case of success. In the case of an error, the LIS replies with an error message.

A MIME type "application/held+xml" is registered in Section 12.3 to distinguish HELD messages from other XML document bodies. This specification follows the recommendations and conventions described in [20], including the naming convention of the type ('+xml' suffix) and the usage of the 'charset' parameter.

Section 6 contains a more thorough description of the protocol parameters, valid values, and how each should be handled. Section 7 contains a more specific definition of the structure of these messages in the form of an XML Schema [14].

5.1. Delivery Protocol

The HELD protocol is an application-layer protocol specified by an XML document. The HELD protocol is defined independently of any lower layers used to transport messages from one host to another. This means that any protocol can be used to transport this protocol providing that it can provide a few basic features:

- o The HELD protocol doesn't provide any mechanisms that enable detection of missing messages and retransmission, thus the protocol must have acknowledged delivery.
- o The HELD protocol is a request, response protocol, thus the protocol must be able to correlate a response with a request.
- o The HELD protocol must provide authentication, confidentiality and protection against modification per Section 10.2.

This document describes the use of a combination of HTTP [3], TLS [2] and TCP [18] in Section 9.

5.2. Location Request

A location request message is sent from the Device to the LIS when the Device requires its own LI. The type of LI that a Device requests is determined by the type of LI that is included in the "locationType" element.

The location request is made by sending a document formed of a "locationRequest" element. The LIS uses the source IP address of the location request message as the primary source of identity for the requesting device or target. It is anticipated that other Device identities may be provided through schema extensions. The successful response to a location request message is a document formed of a "locationResponse" element, unless the request fails, in which case the LIS MUST provide an error indication document.

The LIS MUST ignore any part of a location request message that it does not understand.

5.3. Location Response

The response to a location request MUST contain a PIDF-LO and/or location URI(s). The response SHOULD contain location information of the requested "locationType". The cases whereby a different type of location information MAY be returned are described in Section 6.2.

5.4. Indicating Errors

If the LIS is unable to provide location information based on the received locationRequest message, it MUST return an error message. The LIS may return an error message in response to requests for any "locationType".

An error indication document consists of an "error" element. The "error" element MUST include a "code" attribute that indicates the type of error. A set of predefined error codes are included in Section 6.3.

Error responses MAY also include a "message" attribute that can include additional information. This information SHOULD be for diagnostic purposes only, and MAY be in any language. The language of the message SHOULD be indicated with an "xml:lang" attribute.

6. Protocol Parameters

This section describes in detail the parameters that are used for this protocol. Table 1 lists the top-level components used within

the protocol and where they are mandatory or optional for each of the messages.

Parameter	Location Request	Location Response	Error
responseTime (Section 6.1)	o		
locationType (Section 6.2)	o		
code (Section 6.3)			m
message (Section 6.4)			o
locationUriSet (Section 6.5)		o	
Presence (PIDF-LO) (Section 6.6)		o	

Table 1: Message Parameter Usage

6.1. "responseTime" Parameter

The "responseTime" attribute MAY be included in a location request message. The "responseTime" attribute includes a time value indicating to the LIS how long the Device is prepared to wait for a response and/or a purpose for which the Device needs the location. In the case of emergency services, the purpose of obtaining the LI could be either for routing a call to the appropriate PSAP or indicating the location to which responders should be dispatched. The values defined for the purpose, emergencyRouting and emergencyDispatch, will likely be governed by jurisdictional policies, and should be configurable on the LIS.

The time value in the "responseTime" attribute is expressed as a non-negative integer in units of milliseconds. The time value is indicative only and the LIS is under no obligation to strictly adhere to the time limit implied; any enforcement of the time limit is left to the requesting Device. The LIS should provide the most accurate LI that can be determined within the specified interval for the specific service.

The LIS may use the value of the time in the "responseTime" attribute as input when selecting the method of location determination, where multiple such methods exist. If the "responseTime" attribute is absent, then the LIS should return the most precise LI it is capable of determining, with the time interval being implementation dependent.

6.2. "locationType" Parameter

The "locationType" element MAY be included in a location request message. It contains a list of LI types that are requested by the Device. The following list describes the possible values:

any: The LIS SHOULD attempt to provide LI in all forms available to it. The LIS SHOULD return location information in a form that is suited for routing and responding to an emergency call in its jurisdiction, specifically by value. The LIS MAY alternatively or additionally return a location URI. If the "locationType" element is absent, this value MUST be assumed as the default.

geodetic: The LIS SHOULD return a geodetic location for the Target.

civic: The LIS SHOULD return a civic address for the Target. Any type of civic address may be returned.

locationURI: The LIS SHOULD return a set of location URIs for the Target.

The LIS SHOULD return the requested location type or types. The LIS MAY provide additional location types, or it MAY provide alternative types if the request cannot be satisfied for a requested location type. A location URI provided by the LIS is a reference to the most current available LI and is not a stable reference to a specific location. The location types the LIS returns also depend on the setting of the optional "exact" attribute, as described in the following section.

The "SHOULD"-strength requirements on this parameter are included to allow for soft-failover. This enables a fixed client configuration that prefers a specific location type without causing location requests to fail when that location type is unavailable. For example, a notebook computer could be configured to retrieve civic addresses, which is usually available from typical home or work situations. However, when using a wireless modem, the LIS might be unable to provide a civic address and thus provides a geodetic address.

6.2.1. "exact" Attribute

The "exact" attribute MAY be included in a location request message when the "locationType" element is included. When the "exact" attribute is set to "true", it indicates to the LIS that the contents of the "locationType" parameter MUST be strictly followed. The default value of "false" allows the LIS the option of returning something beyond what is specified, such as a set of location URIs when only a civic location was requested.

A value of "true" indicates that the LIS MUST provide a location of

the requested type or types or MUST provide an error. The LIS MUST provide the requested types only. The LIS MUST handle an exact request that includes a "locationType" element set to "any" as if the "exact" attribute were set to "false".

6.3. "code" Parameter

All "error" responses MUST contain a response code. All errors are application-level errors, and MUST only be provided in successfully processed transport-level responses. For example where HTTP is used as the transport, HELD error messages MUST be accompanied by a 200 OK HTTP response.

The value of the response code MUST be one of the following tokens:

requestError: This code indicates that the request was badly formed in some fashion (other than the XML content).

xmlError: This code indicates that the XML content of the request was either badly formed or invalid.

generalLisError: This code indicates that an unspecified error occurred at the LIS.

locationUnknown: This code indicates that the LIS could not determine the location of the Device.

unsupportedMessage: This code indicates that an element in the XML document for the request, was not supported or understood by the LIS.

timeout: This code indicates that the LIS could not satisfy the request within the time specified in the "responseTime" parameter.

cannotProvideLiType: This code indicates that the LIS was unable to provide LI of the type or types requested. This code is used when the "exact" attribute on the "locationType" parameter is set to "true".

6.4. "message" Parameter

The "error" message MAY include a "message" attribute to convey some additional, human-readable information about the result of the request. This message MAY be included in any language, which SHOULD be indicated by the "xml:lang", attribute. The default language is assumed to be English.

6.5. "locationUriSet" Parameter

The "locationUriSet" element, received in a "locationResponse" message MAY contain any number of "locationURI" elements. It is RECOMMENDED that the LIS allocate a Location URI for each scheme that it supports and that each scheme is present only once. The held: URI scheme as defined in Section 8 is one possible scheme for the

"locationURI" element. URI schemes and their secure variants, such as http and https, MUST be regarded as two separate schemes.

If a "locationUriSet" element is received in a "locationResponse" message, it MUST contain an "expires" attribute, which defines the length of time for which the set of "locationURI" elements are valid.

6.5.1. "locationURI" Parameter

The "locationURI" element includes a single Location URI. Each Location URI that is allocated by the LIS is unique to the device that is requesting it.

A "locationURI" SHOULD NOT contain any information that could be used to identify the Device or Target. Thus, it is RECOMMENDED that the "locationURI" element contain a public address for the LIS and an anonymous identifier, such as a local identifier or unlinked pseudonym. Further guidelines to ensure the the privacy and confidentiality of the information contained in the "locationResponse" message, including the "locationURI", are included in Section 10.2.

6.5.2. "expires" Parameter

The "expires" attribute is only included in a "locationResponse" message when a "locationUriSet" element is included. The "expires" attribute indicates the date/time at which the Location URIs provided by the LIS will expire.

Location responses that contain a "locationUriSet" element MUST include the expiry time in the "expires" attribute. If a Device dereferences a location URI after the expiry time, the dereference SHOULD fail.

6.6. "Presence" Parameter (PIDF-LO)

A "presence" parameter may be included in the "locationResponse" message when specific locationTypes (e.g., "geodetic" or "civic") are requested or a "locationType" of "any" is requested. The details on the information that may be included in the presence parameter (in the form of a PIDF-LO) MUST follow the subset of those rules relating to the construction of the "location-info" element in the PIDF-LO Usage Clarification, Considerations and Recommendations document [12]. The LIS MUST follow those rules in generating the PIDF-LO for the presence parameter in this case. Per the GEOPRIV Location Object format specified in [10], the "entity" element MUST reflect the Target of the Location Information. In addition, the default values for <retransmission-allowed> and <retention-expiry> as specified in

[10] MUST be applied. A default value of "no" SHALL be used for the <retransmission-allowed> element. A default value of 24 hours SHALL be used for <retention-expiry> value of any generated PIDF-LO documents. A LIS MAY provide a shorter value for <retention-expiry> but MUST NOT provide a value longer than 24 hours.

Note that the presence parameter is not explicitly shown in the XML schema Section 7 for a location response message due to XML schema constraints.

7. XML Schema

This section gives the XML Schema Definition [14] of the "application/held+xml" format. This is presented as a formal definition of the "application/held+xml" format. Note that the XML Schema definition is not intended to be used with on-the-fly validation of the presence XML document.

```
 <?xml version="1.0"?>
 <xs:schema
     targetNamespace="urn:ietf:params:xml:ns:geopriv:held"
     xmlns:xs="http://www.w3.org/2001/XMLSchema"
     xmlns:held="urn:ietf:params:xml:ns:geopriv:held"
     xmlns:xml="http://www.w3.org/XML/1998/namespace"
     elementFormDefault="qualified"
     attributeFormDefault="unqualified">

   <xs:annotation>
     <xs:documentation source="https://www.ietf.org/rfc/rfcXXXX.txt">
       <!-- [[NOTE TO RFC-EDITOR: Please replace above URL with URL of
            published RFC and remove this note.]] -->
       This document defines HELD messages.
     </xs:documentation>
   </xs:annotation>

   <xs:import namespace="http://www.w3.org/XML/1998/namespace"/>

   <!-- Return Location -->
   <xs:complexType name="returnLocationType">
     <xs:complexContent>
       <xs:restriction base="xs:anyType">
         <xs:sequence>
           <xs:element name="locationURI" type="xs:anyURI"
                       maxOccurs="unbounded"/>
         </xs:sequence>
         <xs:attribute name="expires" type="xs:dateTime"
```

```
                        use="required"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <!-- responseTime Type -->
    <xs:simpleType name="responseTimeType">
      <xs:union>
        <xs:simpleType>
          <xs:restriction base="xs:token">
            <xs:enumeration value="emergencyRouting"/>
            <xs:enumeration value="emergencyDispatch"/>
          </xs:restriction>
        </xs:simpleType>
        <xs:simpleType>
          <xs:restriction base="xs:nonNegativeInteger">
            <xs:minInclusive value="0"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:union>
    </xs:simpleType>

    <!-- Location Type -->
    <xs:simpleType name="locationTypeBase">
      <xs:union>
        <xs:simpleType>
          <xs:restriction base="xs:token">
            <xs:enumeration value="any"/>
          </xs:restriction>
        </xs:simpleType>
        <xs:simpleType>

          <xs:list>
            <xs:simpleType>
              <xs:restriction base="xs:token">
                <xs:enumeration value="civic"/>
                <xs:enumeration value="geodetic"/>
                <xs:enumeration value="locationURI"/>
              </xs:restriction>
            </xs:simpleType>
          </xs:list>
        </xs:simpleType>
      </xs:union>
    </xs:simpleType>

    <xs:complexType name="locationTypeType">
      <xs:simpleContent>
        <xs:extension base="held:locationTypeBase">
```

```
          <xs:attribute name="exact" type="xs:boolean"
                        use="optional" default="false"/>
        </xs:extension>
      </xs:simpleContent>
    </xs:complexType>

    <!-- Message Definitions -->
    <xs:complexType name="baseRequestType">
      <xs:complexContent>
        <xs:restriction base="xs:anyType">
          <xs:sequence/>
          <xs:attribute name="responseTime" type="held:responseTimeType"
                        use="optional"/>
          <xs:anyAttribute namespace="##any" processContents="lax"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>


    <xs:complexType name="errorType">
      <xs:complexContent>
        <xs:restriction base="xs:anyType">
          <xs:sequence/>
          <xs:attribute name="code" type="xs:token"
                        use="required"/>
          <xs:attribute name="message" type="xs:string"
                        use="optional"/>
          <xs:attribute ref="xml:lang" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:element name="error" type="held:errorType"/>

    <!-- Location Response -->
    <xs:complexType name="locationResponseType">
      <xs:complexContent>
        <xs:restriction base="xs:anyType">
          <xs:sequence>
            <xs:element name="locationUriSet"
                        type="held:returnLocationType"
                        minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax"
                    minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
```

```
    <xs:element name="locationResponse"
                type="held:locationResponseType"/>


    <!-- Location Request -->

    <xs:complexType name="locationRequestType">
      <xs:complexContent>
        <xs:extension base="held:baseRequestType">
          <xs:sequence>
            <xs:element name="locationType"
                        type="held:locationTypeType"
                        minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax"
                    minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:extension>
      </xs:complexContent>
    </xs:complexType>

    <xs:element name="locationRequest"
                type="held:locationRequestType"/>

  </xs:schema>
```

8. HELD: URI Definition

This section defines the schema for a held: URI. This URI schema is one possible URI scheme for the "locationURI" element, described in Section 6.5.1, in a HELD "locationResponse " message. In this case, the held: URI indicates to the Device where to obtain the actual location information for a Target. In addition, the held: URI can be the result of the LIS discovery process [16] and indicates to the Device the LIS from which LI should be requested.

The held: URI is defined using a subset of the URI schema specified in Appendix A. of RFC3986 [22] and the associated URI Guidelines [24] per the following ABNF syntax:

```
HELD-URI = "held" ":" "//"  host [":" port] [ path-absolute ] [? query]
```

The following summarizes the primary elements comprising the HELD-URI:

host: As defined in RFC3986 [22]
port: As defined in RFC3986 [22]. There is no unique port
   associated with location URIs.
path-absolute As defined in RFC3986 [22].
query: As defined in RFC3986 [22]. This allows for additional
   information associated with the URIs such as a unique anonymous
   identifier for the Device associated with the target location.

The held: URI is not intended to be human-readable text, therefore it is encoded entirely in US-ASCII. The following are examples of held: URIs:

```
held://ls.example.com:49152/thisLocation?token=xyz987
held://ls.example.com/THISLOCATION
held://ls.example.com/THISlocation
held://ls.example.com/civic
```

Other than the "host" portion, URIs are case sensitive and exact equivalency is required for HELD-URI comparisons. For example, in the above examples, although similar in information, the 2nd and 3rd URIs are not considered equivalent.

In the case where the held: URI is contained in a "locationURI" element in a HELD locationResponse message, it is important to note that the URI is only valid for the length of time indicated by the "expires" attribute.

9. HTTP Binding

This section describes the use of HTTP [3] as a transport mechanism for this protocol, which all conforming implementations MUST support.

The request is carried in the body of an HTTP POST request. The MIME type of both request and response bodies should be "application/held+xml". This should be reflected in the HTTP Content-Type and Accept header fields.

The LIS populates the HTTP headers so that they are consistent with the contents of the message. In particular, the cache control header SHOULD be set to disable the HTTP caching of any PIDF-LO document or Location URIs. Otherwise, there is the risk of stale locations and/or the unauthorized disclosure of the LI. This also allows the LIS to control any caching with the "expires" parameter. The HTTP status code MUST indicate a 2xx series response for all HELD locationResponse messages.

The use of HTTP also includes a default behaviour, which is triggered by a GET request, or a POST with no request body. If either of these queries are received, the LIS MUST attempt to provide either a PIDF-LO document or a Location URI, as if the request was a location request.

The implementation of HTTP as a transport mechanism MUST implement TLS as described in [4]. TLS provides message integrity and privacy between Device and LIS. The LIS MUST use the server authentication method described in [4]; the Device MUST fail a request if server authentication fails, except in the event of an emergency.

10. Security Considerations

HELD is a location acquisition protocol whereby the a client requests its location from a LIS. Specific requirements and security considerations for location acquisition protocols are provided in [13]. An in-depth discussion of the security considerations applicable to the use of Location URIs and by reference provision of LI is included in [17].

By using the HELD protocol, the client and the LIS expose themselves to two types of risk:

Accuracy: Client receives incorrect location information
Privacy: An unauthorized entity receives location information

These two risks are addressed in the two sections below, followed by a summary of the security considerations for implementations of the HELD protocol.

10.1. Accuracy

The provision of an accurate location to the requestor depends on the success of four steps:

1. The client must determine the proper LIS.
2. The client must connect to the proper LIS.
3. The LIS must be able to return the desired location.
4. HELD messages must be transmitted unmodified between the LIS and the client.

Of these, only the second and the fourth are within the scope of this document. The first step is based on either manual configuration or on the LIS discovery defined in [16], in which appropriate security considerations are already discussed. The third step is dependent on the specific positioning capabilities of the LIS, and is thus outside

the scope of this document.

10.1.1. Assuring that the proper LIS has been contacted

After the client has initiated a connection to a LIS, it can receive different levels of assurance that this LIS is the proper LIS based on whether the proper LIS is identified by a domain name or an IP address.

When the LIS is identified by a domain name and the HELD transaction is conducted using TLS [2], the LIS can authenticate itself to the client using the standard mechanism of presenting a certificate binding that domain name to the public key used in TLS. Therefore, any binding of HELD MUST be capable of being transacted over TLS so that the client can request the above authentication, and a LIS implementation for a binding MUST include this feature. Note that in order for the presented certificate to be valid at the client, the client must be able to validate the certificate; in particular, the validation path of the certificate must end in one of the client's trust anchors, even if that trust anchor is the LIS certificate itself.

When the proper LIS is identified by an IP address, there is a risk that a malicious LIS could mimic the proper LIS by spoofing that IP address. If the client deems this risk unacceptable, it is recommended that the client perform a DNS lookup on the corresponding domain name in the in-addr.arpa domain to determine a domain name for the LIS. If a domain name is available, then the standard TLS authentication mechanism can then be used to authenticate the identity of the LIS. If not, then the client can obtain no further assurance about the authenticity of the contacted LIS. In order to minimize the probability of such spoofing attacks, administrative domains that offer a LIS SHOULD take measures to prevent IP address spoofing as described in [5] and [9].

10.1.2. Protecting responses from modification

In order to prevent that response from being modified en route, messages must be transmitted over an integrity-protected channel. When the transaction is being conducted over TLS (a required feature per Section 10.1.1), the channel will be integrity protected by appropriate ciphersuites. When TLS is not used, this protection will vary depending on the binding; in most cases, without protection from TLS, the response will not be protected from modification en route.

10.2. Privacy and Confidentiality

Location information returned by the LIS must be protected from access by unauthorized parties, whether those parties request the location from the LIS or intercept it en route. As in section Section 10.1.2, transactions conducted over TLS with appropriate ciphersuites are protected from access by unauthorized parties en route. Conversely, in most cases, when not conducted over TLS, the response will be accessible while en route from the LIS to the requestor.

Because HELD is an LCP and identifies clients and targets by IP addresses, a requestor is authorized to access location for an IP address only if it is the holder of that IP address. The LIS MUST verify that the client is the target of the returned location, i.e., the LIS MUST NOT provide location to other entities than the target. Note that this is a necessary, but not sufficient criterion for authorization. A LIS MAY deny requests according to any local policy.

A prerequisite for meeting this requirement is that the LIS must have some assurance of the identity of the client. Since the target of the returned location is identified by an IP address, simply sending the response to this IP address will provide sufficient assurance in many cases. This is the default mechanism in HELD for assuring that location is given only authorized clients; LIS implementations MUST support a mode of operation in which this is the only client authentication.

Using IP return routability as an authenticator means that location information is vulnerable to exposure through IP address spoofing attacks. A temporary spoofing of IP address could mean that a device could request a Location URI that would result in another Device's location. One or more of the following approaches are RECOMMENDED to limit this exposure:

- Location URIs SHOULD have a limited lifetime, as reflected by the value for the expires element in Section 6.5.2.
- The network SHOULD have mechanisms that protect against IP address spoofing, such as those defined in [9].
- The LIS and network SHOULD be configured so that the LIS is made aware of Device movement within the network and addressing changes. If the LIS detects a change in the network that results in it no longer being able to determine the location of the Device, then all location URIs for that Device SHOULD be invalidated.

The above measures are dependent on network configuration, which

SHOULD be considered. For instance, in a fixed internet access, providers may be able to restrict the allocation of IP addresses to a single physical line, ensuring that spoofing is not possible; in such an environment, other measures may not be necessary.

When there are further mechanisms available to authenticate ownership of the IP address, the LIS SHOULD use them to authenticate that the client is the owner of the target IP address. For example, in a TLS transaction, the client could present a certificate with a public key bound to an IPv6 Cryptographically Generated Address, and the LIS could verify this binding.

10.3. Summary of Security Considerations

The following summarizes the security considerations for implementations of the HELD protocol:

- All bindings MUST provide the following security services:
  - Authentication of a LIS domain name
  - Integrity of messages between the client and the LIS
  - Confidentiality of messages between the client and the LIS
- It is RECOMMENDED that all bindings use TLS.
- For the HTTP binding, TLS MUST be implemented. The server authentication methods described in HTTP on TLS [4] MUST be implemented.
- A LIS implementation for a binding MUST support the specified security features
- A LIS MUST verify that the requestor is the target of the returned location.
- A LIS MUST support operation when the only client authentication available is via IP return routability.
- A LIS SHOULD set expiration times for location URIs it issues.
- Administrative domains SHOULD take measures to prevent IP address spoofing.

11. Examples

11.1. HTTP Example Messages

The examples in this section show a complete HTTP message that includes the HELD request or response document.

This example shows the most basic request for a LO. This uses the GET feature described by the HTTP binding. This example assumes that the LIS service exists at the URL "https://lis.example.com/location".

```
GET /location 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,*
```

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

```
POST /location 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"/>
```

The successful response to either of these requests is a PIDF-LO document. The following response shows a minimal PIDF-LO response.

```
HTTP/1.x 200 OK
Server: Example LIS
Date: Tue, 10 Jan 2006 03:42:29 GMT
Expires: Tue, 10 Jan 2006 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="3b650sf789nd">
  <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>
   </geopriv>
  </status>
  <timestamp>2006-01-10T03:42:28+00:00</timestamp>
  </tuple>
</presence>
</locationResponse>
```

The error response to either of these requests is an error document. The following response shows an example error response.

```
      HTTP/1.x 200 OK
      Server: Example LIS
      Expires: Tue, 10 Jan 2006 03:49:20 GMT
      Cache-control: private
      Content-Type: application/held+xml
      Content-Length: 135

      <?xml version="1.0"?>
      <error xmlns="urn:ietf:params:xml:ns:geopriv:held"
             code="locationUnknown"
             message="Unable to determine location"/>
```

Note: To focus on important portions of messages, all examples following this note do not show HTTP headers or the XML prologue. In addition, sections of XML not relevant to the example are replaced with comments.

11.2. Simple Location Request Example

The location request shown below doesn't specify any location types or response time.

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

The response to this location request is a list of Location URIs.

```
   <locationResponse xmlns="urn:ietf:params:xml:ns:geopriv:held">
     <locationUriSet expires="2006-01-01T13:00:00">
       <locationURI>held://ls.example.com:9768/357yc6s64ceyoiuy5ax3o
       </locationURI>
       <locationURI>sip:9769+357yc6s64ceyoiuy5ax3o@ls.example.com
       </locationURI>
     </locationUriSet>
   </locationResponse>
```

An error response to this location request is shown below:

```
         <error xmlns="urn:ietf:params:xml:ns:geopriv:held"
                    code="locationUnknown"
                    message="Location not available"/>
```

11.3. Location Request Example for Multiple Location Types

The following Location Request message includes a request for geodetic, civic and any Location URIs.

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

The corresponding Location Response message includes the requested location information, including two location URIs.

```
       <locationResponse xmlns="urn:ietf:params:xml:ns:geopriv:held">
          <locationUriSet expires="2006-01-01T13:00:00">
          <locationURI>held://ls.example.com:9768/357yc6s64ceyoiuy5ax3o
          </locationURI>
          <locationURI>sip:9769+357yc6s64ceyoiuy5ax3o@ls.example.com:
          </locationURI>
         </locationUriSet>
         <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
              xmlns: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>
```

12. IANA Considerations

This document requires several IANA registrations detailed in the following sections.

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

This section registers a new XML namespace, "urn:ietf:params:xml:ns:geopriv:held", per the guidelines in [7].

URI: urn:ietf:params:xml:ns:geopriv:held
Registrant Contact: IETF, GEOPRIV working group,
(geopriv@ietf.org), Mary Barnes (mary.barnes@nortel.com).

XML:

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

12.2. XML Schema Registration

This section registers an XML schema as per the guidelines in [7].

URI: urn:ietf:params:xml:schema:geopriv:held

Registrant Contact: IETF, GEOPRIV working group, (geopriv@ietf.org), Mary Barnes (mary.barnes@nortel.com).

Schema: The XML for this schema can be found as the entirety of Section 7 of this document.

12.3. MIME Media Type Registration for 'application/held+xml'

This section registers the "application/held+xml" MIME type.

To: ietf-types@iana.org

Subject: Registration of MIME media type application/held+xml

MIME media type name: application

MIME subtype name: held+xml

Required parameters: (none)

Optional parameters: charset

Indicates the character encoding of enclosed XML. Default is UTF-8.

Encoding considerations: Uses XML, which can employ 8-bit characters, depending on the character encoding used. See RFC 3023 [20], section 3.2.

Security considerations: This content type is designed to carry protocol data related to the location of an entity, which could include information that is considered private. Appropriate precautions should be taken to limit disclosure of this information.

Interoperability considerations: This content type provides a basis for a protocol

Published specification: RFC XXXX [[NOTE TO IANA/RFC-EDITOR: Please replace XXXX with the RFC number for this specification.]]

Applications which use this media type: Location information providers and consumers.

Additional Information: Magic Number(s): (none)
File extension(s): .xml
Macintosh File Type Code(s): (none)

Person & email address to contact for further information: Mary Barnes <mary.barnes@nortel.com>

Intended usage: LIMITED USE

Author/Change controller: The IETF

Other information: This media type is a specialization of application/xml [20], and many of the considerations described there also apply to application/held+xml.

12.4. Error code Registry

This document requests that the IANA create a new registry for the HELD protocol including an initial registry for error codes. The error codes are included in HELD error messages as described in Section 6.3 and defined in the schema in the 'codeType' token in the XML schema in (Section 7)

The following summarizes the requested registry:

Related Registry: Geopriv HELD Registries, Error codes for HELD

Defining RFC: RFC XXXX [NOTE TO IANA/RFC-EDITOR: Please replace XXXX with the RFC number for this specification.]

Registration/Assignment Procedures: New error codes are allocated on a first-come/first-serve basis with specification required.

Registrant Contact: IETF, GEOPRIV working group, (geopriv@ietf.org), Mary Barnes (mary.barnes@nortel.com).

This section pre-registers the following seven initial error codes as described above in Section 6.3:

requestError: This code indicates that the request was badly formed in some fashion.

xmlError: This code indicates that the XML content of the request was either badly formed or invalid.

generalLisError: This code indicates that an unspecified error occurred at the LIS.

locationUnknown: This code indicates that the LIS could not determine the location of the Device.

unsupportedMessage: This code indicates that the request was not supported or understood by the LIS.

timeout: This code indicates that the LIS could not satisfy the request within the time specified in the "responseTime" parameter.

cannotProvideLiType: This code indicates that the LIS was unable to provide LI of the type or types requested. This code is used when the "exact" attribute on the "locationType" parameter is set to "true".

12.5. URI Registration

The following summarizes the information necessary to register the held: URI. [NOTE TO IANA/RFC-EDITOR: Please replace XXXX with the RFC number for this specification in the following list.]

URI Scheme Name: held

Status: permanent

URI Scheme syntax: See section

URI Scheme Semantics: The held: URI is intended to be used as a reference to a location object or a location information server. Further detail is provided in Section 8 of RFCXXXX.

Encoding Considerations: The HELD: URI is not intended to be human-readable text, therefore they are encoded entirely in US-ASCII.

Applications/protocols that use this URI scheme: The HELD protocol described in RFCXXXX, the GEOPRIV Location De-reference Protocol [26] and GEOPRIV Location Information Server Discovery [16].

Interoperability considerations: This URI may be used as a parameter for the HELD protocol in the locationResponse message. This URI is also used as an input parameter for the GEOPRIV Location De-reference Protocol [26]. This URI may also be a result of the GEOPRIV Location Information Server Discovery [16] and thus used as the target for the HELD protocol request messages. Refer to Section 8 in RFXXXX for further detail and a particular example on the lack of permanence of a specific HELD: URI and thus the importance of using these URIs only within the specific contexts outlined in the references.

Security considerations: Section 10 in RFXXXX addresses the necessary security associated with the transport of location information between a Device and the LIS to ensure the privacy and integrity of the held: URI. Section 6.5.1 in RFCXXXX also recommends that the URI be allocated such that it does not reveal any detail at all about the content of the PIDF-LO that it may

indirectly reference.

Contact: IETF, GEOPRIV working group, (geopriv@ietf.org), Mary Barnes (mary.barnes@nortel.com).

Author/Change controller: This scheme is registered under the IETF tree. As such, IETF maintains change control.

References: RFC XXXX, GEOPRIV Location De-reference Protocol [26], GEOPRIV Location Information Server Discovery [16]

13. Contributors

James Winterbottom, Martin Thomson and Barbara Stark are the authors of the original document, from which this WG document was derived. Their contact information is included in the Author's address section. In addition, they also contributed to the WG document, including the XML schema.

14. Acknowledgements

The author/contributors would like to thank the participants in the GEOPRIV WG and the following people for their constructive input and feedback on this document (in alphabetical order): Nadine Abbott, Eric Arolick, Richard Barnes (in particular the security section), Peter Blatherwick, Guy Caron, Martin Dawson, Lisa Dusseault, Jerome Grenier, Ted Hardie, Neil Justusson, Tat Lam, Marc Linsner, Patti McCalmont, Roger Marshall, Perry Prozeniuk, Carl Reed, Brian Rosen, John Schnizlein, Shida Schubert, Henning Schulzrinne, Ed Shrum, Doug Stuard and Hannes Tschofenig.

15. Changes since last Version

NOTE TO THE RFC-Editor: Please remove this section prior to publication as an RFC.

Changes from WG 04 to 05 (WGLC comments):

1) Totally replaced the security section with the details provided by Richard Barnes so that we don't need a reference to the location security document.

2) Fixed error codes in schema to allow extensibility. Change the IANA registration to be "specification required".

3) Cleaned up the HELD: URI description, per comments from Martin and James and partially addressing HELD-04 Issue 1. Put the definition in a separate section and clarified the applicability (to also

include being a results of the discovery process) and fixed examples.

4) Updated the LocationURI section to be more accurate, address HELD-04 Issue 3, and include the reference to the new HELD:URI section. Also, fixed an error in the doc in that the top level parm in the locationResponse is actually locationUriSet, which contains any number of locationURI elements and the "expires" parameter. So, Table 1 was also updated and a new section for the LocationURISet was added that includes the subsections for the "locationURI" and "expires". And, then clarified that "expires" applies to "locationURISet" and not per "locationURI".

5) Editorial nits: pointed out offline by Richard (e.g., by-value -> by value, by-reference -> by reference, etc.) and onlist by James and Martin. Please refer to the diff for a complete view of editorial changes.

6) Added text in HTTP binding section to disable HTTP caching (HELD-04 Issue 5 on the list).

Changes from WG 03 to 04:

1) Terminology: clarified in terminology section that "attribute" and "element" are used in the strict XML sense and "parameter" is used as a general protocol term Replaced term "HTTP delivery" with "HTTP transport". Still have two terms "HTTP transport" and "HTTP binding", but those are consistent with general uses of HTTP.

2) Editorial changes and clarifications: per Roger Marshall's and Eric Arolick's comments and subsequent WG mailing list discussion.

3) Changed normative language for describing expected and recommended LIS behaviors to be non-normative recommendations in cases where the protocol parameters were not the target of the discussion (e.g., we can't prescribe to the LIS how it determines location or what it defines to be an "accurate" location).

4) Clarified responseTime attribute (section 6.1). Changed type from "decimal" to "nonNegativeInteger" in XML schema (section 7)

5) Updated Table 1 in section 6 to only include top-level parameters and fixed some errors in that table (i.e., code for locationResponse) and adding PIDF-LO to the table. Added a detailed section describing PIDF-LO (section 6.6), moving some of the normative text in the Protocol Overview to this section.

6) Added schema and description for locationURI to section 6.5. Added IANA registration for HELD: URI schema.

7) Added IANA registry for error codes.

Changes from WG 02 to 03:

1) Added text to address concern over use of IP address as device identifier, per long email thread - changes to section 3 (overview) and section 4 (protocol overview).

2) Removed WSDL (section 8 updated, section 8.1 and 10.4 removed)

3) Added extensibility to baseRequestType in the schema (an oversight from previous edits), along with fixing some other nits in schema (section 7)

4) Moved discussion of Location URI from section 5.3 (Location Response) to where it rightly belonged in Section 6.5 (Location URI Parameter).

5) Clarified text for "expires" parameter (6.5.1) - it's an optional parm, but required for LocationURIs

6) Clarified responseTime parameter: when missing, then the LCS provides most precise LI, with the time required being implementation specific.

7) Clarified that the MUST use in section 8 (HTTP binding) is a MUST implement.

8) Updated references (removed unused/added new).

Changes from WG 01 to 02:

1) Updated Terminology to be consistent with WG agreements and other documents (e.g., LCS -> LIS and removed duplicate terms). In the end, there are no new terms defined in this document.

2) Modified definition of responseTime to reflect WG consensus.

3) Removed jurisdictionalCivic and postalCivic locationTypes (leaving just "civic").

4) Clarified text that locationType is optional. Fixed table 1 and text in section 5.2 (locationRequest description). Text in section 6.2 (description of locationType element) already defined the default to be "any".

5) Simplified error responses. Separated the definition of error response type from the locationResponse type thus no need for

defining an error code of "success". This simplifies the schema and processing.

6) Updated schema/examples for the above.

7) Updated Appendix A based on updates to requirements document, specifically changes to A.1, A.3 and adding A.10.

8) Miscellaneous editorial clarifications.

Changes from WG 00 to 01:

1) heldResponse renamed to locationResponse.

2) Changed namespace references for the PIDF-LO geoShape in the schema to match the agreed GML PIDF-LO Geometry Shape Application Schema.

3) Removed "options" element - leaving optionality/extensibility to XML mechanisms.

4) Changed error codes to be enumerations and not redefinitions of HTTP response codes.

5) Updated schema/examples for the above and removed some remnants of the context element.

6) Clarified the definition of "Location Information (LI)" to include a reference to the location (to match the XML schema and provide consistency of usage throughout the document). Added an additional statement in section 7.2 (locationType) to clarify that LCS MAY also return a Location URI.

7) Modifed the definition of "Location Configuration Server (LCS)" to be consistent with the current definiton in the requirements document.

8) Updated Location Response (section 6.3) to remove reference to context and discuss the used of a local identifier or unlinked pseudonym in providing privacy/security.

9) Clarified that the source IP address in the request is used as the identifier for the target/device for the HELD protocol as defined in this document.

10) Miscellaneous editorial clarifications.

16. References

16.1. Normative References

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

[2] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[3] 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.

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

[5] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000.

[6] Eastlake, D., Reagle, J., and D. Solo, "(Extensible Markup Language) XML-Signature Syntax and Processing", RFC 3275, March 2002.

[7] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, January 2004.

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

[9] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, March 2004.

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

[11] Thomson, M. and J. Winterbottom, "Revised Civic Location Format for PIDF-LO", draft-ietf-geopriv-revised-civic-lo-07 (work in progress), December 2007.

[12] 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.

[13] Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol; Problem Statement and Requirements", draft-ietf-geopriv-l7-lcp-ps-06 (work in progress),

November 2007.

[14] Thompson, H., Maloney, M., Beech, D., and N. Mendelsohn, "XML Schema Part 1: Structures Second Edition", World Wide Web Consortium Recommendation REC-xmlschema-1-20041028, October 2004, <http://www.w3.org/TR/2004/REC-xmlschema-1-20041028>.

[15] Biron, P. and A. Malhotra, "XML Schema Part 2: Datatypes Second Edition", World Wide Web Consortium Recommendation REC-xmlschema-2-20041028, October 2004, <http://www.w3.org/TR/2004/REC-xmlschema-2-20041028>.

[16] Thomson, M. and J. Winterbottom, "Discovering the Local Location Information Server (LIS)", draft-ietf-geopriv-lis-discovery-00 (work in progress), December 2007.

[17] Marshall, R., "Requirements for a Location-by-Reference Mechanism", draft-ietf-geopriv-lbyr-requirements-01 (work in progress), October 2007.

16.2. Informative References

[18] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, September 1981.

[19] Day, M., Rosenberg, J., and H. Sugano, "A Model for Presence and Instant Messaging", RFC 2778, February 2000.

[20] Murata, M., St. Laurent, S., and D. Kohn, "XML Media Types", RFC 3023, January 2001.

[21] 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.

[22] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[23] Polk, J., Schnizlein, J., and M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information", RFC 3825, July 2004.

[24] Hansen, T., Hardie, T., and L. Masinter, "Guidelines and Registration Procedures for New URI Schemes", BCP 115, RFC 4395, February 2006.

[25] Polk, J. and B. Rosen, "Location Conveyance for the Session Initiation Protocol", draft-ietf-sip-location-conveyance-09 (work in progress), November 2007.

[26] Winterbottom, J., Tschofenig, H., Schulzrinne, H., Thomson, M., and M. Dawson, "An HTTPS Location Dereferencing Protocol Using HELD", draft-winterbottom-geopriv-deref-protocol-00 (work in progress), November 2007.

[27] TIA, "ANSI/TIA-1057 Link Layer Discovery Protocol - Media Endpoint Discovery".

Appendix A. HELD Compliance to IETF LCP requirements

This appendix describes HELD's compliance to the requirements specified in the [13].

A.1. L7-1: Identifier Choice

"The L7 LCP MUST be able to carry different identifiers or MUST define an identifier that is mandatory to implement. Regarding the latter aspect, such an identifier is only appropriate if it is from the same realm as the one for which the location information service maintains identifier to location mapping."

COMPLY

HELD uses the IP address of the location request message as the primary source of identity for the requesting device or target. This identity can be used with other contextual network information to provide a physical location for the Target for many network deployments. There may be network deployments where an IP address alone is insufficient to identify a Target in a network. However, any necessary identity extensions for these networks is beyond the scope of this document.

A.2. L7-2: Mobility Support

"The GEOPRIV Layer 7 Location Configuration Protocol MUST support a broad range of mobility from devices that can only move between reboots, to devices that can change attachment points with the impact that their IP address is changed, to devices that do not change their IP address while roaming, to devices that continuously move by being attached to the same network attachment point."

COMPLY

Mobility support is inherently a characteristic of the access network technology and HELD is designed to be access network agnostic. Consequently HELD complies with this requirement. In addition HELD provides specific support for mobile environments by providing an optional responseTime attribute in location request messages. Wireless networks often have several different mechanisms at their disposal for position determination (e.g. Assisted GPS versus location based on serving base station identity), each providing different degrees of accuracy and taking different amounts of time to yield a result. The responseTime parameter provides the LIS with a criterion which it can use to select a location determination technique.

A.3. L7-3: ASP and Access Network Provider Relationship

"The design of the L7 LCP MUST NOT assume a business or trust relationship between the Application Service Provider (ASP) and the Access Network Provider. Requirements for resolving a reference to location information are not discussed in this document."

COMPLY

HELD describes a location acquisition protocol and has no dependencies on the business or trust relationship between the ASP and the Access Network Provider. Location acquisition using HELD is subject to the restrictions described in Section 10.

A.4. L7-4: Layer 2 and Layer 3 Provider Relationship

"The design of the GEOPRIV Layer 7 Location Configuration Protocol MUST assume that there is a trust and business relationship between the L2 and the L3 provider. The L3 provider operates the LIS and needs to obtain location information from the L2 provider since this one is closest to the end host. If the L2 and L3 provider for the same host are different entities, they cooperate for the purposes needed to determine end system locations."

COMPLY

HELD was specifically designed with this model in mind and readily allows itself to chaining requests between operators without a change in protocol being required. HELD is a webservices protocol it can be bound to transports other than HTTP. Using o offers the option of high request throughput over a dedicated connection between an L3 provider and an L2 provider without incurring the serial restriction imposed by HTTP. This is less easy to do with protocols that do not decouple themselves from the transport.

A.5. L7-5: Legacy Device Considerations

"The design of the GEOPRIV Layer 7 Location Configuration Protocol MUST consider legacy residential NAT devices and NTEs in an DSL environment that cannot be upgraded to support additional protocols, for example to pass additional information through DHCP."

COMPLY

HELD is an application protocol and operates on top of IP. A HELD request from a host behind a residential NAT will traverse the NAT acquiring the external address of the home router. The location provided to the host therefore will be the address of the home router in this circumstance. No changes are required to the home router in order to support this function, HELD was designed specifically to address this deployment scenario.

A.6. L7-6: VPN Awareness

"The design of the GEOPRIV Layer 7 Location Configuration Protocol MUST assume that at least one end of a VPN is aware of the VPN functionality. In an enterprise scenario, the enterprise side will provide the LIS used by the client and can thereby detect whether the LIS request was initiated through a VPN tunnel."

COMPLY

HELD does not preclude a LIS on the far end of a VPN tunnel being aware that the client request is occurring over that tunnel. It also does not preclude a client device from accessing a LIS serving the local physical network and subsequently using the location information with an application that is accessed over a VPN tunnel.

A.7. L7-7: Network Access Authentication

"The design of the GEOPRIV Layer 7 Location Configuration Protocol MUST NOT assume prior network access authentication."

COMPLY

HELD makes no assumptions about prior network access authentication. HELD strongly recommends the use of TLS with server-side certificates for communication between the end-point and the LIS. There is no requirement for the end-point to authenticate with the LIS.

A.8. L7-8: Network Topology Unawareness

"The design of the GEOPRIV Layer 7 Location Configuration Protocol MUST NOT assume end systems being aware of the access network topology. End systems are, however, able to determine their public IP address(es) via mechanisms such as STUN or NSIS NATFW NSLP."

COMPLY

HELD makes no assumption about the network topology. HELD doesn't require that the device know its external IP address, except where that is required for discovery of the LIS.

A.9. L7-9: Discovery Mechanism

"The L7 LCP MUST define a single mandatory to implement discovery mechanism."

COMPLY

HELD uses the discovery mechanism in [16].

A.10. L7-10: PIDF-LO Creation

"When a LIS creates a PIDF-LO per RFC 4119 then it MUST put the <geopriv> element into the <device> element of the presence document (see RFC 4479). This ensures that the resulting PIDF-LO document, which is subsequently distributed to other entities, conforms to the rules outlined in ". [12]

COMPLY

HELD protocol overview (Section 4) describes the requirements on the LIS in creating the PIDF-LO and prescribes that the PIDF-LO generated by the LIS MUST conform to [12].

Authors' Addresses

Mary Barnes (editor)
Nortel
2201 Lakeside Blvd
Richardson, TX

Email: mary.barnes@nortel.com

James Winterbottom
Andrew
PO Box U40
Wollongong University Campus, NSW 2500
AU

Phone: +61 2 4221 2938
Email: james.winterbottom@andrew.com
URI: http://www.andrew.com/

Martin Thomson
Andrew
PO Box U40
Wollongong University Campus, NSW 2500
AU

Phone: +61 2 4221 2915
Email: martin.thomson@andrew.com
URI: http://www.andrew.com/

Barbara Stark
BellSouth
Room 7A41
725 W Peachtree St.
Atlanta, GA 30308
US

Email: barbara.stark@bellsouth.com

Full Copyright Statement

Intellectual Property

Acknowledgment

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