GEOPRIV WG
Internet-Draft
Intended status: Standards Track
Expires: April 26, 2007

J. Winterbottom
M. Thomson
Andrew
B. Stark
BellSouth

October 23, 2006

HTTP Enabled Location Delivery (HELD)
draft-winterbottom-http-location-delivery-04.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of 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/1id-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 April 26, 2007.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

A Geopriv using protocol is described that is used for retrieving location information from a server within an access network. The protocol includes options for retrieving location information either by-value or by-reference. The protocol supports mobile and nomadic devices through Location URIs. The protocol is an application-layer protocol that is independent of session-layer; an HTTP, web services binding is specified.

Table of Contents

1. Introduction

The location of a Device is information that is useful for a number of applications. A Device might be able to determine this information using its own resources, but more often than not, the Device must rely on its access network to provide this information. This document describes a protocol that can be used to acquire Location Information (LI) from a service within an access network.

This specification identifies two methods for acquiring LI. Location may be retrieved from a Location Generator (LG) by-value, that is, the Device may acquire LI directly. Alternatively, the Device may request that the LG provide a location URI so that LI can be distributed by-reference. Both of these methods are compatible, and both can be provided concurrently from the same LG so that application needs can be addressed individually.

This specification defines an XML-based protocol that enables the retrieval of LI from a LG. This protocol can be bound to any session-layer protocol, particularly those capable of MIME transport; an HTTP binding is included as a minimum requirement.

1.1. Exclusions

This document defines a protocol for configuration purposes; that is, a protocol for requesting (and receiving) the information necessary to use LI. This document does not define a Geopriv Using Protocol. The LG is assumed to be present within the same administrative domain as the Device (the access network), which limits the security threats that this protocol is exposed to.

This document does not specify how LI is derived. Determination of the physical location of a network termination point is dependent on the type of access network and the capabilities of networking equipment. The specific methods that could be used are innumerable, therefore this is left to individual network and equipment implementations.

Providing LI by-reference implies that a server is able to provide the Device with a public, globally-routable URI. How this URI is provided is not covered by this specification. This includes any interactions between the LG and LS necessary to facilitate the provision of a Location URI.

This document does not define how an LG is discovered or configured. Service discovery techniques are described in two separate documents, [I-D.winterbottom-geopriv-held-dhcp-discovery] describing a DHCP discovery mechansim, and [I-D.thomson-geopriv-held-unaptr] describing

a DNS lookup mechanism.

1.2. Device or Target

LI provided for the Device is often represented as the location of a user. However, in this document LI is attributed to a Device and not a person. Primarily, this is because location determination technologies are generally designed to locate a Device and not a person. In addition to this, unless the Device requires active user authentication, there is no guarantee that any particular individual is using the Device at that instant. Thus, if any claim of veracity is to be made for LI, the distinction between Target and Device must be made explicit.

This distinction should not lead to the impression that the location of the Device does not impact the privacy constraints required by this protocol. Revealing the location of the Device almost invariably reveals some information about the location of the user of the Device, therefore the same level of privacy protection demanded by a user is required for the Device.

It is expected that, for most applications, this distinction will be unnecessary: LI for the Device will be used as an adequate substitute for the user's LI. This requires either some additional assurances about the link between Device and Target, or an acceptance of the aforementioned limitations.

This document assumes that the Device is responsible for the protocol interactions described and that it does so with the authority of the Target and Rule Maker (RM).

1.3. The Bigger Picture

This document describes an interface between a Device and a Location Generator (LG). Detailing the interactions between these two entities requires a wider understanding of other interested parties.

For the Device, the most important consideration is the Target. In some cases, this is the same as the Device, but it is more likely to be a human user. The foundation of this protocol is that the Target is able to direct the dissemination of LI, that is, the Target provides authorization policies and otherwise controls how LI is granted to Location Recipients (LRs). This extends to when a Location Server (LS) is employed to provide a Location URI; the LS cannot provide LI to an LR without express permission from the Target.

The LG exists as an access network service. An Access Provider (AP)

operates this service so that Devices (and Targets) can retrieve LI. The LG exists because not all Devices are capable of determining LI, and because, even if a Device is able to determine its own LI, it may be more efficient with assistance.

The following diagram shows one possible configuration of the roles identified in [RFC3693] and where this protocol applies.

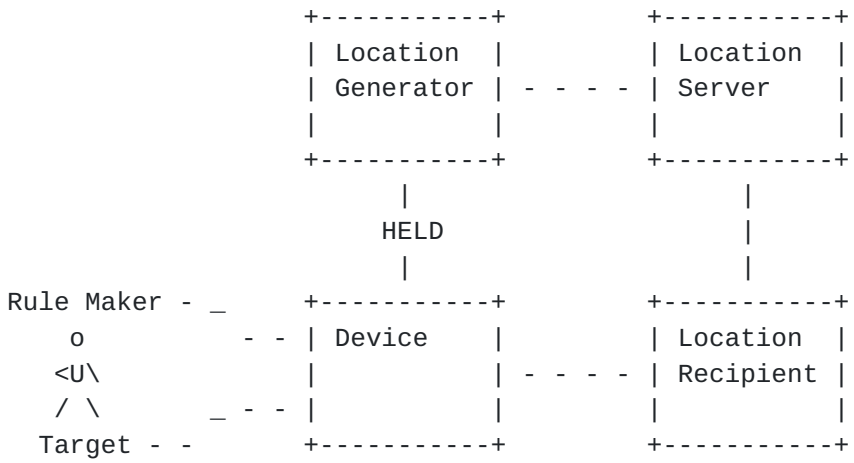

Figure 1: Significant Roles

2. Conventions used in this document

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 specification provides an XML Schema [W3C.REC-xmlschema-1-20041028]. The schema definition is normative.

2.1. GEOPRIV Terminology

This document uses the terms (and their acronym forms) Location Information (LI), Location Object (LO), Device, Target, Access Provider (AP), Location Server (LS), Location Generator (LG), Location Recipient (LR), Rule Maker (RM), Rule Holder (RH) and Using Protocol as defined in [RFC3693].

For convenience, abbreviated versions of RFC 3693 [RFC3693] definitions are included:

Access Provider (AP): An organization that provides physical network connectivity to its customers or users, e.g., through digital subscriber lines, cable TV plants, Ethernet, leased lines or radio frequencies. Examples of such organizations include telecommunication carriers, municipal utilities, larger enterprises with their own network infrastructure, and government organizations such as the military.

Civic Location/Address: A location expressed in a form that is defined by civic demarcations. Civic addresses can be specialized for jurisdictional (general use) or postal (message delivery) purposes, or they can apply to either.

Device: The technical device whereby the location is tracked as a proxy for the location of a Target.

Geodetic Location: A location expressed in coordinate form.

Location Generator (LG): The entity that initially determines or gathers the location of the Target.

Location Information (LI): The data that describes the location of a Device. Note that the term LI does not include the representation of this data.

Location Object (LO): An object conveying Location Information (and possibly privacy rules) to which Geopriv security mechanisms and privacy rules are to be applied [from 3693]; this is a specific by-value representation of Location Information (LI). In this document, LO refers to PIDF-LO [RFC4119].

Location Server (LS): The LS is an element that receives publications of Location Objects from Location Generators and may receive subscriptions from Location Recipients. The LS applies the rules (which it learns from the Rule Holder) to LOs it receives from LGs, and then notifies LRs of resulting LOs as necessary.

In some specifications the Location Server is referred to as a Location Information Server or LIS. Note that in this context, the Location Server is distinct from what is alternatively referred to as a Registrar in other contexts.

Location Recipient (LR): The entity that receives Location Information (LI).

Rule Holder (RH): The entity that provides the rules associated with a particular target for the distribution of Location Information (LI).

Rule Maker (RM): The authority that creates rules governing access to location information for a target (typically, this it the Target themselves).

Target: A person or other entity whose location is communicated by a Location Object (LO).

Using Protocol: A protocol that carries a Location Object.

3. HELD Overview

The HELD protocol facilitates retrieval of LI either by-value, as a PIDF-LO document, or by-reference, as a Location URI.

This section describes how HELD can be used within a larger framework that moves LI from a source (the LG) to a destination (the LR).

3.1. Requesting Location Information Directly

Where a Device requires LI directly, it can request that the LG create a PIDF-LO document. The Device is then able to use the provided PIDF-LO document as it is required, using the appropriate application protocol. Figure 2 illustrates how this usage of HELD fits within the model presented in [RFC3693].

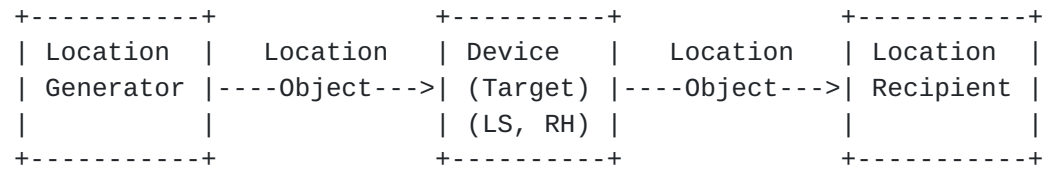

Figure 2: Simple Location Request Model

In this model, the Device in this scenario acts as a Location Server (LS) and Rule Holder (RH); it is responsible for making authorization decisions about which Location Recipients are given LOs.

The LG needs to uniquely identify the Device within the access network. The source address of the request message is sufficient in most cases. Once the Device is identified, the LG uses network domain-specific information to determine the location of the Device.

An LI request does not need to include any identification information other than return addressing. In fact, the HTTP binding (Section 7) includes the option for a GET request. Return routability also addresses a number of security concerns, see Section 8.

The response from the LG is a PIDF-LO document [RFC4119], unless there were errors in processing the request.

The interface between Device (acting as LS) and Location Recipient (LR) is application-specific and outside the scope of this specification.

3.1.1. Shaping the PIDF-LO

A Device can include additional information in an LI request that controls how the LG populates the fields in a PIDF-LO document. Related to privacy, a presentity URI and usage rules can be specified. The Device can also include a location estimate, or request a specific type of location information, including a request for a signed PIDF-LO.

When requesting LI, the Device can include a presentity URI for the Target and a ruleset reference. The LG incorporates this information in the PIDF-LO document, or modifies the document accordingly.

LI contained within a PIDF-LO document can be either geodetic (coordinates using latitude and longitude or some other coordinate system) or civic (street or postal addresses). The Device can request that the LG provide a specific type of LI, including whether a jurisdictional or postal civic address is required.

If a Device is capable of providing its own location it can include this in a request. The LG is then able to include this LI in the returned PIDF-LO. The type of LI is inferred from the request when LI is provided.

The PIDF-LO document generated by an LG MUST follow the rules in [I-D.ietf-geopriv-pdif-lo-profile]. The LI sent in a request MUST follow the subset of those rules relating to the construction of the "location-info" element.

3.2. Requesting a Location URI

Requesting LI directly does not always address the requirements of an application. A Location URI is a URI [RFC3986] of any scheme, which a Location Recipient (LR) can use to retrieve LI. A Device can request a Location URI instead of LI.

Figure 3 illustrates how this usage of HELD fits within the model presented in [RFC3693]. The first aspect of the diagram shows how the Device acts as an agent for the Target and retrieves a Location URI, which it then provides to the Location Recipient. The second aspect has the Device acting as an agent for the Rule Maker; the Device forwards rules to the LG, which forwards them to the LS.

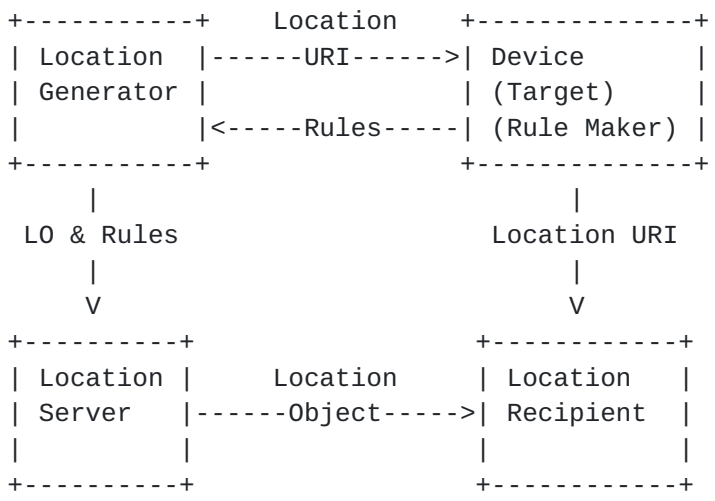

Figure 3: Location URI Usage Model

Note that the Location Server takes the role of a (Private) Rule Holder when the rules are provided by-value. The rules may also be provided to the LG and LS by-reference, in which case, a Public Rule Holder is required; the Public Rule Holder is not shown in this diagram.

The interface between Device (acting as LS) and Location Recipient (LR) is application-specific and outside the scope of this specification. Also, any interface between Device (acting as RM) and a Public Rule Holder is not relevant to this specification.

The merits and drawbacks of using a Location URI approach are discussed in [I-D.winterbottom-location-uri].

3.2.1. Establishing a Location Server Context

A Location URI is allocated for a Device by the LS. If the LS is to be able to service queries for location directed at the Location URI, it must maintain certain information. When the LG receives a request for a Location URI, it requests that the LS allocate a URI for a particular Device. As a part of providing a Location URI, the LS also creates a _context_, which contains the information that it requires to properly service requests to the URI.

This document does not make any normative statements about the interface between the LG and LS. Any assumptions that are made about the nature of this interface are stated where necessary.

A context contains sufficient information for the LS to identify the Device to the LG, so that LI can be generated as required, which could be on a per-request basis. The context also includes

instructions from the Device on how the PIDF-LO is to be generated, as described in Section 3.1.1.

The context contains an authorization policy that describes to whom, and how, LI is granted. This is a common-policy document [I-D.ietf-geopriv-common-policy] that is provided by the Device in the context creation request, either directly, or by reference.

4. Protocol Description

As discussed in Section 3, this protocol provides two basic functions: LI request and Location URI request. Messages are defined as XML documents.

The Location Request message is described in Section 4.2. A Location Request from a Device results in a PIDF-LO document in case of success, or an error message.

In requesting a Location URI, the Device requests that a context be created on the LS. The parameters for the create context request are described in Section 4.3.1. The response to a context creation request includes Location URIs and a password that can be used to update the information contained in the context. The details stored by the LS can be updated at any time after creation using the update context request, described in Section 4.3.2.

Table 1 shows the basic set of messages supported by this protocol and their respective responses, successful or otherwise.

Operation	Request Message	Successful Response	Error Response
Request Location	locationRequest (Section 4.2)	PIDF-LO document [RFC4119]	error (Section 4.5)
Create Context	createContext (Section 4.3.1)	contextResponse	error (Section 4.5)
Update Context	updateContext (Section 4.3.2)	contextResponse	error (Section 4.5)

Table 1: HELD Operations

A MIME type "application/held+xml" is registered in Section 10.5 to distinguish HELD messages from other XML document bodies. This specification follows the recommendations and conventions described in [RFC3023], including the naming convention of the type ('+xml' suffix) and the usage of the 'charset' parameter.

Section 5 contains a more thorough description of the protocol parameters, valid values, and how each should be handled. Section 6 contains a more specific definition of the structure of these messages in the form of an XML Schema [W3C.REC-xmlschema-1-20041028].

4.1. Protocol Binding

The HELD protocol is an application-layer protocol that is defined independently of any lower layers. This means that any protocol can be used to transport this protocol providing that it can provide a few basic features:

- The protocol must have acknowledged delivery.
- The protocol must be able to correlate a response with a request.
- The protocol must provide authentication, privacy and protection against modification.

Candidate protocols that could be used to address these purposes include: TCP [RFC0793], TLS [RFC2246], SASL [RFC2222], HTTP [RFC2616], SIP [RFC3261], BEEP [RFC3080] and SOAP [W3C.REC-soap12-part1-20030624] [W3C.REC-soap12-part2-20030624]. This document includes a binding that uses a combination of HTTP, TLS and TCP in Section 7.

4.2. Location Request

A location request is sent from the Device to the LG when it requires LI. This request can be very simple, including no parameters; in fact, the HTTP binding includes a GET request that does not include a message body.

A Device MAY make an assertion about its own location as part of a location request. Devices that have some means of acquiring LI, either from embedded technology like Global Positioning System (GPS) receivers or from user input, can use this to convey that information to the LG. The "assert" element can be used to convey this information.

The type of LI that a Device requests is determined by the type of LI that is included in the "assert" element. When asserted LI is not provided, the Device MAY specify the type of location requested using the "locationType" element.

LI provided by the Device is potentially more precise than that provided by the LG, therefore the LG MAY use this information to create a response. The LG SHOULD validate the LI provided for accuracy and precision before using this information.

The Device MAY specify a "profile" element that instructs the LG on how to construct the LO. Alternatively, if the Device has created a profile in an LS context, the Device can provide a "context" element

so that the LG can retrieve the profile from the LS.

The location request is made by sending a document formed of a "locationRequest" element. The successful response to a location request is a PIDF-LO document, unless the request fails, in which case the LG SHOULD provide an error indication document.

4.3. Contexts

A context is established by the LS in order to provide a Location URI. The context includes information necessary to identify the Device and determine its location when an LR requests an LO using the Location URI.

4.3.1. Creating Contexts

The Device uses the "createContext" message to request that the LG, and the LS, assign a Location URI. This establishes a context at the LS.

The LS MUST maintain the information provided in the create context request. The create context request includes a time limit, which sets the maximum time that this context can be maintained.

The response to a create context request contains information that the Device can use to identify a context. A set of Location URIs are included, each one MUST uniquely identify the context; that is, the LS MUST be able to identify a context based on a single Location URI. A Device can distribute a Location URI to an LR to allow it retrieve LI from the LS.

A Location URI MUST NOT contain any information that could be used to identify the Device or Target. It is RECOMMENDED that a Location URI contain a public address for the LS and a random sequence of characters that the LS can use to identify a particular context. The presentity identifier included in a PIDF-LO document SHOULD NOT be used for either part or the entirety of a Location URI.

The response to a create context request MUST include the time when the LS will terminate the context. The LS MUST NOT respond to any queries to the context beyond this time. A response to a context creation also includes a password that the Device uses to identify itself when updating the context at any time before the context expiry time.

4.3.2. Updating Contexts

A Device can update any of the information it has provided for a context at any time. The update context request includes the same information as the create context request with the addition of information that identifies an existing context.

A Device uses any one of the Location URIs provided to uniquely identify a context when updating context information. The context password MUST be provided when updating context information.

If a Device includes an authorization policy (or ruleset) in an update context request, the LS MUST refresh any stored copy of the authorization policy. This is especially important for authorization policies that are provided by-reference; the LS MUST update the authorization policy, even if the URI has not changed. Updated authorization policies MUST be processed by the LG and LS before any subsequent requests from LRs are accepted; the LG and LS MAY defer processing of the authorization policy until after a response is sent to the Device.

The update context request is constructed using the "updateContext" element. A successful response is the "contextResponse" element, which is the same as the response to a create context response.

The update context request can also indicate that data can be removed by the context by specifying a _nil_ value for any of the parameters, using the "xsi:nil" attribute. This applies to the profile (Section 5.4) element.

The response to an update context request is identical in form to the create context response, with updated information about the context. The Location URIs MUST be the same as those in the response to the initial create context request, but the password and expiry time MAY be changed.

4.3.3. Terminating Contexts

The update context request can be used to instruct the LS to terminate a context. The "lifetime" element in the request is set to a zero duration. Once the context has been terminated, or it has expired, Location URIs that reference that context can no longer be used and the Device MUST NOT use the Location URIs or password relating to that context.

The LS MAY terminate a context without notifying the Device. The LS SHOULD terminate contexts if it, or the LG, detect that any information relating to the Device changes in a way that invalidates

the context.

When the Device requests that a context be terminated, the LG responds with a "contextResponse" message that does not include any context information; this message MUST include the HELD "201" response code.

4.4. Combined Context and Location Requests

HELD supports an optimization that allows for the creation or update of a context while simultaneously requesting location information. The optional "location" attribute on the "createContext" or "updateContext" request can be used to request that the LG include a PIDF-LO in the "contextResponse". This PIDF-LO is formed according to the profile details associated with the context.

4.5. Indicating Errors

In the event of an error, the LG SHOULD respond to the Device with an error document. The error response applies to all request types and SHOULD also be sent in response to any unrecognized request.

An error indication document consists of an "error" element. The "error" element MUST include a "code" attribute that indicates the type of error. A set of predefined error codes are included in Section 5.8.

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

5. Protocol Parameters

This section describes, in detail the parameters that are used for this protocol. Table 2 lists the top-level components used within the protocol and where they are used.

Parameter	Location Request	Create Context	Update Context
responseTime (Section 5.1)	Request	Request	Request
assert (Section 5.2)	Request		
exact (assert) (Section 5.2.4)	Request		
locationType (Section 5.3)	Request		
exact (locationType) (Section 5.3.1)	Request		
profile (Section 5.4)	Request	Request	Request
signed (Section 5.5)	Request		
lifetime (Section 5.6)		Request	Request
rules (Section 5.7)		Request	Request
code (Section 5.8)	Error	Error & Response	Error & Response
message (Section 5.9)	Error	Error & Response	Error & Response
context (Section 5.10)	Request	Response	Request & Response
location (Section 5.11)		Request	Request

Table 2: Message Parameter Usage

5.1. "responseTime" Parameter

The "responseTime" attribute indicates to the LG how long the Device is prepared to wait for a response. This attribute MAY be added to any request message, although it is primarily used with the location request. The value of this attribute is indicative only, the LG is under no obligation to strictly adhere to the time limit implied; any enforcement of the time limit is left to the Device.

This attribute MAY be either a duration value as defined in XML Schema [W3C.REC-xmlschema-2-20041028], or a decimal seconds value, which may include a decimal point. It is RECOMMENDED that systems support millisecond precision for this parameter.

The LG SHOULD provide the most accurate LI that can be determined within the specified interval. This parameter could be used as input when selecting the method of location determination, where multiple such methods exist. If this parameter is absent, then the LG SHOULD return the most precise LI it is capable of determining.

5.2. "assert" Parameter

The "assert" element allows a Device to provide LI to the LG as part of a location request. Two types of content are allowed: a geodetic structure made up of a Geography Markup Language (GML) geometry object, "_Geometry" as defined by [OGC.GML-3.1.1]; and a civic address structure, "civicAddress" as defined by [I-D.ietf-geopriv-revised-civic-lo]. The contents of this element SHOULD follow the rules in [I-D.ietf-geopriv-pdif-lo-profile].

When used in combination with the "context" element, this LI MAY be used by the LS for requests to Location URIs for that context.

This element is mutually exclusive with the "locationType" parameter, defined in Section 5.3. The type of LI requested is implied by the types included in the assertion.

5.2.1. "method" Parameter

The "method" attribute SHOULD be attached to the "assert" element to indicate the means by which the LI was derived. This attribute follows the rules of the similarly named method element of the PIDF-LO.

5.2.2. "timestamp" Parameter

The "timestamp" attribute SHOULD be attached to the "assert" element to indicate when the LI was generated.

5.2.3. "expires" Parameter

The "expires" attribute MAY be attached to the "assert" element to indicate when the included LI is no longer valid. The LG SHOULD set the "retention-expires" element in the returned PIDF-LO to no later than this time if it uses the LI. This attribute SHOULD NOT be included unless this time is definite.

5.2.4. "exact" Parameter

When the "exact" attribute is set to "true", it indicates to the LG that the contents of the "assert" parameter MUST be strictly followed. The default value of "false" allows the LG the option of ignoring these values.

This attribute indicates that the asserted LI MUST be included in the PIDF-LO response. If the LG cannot do this for any reason, which is usually because it determines that the LI was inaccurate or insufficiently precise, the LG MUST indicate an error.

5.3. "locationType" Parameter

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

any: The LG SHOULD attempt to provide LI in all forms available to it. This value MUST be assumed as the default if no "locationType" is specified. The LG SHOULD return location information in a form that is suited for routing and responding to an emergency call in its jurisdiction.

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

civic: The LG SHOULD return a civic address for the Target. Any type of civic address may be returned. The LG SHOULD ignore this value if a request for jurisdictional or postal civic address has been made and can be satisfied.

jurisdictionalCivic: The LG SHOULD return a jurisdictional civic address for the Target.

postalCivic: The LG SHOULD return a postal civic address for the Target.

The "locationType" element is mutually exclusive with the "assert" element, defined in Section 5.2.

The LG SHOULD return the requested location type or types. The LG MAY provide additional location types, or it MAY provide alternative types if the request cannot be satisfied for a requested location type. If the "exact" attribute is present and set to "true" in a location request, then a successful LG response MUST provide the requested location type only, with no additional location information. The "exact" attribute has no effect when this element is set to "any".

The "SHOULD"-strength requirement on this parameter is included to allow for soft-failover. This enables a fixed client configuration that prefers a specific location type without causing location requests to fail when that location type is unavailable. Unless the "exact" attribute is set, the LG MUST provide LI in any available form if it is unable to comply with the request.

For example, a notebook computer could be configured to retrieve civic addresses, which is usually available from typical home or work situations. However, when using a wireless modem, the LG might be unable to provide a civic address.

5.3.1. "exact" Parameter

When the "exact" attribute is set to "true", it indicates to the LG that the contents of the "locationType" parameter MUST be strictly followed. The default value of "false" allows the LG the option of ignoring these values.

A value of "true" indicates that the LG MUST provide a PIDF-LO that includes LI of the requested type or types. The LG MUST provide the requested types only and these types SHOULD be specified in the same order as they were requested. The LG SHOULD handle an exact request that includes a "locationType" element set to "any" as if the "exact" attribute were set to "false".

5.4. "profile" Parameter

The "profile" element contains a presentity identifier [RFC2778] and GEOPRIV usage rules [RFC4119] information. All fields are optional within this element, but when these fields are included, the LG MUST use these parameters when constructing the PIDF-LO document.

This element MAY be included in location requests, create context requests and update context requests. When included in a location request, the profile is used immediately; when used in create context or update context requests, the profile is stored on the LS and is provided to the LG when the LS responds to requests from LRs.

5.4.1. "presentity" Parameter

The "presentity" element contains a presentity identifier that the LG SHOULD include in the "pres" attribute of the PIDF-LO document.

The LG MAY require authentication of the presentity through any means; the LG SHOULD ignore this parameter if authentication information is not present or authentication information cannot be verified.

5.4.2. "retentionExpiry" Parameter

The "retentionExpiry" element contains an absolute "dateTime" [W3C.REC-xmlschema-2-20041028] value for the "retention-expires" element of the PIDF-LO usage rules. This element is mutually exclusive with the "retentionInterval" element.

The LG MAY use a different value than that specified (or the suggested default) as circumstances dictate, but MUST NOT use a value later than specified. If this value indicates a time that has already passed, the request MUST be rejected with an error. See retentionInterval (Section 5.4.3) for more details.

5.4.3. "retentionInterval" Parameter

The "retentionInterval" element contains a time duration value that is specified in the same fashion as the responseTime attribute (Section 5.1).

This value MUST be added to the time at which the PIDF-LO document is created to set the value of the "retention-expires" element. This element enables the Target to set an interval over which a LR can retain a LO, rather than an absolute time. This element is mutually exclusive with the "retentionExpires" element.

If neither "retentionExpiry" nor "retentionInterval" are specified, the LG SHOULD provide a default value for the "retention-expires" element of the generated PIDF-LO document. The default for this value SHOULD be 24 hours from the receipt of the location request as defined in [RFC4119].

The LG MAY use a different value than that specified (or the suggested default) as circumstances dictate, but MUST NOT use a value larger than specified.

5.4.4. "retransmission" Parameter

The "retransmission" element contains a boolean value that MUST be included in the "retransmission-allowed" element of the generated PIDF-LO usage rules. When this element is not provided, the LG MUST set the "retransmission-allowed" element to "false".

5.4.5. "rulesetURI" Parameter

The "rulesetURI" element contains a URI value that MUST be included in the "ruleset-reference" element of the generated PIDF-LO usage rules.

This datum is only used to construct the usage rules in the PIDF-LO document. Within the context of a profile, this ruleset is not applied by either LG or LS, and the LS does not apply the rules found at the URI.

5.5. "signed" Parameter

The "signed" attribute indicates whether the Device requires a digitally signed PIDF-LO. When present and set to "true", the LG MUST provide a PIDF-LO document that is signed according to XML-Signature [RFC3275].

5.6. "lifetime" Parameter

The "lifetime" element specifies the maximum time that a context should be maintained by the LS. This parameter MUST be included in the context creation request to indicate to the LS the latest time that the context is allowed to be retained. The parameter MAY be included in context update requests to modify this time; when included in an update request with a zero value, it indicates that the context MUST be removed immediately.

The "lifetime" element is a duration value that is specified in the same fashion as the "responseTime" attribute.

This value MUST be added to the current time when received by the LS to determine the time at which the context expires. An LS MAY use any value less than or equal to this value, but MUST NOT use a longer value. The actual expiry time of the context MUST be indicated in the context response.

5.7. "rules" Parameter

The "rules" element contains the authorization policy of the Target that dictates how and to whom LI is provided by the LS. This policy

MUST be applied by the LS when providing LI to LRs.

Authorization policies MUST conform to [I-D.ietf-geopriv-common-policy]. If the authorization policy is invalid, cannot be retrieved, or is otherwise not understood by the LS, the LG SHOULD fail the request. Note that this implies that the LS SHOULD attempt to retrieve an authorization policy that is provided by-reference at the time of a create context request; however, an LS MAY choose to do this later, if the requested response time might be exceeded.

In the absence of an authorization policy, the LS MUST NOT provide LI to any LR. Note that in certain jurisdictions an LS might be required to provide LI to specific parties irrespective of the authorization policy, as mandated by legislation; for example, emergency services in some countries.

5.7.1. "rulesetURI" Parameter

The "rulesetURI" element contains a URI that references the Target's authorization policy. This URI should reference a document of type "application/auth-policy+xml" as defined in [I-D.ietf-geopriv-common-policy].

It is RECOMMENDED that a ruleset URI use the "https" scheme. It is anticipated that, to improve responsiveness and reduce network usage, an LS could cache an authorization policy, consistent with the rules specified by the Rule Holder. For instance, the Rule Holder could specified retention times using the "Expires" header in HTTP [RFC2616]. The impact of changes to authorization policies are discussed in Section 4.3.2.

5.7.2. Common Policy "ruleset" Parameter

The "ruleset" element, which is in the "urn:ietf:params:xml:ns:common-policy" namespace [I-D.ietf-geopriv-common-policy], allows for providing an authorization policy directly as part of a request.

5.8. "code" Parameter

All responses, except a PIDF-LO document, MUST contain a response code. The "code" attribute applies to the "error" and "contextResponse" messages.

The following response codes follow a three decimal form similar to that in HTTP [RFC2616] and SIP [RFC3261]:

200 (Success): This code indicates that the request was successful. This code MUST not be used for an error response.

201 (Context Terminated): This code indicates that the request to terminate a context was successful.

400 (Request Error): This code indicates that the request was badly formed in some fashion.

401 (XML Error): This code indicates that the XML content of the request was either badly formed or invalid.

402 (Authentication Error): This code indicates that the request either did not contain authentication information, or the authentication provided was not accepted.

403 (Asserted Location Error): This code indicates that the LI that was asserted in the request was not acceptable to the LG. This code is used when the "exact" attribute on the "assert" parameter is set to "true".

404 (Context Not Found): This code indicates that the context identified in the request was not found. This code MAY also be used if the password provided was incorrect.

500 (General LG Error): This code indicates that an unspecified error occurred at the LG.

501 (Location Unknown): This code indicates that the LG could not determine the location of the Device.

502 (Unsupported Message): This code indicates that the request was not supported or understood by the LG.

503 (Timeout): This code indicates that the LG could not satisfy the request within the time specified in the "requestTime" parameter.

504 (Cannot Provide LI Type): This code indicates that the LG was unable to provide LI of the type or types requested. This code is used when the "exact" attribute on the "locationType" parameter is set to "true".

Additional response codes within the x00 to x79 range MUST be specified in published RFCs; the range from x80 to x99 is reserved for private usage.

5.9. "message" Parameter

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

5.10. "context" Parameter

The "context" element includes information that is used to identify a context and control access to it. The context is identified by one or more Location URIs and a Device is granted a password which MUST be provided when accessing the context to update the information contained.

When a context is created, the LG provides a "contextResponse" message that contains the "context" element. This element contains all of the Location URIs that can be used for the context, a password, and an expiry time.

To update the details in a context, or reuse profile information stored in the context, the Device provides a "context" element. When identifying a context in this manner, the Device MUST provide only one Location URI and the password.

5.10.1. "locationURI" Parameter

The "locationURI" element includes a single Location URI. Each Location URI is allocated by the LS so that it is able to uniquely identify the context.

A "contextResponse" message contains any number of "locationURI" elements. It is RECOMMENDED that the LS allocate a Location URI for all schemes that it supports and that no scheme is present twice.

All "updateContext" request messages MUST contain only one "locationURI" element, which is all that is necessary to uniquely identify a context. The Device MAY select any of the Location URIs provided by the LS. Location URIs do not change over the lifetime of a context.

5.10.2. "password" Parameter

The "password" element carries a password that is used to access the context after it has been created. The LS generates this value when creating a context and the Device MUST use the exact same value when it wishes to access the context. This value acts as a shared secret between Device and LS.

The value of the password MAY be updated in the response to any "updateContext" message.

This element MAY contain any valid XML character data, within the constraints of the XML Schema "token" type.

5.10.3. "expires" Parameter

The "expires" attribute indicates the time at which the context created by the LS will expire. This attribute is included in the "contextResponse" message only.

Responses to create and update context requests MUST include the expiry time of the context. If the LS has expired a context in response to an update context request, this value SHOULD include a time in the past to avoid problems that could be caused by a slow clock in the Device.

5.11. "location" Parameter

The "location" parameter is a boolean attribute associated with the "createContext" or "updateContext" message. The default for this attribute is "false".

This parameter, when present and set to "true" indicates that the LG SHOULD include a PIDF-LO document in the "contextResponse" message. The success of any request that includes this parameter MUST NOT be affected by any error in providing a location; thus, if the LG is unable to include a PIDF-LO, it is only omitted from the response. If a "contextResponse" does not include a PIDF-LO, the Device can determine the reasons for failure by sending a separate "locationRequest".

6. XML Schema

This section gives the XML Schema Definition [W3C.REC-xmlschema-1-20041028] of the "application/held+xml" format. This is presented as a formal definition of the "application/held+xml" format. Note that the XML Schema definition is not intended to be used with on-the-fly validation of the presence XML document.

```
<?xml version="1.0"?>
<xs:schema
    targetNamespace="urn:ietf:params:xml:ns:geopriv:held"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:held="urn:ietf:params:xml:ns:geopriv:held"
    xmlns:pidf="urn:ietf:params:xml:ns:pidf"
    xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
    xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
    xmlns:cp="urn:ietf:params:xml:ns:common-policy"
    xmlns:gml="http://www.opengis.net/gml"
    xmlns:xml="http://www.w3.org/XML/1998/namespace"
    elementFormDefault="qualified"
    attributeFormDefault="unqualified">

  <xs:annotation>
    <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 HELD messages.
    </xs:documentation>
  </xs:annotation>

  <xs:import namespace="http://www.w3.org/XML/1998/namespace"/>
  <xs:import namespace="urn:ietf:params:xml:ns:pidf:geopriv10"/>
  <xs:import
      namespace="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"/>
  <xs:import namespace="urn:ietf:params:xml:ns:common-policy"/>
  <xs:import namespace="http://www.opengis.net/gml"/>
  <xs:import namespace="urn:ietf:params:xml:ns:pidf"/>

  <!-- Context Information -->
  <xs:complexType name="returnContextType">
    <xs:complexContent>
      <xs:restriction base="xs:anyType">
        <xs:sequence>
          <xs:element name="locationURI" type="xs:anyURI"
                      maxOccurs="unbounded"/>
          <xs:element name="password" type="xs:token"/>
        </xs:sequence>
```

```
          <xs:attribute name="expires" type="xs:dateTime"
                        use="required"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="usesContextType">
      <xs:complexContent>
        <xs:restriction base="xs:anyType">
          <xs:sequence>
            <xs:element name="locationURI" type="xs:anyURI"/>
            <xs:element name="password" type="xs:token"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <!-- Duration Type -->
    <xs:simpleType name="durationType">
      <xs:union>
        <xs:simpleType>
          <xs:restriction base="xs:decimal">
            <xs:minInclusive value="0.0"/>
          </xs:restriction>
        </xs:simpleType>
        <xs:simpleType>
          <xs:restriction base="xs:duration">
            <xs:minInclusive value="PT0S"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:union>
    </xs:simpleType>

    <xs:complexType name="pidfloProfileType">
      <xs:complexContent>
        <xs:restriction base="xs:anyType">
          <xs:sequence>
            <xs:element name="presentity" type="xs:anyURI"
                        nillable="true" minOccurs="0"/>
            <xs:choice minOccurs="0">
              <xs:element name="retentionExpiry" type="xs:dateTime"
                          nillable="true"/>
              <xs:element name="retentionInterval"
                          type="held:durationType" nillable="true"/>
            </xs:choice>
            <xs:element name="retransmission" type="xs:boolean"
                        minOccurs="0" nillable="true"/>
            <xs:element name="rulesetURI" type="xs:anyURI"
```

```
                        minOccurs="0" nillable="true"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="rulesType">
      <xs:choice minOccurs="0">
        <xs:element name="rulesetURI" type="xs:anyURI"/>
        <xs:element ref="cp:ruleset"/>
      </xs:choice>
    </xs:complexType>

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

    <xs:complexType name="locationTypeType">
      <xs:simpleContent>
        <xs:extension base="held:locationTypeBase">
          <xs:attribute name="exact" type="xs:boolean"
                        use="optional" default="false"/>
        </xs:extension>
      </xs:simpleContent>
    </xs:complexType>

    <!-- Location Assertion -->
    <xs:complexType name="locationAssertionType">
      <xs:complexContent>
```

```
        <xs:restriction base="xs:anyType">
          <xs:choice>
            <xs:element ref="ca:civicAddress"/>
            <xs:sequence>
              <xs:element ref="gml:_Geometry"/>
              <xs:element ref="ca:civicAddress" minOccurs="0"/>
            </xs:sequence>
          </xs:choice>
          <xs:attribute name="method" type="xs:token"/>
          <xs:attribute name="timestamp" type="xs:dateTime"/>
          <xs:attribute name="expires" type="xs:dateTime"/>
          <xs:attribute name="exact" type="xs:boolean"
                        use="optional" default="false"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

    <!-- Response code -->
    <xs:simpleType name="codeType">
      <xs:restriction base="xs:nonNegativeInteger">
        <xs:pattern value="[0-5][0-9][0-9]"/>
      </xs:restriction>
    </xs:simpleType>

    <!-- Message Definitions -->
    <xs:complexType name="baseRequestType">
      <xs:complexContent>
        <xs:restriction base="xs:anyType">
          <xs:sequence/>
          <xs:attribute name="responseTime" type="held:durationType"
                        use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>

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

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

    <!-- Create Context -->
    <xs:complexType name="createContextType">
      <xs:complexContent>
        <xs:extension base="held:baseRequestType">
          <xs:sequence>
            <xs:element name="lifetime" type="held:durationType"/>
            <xs:element name="profile" type="held:pidfloProfileType"
                        minOccurs="0"/>
            <xs:element name="rules" type="held:rulesType"
                        minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax"
                    minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="location" type="xs:boolean"
                        default="false"/>
        </xs:extension>
      </xs:complexContent>
    </xs:complexType>

    <xs:element name="createContext" type="held:createContextType"/>

    <!-- Context Response -->
    <xs:complexType name="contextResponseType">
      <xs:complexContent>
        <xs:extension base="held:baseResponseType">
          <xs:sequence>
            <xs:element name="context" type="held:returnContextType"
                        minOccurs="0"/>
            <xs:element ref="pidf:presence" minOccurs="0"/>
          </xs:sequence>
        </xs:extension>
      </xs:complexContent>
    </xs:complexType>

    <xs:element name="contextResponse"
                type="held:contextResponseType"/>

    <!-- Update Context -->
    <xs:complexType name="updateContextType">
      <xs:complexContent>
        <xs:extension base="held:baseRequestType">
          <xs:sequence>
            <xs:element name="context" type="held:usesContextType"/>
            <xs:element name="lifetime" type="held:durationType"
                        minOccurs="0"/>
            <xs:element name="profile" type="held:pidfloProfileType"
```

```
                        minOccurs="0"/>
            <xs:element name="rules" type="held:rulesType"
                        minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax"
                    minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="location" type="xs:boolean"
                        default="false"/>
        </xs:extension>
      </xs:complexContent>
    </xs:complexType>

    <xs:element name="updateContext" type="held:updateContextType"/>

    <!-- ... response to updateContext is contextResponse -->

    <!-- Location Request -->
    <xs:complexType name="locationRequestType">
      <xs:complexContent>
        <xs:extension base="held:baseRequestType">
          <xs:sequence>
            <xs:choice minOccurs="0">
              <xs:element name="locationType"
                          type="held:locationTypeType"/>
              <xs:element name="assert"
                          type="held:locationAssertionType"/>
            </xs:choice>
            <xs:choice minOccurs="0">
              <xs:element name="context" type="held:usesContextType"/>
              <xs:element name="profile"
                          type="held:pidfloProfileType"/>
            </xs:choice>
            <xs:any namespace="##other" processContents="lax"
                    minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="signed" type="xs:boolean"
                        use="optional" default="false"/>
        </xs:extension>
      </xs:complexContent>
    </xs:complexType>

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

  </xs:schema>
```

7. HTTP Binding

This section defines an HTTP [RFC2616] binding for this protocol, which all conforming implementations MUST support. This binding takes the form of a Web Service (WS) that can be described by the Web Services Description Language (WSDL) document in Section 7.1.

The three request messages are carried in this binding as the body of an HTTP POST request. The MIME type of both request and response bodies should be "application/held+xml", except that a PIDF-LO document SHOULD have the MIME type "application/pidf+xml".

The LG populates the HTTP headers so that they are consistent with the contents of the message. In particular, the "Expires" and cache control headers are used to control the caching of any PIDF-LO document. The HTTP status code SHOULD have the same first digit as any "contextResponse" or "error" body included, and it SHOULD indicate a 2xx series response when a PIDF-LO document is included.

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

This binding MUST use TLS as described in [RFC2818]. TLS provides message integrity and privacy between Device and LG. The LG MUST use the server authentication method described in [RFC2818]; the Device MUST fail a request if server authentication fails, except in the event of an emergency.

7.1. HTTP Binding WSDL

The following WSDL 2.0 [W3C.CR-wsdl20-20060106] document describes the HTTP binding for this protocol. Actual service instances MUST provide a "service" with at least one "endpoint" that implements the "heldHTTP" binding. A service description document MAY include this schema directly or by using the "import" or "include" directives.

```
<?xml version="1.0"?>
<wsdl:definitions
    xmlns:wsdl="http://www.w3.org/2005/05/wsdl"
    xmlns:whttp="http://www.w3.org/2005/05/wsdl/http"
    xmlns:held="urn:ietf:params:xml:ns:geopriv:held"
    xmlns:pidf="urn:ietf:params:xml:ns:pidf"
    xmlns:heldhttp="urn:ietf:params:xml:ns:geopriv:held:http"
    targetNamespace="urn:ietf:params:xml:ns:geopriv:held:http"
    type="http://www.w3.org/2005/05/wsdl/http">
```

```
    <wsdl:documentation>
      This document describes the basic HELD web service.
      Please refer to RFCXXXX for details.
   [[NOTE TO RFC-EDITOR: Please replace XXXX with the RFC number
     for this specification and remove this note.]]
     </wsdl:documentation>

     <wsdl:types>
       <xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
         <xsd:import namespace="urn:ietf:params:xml:ns:geopriv:held"
                     schemaLocation="held.xsd"/>
         <xsd:import namespace="urn:ietf:params:xml:ns:pidf"/>
       </xsd:schema>
     </wsdl:types>

     <wsdl:interface name="held">

       <wsdl:operation name="createContext" method="POST">
         <wsdl:input message="held:createContext"/>
         <wsdl:output message="held:contextResponse"/>
         <wsdl:fault message="held:error"/>
       </wsdl:operation>

       <wsdl:operation name="updateContext" method="POST">
         <wsdl:input message="held:updateContext"/>
         <wsdl:output message="held:contextResponse"/>
         <wsdl:fault message="held:error"/>
       </wsdl:operation>

       <wsdl:operation name="locationRequest" method="POST">
         <wsdl:input message="held:locationRequest"/>
         <wsdl:output ref="pidf:presence"/>
         <wsdl:fault message="held:error"/>
       </wsdl:operation>

       <wsdl:operation
           name="getLocation" method="GET"
           pattern="http://www.w3.org/2004/08/wsdl/out-only">
         <wsdl:output ref="pidf:presence"/>
         <wsdl:fault message="held:error"/>
       </wsdl:operation>

     </wsdl:interface>

     <wsdl:binding name="heldHTTP" whttp:defaultMethod="POST">
     <wsdl:operation ref="heldhttp:createContext"
           whttp:inputSerialization="application/held+xml"
           whttp:outputSerialization="application/held+xml"
```

```
          whttp:faultSerialization="application/held+xml"/>
      <wsdl:operation ref="heldhttp:updateContext"
          whttp:inputSerialization="application/held+xml"
          whttp:outputSerialization="application/held+xml"
          whttp:faultSerialization="application/held+xml"/>
      <wsdl:operation
          ref="heldhttp:locationRequest"
          whttp:inputSerialization="application/held+xml"
          whttp:outputSerialization="application/pidf+xml"
          whttp:faultSerialization="application/held+xml"/>
      <wsdl:operation
          ref="heldhttp:getLocation"
          whttp:method="GET"
          whttp:inputSerialization="application/held+xml"
          whttp:outputSerialization="application/pidf+xml"
          whttp:faultSerialization="application/held+xml"/>
    </wsdl:binding>

  </wsdl:definitions>
```

8. Security Considerations

The threat model for this protocol assumes that the LG exists within the same administrative domain as the Device. The LG requires access to network information so that it can determine LI. Therefore, the LG can use network information to protect against a number of the possible attacks.

An in-depth discussion of the security considerations applicable to the use of Location URIs and by-reference provision of LI is included in [I-D.winterbottom-location-uri].

8.1. Return Routability

It is RECOMMENDED that Location Generators use return routability rather than requiring Device authentication. Device authentication SHOULD NOT be required due to the administrative challenge of issuing and managing of client credentials, particularly when networks allow visiting users to attach devices. However, the LG MAY require any form of authentication as long as these factors are considered, in particular see Section 6.3.2 of [I-D.winterbottom-location-uri].

Addressing information used in a request to the LG is used to determine the identity of the Device, and to address a response. This ensures that a Device can only request its own LI.

A temporary spoofing of IP address could mean that a device could request a Location URI that would result in another Device's location. One or more of the follow approaches are RECOMMENDED to limit this exposure:

- Location URIs SHOULD have a limited lifetime, that is, the LG SHOULD enforce a maximum value for the lifetime element (Section 5.6).

- The network SHOULD have mechanisms that protect against IP address spoofing.

- The LG SHOULD ensure that requests can only originate from within its administrative domain.

- The LG and network SHOULD be configured so that the LG is made aware of Device movement within the network and addressing changes. If the LG and LS detect a change in the network that invalidates a context, the context MUST be terminated.

The above measures are dependent on network configuration and SHOULD be considered with circumstances in mind. For instance, in a fixed

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

An identity association can also be used to guard against the theft of a Location URI, as described in [I-D.winterbottom-location-uri].

8.2. Transaction Layer Security

All bindings for this protocol MUST ensure that messages are adequately protected against eavesdropping and modification. Bindings MUST also provide a means of authenticating the LG.

It is RECOMMENDED that all bindings also use TLS [RFC2246].

For the HTTP binding, TLS MUST be used. TLS provides protection against eavesdropping and modification. The server authentication methods described in HTTP on TLS [RFC2818] MUST be used.

8.3. Veracity of Asserted LI

The assert element (Section 5.2) allows a Device the ability to provide LI. However, if an LG uses asserted LI, it is the LG that becomes responsible for the veracity of that information. Therefore, when the Device provides LI in a request, the LG MUST NOT use this information unless it can ensure its accuracy. This prevents the fraudulent provision of LI that could be caused by the LG accepting LI without any checks.

It is unlikely that an LG is able to verify Device-provided LI beyond any uncertainty. The ability of an LG to verify LI is limited by its own capacity to determine the location of the Device. The LG SHOULD indicate the source of LI using the PIDF-LO "method" parameter so that users of LI can make appropriate judgments on its veracity.

9. Examples

9.1. Simple HTTP Binding Example Messages

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

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

```
GET /location HTTP/1.1
Host: lg.example.com
Accept: application/pidf+xml,application/held+xml,application/xml;q=0.8,
    text/xml;q=0.7
Accept-Charset: UTF-8,*
```

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

```
POST /location HTTP/1.1
Host: lg.example.com
Accept: application/pidf+xml,application/held+xml,application/xml;q=0.8,
    text/xml;q=0.7
Accept-Charset: UTF-8,*
Content-Type: application/held+xml
Content-Length: 87

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

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

```
HTTP/1.x 200 OK
Server: Example LG
Date: Tue, 10 Jan 2006 03:42:29 GMT
Expires: Tue, 10 Jan 2006 03:42:29 GMT
Cache-control: private
Content-Type: application/pidf+xml
Content-Length: 594

<?xml version="1.0"?>
<presence xmlns="urn:ietf:params:xml:ns:pidf"
          entity="pres:3650n87934c@ls.example.com">
  <tuple id="3b650sf789nd">
  <status>
   <geopriv xmlns="urn:ietf:params:xml:ns:pidf:geopriv10">
     <location-info>
       <Point xmlns="http://www.opengis.net/gml"
              srsName="urn:ogc:def:crs:EPSG::4326">
         <pos>-34.407 150.88001</pos>
       </Point>
     </location-info>
     <usage-rules>
       <retention-expires>
         2006-01-11T03:42:28+00:00</retention-expires>
     </usage-rules>
   </geopriv>
  </status>
  <timestamp>2006-01-10T03:42:28+00:00</timestamp>
  </tuple>
</presence>
```

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

```
HTTP/1.x 500 Server Error
Server: Example LG
Date: Tue, 10 Jan 2006 03:49:20 GMT
Expires: Tue, 10 Jan 2006 03:49:20 GMT
Cache-control: private
Content-Type: application/held+xml
Content-Length: 135

<?xml version="1.0"?>
<error xmlns="urn:ietf:params:xml:ns:geopriv:held" code="501"
       message="Unable to determine location"/>
```

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

9.2. Location Request Examples

The location request shown below specifies location types and provides a profile that the LG applies to the PIDF-LO document. The request specifies that a response is desired within 10.5 seconds.

```
<locationRequest xmlns="urn:ietf:params:xml:ns:geopriv:held"
                 responseTime="PT10.5S" signed="false">
  <locationType exact="true">
    jurisdictionalCivic
    geodetic
  </locationType>
  <profile>
    <presentity>pres:user@example.com</presentity>
    <retentionInterval>1800</retentionInterval>
    <retransmission>false</retransmission>
    <rulesetURI>https://example.com/~user/ruleset.xml</rulesetURI>
  </profile>
</locationRequest>
```

The response to this location request is the following PIDF-LO document, which shows how the profile values are applied.

```
<presence xmlns="urn:ietf:params:xml:ns:pidf"
          entity="pres:user@example.com">
  <tuple id="dtnv49a3c08ud35q">
  <status>
   <geopriv xmlns="urn:ietf:params:xml:ns:pidf:geopriv10">
     <location-info>
       <civicAddress
           xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
         <!-- Jurisdictional Civic LI here -->
       </civicAddress>
       <Point xmlns="http://www.opengis.net/gml">
         <!-- Geodetic LI here -->
       </Point>
     </location-info>
     <usage-rules>
       <retransmission-allowed>false</retransmission-allowed>
       <retention-expires>
         2006-01-11T03:42:28+00:00</retention-expires>
       <ruleset-reference>
         https://example.com/~user/ruleset.xml
       </ruleset-reference>
     </usage-rules>
   </geopriv>
  </status>
  <timestamp>2006-01-10T03:42:28+00:00</timestamp>
  </tuple>
</presence>
```

The following location request includes a location assertion that includes a user-provided civic address. This message also requests that the LG retrieve profile information from a context that exists on an LS.

```
<locationRequest xmlns="urn:ietf:params:xml:ns:geopriv:held"
                 responseTime="2">
  <assert method="Manual" exact="true">
    <civicAddress
        xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
        xml:lang="en-AU">
      <!-- civic address contents -->
    </civicAddress>
  </assert>
  <context>
    <locationURI>
      https://ls.example.com:9768/357yc6s64ceyoiuy5ax3o
    </locationURI>
    <password>vs76e8cae9873a079888p9y4txwa</password>
  </context>
</locationRequest>
```

Since this request includes the "exact" parameter set to "true", any successful response MUST include the provided LI.

9.3. Context Creation and Update Examples

The following create context request shows the simplest form of this message, which sets a two hour lifetime on the context and includes a "rulesetURI" element for the LS.

```
<createContext xmlns="urn:ietf:params:xml:ns:geopriv:held">
  <lifetime>PT2H</lifetime>
  <rules>
    <rulesetURI>
      https://www.example.com/~user/privacy/ruleset.xml
    </rulesetURI>
  </rules>
</createContext>
```

The following more complex create context request includes additional information. This includes a profile that sets the presentity and some of the "usage-rules" components in the PIDF-LO that the LS serves.

```
<createContext xmlns="urn:ietf:params:xml:ns:geopriv:held">
  <lifetime>PT2H</lifetime>
  <profile>
    <presentity>pres:user@example.com</presentity>
    <retentionExpiry>2006-01-13T12:00:00+00:00</retentionExpiry>
    <retransmission>false</retransmission>
  </profile>
  <rules>
    <rulesetURI>
      https://www.example.com/~user/privacy/ruleset.xml
    </rulesetURI>
  </rules>
</createContext>
```

A typical successful response to this message provides several Location URIs in different schemes (in this case: "https" and "sips"), the exact context expiry time, and a password that can be used to update the context.

```
<contextResponse xmlns="urn:ietf:params:xml:ns:geopriv:held"
                 code="200" message="OK">
  <context expires="2006-01-11T05:38:01+00:00">
    <locationURI>
      https://ls.example.com:9768/357yc6s64ceyoiuy5ax3o
    </locationURI>
    <locationURI>
      sips://ls.example.com:9769/357yc6s64ceyoiuy5ax3o
    </locationURI>
    <password>38cdj38mjcd-0-=54821kj28mp1qms.1</password>
  </context>
</contextResponse>
```

If any aspect of the data stored in a context changes, a "contextUpdate" request is sent to the LG to request that it update the information. This request includes the information necessary to access a context (the location URI and password) and only the information that has changed.

The following request demonstrates how information stored in a context could be updated. For the context previously created, this provides the "retentionInterval" element, which overrides a previously configured "retentionExpiry" value.

```
<updateContext xmlns="urn:ietf:params:xml:ns:geopriv:held"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <context>
    <locationURI>
      https://ls.example.com:9768/357yc6s64ceyoiuy5ax3o
    </locationURI>
    <password>38cdj38mjcd-0-=54821kj28mp1qms.1</password>
  </context>
  <profile>
    <retentionInterval>600</retentionInterval>
  </profile>
</updateContext>
```

To indicate success, the LG provides a "contextResponse" identical in form to the original request.

The following request shows that a context lifetime can be extended or shortened by the Device by updating a context with a new "lifetime" element. The following message requests that the LS maintain the context for two hours beyond the current time.

```
<updateContext xmlns="urn:ietf:params:xml:ns:geopriv:held">
  <context>
    <locationURI>
      https://ls.example.com:9768/357yc6s64ceyoiuy5ax3o
    </locationURI>
    <password>38cdj38mjcd-0-=54821kj28mp1qms.1</password>
  </context>
  <lifetime>PT2H</lifetime>
</updateContext>
```

The response to a request to extend the context includes the new expiry time of the context, if it has changed.

```
<contextResponse xmlns="urn:ietf:params:xml:ns:geopriv:held"
                 code="200" message="OK">
  <context expires="2006-01-11T05:39:46+00:00">
    <locationURI>
      https://ls.example.com:9768/357yc6s64ceyoiuy5ax3o
    </locationURI>
    <locationURI>
      sips://ls.example.com:9769/357yc6s64ceyoiuy5ax3o
    </locationURI>
    <password>38cdj38mjcd-0-=54821kj28mp1qms.1</password>
  </context>
</contextResponse>
```

A zero value for the "lifetime" element terminates the context. The following request terminates the context.

```
<updateContext xmlns="urn:ietf:params:xml:ns:geopriv:held">
  <context>
    <locationURI>
      https://ls.example.com:9768/357yc6s64ceyoiuy5ax3o
    </locationURI>
    <password>38cdj38mjcd-0-=54821kj28mp1qms.1</password>
  </context>
  <lifetime>PT0S</lifetime>
</updateContext>
```

The response to a message that requests the termination of a context appears as follows.

```
<contextResponse xmlns="urn:ietf:params:xml:ns:geopriv:held"
                 code="201" message="Context removed"/>
```

9.4. Sample LG WSDL Document

The following WSDL document demonstrates how a WSDL document can be created for a specific service, in this case, a service at the URI "https://lg.example.com/location".

```
<?xml version="1.0"?>
<wsdl:definitions
    xmlns:wsdl="http://www.w3.org/2005/05/wsdl"
    xmlns:heldhttp="urn:ietf:params:xml:ns:geopriv:held:http"
    targetNamespace="http://lg.example.com/ws/held">

  <wsdl:import
      namespace="urn:ietf:params:xml:ns:geopriv:held:http"/>

  <wsdl:service name="sample-held-svc" interface="heldhttp:held">
    <wsdl:endpoint name="sample-held-ep"
                   binding="heldhttp:heldHTTP"
                   address="https://lg.example.com/location"/>
  </wsdl:service>

</wsdl:definitions>
```

10. IANA Considerations

According to the guidelines in [RFC3688], this document calls for an IANA registry for result codes and registers an XML namespace and schema. It also registers the "application/held+xml" MIME type.

10.1. IANA Registry for HELD Result Codes

IANA will establish and maintain a registry of HELD result codes. Additional values are registered based on the "specification required" option in [RFC3688].

Specifications MUST specify the following information when registering new values in this registry:

Code Value: A three-digit value from 000 to 679. The last 20 codes in each block of 100 (from x80 to x99) are reserved for private or experimental use and cannot be registered.

Short Message: A brief message that describes the general reason for the code.

Publication: A reference to any relevant publication or specification.

Description and Usage: A longer description of the code and the circumstances where it applies. This description does not need to be exhaustive.

The values in Section 5.8 are pre-registered in this registry.

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

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

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

Registrant Contact: IETF, GEOPRIV working group, (geopriv@ietf.org), Martin Thomson (martin.thomson@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 Messages</title>
            </head>
            <body>
              <h1>Namespace for HELD Messages</h1>
              <h2>urn:ietf:params:xml:ns:geopriv:held</h2>
  [[NOTE TO IANA/RFC-EDITOR: Please update RFC URL and replace XXXX
      with the RFC number for this specification.]]
              <p>See <a href="[[RFC URL]]">RFCXXXX</a>.</p>
            </body>
          </html>
        END
```

10.3. XML Schema Registration

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

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

Registrant Contact: IETF, GEOPRIV working group, (geopriv@ietf.org), Martin Thomson (martin.thomson@andrew.com).

Schema: The XML for this schema can be found as the entirety of Section 6 of this document.

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

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

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

Registrant Contact: IETF, GEOPRIV working group, (geopriv@ietf.org), Martin Thomson (martin.thomson@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 HTTP Binding WS</title>
            </head>
            <body>
              <h1>Namespace for HELD HTTP Binding WS</h1>
              <h2>urn:ietf:params:xml:ns:geopriv:held:http</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
```

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

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

To: ietf-types@iana.org

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

MIME media type name: application

MIME subtype name: held+xml

Required parameters: (none)

Optional parameters: charset
Indicates the character encoding of enclosed XML. Default is UTF-8.

Encoding considerations: Uses XML, which can employ 8-bit characters, depending on the character encoding used. See RFC 3023 [RFC3023], section 3.2.

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

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

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

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

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

Person & email address to contact for further information: Martin Thomson <martin.thomson@andrew.com>

Intended usage: LIMITED USE

Author/Change controller: This specification is TBD

Other information: This media type is a specialization of application/xml [RFC3023], and many of the considerations described there also apply to application/held+xml.

11. References

11.1. Normative References

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

[RFC2246] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

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

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

[RFC3275] Eastlake, D., Reagle, J., and D. Solo, "(Extensible Markup Language) XML-Signature Syntax and Processing", RFC 3275, March 2002.

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

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

[RFC4119] Peterson, J., "A Presence-based GEOPRIV Location Object Format", RFC 4119, December 2005.

[I-D.ietf-geopriv-revised-civic-lo] Thomson, M. and J. Winterbottom, "Revised Civic Location Format for PIDF-LO", draft-ietf-geopriv-revised-civic-lo-04 (work in progress), September 2006.

[I-D.ietf-geopriv-pdif-lo-profile] Tschofenig, H., "GEOPRIV PIDF-LO Usage Clarification, Considerations and Recommendations", draft-ietf-geopriv-pdif-lo-profile-04 (work in progress), May 2006.

[I-D.winterbottom-geopriv-held-dhcp-discovery] Winterbottom, J. and M. Thomson, "HELD Service Discovery using DHCP", draft-winterbottom-geopriv-held-dhcp-discovery-00 (work in progress), October 2006.

[I-D.thomson-geopriv-held-unaptr]

Thomson, M. and J. Winterbottom, "U-NAPTR Discovery for HELD Services", draft-thomson-geopriv-held-unaptr-00 (work in progress), October 2006.

[W3C.REC-xmlschema-2-20041028]
Biron, P. and A. Malhotra, "XML Schema Part 2: Datatypes Second Edition", World Wide Web Consortium Recommendation REC-xmlschema-2-20041028, October 2004, <http://www.w3.org/TR/2004/REC-xmlschema-2-20041028>.

[OGC.GML-3.1.1]
Cox, S., Daisey, P., Lake, R., Portele, C., and A. Whiteside, "Geographic information - Geography Markup Language (GML)", OpenGIS 03-105r1, April 2004, <http://portal.opengeospatial.org/files/?artifact_id=4700>.

11.2. Informative References

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

[RFC2222] Myers, J., "Simple Authentication and Security Layer (SASL)", RFC 2222, October 1997.

[RFC2778] Day, M., Rosenberg, J., and H. Sugano, "A Model for Presence and Instant Messaging", RFC 2778, February 2000.

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

[RFC3080] Rose, M., "The Blocks Extensible Exchange Protocol Core", RFC 3080, March 2001.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

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

[I-D.ietf-geopriv-common-policy]
Schulzrinne, H., "Common Policy: A Document Format for Expressing Privacy Preferences", draft-ietf-geopriv-common-policy-11 (work in progress), August 2006.

[I-D.winterbottom-location-uri]
Winterbottom, J., "Rationale for Location by Reference", draft-winterbottom-location-uri-01 (work in progress), January 2006.

[W3C.REC-xmlschema-1-20041028]
Thompson, H., Mendelsohn, N., Beech, D., and M. Maloney, "XML Schema Part 1: Structures Second Edition", World Wide Web Consortium Recommendation REC-xmlschema-1-20041028, October 2004, <http://www.w3.org/TR/2004/REC-xmlschema-1-20041028>.

[W3C.REC-soap12-part1-20030624]
Gudgin, M., Nielsen, H., Hadley, M., Mendelsohn, N., and J. Moreau, "SOAP Version 1.2 Part 1: Messaging Framework", World Wide Web Consortium Recommendation REC-soap12-part1-20030624, June 2003, <http://www.w3.org/TR/2003/REC-soap12-part1-20030624>.

[W3C.REC-soap12-part2-20030624]
Nielsen, H., Hadley, M., Mendelsohn, N., Moreau, J., and M. Gudgin, "SOAP Version 1.2 Part 2: Adjuncts", World Wide Web Consortium Recommendation REC-soap12-part2-20030624, June 2003, <http://www.w3.org/TR/2003/REC-soap12-part2-20030624>.

[W3C.CR-wsdl20-20060106]
Chinnici, R., Moreau, J., Ryman, A., and S. Weerawarana, "Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language", W3C CR CR-wsdl20-20060106, January 2006.

Appendix A. Acknowledgements

The authors would like to thank the following people for their contribution to this document (in alphabetical order): Nadine Abbott, Guy Caron, Martin Dawson, Jerome Grenier, Neil Justusson, Tat Lam, Patti McCalmont, Perry Prozeniuk, John Schnizlein, Henning Schulzrinne, Ed Shrum, and Hannes Tschofenig.

Authors' Addresses

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

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

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

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

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

Email: barbara.stark@bellsouth.com

Full Copyright Statement

Copyright (C) The Internet Society (2006).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

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