Geopriv
Internet-Draft
Intended status: Standards Track
Expires: April 23, 2011

J. Winterbottom
M. Thomson
Andrew Corporation
H. Tschofenig
Nokia Siemens Networks
R. Barnes
BBN Technologies
October 20, 2010

Use of Device Identity in HTTP-Enabled Location Delivery (HELD)
draft-ietf-geopriv-held-identity-extensions-05

Abstract

When a Location Information Server receives a request for location information (using the locationRequest message), described in the base HTTP Enabled Location Delivery (HELD) specification, it uses the source IP address of the arriving message as a pointer to the location determination process. This is sufficient in environments where the location of a Device can be determined based on its IP address.

Two additional use cases are addressed by this document. In the first, location configuration requires additional or alternative identifiers from the source IP address provided in the request. In the second, an entity other than the Device requests the location of the Device.

This document extends the HELD protocol to allow the location request message to carry Device identifiers. Privacy and security considerations describe the conditions where requests containing identifiers are permitted.

Status of this Memo

This Internet-Draft will expire on April 23, 2011.

Copyright Notice

Table of Contents

1. Introduction

Protocols for requesting and providing location information require a way for the requestor to specify the location that should be returned. In a Location Configuration Protocol (LCP), the location being requested is the requestor's location. This fact can make the problem of identifying the Device simple, since IP datagrams that carry the request already carry an identifier for the Device, namely the source IP address of an incoming request. Existing LCPs, such as HTTP-Enabled Location Delivery (HELD) [I-D.ietf-geopriv-http-location-delivery] and DHCP ([RFC3825], [RFC4776]) rely on the source IP address or other information present in protocol datagrams to identify a Device.

Aside from the datagrams that form a request, a Location Information Server (LIS) does not necessarily have access to information that could further identify the Device. In some circumstances, as shown in [RFC5687], additional identification information can be included in a request to identify a Device.

This document extends the HELD protocol to support the inclusion of additional identifiers for the Device in HELD location requests. An XML schema is defined that provides a structure for including these identifiers in HELD requests.

An important characteristic of this addition is that the HELD protocol with identity extensions implemented is not considered an LCP. The scope of an LCP is limited to the interaction between a Device and a LIS, and LCPs can guarantee the identity of Devices

without additional authorization checks. A LIS identifies the Device making the LCP request using the source addressing on the request packets, using return routability to ensure that these identifiers are not spoofed.

HELD with identity extensions allows a requester to explicitly provide identification details in the body of a location request. This means that location requests can be made in cases where additional Device identity checks are necessary, and in cases where the requester is not the Device itself. Third party Location Recipients (LRs) are able to make requests that include identifiers to retrieve location information about a particular Device.

The usage of identifiers in HELD introduces a new set of privacy concerns. In an LCP, the requester can be implicitly authorized to access the requested location information, because it is their own location. In contrast, a third party LR must be explicitly authorized when requesting the location of a Device. Establishing appropriate authorization and other related privacy concerns are

discussed in Section 4.

1.1. Applications

This document defines a means to explicitly include Device identity information in the body of a HELD location request. This identity information is used to identify the Device that is the subject (or Target) of the location request. If device identity is present, the identity of the requester is not used to identify the subject of the request.

Device identifiers in HELD can be used for two purposes:

Location configuration: A Device can use these parameters to identify itself to a LIS. Identification information other than an IP address might be needed to determine the location of a Device.

A LIS can authorize location configuration requests using a policy that allows Devices to acquire their own location (see Section 4.1). If an unauthorized third party falsifies addressing on request packets to match the provided Device identity, the

request might be erroneously authorized under this policy. Requests containing Device identity MUST NOT be authorized using this policy unless specific measures are taken to prevent this type of attack.

This document describes a mechanism that provides assurances that the requester and included Device identity are the same for the Network Access Identifier (NAI) in a WiMAX network. The LIS MUST treat requests containing other identifiers as third party requests, unless it is able to ensure that the provided Device identity is uniquely attributable to the requester.

Third party requests: A third party location recipient can be granted authorization to make requests for a given Device. In particular, network services can be permitted to retrieve location for a Device that is unable to acquire location information for itself (see Section 6.3 of [I-D.ietf-ecrit-phonebcp]). This allows use of location-dependent applications - particularly essential services like emergency calling - where Devices do not support a location configuration protocol or they are unable to successfully retrieve location information.

This document does not describe how a third party acquires an identifier for a Device, nor how that third party is authorized by a LIS. It is critical that these issues are resolved before permitting a third party request. A pre-arranged contract between

the third party, a Rule Maker and the LIS operator is necessary to use Device identifiers in this fashion. This contract must include how the request is authenticated and the set of identifiers (and types of identifiers) that the third party is authorized to use in requests.

Automated mechanisms to ensure privacy constraints are respected are possible. For instance, a policy rules document could be used to express the agreed policy. Formal policy documents, such as the common policy [RFC4745], can be applied in an automated fashion by a LIS.

1.2. Terminology

This document uses the term Location Information Server (LIS) and

Location Configuration Protocol (LCP) as described in [RFC5687] and [I-D.ietf-geopriv-arch].

The term Device is used specifically as the subject of an LCP, consistent with [I-D.ietf-geopriv-http-location-delivery]. This document also uses the term Target to refer to any entity that might be a subject of the same location information. Target is used in a more general sense, including the Device, but also any nearby entity, such as the user of a Device.

A Target has a stake in setting authorization policy on the use of location information. A Rule Maker is the term used for the role that makes policy decisions about authorization, determining what entities are permitted to receive location and how that information is provided.

Device, Target and Rule Maker are defined in [I-D.ietf-geopriv-arch].

The term "requester" is used in this document to refer to the entity making a HELD request.

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].

2. Device Identity

Identifiers are used as the starting point in location determination. They should not be confused with measurement information ([I-D.thomson-geopriv-held-measurements]). Measurement information is information about a Device and the time varying details of its network attachment. Identifiers might be associated with a different Device over time, but their purpose is to identify the Device, not to

describe its environment or network attachment.

2.1. Identifier Suitability

Use of any identifier MUST only be allowed if it identifies a single Device at the time that location is determined. The LIS is responsible for ensuring that location information is correct for the Device, which includes ensuring that the identifier is uniquely attributable to the Device.

Some identifiers can be either temporary or could potentially identify multiple Devices. Identifiers that are transient or ambiguous could be exploited by an attacker to either gain information about another Device or to coerce the LIS into producing misleading information.

The identifiers described in this document MUST only be used where that identifier is used as the basis for location determination. Considerations relating to the use of identifiers for a Device requesting its own location are discussed in Section 5 of [RFC5687]; this section discusses use of identifiers for authorized third party requests.

> It is tempting for a LIS implementation to allow alternative identifiers for convenience or some other perceived benefit. The LIS is responsible for ensuring that the identifier used in the request does not refer to a Device other than the one for which it determines location.

Some identifiers are always uniquely attributable to a single Device. However, other identifiers can have a different meaning to different entities on a network. This is especially true for IP addresses [RFC2101], but this can be true for other identifiers to varying degrees. Non-uniqueness arises from both topology (all network entities have a subjective view of the network) and time (the network changes over time).

2.1.1. Subjective Network Views

Subjective views of the network mean that the identifier a requester uses to refer to one physical entity could actually apply to a different physical entity when used in a different network context. Unless an authorized third party requester and LIS operate in the same network context, each could have a different subjective view of the meaning of the identifier.

Where subjective views differ, the third party receives information that is correct only within the network context of the LIS. The location information provided by the LIS is probably misleading: the requester believes that the information relates to a different entity than it was generated for.

Authorization policy can be affected by a subjective network view if it is applied based on an identifier, or its application depends on identifiers. The subjective view presented to the LIS and Rule Maker need to agree for the two entities to understand policy on the same terms. For instance, it is possible that the LIS could apply the incorrect authorization policy if it selects the policy using a subjective identifier. Alternatively, it may use the correct policy but apply it incorrectly if subjective identifiers are used.

> In IP networks, network address translation (NAT) and other forms of address modification create network contexts. Entities on either side of the point where modification occurs have a different view of the network. Private use addresses [RFC1918] are the most easily recognizable identifiers that have limited scope.

A LIS can be configured to recognize scenarios where the subjective view of a requester or Rule Maker might not coincide with the view of the LIS. The LIS can either provide location information that takes the view of the requester into account, or it can reject the request.

> For instance, a LIS might operate within a network that uses a private address space, with NAT between that network and other networks. A third party request that originates in an external network with an IP address from the private address space might not be valid - it could be identifying an entity within another address space. The LIS can be configured to reject such requests, unless it knows by other means that the request is valid.

> In the same example, the requester might include an address from the external space in an attempt to identify a host within the network. The LIS could use knowledge about how the external address is mapped to a private address, if that mapping is fixed,

to determine an appropriate response.

The residential gateway scenario in Section 3.1 of [RFC5687] is a particular example of where a subjective view is permitted. The LIS knowingly provides Devices on the remote side of the residential gateway with location information. The LIS provides location information with appropriate uncertainty to allow for the fact that the residential gateway serves a small geographical area.

2.1.2. Transient Identifiers

Some identifiers are temporary and can, over the course of time, be assigned to different physical entities. An identifier that is reassigned between the time that a request is formulated by a requester and when the request is received by the LIS causes the LIS to locate a different entity than the requester intended. The response from the LIS might be accurate, but the request incorrectly associates this information with the wrong subject.

A LIS should be configured with information about any potentially temporary identifiers. It can use this information to identify when changes have occurred. A LIS must not provide location information if the identifier it uses might refer to a different Device. If an identifier might have been reassigned recently, or it is likely to be reassigned, it is not suitable as an identifier.

It's possible that some degree of uncertainty could persist where identifiers are reassigned frequently; the extent to which errors arising from using transient identifiers are tolerated is a matter for local policy.

2.2. Identifier Format and Protocol Details

XML elements are used to express the Device identity. The "device" element is used as a general container for identity information. This document defines a basic set of identifiers. An example HELD request, shown in Figure 1, includes an IP version 4 address.

```
<locationRequest xmlns="urn:ietf:params:xml:ns:geopriv:held"
                 responseTime="8">
  <locationType exact="true">geodetic</locationType>
  <device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
    <ip v="4">192.0.2.5</ip>
  </device>
</locationRequest>
```

Figure 1

A LIS that supports this specification echoes the "device" element in a successful HELD response, including the identifiers that were used as the basis for location determination. Absence of this indication means that the location information was generated using the source IP address in the request.

A "badIdentifier" HELD error code indicates that the requester is not authorized to use that identifier or that the request contains an identifier that is badly formatted or not supported by the LIS. This code is registered in Section 7.3.

If the LIS requires an identifier that is not provided in the request, the desired identifiers MAY be identified in the HELD error response, using the "requiredIdentifiers" element. This element contains a list of XML qualified names [W3C.REC-xml-names11-20060816] that identify the identifier elements required by the LIS. Namespace prefix bindings for the qualified names are taken from document context. Figure 2 shows an example error indicating that the requester needs to include a MAC address (Section 3.2) and IP address (Section 3.1) if the request is to succeed.

```
<error xmlns="urn:ietf:params:xml:ns:geopriv:held"
       code="badIdentifier">
  <message xml:lang="en">MAC address required</message>
  <requiredIdentifiers
      xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
    mac ip
  </requiredIdentifiers>
</error>
```

Figure 2

3. Identifiers

A limited selection of identifiers are included in this document. The basic Device identity schema allows for the inclusion of elements from any namespace, therefore additional elements can be defined using different XML namespaces.

3.1. IP Address

The "ip" element can express a Device identity as an IP address. The "v" attribute identifies the IP version with a single hexadecimal digit. The element uses the textual format specific to the indicated IP version ([RFC0791] for IPv6, [RFC4291] for IPv6).

```
<device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
  <ip v="6">2001:db8::1:ea7:fee1:d1e</ip>
</device>
```

In situations where location configuration does not require additional identifiers, using IP address as an identifier enables authorized third party requests.

3.2. MAC Address

The media access control (MAC) address used by the IEEE 802 family of access technologies is an identifier that is assigned to a particular network Device. A MAC address is a unique sequence that is either assigned at the time of manufacture of a Device, or assigned by a local administrator. A MAC address rarely changes; therefore, a MAC address is an appropriate identifier for a Device.

A MAC address can be represented as MAC-48, EUI-48 or EUI-64 address

([IEEE802], or extended unique identifier [EUI64]) using the hexadecimal representation defined in [IEEE802].

```
<device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
  <mac>A0-12-34-56-78-90</mac>
</device>
```

3.3. TCP or UDP Port Number

On its own, a TCP or UDP port number is insufficient to uniquely identify a single host, but in combination with an IP address, it can be used in some environments to uniquely identify a Device.

Use of a particular port number can be transient; often significantly more than use of any given IP address. However, widespread use of network address translation (NAT) means that some Devices cannot be

uniquely identified by IP address alone. An individual Device might be identified by a flow of packets that it generates. Providing that a LIS has sufficient knowledge of the mappings used by the NAT, an individual target on the remote side of the NAT might be able to be identified uniquely.

```
<device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
  <ip v="4">192.0.2.75</ip>
  <udpport>51393</udpport>
</device>
```

Use of port numbers is especially reliant on the value remaining consistent over time.

3.4. Network Access Identifier

A Network Access Identifier (NAI) [RFC4282] is an identifier used in network authentication in a range of networks. The identifier establishes a user identity within a particular domain. Often, network services use an NAI in relation to location records, tying network access to user authentication and authorization.

```
<device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
  <nai>user@example.net</nai>
</device>
```

The formal grammar for NAI [RFC4282] permits sequences of octets that are not valid UTF-8 [RFC3629] sequences. These sequences cannot be expressed using XML. Therefore, this expression of NAI permits escaping. Sequences of octets that do not represent a valid UTF-8 encoding can be expressed using a backslash ('\') followed by two case-insensitive hexadecimal digits representing the value of a single octet.

The canonical representation of an NAI is the sequence of octets that is produced from the concatenation of UTF-8 encoded sequences of unescaped characters and octets derived from escaped components. The resulting sequence of octets MUST conform to the constraints in [RFC4282].

For example, the NAI "f<U+FC>\<0xFF>@bar.com" that includes the UTF-8 encoded u-umlaut character (U+FC) and an invalid UTF-8 octet (0xFF) might be represented as "f\c3\bc\5c\90@bar.com", though the u-umlaut character might be included directly.

3.4.1. Using NAI for Location Configuration

An NAI in WiMAX is uniquely attributable to a single Device at any one time. An NAI either identifies a Device or a service subscription, neither of which can have multiple active sessions.

In a WiMAX network, an IP address is not sufficient information for a LIS to locate a Device. The following procedure relies on an NAI to identify the Device. This procedure and the messages and parameters is relies upon are defined in [WiMAX-T33-110-R015v01-B].

Location requests in a WiMAX network always require the inclusion of an NAI. However, if a LIS receives a request that does not come from an authenticated and authorized third party requester, it can treat this request as a location configuration request.

After receiving a location request that includes an NAI, the LIS sends a "Location-Requestor-Authentication-Protocol" access request

message to the Authentication, Authorization and Accounting (AAA) server. This request includes an "MS-Identity-Assertion" parameter containing the NAI.

The AAA server consults network policy and if the request is permitted, the response includes the IP address that is currently assigned to the Device. If this IP address matches the source IP address of the HELD location request, the location request can be authorized under the LCP policy (see Section 4.1). Otherwise, the request must be treated as a third party request.

This relies on the same IP address spoofing protections that are required by [I-D.ietf-geopriv-http-location-delivery]. In addition, the request made of the AAA uses either Diameter [RFC3588] or RADIUS [RFC2865], and therefore relies on the protections provided by those protocols. In order to rely on the access request, the AAA server MUST be authenticated to be a trusted entity for the purpose of providing a link between the NAI and IP address. The AAA protocol MUST also provide protection from modification and replay attacks to ensure that data cannot be altered by an attacker.

3.5. URI

A Device can be identified by a URI [RFC3986]. Any URI can be used providing that the requester and LIS have a common understanding of the semantics implied by use of the URI.

```
<device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
  <uri>sip:user@example.net;gr=kjh29x97us97d</uri>
</device>
```


Particular care needs to be taken in ensuring that a particular URI only refers to a single Device. In many cases, a URI can resolve to multiple destinations. For example, a SIP address of record URI can correspond to a service subscription rather than a single Device.

A "tel:" URI [RFC3966] can be used identify a Device by telephone number:

```
<device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
  <uri>tel:800-555-1111;extension=1234;phone-context=+1</uri>
</device>
```

3.6. Fully Qualified Domain Name

A fully-qualified domain name can be used as the basis for identification using the "fqdn" element.

```
<device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
  <fqdn>host.example.net</fqdn>
</device>
```

This IDN-aware domain name slot [I-D.ietf-idnabis-defs] is formed from any sequence of valid U-labels or NR-LDH-labels.

A domain name does not always correspond to a single IP address or host. If this is the case, a domain name is not a suitable identifier.

3.7. Cellular Telephony Identifiers

A range of different forms of mobile station identifiers are used for different cellular telephony systems. Elements are defined for these identifiers. The following identifiers are defined:

msisdn: The Mobile Station International Subscriber Dial Number (MSISDN) is an E.164 number between 6 and 15 digits long.

imsi: The International Mobile Subscriber Identity (IMSI) an identifier associated with all GSM and UMTS mobile subscribers.

imei: The International Mobile Equipment Identifier (IMEI) is a unique device serial number up to 15 digits long.

min: The Mobile Identification Number (MIN) is a unique number assigned to CDMA handsets.

mdn: The Mobile Directory Number (MDN) is an E.164 number, with usage similar to MSISDN.

Each identifier contains a string of decimal digits with a length as

specified.

```
<device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
  <msisdn>11235550123</msisdn>
</device>
```

3.8. DHCP Unique Identifier

The Dynamic Host Configuration Protocol (DHCP) uses a binary identifier for its clients. The DHCP Unique Identifier (DUID) is expressed in Option 61 of DHCPv4 (see [RFC4361]) or Option 1 of DHCPv6 and follows the format defined in Section 9 of [RFC3315]. The "duid" element includes the binary value of the DUID expressed in hexadecimal.

```
<device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
  <duid>1234567890AaBbCcDdEeFf</duid>
</device>
```

4. Privacy Considerations

Location configuration protocols can make use of an authorization model known as "LCP policy", which permits only Targets to be the recipients of their own locations. In effect, an LCP server (that is, the LIS) follows a single rule policy that states that the Target is the only authorized Location Recipient.

The security and privacy considerations of the base HELD protocol [I-D.ietf-geopriv-http-location-delivery] are applicable. However, the considerations relating to return routability do not apply to third party requests. Return routability may also not apply to requests from Targets for their own location depending on the anti-spoofing mechanisms employed for the identifier.

4.1. Targets Requesting Their Own Location

When a Target uses identity extensions to obtain its own location, HELD can no longer be considered an LCP. The authorization policy that the LIS uses to respond to these requests must be provisioned by one or more Rule Makers.

In the case that the LIS exclusively provides Targets with their own locations, the LIS can still be said to be following the "LCP policy". The "LCP policy" concept and further security and privacy considerations can be found in [I-D.ietf-geopriv-arch].

The spoofing protections provided when using HELD with identity extensions to provide Targets with their own locations differ from the protections inherent in an LCP. For an LCP, return routability is considered sufficient protection against spoofing. For a similar policy to be used, specific measures MUST be defined to protect against spoofing of the alternative identifier. This document defines this for an NAI when used in WiMAX networks (see Section 3.4.1), but for no other identifier.

A Rule Maker might require an assurance that the identifier is owned by the requester. Any multi-stage verification process that includes a return routability test cannot provide any stronger assurance than return routability alone; therefore, policy might require the use of additional, independent methods of verification.

Care is required where a direct one-to-one relationship between requester and Device identity does not exist. If identifiers are not uniquely attributable to a single Device, the use of HELD identity extensions to provide Targets with their own locations could be exploited by an attacker.

It might be possible in some networks to establish multiple concurrent sessions using the same credentials. For instance, Devices with different MAC addresses might be granted concurrent access to a network using the same NAI. It is not appropriate to provide Targets with their own locations based on NAI in this case. Neither is it appropriate to authenticate a Device using NAI and allow that Device to provide an unauthenticated MAC address as a Device identifier, even if the MAC address is registered to the NAI. The MAC address potentially identifies a different Device to the one that is making the request. The correct way of gaining authorization is to establish a policy that permits this particular request as a third party request.

Section 3.4.1 discusses the implications of using an NAI as an identifier for location requests made of a LIS serving a WiMAX network. Additional security considerations are discussed in [WiMAX-T33-110-R015v01-B].

4.2. Third Party Requests

The "LCP policy" does not allow requests made by third parties. If a LIS permits requests from third parties using Device identity, it assumes the rule of a Location Server (LS). As a Location Server, the LIS MUST explicitly authorize requests according to the policies that are provided by Rule Makers, including the Target. The LIS MUST also authenticate requesters according to any agreed-upon authorization policy.

An organization that provides a LIS that allows third party requests must provide a means for a Rule Maker to specify authorization policies as part of the LIS implementation (e.g, in the form of access control lists). Authorization must be established before allowing third party requests for the location of any Target. Until an authorization policy is established, the LIS MUST reject requests by third parties (that is, the default policy is "deny all").

When the LIS is operated by an access network, the relationship between the Target and the LIS can be transient. As the Target is a potential Rule Maker, this presents a problem. However, the process of establishing network access usually results in a form of agreement

between the Target and the network provider. This process offers a natural vehicle for establishing location privacy policies. Establishing authorization policy might be a manual process, an explicit part of the terms of service for the network, or an automated system that accepts formal authorization policies (see [RFC4745], [RFC4825]). This document does not mandate any particular mechanism for establishing an authorization policy.

5. Security Considerations

The security considerations in [I-D.ietf-geopriv-http-location-delivery] describe the use of Transport Layer Security (TLS) [RFC5246] for server authentication, confidentiality and protection from modification. These protections apply to both Target requests for their own locations and requests made by third parties.

All HELD requests containing identity MUST be authenticated by the LIS. How authentication is accomplished and what assurances are desired is a matter for policy.

The base HELD protocol uses return reachability of an IP address implied by the requester being able to successfully complete a TCP handshake. It is RECOMMENDED that any means of authentication provide at least this degree of assurance. For requests that include Device identity, the LIS MUST support HTTP digest authentication [RFC2617]. Unauthenticated location requests containing Device identity can be challenged with an HTTP 401 (Unauthorized) response or rejected with an HTTP 403 (Forbidden) response.

5.1. Identifier Suitability

Transient and ambiguous identifiers can be exploited by malicious requests and are not suitable as a basis for identifying a Device. Section 2.1 provides further discussion on this subject.

Identifier transience can lead to incorrect location information being provided. An attacker could exploit the use of transient identifiers. In this attack, the attacker either knows of a re-allocation of that identifier or is able to force the identifier to be re-allocated during the processing of the request.

An attacker could use this to acquire location information for another Device or to coerce the LIS to lie on its behalf if this re-allocation occurs between the time where authorization is granted and location information is granted.

Ambiguous identifiers present a similar problem. An attacker could legitimately gain authorization to use a particular identifier. Since an ambiguous identifier potentially refers to multiple Devices, if authorization is granted for one of those Devices, an attacker potentially gains access to location information for all of those Devices.

5.2. Targets Requesting Their Own Location

Requests made by a Device for its own location are covered by the same set of protections offered by HELD. These requests might be authorized under a policy similar to the "LCP policy" that permits a Target access to location information about itself.

Identity information provided by the Device is private data that might be sensitive. The Device provides this information in the expectation that it assists the LIS in providing the Device a service. The LIS MUST NOT use identity information for any other purpose other than serving the request that includes that information.

5.3. Third Party Requests

Requests from third parties have the same requirements for server authentication, confidentiality and protection from modification as Target requests for their own locations. However, because the third party needs to be authorized, the requester MUST be authenticated by the LIS. In addition, third party requests MUST be explicitly authorized by a policy that is established by a Rule Maker.

More detail on the privacy implications of third party requests are covered in Section 4.

6. XML Schema

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

  <xs:annotation>
    <xs:appinfo
        source="urn:ietf:params:xml:schema:geopriv:held:id">
      HELD Device Identity
    </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 Device identity elements for HELD.
    </xs:documentation>
  </xs:annotation>
```

```
<xs:element name="device" type="id:deviceIdentity"/>
<xs:complexType name="deviceIdentity">
  <xs:sequence>
    <xs:any namespace="##any" processContents="lax"
            minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:element name="requiredIdentifiers" type="id:qnameList"/>
<xs:simpleType name="qnameList">
  <xs:list itemType="xs:QName"/>
</xs:simpleType>

<xs:element name="ip" type="id:ipAddress"/>
<xs:complexType name="ipAddress">
  <xs:simpleContent>
    <xs:extension base="xs:token">
      <xs:attribute name="v" use="required">
        <xs:simpleType>
          <xs:restriction base="xs:token">
            <xs:pattern value="[\da-fA-F]"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
```



```
<xs:element name="mac" type="id:macAddress"/>
<xs:simpleType name="macAddress">
  <xs:restriction base="xs:token">
    <xs:pattern
value="[\da-fA-F]{2}(-[\da-fA-F]{2}){5}((-[\da-fA-F]{2}){2})?"/>
  </xs:restriction>
</xs:simpleType>

<xs:element name="udpport" type="id:portNumber"/>
<xs:element name="tcpport" type="id:portNumber"/>
<xs:simpleType name="portNumber">
  <xs:restriction base="xs:nonNegativeInteger">
```

```
        <xs:maxInclusive value="65535"/>
      </xs:restriction>
    </xs:simpleType>

    <xs:element name="nai" type="id:naiType"/>
    <xs:simpleType name="naiType">
      <xs:restriction base="xs:token">
        <xs:pattern
            value="([^\\]|\\[\dA-Fa-f]{2})*
                   (@([A-Za-z\d]([A-Za-z\d\-]*[A-Za-z\d])*\.)+
                    [A-Za-z\d]([A-Za-z\d\-]*[A-Za-z\d])*)?"/>
      </xs:restriction>
    </xs:simpleType>

    <xs:element name="uri" type="xs:anyURI"/>
    <xs:element name="fqdn" type="xs:token"/>

    <xs:element name="duid" type="xs:hexBinary"/>

    <xs:element name="msisdn" type="id:e164"/>
    <xs:element name="imsi" type="id:e164"/>
    <xs:element name="imei" type="id:digit15"/>
    <xs:element name="min" type="id:digit10"/>
    <xs:element name="mdn" type="id:e164"/>
    <xs:simpleType name="digits">
      <xs:restriction base="xs:token">
        <xs:pattern value="[\d]+"/>
      </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="e164">
      <xs:restriction base="id:digit15">
        <xs:minLength value="6"/>
      </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="digit15">
      <xs:restriction base="id:digits">
```



```
        <xs:maxLength value="15"/>
      </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="digit10">
      <xs:restriction base="id:digits">
```

```
        <xs:length value="10"/>
      </xs:restriction>
    </xs:simpleType>

  </xs:schema>
```

7. IANA Considerations

This document registers an XML namespace and schema with IANA in accordance with guidelines in [RFC3688].

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

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

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

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 Device Identity Parameters</title>
     </head>
     <body>
       <h1>Namespace for HELD Device Identity Parameters</h1>
       <h2>urn:ietf:params:xml:ns:geopriv:held:id</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:id

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 6 of this document. [IANA Note: The pattern attribute for naiType does not contain whitespace.]

7.3. Registration of HELD 'badIdentifier' Error Code

This section registers the "badIdentifier" error code in the "Geopriv HELD Registries, Error codes for HELD" IANA registry.

badIdentifier This error code indicates that a Device identifier used in the HELD request was either: not supported by the LIS, badly formatted, or not one for which the requester was authorized to make a request.

8. Acknowledgements

The the NENA VoIP location working group provided assistance in the definition of the schema used in this document. Special thanks go to Barbara Stark, Guy Caron, Nadine Abbott, Jerome Grenier and Martin Dawson. Bob Sherry provided input on use of URIs. Thanks to Adam Muhlbauer and Eddy Corbett for providing further corrections. Bernard Aboba provided excellent feedback on use cases and the security model; Bernard, along with Alan DeKok, also helped resolve an issue with NAIs. Ray Bellis provided motivation for the protocol port parameters. Marc Linsner and Alissa Cooper provided guidance and text (respectively) that greatly clarified the discussion relating to LCPs. Thanks to Jon Peterson and Cullen Jennings for forcing this to be practical.

9. References

9.1. Normative references

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

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

[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.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

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

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

[RFC4282] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4361] Lemon, T. and B. Sommerfeld, "Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)", RFC 4361, February 2006.

[I-D.ietf-idnabis-defs]
Klensin, J., "Internationalized Domain Names for

Applications (IDNA): Definitions and Document Framework", draft-ietf-idnabis-defs-13 (work in progress), January 2010.

[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.

[W3C.REC-xml-names11-20060816]
Hollander, D., Layman, A., Tobin, R., and T. Bray, "Namespaces in XML 1.1 (Second Edition)", World Wide Web Consortium Recommendation REC-xml-names11-20060816, August 2006, <http://www.w3.org/TR/2006/REC-xml-names11-20060816>.

[IEEE802] IEEE, "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture", 802, February 2002.

[EUI64] IEEE, "Guidelines for 64-bit Global Identifier (EUI-64)

Registration Authority", March 1997, <http://standards.ieee.org/regauth/oui/tutorials/EUI64.html>.

[WiMAX-T33-110-R015v01-B] WiMAX Forum, "Protocols and Procedures for Location Based Services", WiMAX Forum Network Architecture T33-110-R015v01-B, May 2009.

9.2. Informative references

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC2101] Carpenter, B., Crowcroft, J., and Y. Rekhter, "IPv4 Address Behaviour Today", RFC 2101, February 1997.

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

[RFC3966] Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966, December 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.

[RFC4776] Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", RFC 4776, November 2006.

[RFC4825] Rosenberg, J., "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)", RFC 4825, May 2007.

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

[RFC5687] Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol: Problem Statement and

Requirements", RFC 5687, March 2010.

[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-03 (work in progress), October 2010.

[I-D.ietf-ecrit-phonebcp]
Rosen, B. and J. Polk, "Best Current Practice for Communications Services in support of Emergency Calling", draft-ietf-ecrit-phonebcp-15 (work in progress), July 2010.

[I-D.thomson-geopriv-held-measurements]
Thomson, M. and J. Winterbottom, "Using Device-provided Location-Related Measurements in Location Configuration Protocols", draft-thomson-geopriv-held-measurements-06 (work in progress), May 2010.

[TS.3GPP.23.271]
3GPP, "Functional stage 2 description of Location Services (LCS)", 3GPP TS 23.271 8.0.0, December 2008.

Authors' Addresses

James Winterbottom
Andrew Corporation
Andrew Building (39)
Wollongong University Campus
Northfields Avenue

Wollongong, NSW 2522
AU

Phone: +61 2 4221 2938
Email: james.winterbottom@andrew.com

Martin Thomson
Andrew Corporation
Andrew Building (39)
Wollongong University Campus
Northfields Avenue
Wollongong, NSW 2522
AU

Phone: +61 2 4221 2915
Email: martin.thomson@andrew.com

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

Richard Barnes
BBN Technologies
9861 Broken Land Pkwy, Suite 400
Columbia, MD 21046
USA

Phone: +1 410 290 6169
Email: rbarnes@bbn.com