Geopriv	J. Winterbottom	
Internet-Draft	Andrew Corporation	
Intended status: Standards Track	H. Tschofenig	
Expires: April 25, 2010	Nokia Siemens Networks	
	M. Thomson	
	Andrew Corporation	
	October 22, 2009	

TOC

Location URI Contexts in HTTP-Enabled Location Delivery (HELD)
draft-winterbottom-geopriv-held-context-05

Status of This Memo

Copyright Notice

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 are described that allow control over how long the URI is valid for and the access policy used when a location URI is accessed.

Table of Contents

---

1. Introduction

TOC

The HTTP Enabled Location Delivery (HELD) protocol specification [I-D.ietf-geopriv-http-location-delivery] (Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, "HTTP Enabled Location Delivery (HELD)," August 2009.) 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 (Marshall, R., "Requirements for a Location-by-Reference Mechanism," November 2009.) [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 more able to protect the privacy of the Target. [I-D.ietf-geopriv-lbyr-requirements] (Marshall, R., "Requirements for a Location-by-Reference Mechanism," November 2009.) enumerates several requirements relating to location URIs that cannot be achieved using the basic HELD specification. This specification addresses 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 (HELD Contexts).

---

2. Terminology

TOC

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] (Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.).
This document uses the terms defined in [I-D.ietf-geopriv-arch] (Barnes, R., Lepinski, M., Cooper, A., Morris, J., Tschofenig, H., and H. Schulzrinne, "An Architecture for Location and Location Privacy in Internet Applications," October 2009.) (Target, Location Recipient, Location Server), [I-D.ietf-geopriv-lbyr-requirements] (Marshall, R., "Requirements for a Location-by-Reference Mechanism," November 2009.) (location URI), and [I-D.ietf-geopriv-l7-lcp-ps] (Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol; Problem Statement and Requirements," July 2009.) (Location Information Server, or LIS).

---

3. HELD Contexts

TOC

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.
The LS role could be assumed by the LIS that provides the location URI to the Device, or it could be a separate entity.
In HELD (Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, "HTTP Enabled Location Delivery (HELD)," August 2009.) [I-D.ietf-geopriv-http-location-delivery], the establishment of the necessary contextual information is implicit. Creation of a location URI implies that the identified LS has 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. 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 (Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J., and J. Rosenberg, "Common Policy: A Document Format for Expressing Privacy Preferences," February 2007.) [RFC4745] that provide greater control over how a location URI is served by the LS.

3.1. Simplified Model

TOC

The model assumed in this specification, shown in Figure 1 (HELD Contexts Model), is a simplified variant of that in [I-D.ietf-geopriv-arch] (Barnes, R., Lepinski, M., Cooper, A., Morris, J., Tschofenig, H., and H. Schulzrinne, "An Architecture for Location and Location Privacy in Internet Applications," October 2009.) that includes the LIS entity.

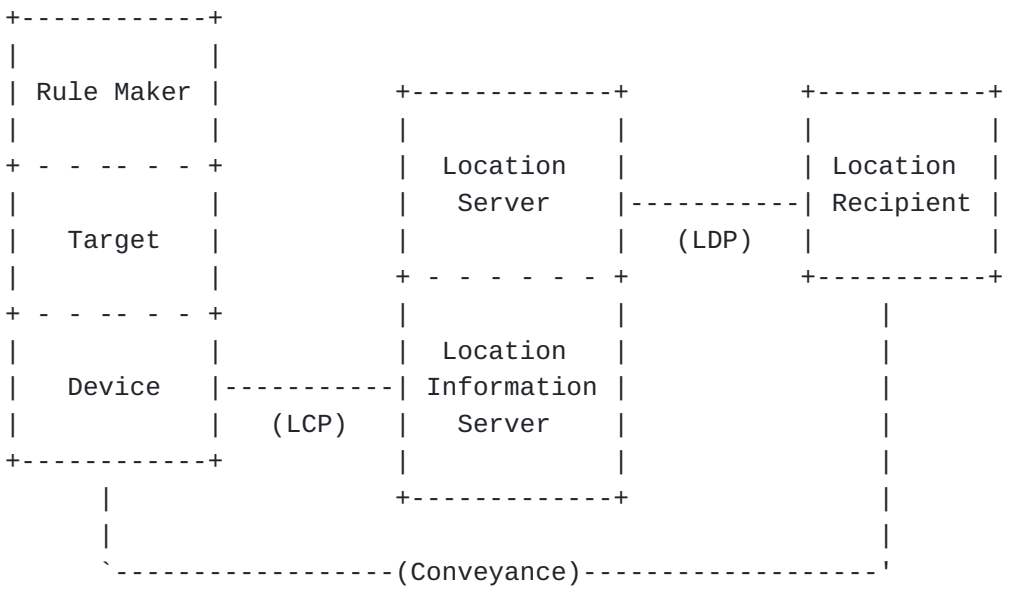

Figure 1: HELD Contexts Model

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

TOC

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 (Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J., and J. Rosenberg, “Common Policy: A Document Format for Expressing Privacy Preferences,” February 2007.) [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] (Marshall, R., “Requirements for a Location-by-Reference Mechanism,” November 2009.)) is to be applied. The LS uses the authorization policy document to control how location information is provided to Location Recipients.
A Device is able to indicate that the LS is permitted to apply the "authorization by possession" model to the context (see [I-D.ietf-geopriv-lbyr-requirements] (Marshall, R., “Requirements for a Location-by-Reference Mechanism,” November 2009.) and [I-D.ietf-geopriv-arch] (Barnes, R., Lepinski, M., Cooper, A., Morris, J., Tschofenig, H., and H. Schulzrinne, “An Architecture for Location and Location Privacy in Internet Applications,” October 2009.)). 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 MUST contain enough random entropy proof of possession of the URI more likely to be as a result of receiving the location URI from the Device than guessing.

3.3. Context Lifetime

TOC

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 MAY remove a context sooner, particularly if it has a means of detecting when the Device becomes absent.
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 any period less than the requested time. Later requests by the Device can be used to delay the expiration of a context by requesting an extended lifetime. With regular updates a context could persist indefinitely.

> Note that a LIS SHOULD NOT allow URIs that follow the authorization by possession model to exist indefinitely, since no means is provided for updating policy to revoke access to location information.

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

3.4. Snapshot Contexts

TOC

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

TOC

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] (Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, "HTTP Enabled Location Delivery (HELD)," August 2009.).
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 (Context Errors).
The specification assumes that the LIS was discovered as part of the LIS discovery (Thomson, M. and J. Winterbottom, "Discovering the Local Location Information Server (LIS)," March 2010.)
[I-D.ietf-geopriv-lis-discovery] and that the LIS is able to provide location information.

4.1. Create Context

TOC

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

```
<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 (Snapshot Contexts)). This a boolean parameter with a default value of false, meaning that the location is generate each time that the location URI is dereferenced or recently cached information is used.

policy: An authorization policy, either included directly as an instance of a common policy (Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J., and J. Rosenberg, "Common Policy: A Document Format for Expressing Privacy Preferences," February 2007.) [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 (Rosenberg, J., "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)," May 2007.) [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: This element indicates that authorization by possession (Marshall, R., "Requirements for a Location-by-Reference Mechanism," November 2009.) [I-D.ietf-geopriv-lbyr-requirements] is to be used for the context.

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

TOC

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] (Marshall, R., "Requirements for a Location-by-Reference Mechanism," November 2009.) 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 (Location URI and Context Identifier Generation Rules) for more details.

4.3. Context Response Message

TOC

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 any attempts to update the context. 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 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 (Create Context Example) might look like Figure 5 (Context Response Example).

```
<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

TOC

A set of 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 by the LS. 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

TOC

Location URIs generated by a LIS (or LS) MUST meet the construction requirements in [I-D.ietf-geopriv-lbyr-requirements] (Marshall, R., "Requirements for a Location-by-Reference Mechanism," November 2009.). If the LIS permits changing of the authorization model that applies to a context, then the more stringent requirements MUST be complied with. 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 rely on being difficult to guess to prevent unintential disclosure of location information. A LIS MUST include a sequence of characters with random entropy sufficient to prevent guessing. In general, more entropy is needed for location URIs with longer lifetimes.

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 contain sufficient random entropy that they are not easily guessable.

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. This might be achieved by including a monotonically increasing sequence number in addition to the random sequence.

TOC

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: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

TOC

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 (Rescorla, E., "HTTP Over TLS," May 2000.) [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 (Location URI and Context Identifier Generation Rules) of this document.
HELD (Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, "HTTP Enabled Location Delivery (HELD)," August 2009.)
[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

TOC

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 (see [I-D.ietf-geopriv-l7-lcp-ps] (Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol; Problem Statement and Requirements," July 2009.)). 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 are controlled by different Rule Makers. Therefore, different contexts might be used 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. To ensure that LIS resources are not exhausted, the LIS MUST limit the number of contexts that it permits from each identifier.

> Any limits need to consider the usage pattern expected. For instance, if home gateways are commonly deployed in the access network, then the LIS might allow for more than one context for each discrete identifier.

---

7. IANA Considerations

TOC

This document registers the schema and associated namespace with IANA.

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

TOC

This section registers a new XML namespace, urn:ietf:params:xml:ns:geopriv:held:context, as per the guidelines in [RFC3688] (Mealling, M., “The IETF XML Registry,” January 2004.).

> 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

TOC

This section registers an XML schema as per the guidelines in [RFC3688] (Mealling, M., "The IETF XML Registry," January 2004.).

> **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 (XML Schema) of this document.

7.3. HELD Error Code Registration

TOC

Reference: Section 4.4 (Context Errors) 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 respository created in [I-D.ietf-geopriv-http-location-delivery] (Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, "HTTP Enabled Location Delivery (HELD)," August 2009.).

---

8. Acknowledgements

TOC

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

TOC

9.1. Normative References

TOC

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC2818]	Rescorla, E., "HTTP Over TLS," RFC 2818, May 2000 (TXT).
[RFC3688]	Mealling, M., "The IETF XML Registry," BCP 81, RFC 3688, January 2004 (TXT).
[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 (TXT).
[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-16 (work in progress), August 2009 (TXT).

9.2. Informative References

TOC

[RFC3693]	Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements," RFC 3693, February 2004 (TXT).
[RFC4825]	Rosenberg, J., "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)," RFC 4825, May 2007 (TXT).
[I-D.ietf-geopriv-arch]	Barnes, R., Lepinski, M., Cooper, A., Morris, J., Tschofenig, H., and H. Schulzrinne, "An Architecture for Location and Location Privacy in Internet Applications," draft-ietf-geopriv-arch-01 (work in progress), October 2009 (TXT).
[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 (TXT).
[I-D.ietf-geopriv-lbyr-requirements]	Marshall, R., "Requirements for a Location-by-Reference Mechanism," draft-ietf-geopriv-lbyr-requirements-09 (work in progress), November 2009 (TXT).
[I-D.ietf-geopriv-lis-discovery]	Thomson, M. and J. Winterbottom, "Discovering the Local Location Information Server (LIS)," draft-ietf-geopriv-lis-discovery-15 (work in progress), March 2010 (TXT).

Appendix A. Compliance to Location by Reference Requirements

TOC

This section describes how HELD and this specification comply to the location configuration protocol requirements stipulated in [I-D.ietf-geopriv-lbyr-requirements] (Marshall, R., “Requirements for a Location-by-Reference Mechanism,” November 2009.).

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 MUST, through randomization and uniqueness, ensure that the location URI does not contain location information specific components."
Compliant: The URIs produced for a HELD context are required to comply with this condition, see Section 4.5 (Location URI and Context Identifier Generation Rules).

C5. "Target Identity Protection: The location URI MUST NOT contain information that identifies the Target (e.g., user or device)."
Compliant: The URIs produced for a HELD context are required to comply with this condition, see Section 4.5 (Location URI and Context Identifier Generation Rules).

C6. "Reuse indicator: There SHOULD be a way to allow a Target to control whether a location URI can be resolved once only, or multiple times."
Not compliant: No means is provided to control how often a URI can be resolved. Extensions to this mechanism or additions to authorization policy definitions might provide this function.

C7. "Selective disclosure: The location configuration protocol MUST provide a mechanism to control what information is being disclosed about the Target."
Compliant: Policy (Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J., and J. Rosenberg, “Common Policy: A Document Format for Expressing Privacy Preferences,” February 2007.) [RFC4745] is used to control what information is

disclosed about the target. No information about the Target is included in a location URI.

C8. "Location URI Not guessable: As a default, the location configuration protocol MUST return location URIs that are random and unique throughout the indicated lifetime. A location URI with 128-bits of randomness is RECOMMENDED."
Compliant: Section 4.5 (Location URI and Context Identifier Generation Rules) describes how this requirement is met by implementations.

C9. "Location URI Options: In the case of user-provided authorization policies, where anonymous or non-guessable location URIs are not warranted, the location configuration protocol MAY support a variety of optional location URI conventions, as requested by a Target to a location configuration server, (e.g., embedded location information within the location URI)."
Partially compliant: The authorization model is explicitly selected by the Device in the request. This determines the constraints on how the location URI is created. No means is provided for a Target or other entity to otherwise influence what information is included in a location URI. This may be provided by extension documents.

Authors' Addresses

TOC

	James Winterbottom
	Andrew Corporation
	PO Box U40
	University of Wollongong, NSW 2500
	AU
Phone:	+61 242 212938
EMail:	james.winterbottom@andrew.com
URI:	http://www.andrew.com/products/geometrix
	Hannes Tschofenig
	Nokia Siemens Networks
	Linnoitustie 6
	Espoo 02600
	Finland
Phone:	+358 (50) 4871445
EMail:	Hannes.Tschofenig@gmx.net
URI:	http://www.tschofenig.priv.at
	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