

Geopriv  
Internet-Draft  
Intended status: Standards Track  
Expires: October 16, 2009

J. Winterbottom  
Andrew Corporation  
H. Tschofenig  
Nokia Siemens Networks  
M. Thomson  
Andrew Corporation  
April 14, 2009

Establishing Location URI Contexts using HTTP-Enabled Location Delivery  
(HELD)

[draft-winterbottom-geopriv-held-context-04](#)

Status of This Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on October 16, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (<http://trustee.ietf.org/license-info>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Internet-Draft

HELD Contexts

April 2009

## Abstract

This document describes a protocol extension for the HTTP-Enabled Location Delivery (HELD) protocol. It allows a Target to manage their location information on a Location Information Server (LIS) through the application of constraints invoked by accessing a location URI. Constraints described in this memo restrict how often location can be accessed through a location URI, how long the URI is valid for, and the type of location information returned when a location URI is accessed. Extension points are also provided.

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction . . . . .</a>	<a href="#">3</a>
<a href="#">2.</a>	<a href="#">Terminology . . . . .</a>	<a href="#">3</a>
<a href="#">3.</a>	<a href="#">HELD Contexts . . . . .</a>	<a href="#">4</a>
<a href="#">3.1.</a>	<a href="#">Simplified Model . . . . .</a>	<a href="#">4</a>
<a href="#">3.2.</a>	<a href="#">Authorization Policies . . . . .</a>	<a href="#">5</a>
<a href="#">3.3.</a>	<a href="#">Context Lifetime . . . . .</a>	<a href="#">6</a>
<a href="#">3.4.</a>	<a href="#">Snapshot Contexts . . . . .</a>	<a href="#">6</a>
<a href="#">4.</a>	<a href="#">Protocol Details . . . . .</a>	<a href="#">6</a>
<a href="#">4.1.</a>	<a href="#">Create Context . . . . .</a>	<a href="#">7</a>
<a href="#">4.2.</a>	<a href="#">Update Context . . . . .</a>	<a href="#">8</a>
<a href="#">4.3.</a>	<a href="#">Context Response Message . . . . .</a>	<a href="#">10</a>
<a href="#">4.4.</a>	<a href="#">Context Errors . . . . .</a>	<a href="#">11</a>
<a href="#">4.5.</a>	<a href="#">Location URI and Context Identifier Generation Rules . . .</a>	<a href="#">12</a>
<a href="#">5.</a>	<a href="#">XML Schema . . . . .</a>	<a href="#">12</a>
<a href="#">6.</a>	<a href="#">Security Considerations . . . . .</a>	<a href="#">15</a>
<a href="#">6.1.</a>	<a href="#">Multiple Contexts from the 'Same' Target . . . . .</a>	<a href="#">16</a>
<a href="#">7.</a>	<a href="#">IANA Considerations . . . . .</a>	<a href="#">16</a>
7.1.	URN Sub-Namespace Registration for urn:ietf:params:xml:ns:geopriv:held:context . . . . .	<a href="#">17</a>
<a href="#">7.2.</a>	<a href="#">XML Schema Registration . . . . .</a>	<a href="#">17</a>
<a href="#">7.3.</a>	<a href="#">HELD Error Code Registration . . . . .</a>	<a href="#">18</a>
<a href="#">8.</a>	<a href="#">Acknowledgements . . . . .</a>	<a href="#">18</a>
<a href="#">9.</a>	<a href="#">References . . . . .</a>	<a href="#">18</a>
<a href="#">9.1.</a>	<a href="#">Normative References . . . . .</a>	<a href="#">18</a>
<a href="#">9.2.</a>	<a href="#">Informative References . . . . .</a>	<a href="#">19</a>
<a href="#">Appendix A.</a>	<a href="#">Compliance to Location by Reference Requirements . .</a>	<a href="#">20</a>

Internet-Draft

HELD Contexts

April 2009

## 1. Introduction

The HTTP Enabled Location Delivery (HELD) protocol specification [[I-D.ietf-geopriv-http-location-delivery](#)] provides a set of features that can be used by a Target to retrieve location information from a Location Information Server (LIS). The LIS is able to optionally provide a location URI [[I-D.ietf-geopriv-lbyr-requirements](#)], which provides a reference to location information.

A location URI that is provided by a LIS using the basic HELD specification, is essentially immutable once retrieved. There is no means provided of controlling how the URI is used. A default policy is applied to the URI, which is fixed until the location URI expires; a Location Recipient in possession of the location URI can retrieve the Target's location until the expiry time lapses.

This basic mechanism may be reasonable in a limited set of applications, but is unacceptable in a broader range of applications. In particular, the ability to change policy dynamically is required to better protect the privacy of the Target.

[[I-D.ietf-geopriv-lbyr-requirements](#)] enumerates several requirements relating to location URIs that cannot be achieved using the basic HELD specification. This specification provides support for these requirements in HELD.

Two new forms of HELD request are defined by this document. These requests relate to the creation and maintenance of a `_HELD context_`, a concept that is explained in more detail in [Section 3](#).

## 2. Terminology

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

This document uses the terms defined in [[RFC3693](#)] (Target, Location

Recipient, Location Server), [[I-D.ietf-geopriv-lbyr-requirements](#)] (location URI), and [[I-D.ietf-geopriv-l7-lcp-ps](#)] (Location Information Server, or LIS).

The distinction between Location Server (LS) and Location Information Server (LIS) is important. LS is used to refer to the role that serves a location URI, whereas a LIS is the role that provides the location configuration. Both roles might be assumed by the same entity, but the roles could be separate.

### [3.](#) HELD Contexts

A location URI is a reference to the current location of a Target. The host identified in the URI, the Location Server (LS), serves requests to a location URI using two classes of data:

authorization policy: Authorization policies are set by Rule Makers and determine whether the requester is permitted to receive location information and whether there are any constraints on that information.

location determination inputs: Information on the identity of the Target and how location information for that Target can be acquired might be saved by the LS.

This information is associated with every location URI served by an LS. The collection of data used by the LS establishes a "context" for the location dereference request made by a Location Recipient.

In HELD [[I-D.ietf-geopriv-http-location-delivery](#)], the establishment of the necessary contextual information is implicit. Creation of a location URI implies that the LIS has provided the LS with sufficient information to service requests to that URI.

This document provides a more explicit mechanism for the creation and management of the contextual information used in serving a location URI. This information - dubbed a "HELD context" (simply "context" in this document) - can be created, updated and destroyed at the request of the Device. In addition, a Device is able to establish

authorization policies in the form of common policy documents [RFC4745] that provide greater control over how a location URI is served by the LS.

### 3.1. Simplified Model

The model assumed in this specification, shown in Figure 1, is a simplified variant of that in [RFC3693] that includes the LIS entity.

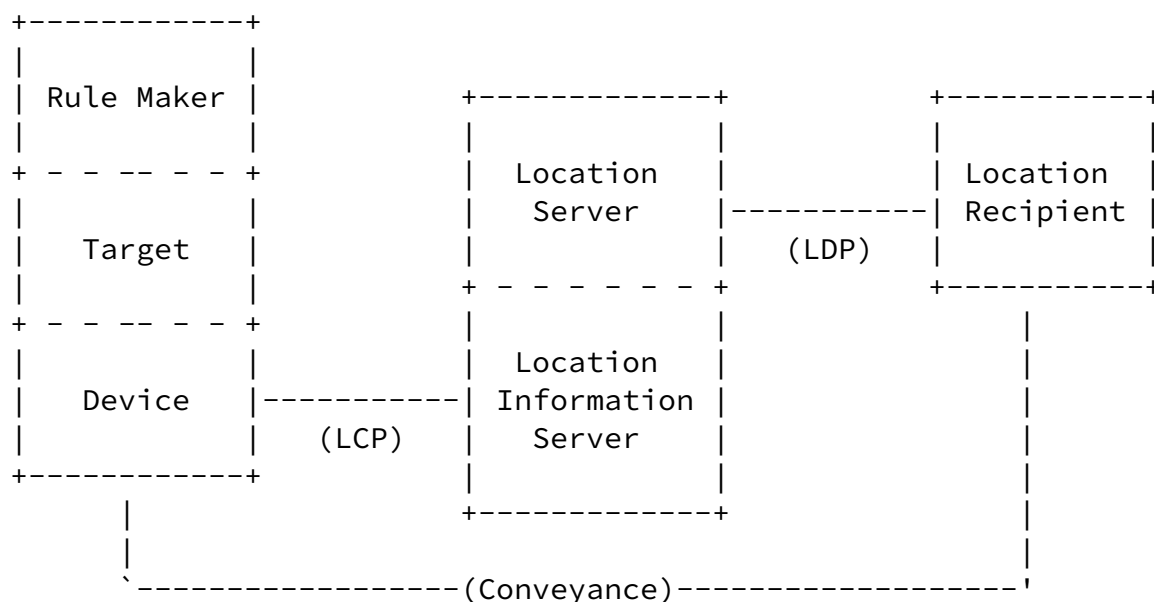


Figure 1: HELD Contexts Model

This model assumes some form of relationship between a Rule Maker, Target and Device; for instance, the Rule Maker and Target might be the same person. The Device is operated under the control of a Rule

Maker and is able to provide authorization policies or disseminate location URIs in accordance with the Rule Maker's wishes.

This document also assumes a relationship is assumed between LIS and LS. LIS and LS together generate location URIs and maintain context information. These roles could be filled by the same entity.

The location configuration protocol (LCP) interface is extended by this document to include a rules interface for the Rule Maker associated with the Target and Device. This model does not preclude the existence of other Rule Makers that use other rules interfaces.

### [3.2.](#) Authorization Policies

A Device is able to specify an authorization policy when creating or updating a context. The authorization policy states which Location Recipients are able to access location information through the context and the associated URIs, plus any other constraints on this access.

A Device is able to provide a policy document in the form of a common policy document [[RFC4745](#)] or an "https:" reference to one. Existence of an explicit authorization policy implies that the "authorization by access control lists" model ([\[I-D.ietf-geopriv-lbyr-requirements\]](#)) is to be applied. The LS uses the authorization policy document to control how location information is provided to Location Recipients.

Absence of policy, or an explicit indication otherwise, indicates that the LS is permitted to apply the "authorization by possession" model ([\[I-D.ietf-geopriv-lbyr-requirements\]](#)). Any Location Recipient that proves possession of the location URI by making a location dereference request to the URI is granted permission to receive the location information. Location URIs for the associated context have random components with enough entropy to make possession more likely to be as a result of receiving the location URI from the Device than guesswork.

### [3.3.](#) Context Lifetime

A HELD context has a finite lifetime. This limits the time that a context might refer to a Device that has since left the network. Of course, a LIS might have a means of detecting the absence of a given

Device, invalidating any contexts when the Device is no longer present.

The lifetime of the context is negotiated between Device and LIS. The Device requests a certain lifetime and the LIS provides a location URI that is valid for up to the requested time. A Device is able to extend the lifetime of a context by updating the context information. Given regular updates, a context might persist indefinitely, providing that authorization by possession is not used.

A Device can request that the LIS remove context information, invalidating the associated location URIs, by the same mechanism used to extend the lifetime.

### [3.4.](#) Snapshot Contexts

At the time that a context is created, the Device is able to request that the context refer to a static document that is created at the time of request. The LIS creates a Location Object (LO) based on the associated HELD request parameters and stores the LO. All requests to the location URI created in response to this request are served based on the stored LO.

This basic constraint on the context applies for the life of the context. Only the application of authorization policy rules can change what is provided to different Location Recipients. If authorization by possession is used, the associated location URI is different to a Location Object only in that it needs to be dereferenced.

## [4.](#) Protocol Details

This specification introduces three new HELD messages, create context (<createContext>), update context (<updateContext>), and context

response (<contextResponse>).

All context-related messages are HELD messages, sent using the "application/held+xml" MIME type defined in [\[I-D.ietf-geopriv-http-location-delivery\]](#).

A LIS that does not understand this specification returns a HELD "unsupportedMessage" error code in a HELD "error" message. A LIS

that does understand this specification returns errors associated with context operations in a HELD error message. New error codes relating to failed context operations are defined in [Section 4.4](#).

The specification assumes that the LIS was discovered as part of the LIS discovery [[I-D.ietf-geopriv-lis-discovery](#)] and that the LIS is able to provide location information.

#### [4.1](#). Create Context

The Device creates a context on the LIS using a create context message. A sample create context request is shown in Figure 2.

```
<createContext
  xmlns="urn:ietf:params:xml:ns:geopriv:held:context">
  <lifetime>7200</lifetime>
  <snapshot>false</snapshot>
  <policy>
    <ruleset-reference>
      http://policy.example.com/geolocation-policy/users/alice/index
    </ruleset-reference>
  </policy>
</createContext>
```

Figure 2: Create Context Example

The following parameters of the create context request are defined:

**lifetime:** The maximum lifetime of the context in seconds. All create contexts requests include this parameter. The LIS MAY create the context with a shorter lifetime than was requested, but the lifetime MUST NOT be longer than was requested.

**snapshot:** Whether the value provided to location Recipients is fixed from the time that the context is created (see [Section 3.4](#)). This a boolean parameter with a default value of "false", meaning that the context the Target's location at the time that the location URI is dereferenced.

**policy:** An authorization policy, either included directly as an



instance of a common policy [[RFC4745](#)] document, or by reference as a URI. Only one of the following forms of policy are permitted:

**cp:ruleset:** The Device is able to provide an authorization policy explicitly in the request by including a common policy document in the create context request. A "ruleset" element is included as a child of the "policy" element.

**ruleset-reference:** Alternatively, a reference to a policy document can be included using the "ruleset-reference" element. A Rule Maker might maintain an authorization policy on a server (perhaps with XCAP [[RFC4825](#)]). This reference MUST be an "https:" URI. The LS MUST retrieve the policy before granting any Location Recipient access to location information; the policy MAY either be retrieved immediately or as a Location Recipient makes a request. The LS can be expected to retrieve the policy document once only, but it MAY be retrieved multiple times.

Note that the LIS could be unable to detect errors in policy before sending a response to a request that includes this element. A successful context response might be sent, even if the policy document cannot be retrieved by the LIS or the referenced policy document is not understood by the LIS.

**possession:** Absence of policy information in a create context request implies that authorization by possession [[I-D.ietf-geopriv-lbyr-requirements](#)] is used for the context. The "possession" element provides an explicit indication that this policy is to be applied.

**otherPolicy:** Alternative policy information might be provided. This element is provided to allow for expansion. A LIS MAY reject requests that contain policy that it does not understand with the "badPolicy" error code.

#### [4.2.](#) Update Context

A Device is able to update policy or change the lifetime of a context using an update context request. Other context parameters defined in other specification might also be updated using this method.

Once created, a context that contains a "snapshot" of the Target's location cannot be made dynamic; the same applies in converse, a dynamic context cannot be made into a static snapshot.

A Device might maintain more than one HELD context; therefore, the

request needs to identify the context to be updated. The "context-id" is included in this message.

```
<updateContext
  xmlns="urn:ietf:params:xml:ns:geopriv:held:context">
  <context-id>uhvuhdbnuiehudbnvcujevuijeijcvij3</context-id>
  <lifetime>3600</lifetime>
  <policy>
    <cp:ruleset xmlns:cp="urn:ietf:params:xml:ns:common-policy">
      <!-- authorization policy rules -->
    </cp:ruleset>
  </policy>
</updateContext>
```

Figure 3: Update Context Example

When a Device includes a "lifetime" element in an update context message, the lifetime of the context is modified. If the requested lifetime is longer than the time remaining before the context expires, the context lifetime is lengthened. If the requested lifetime is shorter than the remaining time, the context lifetime is shortened.

A context that is updated continuously can be maintained indefinitely using this mechanism. The LIS MAY provide a shorter lifetime than the requested time. In particular, the total lifetime of contexts that use authorization by possession MUST be limited.

This mechanism also allows for the cancellation of contexts. The Device indicates a context lifetime of 0 in the update context request. The LIS MAY also terminate a context immediately if the lifetime value is less than 10 seconds.

```
<updateContext
  xmlns="urn:ietf:params:xml:ns:geopriv:held:context">
  <context-id>uhvuhdbnuiehudbnvcujevuijeijcvij3</context-id>
  <lifetime>0</lifetime>
  <policy>
    <possession/>
  </policy>
</updateContext>
```

Figure 4: Update Context Termination Example

When an update context request contains policy information, that policy information replaces any existing policy. Omitting the

"policy" element means that the previous policy remains unchanged. If a "ruleset-reference" element is provided, the LS MUST retrieve

the referenced policy document before serving subsequent requests from Location Recipients. Conditional HTTP requests, such as those containing the "If-Modified-Since" header MAY be used to avoid retrieval of the entire policy.

The rules regarding the construction of location URIs in [[I-D.ietf-geopriv-lbyr-requirements](#)] differ based on the authorization model used. The LIS MUST NOT permit a change in policy if the location URIs associated with the context do not meet the requirements for the updated authorization model. See [Section 4.5](#) for more details.

#### [4.3.](#) Context Response Message

The context response message is sent in response to a create context request or an update context request. This message includes information about the context that has been created, updated or destroyed.

The "code" attribute of the context response indicates what action was accomplished by the request:

created: The context was successfully created.

updated: The context was successfully updated.

destroyed: The context was destroyed.

The context response contains a "context" element that includes information about the context that was the subject of the request.

id: A value that uniquely identifies the context within the context of the LIS. This identifier is used to identify a context for update context requests. Knowledge of this value is used by the LIS to authenticate and authorize update context requests. The Target MUST keep this value secret.

expires: The time at which the context will expire. After this time, all location URIs that reference this context no longer

work.

snapshot: Whether the context contains a snapshot of the Target's location. This value has a default value of "false".

The LIS also provides a set of URIs that can be used to access the Target's location using the created context. The set of URIs does not change over the lifetime of the context.

A context response message sent in reply to the create context message in Figure 2 might look like Figure 5.

```
<contextResponse code="created"
  xmlns="urn:ietf:params:xml:ns:geopriv:held:context">
  <context id="uhvuhdbnuiehudbnvcujevuijeijcvij4"
    snapshot="false" expires="2007-11-01T13:30:00">
    <locationUriSet>
      <locationURI>
        https://lis.example.com:9768/357yc6s64ceyoiuy5ax3o4
      </locationURI>
      <locationURI>
        pres:357yc6s64ceyoiuy5ax3o4@lis.example.com:9769
      </locationURI>
    </locationUriSet>
  </context>
</contextResponse>
```

Figure 5: Context Response Example

#### [4.4.](#) Context Errors

A set of new HELD error codes are minted for use in context requests and responses:

**badPolicy:** The LIS (or LS) was unable to use the included policy due to it being invalid, badly formed, or inaccessible (when "ruleset-reference" is used). A LIS MAY return an error with this code if the policy contains no rules that could be used under any circumstances. For instance, all the rules might have validity intervals that do not correspond with the lifetime of the URI, or rules might require authentication modes that are not supported by

the LS.

**unknownContext:** The LIS was unable to find the context, possibly because the context identifier provided was invalid or because the context has already expired.

**contextFailure:** The LIS was unable to create or update the context.

Any other HELD error message can be provided in response to a create or update context request.

The following HELD error is sent in response to a create context request where the LIS indicates that snapshot is not supported.

```
<error xmlns="urn:ietf:params:xml:ns:geopriv:held"
  code="contextFailure" message="Snapshot is not supported"/>
```

Figure 6: Example Error Message

#### [4.5.](#) Location URI and Context Identifier Generation Rules

Location URIs generated by a LIS (or LS) MUST meet the construction requirements in [[I-D.ietf-geopriv-lbyr-requirements](#)]. In particular, the requirements for a location URI that operates on the authorization by possession model are more stringent than one that operates on an authorization policy.

Location URIs that operate on authorization by possession MUST be difficult to guess. Inclusion of a sequence of characters with at least 128 bits of random entropy is RECOMMENDED. More entropy might be required for location URIs with longer lifetimes. If the LIS permits changing of the authorization model that applies to a context, then the more stringent requirements MUST be complied with.

The context identifier provided by the LIS to the Target in the context response message MUST be unique. Context identifiers are

secrets used to indicate authorization for context update requests. Therefore, context identifiers MUST NOT be easily guessable. Inclusion of a sequence of characters with at least 128 bits of random entropy is RECOMMENDED.

A location URI MUST NOT include information that could be used in any way to derive the value of a context identifier. Similarly, context identifiers MUST NOT be based on Target identity.

New contexts MUST have unique location URIs that have not previously been used for other contexts, even if the previous context was for the same Target.

## [5.](#) XML Schema

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

```
<xs:annotation>
  <xs:appinfo
    source="urn:ietf:params:xml:schema:geopriv:held:context">
    HELD Context Management
  </xs:appinfo>
  <xs:documentation source="http://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 messages for HELD context management.
  </xs:documentation>
</xs:annotation>

<xs:import namespace="urn:ietf:params:xml:ns:common-policy"/>

<xs:complexType name="policyType">
  <xs:complexContent>
    <xs:restriction base="xs:anyType">
      <xs:choice>
```

```

        <xs:element name="ruleset-reference" type="xs:anyURI"/>
        <xs:element ref="cp:ruleset"/>
        <xs:element name="possession" type="ctxt:empty"/>
        <xs:element name="otherPolicy" type="xs:anyType"/>
    </xs:choice>
</xs:restriction>
</xs:complexContent>
</xs:complexType>

<xs:complexType name="createContextType">
    <xs:complexContent>
        <xs:restriction base="xs:anyType">
            <xs:sequence>
                <xs:element name="lifeTime" type="xs:nonNegativeInteger"/>
                <xs:element name="snapshot" type="xs:boolean"/>
                <xs:element name="policy" type="ctxt:policyType"
                    minOccurs="0"/>
                <xs:any namespace="##other" processContents="lax"
                    minOccurs="0" maxOccurs="unbounded"/>
            </xs:sequence>
            <xs:anyAttribute namespace="##any" processContents="lax"/>
        </xs:restriction>
    </xs:complexContent>
</xs:complexType>

<xs:complexType name="updateContextType">
    <xs:complexContent>
        <xs:restriction base="xs:anyType">
            <xs:sequence>
                <xs:element name="context-id" type="xs:NCName"/>
            </xs:sequence>
        </xs:restriction>
    </xs:complexContent>
</xs:complexType>

```

```

        <xs:element name="lifeTime" type="xs:nonNegativeInteger"
            minOccurs="0"/>
        <xs:element name="policy" type="ctxt:policyType"
            minOccurs="0"/>
        <xs:any namespace="##other" processContents="lax"
            minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:restriction>
</xs:complexContent>
</xs:complexType>

```

```

<xs:simpleType name="codeType">
  <xs:restriction base="xs:token">
    <xs:enumeration value="created"/>
    <xs:enumeration value="updated"/>
    <xs:enumeration value="destroyed"/>
  </xs:restriction>
</xs:simpleType>

<xs:complexType name="uriSetType">
  <xs:complexContent>
    <xs:restriction base="xs:anyType">
      <xs:sequence>
        <xs:element name="locationURI" type="xs:anyURI"
          minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="contextType">
  <xs:complexContent>
    <xs:restriction base="xs:anyType">
      <xs:sequence>
        <xs:element name="locationUriSet" type="ctxt:uriSetType"/>
        <xs:any namespace="##other" processContents="lax"
          minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
      <xs:attribute name="id" type="xs:ID" use="required"/>
      <xs:attribute name="expires" type="xs:dateTime"
        use="required"/>
      <xs:attribute name="snapshot" type="xs:boolean"
        use="optional"/>
      <xs:anyAttribute namespace="##any" processContents="lax"/>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>

```

```

<xs:complexType name="contextResponseType">
  <xs:complexContent>
    <xs:restriction base="xs:anyType">
      <xs:sequence>

```



```

        <xs:element name="context" type="ctxt:contextType"/>
        <xs:any namespace="##other" processContents="lax"
            minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="code" type="ctxt:codeType"
        use="required"/>
    <xs:anyAttribute namespace="##any" processContents="lax"/>
</xs:restriction>
</xs:complexContent>
</xs:complexType>

<xs:element name="createContext" type="ctxt:createContextType"/>
<xs:element name="updateContext" type="ctxt:updateContextType"/>
<xs:element name="contextResponse" type="ctxt:contextResponseType"/>

</xs:schema>

```

## 6. Security Considerations

The data that is maintained in a HELD context is privacy sensitive information. This information is provided by a Device for the purposes of providing authorized Location Recipients with location information. The LIS MUST NOT use the information it stores in a HELD context for anything other than serving requests to the associated location URIs.

The LS MUST enforce the authorization policy established by the Device. The authorization policy determines which Location Recipients are permitted to receive location information, and how that location information is provided. An authorization policy can be updated by the Device at any time using the update context request; after the LIS responds to this request, the authorization policy applies to all subsequent requests from Location Recipients.

An authorization policy can be referenced using "ruleset-reference" in a create context or update context request. The LS MUST retrieve any referenced authorization policy using HTTP over TLS [[RFC2818](#)] before providing location information to any Location Recipient.

Context identifiers are confidential information shared only between LIS and Device. Location URIs are also confidential if authorization by possession is chosen by the device, in which case the location URI is shared only between LIS, Device and authorized Location Recipients. The LIS MUST ensure that context identifiers and

location URIs are constructed following the rules described in [Section 4.5](#) of this document.

HELD [[I-D.ietf-geopriv-http-location-delivery](#)] mandates the use of TLS for exchanges between a Device and the LIS. TLS provides confidentiality, protection from modification, LIS (and possibly Device) authentication. Messages related to HELD contexts contain information that requires the same protections.

### [6.1.](#) Multiple Contexts from the 'Same' Target

It is conceivable that a LIS will be required to provide location to Devices residing behind a NAT. A home gateway is a good example of a situation where the relatively small geographic area served by the gateway is adequately served by a LIS external to that network. Devices within the home network appear to have the same identity information to a LIS - requests all originate from the same IP address. In this case, each Device might create its own context on the LIS. The LIS treats each context individually even though the LIS might be unable to distinguish between the actual Devices making the requests.

It is also possible that a single Device could request multiple contexts. Devices might have multiple users, or multiple applications running that each have have different privileges, different privacy requirements or different Rule Makers. Therefore, might create different contexts for different uses: each might a different policy that reflects the needs of the user or application. Information provided by a Device related to a context MUST NOT be used by the LIS outside of that context.

The state information maintained by the LIS or LS in providing a context presents a denial of service attack vector. Limiting the number of contexts that the LIS allows to be created can protect against such attacks. Any limits need to consider the usage pattern expected. If home gateways are commonly deployed in the access network, then the LIS MUST allow for more than one context for each discrete identifier. However, to ensure that LIS resources are not exhausted, the LIS MUST limit the number of contexts that it permits from each identifier.

## [7.](#) IANA Considerations

This document registers the schema and associated namespace with IANA.

Internet-Draft

HELD Contexts

April 2009

### [7.1.](#) URN Sub-Namespace Registration for urn:ietf:params:xml:ns:geopriv:held:context

This section registers a new XML namespace,  
"urn:ietf:params:xml:ns:geopriv:held:context", as per the guidelines  
in [[RFC3688](#)].

URI: urn:ietf:params:xml:ns:geopriv:held:context

Registrant Contact: IETF, GEOPRIV working group,  
(geopriv@ietf.org), James Winterbottom  
(james.winterbottom@andrew.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 Context Management Messages</title>
    </head>
    <body>
      <h1>Namespace for HELD Context Management Messages</h1>
      <h2>urn:ietf:params:xml:ns:geopriv:held:context</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
```

### [7.2.](#) XML Schema Registration

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

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

Registrant Contact: IETF, GEOPRIV working group, (geopriv@ietf.org),  
James Winterbottom (james.winterbottom@andrew.com).

Schema: The XML for this schema can be found as the entirety of  
[Section 5](#) of this document.

### [7.3.](#) HELD Error Code Registration

Reference: [Section 4.4](#) of RFCXXXX (i.e., this document) specifies the following HELD error codes:

badPolicy

unknownContext

contextFailure

These error codes and their descriptions are added to the HELD error code repository defined in  
[\[I-D.ietf-geopriv-http-location-delivery\]](#).

## [8.](#) Acknowledgements

Thanks to Adam Muhlbauer and Neil Justusson for their comments on the pre-version of this draft.

Thanks also to Tim Zelinski and Michael Diponio, who pointed out a problems while implementing an early revision of this specification.

## [9.](#) References

### [9.1.](#) Normative References

[RFC2119]

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

- [RFC2818] Rescorla, E., "HTTP Over TLS", [RFC 2818](#), May 2000.
- [RFC3688] Mealling, M., "The IETF XML Registry", [BCP 81](#), [RFC 3688](#), January 2004.
- [RFC4745] Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J., and J. Rosenberg, "Common Policy: A Document Format for Expressing Privacy Preferences", [RFC 4745](#), February 2007.

Winterbottom, et al. Expires October 16, 2009 [Page 18]

---

Internet-Draft HELD Contexts April 2009

- [I-D.ietf-geopriv-http-location-delivery] Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, "HTTP Enabled Location Delivery (HELD)", [draft-ietf-geopriv-http-location-delivery-13](#) (work in progress), February 2009.

## [9.2](#). Informative References

- [RFC3693] Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements", [RFC 3693](#), February 2004.
- [RFC4825] Rosenberg, J., "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)", [RFC 4825](#), May 2007.
- [I-D.ietf-geopriv-l7-lcp-ps] Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location

	Configuration Protocol; Problem Statement and Requirements", <a href="#">draft-ietf-geopriv-l7-lcp-ps-09</a> (work in progress), February 2009.
[I-D.ietf-geopriv-lbyr-requirements]	Marshall, R., "Requirements for a Location-by-Reference Mechanism", <a href="#">draft-ietf-geopriv-lbyr-requirements-07</a> (work in progress), February 2009.
[I-D.ietf-geopriv-lis-discovery]	Thomson, M. and J. Winterbottom, "Discovering the Local Location Information Server (LIS)", <a href="#">draft-ietf-geopriv-lis-discovery-09</a> (work in progress), March 2009.

## [Appendix A](#). Compliance to Location by Reference Requirements

This section describes how HELD and this specification comply to the location configuration protocol requirements stipulated in [\[I-D.ietf-geopriv-lbyr-requirements\]](#).

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

Compliant: HELD only provides location references in URI form.

- C2. "Location URI expiration: When a location URI has a limited validity interval, its lifetime MUST be indicated."

Compliant: All location URIs provided expire; the context response message indicates when the URI expires.

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

specific location URI."

Compliant: Updating a context with a lifetime set to zero cancels a context.

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

Compliant: With an explicit reference to this requirement, the URIs produced for a HELD context are required to comply with this condition.

- C5. "User Identity Protection: The location URI MUST NOT contain any user identifying information that identifies the user, device or address of record, (e.g., which includes phone extensions, badge numbers, first or last names, etc.), within the URI form."

Compliant: With an explicit reference to this requirement, the URIs produced for a HELD context are required to comply with this condition.

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

Not compliant.

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

Compliant: The "expires" attribute indicates the time when the context becomes invalid.

- C8. "Location only: The location URI MUST NOT point to any information about the Target other than it's location."

Compliant: PIDF-LO documents that are produced by the LS in response to a request at the URI do not contain Target

identification, unless policy states otherwise.

- C9. "Location URI Not guessable: Where location URIs are used publicly, any location URI MUST be constructed using properties of uniqueness and cryptographically random sequences so that it is not guessable. (Note that the number of bits depends to some extent on the number of active location URIs that might exist at the one time; 128-bit is most likely enough for the near term.)"

Compliant: [Section 4.5](#) describes how this requirement is met by implementations.

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

Not compliant: The format of location URIs generated by the LIS cannot be influenced through any of the parameters described in this document.

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

Compliant: The authorization model is explicitly selected by the Device in the request.

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

Duplicate requirement.



University of Wollongong, NSW 2500  
AU

Phone: +61 242 212938  
EMail: james.winterbottom@andrew.com  
URI: <http://www.andrew.com/products/geometrix>

Hannes Tschofenig  
Nokia Siemens Networks  
Linnoitustie 6  
Espoo 02600  
Finland

Phone: +358 (50) 4871445  
EMail: Hannes.Tschofenig@gmx.net  
URI: <http://www.tschofenig.priv.at>

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

Phone: +61 242 212915  
EMail: martin.thomson@andrew.com  
URI: <http://www.andrew.com/products/geometrix>