GEOPRIV WG
Internet-Draft
Intended status: Standards Track
Expires: March 1, 2010

M. Barnes, Ed.
Nortel

Aug 28, 2009

HTTP Enabled Location Delivery (HELD)
draft-ietf-geopriv-http-location-delivery-16.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) and HTTP over Transport Layer Security (HTTP/TLS) as transports 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 [I-D.ietf-geopriv-l7-lcp-ps] provides some scenarios in which a Device might rely on its access network to provide location information. The Location Information Server (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 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) and HTTP over Transport Layer Security (HTTP/TLS) as transports 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 [RFC2119].

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 [RFC3693] . 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 [I-D.ietf-geopriv-l7-lcp-ps]. 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). 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. An Access Provider (AP) operates the LIS so that Devices (and Targets) can retrieve their LI. This document assumes that the Device and Access Provider have no prior relationship other than what is necessary for the Device to obtain network access.

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 [RFC3693] and the LIS defined in [I-D.ietf-geopriv-l7-lcp-ps] and where this protocol applies, with the Rule Maker and Target represented by the role of the Device. Note that only the interfaces relevant to the Device are identified in the diagram.

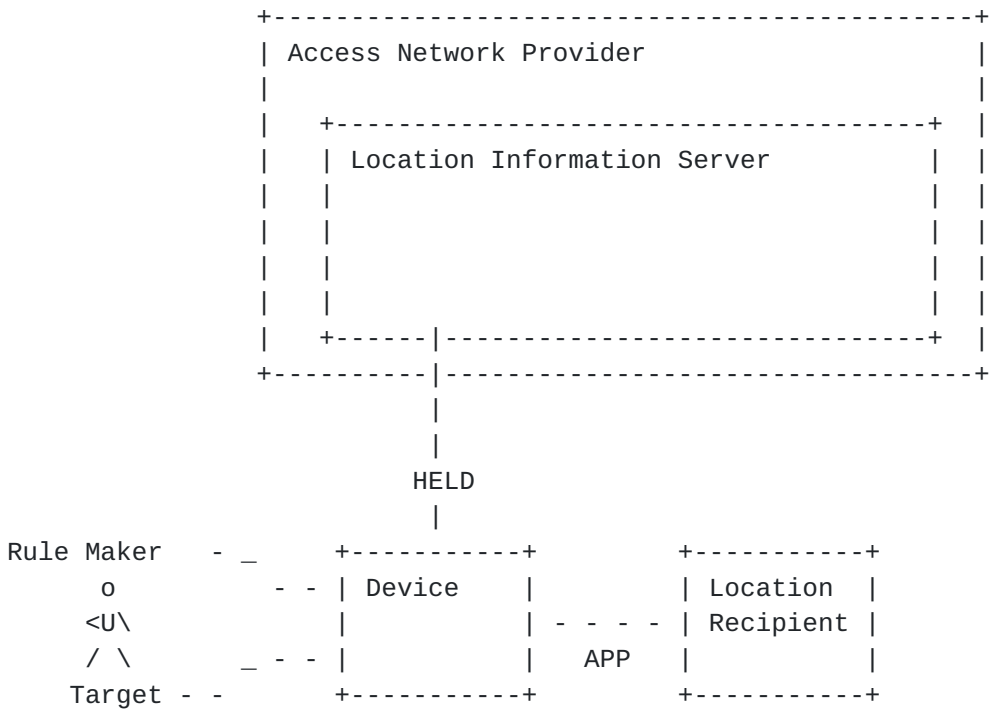

Figure 1: Significant Roles

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 [I-D.ietf-sipcore-location-conveyance].

4. Protocol Overview

A device uses the HELD protocol to retrieve its location either directly in the form of a Presence Information Data Format Location Object (PIDF-LO) document (by value) and indirectly as a Location URI (by reference). The security necessary to ensure the accuracy, privacy and confidentiality of the device's location is described in the Security Considerations (Section 9).

As described in the L7 LCP problem statement and requirements [I-D.ietf-geopriv-l7-lcp-ps], the Device MUST first discover the URI for the LIS for sending the HELD protocol requests. The URI for the LIS SHOULD be obtained from an authorized and authenticated entity. The details for ensuring that an appropriate LIS is contacted are provided in Section 9 and in particular Section 9.1. The LIS discovery protocol details are out of scope of this document and are specified in [I-D.ietf-geopriv-lis-discovery]. The type of URI provided by LIS discovery is RECOMMENDED to be an https: URI.

The LIS requires an identifier for the Device in order to determine the appropriate location to include in the location response message. In this document, the IP address of the Device, as reflected by the source IP address in the location request message, is used as the identifier. Other identifiers are possible, but are beyond the scope of this document.

4.1. 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 4.1.2 provides recommendations to address this issue.

4.1.1. Devices and VPNs

To minimize the impact of connections or tunnels setup for security purposes or to traverse middleboxes, Devices that connect to servers such as VPN servers, SOCKS servers and HTTP proxy servers should perform their HELD query to the LIS prior to establishing a connection to other servers. It is RECOMMENDED that discovery [I-D.ietf-geopriv-lis-discovery] and an initial query are performed

before establishing any connections to other servers. If a Device performs the HELD query after establishing a connection to another server, 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. In this case, 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. Otherwise, the other devices would be totally unaware that they could receive inaccurate location information.

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)[RFC3825] or Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) [LLDP-MED]. For this case, the VPN device that serves as a LIS may first acquire its own location using HELD.

4.1.2. 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 LI for the device, it should provide an error response 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 indicate Devices on the remote side of a NAT or VPN. In order to serve the Devices on the remote side of a NAT or VPN, a LIS needs to have a presence on the the side of the NAT or VPN nearest the Device.

4.2. 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 [RFC5491]. Further detail is included in the detailed protocol section of this document Section 6

4.3. 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 [RFC3986] 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, possession of the URI does not in any way suggest that the LIS indiscriminately reveals the location associated with the location URI. The specific requirements associated with the dereference of the location are specified in [I-D.ietf-geopriv-lbyr-requirements]. The location dereference protocol details are out of scope of this document. As such, many of the requirements in [I-D.ietf-geopriv-lbyr-requirements] (e.g., cancelling of location references) are not intended to be supported by this specification. It is anticipated that future specifications may address these requirements.

5. Protocol Description

As discussed in Section 4 the HELD 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 5.1. 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 11.3 to distinguish HELD messages from other XML document bodies. This specification follows the recommendations and conventions described in [RFC3023], 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 [W3C.REC-xmlschema-1-20041028].

This document describes the use of a combination of HTTP [RFC2616], TLS [RFC5246] and TCP [RFC0793] in Section 8.

5.1. 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 LIS MUST ignore any part of a location request message that it does not understand, except the document element. If the document element of a request is not supported, the LIS MUST return an error with the unsupportedMessage error code.

5.2. Location Response

A successful 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.

5.3. 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 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 Public Safety Answering Point (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 provides 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.
geodetic: The LIS SHOULD return a location by value in the form of a geodetic location for the Target.
civic: The LIS SHOULD return a location by value in the form of a civic address for the Target.
locationURI: The LIS SHOULD return a set of location URIs for the Target.

The LIS SHOULD return the requested location type or types. The location types the LIS returns also depend on the setting of the optional "exact" attribute. If the "exact" attribute is set to "true" then the LIS MUST return either the requested location type or provide an error response. The "exact" attribute does not apply (is ignored) for a request for a location type of "any". Further detail of the "exact" attribute processing is provided in the following Section 6.2.1.

In the case of a request for specific locationType(s) and the "exact" attribute is false, the LIS MAY provide additional location types, or it MAY provide alternative types if the request cannot be satisfied for a requested location type. The "SHOULD"-strength requirements on this parameter for specific location types 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.

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, a value of "any" MUST be assumed as the default. 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.

It should be noted that the protocol does not support a request to just receive one of a subset of location types. For example, in the case where a Device has a preference for just "geodetic" or "civic", it is necessary to make the request without an "exact" attribute, including both location types. In this case, if neither is available a LIS SHOULD return a locationURI if available.

The LIS SHOULD provide the locations in the response in the same order in which they were included in the "locationType" element in the request. Indeed, the primary advantage of including specific location types in a request when the "exact" attribute is set to "false" is to ensure that one receives the available locations in a specific order. For example, a locationRequest for "civic" could yield any of the following location types in the response:

- civic
- civic, geodetic
- civic, locationURI
- civic, geodetic, locationURI
- civic, locationURI, geodetic
- geodetic, locationURI (only if civic is not available)
- locationURI, geodetic (only if civic is not available)
- geodetic (only if civic is not available)
- locationURI (only if civic is not available)

For the example above, if the "exact" attribute was "true", then the only possible response is either a "civic" location or an error message.

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/HTTPS is used as the transport, HELD error messages MUST be carried by a 200 OK HTTP/HTTPS response.

The value of the response code MUST be an IANA-registered value. The following tokens are registered by this document:

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. The same request can be sent by the Device at a later time. Devices MUST limit any attempts to retry requests.

unsupportedMessage: This code indicates that an element in the XML document for the request, was not supported or understood by the LIS. This error code is used when a HELD request contains a document element that is not supported by the receiver.

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".

notLocatable: This code indicates that the LIS is unable to locate the Device, and that the Device MUST NOT make further attempts to retrieve LI from this LIS. This error code is used to indicate that the Device is outside the access network served by the LIS; for instance, the VPN and NAT scenarios discussed in Section 4.1.2.

6.4. "message" Parameter

The "error" message MAY include one or more "message" attributes to convey some additional, human-readable information about the result of the request. The message MAY be included in any language, which SHOULD be indicated by the "xml:lang", attribute. The default language is assumed to be English ("en") [I-D.ietf-ltru-4646bis].

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. 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. In order for a URI of any particular scheme to be included in a response, there MUST be a specification that defines how that URI can be used to retrieve location information. The details of the protocol for dereferencing must meet the location dereference protocol requirements as specified in [I-D.ietf-geopriv-lbyr-requirements] and are outside the scope of this base HELD specification.

Each Location URI that is allocated by the LIS is unique to the device that is requesting it. At the time the location URI is provided in the response, there is no binding to a specific location type and the location URI is totally independent of the specific type of location it might reference. The specific location type is determined at the time of dereference.

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.

When a LIS returns a "locationURI" element to a Device, the policy on the "locationURI" is set by the LIS alone. This specification does not include a mechanism for the HELD client to set access control policies on a "locationURI". Conversely, there is no mechanism, in this protocol as defined in this document, for the LIS to provide a Device the access control policy to be applied to a "locationURI". Since the Device is not aware of the access controls to be applied to (subsequent) requests to dereference a "locationURI", the client SHOULD protect a "locationURI" as if it were a Location Object - i.e., the Device SHOULD send a "locationURI" over encrypted channels, and only to entities that are authorized to have access to the location.

Further guidelines to ensure the privacy and confidentiality of the information contained in the "locationResponse" message, including the "locationURI", are included in Section 9.3.

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. The "expires" attribute does not define the length of time a location received by dereferencing the location URI will be valid. The "expires" attribute is RECOMMENDED not to exceed 24 hours and SHOULD be a minimum of 30 minutes.

All date-time values used in HELD MUST be expressed in Universal Coordinated Time (UTC) using the Gregorian calendar. XML Schema allows use of time zone identifiers to indicate offsets from the zero meridian, but this option MUST NOT be used with HELD. The extended date-time form using upper case "T" and "Z" characters defined in [W3C.REC-xmlschema-2-20041028] MUST be used to represent date-time values.

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 single "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 LIS MUST follow the subset of the rules relating to the construction of the "location-info" element in the PIDF-LO Usage Clarification, Considerations and Recommendations document [RFC5491] in generating the PIDF-LO for the presence parameter.

The LIS MUST NOT include any means of identifying the Device in the PIDF-LO unless it is able to verify that the identifier is correct and inclusion of identity is expressly permitted by a Rule Maker. Therefore, PIDF parameters that contain identity are either omitted or contain unlinked pseudonyms [RFC3693]. A unique, unlinked presentity URI SHOULD be generated by the LIS for the mandatory presence "entity" attribute of the PIDF document. Optional parameters such as the "contact" element and the "deviceID" element [RFC4479] are not used.

Note that the presence parameter is not explicitly shown in the XML

schema in Section 7 for a location response message, due to XML schema constraints, since PIDF is already defined and registered separately. Thus, the "##other" namespace serves as a placeholder for the presence parameter in the schema.

7. XML Schema

This section gives the XML Schema Definition [W3C.REC-xmlschema-1-20041028], [W3C.REC-xmlschema-2-20041028] 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. Whitespaces are included in the schema to conform to the line length restrictions of the RFC format without having a negative impact on the readability of the document. Any conforming processor should remove leading and trailing white spaces.

```
<?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>
      This document (RFC xxxx) defines HELD messages.
      <!-- [[NOTE TO RFC-EDITOR: Please replace XXXX
           with the RFC number for this specification.]] -->
    </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:restriction base="held:locationTypeList">
          <xs:minLength value="1"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:union>
  </xs:simpleType>

  <xs:simpleType name="locationTypeList">
    <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: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:element name="message" type="held:errorMsgType"
                        minOccurs="0" maxOccurs="unbounded"/>
            <xs:any namespace="##other" processContents="lax"
                    minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="code" type="xs:token"
                        use="required"/>
          <xs:anyAttribute namespace="##any" processContents="lax"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="errorMsgType">
      <xs:simpleContent>
        <xs:extension base="xs:token">
          <xs:attribute ref="xml:lang"/>
          <xs:anyAttribute namespace="##any" processContents="lax"/>
        </xs:extension>
      </xs:simpleContent>
    </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. HTTP Binding

This section describes the use of HTTP [RFC2616] and HTTP Over TLS [RFC2818] as transport mechanisms for the HELD protocol, which a

conforming LIS and Device MUST support.

Although HELD uses HTTP as a transport, it uses a strict subset of HTTP features, and due to the restrictions of some features, a LIS is not a fully compliant HTTP server. It is intended that a LIS can easily be built using an HTTP server with extensibility mechanisms, and that a HELD Device can trivially use existing HTTP libraries. This subset of requirements helps implementors avoid ambiguity with the many options the full HTTP protocol offers.

A Device that conforms to this specification MAY choose not to support HTTP authentication [RFC2617] or cookies [RFC2965]. Because the Device and the LIS may not necessarily have a prior relationship, the LIS SHOULD NOT require a Device to authenticate, either using the above HTTP authentication methods or TLS client authentication. Unless all Devices that access a LIS can be expected to be able to authenticate in a certain fashion, denying access to location information could prevent a Device from using location-dependent services, such as emergency calling. Extensions to this protocol might result in the addition of request parameters that a LIS might use to decide to request Device authentication.

A HELD request is carried in the body of an HTTP POST request. The Device MUST include a Host header in the request.

The MIME type of HELD request and response bodies is "application/held+xml". LIS and Device MUST provide this value in the HTTP Content-Type and Accept header fields.If the LIS does not receive the appropriate Content-Type and Accept header fields, the LIS SHOULD fail the request, returning a 406 (not acceptable) response. HELD responses SHOULD include a Content-Length header.

Devices MUST NOT use the "Expect" header or the "Range" header in HELD requests. The LIS MAY return 501 (not implemented) errors if either of these HTTP features are used. In the case that the LIS receives a request from the Device containing a If-* (conditional) header, the LIS SHOULD return a 412 (precondition failed) response.

The POST method is the only method REQUIRED for HELD. If a LIS chooses to support GET or HEAD, it SHOULD consider the kind of application doing the GET. Since a HELD Device only uses a POST method, the GET or HEAD MUST be either an escaped URL (e.g., somebody found a URL in protocol traces or log files and fed it into their browser) or somebody doing testing/ debugging. The LIS could provide information in the HELD response indicating that the URL corresponds to a LIS server and only responds to HELD POST requests or the LIS could instead try to avoid any leak of information by returning a very generic HTTP error message such as 404 (not found).

The LIS populates the HTTP headers of responses so that they are consistent with the contents of the message. In particular, the "CacheControl" header SHOULD be set to disable caching of any PIDF-LO document or Location URIs by HTTP intermediaries. 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 HELD "expires" parameter. The HTTP status code MUST indicate a 2xx series response for all HELD locationResponse and HELD error messages.

The LIS MAY redirect a HELD request. A Device MUST handle redirects, by using the Location header provided by the server in a 3xx response. When redirecting, the Device MUST observe the delay indicated by the Retry-After header. The Device MUST authenticate the server that returns the redirect response before following the redirect, if a Device requires that the server is authenticated. A Device SHOULD authenticate the LIS indicated in a redirect.

The LIS SHOULD support persistent connections and request pipelining. If pipelining is not supported, the LIS MUST NOT allow persistent connections. The Device MUST support termination of a response by the closing of a connection.

Implementations of HELD that implement HTTP transport MUST implement transport over TLS [RFC2818]. TLS provides message integrity and confidentiality between Device and LIS. The Device MUST implement the server authentication method described in Section 3.1 of [RFC2818], with an exception in how wildcards are handled. The leftmost label MAY contain the wildcard string "*", which matches any single domain name label. Additional characters in this leftmost label are invalid (that is, "f*.example.com" is not a valid name and does not match any domain name).

The device uses the URI obtained during LIS discovery to authenticate the server. The details of this authentication method are provided in section 3.1 of HTTPS [RFC2818]. When TLS is used, the Device SHOULD fail a request if server authentication fails, except in the event of an emergency.

9. 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 [I-D.ietf-geopriv-l7-lcp-ps]. An in-depth discussion of the security considerations applicable to the use of Location URIs and by reference provision of LI is included in

[I-D.ietf-geopriv-lbyr-requirements].

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

The provision of an accurate and privacy/confidentiality protected location to the requestor depends on the success of five 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 identify the device by its identifier (IP Address).
4. The LIS must be able to return the desired location.
5. HELD messages must be transmitted unmodified between the LIS and the client.

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

9.1. Assuring that the proper LIS has been contacted

This document assumes that the LIS to be contacted is identified either by an IP address or a domain name, as is the case for a LIS discovered as described in LIS Discovery [I-D.ietf-geopriv-lis-discovery]. When the HELD transaction is conducted using TLS [RFC5246], the LIS can authenticate its identity, either as a domain name or as an IP address, to the client by presenting a certificate containing that identifier as a subjectAltName (i.e., as an iPAddress or dNSName, respectively). In the case of the HTTP binding described above, this is exactly the authentication described by TLS [RFC2818]. If the client has external information as to the expected identity or credentials of the proper LIS (e.g., a certificate fingerprint), these checks MAY be omitted. 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.

9.2. 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 9.1), 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.

9.3. 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 9.2, 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 to 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 c ould request a Location Object or Location URI that would result in receiving another Device's location if the attacker is able to receive packets sent to the spoofed address. In addition, in cases where a Device drops off the network for various reasons, the re-use of the Device's IP address could result in another Device receiving

the original Device's location rather than its own location. These exposures are limited by the following:

- Location URIs MUST have a limited lifetime, as reflected by the value for the expires element in Section 6.5.2. The lifetime of location URIs necessarily depends on the nature of the access.
- 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, additional measures may not be necessary.

10. Examples

The following sections provide basic HTTP/HTTPS examples, a simple location request example and a location request for multiple location types example along with the relevant location responses. To focus on important portions of messages, the examples in Section 10.2 and Section 10.3 do not show HTTP/HTTPS headers or the XML prologue. In addition, sections of XML not relevant to the example are replaced with comments.

10.1. HTTPS Example Messages

The examples in this section show complete HTTP/HTTPS messages that include the HELD request or response document.

This example shows the most basic request for a LO. The POST includes an empty "locationRequest" element.

```
POST /location HTTP/1.1
Host: lis.example.com:49152
Content-Type: application/held+xml;charset=utf-8
Content-Length: 87

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

Since the above request does not include a "locationType" element, the successful response to the request may contain any type of location. The following shows a response containing a minimal PIDF-LO.

```
HTTP/1.1 200 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;charset=utf-8
Content-Length: 856

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

The error response to the request is an error document. The following response shows an example error response.

```
HTTP/1.1 200 OK
Server: Example LIS
Expires: Tue, 10 Jan 2006 03:49:20 GMT
Cache-control: private
Content-Type: application/held+xml;charset=utf-8
Content-Length: 182

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

10.2. 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 example response to this location request contains a list of Location URIs.

```
<locationResponse xmlns="urn:ietf:params:xml:ns:geopriv:held">
   <locationUriSet expires="2006-01-01T13:00:00.0Z">
    <locationURI>https://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"
  </message>
</error>
```

10.3. 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="2006-01-01T13:00:00.0Z">
  <locationURI>https://ls.example.com:9768/357yc6s64ceyoiuy5ax3o
  </locationURI>
  <locationURI>sip:9769+357yc6s64ceyoiuy5ax3o@ls.example.com:
  </locationURI>
 </locationUriSet>
 <presence xmlns="urn:ietf:params:xml:ns:pidf"
   entity="pres:ae3be8585902e2253ce2@10.102.23.9">
 <tuple id="lisLocation">
  <status>
   <geopriv xmlns="urn:ietf:params:xml:ns:pidf:geopriv10">
   <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
         xmlns:gbp="urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy">
        <gbp:retransmission-allowed>false
        </gbp:retransmission-allowed>
        <gbp:retention-expiry>2007-05-25T12:35:02+10:00
        </gbp:retention-expiry>
       </usage-rules>
       <method>Wiremap</method>
     </geopriv>
    </status>
    <timestamp>2007-05-24T12:35:02+10:00</timestamp>
   </tuple>
  </presence>
  </locationResponse>
```

11. IANA Considerations

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

11.1. 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

[RFC3688].

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 replace XXXX
 with the RFC number for this specification.]
        <p>See RFCXXXX</p>
    </body>
  </html>
END
```

11.2. XML Schema Registration

This section registers an XML schema as per the guidelines in [RFC3688].

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.

11.3. 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
Same as the charset parameter of "application/xml" as specified in RFC 3023 [RFC3023], section 3.2.
Encoding considerations: Same as the encoding considerations of "application/xml" as specified in RFC 3023 [RFC3023], 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): "TEXT"
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 [RFC3023], and many of the considerations described there also apply to application/held+xml.

11.4. 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: Following the policies outlined in [RFC5226], the IANA policy for assigning new values for the Error codes for HELD shall be Standards Action: Values are assigned only for Standards Track RFCs approved by the IESG.

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. This error code is used when a HELD request contains a document element that is not supported by the receiver.

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".

notLocatable: This code indicates that the LIS is unable to locate the Device, and that the Device MUST NOT make further attempts to retrieve LI from this LIS. This error code is used to indicate that the Device is outside the access network served by the LIS; for instance, the VPN and NAT scenarios discussed in Section 4.1.2.

12. 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.

13. 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, Bernard Aboba, Eric Arolick, Richard Barnes (in particular the security section), Peter Blatherwick, Ben Campbell, Guy Caron, Eddy

Corbett, Martin Dawson, Lisa Dusseault, Robins George, Jerome Grenier, Ted Hardie, Cullen Jennings, Neil Justusson, Tat Lam, Marc Linsner, Patti McCalmont, Alexey Melnikov, Roger Marshall, Tim Polk, Perry Prozeniuk, Carl Reed, Julian Reschke, Eric Rescorla, Dan Romascanu, Brian Rosen, John Schnizlein, Shida Schubert, Henning Schulzrinne, Ed Shrum, Doug Stuard, Hannes Tschofenig and Karl Heinz Wolf.

14. Changes since last Version

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

Changes from 15 to 16(IESG Review DISCUSSES/comments):

1) Editorial Clarifications.

2) Section 6.4 added explicit reference to draft-ietf-ltru-4646bis

3) Section 6.5.3/examples (Expiry Time): clarified the details (UTC/ Gregorian calendar) for the expiry time and updated examples to include fractional seconds and trailing 'Z'.

4) Section 8: Clarified the usage of wildcards in the domain name for server authentication.

5) Section 10.1: Fixed examples - added charset attribute to Content Type and fixed lengths

6) Section 11.3 (IANA mime registration), replaced text for Optional paramters and Encoding considerations with references to RFC 3023. Fixed Macintosh File Type Code.

7) Updated location-conveyance reference to SIPCORE document.

Changes from 14 to 15(Gen-Art and IETF discussion ML comments post 3rd IETF LC):

1) Clarification around device support for cookies or basic/digest authentication.

2)Additional text in section 6.3 (PIDF-LO) around the LIS including (and not including) any information identifying the device in the returned PIDF-LO.

3) As always, a few additional editorial changes and clarifications.

Changes from 13 to 14 (AD comments post 2nd IETF LC):

1) Section 4.3: Removed reference to location-dereference protocol document. Generalized statement wrt HELD not meeting all the lbyr requirements (e.g., cancelling of location references).

2) Removed section 5.1 (Delivery Protocol) and just left the statement that this document describes the use of HTTP and that HELD is an application layer protocol.

3) Section 6.1: "the LIS should provide the most accurate LI" -> "the LIS provides the most accurate LI" to avoid the inference of a normative requirement.

4) Section 6.3: clarified "locationUnknown" error code.

5) Section 6.4: changed text to indication that errors can contain multiple "message" parameters to accommodate errors in different languages.

6) Section 7 : updated XML schema to reflect change in error message to accommodate multiple "message" parameters. Note, a few other changes to XML schema based on "strict" validation.

7) Section 8: clarified that redirect should be authenticated if the Device requires that the redirect server is authenticated.

8) Section 10:

- updated examples due to updates to XML schema

- removed empty POST example.

9) Section 11.4: Changed IANA registration for error codes from "Specification Required" to "Standards Action"

10) Other minor clarifications.

Changes from WG 12 to 13 (Post-2nd WGLC):

1) Fixed editorial error in section 6.2 with regards to empty "locationType" - error was introduced in 06 to 07 changes.

2) Added additional text in section 6.5.1 to improve security associated with locationURIs.

3) Modified XML schema for errorType and responseType to allow an attribute to be returned. Also, added extensibility to errorType.

Changes from WG 11 to 12 (Post-2nd WGLC):

1) Expanded text in section 8 (HTTP binding) to provide more detail about the requirements for an HTTP implementation supporting HELD. Clarified the mandatory functionality and specific handling of other functionality of HTTP.

2) Clarification in section 9.1 for clients that have external info wrt the identity or credentials of the LIS.

3) More nits.

Changes from WG 10 to 11 (Post-2nd WGLC):

1) Added additional text around the scope and applicability of the URI returned from LIS Discovery (section 4).

2) Removed HTTP GET - will always use POST.

3) Removed sentence wrt mobile devices in section 6.2.

4) Added specific recommendation for minimum value for expires in section 6.5.2 (30 Minutes).

5) Remove reference to RFC 3704 (for IP address spoofing) in section 9.3 (bullet 2).

6) Clarified that both HTTP and HTTPS are allowed - changed last bullet in section 5.1 from REQUIRES to RECOMMENDS.

7) Clarification wrt "presence" parameter in section 6.6 - a "single" presence parameter may be included.

Changes from WG 09 to 10 (2nd WGLC):

1) Updated text for Devices and VPNs (section 4.1.1) to include servers such as HTTP and SOCKs, thus changed the text to be generic in terms of locating LIS before connecting to one of these servers, etc.

2) Fixed (still buggy) HTTP examples.

3) Added text explaining the whitespaces in XML schema are for readability/document format limitations and that they should be handled via parser/schema validation.

4) Miscellaneous editorial nits

Changes from WG 08 to 09 (Post-IETF LC: continued resolution of sec-dir and gen-art review comments, along with apps-area feedback):

1) Removed heldref/heldrefs URIs, including fixing examples (which were buggy anyways).

2) Clarified text for locationURI - specifying that the deref protocol must define or appropriately restrict and clarifying that requirements for deref must be met and that deref details are out of scope for this document.

3) Clarified text in security section for support of both HTTP/HTTPS.

4) Changed definition for Location Type to force the specification of at least one location type.

Changes from WG 07 to 08 (IETF LC: sec-dir and gen-art review comments):

1) Fix editorial nits: rearranging sections in 4.1 for readibility, etc.

2) Added back text in Device and VPN section referencing DHCP and LLDP-MED when a VPN device serves as a LIS.

3) Clarified the use of both HTTP and HTTPS.

4) Defined two URIs related to 3 respectively - divided IANA registrations into sub-sections to accomodate this change. (Note: LIS Discovery will now define that URI, thus this document defines the one associatied with a Location reference).

5) Clarified the description of the location URI in Protocol Overview and Protocol parameter sections. Note that these sections again reference location dereference protocol for completeness and clarification of issues that are out of scope for this base document.

6) Defined new error code: notLocatable.

7) Clarifications and corrections in security section.

8) Clarified text for locationType, specifically removing extra text from "any" description and putting that in a separate paragraph. Also, provided an example.

9) Added boundaries for "expires" parameter.

10) Clarified that the HELD protocol as defined by this document does

not allow for canceling location references.

Changes from WG 06 to 07 (PROTO review comments):

1) Fix nits: remove unused references, move requirements to Informational References section, fix long line in ABNF, fix ABNF (quotes around '?'), add schemaLocation to import namespace in XML schema.

2) Remove text in Device and VPN section referencing DHCP and LLDP-MED when a VPN device serves as a LIS, per Issue 1 resolution at IETF-71. (Editorial oversight in producing version 06).

Changes from WG 05 to 06 (2nd WGLC comments):

1) Updated security section based on WG feedback, including condensing section 10.1.1 (Assuring the proper LIS has been contacted), restructuring sections by flattening, adding an additional step to the list that had been in the Accuracy section and removing summary section.

2) Changed URI schema to "helds" to address concerns over referential integrity and for consistency with mandate of TLS for HELD.

3) Editorial clarifications including fixing examples to match HELD URI definition (e.g., adding port, adding randomness to URI examples, etc.)

4) Updated references removing unused references and moving requirements docs to Informational Reference section to avoid downrefs.

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.

15. References

15.1. Normative References

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

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

[RFC2965] Kristol, D. and L. Montulli, "HTTP State Management Mechanism", RFC 2965, October 2000.

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, January 2004.

[RFC5491] Winterbottom, J., Thomson, M., and H. Tschofenig, "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations", RFC 5491, March 2009.

[W3C.REC-xmlschema-1-20041028] Maloney, M., Thompson, H., Mendelsohn, N., and D. Beech, "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>.

[W3C.REC-xmlschema-2-20041028] Malhotra, A. and P. Biron, "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>.

[I-D.ietf-geopriv-lis-discovery] Thomson, M. and J. Winterbottom, "Discovering the Local Location Information Server (LIS)", draft-ietf-geopriv-lis-discovery-11 (work in progress), May 2009.

15.2. Informative References

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, September 1981.

[RFC2617] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[RFC3023] Murata, M., St. Laurent, S., and D. Kohn, "XML Media Types", RFC 3023, January 2001.

[RFC3693] Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements", RFC 3693, February 2004.

[RFC3825] Polk, J., Schnizlein, J., and M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information", RFC 3825, July 2004.

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

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[I-D.ietf-ltru-4646bis] Phillips, A. and M. Davis, "Tags for Identifying Languages", draft-ietf-ltru-4646bis-23 (work in progress), June 2009.

[RFC4479] Rosenberg, J., "A Data Model for Presence", RFC 4479, July 2006.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[I-D.ietf-geopriv-l7-lcp-ps] Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol; Problem Statement and Requirements", draft-ietf-geopriv-l7-lcp-ps-10 (work in progress), July 2009.

[I-D.ietf-geopriv-lbyr-requirements] Marshall, R., "Requirements for a Location-by-Reference Mechanism", draft-ietf-geopriv-lbyr-requirements-07 (work in progress), February 2009.

[I-D.ietf-sipcore-location-conveyance] Polk, J. and B. Rosen, "Location Conveyance for the

Session Initiation Protocol",
draft-ietf-sipcore-location-conveyance-01 (work in
progress), July 2009.

Appendix A. HELD Compliance to IETF LCP requirements

This appendix describes HELD's compliance to the requirements specified in the [I-D.ietf-geopriv-l7-lcp-ps].

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 between a Device and a LIS. In the context of HELD, the LIS is within the Access Network. Thus, HELD is independent of the business or trust relationship between the Application Service Provider (ASP) and the Access Network Provider. Location acquisition using HELD is subject to the restrictions described in Section 9.

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 which can be bound to transports other than HTTP, such as BEEP. Using a protocol such as BEEP 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 [I-D.ietf-geopriv-lis-discovery].

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 ". [RFC5491]

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 [RFC5491].

Authors' Addresses

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

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 7A43
725 W Peachtree St.
Atlanta, GA 30308
US

Email: barbara.stark@att.com